An Analysis and Enumeration of the Blockchain and Future Implications

Nathanial LeBlanc

A Senior Thesis submitted in partial fulfillment
of the requirements for graduation
in the Honors Program
Liberty University
Spring 2020

Acceptance of Senior Honors Thesis

This Senior Honors Thesis is accepted in partial
fulfillment of the requirements for graduation from the
Honors Program of Liberty University.

_____
Robert Tucker, Ph.D.
Thesis Chair

_____
Melesa Poole, Ph.D.
Committee Member

_____
David Schweitzer, Ph.D.
Assistant Honors Director

_____
Date

Abstract

The blockchain is a relatively new technology that has grown in interest and potential research since its inception. Blockchain technology is dominated by cryptocurrency in terms of usage. Research conducted in the past few years, however, reveals blockchain has the potential to revolutionize several different industries. The blockchain consists of three major technologies: a peer-to-peer network, a distributed database, and asymmetrically encrypted transactions. The peer-to-peer network enables a decentralized, consensus-based network structure where various nodes contribute to the overall network performance. A distributed database adds additional security and immutability to the network. The process of cryptographically securing individual transactions forms a core service of the blockchain and enables semi-anonymous user network presence.

An Analysis and Enumeration of the Blockchain and Future Implications

Introduction

Blockchain is a relatively new technology that has only in the past few years begun to rise in popularity and innovation outside of its current primary use: providing the backbone of cryptocurrency. The blockchain is essentially a network framework alternative to the traditional client-server model and any enumerations that have proceeded from this structure. Blockchain is designed to easily run and verify the validity of transactions occurring on the network. Bernard Marr (2018) succinctly describes blockchain as, "At its core, blockchain is an open, decentralized ledger that records transactions between two parties in a permanent way without needing third-party authentication" (Blockchain Separates from Bitcoin, par. 1). This ease of use and inherent security molded into the framework of this network style are essential aspects of blockchain. This thesis seeks to examine the history of the blockchain, the primary components that together form the blockchain, the security advantages and disadvantages provided by the blockchain, and an analysis of the current applications of blockchain technology and where blockchain technology could be applied in the future.

Description of The History and Fundamental Components of Blockchain

Blockchain technology is a relatively recent development in technology and even more recently began to be investigated as a possible network style of the future. First publicly emerging in 2008 with the launch of Bitcoin, blockchain technology is still very much a growing field. Blockchain for years has been tied to cryptocurrency, and its fate was dependent on the product it supported. Only in the past few years have people and companies begun viewing blockchain as a potential asset for the future of networking and transactions. There are three

major aspects of the blockchain that join together to form the backbone of blockchain technology: private and public key cryptography, a peer-to-peer network, and a distributed database. These will be analyzed in detail following a summary of the history of blockchain technology.

Background and History of Blockchain

From the beginning of its creation, blockchain has been tied to the cryptocurrency Bitcoin. Blockchain was released to the public along with Bitcoin in 2008. In 2008, someone utilizing the pseudonym Satoshi Nakamoto published an article detailing the creation of Bitcoin. Thombs and Tillman (2018) write:

> In October of 2008, a pseudo-individual named Satoshi Nakamoto, sent a white paper (*Bitcoin: A Peer-to-Peer Electronic Cash System*) attached to an email to a small group of Cyberpunks and Cryptologists and introduced a new form of electronic digital currency named Bitcoin. (p. 1)

An interesting note must be provided regarding Satoshi Nakamoto. For years the true identity of the Bitcoin creator was unknown. In 2016, an Australian computer scientist named Craig Wright claimed to be Satoshi Nakamoto. Mike Butcher (2016) then explored this claim of Craig Wright. The article states that many in the technology and cryptocurrency industry were skeptical of Wright's claim and believed that he had not sufficiently proven that he was Nakamoto. Thus, to this day, the identity of Nakamoto is shrouded in doubt and skepticism.

It wasn't for several years that blockchain began to be explored for its potential outside of cryptocurrency. The use of the blockchain as a foundational piece of cryptocurrency and the

lessons learned from this practice bear an important role in future blockchain uses. The current applications of blockchain and its potential future implications are analyzed later in this thesis.

An Overview of The Fundamental Components of The Blockchain

The blockchain is an intricate, unique method of networking and processing transactions. While blockchain itself may be complex and at times difficult to understand, it is comprised of several parts that each on their own are simple yet foundational components. This section provides an overview of the various parts of the blockchain and how they fit together to comprise the blockchain.

The blockchain is a string of blocks viewable by all users participating in the blockchain. Each block consists of several separate, verified transactions between users. A block is verified and added to the blockchain through what is known as a consensus mechanism. Each block in the chain stores information about transactions between users, and the blocks are connected to each other through hash functions. There are three fundamental components of the blockchain: private and public key cryptography, a peer-to-peer network, and a distributed database.

Peer-to-peer network The blockchain attempts to solve the problem of unverified transactions on a network and the subsequent need for a third-party verification system. This essentializes the need for blockchain to be formed around a peer-to-peer (P2P) network format. This demonstrates the purpose behind P2P networks as P2P networks are designed to operate without a central server. The point of a P2P network is to do away with the need for a central server. In the traditional client-server network model, there would be one or more servers that store information and control the flow of information to client computers. Clients make requests to the central server for needed information or to process some action or request. In a traditional

peer-to-peer network setup, the various computers on the network act as both the client and the server. All of the computers on the network lend computing power to operate the network, and when users wish to make a transaction or pass information, then one assumes the role of the client and the other passing information acts as a server. In this way, a P2P network allows for the elimination of dedicated servers and simply consists of the client devices.

P2P networking is essential to the blockchain framework. The point of the blockchain, especially when used to support cryptocurrency, is to provide a secure framework in which two users can complete a transaction securely directly between them. Utilizing the classic Alice and Bob framework of explaining different technological concepts, Subramanian and Chino (2015) outline the role of P2P networking in the blockchain:

> When Alice creates a transaction - i.e. to transfer some funds to Bob, she propagates the transaction into the P2P network. Alice does this by connecting to another node on the P2P network and making a simple transfer of the transaction data. (p. 5)

This demonstrates the direct connection aspect of the blockchain. This process is significantly more complex within a blockchain network, however. Individual transactions are verified by other users on the network after these transactions are completed. Users send and receive information and data directly from each other.

Distributed database. Another crucial component of blockchain is the distributed database that builds inherent security into the system. The blockchain, in essence, is a string of blocks connected together. This string of blocks is stored on a database. This database, however, is not stored on a singular server. There is no master copy of the database; instead, every user obtains a copy of the database. Different transactions are then verified through a

process called mining. This will be explained more deeply later in this thesis. Once the database has been validated (see section titled "A detailed consideration of the blockchain database and mining process" for a detailed explanation of this process) a sufficient number of times by various users, this highly authenticated database version is accepted as the legitimate database, and every user's copy is updated. This distribution of the database provides two benefits. First, it aids the decentralized structure of the blockchain and keeps the transactions out in the open. This makes fraud more difficult since all transactions must be verified before they are added to the blockchain. Second, and more importantly, this distributed database adds security into the blockchain structure and transaction process. Rechtman (2017) writes, "What started as a theoretical vision of integrity in recordkeeping has evolved into a distributed database structure with high fidelity of information quality and availability" (p. 1). A distributed database is difficult to manipulate or hack. A malicious person would need to modify every database or at least a majority of database copies to falsify information. With a traditional client-server network architecture, a hacker simply needs to find a way to deftly alter the singular master copy stored on the central server. In this way, blockchain technology greatly increases the security of transactions and the underlying database.

The role of cryptographic keys. There are two broad security elements that form the overall security component of blockchain. First, the network is secured as a whole through its structure and the verification of the blockchain and new blocks added. Second, each individual transaction is secured through some form of cryptographic key signature and hashing function. Wilczyński and Widłak (2019) write, "The data stored in the blocks are protected and encrypted by using the cryptographic methods specified for a given BC network. Usually, these include

public and private keys, digital signatures and cryptographic hash methods" (p. 3). The details of this process will be more deeply analyzed in the following section. Cryptography is an essential component of the blockchain and the blockchain's ability to provide secure, direct transactions.

Three primary benefits emerge from an analysis of blockchain's cryptographically secured transactions. Each transaction is semi-anonymous. Through the use of private and public keys, users need to provide a minimal amount of personal information to successfully complete a transaction. Each transaction is secured through the use of keys and a digital signature attached to a transaction throughout its completion process. Finally, each transaction is treated as a block that is secured to the blockchain through a hash function. This creates a link between the various blocks and forms the chain aspect of the blockchain. A more detailed examination of the various components of the blockchain will now be performed followed by a security examination and applications review.

An In-Depth Analysis of The Major Components of The Blockchain

Proceeding from a broad overview of blockchain and its fundamental components, this section provides greater analysis of the fundamental components of the blockchain, how they operate, and a discussion of the security strengths and weaknesses of the blockchain. The three fundamental components of the blockchain are: cryptographically secured transactions, a distributed database, and a P2P network format.

Investigation of The Three Major Components of The Blockchain

Once the various parts of the blockchain are understood, it is easier to see how they work together to form the blockchain. Thombs and Tillman (2018) produced an article outlining the idea and arguing for a class teaching the fundamentals of blockchain and Bitcoin. Within this

article, they succinctly summarized the main concepts that blockchain encompasses. They explain, “The important features that must be included in any treatment of blockchain must include: peer-to-peer, distributed, consensus-based, crypto logically secure, immutable, global, semi-anonymous, and decentralized” (p. 8).

An explanation of the blockchain’s cryptographic security features. There are two primary subjects that relate closely to the cryptographic security of the blockchain: cryptographic keys and hash functions. Cryptographic keys are used to secure individual transactions, and secondly hash functions are utilized to connect and secure consecutive blocks with each other. These provide the overall security of the block however there is much more contained within the block than simply a hash function and several transactions. Wilczyński and Widłak (2019) describe the common components of a block on the blockchain. First, a block contains multiple transactions between users. It contains a record of who transferred what and who received it. The blockchain achieves more efficiency by storing multiple transactions in a singular block. These transactions are secured as system of cryptographic keys, digital signatures, and transaction verification. Wilczyński and Widłak (2019), describing this process, write:

> Asymmetric key cryptography is usually used in BC systems for the authorization of processed transactions. A private key is used to sign transactions, a public key to identify addresses assigned to the user and to verify the signatures generated with the use of private key. (p. 3)

Asymmetric encryption is known for its use of two keys, a public key and a private key. Stallings (2017) defines asymmetric encryption according to these lines. He writes that two algorithms are used in asymmetric encryption: one for encryption and one for decryption.

Similarly, the two keys are used for this same purpose. Second, he states that users in a transaction have their own private keys and they share a public key. In relation to the blockchain, this encryption process is used to securely exchange information or data between users. Senders sign the transaction with their private key and then send the transaction to the recipient. This transaction now contains the digital signature provided by the sender and the public key that these users share for this transaction. Provided with the digital signature, a node on the blockchain can then verify the transaction (Wilczyński and Widłak, 2019). Thom and Tillman (2018) define semi-anonymous transactions as a core component of blockchain technology. This concept allows for minimal sharing of information. Users provide only enough personal information to make the transaction secure. This may include basic personal identifying information and encompasses the digital signature process. This method of processing transactions provides a marginal amount of personal information in transactions and thus maintains a higher level of privacy and security of personal information.

Blockchain technology relies heavily on the strength of hash functions. Each individual digital signature is a hash function that has been created using the public key and private key of the sender. Additionally, hash functions are invaluable for securing whole blocks on the blockchain. Stallings (2017) describes a cryptographic hash function as, "an algorithm for which it is computationally infeasible to find either (a) a data object that maps to a pre-specified hash result or (b) two data objects that map to the same hash result" (p. 340). This introduces two important principles regarding secure hash functions. First, there must be almost no chance that someone can find another number that maps to the same hash location as the one the function already has. This is called collision resistance. Second, a hash function must be completely

infeasible for someone to hack the hash function by using a pre-identified value to compare to. This is called preimage resistant. A block generally contains three hash values along with the transaction information. The first value is the hash value of the block itself. This is used in the process of mining, which verifies individual blocks. Second, the block contains the hash value of the previous block so as to link it to the blockchain. Finally, the block often contains a Merkle tree hash. This hash value is acquired through the combination of hashing the individual hash values for the separate transactions. Blockchain hash functions can theoretically be any hash function, but only the best and strongest should be used for optimal security. This largely includes the world's most used hash algorithm, SHA (Secure Hash Algorithm). Explaining the process of SHA hash functions is beyond the purview of this thesis; however, it should be mentioned briefly that many products that utilize the blockchain use SHA hashing. For instance, Bitcoin hashes its values using the double SHA-256 standard (Subramanian and Chino, 2015).

This demonstrates the best process for making the blockchain "crypto logically secure" (Thombs and Tillman, 2018, p. 8). The process must be simple to execute yet cryptographically secure simultaneously. The blockchain marries these two concepts together. Keys and hash algorithms employed by blockchain networks are most often secure, or secure technology is recommended. Users need not worry about the encryption or security process. They only need to keep secret and secure their private key.

There are two final components of a standard block on the blockchain. First, a block will contain a timestamp. This will signify when it is officially added to the blockchain. Second, the block contains a numerical value known as the nonce. The nonce is described as a random seed. (Subramanian and Chino, 2015). Nofer, Gomber, Hinz, and Schiereck (2017) describe the nonce

as, “a random number for verifying the hash” (p. 2). The nonce is appended to the hash value for that block. This combination of hash and nonce is used in the mining process and represents the target value which miners must achieve. Miners attempt to solve difficult mathematical problems to verify a blockchain block. A problem is considered solved once the miner gets an output value that matches the combination of hash and nonce mentioned above. This is an important piece of the process of verifying individual blocks and adding them to the blockchain.

An analysis of the peer-to-peer network framework and blockchain structure Now that the components of an individual block and the transaction process have been examined, an analysis of the overall network structure must be considered. As mentioned in the overview section, blockchain networks and applications that utilize blockchain employ P2P network frameworks. The purpose is to form a network that is peer-to-peer, global, and decentralized (Thombs and Tillman, 2018). The blockchain must be peer-to-peer. Information and data are not funneled through one source, i.e. a central server. All users on the network act as both clients and servers. A blockchain network is decentralized: it is not controlled by a single user or group of users, but instead, all users theoretically have the same power and abilities on the network. Finally, a blockchain is global. This simply means that it is accessible and available to everyone in the target audience. For instance, Bitcoin is designed so that anyone can interact with it so its blockchain is extremely large and accessible by anyone. A private blockchain would be accessible by whoever has access to and has permissions on that network.

A blockchain network consists of four distinct parts. It contains the blockchain database containing the information and transactions previously discussed, ordinary users participating in transactions, nodes for verifying transactions, and mining nodes for adding blocks to the

blockchain. The majority of nodes on the network constitute users that only participate in transactions and do not serve any other extra purpose. Other nodes on the network perform additional actions that benefit the blockchain as a whole. The main purpose of these nodes is to verify individual transactions and thus increase the security level of the blockchain. These nodes review a transaction, examine the key signatures of the sender and receiver, and then verify the authenticity of the transaction if everything matches. These nodes have algorithms to verify transactions once the transaction has moved past the sender and receiver. After the transaction is verified by a node it is considered complete and added to a block of transactions. Finally, the mining nodes are used to verify whole blocks themselves. This is accomplished through the solving of difficult computational problems.

A detailed consideration of the blockchain database and mining process. Returning to the outline of standard blockchain characteristics, a blockchain is also distributed, immutable, and consensus based (Thoms and Tillman, 2018). Due to the P2P network setup and the distributed database, the blockchain is decentralized; it draws support and structure from the various nodes on the network acting to achieve a common goal of keeping a secure, smooth-running network structure. Each node receives a copy of the blockchain database. Data stored on a singular server is at risk of outside manipulation. Malicious parties have the potential to, if they bypass certain security measures, change the content or state of data in a database. If this is successful, the data is untrustworthy, and this launches a multitude of potential issues. The blockchain is designed to be immutable. This means that someone cannot access the database, change data, and cause harm to the network at large. Since the blockchain is distributed, it is far more difficult to convincingly change data on the blockchain. At the very least, a hacker would

need to modify a plurality of copies of the blockchain to get this version of the blockchain accepted as the standard version. This inherent security provides a major benefit over traditional network models. However, this practice has its weaknesses as well. There are vulnerabilities in this setup that can be exploited. These weaknesses will be reviewed in further detail in subsequent sections focusing on the security of the blockchain.

The final essential blockchain descriptor outlined by Thoms and Tillman (2018) states that the blockchain is consensus-based. This refers to the process of adding blocks to the blockchain. To officially add a block to the blockchain, a majority of nodes on the network must have verified the block and agreed to add it to the blockchain. This process is known as mining and constitutes a vital part of the blockchain. Mining nodes on a blockchain network verify individual blocks, confirm the result with other nodes on the network, and finally attach the block to the blockchain once it has been sufficiently vetted. A block is verified and added to the blockchain through what is known as a consensus mechanism. A consensus mechanism is explained by Nofer et al. (2017), "If the majority of nodes in the network agree by a consensus mechanism on the validity of transactions in a block and on the validity of the block itself, the block can be added to the chain" (p. 2). There are two primary consensus mechanisms utilized by blockchain applications. These are proof of work and proof of stake models.

Wilczyński and Widłak (2019) explain the process of proof of work mining as: "Here, each external user may add a new block to the existing chain after solving a computationally intensive puzzle" (p. 4). This consensus mechanism is by far the most popular method of verifying blocks. The authors proceed further to discuss the requirements of these puzzles. They must meet two standards to be considered a rigorous process. The computation must be non-

trivial and difficult to solve. This provides a difficult standard that, if met, one can be confident the problem was solved legitimately. The second standard is that the solution must be easily verified once it is found. Other nodes on the network need to be able to easily check and verify the work of the mining node. The process involves three components: the nonce value for that block, the hash value for that block, and an additional component included often to make the calculations more difficult. The goal of the miner is to successfully identify a hash value of the nonce combined with the extra component (it is often a string or something that will combine with the nonce to be hashed) that matches the hash value of the block under examination. This process is difficult and requires much computing power. In order to incentivize user nodes on the blockchain network to participate in proof of work mining, a reward is provided for successfully solving a puzzle and verifying a block. For example, the Bitcoin blockchain rewards a successful mine with a part of a Bitcoin.

The second consensus mechanism worth mentioning is the proof of stake (PoS) method. Wilczyński and Widłak (2019) describe this method as:

> In the proof of stake model, the consensus between network blocks is not achieved by mining nodes, but through the miners having stake/tokens. The higher the stake of a given user, the more likely they are to join the block to BC. (p. 5)

There are several different implementations of PoS that provide different benefits and drawbacks. One popular aspect of proof of stake verification, especially in older implementations, is the coin age. Coin age represents how long a user has held an unspent cryptocurrency. The longer it has been held without being involved in a transaction, the more power it has in influencing the verification of different blocks. A limit is placed often on the

maximum power a coin can hold after a certain number of days. This is to prevent a scenario where a large amount of cryptocurrency, held out of transactions for a long period of time dominates the verification process. This method is designed to be less taxing and consume less resources than the proof of work model. “The advantage of PoS consensus is that it does not require participants to go through an expensive mining process such as PoW” (Sayeed and Marco-Gisbert, 2019, p. 7).

An Analysis of The Current Security Strengths and Weaknesses of The Blockchain

The blockchain generally presents an upgrade in overall security and anonymity when compared to a traditional client-server model network. Data is generally more secure on the blockchain database than sitting on a single server. The use of cryptographically secure transactions along with the removal of third-party authentication also enhances the security of the blockchain. There are weaknesses in the blockchain that have emerged, however. The blockchain is poor at storing information that must be kept completely secret due to the current structure of the network. Additionally, the blockchain tends to be at risk of attacks centering around the mining process and users’ greed.

Security strengths of the blockchain. The foundation of the blockchain and blockchain security is based on two concepts: the security of the blockchain itself as a whole and the security and validation of each individual block of the blockchain. One of the risks of a central server and database is someone gaining unauthorized access to the database and stealing or manipulating information. This manipulation is much more difficult on the blockchain because of the distributed nature of the blockchain. A malicious hacker would need to figure out a way to change the information on everyone’s copy of the blockchain.

On an individual level, each individual user's information is secured through cryptographic keys and encryption. Each user possesses a private and public key that are used for transactions to access information on the blockchain. Users control their information or data because their private key is linked to this information and thus no one can just try and use the information. These keys are also used for making transactions with other users. This protects both the data in transit and a certain level of anonymity for the users. These transactions must also be verified as not being fraudulent for this process to be sustainable. In this vein, the blockchain also provides a method of verifying transactions. These transactions are attempted by the users and then before this block of a transaction is added to the blockchain a plethora of computers utilizing a certain amount of their CPU verify these transactions. In the case of Bitcoin, users that perform this action receive Bitcoin for their troubles. In this scenario, users do not want someone to be able to send their bitcoin to multiple people at once and thus cheat the system. Nolan Bauerle (2019) describes this overall process as:

> To achieve this, the nodes serving the network create and maintain a history of transactions for each bitcoin by working to solve proof-of-work mathematical problems. They basically vote with their CPU power, expressing their agreement about new blocks or rejecting invalid blocks. When a majority of the miners arrive at the same solution, they add a new block to the chain (Network Servicing Protocol, paras. 5-6).

Thus, the process of individual transactions is secured by the overarching community.

There are several specific security topics that play a crucial role in the overall security level of the blockchain. They exist more as standards that, if not adhered to, severely limit the security of the blockchain and open it up to unneeded risks. The first such topic is the

asymmetric encryption employed to secure individual transactions and the users participating in them. There are several standards that quality, secure algorithms must meet. Stallings (2017) outlines three characteristics of asymmetric encryption needed for security:

1. One of the two keys must be kept secret
2. It must be impossible or at least impractical to decipher a message if one of the keys is kept secret
3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be inefficient to determine the other key. (p. 289)

The first rule is the simplest to understand and simply states that in order for the algorithm to work, one of the keys must be secret. If it were not, then anyone could decrypt what was encrypted since both pieces are public. The second rule means that the algorithm must generate encryptions that cannot be deciphered/hacked without the presence of the secret private key. Finally, the algorithm must be complex enough that even provided the public key, knowledge about the algorithm itself, and some text encrypted by the algorithm, someone still cannot determine what the private key is. This demonstrates the rigorous requirements that quality algorithms must meet and thus all blockchain applications should utilize proven, secure encryption.

The final security strength discussed here is the blockchain's ability to support semi-anonymous transactions and user presence. Users on blockchain networks often need to provide less authentication than users on standard networks. This is due to the cryptographically secure transaction process and digital signature. These keys and digital signatures provide a level of certainty in that someone is dealing with a trusted user, trust that would normally need to be

evidenced through more personal information and a good track record. This provides a good opportunity and common ground to shift into an important security practice, minimal privilege. This security practice states that users should have the least amount of access needed to perform their role in the company or on the network. No one user on a blockchain network has an imbalanced amount of power compared to his/her peers. Minimal privilege is an important security practice and should be adhered to.

Security weaknesses of the blockchain. While the blockchain does offer new and innovative methods of securing data and transactions, it is by no means perfectly secure. The blockchain is still susceptible to various network-based attacks such as denial of service attacks. Additionally, as with all systems, the blockchain users are the most vulnerable element of the system. Users could get their information stolen if they are not careful with it, such as logging in or making transactions while connected to an untrusted network. Social engineering practices such as phishing, pharming, and in person social engineering are all risks as well. One of the weaknesses of the blockchain is also one of its strengths. The verification process of the blockchain, especially for something like Bitcoin where miners get a large incentive for maximizing their mining capabilities and output can play against a blockchain. There are various attacks and manipulations that take advantage of this mentality and weakness. Additionally, blockchains simply are not feasible for storing highly sensitive or private data. The blockchain is designed more for secure and distributed transactions. This works because the transactions contain select information about what the blocks contain but not the entire picture. Highly sensitive information stored statically on a database can’t have even this select information available. This increases the chances that someone may be able to hack a certain

person or block and gain access to this information. Having more copies of the database provides more opportunities for someone to hack the database based upon varying personal security protocols of those connected to the blockchain network. Ultimately, the blockchain is best suited for secure, encrypted data transactions instead of storing highly sensitive information.

A discussion of specific blockchain vulnerabilities. A discussion is now necessary to analyze several important and specific blockchain attacks. The two topics discussed in this section will be the standard DDoS attack and what is known as the 51% attack. A DDoS attack is a distributed denial-of-service attack. In this type of attack someone, usually a malicious organization or botnet, floods a network with traffic or server requests, effectively making the network inoperable. Sayeed and Marco-Gisbert (2019) describe the potential impact of DDoS attacks saying:

> DDoS is one of the most common attacks in the blockchain network used by attackers to obstruct authentic transactions so that invalid transactions can be executed. However, due to the decentralized nature of blockchain, DDoS can mitigate network activity only to a certain level. (p. 5)

The authors demonstrate that DDoS attacks are a problem for blockchain networks and slow valid transactions while allowing inauthentic transactions to slip through. Blockchain networks, however, do often provide better resistance to DDoS attacks as compared to traditional network models due to the distributed nature of the blockchain.

The 51% attack is unique to the blockchain, specifically the proof of work consensus model. Sayeed and Marco-Gisbert (2019) define this attack:

> The 51% attack is a technique that occurs when an attacker is in possession of 51% of the hashing power. This attack starts by creating a chain of blocks privately, which is fully isolated from the real version of the chain. At a later stage, the isolated chain is presented to the network to be established as a genuine chain. (pp. 2-3)

This is a rare attack due to the computing power required to achieve this result, however with growth in technology it is becoming easier to perform. The thought process of this attack stems from the desire to control what is added to the blockchain. If a mining node can control a majority of the hashing power, then they form the consensus on what blocks are added to the blockchain. This allows attackers to introduce their own, self-beneficial and inaccurate blockchain copy. A similar attack known as the selfish mining attack uses the greed of miners to convince them to join the malicious miner block and gain 51% of the hashing power on the network. (Bai et al. 2018).

Present and Future Applications of The Blockchain

Blockchain is still a young technology that has many potential applications. Currently it is still dominated by cryptocurrency in terms of usage. However, efforts have been made in recent years to examine blockchain's potential for a wider variety of topics including some unorthodox. Rossi, Mueller-Bloch, Thatcher, and Beck (2019) write, "Blockchain's potential to transform markets and societies has motivated public and private organizations to make deep investments" (p. 1).

An Analysis of Present Applications for Blockchain

Blockchain technology is a fascinating topic that has begun to enthrall companies with its potential. Major research has been dedicated to analyzing the potential applications of blockchain technology. The blockchain, since its inception, has been tied to cryptocurrency, specifically Bitcoin. This domination in use cases by cryptocurrency, while slowly shifting, still has not changed in a significant way. Nofer et al. (2017) write, "Blockchain technology and distributed ledgers are attracting massive attention and trigger multiple projects in different industries. However, the financial industry is seen as a primary user of the blockchain concept" (p. 1). Cryptocurrency utilizes the security, distribution, and semi-anonymity of the blockchain structure to create global networks of purely digital, valued currency.

An Analysis of Potential Future Applications for Blockchain Technology

There are two dominating areas of potential blockchain applications in research currently. First, the ability of blockchain to support activities involving standard operations or practices and relative anonymity is currently being investigated. This includes activities such as banking, the power grid, and voting. The other primary application under research is utilizing blockchain with Information of Things technology.

Current research is centered largely around blockchain's potential application for somewhat standardized, distributed products. It appears that the best use for blockchain is in fields with little fluctuation in user action or product use cases. The system naturally tends to gravitate towards a distributed network setup, and semi-anonymous transactions or actions would be the preferred state on a P2P network. Chong, Lim, Hua, Zheng, and Tan (2019) write:

> Due to a paucity of studies on the business applications of blockchain, scholars are divided on the extent to which value can be appropriated from blockchain. On the one hand, blockchain proponents regard blockchain as a disruptive technology that will pave the way for novel business models centered on distributed consensus. (p. 3)

These "novel business models" (Chong et al. 2019, p. 3) include things such as the power grid and voting. These make good potential applications for blockchain due to the security required of their actions, the primary action (paying a bill or voting) is fairly standardized across a potential network. This standardized action makes it easier for a blockchain network to be built around it and protect it. Finally, these models are best run where the users have a level of anonymity from each other. This is a strength of the blockchain. This brings the discussion back to what doesn't work on the blockchain. Things that have a high degree of variability in the actions performed or the way they are performed struggle to translate to the blockchain. Additionally, the blockchain struggles to hold top secret information due to its natural tendency to work better in an environment involving many transactions. The P2P network layout would make keeping the type of information secret as well.

The final future application being currently researched is blockchain's potential impact on Internet of Things (IoT) devices. An IoT device is a device that is connected to the internet or a network, yet its primary function is not internet related. An example would be a smart refrigerator. The primary purpose is to act as a refrigerator, but it can also connect to the internet to enhance user experience. Atlam, Alenezi, Alassafi, and Wills (2018) describe IoT as, "the connection and communication of different devices over the Internet" (p. 2). The authors of this article outline several reasons for why IoT may possibly adopt blockchain. The distributed, P2P

network structure is ideal for IoT. It allows IoT devices to be connected and controlled by the blockchain at large and the inerrant security it provides. IoT transactions are best suited for the semi-anonymous, secure state of the blockchain. Atlam et al. (2017) write, "The decentralized, autonomous, and trustless capabilities of the blockchain make it an ideal component to become a foundational element of IoT solutions" (p. 5). There are challenges, however. Blockchain technology tends to consume a lot of resources, and this may hinder the growth of IoT. Finally, IoT is also a rapidly growing field, and networks of IoT devices would need the potential to grow very large. Currently, blockchain networks tend to scale poorly when too many devices or nodes are added to the network. All said, however, blockchain is an interesting companion for IoT and IoT connected networks.

Conclusion

The blockchain is a unique networking structure that is still relatively new. Invented in 2008, blockchain is still dominated by cryptocurrency in terms of usage. Blockchain was built specifically to provide a decentralized, peer-to-peer platform to support Bitcoin and now multiple different cryptocurrencies. The blockchain consists of a P2P network with a distributed database. A hallmark of blockchain technology is a semi-anonymous transaction process with cryptographically secure transactions. The blockchain provides many security benefits over traditional central networks including a high level of immutability. Weaknesses in the mining process of the blockchain do exist, however, and can leave the blockchain vulnerable to sophisticated 51% attacks. Current applications are still dominated by cryptocurrencies; however, major research is being conducted to investigate the viability of blockchain for more traditional uses and potential IoT applications.

References

Abdullah, R. S., & Faizal, M. A. (2018). Block chain: Cryptographic method in fourth industrial revolution. *International Journal of Computer Network and Information Security*, *9*(11), 9. Retrieved from http://dx.doi.org.ezproxy.liberty.edu/10.5815/ijcnis.2018.11.02

Atlam, H. F., Alenezi, A., Alassafi, M. O., & Wills, G. B. (2017). Blockchain with Internet of Things: Benefits, challenges, and future directions. *Intelligent Systems and Applications, 10*(6), 40-48. DOI: 10.5815/ijisa.2018.06.05

Augos, W.H. (2018). 10 Interesting Facts about blockchain history that everyone should know *M2 Presswire*. Retrieved from http://ezproxy.liberty.edu/login?url=https://search.proquest.com/docview/2154953194?accountid=12085

Bai, Q., Zhou, X., Wang, X., Xu, Y., Xin, W., Kong, Q. (2018). A deep dive into blockchain selfish mining. *Cornell University: arXiv.org* Retrieved from arXiv:1811.08263

Bauerle, N. Blockchain 101. *Coindesk.* November 22, 2019. Retrieved from: https://www.coindesk.com/learn/blockchain-101/what-is-blockchain-technology

Butcher, M. (2016). Major questions arise over Craig Wright's claim to be Satoshi Nakamoto. Retrieved from https://techcrunch.com/2016/05/02/major-questions-arise-over-craig-wrights-claim-to-be-satoshi-nakamoto/

Buterin, V. (2013). *Selfish mining: A 25% attack against the Bitcoin Network*. Bitcoin Magazine. Retrieved from https://bitcoinmagazine.com/articles/selfish-mining-a-25-attack-against-the-bitcoin-network-1383578440

Chong, A. Y. L., Lim, E. T. K., Hua, X., Zheng, S., Tan, C-W. (2019). Business on chain: A comparative case study of five blockchain-inspired business models. *Journal of the Association for Information Systems 20*(9), 1308-1337. doi: 10.17705/1jais.00568

Cole, R., Stevenson, M., & Aitken, J. (2019). Blockchain technology: implications for operations and supply chain management. *Supply Chain Management: An International Journal 24*(4), 469-483. DOI 10.1108/SCM-09-2018-0309

Cope, J. (2002). What's a Peer-to-Peer (P2P) network? Retrieved from https://www.computerworld.com/article/2588287/networking-peer-to-peer-network.html

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond Bitcoin. *Applied Innovation Review June 2016*(2), 6-19. Retrieved from https://j2-capital.com/wp-content/uploads/2017/11/AIR2016-Blockchain.pdf

Hyland-Wood, D. & Khatchadourian, S. (2018). A future history of international blockchain standards. *The Journal of The British Blockchain Association 1*(11), 2516-3949. doi: 10.31585/jbba-1-1-(11)2018

Kot, I. (2019). A weak link: Is blockchain as secure as we think it is? *ITProPortal*. Retrieved from https://www.itproportal.com/features/a-weak-link-is-blockchain-as-secure-as-we-think-it-is/

Lone, A. H. & Mir, R. N. (2018). Investigating and analyzing bitcoin blockchain protocol using Wireshark. *Computer Network and Information Security 11*(7), 36. DOI: 10.5815/ijcnis.2018.07.04

Marr, B. (2018). A very brief history of blockchain technology everyone should read. *Forbes*. Retrieved from https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read/#2c82915e7bc4

Martin, T. How blockchain will disrupt your industry. Image retrieved from https://www.slalom.com/insights/how-blockchain-will-disrupt-your-industry

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering 59*(3), 183–187. DOI 10.1007/s12599-017-0467-3

Orgera, S. (2018). Blockchain Technology Explained. *Chinese American Forum, 34*(1), 9–10. Retrieved from https://search.ebscohost.com/login.aspx?direct=true&db=asn&AN=131557863&site=ehost-live&scope=site

Pederson, A. B., Kisius, M., & Beck, R. (2019). A ten-step decision path to determine when to use blockchain technologies. *MIS Quarterly Executive 18*(2), 99-115. Retrieved from https://www.researchgate.net/publication/333545589_A_Ten-Step_Decision_Path_to_Determine_When_to_Use_Blockchain_Technologies

Rechtman, Y. (2017). Blockchain: The making of a simple, secure recording concept. *The CPA Journal 87*(6), 15-17. Retrieved from https://www.cpajournal.com/2017/07/14/blockchain-making-simple-secure-recording-concept/

Rossi, M., Mueller-Bloch, C., Thatcher, J. B., & Beck, R. (2019). Blockchain research in information systems: Current trends and an inclusive future research agenda. *Journal of the Association for Information Systems 20*(09), 1388-1403. doi: 10.17705/1jais.00571

Sayeed, S. & Marco-Gisbert, H. (2019). Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack. *Applied Sciences 9*(9), 1-17. doi:10.3390/app9091788

Stallings, W. (2017). *Cryptography and network security*. Uttar Pradesh, India. Pearson Education Limited

Subramanian, R. & Chino T. (2015). The state of cryptocurrencies, their issues and policy interactions. *International Information Management Association, Inc 24*(3), 25-40. Retrieved from https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1045&context=jitim

Thombs, M. & Tillman, A. A. (2018). Designing 21st century curriculum for Bitcoin and blockchain studies. *International Journal of Global Business, 11*(1), 67-80. Retrieved from https://gsmi-ijgb.com/wp-content/uploads/IJGB-V11-N1-P04-Michael-Thombs-Bitcoin.pdf

Wilczyński, A. & Widłak, A. (2019). Blockchain networks – Security aspects and consensus models. *Journal of Telecommunications and Information Technology* (2), 46-52. Retrieved from https://doi.org/10.26636/jtit.2019.132019