On the Applications of Blockchain-Enabled Distributed Ledger Technology in the Financial Industry

by

Brian Schroeder

Adviser: Brett Hemenway

EAS-499 Senior Capstone Thesis

School of Engineering and Applied Science

University of Pennsylvania

April 27, 2016

CONTENTS

1 INTRODUCTION

Since its introduction nearly 8 years ago, the Bitcoin cryptocurrency has seen explosive growth in adoption and value. It has been a catalyst for the launch of a plethora of alternative digital stores of value, and has generated immense buzz around the cryptocurrency space. Until recently, however, the technology core to Bitcoin—blockchain networks—received little attention on its own. Over the last two years this has rapidly changed as researchers, entrepreneurs, and large institutions alike look toward its promise to disrupt long-standing systems when applied outside cryptocurrencies. In particular, much of this interest has been driven by the financial industry, which sees potential to streamline existing infrastructure, benefitting our financial system through reduction in overall costs, more effective management of systemic risk, and the addition of much-needed transparency.

In this paper, we explore the evolution of what is widely referred to as distributed ledger technology and how it could impact the financial industry. In Section 2, we first briefly explain Bitcoin and how its underlying blockchain network functions. Section 3 separates the notion of blockchain from Bitcoin, and describes the characteristics that differentiate the possible types of blockchain networks. Section 4 builds upon that foundation, explaining some of the common consensus mechanisms used to keep such networks in synch. Section 5 provides a useful abstraction illustrating how blockchain networks can implement replicated, shared databases. Section 6 introduces smart contracts, and explains how they can add value to a shared ledger. Throughout, we compare blockchain-based implementations to traditional solutions and consider the tradeoffs between them. In Section 7, we discuss some of the ways in which distributed ledger technology can impact the financial industry, and in Section 8 we address the role regulators might play, either facilitating or hindering the realization of those applications.

2 BITCOIN – THE ORIGINAL BLOCKCHAIN NETWORK

History

In 2008, Satoshi Nakamoto[1] published a white paper describing a peer-to-peer electronic cash system that would allow payments to be remitted electronically, and directly, without the need of financial intermediaries, or trust between counterparties [1]. Nakamato's proposed system, known as Bitcoin, quickly became a reality, and has since had an immense impact on society. As of April 2016, the market capitalization of the Bitcoin cryptocurrency is estimated at over $7 billion [2].

This paper focuses on the technology underlying cryptocurrencies, and how that technology will be applied outside that space. As a foundation for our analysis, we begin with a high-level description of how Bitcoin works. Although the real-world implementation of the Bitcoin system is highly complex and has evolved over time, Nakamoto's original paper provides a sufficient sketch that defines core concepts and illustrates its basic functionality.

How Does Bitcoin Work?

Every decentralized electronic cash system faces the following problem: with no central authority or premise of trust between nodes, how can all participants in the network agree on a singular truth regarding who owns what?

At its core, Bitcoin provides a method for the distributed computation of a public ledger. This ledger is composed of a sequence of transactions, where a Bitcoin transaction is a message stating that one owner of bitcoin has authorized the transfer of some amount to a new owner.

Every transaction on the Bitcoin network is broadcast publicly, transactions that have been verified are grouped into blocks, and the complete history of such transactions is maintained in a public ledger known as the "blockchain". New blocks are added to the blockchain through the "mining process," further described below.

The Bitcoin blockchain serves as the authoritative ledger of every transaction that has taken place on the network, and thus the record of all bitcoin ownership.

Transactions: At a high level, a Bitcoin transaction consists of one or more inputs, one or more outputs, and a digital signature proving ownership of each of the aforementioned inputs. A transaction input is generally a reference to some unspent transaction output from a previous transaction. A transaction output, on the other hand, takes the form of a script that assigns a new owner to the input value by associating it with a destination key, called an encumbrance. The value transferred by a transaction may only be redeemed by presenting its output script with a valid digital signature produced by the private key associated with the encumbrance. In other words, if Alice transfers one bitcoin to Bob, only someone with access to Bob's private key (namely Bob) can use that bitcoin.

Once constructed, a transaction must be broadcast to at least one other node on the peer-to-peer Bitcoin network. Next, the transaction is independently verified by each receiving node, and, if found to

[1] Satoshi Nakamoto is likely a pseudonym for the author or possible group of authors, and his true identity remains a source of intense speculation [42].

be valid, forwarded to more nodes until it has propagated to and been verified by all full participants of the network.

Mining: As new transactions are broadcast to the network, a subset of the nodes on the network, known as mining nodes, independently group such valid transactions into new blocks, and work to produce a solution to a cryptographic "puzzle" that serves as proof of computational expense—this is known as proof of work and will be described later. Mining serves two key purposes. Mining injects new bitcoin into circulation, while also securing the system against fraudulent or otherwise invalid transactions, such as attempts to spend the same bitcoin more than once (i.e., double-spending). Miners effectively spend processing power for the chance to earn newly minted bitcoin [as well as transaction fees] by working on "puzzles" whose solutions are computationally expensive to find, yet easy to verify as correct.

Miners are only rewarded for their work when a block they mine is included in the blockchain. This is because miners are rewarded via the inclusion of a generation transaction—a payment to him/herself—as the first transaction in a mined block. Since each block must be independently verified by every node on the network, miners, who bear real costs (e.g. electricity consumption), are incentivized to behave honestly and only broadcast valid blocks, as invalid ones will be rejected and thus not included in any chain.

Consensus: As mining nodes broadcast new blocks to the network, every node independently verifies each proof of work and appends valid blocks to a locally maintained chain. Every node independently selects the chain with the most cumulative demonstrated computation (typically the longest one) as the main chain—for mining nodes, this also means selecting the chain to extend in attempting to mine the next block, thus restarting the process.

In summary, the Bitcoin network is comprised of:

- A peer-to-peer network of nodes running the Bitcoin client
    - Any node may broadcast a transaction
    - Nodes collect transactions, and propagate valid ones
    - A subset of nodes acting as miners collect valid transactions into a block, find a proof of work for the block, and broadcast it to the network
    - Nodes accept the block if its proof of work is valid, and all transactions in it are valid and unspent
    - Nodes express this acceptance by working on creating the next block in the chain, and back-linking it to the accepted block
- Bitcoin blockchain ledger distributed among the nodes on the network
    - The chain with the most proof of work, generally the longest chain, is considered to be the valid ledger
    - This serves as the authenticated record of the history of the Bitcoin network's activity
    - From it, anyone can determine the full provenance of all bitcoin at any point in time

3 Other Types of Blockchain Networks

Though the blockchain ledger built up from the activity on the Bitcoin network records transfer of bitcoin ownership, blockchain ledgers are capable of storing arbitrary data as well. Thus, one can describe a general blockchain network as:

- A peer-to-peer network of nodes running a blockchain client
  - Nodes broadcast transactions, containing data
  - Nodes collect transactions, and propagate valid ones as defined by the rules set forth in the blockchain network's design
  - A subset of nodes acting as validators collect valid transactions into a block, and broadcast it to the network
  - Nodes accept the block if all transactions in it are valid
  - Nodes express this acceptance by working on creating the next block in the chain, and back-linking it to the accepted block
- Blockchain ledger distributed among the nodes on the network
  - Some consensus mechanism—a set of rules and processes to ensure convergence on a single truth about the data—determines which chain is considered to be the valid ledger
  - This serves as the authenticated record of the history of the network's activity
  - From it, anyone can determine the singular, true state of the data distributed on the network at any point in time

The Bitcoin protocol was designed to create a peer-to-peer system of "electronic cash" that is not reliant on any central party to facilitate the transfer of ownership [1]. That specific purpose, and its underlying assumptions and threat model, directly drive the design of the Bitcoin blockchain network. Although Bitcoin's blockchain network is the most well-known, it represents only one of several possible kinds. It is thus useful to define a framework for categorizing blockchain network implementations. For this paper, I will use two[2] of the four axes proposed by Arthur Breit in his blog post titled, "A Functional Nomenclature of Cryptographic Ledgers," which are as follows:

- Permissionless vs. Permissioned
- Tokenized vs. Tokenless

Permissionless vs. Permissioned

A blockchain network can be classified as permissionless or permissioned. In the latter case, the members of the network can restrict who is allowed to participate in its consensus mechanism. On the other hand, in a permissionless network, such as Bitcoin's, any member is allowed to participate in consensus, i.e., play the role of a validator.

Permissioned networks offer several practical benefits. A permissioned networks is inherently more performant than an otherwise identical permissionless one as there are simply fewer nodes performing

[2] We omit the other two axes Decentralized vs. Centralized and Distributed vs. Localized. In the context of the blockchain networks consider, a permissioned network is inherently centralized, and blockchain networks are distributed by nature.

validation computation. Further, permissioned networks are cheaper to maintain than permissionless networks for reasons related to spam control. While permissioned networks can rely on their access control layer to ignore submissions from unknown actors and hold known actors accountable for their malicious submissions, permissionless networks must rely on some alternate means of controlling spam. Most permissionless networks deter spam/bad acting through an economic incentive structure that makes it costly to submit blocks for inclusion on the chain (e.g., Bitcoin's intentionally expensive proofof work algorithm) [3].

Tokenized vs. Tokenless

A tokenized blockchain network is one that requires a native token—a digital asset tracked on the underlying ledger—to function. All cryptocurrency blockchain networks are tokenized, and the native token is the cryptocurrency itself (e.g., bitcoin on the Bitcoin network, and ethers on the Ethereum network). These tokens typically serve the dual purpose of incentivizing validators to secure the network through the issue of mining rewards, and preventing spam/denial-of-service by imposing small transaction fees. Tokenless blockchain networks do not rely on such economic incentives, and thus are only feasible in environments where the validators can be known and pre-approved so that other means of achieving consensus may be employed [4].

Today, it is generally agreed upon that tokens are not inherent to the benefits blockchain networks provide as distributed data stores. However, as an interesting aside, at this time last year the community hotly debated the possibility of tokenless blockchains, and their merits seemed far more uncertain. Though both sides of the argument saw the same potential for the use of blockchain networks, they vehemently disagreed on how those applications would take shape. The token maximalist camp argued that without tokens, there is no way to incentivize the decentralized validation function miners perform. Thus they proposed data should be stored on the Bitcoin blockchain (or sometimes more conservatively, on a Bitcoin-like tokenized blockchain) by encoding it in transaction metadata[345]. The opposition responded that tokens are only necessary in environments where consensus must be achieved through proof of work, and thus tokens are not required on permissioned blockchain networks where validators are known and can be incentivized through off-chain means such as contractual obligations[6].

[3] May 18, 2015 post by Adam Ludwin, CEO of Chain.com - https://medium.com/investing-2-0/wall-street-meet-block-chain-b2747909eb90#.exdjezk3f

[4] June 3, 2015 Nasdaq.com article by Martin Tiller - http://www.nasdaq.com/article/is-a-blockchain-without-bitcoin-possible-or-practical-cm482964

[5] December 17, 2015 Tiller revises stance - http://www.nasdaq.com/article/does-a-blockchain-without-bitcoin-harm-or-hurt-the-currency-cm556009

[6] June 5, 2015 post by Tim Swanson, Director of Market Research at R3 CEV - http://www.ofnumbers.com/2015/06/05/needing-a-token-to-operate-a-distributed-ledger-is-a-red-herring/

4 CONSENSUS MECHANISMS IN BLOCKCHAIN NETWORKS

Separate from the above categorization, a particular blockchain network implementation is also characterized by its choice of consensus mechanism. A consensus mechanism in a blockchain network is a set of rules and procedures in place to ensure that the validating nodes on the network, by independent choice/acceptance, eventually converge on selecting the same blockchain to extend. They impose a distribution over which node will submit the next block, and determine which one of all proposed blocks should be accepted and built upon moving forward.

Common Consensus Mechanisms

Proof of Work: A Proof of Work (PoW) consensus mechanism is one in which nodes accept as the next valid block the one with the most cumulative proof of computational work. Cumulative proof of work for a block is calculated by summing the target difficulties of that block, and every other block on the chain it extends. As Nakamoto describes, PoW allows for majority decision-making based on "one-CPU-one-vote."

In constructing a block (after selecting a set of valid transactions), a node performs a PoW algorithm based on Adam Back's Hashcash [5]. At a high level, this involves repeatedly computing a cryptographic hash[7] of some representation of the information contained in the block combined with an extra field, called a nonce. The nonce is initialized at 0 and is incremented after each hash, until the resulting hash's value is less than the target. This target is represented as a number, and thus decreasing that number increases the difficulty of finding a hash of lower value. Due to the property of the cryptographic hash functions used in PoW algorithms, there is no better way to find such a hash other than the brute force method described above.

The range of possible values the nonce can take on, holding the target difficulty fixed, determines the expected number of hashing iterations required to find a satisfying hash. A typical range for the nonce is $[0, 2^{32} - 1]$[8]. The large range of values which must be iterated over to find a satisfying proof makes PoW an expensive means of achieving consensus.

$$PoW \rightarrow hash(B, nonce) \leq D$$

Proof of Stake: A Proof of Stake (PoS) consensus mechanism is one in which nodes accept as the next valid block the one with the most cumulative proof of some notion of stake in the network[9]. In a typical crytocurrency network, stake is easily defined as some function of a user's ledger balance. In tokenless blockchain networks, stake can be represented through alternative means such as a time-locked deposit of some off-chain asset.

[7] A cryptographic hash function takes an arbitrary length message as input and outputs a fixed-length value. An effective hash function provides a one-way mapping from message to hash value in that there should be an extremely low probability of two different messages hashing to the same value (i.e., low probability of collision) [43].

[8] Bitcoin's current implementation uses a 32-bit nonce, allowing it to take on $2^{32} - 1 = 4{,}294{,}967{,}295$ possible values [44].

[9] There have been a number of proposed methods for block selection in PoS-based networks. See Bitfury's white paper, "Proof of Stake vs Proof of Work" for a more detailed explanation of each and the tradeoffs between them [6].

In constructing a block B on top of block B', a node with wallet address A, must perform a PoS algorithm. A typical implementation requires hashing B', A, and the UTC timestamp t until a value is found that is less than the target difficulty multiplied by the balance in A.

Most PoS implementations impose a restriction on the values t can take—for example, requiring that t differ by no more than one hour from the UTC timestamp on other network nodes allowing a range of $[UTC - 3600, UTC + 3600]$. Compared to PoW, PoS algorithms require far fewer hashing iterations to find a satisfying hash, and are thus a less expensive means of achieving consensus [6].

$$PoS \rightarrow hash(B', A, t) \leq balance(A) * D$$

Hybrid Approach: Tokenized blockchain networks utilizing PoS suffer from what is known as the initial distribution problem in that tokens must be in circulation on the network in order to use PoS consensus. To combat this, many use a hybrid approach wherein PoW is used during an initial period to create the initial token supply, and then PoS is used thereafter[10].

What Makes Sense on a Permissioned Network?

Proof of work should not be used as the consensus mechanism for a permissioned network. While PoW is a valid means to achieve emergent consensus, its design is intentionally inefficient so as to deter external attacks on the network. Specifically, PoW is a costly way to secure a blockchain network from (a) Sybil [7] (i.e., 51%) and (b) Denial-of-Service (DoS) attacks. PoW protects the network from these attack vectors by making it computationally (and thus economically) expensive for someone to (a) pseudonymously gain control over a majority of validating nodes on the network, or (b) flood the network with a large volume of transactions so as to prevent it from operating normally. Since the true identity of a node in a permissionless network is unknown, and thus its operator free from legal accountability, imposing economic cost provides the best way to discourage malicious behavior. In a permissioned environment, on the other hand, members of the network are restricted to a set of known entities—and in commercial settings, likely bound by legal obligation to behave honestly. Even if an attack were launched, the attacker would be identifiable and held accountable via some standard means (e.g., legal action). Thus, alternative consensus mechanisms will be used by the set of known validators in a permissioned blockchain network.

Tendermint (BFT-like[11]): Tendermint's consensus mechanism enforces a round-robin scheduling of which validators may propose blocks. Each validator has an account to which they are required to post collateral—the amount determines their voting power—that remains locked as long as they remain a validator (this collateral could be posted on-chain in a tokenized network, or the amount recorded on-chain but held elsewhere in tokenless networks). The frequency with which validators are assigned the role of proposer is in proportion to their voting power. Tendermint's protocol consists of running one or more voting-based rounds, each with up to five steps, until the next block at a given height is committed to the chain [8].

[10] Cryptocurrency BlackCoin's network uses this approach - http://blackcoin.co/#specs

[11] Based on traditional Byzantine Fault Tolerant algorithms that consist of rounds of explicit voting to achieve consensus

Proof of Elapsed Time (Nakamoto/Lottery-like[12]): Intel's "Sawtooth Lake" distributed ledger platform offers a consensus mechanism similar to that used on the Bitcoin network, in that it uses a lottery mechanism to determine which validator proposes the next block[13]. The Proof of Elapsed Time (PoET) consensus algorithm must be run in a trusted execution environment (TEE)[14] on each node. Under PoET, each potential validator calls a special function to request a timer, created by the TEE, which has an exponentially distributed random wait time. Validators run the timer assigned to them, and once the timer has expired, it produces a certificate proving that the validator waited the appropriate amount of time. Since a valid block must include the proof of elapsed time, the validator assigned the timer with shortest expiration wins the lottery and proposes the next block to the network. The other validators express their acceptance of the block by adding it to a chain of accepted blocks and proposing subsequent blocks that build upon it [9]. Overall, PoET is analogous to PoW, but replaces repeated computation with idle CPU cycles, making it less expensive to achieve consensus, assuming reliance on a TEE is not considered a practical cost.

[12] Based on a process that probabilistically selects a validator to propose the next block, for which network participants implicitly vote by accepting it as the next block to build upon

[13] The winner of the Bitcoin "lottery" is the miner who is first to find a valid proof of work for the next block.

[14] See Section 2 of GlobalPlatform's "The Trusted Execution Environment" white paper for explanation [45].

5 Permissioned Blockchain Networks as Replicated, Shared Databases

We have now defined abstractly what a blockchain network is, described the forms it can take, and explored some of the different protocols it can implement to achieve consensus over the data it houses on its underlying ledger. As the focus of this paper is enterprise use of blockchain networks in the financial services sector, the following analysis is restricted to permissioned blockchain network implementations[15].

Thus far, we have seen that blockchain networks allow multiple parties, with differing incentives, to collectively build and interact with a single, shared ledger [10]. In other words, blockchain networks enable shared databases with multiple non-trusting writers. However, there already exist a myriad of alternative shared database solutions that are well-tested, highly optimized, and have an entire service industry surrounding them that has been in place for decades. These include regular file storage, centralized databases, master-slave database replication, and multiple databases to which users can subscribe [11]. It is therefore worth exploring what benefits a blockchain-enabled solution offers over a traditional database system.

Traditional databases (i.e., modern relational databases) are repositories of structured information, organized into tables. Databases are modified via transactions, which are sets of changes to be made to the database that are accepted or rejected as a unit based on rules encoded in the database implementation. These rules—primarily in place to prevent programmer error—provide an answer to the question, "is the database in a valid state?" They can prevent malformed input from being entered into the database, but cannot exclude well-formed input that is simply incorrect. In an environment where the database is kept completely private (one entity can read from and write to it), such rules are sufficient. Further, they continue to suffice if one entity retains exclusive write access but multiple entities have read access. Shared writing can also work seamlessly when one entity owns a database and allows other entities to write to it. Bad activity on the part of the external writers is a non-issue as the owner can see, and if necessary reverse, the transactions they perform (and even revoke their access altogether).

Complexities arise when multiple entities want to share a database which none of the entities control, can be written to by any entity, and can be relied upon by all entities [12]. The traditional solution has been to use a trusted intermediary that maintains a central database, provisions access to all entities involved, and ensures the validity of operations with respect to known and agreed upon rules. This solution has its downsides in practice, especially in the financial services industry, as each entity still maintains a local copy of the data (the trusted intermediary isn't *that* trusted), and thus a lot of effort is spent on checking whether the local databases agree (i.e., reconciliation).

[15] It should be clear that permissionless blockchain networks are not suitable for use in that space for a multitude of reasons—at a minimum, it is reasonable to assume financial institutions require control over access to their data.

G. Greenspan argues that in order to avoid the use of a trusted intermediary, we need a suite of functionality, not supported by today's databases, that includes:

- A peer-to-peer network that allows transactions to be created by anyone, and that propagate quickly
- A means of identifying conflicts between transactions and resolving them automatically
- Synchronization technology to ensure consensus over the data
- A means of tying pieces of information to each entity, and the ability to enforce data ownership without a central authority
- A protocol for expressing transactional rules

In his words, "We need a whole bunch of new stuff for shared write databases to work, and it just so happens that blockchains provide them" [12]. So, at a minimum, blockchain networks can enable a real shared-write scenario. Further, blockchain network-enabled shared databases provide other key advantages including:

- Resiliency – Blockchain networks offer extreme fault tolerance through redundancy and use of peer-to-peer networks for data transmission.
- Verifiability – Transaction logs are not a byproduct of database modifications as they are in traditional systems, but rather are used to build the state of the data. Since blockchain networks utilize cryptographic authentication of time-stamped blocks, the entire network can be certain of its entire history [10].

Blockchain networks are not free from drawbacks. Compared to a centralized database solution, a blockchain-enabled shared database suffers from decreased [13]:

- Performance – Blockchain networks are inherently slower than centralized databases due to the burdens of signature verification, consensus mechanisms, and redundancy.
- Confidentiality – Many of the benefits of blockchains are due to the independent verification of every transaction by every node; this security comes at the cost of privacy. Centralized databases, on the other hand, need only impose restrictions on and house data in a single location. Read and write controls are implemented easily in centralized databases, whereas a blockchain is, at its core, only write-controlled. There are potential solutions to this problem (e.g., confidential transactions[16], zero-knowledge proofs[17]), but they come at the expense of computational burden.

[16] https://elementsproject.org/elements/confidential-transactions/
[17] https://z.cash/tech.html

6 Smart Contracts – Embedding Business Logic in the Blockchain

As explained above, blockchain networks can enable real shared-write databases in environments of limited trust. This can reduce costs arising from the redundancy of multiple entities maintaining and reconciling individual copies of a shared ledger, and save resources spent by central intermediaries on maintaining the trust of their clients via expensive protection mechanisms.

Another area suffering from inefficiency due to duplication of work is in developing business logic to govern data-driven, multi-party relationships. Each party to a mutual agreement must independently fulfill their obligations, and should be able to verify that their counterparties are doing the same. This is true regardless of whether they share the exact same view of the data, as would be the case if using a blockchain-based shared ledger—and especially true if they are not. Smart contracts, a concept introduced by Nick Szabo in 1997, offer the potential to eliminate such redundancies as well as provide increased verifiability and certainty of the performance of obligations arising from data-driven agreements [14]. Szabo's smart contract protocol relies on an abstract "mutually trusted virtual computer." In the context of blockchain networks, this takes the form of by a distributed virtual machine powered via the computation performed by each blockchain client in the network.

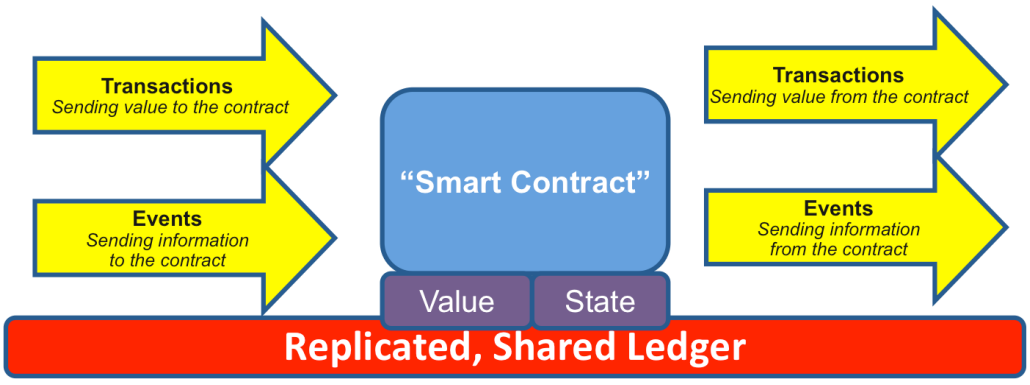
What is a Smart Contract?

While "smart contract" is the widely used and generally accepted term, it has its semantic downsides, and should probably be revised as it references something that is neither necessarily smart, nor necessarily a contract. Nonetheless, I will continue to use the term throughout the paper and will rely on Richard Brown's formal definition [15]:

> *"A smart-contract is an event-driven program, with state, which runs on a replicated, shared ledger and which can take custody over assets on that ledger."*

Brown envisions the process of creating a smart contract as follows:

1. In negotiation of an agreement, this agreement is formalized as computer code
2. Agree on information sources (external data), and how disputes will be resolved
3. Both parties examine and test the code to ensure that it satisfies the requirements of each
4. Deploy the code to a replicated, shared ledger



(Source: R. G. Brown [15])

How is a Smart Contract Different from Any Other Script?

Verifiability: Smart contracts are completely verifiable, whereas off-chain, general purpose scripts (e.g., a simple Ruby script) are only somewhat so. Without being able to observe the actual code of an ordinary script (assuming it is housed in a third-party environment), verification is typically limited to observing the outcome of its execution—it's a black box. Source code aside, the outcome of running a script can be altered by its execution environment (environment variables, language version, operating system, etc.) as well. In contrast, smart contracts are stored and ran entirely on the blockchain, meaning that not only is the source code verifiable, but so is every consequence of its execution.

Privacy: For the same reasons that smart contracts are more verifiable than ordinary scripts, they are also harder to keep private. Though there are potential solutions in development (see footnotes above regarding zero-knowledge proofs, etc.), none exists today that provides both privacy and verifiability [16].

Further Concerns

Technical Bugs: What happens when something goes wrong, or an unforeseen edge case leads to malfunction? Many of the aspects that make blockchain networks attractive also pose obstacles to their adoption—immutability is no exception. Once a smart contract is deployed to a shared ledger, no one party can unilaterally remove it or "turn it off," so to speak. This could be especially problematic in the event that a smart contract's incorrect execution asymmetrically affects the parties to the agreement it was designed to represent.

External Input: Most realistic use cases for smart contracts will likely rely on the existence of persistent and high-quality external data sources. While there are plausible methods of injecting real-world state as inputs to smart contracts[18], it might prove difficult to handle changes in the format, location, or quality of data sources for the same reasons that might inhibit general bug fixes (see above).

Legal Validity: Despite their name, smart contracts have no inherent notion of legal enforceability. Thus it is key to tie smart contracts to contracts at law. Eris Industries, a blockchain-based PaaS provider, encourages smart contract users to employ "Dual Integration" [17]. The result is a smart contract that references the hash of a real world contract, and a real world contract that references the fingerprint of the aforementioned smart contract. This ensures, to a cryptographic certainty, that the file containing the real world contract and the corresponding smart contract both reference each other. The dual integration process works as follows:

1. Deploy a smart contract
2. Reference the unique identity of the smart contract and the blockchain on which it resides in the real world contract
3. Finalize the real world contract, and generate its checksum
4. Send a transaction logging the checksum of the real world contract into the storage of the smart contract

[18] Brown offers "oracles" and "n-of-m" schemes as examples [15].

7 Potential for Blockchain + Smart Contract Solutions

We've shown conceptually that smart-contract enabled blockchain networks allow the implementation of distributed data-stores that are highly resilient, offer true shared-write capabilities, and can house verifiable business logic with reach extending across individual enterprises. As stated previously, I will focus on the financial industry in exploring the applications made possible by distributed ledger technology.

Why the Financial Industry?

Due to its scale[19], this industry is able to invest significant capital in developing the technology, and stands to gain large costs savings if distributed ledger technology lives up to its potential. Financial firms are particularly motivated to cut costs at this time as return on equity for financials has steadily declined in recent years, largely due to regulatory requirements [18]. Efficiency-based cost savings aside, distributed ledger technology may increase the ease with which firms can comply with regulators by adding transparency to the financial system. Moreover, as early adopter and primary investor, the financial industry will likely accelerate the maturation of distributed ledger technology for more general applications as well.

Why Now?

There has been a veritable media frenzy surrounding the purported potential for blockchain networks to completely transform the financial services industry. Technology-focused consulting firm Accenture has identified blockchains as "possibly the biggest opportunity [for banks] from taking an open approach to innovation," [19] and has even added a blockchain-specific practice to its portfolio [20].

Investment dollars have been pouring into this new space, going toward funding startups[20] developing blockchain-enabled shared database solutions, consortia[21] of banks experimenting with those solutions, and open source collaboration efforts[22] taking on a hybrid of those roles.

According to a September 2015 report, market research firm Aite Group estimates that investment in blockchain technology for capital markets applications, alone, will rise from $75mm in 2015 to $400mm in 2019 [21].

In a June 2015 report titled "The Fintech 2.0 Paper: rebooting financial services," Santander InnoVentures, the banking group's corporate venture arm, estimated that blockchain-enabled distributed ledgers could save banks $15-20 billion per year on cross border payments, securities trading, and regulatory compliance [22].

---

[19] The financial services industry represented 7.2% ($1.26 trillion) of United States GDP in 2014 - http://selectusa.commerce.gov/industry-snapshots/financial-services-industry-united-states

[20] Such startups range from generic PaaS providers such as Eris Industries (https://erisindustries.com/) to solution-specific providers such as Digital Asset (https://digitalasset.com/).

[21] The largest is R3 CEV (http://r3cev.com/), a blockchain technology firm that leads a growing consortium of over 40 financial institutions in exploring blockchain use in the financial industry.

[22] Housed under the non-profit Linux Foundation, the Hyperledger Project (https://www.hyperledger.org/) is a collaborative effort to develop a distributed ledger framework to be used across industries.

Year-to-date, there has scarcely been a day where there was not an announcement of a new partnership between a financial institution and blockchain service provider, or the completion of a trial evaluating a new use-case of blockchain networks. It should be noted that across conversations I have had with executives at some of the industry's largest financial institutions (banks, exchanges, settlement/clearing houses), there was a consistent sentiment that much of the publicly available information on blockchain technology implementation activity is better attributed to PR warfare than necessarily to tangible progress being made. This is not to say that financial institutions are not devoting significant research and development effort or not progressing down the path to implementation, but rather underscores the fact that the technology is rather nascent with its future applications shrouded in a large degree of uncertainty.

That said, the implementation of shared ledgers through smart contract-enabled blockchain networks has the potential to disrupt the operations of all major players in the industry. Changes will be rolled out gradually, and the industry is likely to follow an iterative approach to adoption—starting with the lowest hanging fruit, experimenting with evaluating performance of those initial applications, gauging the regulatory response, codifying lessons learned, and starting the cycle again.

Accenture provides a rough timeline (specific to investment banks, but there is no reason to believe that the other players will not follow a similar timeline) that generally corresponds to the standard diffusion of innovation framework [23]:

This is in agreement with the views offered in the aforementioned conversations I have had with key stakeholders in the industry—internal processes will be improved first, followed by markets in which automation and standardization are low, and ultimately trailed by large-scale reorganization of industry-wide infrastructure.

Post-trade Clearing and Settlement

With respect to financial markets, the most oft-cited use case in the news, consulting research reports, at conferences, and in other public forums is that of simplifying the current post-trade ecosystem. Over the last several decades, the financial industry has gradually built up a complex network of systems and service providers to process the increasing volume and complexity of financial transactions that take place each day. Michael Bodson, President and CEO of the Depository Trust and Clearing Corporation (DTCC)—arguably the firm most central to said network—admitted, himself, at a recent conference that "many parts of the system were not created through intentional architecture and design and, in some cases, has become unnecessarily complex as markets have evolved and become more global" [24]. Bodson is broadly referring to the infrastructure in place to handle all the processes and validations that must occur throughout the lifecycle of a trade, which is comprised of trade execution, clearing, and settlement.

Clearing occurs between the time a trade is executed (i.e., an agreement has been made between two or more parties to exchange assets) to the time at which the trade is considered settled (i.e., the obligations defined by the agreement have been fulfilled and the transfer of asset ownership irrevocably finalized). Clearing includes trade valuation, credit monitoring, risk and collateral management, netting, and failure handling [25]. The length of this cycle is defined relative to the date of the trade, and varies by asset class and market jurisdiction/location. For example, United States equities trade on a "T+3" cycle meaning that an equity trade must be settled no more than three business days following the initial execution of the trade. On the other hand, government securities operate on a T+1 settlement cycle [26].

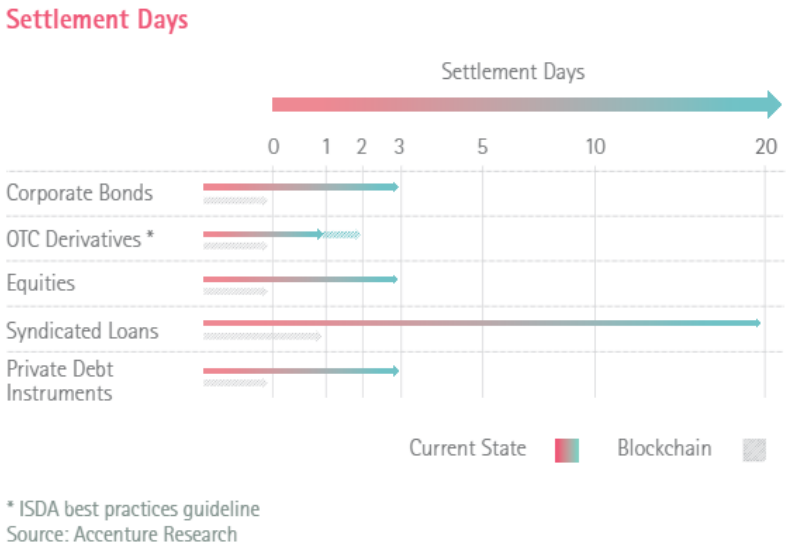
As described previously, smart contract-enabled blockchain solutions offer benefits through decentralization, disintermediation, and automation. In the context of the trade lifecycle, one can imagine a solution consisting of stacked layers of blockchain networks—each made up of nodes responsible for the corresponding stage of the lifecycle. Peters and Panayi describe a concrete example of how a trade might look in such a system [27]:

1. Buyer (and, independently, seller) submits an order through a broker to purchase (sell) an amount of some asset
2. The brokers create a transaction for the trade and submit it to the exchange-level blockchain network
3. Once the transaction is validated on the exchange network, another is created and submitted to the clearing-level blockchain network
4. Once that transaction is validated, by what is effectively a decentralized clearing house[23], a new transaction is created and submitted to the settlement-level blockchain network
5. Finally, once that transaction is validated by the members of the settlement network, the settling transaction is created and submitted—triggering the transfer of assets once confirmed

[23] The authors note that this eliminates the need for a central counterparty. While this may be true, CCPs play a critical role in stabilizing and removing systemic risk from the market. It remains to be seen whether blockchain networks can, or should, replace them completely.

Such an implementation underlies the promise of near-instantaneous (i.e., T+0) trade settlement through distributed ledger technology[24]. Whether through the use of blockchain technology or not, increasing the speed of the settlement cycle from days or weeks to seconds or minutes has major benefits. First, it mitigates counterparty risk between the time of trade execution and trade settlement—this will lead to a reduction in the margin required of members of clearing houses/consortiums. Even a one day reduction from a T+3 to T+2 cycle would imply a reduction in the average clearing fund requirement of 15% during typical periods and 24% in periods of high market volatility [28]. Those reductions are on the basis of approximately $4 billion per member, and thus imply a significant increase in the efficiency of capital deployment [29]. Second, it mitigates settlement risk—the risk of one leg of a transaction being completed while the other is not. Third, from a non-systemic standpoint, e.g., from that of an individual investor, shortening the settlement cycle simply provides access to the proceeds from a security sale sooner.

Of course, there is more to be gained (especially relative to what's at stake in the event of failure) by using a blockchain-enabled solution to trade some asset classes than for others [19]:



Whether a particular asset class is well-suited for trading on a distributed ledger will have to be evaluated on a case-by-case basis, and the economic benefits of such migrations weighed against the cost of better standardizing existing industry workflows to gain efficiency.

For example, improving equity market processes is not a likely first use-case. Equity markets are highly standardized, have huge volume[25], and require extremely low latency. Given the nascency of the technology, it is not yet clear that applying blockchain network solutions to equity markets will provide efficiencies outweighing explicit implementation costs and the potential for increased systemic risk. Further, the industry has already been exploring ways to shorten the cash equity settlement cycle since

[24] Perhaps more interesting than the possibility of instantaneous settlement is that of optimized, or on-demand, settlement. Whereas retail investors might desire the use of proceeds from a securities sale instantly, institutional investors might prefer a cycle long enough to allow netting of their trades to reduce transaction costs.
[25] The United States equity market traded over $41 trillion in 2015 - http://data.worldbank.org/indicator/CM.MKT.TRAD.CD

2012, and has developed an implementation roadmap, not dependent on distributed ledger technology, with expected completion by Q3 2017 [30].

However, there is some degree of consensus (across personal conversations with directors at large banks, industry-commissioned reports, announced commercial trials, etc.) pointing to a likely first candidate—improving the issuance, maintenance, and trading of syndicated loans. A syndicated loan is a loan provided to a single borrower by a group of lenders (i.e., the syndicate), generally structured, arranged, and administered by one or more commercial or investment banks (i.e., arrangers) [31]. Though the United States syndicated loan market is huge—representing $2.6 trillion across just under 5,000 transactions in 2015 [32]—it suffers from relatively immature standards and low automation. Syndicated loans are traded over-the-counter and have no central clearing house. Their T+20 settlement cycle leaves a lot of room for improvement, and the use of smart contracts could drastically reduce the cost to arrangers (and thus their clients) of maintaining syndicated loans' complex, tailor-made term structures.

Other Selected Use Cases

Industry Master Data Management: Master data is non-transactional information essential to a firm's operations. This can include information about entities, assets, business day and holidays, etc. Some master data is specific to an individual firm, while some is common across an industry. Generally, each firm has its own system of managing master data, and the industry lacks standards on technology, format, and symbology. DTCC lists basic industry master data as an "ideal candidate" for improvement using distributed ledger technology. Industry master data is used by the entire industry, by definition, and inconsistent views across firms have historically led to recurrent problems in the financial services sector. An implementation for moving industry master data to a distributed ledger might involve a network consisting of data submitters, data validators, and data consumers, each set having different permissions [33].

Proxy Voting: In the United States, shareholders of a firm have the right to vote on issues relating to the organization or governance of the company [34]. Shareholder voting is the primary means by which owners of a company's stock can influence the firm, and typically takes place at the firm's annual general meeting. However, most shareholders are unable to attend such meetings in person, and thus may vote by proxy via mail, phone, or online. The current proxy voting process is highly manual and time-consuming, and for retail investors, is often paper-based. Last year, for over 98% of institutional shares, proxy materials were delivered through an electronic platform. However, electronic delivery was only used for 34% of retail shares, with the remaining proxy materials delivered in paper form by mail. Despite retail investors owning, on average, 32% of publicly traded US companies, they tend to be underrepresented in the proxy voting process. In the 2015 spring proxy season, only 28% of retail shares were voted (compared to 91% of institutional shares) [35]. This means that, relative to institutional investors, retail investors are underrepresented in proxy voting by a factor of 6-7x per share held. Delivery mechanism may be a reason for low retail participation. However, Internet-based voting methods in use today suffer from several security risks and privacy problems [36]. Migrating proxy voting to a distributed ledger has the potential to standardize the format and increase the access to proxy voting materials. Even if that does not increase proxy voting participation, it will dramatically increase transparency and verifiability of the voting process. In the words of Bob Greifeld, CEO of

Nasdaq, proxy voting will be put “on the blockchain, on the immutable ledger and obviously enable people to do that with their cell phone and have that record with them forever” [37].

Asset Issuance and Servicing: Asset issuance could be migrated to distributed ledgers, offering benefits to both issuers and owners by providing a single source of truth regarding the full provenance of ownership of the asset. Further, mandatory post-issuance events such as dividend or interest distributions could be managed via smart contracts embedded in the asset ledger [38]. A key challenge, however, will be integrating on-chain and legacy assets in a manner that aligns with regulatory requirements. We may still require a trusted intermediary to provide an interface between new distributed asset ledgers and the repositories of assets kept at central depositories [33].

In general, blockchain-enabled solutions will be most valuable in business situations where:

- There is a need to keep track of complex relationships between multiple parties
- Existing infrastructure lacks a central authority, and processes suffer from low standardization and automation
- Cryptographically authenticated and secured audit trails are required, whether for internal accounting or regulatory reporting

8 REGULATION

Uncertainty regarding the future regulatory landscape surrounding some of the above applications may pose an obstacle for adoption. Technology development is moving extremely quickly, and undoubtedly faster than corresponding regulatory frameworks. A number of key regulatory questions need to be answered in order for financial institutions to feel confident in their quickly growing, and already substantial, investment in distributed ledger technology[26]. Will regulators view distributed ledger technology as a means of improving back-office processes or as the enabler of an entirely new paradigm subject to new rules? How will the opinions of regulators be reconciled in the case where a distributed ledger application spans jurisdictions? In reference to the discrepancy between the SEC and CFTC in defining settlement finality, Charlie Cooper of R3 CEV asks, "If we are out talking to those two organizations, if they have two different rules on settlement finality, what do we do" [39]. This uncertainty seems to be felt across the industry and has caused financial institutions to desire the collaboration of regulators in developing standards. However, such aspirations should not be one-sided—regulators themselves stand to benefit from widespread adoption of distributed ledger technology. Shared ledgers will offer cost savings to regulatory bodies as they are able to do their job more efficiently, and making compliance cheaper for financial institutions can't hurt either [40]. Fortunately, some rule makers seem to favor an open approach to dealing with the rapidly evolving landscape. At a recent blockchain symposium held by the DTCC, CFTC Commissioner Giancarlo recommended regulators follow a "Do No Harm" approach to distributed ledger technology. He references United States legislation surrounding the early Internet as a good model for regulation—avoid undue restrictions and let the private sector lead [41].

[26] Magister Advisors estimates that over $1 billion will be spent by large financial institutions on blockchain projects by the end of 2017 [46].

9 CONCLUSIONS

Blockchain networks have clearly demonstrated their value outside of traditional cryptocurrency contexts. Blockchain networks embedded with smart contracts enable distributed ledger solutions that offer increased resiliency, verifiability, and even entirely new functionality when compared to traditional database systems. Such distributed ledgers have the potential to disrupt many of the processes core to the operation of the financial industry. However, as the technology is immature and evolving rapidly, in the short term, we will continue to see incumbents experimenting to determine which use cases are most feasible and how to best leverage distributed ledger technology for them. Collaboration will be key on the path to adoption—distributed ledgers are most valuable when used across different enterprises and thus, the industry will benefit from standardized, interoperable protocols. Regulators will play an important role in determining the ultimate value added by the technology, and must be included in discussions at each step of the development and deployment process. We are moving toward a world where power is shifting outward to the edges of commercial and social networks. The adoption of distributed ledger technology by the financial industry, and certainly others too, is another step in that direction. It will be exciting to watch the developments unfold and discover how disruptive distributed ledger technology will be.

10 REFERENCES

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.

[2] “CoinDesk BPI.” [Online]. Available: http://www.coindesk.com/price/. [Accessed: 26-Apr-2016].

[3] Eris Industries, “Explainer | Permissioned Blockchains.” [Online]. Available: https://docs.erisindustries.com/explainers/permissioned_blockchains/. [Accessed: 18-Apr-2016].

[4] G. Greenspan, “Ending the bitcoin vs blockchain debate,” 2015. [Online]. Available: http://www.multichain.com/blog/2015/07/bitcoin-vs-blockchain-debate/.

[5] A. Back, “Hashcash - A Denial of Service Counter-Measure,” pp. 1–10, 2002.

[6] BitFury, “Proof of Stake versus Proof of Work,” 2015.

[7] J. Douceur, “The sybil attack,” *Peer-to-peer Syst.*, pp. 251–260, 2002.

[8] J. Kwon, “TenderMint : Consensus without Mining,” 2014.

[9] IntelLedger, “Proof of Elapsed Time — Distributed Ledger latest documentation,” 2016. [Online]. Available: http://intelledger.github.io/introduction.html#proof-of-elapsed-time-poet.

[10] Eris Industries, “Explainer | Blockchains.” [Online]. Available: https://docs.erisindustries.com/explainers/blockchains/. [Accessed: 18-Apr-2016].

[11] G. Greenspan, “Avoiding the pointless blockchain project,” 2015. [Online]. Available: http://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/.

[12] G. Greenspan, “Private blockchains are more than ‘just’ shared databases,” 2015. [Online]. Available: http://www.multichain.com/blog/2015/10/private-blockchains-shared-databases/.

[13] G. Greenspan, “Blockchains vs centralized databases,” 2016. [Online]. Available: http://www.multichain.com/blog/2016/03/blockchains-vs-centralized-databases/.

[14] N. Szabo, “Formalizing and Securing Relationships on Public Networks,” *First Monday*, vol. 2, no. 9. 01-Sep-1997.

[15] R. G. Brown, “A Simple Model for Smart Contracts,” 2015. [Online]. Available: https://gendal.me/2015/02/10/a-simple-model-for-smart-contracts/. [Accessed: 04-Dec-2016].

[16] Eris Industries, “Explainer | Smart Contracts.” [Online]. Available: https://docs.erisindustries.com/explainers/smart_contracts/. [Accessed: 18-Apr-2016].

[17] Eris Industries, “Eris Industries | eris:legal.” [Online]. Available: https://erisindustries.com/components/erislegal/. [Accessed: 18-Apr-2016].

[18] Morgan Stanley Resarch, “Global Insight: Blockchain in Banking: Disruptive Threat or Tool?,” 2016.

[19] Accenture, “Blockchain Technology: Preparing for Change,” 2016.

[20] Accenture, “Accenture Launches Blockchain Practice for Financial Services Industry and Enters Alliance with Digital Asset Holdings.” [Online]. Available: https://newsroom.accenture.com/news/accenture-launches-blockchain-practice-for-financial-services-industry-and-enters-alliance-with-digital-asset-holdings.htm. [Accessed: 18-Apr-2016].

[21] Aite Group, “Demystifying Blockchain in Capital Markets: Innovation or Disruption?” [Online]. Available: http://aitegroup.com/report/demystifying-blockchain-capital-markets-innovation-or-disruption. [Accessed: 13-Apr-2016].

[22] Santander InnoVentures, Oliver Wyman, and Anthemis Group, “The Fintech 2.0 Paper: rebooting financial services,” 2015.

[23] Accenture, “Blockchain-Enabled Distributed Ledgers: Are Investment Banks Ready?”

[24] M. Bodson, “Opening Remarks By Michael Bodson, DTCC President and CEO,” in *2016 Blockchain Symposium*, 2016.

[25] R. R. Bliss and R. S. Steigerwald, “Derivatives clearing and settlement : A comparison of central counterparties and alternative structures,” *Fed. Reserv. Bank Chicago - Econ. Persperctives*, no. 4,

pp. 22–29, 2006.
[26] U.S. Securities and Exchange Commission, “Settling Securities Transactions, T+3.” [Online]. Available: https://www.sec.gov/answers/tplus3.htm.
[27] G. W. Peters and E. Panayi, “Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money,” *arXiv Prepr. arXiv1511.05740*, pp. 1–33, 2015.
[28] The Boston Consulting Group, “Cost benefit analysis of shortening the settlement cycle,” 2012.
[29] DTCC, “National Securities Clearing Corporation: Disclosure under the Principles for Financial Market,” 2015.
[30] DTCC, “Shortening the Settlement Cycle: The Move to T+2,” 2015.
[31] Standard & Poor’s Rating Services, “A Guide to the U.S. Loan Market,” 2013.
[32] Thomson Reuters, “Global Syndicated Loans Review: Managing Underwriters,” 2016.
[33] DTCC, “Embracing Disruption: Tapping the Potential of Distributed Ledgers to Improve the Post-STrade Landscape,” 2016.
[34] SEC Office of Investor Education and Advocacy, “Exercise your Shareholder Voting Rights in Corporate Elections.” 2010.
[35] Broadridge and PwC, “ProxyPulse: 2015 Proxy Season Wrap-up.”
[36] “Security risks and privacy issues are too great for moving the ballot box to the Internet,” 2015. [Online]. Available: http://phys.org/news/2015-03-privacy-issues-great-ballot-internet.html. [Accessed: 24-Apr-2016].
[37] T. Cave and A. Irrera, “Nasdaq’s Bob Greifeld unveils European blockchain initiative,” 2015. [Online]. Available: http://www.efinancialnews.com/story/2015-10-22/nasdaq-reveals-new-blockchain-project-bob-greifeld. [Accessed: 26-Apr-2016].
[38] Oliver Wyman, “Blockchain in Capital Markets: The Prize and the Journey,” 2016.
[39] H. Engler, “Blockchain faces maze of regulatory complexities, questions and challenges,” *Thomson Reuters Regulatory Intelligence*, 2016. [Online]. Available: https://blogs.thomsonreuters.com/answerson/blockchain-faces-maze-of-u-s-regulatory-complexities-questions-and-challenges/. [Accessed: 26-Apr-2016].
[40] M. Ross, “Blockchain plus smart contracts equals boon for regulators,” 2016. [Online]. Available: http://www.paragonpr.com/blockchain-plus-smart-contracts-equals-boon-for-regulators/. [Accessed: 26-Apr-2016].
[41] J. C. Giancarlo, “Regulators and the Blockchain: First, Do No Harm,” in *2016 Blockchain Symposium*, 2016.
[42] “Who is Satoshi Nakamoto? The creator of Bitcoin remains elusive.” [Online]. Available: http://www.coindesk.com/information/who-is-satoshi-nakamoto/. [Accessed: 26-Apr-2016].
[43] S. Northcutt, “Hash Functions.” [Online]. Available: http://www.sans.edu/research/security-laboratory/article/hash-functions. [Accessed: 26-Apr-2016].
[44] “Bitcoin Developer Reference.” [Online]. Available: https://bitcoin.org/en/developer-reference#block-headers. [Accessed: 26-Apr-2016].
[45] GlobalPlatform, “The Trusted Execution Environment: Delivering Enhanced Security at a Lower Cost to the Mobile Market,” 2011.
[46] Magister Advisors, “Blockchain & Bitcoin 2016: A Survey of Global Leaders,” 2016.