University of Windsor

Computer Networks

03-60-367 Fall 2017

Blockchain - A Networking Perspective

Author:
Joel Rorseth 104407927

Supervisor:
Dr. Robert Kent

November 26, 2017

Blockchain - A Networking Perspective

Joel Rorseth
School of Computer Science
University of Windsor
Windsor, Ontario
Email: rorsethj@uwindsor.ca

***Abstract*—With the recent rise of cryptocurrencies such as Bitcoin and Ethereum, so too has skepticism and scrutiny about the security and technology backing this next generation currency. Yet despite this, a new age of networking technology and security is being ushered in. Blockchain, the backing technology of Bitcoin, has leveraged the security and efficiency of traditional Peer-to-Peer networks to host revolutionary, transparent distributed ledgers. Using the connected nodes in the network, open ledgers can be maintained, associating definitive and authoritative history to virtually anything that can be quantified or owned. By utilizing advanced encryption and cryptography mechanisms, data can be open sourced by allowing users to verify, store and create transaction that will forever be maintained as history. Blockchain is realizing security principles such as data transparency and decentralization on a global scale, and is ushering in the largest revolution in networking technology since the creation of the world wide web.**

I. Introduction

Following the rise of revolutionary paradigms in modern computing such as personal computers, the Internet, and social networks, we have seen countless new technologies, companies, and hardware developed in their shadow. With the unrivaled explosion of cryptocurrencies in the 2010's, we are undoubtedly part of yet another revolution of modern computer technology. With the formal introduction of Bitcoin in 2009, the concept of a global scale decentralized network was made a reality. Similarly to how the Internet's technology has provided a foundation for websites, streaming services and more, the core technology of cryptocurrency will drive a new generation of innovation. This backing technology, known as Blockchain, has applications that began in currency, but is rapidly expanding to all areas of modern society.

From a networking perspective, Blockchain is the culmination of several recent, advanced networking concepts. From the start, the methodology behind cryptocurrency has been to offer a traceable and secure currency, free from third parties (such as a central bank) and digital tampering. To prevent people from stealing currency or double charging, the concept of an authoritative distributed ledger was implemented in the form of a Peer-to-Peer file sharing network. Acting as the backbone to the security of cryptocurrency, the public ledger represents a much broader decentralized network, shared and visible to all participants. In a general sense, all existing Bitcoins are nodes in a massive distributed network, acting together as a database for maintaining records of all transactions.

II. Origins in Bitcoin

In order to fully understand the Blockchain concept, we must first investigate Bitcoin to form a technological distinction between these two tightly knit concepts.

A. History

Due to its recent birth, the term Blockchain has commonly been misinterpreted and confused with several concepts from Bitcoin. Blockchain technology was given life in 2009 with the formal invention of Bitcoin, from which Blockchain originates. The Bitcoin Blockchain, perhaps the most famous Blockchain implementation to date, is simply one large distributed network dedicated to maintaining authoritative transaction history. Formally, Bitcoin made its debut in November 2008 with Bitcoin: A Peer-to-Peer Electronic Cash System [1], a comprehensive thesis distributed across an American cryptography mailing list. Written by anonymous Bitcoin mastermind Satoshi Nakamoto, it details the architecture and implementation behind the Bitcoin technology. Bitcoin, an entirely virtual currency, builds itself upon a ledger of transaction history distributed and maintained by participating nodes in the Bitcoin blockchain. In order to fulfill the function of traditional, physical currency, three primary purposes were established for this technology:

1) To simplify the exchange of assets
2) To represent value that users may own and save for future purpose
3) To represent a standard unit for measuring value in all forms of assets, goods or services

B. Building on Blockchain

Prior to the release of Bitcoin, digital currency had been deemed unfit for many reasons, posing many inherent flaws and potential security concerns. However, with the advent of Blockchain, the possibility of a feasible digital currency became a reality. Put simply, the blockchain originated as an architectural solution for storing transactional information in the original Bitcoin source code. It has since been adopted and repurposed for all kinds of technology applications, and is still very much in its infancy. The blockchain technology specifically addresses the historical issues of virtual currency, and is the primary reason that cryptocurrency has been able to break into the economy. With Bitcoin, all transactions are permanently recorded by Bitcoin's blockchain, essentially a completely public ledger that anybody may view. To maintain

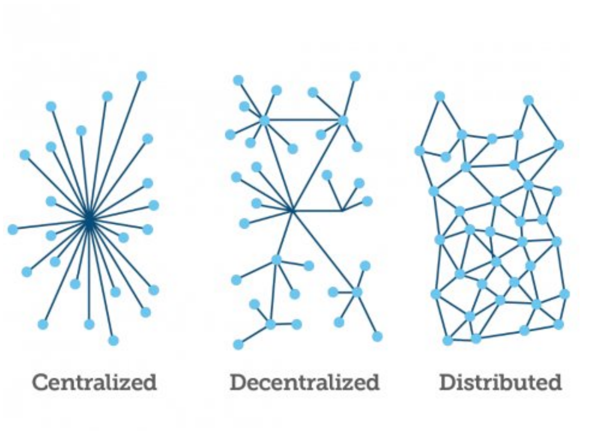


Fig. 1. Comparison of blockchain distributed network to competing designs

the ledger, this history is represented in a massive distributed network shared and verified by all Bitcoin users. Harnessing the power of the Blockchain theory, cryptocurrencies may easily enforce the following core principles cited by Satoshi Nakamoto in [1]:

- Facilitate transactions directly without involving a trusted third party
- Prevent double spending
- Persistent transaction history with irreversible transactions
- Decrease transaction fees and minor credit cost

With these values strictly enforced, Bitcoin has been able to maintain constant, uninterrupted operation since inception. Users have been increasing worldwide, growing the Bitcoin blockchain to all parts of the world.

C. Distinction Between Bitcoin and Blockchain

Before proceeding with a technical investigation of blockchains, we must distinguish between the functionality strictly encompassed by Bitcoin and blockchains respectively. In short, Bitcoin is strictly a virtual currency, in which users may obtain bitcoins by means of mining or exchange. Blockchain is strictly a distributed ledger, which achieved fame by providing the supporting ledger to Bitcoin. While Bitcoin has experienced much controversy for its unregulated operation and potential use in illicit transactions, blockchains have garnered a significantly cleaner reputation with the potential to usher in a new generation of security. Bitcoin employs several networking technologies that are also associated with blockchains, such as Peer-to-Peer networking and distributed systems. Moreover, Bitcoin is itself an expansive network of currency, while the blockchain (in the context of Bitcoin) is more akin to a distributed database. Considering the fact that a blockchain maintains a distributed ledger, the networking of such a ledger on a massive scale is a highly important topic. Although blockchains are being deployed separately across the world, the networking implementation will play a vital role in the mainstream adoption of its technology and the security advances it promotes. Undoubtedly, such networks will demand scalability, reliability, speed and methods to ensure security and data verification. These concepts are essential to any network, but are of extreme importance in the context of currency. As such, a networking analysis will the focal point of discussion for the remainder of this paper.

III. Blockchain Architecture

From a networking perspective, a blockchain is an application running across a distributed network of servers. This network model is implemented using the Peer-to-Peer (P2P) distributed application architecture. This essentially puts blockchains in the Application Layer of the traditional network stack model. The blockchain application is merely a database, which models a ledger of transactions by storing and sharing data across this network of servers. In this massive network, nodes are distinguished as being miners or users. In order to distribute the ledger database efficiently, the recorded transactions are broken up into blocks. Blocks store all information about recent transactions in the network, combined with a history of its past and data about the future.

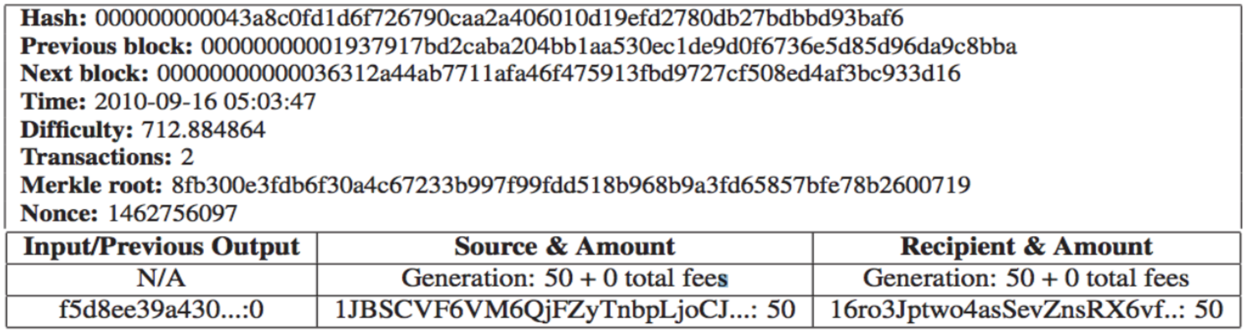
These aspects of the blockchain architecture will now be explored in great detail in the following subsections.

A. Nodes

Participants in a blockchain network identify themselves as nodes of two distinct categories, miners and users. While users are the average currency holders and creators of transactions, miners are the network members who uphold and verify the distributed ledger via a widespread consensus.

1) Users: In light of the computational advantages of traditional Peer-to-Peer networks, certain realities must be accepted for the system to work. In Peer-to-Peer networks, every node is a participant whom hosts a certain amount of a file to be shared to every other participant in the network. Likewise, files are stored across most participant machines to avoid a central server bearing this responsibility on its own. However, blockchain allows nodes to participate in the network without bearing any responsibility of broadcasting shared data. In reality, users are real people who are making transactions, sending or receiving money, or simply observing the public ledger independently. The design of blockchain networks prioritizes this minimal involvement for everyday users, which may grow to support billions of people in a currency application such as Bitcoin. Thus, users may utilize the network without downloading a full copy of the blockchain ledger [3]. This is quite the opposite of the miner nodes, whom in exchange for hosting a constantly updated complete ledger copy, possess voting rights for changes occurring in the blockchain network.

2) Miners: Traditionally, Peer-to-Peer networks have been susceptible to selfish behaviour. Users who intend to download files from the distributed participants may afterwards leave, and avoid contributing by redistributing the file to others. This dilemma, dubbed the Free-Riding Problem [4], is addressed uniquely in blockchain networking. With miners, blockchain is allowing nodes to be a foundational participant in exchange



Hash: 000000000043a8c0fd1d6f726790caa2a406010d19efd2780db27bdbbd93baf6
Previous block: 00000000001937917bd2caba204bb1aa530ec1de9d0f6736e5d85d96da9c8bba
Next block: 00000000000036312a44ab7711afa46f475913fbd9727cf508ed4af3bc933d16
Time: 2010-09-16 05:03:47
Difficulty: 712.884864
Transactions: 2
Merkle root: 8fb300e3fdb6f30a4c67233b997f99fdd518b968b9a3fd65857bfe78b2600719
Nonce: 1462756097

Input/Previous Output	Source & Amount	Recipient & Amount
N/A	Generation: 50 + 0 total fees	Generation: 50 + 0 total fees
f5d8ee39a430...:0	1JBSCVF6VM6QjFZyTnbpLjoCJ...: 50	16ro3Jptwo4asSevZnsRX6vf..: 50

Fig. 2. Example of a typical block representation for a Bitcoin block, as illustrated in [10]. This block contains two transactions as seen at the bottom, one of whom is responsible for awarding the winning miner with 50 bitcoins.

for possible incentives. Miners take responsibility and compete to be the first to calculate a target hash. In the case of Bitcoin, Bitcoins are awarded as incentive, although more is required by miners in Bitcoin's specific blockchain network to be awarded these. Miners play a vital role in the operation of the blockchain network, with each storing a full copy of the ledger on their machines. The blockchain network depends on these nodes specifically, as they collectively act as the decentralized backup for the entire network. More notably, miners confirm blocks of transactions being added and processed on the blockchain. All miner nodes in the network use a designated consensus mechanism, discussed in a subsequent section, to cumulatively verify and secure all information on the blockchain. Miners also gain the right to vote for changes taking place in the network, which is of particular interest to these nodes.

B. Blocks

Arguably the most integral component of the blockchain, blocks are the means by which transactions are recorded and stored for the eventual integration into the consensus blockchain [5]. In Bitcoin, transactions are typically, but not always, a recording of an exchange of money between multiple participants. In other applications of the blockchain concept, transactions may be interpreted as being any suitable type of data in which the network has been established to maintain. A large number of transactions are recorded by blockchain applications constantly, then grouped together by the network into blocks. This grouping is chronological, such that a block will contain all transactions that have occurred on the network within a certain recent timeframe. Once a block has been formed by the network, a majority of the network miners must verify and confirm it. It is then reintegrated back into the master blockchain, and all nodes receive an update that informs them of this new authoritative addition to the chain. The time taken to reach a majority, referred to as block confirmation times, varies significantly. Most notably, the Bitcoin blockchain takes an average of nine to ten minutes to confirm a single block. This principle of maintaining verification by a majority prevents any illegal tampering, as the verification process each host performs will easily detect illegitimate transactions.

At a low level, blocks themselves are typically implemented by following a relatively simple design pattern. The original source code implementation for blocks and all other components of blockchain are still available as open source software on the internet. As seen in Figure 2, the typical block is composed of four primary fields:

1) A timestamp of the block creation as an unsigned integer
2) Hash code identifying the preceding block in the blockchain, represented as a 256-bit unsigned integer
3) A nonce, a 32-bit random integer that acts as a sort of checksum
4) A vector of information about transaction records encompassed by this block

At a glance, most information in the block is self explanatory. Similarly to a typical networked packet, blocks contain the above fields as components. The header typically contains all information about the block itself, such as the timestamp, hash code and nonce in Figure 2. Each block has an attached payload, which is the larger portion containing transactional data and a the miner incentive award (not pictured) if applicable in the network. Timestamps and the data itself are dictated by the transactions and the block itself. In a legitimate block, the timestamp must be greater than the median of the timestamps from the previous eleven nodes in the chain. The hash code of the preceding block gives a form of destination address on the master blockchain where the current block will be placed if verified. The nonce is to be given as input to a miner's cryptographic hash function, and will be tested and changed continually until it can use it to confirm the hash. Without diverging from the topic of networking and entering the realm of cryptography, the nonce and certain other possible block inputs must be used in some combination to verify the legitimacy of all transactions in the current block.

C. The Chain

Following the technical breakdown of blocks, a sensible explanation as to where blocks are stored is in order. The blockchain itself is defined as a complex file, in which blocks are stored in a linear fashion, being linked together. The underlying implementation of this treats blocks as independent data structures, with the blockchain itself being equivalent to a linked list of the blocks. To make an analogy to low level C programming, the chain and its blocks are linked together using a form of pointer, so to define an ordered sequence of the blocks in memory. To process and attempt to add a new block to the chain, the hash value of the all previous blocks is provided as seen in Figure 2. A miner will then proceed by generating nonce values that, when hashed with the other inputs, yields a number less than a given target hash. [10]. If found, the miner includes this value in the new block it is forming, before publicly broadcasting the solution for consensus. This process is attempted by all miners, in which one will calculate a correct hash first. The calculation process is largely a guessing game aided by computational power. Miners use the hash of the previous block, hash of all previous data (dubbed the Merkle hash), the nonce, and significant processing power to help generate the first correct block hash value. All other miners continue to guess until the miners establish that some miner has indeed found the correct nonce and hash. It is by this competitive hashing procedure that blocks are added to the chain, and in systems such as Bitcoin, a reward is distributed.

D. *Consensus Mechanisms*

In the context of Bitcoin, consensus machanisms are the most important part in generating bitcoins and verifying blocks. In order to verify consistently across all participants, a common consensus mechanism is decided upon by the blockchain network. The most common mechanism is Proof-of-Work (POW), which is the most secure and popular option, currently used by Bitcoin. In POW, the computationally expensive process of confirming blocks is arranged in a competitive format, in which each miner attempts to solve a complex algorithm, known as hashing. The hashing process facilitates the encryption required to store a transaction securely. Hashing poses a complex mathematical puzzle, which intentionally becomes increasingly difficult. Once a single node wins the race to solve the hashing function (puzzle), the solution is broadcasted to other participating nodes, whom must verify the hashing solution as being correct. Most importantly, the miner who solves the puzzle first and receives consensus from peers initiates a permanent write operation of the transaction into the blockchain. In the case of Bitcoin, a reward in the form of small Bitcoin commission is bestowed to the winning miner in the Bitcoin system.

E. *Operation*

In an operational sense, blockchain is a type of Peer-to-Peer network utilizing the IP protocol and the internet. Much like Peer-to-Peer, the initialization process of the blockchain network involves all nodes performing a peer discovery [6]. Connections between nodes in the blockchain network are then established using a given port over TCP connection.

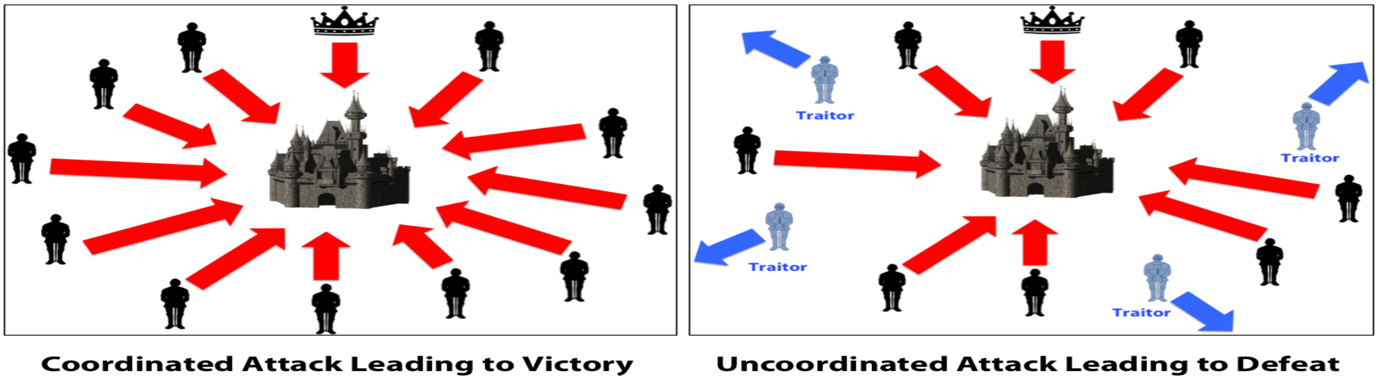
IV. Problems Solved

In a manner similar to the creation of the internet, society is experiencing yet another revolution in computer technology with the rise of Bitcoin and blockchain. With the success of Bitcoin and other cryptocurrencies, proof of concept for blockchain technology has been established, and is being acknowledged for its revolutionary strengths in network decentralization, data security and general durability. Blockchain has proven an effective design to eliminate central banks, thirds parties, bank and transaction fees, and expedite the financial ecosystem operation with Bitcoin. As discussed in another section, blockchain has already been applied to a large number of industries and applications. The open and public status of transactions on the Bitcoin blockchain has logicially defeated any notion of theft, as every transaction becomes a permanent and public record that is stored by hundreds of thousands of participants across the world. In the following subsections, more light will be shed on the most prominent problems solved by blockchain networks.

A. *Network Decentralization*

As discussed, blockchain implementations leverage the advantages of Peer-to-Peer as a foundation to their network stack. The underlying Peer-to-Peer design is integral to the blockchain concept, since the sheer number of users constantly demanding the network resources would make a traditional client-server model expensive. Client-server places all responsibility of maintaining data on the servers exclusively. In constrast, the Peer-to-Peer design allows data to be shared by many hosts instead of a finite number of servers. This idea is referred to as decentralization, which in a networking context refers to the process of moving dependency from a small, finite set of nodes to be shared across other nodes instead. Decentralization solves many problems posed by traditional networks, but does even more justice to the security of the data in network than the efficiency itself. Due to the fact that the blockchain data is stored and synchronized by a large number of participants, a copy of every transaction will always be maintained by a significant number of nodes. If a server were to disconnect or experience difficulties, any number of other nodes would easily step in and offer identical data. Thus, blockchain networks are inherently persistent and authoritative, giving the assurance of complete database reliability for all important record keeping applications.

From a networking security standpoint, decentralization opens the door for any participant to host data and contribute to the consensus. While this creates potential for network penetration, an actual threat is near impossible to be successful. The power of the network lies in the number of participants, whom the majority of are assumed to be non-threatening. With this assumption on the number of legitimate participants, it has been proven that a correct overall judgment of transaction legitimacy will always be reached in the network consensus. This famous computing problem, known as The Byzantine General's Problem, is solved by the blockchain design and warrants a brief explanation to follow.



Coordinated Attack Leading to Victory

Uncoordinated Attack Leading to Defeat

Fig. 3. A visual representation of the Byzantine General's Problem

B. The Byzantine General's Problem

The Byzantine General's Problem poses an abstract situation in which a correct decision must be made given possible misinformed input. In this historic problem, we consider a situation where divisions of the Byzantine army, each commanded by a general, surround an enemy city from various angles [7]. The generals must coordinate a common plan of action by messenger, however a given number of generals may be traitors and will send messages to prevent the loyal generals from reaching an optimal consensus. A solution is proven formally by contradiction [7], in which we discover the following:

$$c(g,m) = \begin{cases} 1 & \text{if } g \geq 3m+1 \\ 0 & \text{otherwise} \end{cases}$$

where g is the number of generals, m is the number of traitors, and $c(g,m)$ determines if generals will reach a valid consensus.

In the context of blockchain, the network may be represented as a large group of generals, in which there may be malicious users (the traitors) who wish to sabotage the hashing or transaction verification consensus. Blockchain provides protection against this Byzantine General Dilemma in the form of its consensus mechanism, typically Proof-of-Work. For a sufficiently large network of blockchain participants or nodes, this consensus mechanism effectively yields Byzantine Fault Tolerance (BFT). While secure, this decentralized consensus method is relatively complex for a simple verification process. Regardless, this approach is cohesive and necessary to the design of the blockchain, and has proven to be comletely secure in Bitcoin. The only known, potential flaw in this consensus situation is the 51% Attack, discussed in a later section.

C. Data Security

With worldwide applications such as Bitcoin, the security and validity of the data being stored in blockchains is paramount to the success and mainstream acceptance of the technology. As such, extreme cryptographic measures are taken to be able to guarantee this. Transactions, such as financial recordings in the world of Bitcoin, simply cannot tolerate being misrepresented, fraudulent or missing in the context of most real world blockchains. In To combat this, Bitcoin and other blockchains are permissionless [8]. In permissionless blockchains such as Bitcoin, any willing user or miner may read and write to the current blockchain. This design is intentional however, as every user maintains and operates their own copy of the blockchain for the time being. A meaningful write may only occur when the hashing solution is confirmed by the other nodes, at which point a consensus verifies the write operation, committing the transaction to the master blockchain and pushing the new standardized blockchain to every node. As a result, a dishonest miner will never be able to forge false transactions of any kind, steal bitcoins from another account or create bitcoins out of thin air [8].

D. Encryption

To replace traditional currency, Bitcoin's blockchain would have to replace and improve upon the process of verifying transactions, historically brokered by a bank since the development of central modern banking several centuries ago. On a technical level, blockchain networks employ cryptographic hash functions throughout its design. To lock down blocks, an extremely complex hash function yeilds a 256-bit alphanumeric hash value that aims to uniquely identify its input in an encrypted format. Using a hash, it is near impossible to determine the original input given the calculated hash. The process is specifically designed to determine a value to represent any binary representable input as a fixed length alphanumeric string, in which the process of transforming it back is near impossible without simply knowing the original input. The hashed value is then used to store the block instead of its original transactional payload data. Given this encryption scheme, blockchains require that any user or miner participating in a blockchain has to remember the hash, not the input, in order to retrieve any information about the block after being permanently written [9].

The encryption scheme behind blockchains completely replaces the notion of a central bank, requiring no regulation by a third party. Unlike the current banking system which has

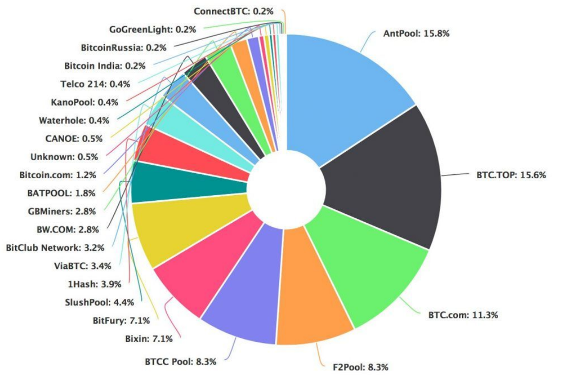


Fig. 4. A visual breakdown of Bitcoin ownership, obtained by the security firm Kaspersky [16]. A shocking amount of the network is controlled by large parties, which could easily overtake 50% if amalgamated.

allowed millions of people to fall victim to theft and financial fraud, the blockchain network and supporting encryption make it near impossible to even attempt illegal behaviour without unreasonably expensive computer equipment.

V. Problems Still Faced

After many successful years of use cases and developments utilizing blockchain networks, there are ultimately a few realities that are part of the design. The quest for a utopian network has been, and will always be, limited by physics. Being the large distributed network that it is, blockchains offer tradeoffs for security and power in numbers. These sacrifices and potential flaws of the design may pose a threat to real systems with millions of users at stake.

A. 51% Attack

Throughout the years since the inception of Bitcoin, investors and security experts have contested the validity and inherent worth of this currency from thin air. With the Peer-to-Peer architecture, every participant in the blockchain network carries equal responsibility in verifying, creating and hosting blocks of data. In theory, the consensus it the sole factor regulating the validity of transactions in the Bitcoin network. This process works well, such that if a few malicious miners enter the network, they are a long way from having enough influence to incur data manipulation. The 51% attack, a plague to several similar types of computer networks, poses a risk to any blockchain. By definition, if a user controls 51% of the nodes in a network, he or she has a majority position, and may thus deterministically influence the behaviour of the network. For example, a Bitcoin miner owns 51% or more of the miner nodes in the Bitcoin network will be able to completely control to consensus process for transactions, and thus write Bitcoin history as it pleases.

Though this may seem unlikely, even Bitcoin, one of the largest blockchain implementations, is surprisingly vulnerable. Considering the fact that Bitcoin is public traded and holds millions of users' financial assets, this threat could be catastrophic if acted upon. In Figure 4 above, a pie chart is given showing the node distribution of the Bitcoin blockchain by user pool. Since participants, in some capacity, eventually pool together in a larger pool, companies and organizations such as BTC.com and AntPool collectively own large amounts of the network. If four of the largest pools listed above merged into one, this seemingly unlikely 51% attack could become a reality [16]. This issue has yet to be solved, but is unfortunately a consequence of the distributed, community-based nature of the blockchain network.

B. Computing Power

Reasonably assumed by most, blockchain networks appear to be the epitome of giant, powerful networking potential. With their networked and pooled resources, it would appear that this is the case. Upon deeper analysis, this notion is false. Although resources may be daisy chained and pooled together, all miners in the blockchain are maintaining the network by racing to calculate the exact same thing [16]. In reality, all miners verify the same transactions by indentical target hashes, eventually recording this same data into a duplicated copy of the blockchain. The entire history of transactions that is the blockchain is stored identically by every miner. These seemingly negative features are the sacrifice that must be made to bring a blockchain to life.

VI. Maintenance

In harmony with the momentous movement for open source information and software, blockchain networks are designed to be a community based effort. The source code behind the network infrastructure is open source, and has long since established itself as being dependable. Fortunately, blockchains avoid involving or requiring the regulation of any third party. The day to day operation of the network is made possible by the worldwide distribution of miner-accountants of the public ledger [2]. Alongside public blockchain implementations such as Bitcoin, private or semidecentralized public ledgers allow for institutions or organizations to maintain network nodes for their own interest. The blockchain concept allows for flexible, easily controlled implementation that can be maintained in any way for which the application deems suitable. In the case of Bitcoin, the users of their blockchain are merely servers set up to continuously check, confirm and record new transactions in hopes of becoming the next successful hash generator [2]. While incentive is still being offered, participants will continue to thrive in the Bitcoin ecosystem and offer their hardware to the distributed network.

VII. Current State of Affairs

In recent years since the explosion of Bitcoin and cryptocurrencies, competition and value in these blockchain networks has reached unimaginable levels. Large companies have been formed, creating farms of server all linked together to take a stab at winning bitcoins. Before reaching global popularity, entire bitcoins could be mined by a few consumer grade computers [11]. Due to this overshadowing by enormous miners, pools have been formed in which many people wishing to contribute to the blockchain may dedicate their computers to a larger pool. Companies have created an ecosystem where a tiny amount of bitcoins are rewarded to pooled users. However, other applications of the blockchain are non-competitive, and are not looking to drive up the value of a virtual currency. While the success of cryptocurrencies themselves will vary over time, the blockchain technology is being refined for more important applications. As stated by the Harvard Business Review [12], there is a clear parallel between blockchain and TCP/IP, both revolutionary networking concepts that were first realized for very different applications. Like blockchain, which was designed for the release of Bitcoin, TCP/IP was created as a basis for e-mail among researchers on ARPAnet, the U.S. Department of Defense's first attempt at creating internet. In a similar way, blockchain as a concept is currently in its infancy. Society has barely scratched the surface in repurposing its potential. The move from proof-of-concept applications has yet to happen on a large scale. As a starting point, the Blockchain organization has opened up APIs to allow implementations and experimentation in new ways.

VIII. Future of Blockchain

Due to the large number of theoretical possibilities for blockchain applications, blockchain evolution is commonly broken down into three distinct versions [2]:

- Blockchain 1.0 - Cryptocurrency
- Blockchain 2.0 - Financial and other applications
- Blockchain 3.0 - Applications beyond finance

As the future of blockchain is arguably more important than its current business, we will briefly consider each of these hyptothetical iterations with specific use cases we may be able to find for the technology itself.

A. Blockchain 1.0

Considering how revolutionary it has already become, cryptocurrency is the modern day version of the blockchain technology. The invention of the Bitcoin protocol has helped to demonstrate the scalability of blockchains on the world stage. This version is, and will be the most important. Version 1.0 must establish a large, demonstrated network to act as a proof-of-concept for other potential investors and developers. In this version, blockchain has facilitated the creation of many currencies such as Bitcoin, Ethereum, and Realcoin. More importantly, blockchain has made possible a new era of banking. The entire financial sector is inevitably being changed, with intermediaries being eliminated and miners developing an ecosystem. This version has become a tested networking practice that will contribute in growing the number of connected devices worldwide to the projected number of 20.4 billion by 2020 [13].

B. Blockchain 2.0

Looking forward, Blockchain 2.0 is the up and coming tier of blockchain applications. Already, this tier includes developing protocols and applications being referred to as Blockchain 2.0, Bitcoin 2.0, Dapps (decentralized applications) and DAOs (decentralized autonomous organizations) among others [2]. Using blockchain as the backing network, this next generation of blockchain application hopes to decentralize entire markets and exchanged assets by means of its network. As we have noted, blockchain is considered to be sitting on top of the application layer o the traditional network stack. With the introduction of Blockchain 2.0, protocols will be invented to in turn sit above Blockchain 1.0 technology on the stack. In a similar way to how application layer protocols like HTTP and FTP were built on top of TCP/IP, Blockchain 2.0 is on track to introduce protocols that will build upon its successor. This will encompass new software that will sit on the shoulders of blockchain's current design, extending it to new domains through new and private blockchain networks. To highlight, an up and coming Blockchain 2.0 technology, coined Smart Property, is being designed to provide a definitive distributed asset registry for all assets (including hard such as automobiles, or intangible such as votes and health data) [2]. This specific iteration in blockchain's lifespan will move its concept into new domains, in the same way that internet technology led to the creation of social networks.

In an attempt to group some of these new applications, the blockchain community is generally referring to a new way of interpreting and using the blockchain as Smart Contracts. This concept formalizes the idea of using the blockchain to go beyond conventional transactional representation, instead recording data to help formalize agreement between parties. The notion of trust between two people will be fulfilled by some blockchain network, which will enforce cooperation in a contractual manner by means of autonomy. Smart contracts will be designed to enforce any agreement or set of rules in an automatic fashion.

C. Blockchain 3.0

Considering the design principles of blockchain networks, one may agree that the concept of decentralization can be very powerful when used effectively. In the category of Blockchain 3.0, applications are expected to be created to organize data outside of the world of finance and asset recording. Although products grouped under this version are still being researched and developed, many ideas have been formed including applying blockchain to DNS registrars, digital media, identity verification and censored information [14]. In Blockchain 3.0, a distributed ledger can prove ownership of music and video files, and make an attempt to eliminate illegal pirating altogether. With authoritative and decentralized record keeping, censored information such as political leaks and documents would be impossible to erase once entered into a blockchain. In summary, Blockchain 3.0 applications may advance a new, computerized society in which almost anything can be recorded and proven, for better or worse.

IX. Conclusion

In summary, the blockchain networking model has already proven its worth with the growth of the Bitcoin protocol. Blockchain's distributed, decentralized Peer-to-Peer network provides a revolutionary foundation for which all formats of data may eventually be maintained in a secure, unbreakable network. The blockchain network is able to leverage its peers to support a massive network, one in which no government or third party will likely be able to influence or compromise. With more support and education on this topic, the future with blockchain will redefine how we persist data in all industries and areas of society. Without a doubt, blockchain will continue to grow and develop to see more important applications, following in the footsteps of its historic predecessors.

References

[1] S. Nakamoto. (2008, Nov.) “Bitcoin: A Peer-to-Peer Electronic Cash System”. [Online.] Available: https://bitcoin.org/bitcoin.pdf

[2] M. Swan. *Blockchain Blueprint for a New Economy.* (1st edition). Sebastopol, CA: O’Reilly, 2015.

[3] Bitmalta. “How Does the Blockchain Work?”. [Online.] Available: https://bitmalta.com/blockchain-explanation/

[4] M. P. Singh and S. Tu. (2009, Mar.) “Free Riding in Peer-to-Peer Networks”. [Online.] Available: http://www.cs.bilkent.edu.tr/ korpe/nsrg/pubs/ic.pdf

[5] G. Caffyn. (2015, Aug.) “What is the Bitcoin Block Size Debate and Why Does it Matter?” [Online.] Available: https://www.coindesk.com/what-is-the-bitcoin-block-size-debate-and-why-does-it-matter/

[6] V. Chemitiganti’s. (2016, Jan.) “The Architecture of Blockchain.. (4/5)” [Online.] Available: http://www.vamsitalkstech.com/?p=1615

[7] L. Lamport, R. Shostak and M. Pease. (1982, July) “The Byzantine Generals Problem” *ACM Transactions on Programming Languages and Systems*. Vol. 4, No. 3. Available: https://www.microsoft.com/en-us/research/publication/byzantine-generals-problem/?from=http

[8] A. Lewis. (2015, Sep.) “A Gentle Introduction to Blockchain Technology” [Online.] Available: https://bitsonblocks.net/2015/09/09/a-gentle-introduction-to-blockchain-technology/

[9] Nomura Rsearch Institute. (2016, Mar.) “Survey on Blockchain Technologies and Related Services” [Online.] Available: http://www.meti.go.jp/english/press/2016/pdf/053101f.pdf

[10] G. O. Karame, E. Androulake and S. Capkun. (2012) “Double-Spending Fast Payments in Bitcoin” [Online.] Available: https://www.eecis.udel.edu/ ruizhang/CISC859/S17/Paper/p9.pdf

[11] D. Gewirthz. (2014, Jan.) “Want to make money mining bitcoins? Criminals have you beat” [Online.] Available: http://www.zdnet.com/article/want-to-make-money-mining-bitcoins-criminals-have-you-beat/

[12] M. Iansiti and K. R. Lakhani. (2017, Jan.) “The Truth About Blockchain” *Harvard Business Review*, January-February 2017 Issue

[13] S. Accornero. (2017, Sep.) “Blockchain 1.0 (past)” [Online.] Available: https://community.innoenergy.com/groups/blockchain/blog/2017/09/23/blockchain-10-past

[14] E. Mesropyan. (2016, Dec.) “21 Areas of Blockchain Application Beyond Financial Services” [Online.] Available: https://medium.com/@LetsTalkPayments/21-areas-of-blockchain-application-beyond-financial-services-9a007f3db2f1

[15] A. M. Antonopoulos. *Matering Bitcoin - Programming th Open Blockchain*. (2nd edition). Sebastopol, CA: O’Reilly, 2017.

[16] A. Malanov. (2017, Aug.) “Six myths about blockchain and Bitcoin: Debunking the effectiveness of the technology”. [Online.] Available: https://www.kaspersky.com/blog/bitcoin-blockchain-issues/18019/