How Secure is Bitcoin ?

by Garret Tonra

Abstract—
In This Paper we shall discuss the security of Bitcoin Technology and the mechanisms that are already in place that help to work for and against the system. We shall discuss how users have tried to make the system work to their advantage and what protocols are in place to help keep these types of attacks from happening. As well as that we shall look at miners and the mining pool process and how these people along with the blockchain are quintessentially important to Bitcoins Security and its solidity as a cryptocurrency. Finally we will discuss , a few security breaches noted in the research of this literature review

I. Introduction

.

The Emerging Technology that will be focused on for this Literature Review is bitcoin security. So what exactly is bitcoin?

Bitcoin is basically the first ever created decentralized digital Currency. Bitcoin was first created in October 2008 by a unknown entity or entities taking the name of Satoshi Nakamoto. that person or persons are still anonymous to this present day. When creating bitcoin Satoshi had also implemented the first ever blockchain database as well as a Paper describing the system [1]. Bitcoin is known as a peer-2-peer system or P2P It is a transaction system that takes out the middleman in most cases the banks. This results in a very low transaction costs for a user. Bitcoin can be used to pay for virtually anything you want, It is a neutral currency. Bitcoin Transactions are managed by miners these are people who verify P2P transactions and are rewarded by newly generated Bitcoins. Once the transactions are verified by the miners they are then recorded and saved in the Public Ledger this is described in detail by Satoshi Nakamoto in there Paper [1]. Since bitcoins emergence in 2009 it has steadily grown and is used more and more frequently as a means of paying for goods and services but is bitcoin a secure form of Currency or is it too early to know in the next sections we shall be looking at this cryptocurrency and how secure is its design?

II. blockchain security

.

Blockchain technology is the essential component to bitcoins goal of the P2P system,Since the blockchain is a decentralized system meaning it does not need a trusted 3rd party to make transactions

Blockchain stores the transaction information of every single transaction ever made across a network of personal computers,Which means that no central company or person owns the blockchain system but everybody can still access it and help to maintain and run it. The Blockchain is the fundamental piece of the puzzle that makes a P2P system very hard to compromise,as it has no central point to attack,compared to a Trusted party system where there usually is a main point of centralization that attackers can focus on. A blockchains security is stronger compared to a centralized point system is the way it is structured together each block that is a verified transaction is added to the chain. Inside that block it has the cryptographic hash value of the previous block. This previous hash value then acts as a unique ID for the previous block. From this system the blockchain implements a log system of all transactions that have ever taken place. Starting back from the first block created the ”Genesis Block”. Thus this system can verify every transaction ever completed and calculate the value of every piece of a bitcoin address. As well as that every node that was or will be offline will be easily able to reach the most up to date block by reading a few recent blocks that were missing. The blockchain is always increasing. Adding from the previous block and in turn referencing that blocks unique cryptographic hash value each time a new one is added. There are always vasts amounts of new blocks inside the network so to ensure a consistent chain,blocks are only allowed to have transactions that are matching the current balance of the previous block of the chain. If the Nodes hold the same copy of the blockchain then we can actually account for every piece of the bitcoin as well as the ownership of each piece only if all the nodes have the same copy of the blockchain. Since this is not a centralized system it is not fool proof. If two blocks are created at roughly the same time and they are created by different nodes. Then the different nodes might branch from the same parent but have two different chains which will show different versions of the transactions log. If this happens then how does the blockchain figure out which is the right log ?. Here is where the blockchains Protocol is Essential to the system. The blockchain has two mechanisms which essentially prevent this sort of chain forking simply by these two systems 1.”Proof of Work”[2] and the second mechanism is 2.”Adopt the Longest Chain”[3]

A. *proof of work*

a proof of work for bitcoin is the computation which bitcoin Miners must complete to verify a transaction to the public ledger. there reason for doing this is for personal reward. To complete this computation the miners must produce a challenge string that matches the cryptographic string from the previous block,when concatenated together in a hash function. The reason this is so hard to produce is the that the challenge string may need to produce for example a string with 40 or more leading zero’s bits at the start of it. for the computer to produce a string with a that amount of leading zeros the computer may have to reproduce over 1 billion challenge strings before the string matches the previous cryptographic

block. Depending on how lucky or unlucky the miner is this could be a value lower than 1 billion or a value higher it depends on the complexity of the previous cryptographic block.Once a miner has then got an answer to match the previous block that miner will send there answer forward for verification to the rest of the nodes. The other nodes will simply put the answer provided and the previous cryptographic block into a hash function and if the two strings match then the transaction is verified by the all nodes and the block is added to the chain and the transaction published on the public ledger. This protocol makes the creation of blocks hard as it requires a cryptographic hash of each blocks header which will be a low number under some threshold it is explained in great detail in "Bitcoin: under the Hood" article [2]

B. Adopt the longest chain.

The adopt the longest chain protocol ties in with the proof of work in that the system will be secure as long as the honest nodes are more that 51% of the total nodes contributing to the longest chain.[1] If nodes that have a block that they believe is the longest block and then learn about another block that is longer than the block they are currently working with. These nodes will abandon there existing block that is shorter and work with the conflicting longer block. Once the nodes know the block is the longest then it is the most accurate and correct blockchain and can be easily verified. The two systems ("Proof of Work" and "Adopt the Longest Chain") work together to maintain the blockchains security and the history of transactions on the public ledger [2]

III. DOUBLE SPENDING

.

since bitcoin is a digital file its is easier to duplicate than actual money since this is the case some people in the bitcoin world will try to double spend there bitcoin by paying for two different items or products with the same coin this is called Double spending.how it is done on a basic level for example (if **person A** sends **Person B** a bitcoin for a product then that transaction called **transaction A** will fall into the unconfirmed transactions pool and at the same time **Person A** sends a bitcoin to **Person C** that transaction called **transaction B** will also fall into the unconfirmed transactions pool once the transactions are taken out of the unconfirmed pool and put into the blockchain they are then validated. So for instance if **transaction A** is pulled out of the pool and validated it will be added to the blockchain and then **transaction B** is pulled out of the pool for validation **transaction b** will fail as the bitcoin is already spent for **transaction A**. If the two transactions are pulled out at the same time then the transactions will both adopt a different branch of the blockchain when this happens then there will be a race from each branch to get the next verified block of confirmations. the branch that receives this next block first will obtain the verified spend but if the two branches in this case were both to receive another verified block of confirmations at the same time then the race as such would continue until one branch outruns the other to claim the spend.Although double spending is hard to accomplish as it is said that the attacker or attackers are to need at least 50% of the overall computational power of the system to for it to work in there favour as well as the vasts amount computers they would need to make a block that would outpace the longest blockchain so far as mentioned by Satoshi[1] as well in [2][6]. in the survey about security and privacy issues in bitcoin[6] the authors highlighted a couple of ways to double spend and trick the miners to approve the dishonest transaction a few ways done have been like the **Finney Attack** where a non conforming miner will try to add a pre-mined block as a way of double spending. once the non-conforming miner receives the product off of the vendor. The miners priority target in this case is the seller of the products. To prevent this type of attack the seller should wait for multiple confirmation messages to be confirmed first. another attack talked about by the authors[6] is the **Double Spending or Race attack**. This would be the more common attack used where a user double spends a coin. The user spends a coin then with little time between the first transaction he spends the coin again. This causes two blockchains to compete to verify the transaction. so the user gets his product for one item free while the vendor is left with no payment for the goods sent. a way to combat double spending attacks like this is to have an observer of the over the network to detect this kind of activity and stop it. Nearby Peers should be able to warn the merchant of this type attack if picked up on by the peer nodes[6].

IV. MINING POOLS

.

bitcoins miners are one of the cornerstones of bitcoins security and strengths. a As a miner you are tasked with producing a simple easily verifiable answer to a complex mathematical problem, by way of an algorithm to solve these problems the fastest node to produce this answer will win the race and be rewarded for there answer as long as it is verified by the rest of the nodes as the right solution. the reward for the miner is a piece of bitcoin that is created in the mining process. the problem with mining is that bitcoin mining is it uses alot of a computer or multiple computers CPU power to solve the algorithm this causes the miners to need a vast amount of CPU power to solve the problem fast as well as having very high electricity consumption [8]. so they can be the first one to solve it and gain a bulk of the reward for the solution.but with so many miners in the system now as well as the problems to be solved become more complex,For a single miner the solution to a problem may take months that's months without any reward or incentive to stay mining this is where mining pools come into the frame where a group of miners come together to pool there mining resources to solve the problems alot quicker and the miners will share the profits fairly depending on the amount of work each miner has done to solve the problem this has been alot of discussion about mining pools in the articles and surveys [2][6] some see it as a problem to have only a few mining pools that are contributing mainly to the blockchain as if these pools gain 50% [7] or 51% [9] of the total network then they could use the system to their advantage or if attackers focused on the

pool of miners they could potentially hack the system and use it to their advantage causing a massive security issue for the bitcoin system. there have been some notable types of mining pool attacks on recent one was the ”Bribery attack”[6] where a attack will try obtain the majority of the system for a very short period of time. they are three types of ways to implement this type of attack ”negative-fee attacks mining attacks”,”Out-of-Band Payment” and ”In-Band payment via-Forking” what these attacks try to do is to bribe miners by providing higher incentives for by taking bribes for a higher short term gain this way the attackers will obtain the majority rule of the system for short periods to launch Distributed Denial of service attacks and double spending attacks.

V. SECURITY BREACHES AND ISSUES

.

In Satoshi’s paper[1]they spoke that the system could be used dishonestly by attackers only if they could obtain 50-51% of the system which would be difficult to obtain but not impossible in two articles found - Majority is not Enough [4] and Optimal Selfish Mining Strategies in Bitcoin[5]the authors in these articles state that you in fact do not need 50-51% of the system for the attackers to make it work to there benefit they say that as little as 25% would suffice and that the way the user would make it work to there advantage was that they would basically use a selfish mining attack. A selfish mining attack is when the attackers are able to obtain a larger revenue than its mining power ratio size. What the attackers do then is keep the block mined to themselves and branch off the blockchain. They convince the honest miners to change onto the dishonest branch they are using by selectively introducing the privately held blocks they had previously in turn causing all the work the honest miners previously done wasted. As the selfish miners have the honest nodes switched over to the dishonest block since there block is the longer of the two branches. Since the selfish miners are always technically a block ahead they will then be able to compute the next value of the blockchain before the honest miners as long as they have enough CPU power held to match the mathematical problem before the honest miners. In this case the selfish miners are gaining all the rewards for verifying the transactions if this was to happen for a sustained period of time the honest miners will eventually give up mining as there is never a chance to gain reward as the system is not honest and fair.
below is a selfish mine algorithm explanation

.

Algorithm 1: Selfish-Mine

```
1  on Init
2      public chain ← publicly known blocks
3      private chain ← publicly known blocks
4      privateBranchLen ← 0
5      Mine at the head of the private chain.

6  on My pool found a block
7      Δ_prev ← length(private chain) − length(public chain)
8      append new block to private chain
9      privateBranchLen ← privateBranchLen + 1
10     if Δ_prev = 0 and privateBranchLen = 2 then        (Was tie with branch of 1)
11         publish all of the private chain               (Pool wins due to the lead of 1)
12         privateBranchLen ← 0
13     Mine at the new head of the private chain.

14 on Others found a block
15     Δ_prev ← length(private chain) − length(public chain)
16     append new block to public chain
17     if Δ_prev = 0 then
18         private chain ← public chain                   (they win)
19         privateBranchLen ← 0
20     else if Δ_prev = 1 then
21         publish last block of the private chain        (Now same length. Try our luck)
22     else if Δ_prev = 2 then
23         publish all of the private chain               (Pool wins due to the lead of 1)
24         privateBranchLen ← 0
25     else                                               (Δ_prev > 2)
26         publish first unpublished block in private block.
27     Mine at the head of the private chain.
```

.

VI. CONCLUSION

.

Bitcoins Design is fundamentally a game changer in many ways. bitcoin security has reinvented currency in a new light it takes the trust based system of the middlemen who provide this trust in exchange for fees and rips it apart by providing an incentive based protocol. Which works to every ones benefit and is very secure and publicly open compared to a centralized system. Even if an attacker was to try disrupt the bitcoin system the amount of power and effort it would take them to do so would be so costly that it actually would be more beneficial for that attacker to work with the system for personal reward than to destroy it. That being said it is not full proof like every system there are flaws that will always cast doubt and attackers are always coming up of new ways to breach systems but these security issues are hard to coordinate and execute. Since its fruition in 2009 bitcoin technology has gone from strength to strength and the security of the Cyrptocurrency is really starting to establish itself as a viable universal currency For the world

REFERENCES

[1] *Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System.* https://bitcoin.org/bitcoin.pdf

[2] *Bitcoin: Under the Hood.* http://search.ebscohost.com/login.aspx?direct=truedb=bthAN=109256850site=eds-live

[3] *Bitcoin and blockchain security.* https://books.google.ie/books?id=YYSuDgAAQBAJlpg=PA66ots=juNWOMcuI6dq

[4] *Majority is not Enough: Bitcoin Mining is Vulnerable.* http://www.cs.cornell.edu/ ie53/publications/btcProcArXiv.pdf

[5] *Optimal Selfish Mining Strategies in Bitcoin.* https://arxiv.org/abs/1507.06183

[6] *A Survey on Security and Privacy Issues of Bitcoin.* https://arxiv.org/abs/1706.00916v2

[7] *Bitcoin: Economics, Technology, and Governance.* http://search.ebscohost.com/login.aspx?direct=truedb=bthAN=102341027site=eds-live

[8] *Bitcoin: Technical Background and Data Analysis.* http://search.ebscohost.com/login.aspx?direct=truedb=bthAN=100292456site=eds-live

[9] *Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions.* http://search.ebscohost.com/login.aspx?direct=truedb=a9hAN=124814121site=eds-live

[10] *Research Perspectives and Challenges for Bitcoin and Cryptocurrencies.* https://courses.csail.mit.edu/6.857/2015/files/BMCNKF15-IEEESP-bitcoin.pdf