Blockchain Security and Demonstration

Yao Yao, Jack Rasmus-Vorrath, Ivelin Angelov

Abstract - Blockchain promises greater speed, security, accuracy, and transparency for every electronic transactional or record-keeping process. Proponents say Blockchain will make processing payments, trading stocks, managing health-care records and birth certificates, processing property titles, monitoring digital supply chains, and coordinating the growing Internet of Things (IoT) faster, easier, and cheaper. Notwithstanding this growing litany of theoretical benefits and proposed use cases, Blockchain's real potential of attaining wide-spread adoption is unclear. Commentators are characterizing the next two years as an early adopter phase that will prepare industry, government, and society for the real Blockchain revolution yet to begin. The goal of this research paper is to present evidence of early adopter activity indicating that Blockchain is on track to fulfill its potential to adapt to, and transform our society. The research includes historical background, a survey of current literature on early adopter activities, and a brief evaluation of various implementations of Blockchain, including a discussion of their current application.

Index Terms—**Blockchain, Bitcoin, Ethereum, Hyperledger, Quorum, Cryptography, Data Security**

I. INTRODUCTION

BLOCKCHAIN is a distributed ledger software technology that constitutes the underlying platform of Bitcoin. It is used to establish a peer-to-peer (P2P) public ledger maintained over a network of computers, and can provide an alternative to the centralized governance characteristic of traditional currencies. Its basic principles are:

1. Distributed Database
2. Peer-to-Peer Transmission
3. Transparency with Pseudonymity
4. Immutability of Records
5. Computational Logic

Transactions are clustered into chronologically chained blocks of data using a hashing algorithm that theoretically makes the record immutable. The Blockchain is replicated to each participating node on the network, and administration of the software is orchestrated by consensus of the participating nodes, where the self-validating process replaces the trusted intermediary roles of banks, title companies, and other market middlemen.

The purpose of this paper is to provide a survey and tutorial on Blockchain technology, to review the potential uses, vulnerabilities, and barriers, and to present case studies of current Blockchain applications. Developing the project included the creation and live demonstration of a standard Blockchain implementation [1].

A. History of Blockchain

The conceptual principles of Blockchain were introduced by Haber and Stornetta in 1991. Their proposal was to digitally time stamp intellectual property documents in chronological order to authenticate authorship, providing ownership protection for the author. The stamp would be in the form of a hash code, and each hash would be dependent on the ones preceding it in the chain. Thus, a block's data could not be altered without altering all the other blocks chained to the one in question. As a further precaution, they advocated publishing the sequence of records in a public forum so data could be reviewed and verified by any interested third party, essentially crowd-sourcing the verification function.

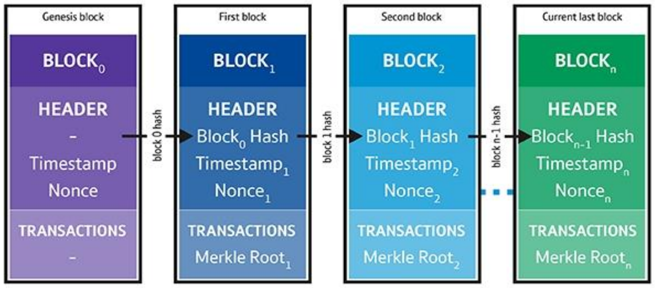
The term "Blockchain" originated in reference to a "chain of blocks" as described by Satoshi Nakamoto (pseudonym) in 2008; it was conceived as a method for validating ownership of virtual currency in a publicly distributed ledger. Nakamoto's purpose in proposing a peer-to-peer electronic cash system was to make powerful, centralized third parties obsolete by disintermediating financial transactions. In 2009, the first application of Blockchain technology appeared in the source code for the digital cryptocurrency Bitcoin. Since then, Blockchain has expanded its functionality and now supports an array of different transactions. After seven years of successful use with Bitcoin, Blockchain technology is now being considered as an alternative to centralized accounting ledgers and other identity- and ownership-based record keeping systems.

Note that the term "Blockchain" often refers to the implementation of the distributed ledger technology supporting Bitcoin; however, "Blockchain" or "Blockchain technology" may also be used in general reference to distributed ledger technology or to the data structure itself, depending on the context. Occasionally the acronym DLT is used independently to refer to Distributed Ledger Technology [2].

B. Characteristics and Benefits

Blockchain is a decentralized ledger on a peer-to-peer network which allows transactions to be processed without recourse to a central authority, thereby eliminating any single point of failure. Blockchain can be likened to an operating system for cryptocurrencies, smart contracts, and other things of value transacted within the system.

Figure 1- The Blockchain



The Bitcoin Blockchain provides unique and compelling solutions for the financial marketplace (Figure 1):

- **Data structure** - Transactions are formatted into blocks that are linked together using a cryptographic hashing algorithm which takes as its input prior entry data. The resulting output is comprised of a secure data chain in which one block cannot be altered without invalidating the hash.
- **Distributed** – Every node in the network contains a full copy of all the data since the genesis block (i.e., the first block in the chain), eliminating any single point of failure.
- **Security** – Cryptographic hash functions ensure the data integrity of the Blockchain. Authenticity is also ensured through the use of private keys. Modifying or altering a block would result in a change of its hash function that would render the block inconsistent with all subsequently chained blocks; this would be detected by the other nodes in the system and cause the change to be rejected.
- **Consensus** – Nodes algorithmically validate new entries; entries that are validated by a majority of nodes are included in the Blockchain.
- **Transparency with privacy** – Not only are transactions visible to everyone—they are also traceable throughout the chain; all transactions in the ledger can be viewed by all participants. Although all participants have full copies of the database transactions, none of the users' identities are visible.
- **Timestamps** – Timestamping ensures the order of transactions is accurate and complete.
- **Software updates by consensus** – Updates to the Blockchain software are also accepted through verification by consensus.
- **Disintermediation** – Blockchain eliminates the need for intermediaries, significantly reducing overhead costs.
- **Turing Complete** – Computability is unbounded, provided one has the required resources; one can write contracts for almost any computational problem.

By virtue of these traits, Blockchain offers several key benefits when compared to traditional approaches to similar tasks:

- **Data integrity** – The cryptographically secure nature of the data structure rules out questions concerning asset identity, asset ownership, and transaction history; it is unfeasible to reverse or tamper with previous transactions. Any changes to the Blockchain are made by adding a new block instead of modifying existing ones. Once a block is added to the chain, it cannot be altered or removed.
- **Operational resilience** – A distributed data model with a complete set of data at every node means that the data is always accurate and accessible.
- **Built-in audit trail** – Information on the time of, and parties to all transactions are built into the data structure itself, automatically establishing audit trails.
- **Ownership** – Blockchain provides an immutable record of ownership and is designed to prevent double-spending of assets.

Creating a reliable, shared, immutable record of ownership and transactions should naturally result in 'disintermediation'-- the elimination of reliance on trusted third-party service providers in the reconciliation and validation process currently required to finalize transactions.

On this note, Oliver Wyman and the Anthemis Group, Santander Innoventure, claim in their recent paper that "Blockchain technology could reduce banks' infrastructural costs by $15-20 billion a year by 2022" by reducing middlemen fees and cutting overhead costs [3].

C. How Blockchain Works

1. **Transaction** - Two parties exchange data: money, contracts, deeds, medical records, customer details, or any other asset that can be digitally formatted and exchanged.
2. **Verification** - Depending on the network's parameters, the transaction is either verified instantly or transcribed into a secure record and placed in a queue of pending transactions. In this case, nodes--the computers or servers in the network--determine if the transactions are valid based on a set of rules to which the network has agreed.
3. **Structure** - Each block is identified by a hash, a 256-bit number created using an algorithm agreed upon by the network. A block contains a header, a reference to the previous block's hash, and a group of transactions. The sequence of linked hashes creates a secure, interdependent chain.
4. **Mining** - Miners try to "solve" the block by making incremental changes to one variable in the algorithm until the solution satisfies a network-wide target. This is called demonstrating "proof-of-work;" correct answers cannot be falsified and solutions must prove the appropriate level of computing power was drained in the solving process.
5. **Validation** - When a block is validated, the miners that solved the puzzle are rewarded, and the block is

distributed throughout the network. Each node adds the block to the majority chain, i.e., the network's immutable and auditable Blockchain.

6. **Defense** - If a malicious miner tries to submit an altered block to the chain, the hash of that block would change, and the hash of all subsequent blocks would necessarily reflect that change. The other nodes would detect the alteration and reject the block from the majority chain, preventing corruption.

For every Bitcoin owner, there is a record on the Blockchain that contains the coins owned as well as a digital signature. This digital signature verifies ownership of the coins rewarded in solving the block's computational puzzle. The signature requires use of a private key contained in the keyholder's Bitcoin wallet. Only the asset owner has corresponding access permissions. Game theoretical principles underpin the security of the cryptographically verified and validated ledger. It is considered virtually hack-proof--a malicious agent would have to change the same block on every computer running the database to ensure that the chain remains identical across the network.

Mining – To validate/verify blocks and permanently append them to the Blockchain, every transaction requires a miner (i.e. verifier) to present proof of "computational effort." This is the heart of the proof-of-work (PoW) system, which requires solving a mathematical puzzle. This puzzle is designed to be computationally difficult to solve, but simple to verify. The puzzle essentially consists of an inverse hashing operation to determine the nonce which, when entered into an algorithm, is less than a given target value. PoW can be represented in the following form:

$H(prevHash||Tx1||...||Nonce) < Target$

Bitcoin, e.g., relies on a cryptographic double SHA256 hashing algorithm, whose target is a 256-bit number. The target value is adjusted to increase difficulty approximately every 14 days, motivating miners to continuously improve their methods for efficiently solving these puzzles. The mining process is characterized by the amount of time it takes to find the solution by computational brute-force, according to the current target difficulty. Upon completion of PoW, it is broadcast to the network, consensus is reached, and the transaction block is added to the Blockchain.

Proof of Stake (PoS) – This is an alternative to the PoW system, preferred for its reductions in processing time and costs. In PoS, mining involves determining the creator of the next block by taking turns proposing/voting it and by applying combinations of random selection and criteria of existing wealth or 'stake'; it is especially designed for the writing of smart contracts used by Ethereum, another popular cryptocurrency based on the Blockchain framework.

Instead of proportionally splitting blocks according to the relative hash rates of miners (i.e. their mining power), proof-of-stake protocols proportionally split stake blocks according to the current wealth of miners. The higher one's stake, the greater one's chance of validating a block.

Upon completion of the mining process, the block in question is irrevocably added to the chain and will henceforth contain the previous hash, the nonce, and the corresponding transactions.

STRUCTURE OF A BLOCK [33]

Table 1- Structure of a Block

Size	**Field**	**Description**
4 bytes	Block Size	The size of the block, in bytes, following this field
80 bytes	Block Header	Several fields form the block header
1-9 bytes (VarInt)	Transaction Counter	How many transactions follow
Variable	Transactions	The transactions recorded in this block

A block is a "container" of information consisting of data relating to each transaction. It contains the list of transactions as well as a header which houses all metadata for the block. Only a fraction of the total size of the block is contained in the header; the bulk of it consists of transaction data.

Table 2-Block Header Structure

Size	**Field**	**Description**
4 bytes	Version	A version number to track software/protocol upgrades
32 bytes	Previous Block Hash	A reference to the hash of the previous (parent) block in the chain
32 bytes	Merkle Root	A hash of the root of the Merkle tree of this block's transactions
4 bytes	Timestamp	The approximate creation time of this block (seconds from Unix Epoch)
4 bytes	Difficulty Target	The proof-of-work (PoW) algorithm difficulty target for this block
4 bytes	Nonce	A counter used for the PoW algorithm

The block header is broken down into three sets of block metadata, as summarized in Table 2:

Set 1 – Previous block's hash
Set 2 – Difficulty, Timestamp, Nonce
Set 3 – Merkle Tree Root

TYPES OF BLOCKCHAIN

Public - Anyone is allowed to set up their computer as a node, which is then synched to the Blockchain. Every node has an exact copy of the ledger history that is updated with every transaction. This repetition is computationally expensive and can be slow and wasteful. However, the redundancy is necessary to ensure the security of the Blockchain, especially when one is dealing with cryptocurrency Blockchains. However, public Blockchains allow for complete transparency and ensure anonymity of the participants; they are arguably the best choice for decentralized networks.

Consortium - A few predetermined nodes verify and add transactions to the Blockchain. Just like a private Blockchain, consortium Blockchains are more efficient and guarantee a higher level of privacy without relegating all control to a single entity.

Private – Corporate entities, companies, or government institutions wield varying measures of power over how transactions are verified and written to the Blockchain. This allows for greater efficiency and faster transaction verification. The entity or entities in question also control who has read access, which allows for greater privacy than one has in a public Blockchain setting.

Permissioned vs Permission-less – The Blockchain system can impose various restrictions, such that only a few have the privilege to access and validate transactions. In some cases, a permissioned Blockchain can restrict access to creating smart contracts.

BLOCKCHAIN IMPLEMETATION

Blockchain technology is applied in at least three principle respects:

Digital payments – Traditionally, transactions are conducted through a middleman (some single authority) like a bank. All transactions must be approved by the central authority, and only the participating accounts are updated or affected. In Blockchain, the transaction information is transmitted to all of the member computers at once in the form of new blocks. This is done without relying on a trusted third party. Such transactions are performed with the use of cryptocurrencies like Bitcoin.

Smart Contracts – Computer protocols are used for facilitating, verifying, or enforcing the negotiation or performance of contracts concerning the exchange of property, shares, or money without relying on intermediaries. This is accomplished through smart contract cryptographic systems, such as those implemented on the Ethereum RootStock smart contract platform. Smart contracts run on the Blockchain exactly as programmed, without any possibility of censorship, downtime, fraud, or third-party interference. Traditionally, contracts are written and enforced by governmental or other legal regulatory entities.

Database and record management – The immutable and irreversible properties of the Blockchain make it ideal for the safekeeping of public records.

II. Proposed Uses

Potential applications of Blockchain extend beyond the domain of cryptocurrency into various branches of infrastructure, in ways which may alter traditional IT implementations. Stock sales post-trade processing could be a candidate for Blockchain applications, where disintermediation could result in faster and cheaper transactions. A trackable history of stock ownership could simplify stockholder voting and dividend payments. Blockchain has also been proposed to simplify traditional corporate functions like auditing, financial reporting, and the enforcement of compliance procedures. Blockchain smart contracts also facilitate the implementation of programmable transactions, e.g., in money transfers of the kind currently managed by services like PayPal.

Since Blockchain was conceived early on as a way of tracking Intellectual Property rights, it excels at establishing and tracking asset ownership; applicable use cases include the management of public records for birth certificates, driver's licenses, university degrees, court records, and property titles. Another proposed use is the implementation of 'smart inventory' to track high value assets, like precious gems and metals, art, and sports memorabilia, not only to establish ownership, but also to prevent forgery, fraud, or modification. Similar principles are applicable to efforts in deterring online media piracy.

Blockchain-enabled applications could also be used in managing healthcare records [5], in web-based content distribution [6], in identifying terrorist threats [7], and in increasing security for the emerging Internet of Things (IoT) [8]. Blockchain may also be used for a variety of peer-to-peer crowd-sourcing and crowd-sharing applications. Worth noting are the several use cases it presents for entities operating in the 'shadow banking' economy. Crowd funding, peer-to-peer lending, seed capital platforms, and charitable donation applications are all potential targets for Blockchain enablement.

Going beyond Bitcoin, proponents of Blockchain believe the technology can create enormous benefits to society. Expectations range from the logical--creating transparency in stock transactions to reduce corrupt behaviors by regulators, exchanges, and listed companies--to the fantastic—engendering visions of a utopian society that has eliminated the corruption of strong central powers, and created an economy of abundance based on peer-to-peer exchanges [9].

III. Barriers

While the promise of Blockchain is significant, the associated barriers and risks are equally great.

A. Barriers

Cyperattacks on Blockchain applications: A cyber-attack on Ethereum, a cryptocurrency Blockchain application, successfully diverted $50M worth of tokens. To counter this attack, 85% of Ethereum users voted for a 'hard fork' in the chain, which essentially rolled back the effects of the attack and restarted the chain before its occurrence. The remaining 15% of users continued to use the affected data, referring to it as 'Ethereum Classic.' The second event involved the bankruptcy of the Mt. Gox Bitcoin exchange, which had handled 70% of Bitcoin traffic in 2014. Investigation of the bankruptcy revealed that $480M in Bitcoin was stolen from the bank [10]. These two events shook confidence in the Blockchain software by showing their vulnerability to cyber-attacks.

Currency and financial markets are heavily regulated. As yet, no global consensus on the appropriate regulation of cryptocurrencies has been reached. Most countries have not yet tried to regulate this phenomenon, and those which have tried have adopted widely differing approaches [11]. Traditional currency regulation in the United States, e.g., has rules in place to prevent money laundering and racketeering. While Blockchain does record the user associated with each transaction, the use of private key cryptography makes it difficult to track that user back to an individual person who can be held accountable for actions and decisions. Notwithstanding, the need for genuine anonymity remains a legitimate concern, as maintaining the privacy of the owner's identity may be appropriate for certain records. Exposing sensitive transaction information to market forces may have unforeseen and potentially adverse consequences. In such cases, too much transparency can be a problem.

Financial systems require a very high level of stability and user confidence. The US stock market system attests to the way in which the financial infrastructure has developed naturally over time to meet the needs and requirements of users and regulators. The incorporation of, or transition to a new architecture involves risk, and would likely introduce volatility, so rapid infrastructural change is unlikely [12].

Historical Reputation: Because of its history of being used as a commercial framework for Dark Web activity, the Bitcoin Blockchain must also work to restore its public reputation if it is to generate widespread adoption and assume the crucial infrastructural roles of which the technology is capable.

51% Attack: In 2009, Bitcoin miners (data verifiers) began operation using home computers. Today, there is an entire industry of high-end super computers exclusively dedicated to mining Bitcoin, and it is no longer feasible to competitively mine using the kind of technology typically found in the private home. In lending themselves to the concentration of Bitcoin wealth, these technological developments engender problematic centralization of network influence.

If any mining pool controls more than 50% of the total hashing power of the entire Blockchain, it is capable of determining the validity and direction of the course of the transaction history. The 51% attacker essentially becomes the authoritative host of the entire Blockchain. Since consensus decisions are based on mining power, it is possible that the most powerful miners may accept only code changes advantageous to themselves, shoring up their influence. Other situations involving coercion or collusion are also conceivable. Influential miners could receive compensation (i.e., bribes) for accepting code changes of little consequence to them. Software changes could be packaged to deceive those who accept them. Moreover, the absence of any single regulative authority over the Blockchain might leave it vulnerable to sabotage. This is to say that a saboteur group could compromise the integrity of the Blockchain data if it were capable of asserting control over a majority of the mining power, enabling it to organize a so-called "51% attack" [13].

Double-spending: This type of attack is perpetrated by a malicious client attempting to transfer coins to multiple vendors before the transactions are fully verified. For Bitcoin cryptocurrency, the average processing time for confirming the transactions of a new block is about 10 minutes, with a standard deviation of 20 minutes. With this much time between the proposal and transfer of payment, an attacker can double-spend before transactions are fully validated [14]. Another way of double-spending presents itself when a malicious client leverages a discrepancy over the valid direction of the Blockchain in the event of a "hard fork," or temporary divergence in the chain. Since the longest block fork is eventually established as the valid chain, this may result in an "extinct fork," i.e., the extinction of the original prong in the fork [15].

Selfish mining: Instead of publishing blocks to the network immediately, a "selfish miner" may operate on their own private chain before publishing several blocks at once, potentially forcing other nodes to discard blocks and lose revenue. This is costly to the selfish miner in the short term, but may have an even more substantial impact on the revenue of other nodes, such that others are incentivized to continue working on the attacker's newly published chain. This may eventually invalidate the existing public branch, and credit the selfish miner for the overlap [16].

Transaction Privacy Leakage: Although Blockchains are designed for anonymity, its privacy protection protocols are not very robust. An attacker may use methods such as taint analysis (where "taint" is the percentage of funds received by one address that are traceable to another) and payment tracking, IP address monitoring, and web crawling [17]. Furthermore, if an attacker obtains private information from a vendor such as an email or shipping address, then it can be linked to the Bitcoin address and the owner's identity.

Smart contract attacks: There is concern over how well predetermined mechanisms perform when issues like disputes over transaction finality or delays create a need for human intervention. Smart contracts may be susceptible to attacks of the kind perpetrated against the Decentralized Autonomous Organization (DAO) in June of 2016, when a recursive call bug in the software was exploited, allowing the attacker to drain the DAO of $3.6M in Ether (approximately equivalent to $45M), collected from the sale of its tokens [18]. Refer to Appendix Tables A and B for more on smart contract vulnerabilities.

Private Key Security: Bitcoin and Ethereum utilize the Elliptic Curve Digital Signature Algorithm (ECDSA) for payment authorization [19]. There are concerns that insufficient randomness is incorporated into the process of generating ECDSA digital signatures [20]. Such vulnerabilities in the ECDSA implementation were exploited in August 2013 by a hacker by the name of “Gomez,” who successfully stole 59 Bitcoins from users who were the victims of a failure in random signature generation [21]. Once a private key used in signature generation is recovered by a malicious agent, they can transfer the coins in the account, and the owner will not be able to trace the attacker.

Other Technical limitations: Although change is underway, the development of protocols and standards for interoperability with Blockchain is still in its infancy. For interoperability with traditional large-scale payment systems in particular, optimizing processing speed and supporting scalability are of particular concern.

IV. Application Survey

A. Governments

Healthcare Records: Data security startup Guardtime has announced a partnership with the Estonian eHealth Foundation to deploy a Blockchain-based system to secure over 1-million patient healthcare records [22]. The foundation will integrate Guardtime's keyless signature infrastructure (KSI) blockchain into the foundation's Oracle database engine to provide real-time visibility into the state of patient records.

Land Registries: Both Honduras and the Republic of Georgia are moving toward electronic land registries based on Blockchain databases [23]. The project undertaken by Honduras had initially stalled in the face of widespread corruption and a lack of clear authentication of ownership of real properties. However, implementation partners have since stated that issues have been resolved, and are resuming the project [24]. The Republic of Georgia does not appear to have had the same issues, and the project is expected to proceed as planned.

B. Banks

Deutsche Börse Group: Deutsche Börse Group has developed a concept for riskless transfer of commercial bank assets by combining Blockchain technology with its proven post-trade infrastructure [25]. As a next step, Deutsche Börse will consult with clients, regulators, and central banks to obtain feedback on its concept. A functional and technical prototype based on Hyperledger Fabric (whose original contributors include IBM and Digital Asset) is currently being developed.

Bank of England: The Bank of England announced in March of 2017 that it is engaged in the proof of concept (PoC) phase of a project with Ripple focused on cross-border payments and settlement using two different Real Time Gross Settlement (RTGS) systems [26]. The first of its kind, this collaboration enables a central bank to explore how it can use Blockchain technology to facilitate and optimize cross-border payment processing. Ripple’s solution is built upon the open and neutral Interledger Protocol, and allows for interoperable payments across different ledgers and networks. The goal of this PoC is to demonstrate the synchronized movement of different currencies across different RTGS systems; such synchronization could lower settlement risk and improve cross-border payment speed and efficiency.

C. Corporations

Overstock.com: Online retailer Overstock.com became the first publicly traded company to issue internet stock, distributing some 126,000 company shares with technology based on the Bitcoin Blockchain framework [27]. Together with subsidiary tØ, Overstock has been developing such technology for the past three years to transform the financial securities trade. Overstock subsidiary Medici Ventures has also recently added to its portfolio the Belgium-based firm SettleMint, whose Ballot Box product has demonstrated the security of recording voting activity to the Bitcoin Blockchain [28].

Visa: Visa has announced their forthcoming business-to-business payments service developed in partnership with Chinese Blockchain startup, Chain. Dubbed Visa B2B Connect, the near real-time settlement platform is aimed at providing a more secure, transparent mechanism for businesses making payments via Visa’s network [29].

D. Collaborative efforts

The Hyperledger Project (HLP): The Hyperledger Project is an open-source, collaborative effort hosted by the Linux Foundation [30]. Hyperledger Fabric, the product of a hackathon whose original contributors were IBM and Digital Asset, is a Blockchain implementation intended to serve as a foundation for developing modular applications that leverage systems of consensus, smart contract hosting, and membership services.

Ethereum: The Ethereum Foundation, a Swiss nonprofit, has developed a decentralized platform for running smart contracts designed to avert downtime, censorship, fraud, and third-party interference. In addition to writing, deploying, and using smart contracts, one can use one’s Ethereum Wallet for holding and securing Ether and other crypto-assets built on Ethereum [31].

V. Quorum Case Study

A. Background

Quorum was developed by JP Morgan in 2015 and open-sourced for public use and review in 2016, as an enterprise-focused distributed ledger protocol based on the Ethereum framework [32]. Ethereum features a permissioned Blockchain implementation. Permissioning allows only specific network entities to perform and validate transactions, in contrast with non-permissioned Blockchain implementations like Bitcoin.

The financial industry is highly regulated, which slows and impedes wider adoption of Blockchain technology. Quorum was designed to satisfy regulatory requirements by allowing regulators to view transactions, while keeping transaction details confidential. Quorum thus provides the financial services industry with a permissioned Ethereum implementation that allows for transaction and contract privacy [33].

B. Security Implementation Features

Quorum's focus is on adding security features and mechanisms to promote wider adoption of Blockchain technology, specifically among financial institutions. As described by the JPMorgan documentation, the primary features of Quorum that represent extensions to public implementations of Ethereum include:

- Transaction and contract privacy
- Voting-based consensus mechanisms
- Network and peer permissions management
- Enhanced performance

A number of proposals to address smart contract data privacy issues are beginning to emerge; Quorum proposes a voting-based consensus algorithm, and achieves data privacy by incorporating a private transaction identifier into its system [34]. Cryptographic encryption of transaction data and segmentation of each node's local state database ensures that while all nodes in the network can validate public transactions, validation of private transactions is restricted to nodes party to those transactions. Transaction validation is thus based on voting consensus among the involved nodes. In effect, each node's local state database is populated only with public data and private data to which they are party.

Quorum uses symmetric key cryptography to achieve data privacy. Symmetric keys are generated for each transaction and sent (encrypted with the public keys of nodes involved in the transaction) to the Transaction Manager, along with the hash of the encrypted private data as the payload. The Transaction Manager is responsible for notifying all nodes in the transaction of the available payload, and for validating that the correct nodes are responding through their signatures. If the correct node responds with the correct signature and public key, the payload and the symmetric key are sent to the responding node for decryption and local storage.

C. Controversial Forks

Because Quorum is built on the Ethereum framework, it inherits its easily extensible capabilities, but also its associated vulnerabilities, one instance of which was exploited by the aforementioned DAO hack [35]. In this case, the attackers were able to siphon assets without a proper exchange of value. The first recourse against such an attack is a "soft fork," which entails a majority of miners voting to roll back the changes in the network to a point prior to the attack. However, it was discovered that soft forking was not a suitable fix for the DAO, as doing so would have left the network vulnerable to subsequent denial-of-service attacks [36]. This realization led to a "hard fork," i.e., a permanent modification to the network protocols and Blockchain data, whereby the end of the chain is set to predate the offending event. At this reset point, the new chain begins, resulting in two paths forward. As mentioned, the old chain, "Ethereum Classic," still exists and is used by 15% of the Ethereum community; the remaining 85% continued working with the new chain.

As a private implementation built by JP Morgan, Quorum is ultimately subject to its governance on the question of whether and how to implement hard forks under such circumstances. Many view such unilateral authority as being counter to the principles of transparency and community ownership characteristic of Blockchain technology, undermining its credibility, and threatening the game-theoretic security of a fundamentally decentralized system.

In summary, Quorum is still early in its lifecycle, but shows promise as an easily deployed and developed platform. Leveraging the strengths of the Ethereum framework, Quorum has built its formidable security architecture with a focus on banking in mind. However, even (or perhaps, especially) in private and permissioned Blockchain implementations like Quorum, there remain vulnerabilities open to malicious users and administrators alike.

D. Hyperledger vs Quorum

Hyperledger can be viewed as a toolbox for building business Blockchain applications in private networks [37]. Insofar as it allows one to implement many different kinds of distributed ledgers, one of its principle strengths is its flexibility; its consensus algorithms are customizable to the use-case in question. Meanwhile, Quorum, as a system expressly designed for private and permissioned networks, lays claim to the performance advantages that come with a consensus algorithm that depends only on the cooperation of the permissioned parties involved. Other performance and privacy advantages have resulted from Quorum's development of data sharding techniques, through which large stores of data are segmented into smaller, faster, more easily managed parts. Such sharding enhances Blockchain network throughput, allowing a subset of nodes to communicate and validate transactions without having to replicate the database every time. Not every node has to validate every transaction—only public transactions or those private transactions to which a given node is party. Sharing techniques not only increase scalability, but could also cut down on development time for new Blockchain applications.

E. Security Concerns

Blockchain implementations promise a kind of security unlike any yet conceived in traditional banking systems, while simultaneously cutting costs and increasing efficiency. However, the system in practice has shown that more time, research, and resources will be needed to ensure the level of security of which the technology is capable [38]. This is more easily accomplished with private and permissioned ledgers, but public ledgers in particular will require more attention. The strength of the cryptography on which the technology is based is well evidenced. However, according to the specific requirements of the implementation, proper governance and administration is also needed to make networks secure. Successful deployment entails careful planning, and transparency is a must in system design, such that appropriate rules and decision-making processes are well defined in advance.

One particular security concern is the possibility of inconsistent results in the event of a distributed denial of service (DDoS) attack. Although new applications of Blockchain technology are emerging to address precisely this issue [39], more sophisticated DDoS attacks could potentially leverage enough computing power to take over 50% of the network. Mercenary DDoS operators could employ powerful botnets to overwhelm vulnerable targets. For defending against such attacks, firewalls and related network security measures will continue to play a crucial role.

Another security challenge relating to governance involves the ownership and storage of confidential consumer data. Historically, EU privacy laws have dictated that consumer data must reside within one’s country of residence, posing a challenge to the increasingly distributed nature of identifying information [40]. However, emerging Blockchain applications are viewed by some as meeting in stride the forthcoming requirements of the European General Data Protection Regulation (May 2018) [41]. One possible solution entails separating public and private data. Data such as transaction amounts, currency used, dates, etc., require no special treatment, and ports can be opened to machines residing in different nations to retrieve more specific user data on an as-needed basis. Such an arrangement could meet the requirement that certain data not leave a country’s borders.

VI. CONCLUSION

Given the continuously growing number of providers and platforms available, it is, of course, difficult to objectively measure the status of Blockchain adoption. Extensive experimentation and investment has brought unique and compelling products and applications to the market, but widespread use still seems to be forthcoming. Nonetheless, the possible benefits of cost-effectiveness, networks of trust, decentralized data integrity, and performance efficiency are tremendous. With ongoing improvements in data privacy and security, Blockchain is likely to become increasingly integrated with our current systems in the years to come.

VII. Appendix

Table A - Smart Contracts Vulnerabilities

Number	Vulnerability	Cause	Level
1	Call to the unknown	Invoked function not exiting	Script source code (Solidity)
2	Gasless send	Fee for the fallback function is more expensive than 2300 gas limit to send function	
3	Exception disorders	Inconsistency in exception handling	
4	Type casts	Type handler not showing errors	
5	Reentrancy	Fallback allows function reentry (e.g., DAO attack.)	
6	Keeping secrets	Secret field can be revealed by cryptanalysis	
7	Immutable bugs	Consequence of bugged contracts that cannot be corrected	EVM bytecode
8	Ether lost in transfer	Specifying wrong recipient address	
9	Stack size limit	Call stack bounded to 1024 frames. Exceptions with higher stack exploited	
10	Unpredictable state	State of contract of a short fork branch can be reverted	Blockchain system
11	Generating randomness	Craft block to bias PRNG for distribution	
12	Time Constraints	Ability to choose a timestamp by a miner	

UNDER-OPTIMIZED SMART CONTRACTS

There may be transaction fees on miners processing the smart contracts issued by users. Code may be under-optimized, such that the smart contract is longer or less efficient than it should be. The transaction fee is often proportional to the size of the bytecode of the smart contract, such that under-optimization results in overcharging users.

Table B - Under-optimized Smart Contract Types

Number	Pattern	Category
1	Dead code	Useless Code Related Patterns
2	Opaque predicate	
3	Expensive operations	Expensive operations in a loop
4	Constant outcome	
5	Loop fusion	
6	Repeated computations	
7	Comparison with unilateral outcome	

“Dead code” is a section of code that will never run, but whose extra length still increases the transaction cost. For example, if an “if-statement” such as ‘x >5’ is followed by an if-statement like ‘x*x < 20’, then the nested if-statement is dead code that will never run. Opaque predicates are most often Boolean expressions for which the outcome is known by the programmer in advance. Numbers three to seven in Table B above refer to expensive code patterns. Such expensive operations are generally caused by the inefficient use of looping structures. It is estimated that 93.5%, 90.1%, and 80% of smart contracts are under-optimized in the following three ways, respectively: Dead code, Opaque predicates, and Expensive operations [42].

REFERENCES

[1] "post2web/basic_blockchain", *GitHub*, 2017. [Online]. Available: https://github.com/post2web/basic_blockchain/blob/master/blockchain_database_implementation.pdf. [Accessed: 03- Dec- 2017].

[2] A. Collob and K Sok. (3rd quarter, 2016). Blockchain / Distributed Ledger Technology (DLT): What Impact on the Financial Sector? *Digiworld Economic Journal*. [Online] *No. 103*, p. 93. Available: http://www.academia.edu/30192464/Blockchain_Distributed_Ledger_Technology_DLT_What_Impact_on_the_Financial_Sector

[3] "Santander: Blockchain Tech Can Save Banks $20 Billion a Year", *CoinDesk*, 2017. [Online]. Available: https://www.coindesk.com/santander-blockchain-tech-can-save-banks-20-billion-a-year/. [Accessed: 03- Dec- 2017].

[4] D. Yermack. (2016, November 28). Corporate Governance and Blockchains. *Review of Finance*. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2700475

[5] X. Yue, H. Wang, D. Jin, M. Li, W. Jiang. (August, 2016). Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. *Journal of Medical Systems*. [Online]. Available: https://www.ncbi.nlm.nih.gov/pubmed/27565509

[6] N. Fotiou. (September, 2016). Decentralized Name-based Security for Content Distribution using Blockchains. Presented at Conference IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7562112/

[7] A. Modi. (November, 2016). Towards Automated Threat Intelligence Fusion. Presented at Conference 2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC). [Online]. Available: http://ieeexplore.ieee.org/document/7809731/

[8] K. Korpela. J. Hallikas, T. Dahlberg. (January, 2017). Digital Supply Chain Transformation toward Blockchain Integration. Presented at Conference Hawaii International Conference on System Sciences (HICSS) 2017. [Online]. Available: https://scholarspace.manoa.hawaii.edu/handle/10125/41666

[9] B. Goertzel. (January, 2017). The global brain and the emerging economy of abundance: Mutualism, open collaboration, exchange networks and the automated commons. *Technological Forecasting & Social Change* , *Issue 114* , pp. 65-73. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0040162516300117

[10] "Mt. Gox Seeks Bankruptcy After $480 Million Bitcoin Loss", *Bloomberg.com*, 2017. [Online]. Available: https://www.bloomberg.com/news/articles/2014-02-28/mt-gox-exchange-files-for-bankruptcy. [Accessed: 03- Dec- 2017].

[11] A. Borroni.(November, 2016). Bitcoins: Regulatory Patterns. *BANKING & FINANCE LAW REVIEW*, *32 B.F.L.R*, pp. 47-68.[Online] Available: http://search.proquest.com/openview/6ece22fc121cd28589d6a098898103c2/1?pq-origsite=gscholar&cbl=44976

[12] F. Glaser, Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis. Presented at Conference Hawaii International Conference on System Sciences (HICSS) 2017. [Online]. Available: https://scholarspace.manoa.hawaii.edu/bitstream/10125/41339/1/paper0190.pdf

[13] Dean, 51% attack (2015). URL http://cryptorials.io/glossary/51-attack/

[14] G. O. Karame, E. Androulaki, M. Roeschlin, A. Gervais, and S. Čapkun, "Misbehavior in Bitcoin," ACM Transactions on Information and System Security, vol. 18, no. 1, pp. 1–32, 2015.

[15] "Double Spending Risk Remains After July 4th Bitcoin Fork", *CoinDesk*, 2017. [Online]. Available: https://www.coindesk.com/double-spending-risk-bitcoin-network-fork/. [Accessed: 04- Dec- 2017].

[16] V. Buterin, "Selfish Mining: A 25% Attack Against the Bitcoin Network — Bitcoin Magazine", *Bitcoin Magazine*, 2017. [Online]. Available: https://bitcoinmagazine.com/articles/selfish-mining-a-25-attack-against-the-bitcoin-network-1383578440/. [Accessed: 04- Dec- 2017].

[17] *Novetta.com*, 2017. [Online]. Available: http://www.novetta.com/wp-content/uploads/2015/10/NovettaBiometrics_BitcoinCryptocurrency_WP-W_9182015.pdf. [Accessed: 04- Dec- 2017].

[18] "Deconstructing the DAO Attack: A Brief Code Tour", *Peter Vessenes*, 2017. [Online]. Available: http://vessenes.com/deconstructing-thedao-attack-a-brief-code-tour/. [Accessed: 04- Dec- 2017].

[19] J. W. Bos, J. Alex Ahlderman, N. Heninger, J. Moore, M. Naehrig, and E. Wustrow, "Elliptic Curve Cryptography in Practice," *ResearchGate.net*, 2017. [Online]. Available: https://www.researchgate.net/publication/274651795_Elliptic_Curve_Cryptography_in_Practice. [Accessed: 04- Dec- 2017].

[20] H. Mayer, "ECDSA Security in Bitcoin and Ethereum", *Blog.coinfabrik.com*, 2017. [Online]. Available: https://blog.coinfabrik.com/wp-content/uploads/2016/06/ECDSA-Security-in-Bitcoin-and-Ethereum-a-Research-Survey.pdf. [Accessed: 04- Dec- 2017].

[21] "How to Build a Better Bitcoin Wallet: Security Researcher Filippo Valsorda Calls For Developers To Use Safer ECDSA Operations", *Player.One*, 2017. [Online]. Available: http://www.player.one/how-build-better-bitcoin-wallet-security-researcher-filippo-valsorda-calls-developers-390197. [Accessed: 04- Dec- 2017].

[22] D. Palmer. (March, 2016). Blockchain Startup to Secure 1 Million e-Health Records in Estonia. [Online]. Available: http://www.coindesk.com/Blockchain-startup-aims-to-secure-1-million-estonian-health-records/

[23] L. Shin. (April, 2016). Republic of Georgia To Pilot Land Titling On Blockchain With Economist Hernando De Soto, BitFury. *Forbes.* Available: https://www.forbes.com/forbes/welcome/?toURL=https://www.forbes.com/sites/laurashin/2016/04/21/republic-of-georgia-to-pilot-land-titling-on-Blockchain-with-economist-hernando-de-soto-bitfury/&refURL=&referrer=#2d38f56f44da

[24] "Blockchain Land Title Project 'Stalls' in Honduras", *CoinDesk*, 2017. [Online]. Available: https://www.coindesk.com/debate-factom-land-title-honduras/. [Accessed: 04- Dec- 2017].

[25] Deutsche Börse Press Release. (January, 2017). "Deutsche Börse presents Blockchain concept for risk free cash transfer." [Online]. Available: http://deutsche-boerse.com/dbg-en/media-relations/press-releases/Deutsche-Boerse-presents-Blockchain-concept-for-risk-free-cash-transfer/2883236

[26] S. Leonard. (March, 2017). Ripple Selected to Participate in the Bank of England FinTech Accelerator. [Online]. Available: https://ripple.com/insights/ripple-selected-to-participate-in-the-bank-of-england-fintech-accelerators-exploration-of-the-use-of-Blockchain-for-global-rtgs/

[27] C. Metz. (December, 2016). Overstock Begins Trading Its Shares Via the Bitcoin Blockchain. *Wired.* [Online]. Available: https://www.wired.com/2016/12/overstock-com-issues-stock-via-bitcoin-Blockchain/

[28] "Overstock.com, Inc. - News Release", *Investors.overstock.com*, 2017. [Online]. Available: http://investors.overstock.com/mobile.view?c=131091&v=203&d=1&id=2220354. [Accessed: 04- Dec- 2017].

[29] Visa Press Release. (October, 2016). "Visa Introduces International B2B Payment Solution Built on Chain's Blockchain Technology", *Businesswire.com*, 2017. [Online]. Available: http://www.businesswire.com/news/home/20161021005212/en/Visa-Introduces-International-B2B-Payment-Solution-Built. [Accessed: 04- Dec- 2017].

[30] "About", *Hyperledger*, 2017. [Online]. Available: http://hyperledger.org/about. [Accessed: 04- Dec- 2017].

[31] "Ethereum Blockchain App Platform", *Ethereum.org*, 2017. [Online]. Available: [32] https://www.ethereum.org/. [Accessed: 04- Dec- 2017].

[32] "Quorum | J.P. Morgan", *Jpmorgan.com*, 2017. [Online]. Available: https://www.jpmorgan.com/country/US/EN/Quorum. [Accessed: 04- Dec- 2017].

[33] T. Lobban. (March, 2017). Quorum Overivew. *Github.* [Online]. Available: https://github.com/jpmorganchase/quorum/wiki/Quorum-Overview

[34] Quorum users (various, anonymous). (November, 2016). Quorum Whitepaper. *Github.* [Online]. Available: https://github.com/jpmorganchase/quorum-docs/blob/master/Quorum%20Whitepaper%20v0.1.pdf

[35] J. I. Wong, I. Kar. (July 2016). Everything you need to know about the Ethereum "hard fork". *Quartz.* [Online]. Available: https://qz.com/730004/everything-you-need-to-know-about-the-ethereum-hard-fork/

[36] "Ethereum's DAO Wars Soft Fork is a Potential DoS Vector", *Hacking Distributed*, 2017. [Online]. Available: http://hackingdistributed.com/2016/06/28/ethereum-soft-fork-dos-vector/. [Accessed: 04- Dec- 2017].

[37] "An overview of the blockchain universe – Blockchainers", *Blockchainers.org*, 2017. [Online]. Available: http://blockchainers.org/index.php/2016/12/27/blockchain_universe/. [Accessed: 04- Dec- 2017].

[38] M. Conti, S. E, C. Lal and S. Ruj, "A Survey on Security and Privacy Issues of Bitcoin", *Arxiv.org*, 2017. [Online]. Available: https://arxiv.org/abs/1706.00916. [Accessed: 04- Dec- 2017].

[39] "Could Blockchain Wipe Out DDoS Attacks? - BestVPN.com", *BestVPN.com*, 2017. [Online]. Available: https://www.bestvpn.com/blockchain-gladius-ddos/. [Accessed: 04- Dec- 2017].

[40] "Storing Data in the Cloud and Data Residency Laws", *Vaultive.com*, 2017. [Online]. Available: https://vaultive.com/wp-content/uploads/2015/08/Vaultive_storing-data-cloud-data-residency.pdf. [Accessed: 04- Dec- 2017].

[41] "The EU General Data Protection Regulation and the Blockchain", *Medium*, 2017. [Online]. Available: https://medium.com/learning-machine-blog/the-eu-general-data-protection-regulation-and-the-blockchain-1f1d20d24951. [Accessed: 04- Dec- 2017].

[42] T. Chen, X. Li, X. Luo, X. Zhang, "Under-optimized smart contracts devour your money - IEEE Conference Publication", *Ieeexplore.ieee.org*, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/7884650/. [Accessed: 04- Dec- 2017].