Blockchain Technology and Consensus Algorithms

Matthew Rinker
Denison University
Granville, OH, USA

July 15, 2020

Abstract

Bitcoin is a purely peer to peer online cash system. It is the world's first online decentralized currency. Bitcoin operates on a system called the blockchain. The blockchain is a system created by interconnected peer nodes which operates as a transaction log and verifies that each transaction is valid. The blockchain protects itself via cryptographic methods and incentives for miners ensures that the processing power of the network is large enough that makes malicious attacks impossible.

1 Introduction

As we move further and further into the digital age the libertarian movement continues to grow and find outlets through the use of technology. A point of contention is the decentralization of currency. In 2008 a paper appeared alongside a proposed online currency called Bitcoin [7]. Bitcoin has been embraced by libertarian minded individuals but has been criticized since its private nature has also led to its adoption by criminals. Should we place our faith and our financial well-being in the hands of something that has no governing body and is overseen through cryptographic algorithms? To make an informed decision we must understand the underlying architecture of currency, and its contemporaries, and take notes of the risks and applications of this technology.

Bitcoin is built on the principles that, through cryptography and network verification, transactions can be conducted anonymously and securely. Bitcoin's main claim to fame is that transactions are completed faster than traditional bank transfers as well as being completed almost completely anonymously. To do this, Bitcoin opted to cut out the trusted third party which slows down online currency exchange. The cryptographic peer-to-peer network acts as the verifying party and due to its automated nature transactions clear significantly faster than when working with a bank's clearing house. The strength of Bitcoin comes from the agreement of the Bitcoin network, the only way to exploit the Bitcoin Network would be to control more computing power than the collective power of all legitimate Bitcoin nodes. To incentivize users to contribute power to the network there is a reward for being the quickest to solve the algorithm associated with each group of transactions.

Bitcoin itself pioneered blockchain technology, however, the original paper was not perfect. Since the introduction of Bitcoin and the mining of the first block by Satoshi Nakamoto the source code of Bitcoin has been updated by the community. Bitcoin's source code is open and available on github for anyone who wishes to develop for Bitcoin to fork and try to implement their ideas. There are currently 613 people who have been permitted to commit to the master branch of the Bitcoin repository. The changes these individuals created were voted upon by the community before they were permitted access to commit the changes to the master branch. Some of these changes were drastic to the nature of Bitcoin, for example the introduction of Lightning network technology to the blockchain. In the event that the userbase is split on whether to update the source code or not the Bitcoin code can be forked and essentially a new coin created. This was the case in August 2017 when Bitcoin was forked to create a duplicate coin which worked slightly differently called Bitcoin Cash. Since then the two coins have diverged and are distinctly different.

Since the introduction of Bitcoin professionals in various industries have been looking into blockchain technology and how they could possibly adapt it for their uses. Banks are currently developing a coin called Ripple with the trading tag XRP. Anyone can buy it, howeve, only the banks have the ability to mine it making it semi-centralized and protected. The idea behind this coin is that by banks trading this coin with each other they can transfer money between banks without the hassle of actually transferring the currency. Therefore, this would speed up the time an actual bank transfer would take to process and complete. In other industries, researchers are looking to repurpose blockchain technology entirely. They are seeking to make some entirely new technology out of the essence of blockchain, for example the group BigChainDB are theorycrafting a database system powered by blockchain technology [6].

The actual underlying algorithm for the blockchain is a type of algorithm called a consensus algorithm. These types of algorithms are essentially algorithms for deciding an outcome amongst a group such that it benefits all members of the group. Typically these types of algorithms are collaborative and hinge upon all members of the group working together towards a common goal. These kind of algorithms can be framed by the following problem:

Suppose there are a group of Byzantine generals organizing a mission. They can only communicate via messenger. Generals create reports that are sent to the other generals via messenger. The goal of the system of messengers and generals is to create a plan to succeed in their mission, in this framing problem it is often said to be a plan of attack to conquer a city (However, this framework does not quite matter for the spirit of the problem). There are m traitors amongst the group of n generals and messengers. Traitors could either be a messenger or a general. Therefore, a traitorous general could provide a false report representing false information or a traitorous messenger could change a valid report to represent false information. The solution to the Byzantine generals problem is some way of forming a plan that will work regardless if some information is falsely generated. This is called a consensus problem is that this problem would come from the majority of the generals agreeing to the plan based on the information they have and some small number of traitors providing false information would have no impact on the overall plan. [3]

2 Notation

To properly discuss bitcoin we must define the terms of the specific parts of the Bitcoin system as well as some related terminology.

Definition 1 ***Transaction*** *A transaction is defined as any one instance of Bitcoin changing hands between two Bitcoin Wallets.*

Transactions are the basis of the bitcoin system. At its most basic it is a currency and since it is digital there must be some way of recording when bitcoin changes hands.

Definition 2 ***Block*** *A block is a data structure containing many transactions that will be verified as a group by the Bitcoin Network.*

Blocks are the units of storage for Bitcoin. Each block contains all transactions that occured after the block before it.

Definition 3 ***Blockchain*** *The Blockchain is the network verified chain of blocks that serves as a log of all transactions of the network and the way to verify that a transaction is valid.*

Just like it sounds, the blockchain is the chain of all blocks.

Definition 4 ***Miner*** *A miner is any computer connected to the Bitcoin network providing its computing power to solve algorithms and therefore verify transactions and creating blocks.*

The blockchain is managed by miners. Miners lend their computing power to solve an algorithm and therefore generate blocks and verify that transactions have indeed happened.

Definition 5 ***Consensus Algorithm*** *A consensus algorithm is an way a group can make a decision such that the decision is the best for each individual. This type of algorithm ensures that the individual members of the group must support the majority's resolution to best benefit themselves.*

The specific type of algorithm the miners work together to solve is called a consensus algorithm.

Definition 6 ***Crypytographic Nonce*** *A cryptographic nonce is a single use integer for Cyptography. This is a throwaway number usually generated through random or pseudorandom number generation and is generally used so that old communications cannot be reused.*

The specific problem of the algorithm that the miners are working to solve makes use of a nonce. We will discuss the algorithm and the role of the nonce within the algorithm later in this paper.

3 Structure

The structure of Bitcoin is a sort of tiered structure. At the most basic is a Bitcoin. It has private and public keys associated with it so that everyone can see what the records of where the Bitcoin has been. Each Bitcoin lives in a wallet, which is essentially a paper, hardware, or software method of storing the private and public keys of the Bitcoin in the wallet. Bitcoins are exchanged in transactions, each transaction is stored by recording the amount, public keys of Bitcoins, and wallet addresses involved. These transactions make up blocks.

Each block contains a header, the hash for the previous block, and any transactions that are being confirmed by the blockchain during the time when the block was created. These blocks make up the blockchain. The blockchain is no named because the blocks are technically chained together. The header of the second block in the blockchain contains the hash answer for the first block and so on. This ensures that all blocks are tethered together and there is a definite sequence. In this way, the blockchain is not a literal chain as there are no pointers connecting the two blocks. However, given a block it is always possible to know which block . The miners themselves are the ones who create these blocks in that while the blockchain itself handles the creation of new blocks it is not possible without the facilitation of the miners through a consensus algorithm. [7] [3]

In Fig 1. we see a common graphical representation of the blockchain as a Merkle Tree. In this representation we see the genesis block, a common term for the first block mined, in green. The blocks in black are the actual blocks of the blockchain as they are part of the longest chain of blocks and thus accepted by the network as the actual chain of events that has transpired. The purple blocks are some blocks generated that were not accepted by the mining network and thus are not used by the network. These blocks could have been malicious attempts to hijack the network or simply the product of two answered being accepted simultaniously and thus the miners of the network worked off of whichever answer they received first and whichever group finished the next block first would continue the chain and the other miners would abandon their work and follow the consensus.

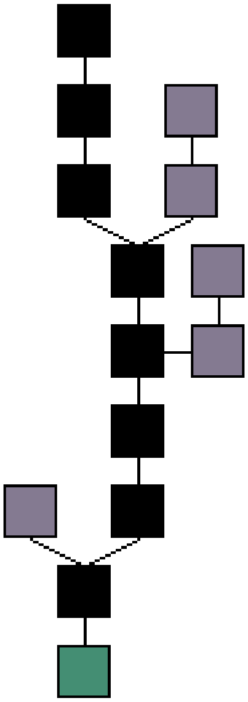

Figure 1: A Graphical Representation of the Blockchain as a Merkle Tree [1]

4 Byzantine Generals Revisited

Now that we have some idea of the terminology and structure involved in the discussion of Bitcoin we can revisit our overarching problem, the Byzantine Generals Problem, and look at it in terms of a network. Think of the miners in the network as Generals, and the transmissions they send between each other and the network to be messages carried by Messengers. In a network "Traitors" would be malicious individuals attempting to falsify information on the network to change what is known to be true. In the case of Bitcoin this would likely be trying to falsify a correct answer to a mined block as this would give the malicious individual all rewards entitled to the miner who solved a block. Thus, our network of miners attempt to reach a consensus on who has correctly mined each block by transmitting answers to each other and checking them against the information they have available (the problem given to them by the blockchain).

5 Blockchain

The specific consensus algorithm used by Bitcoin blockchain technology is the Proof of Work algorithm. The blockchain hinges upon the miners of the system confirming all transactions to ensure that everything is working correctly and there is no cheating going on in the system. In terms of the problem stated in the introduction, the generals and messengers are the miners. The mission they are working together to plan and execute is the verification of a certain block in the blockchain.

A proof of work algorithm functions as follows. There is some mathematical problem that needs to be solved given by the governing body. In this case the governing body is the blockchain. The blockchain attempt to create a block but it needs a problem to be completed by miners first. This solution to the problem is known as a hash. Each mining client works to solve this mathematical problem, in the case of Bitcoin this is a SHA-256 hash. The work each client does is taking a nonce appended to the data in the block, incrementing it and hashing the entire block using SHA-256 protocol. The goal is to find a nonce such that the entire block hashes to a value with a number of leading zero bits (the target number). This hash is then sent into the network for verification. If it is accepted by both the blockchain and other miners as a valid answer the client is rewarded with coins by the blockchain and a new block is generated. The pseudocode for this protocol is given in algorithms 1 and 2: [3]

First, the mining client receives the hashing string from the blockchain. This contains the answer to the previous block (to ensure linkage) as well as all transactions which have occured and need to be verified for this new block. Finally, there will be a transaction at the end for a new set of Bitcoins. This reward was originally 50 Bitcoins plus the transaction fees for all transactions in the block. This 50 coin reward halves every 210,000 blocks and as of the 13th of May 2019 was 12.50 Bitcoin. The client then takes the data received from the blockchain and appends a nonce to the end of the data. This is some string of bits to change the value of

Algorithm 1 The Miner Side of the Proof of Work Protocol

```
Receive hashing string from Blockchain
Receive hash function from Blockchain
while not solved do
    generate a nonce
    append nonce to hashing string
    Hash string with SHA-256 Protocol
    Submit hash to blockchain
    if hash is accepted then
        receive reward
        break
    else if Blockchain accepts other miner's hash then
        break
    end if
end while
```

Algorithm 2 The Blockchain Side of the Proof of Work Protocol

```
Generate hashing string
Generate hash function
Generate target number (between 0 and 256 bits) if 2016 blocks have been solved
Send hashing strings and function to miners
while unsolved do
    Receive hash from miner
    if hash size is below target then
        Send to miners for verification
        if accepted then
            Reward miner
            Create block
            break
        else
            reject hash
        end if
    end if
end while
```

the string received after hashing. The client then hashes this completed string with SHA-256 protocol and creates a hash. This nonce is then sent to the blockchain and then to be verified. If it is verified to be correct then the block is mined and created. The act of verification itself is simple since the nonce is transmitted to all clients. The nonce is attached to the data the client has and personally holds to be true (like each general with their own information) and hashed through the SHA-256 protocol. If it is found to be a valid by enough miners then the blockchain will mark it as valid and create the block.

Since each block contains the answer of the block before it it ensures that for some malicious entity to try to change the contents of the blockchain it must first solve every block following their targeted block. This makes the computation exceedingly expensive in terms of CPU cycles and effectively impossible to do effectively.

With each successive block the reward for successfully mining a block is reduced. In theory, the reward reduction will be negligible as this is supplemented by the transaction fees of all transactions in the mined block. However, this reduction in rewards helps deter attackers from conducting a 51% attack. [5] [7]

6 The 51% Attack

A 51% attack is defined as some attack where the attacker controls 51% or more of the mining power and leverages this to either stop other users from mining blocks and stopping blocks from being mined and also taking the majority of rewards.

The reasoning why a malicious individual would have to control 51% of the mining power, and hence the reasoning behind the name, is quite simple. If we once again think of mining as a consensus problem we can see the issue. In terms of the Byzantine generals should over half the group be working for the enemy then no consensus could ever be reached that would reach a favorable outcome. For, every plan that was proposed that would lead in a Byzantine victory would be voted down and discredited by the traitors via their false information. Thus, should a malicious entity possess the majority of the mining power (51% is a simple majority) it would be disastrous for a system relying on a consensus algorithm.

The nature of blockchain operations deters a 51% attack. By default, the reduction of rewards and the sheer computation power needed would make the attack non-profitable. Additionally, since the rewards are given in Bitcoin the attack would require the value of Bitcoin to increase or stay stable to be profitable. By hijacking the network an attack would guarantee that the value be diminished. Finally, due to the nature of a proof of work algorithm it would be entirely impossible to guarantee that an attacker would get all rewards without having 100% of the processing power. This is because mining is generally at its most basic a pseudorandom method which allows for even those with less processing power to have a chance at earning a reward. This also contributes to the growth of the total computational power of the network since it gives incentive for new miners to join the network. [4] [7]

7 Time Complexity

The Time complexity of this algorithm is not inherently clear. As can be seen in the pseudocode above, there is no bound for the loop. This means that there is no real way to bound the

Proof of Work (PoW)

The amount of work done by a particular miner determines his/her possibility of mining a single block and the reward of getting a coin.

The miners get lesser Bitcoins over time. Such smaller incentives ensure less chance of the 51% attack.

The community-bond of the miners of PoW is extremely strong. Thus the possibility of the community to become more centralized increases with time.

101 Blockchains
Created by 101blockchains.com

Figure 2: A Graphic Giving a Top Level Description of the Proof of Work Algorithm [3]

algorithm's time complexity in terms of n. The computation is

This comes from the fact that the algorithm ends when the hash is solved. This could happen at the first attempt by the very first miner or it could happen after billions of attempts from all the miners in the network.

What we do know is that the average completion time for each block is 10 minutes. This has been kept steady throughout the history of Bitcoin, as was intended by the creator Satoshi Nakamoto [7]. The reason behind this is the difficulty of solving a block and the target number. The blockchain changes the target number to modify the difficulty of solving a block. The chosen difficulty hinges upon various factors but the most influential of these factors is the amount of computational power in the network. Part of the Bitcoin system is that it wants to keep itself at a difficulty where the collective power of the network will take around 10 minutes to solve a block. Therefore, the difficulty and target number change to reflect this. The target number is changed every 2016 blocks to update the difficulty of mining a new block. The formula for the target number is as follows:

$t' = t/d'$ where t is the old target number, t' is the new target number, and d' is the new difficulty. The d' is calculated as $d' = d * (2016 * 10)/(a * 2016)$ where d is the old difficulty and a is the average time to complete the last 2016 blocks in minutes.

Thus the entire formula for t' is $t' = t/(d*(2016*10)/(a*2016))$. Interestingly, it took 32,255 blocks for the difficulty to increase at all. At the 32,256th block the difficulty was increased to 1.18. That is to say, it took 244 days after the launch of Bitcoin for the computational power of the network to become large enough to require raising the difficulty to ensure blocks would continue to be mined at the rate of 1 every 10 minutes. The current difficulty of the blockchain on the 13th of May 2019 was 6,379,265,451,411. To put these numbers in perspective, this means that due to the sheer computational power of the network to keep blocks being mined at the rate of roughly 1 per 10 minutes the difficulty of the computation to be solved per block is now 6,379,265,451,411 times more difficult than the first block to ever be mined. In fact, it is that many times more difficult than the first 32,255 blocks to be mined. [2]

8 Conclusion

Bitcoin is a modern currency system that is popular because of its decentralization. The blockchain works as an autonomous governing body that secures the network through a proof of work algorithm. This ensures that the network cannot be hijacked except by an extremely lucky 51% attack. However, the inherent structure of the network stops such an attack from being viable. Ultimately, the importance of the proof of work algorithm is maintaining the integrity of the system. While still technically vulnerable, it maintains itself in such a way that attacking it is near impossible. This autonomy where the governance of the currency is left to mere code and cryptography is attractive to those disenfranchised with the governments and corruption that comes with them, and as such Bitcoin promises to be

References

[1] Block chain. *Bitcoin Wiki*.

[2] Difficulty in mining. *Bitcoin Wiki*.

[3] H. Anwar. Consensus algorithms: The root of the blockchain technology. 2018.

[4] I. Eyal and E. G¨un Sirer. Majority is not enough: Bitcoin mining is vulnerable. 2014.

[5] Y. Lewenberg, Y. Sompolinsky, and A. Zohar. Inclusive block chain protocols. 2015.

[6] T. McConaghy, R. Marques, A. Müller, D. De Jonghe, T. McConaghy, G. McMullen, R. Henderson, S. Bellemare, and A. Granzotto. Bigchaindb 2.0: The blockchain database. 2017.

[7] N. Satoshi. Bitcoin: A peer-to-peer electronic cash system. 2008.

Figure 3: Sardor and Matt Demonstrating All They Learned From CS 371