Breaking Down of 51% Double Spend Attack (DSA) in Blockchain Technology

S.Brilly Sangeetha, S.J. Jereesha Mary, S.Sebastin Antony Joe

Abstract— *Today the emerging trend and innovative technology is block chain technology. The actual question is how to manage this. The basic concept behind this is mining. Block chain is equal to governance. It is basic type of governance. It governs a book called ledger which contains information. Here we focus on double spend attack in block chain. The attackers has a space to block the new transactions from gaining access to acknowledgements. They make half payments between some or all users. It is even possible to reverse transactions when using the network or holding the complete control of the network thus spending the coins twice which means double spend coins. This attack always exist as a thread and users are panic about their transactions being used by a corrupted miner. The solution for this malicious mining is Proof of Work (PoW) which is proved to be not sufficiently decentralized or secure. So here we are focusing on Proof of Stake (PoS) concept which is a response to the treat of centralization.*

Keywords—*Blockchain Technology, Double spend, Governance, Mining, Transactions*

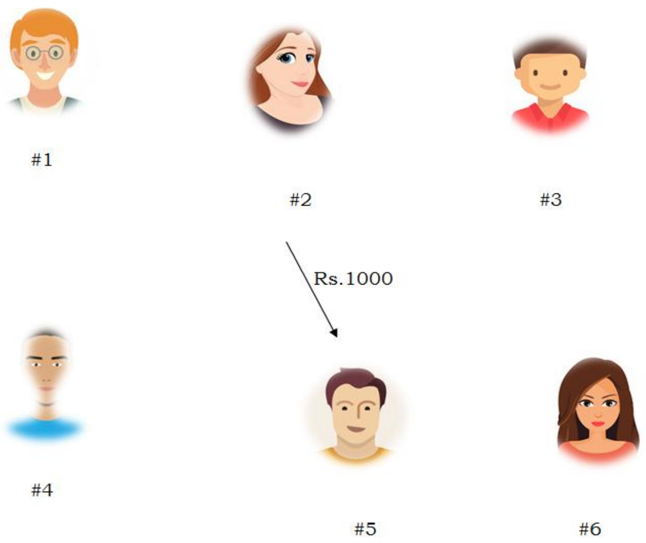
1. INTRODUCTION

Block chain technology is a technology which governs a book (ledger) of data. For example transactions of information. It is mandatory to learn about the blockchain protocols. This protocol is designed on democracy that is most of the miners on the connected network will decide which type of the block chain represents the real data .Its a singly linked list of blocks with each other blocks having many number of transactions. The properties are

1. Decentralized ,immutable data store
2. Shared book that records all transactions
3. Greater transparency
4. Trust to all parties

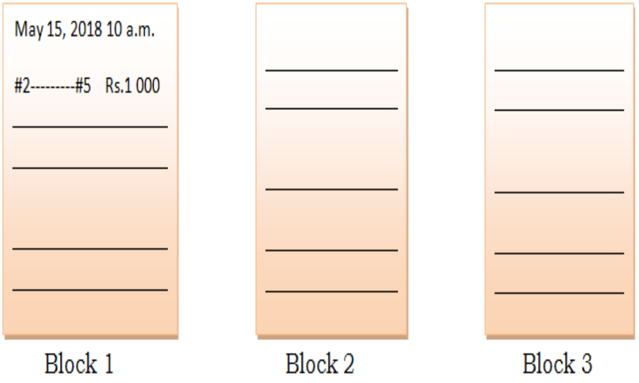
The basic concept is if we want to transfer money from one end to another we do it by trusting a third party. But in blockchain technology takes away the need for trust which is the core for bankings and financial sectors.

For example- we deposit money in banks and borrow money or transfer money with the help of banks. Here we can do the transfer of money without the help of bank with technology potential to reduce the role of banks, auditors and accountants. Transferring money defines the entry in the register. Is there any way to maintain a register by ourselves instead of someone else (third parties)? Yes, Blockchain technology does it. To implement block chain upon mutual agreement, consider six persons keeping details of other accounts without knowing the other’s identity.



Algorithm for implementation of blockchain technology with example

1. Every one will have an empy folder initially and keep on adding pages which makes register.
2. Everyone will be ready to make entry on their pages if transaction happens.
3. #2 wants to transfer an amount of Rs 1000/- and it shouts in the group that I am transferring an amount of RS 1000/- to #5.



4. Everyone will check if #2 is eligible to transfer the amount and note this in their page. The transaction is completed.

Revised Version Manuscript Received on July 18, 2019.

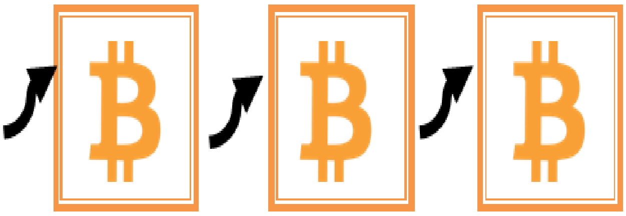
S.Brilly Sangeetha, Associate Professor, Department of Computer Science and Engineering, IES College of Engineering, Kerala, India.(E-Mail: brillyvino82@gmail.com)

S.J. Jereesha Mary, Faculty in Dept of IT, Al Musanna College of Technology, Oman. (E-Mail: jereesha@act.edu.com)

S.Sebastin Antony Joe, Faculty in Dept of Computing Sciences, Gulf College of Technology, Oman. (E-Mail: ssa_joe@yahoo.com)

5. This will be done by many users in the network and this process is called as hard hitting.

Bitcoin, a cryptocurrency, is the important application of the blockchain technology. Then **why is the term Bitcoin and Block chain get confused?**

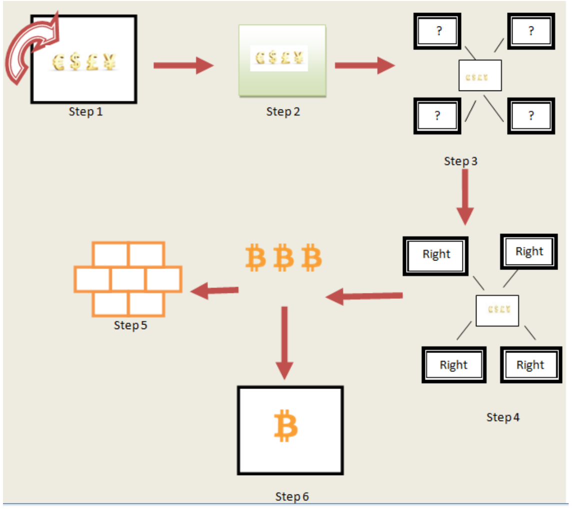


Cryptocurrency was first introduced in 2008 by an anonymous entity calling as Satoshi Nakamoto dictated in the paper titled *'Bitcoin: A Peer-to-Peer Electronic Cash System'* which spoke about electronic (non-physical) cash transactions without resorting to a financial institution. It was an underlying technology for making cryptocurrency transactions, which is now known as blockchain.

With Bitcoin being connected with blockchain technology, and the reason blockchain technology was discovered – the two terms are frequently used together, and therefore, are often confused.

II. HOW A BLOCK CHAIN WORKS?

The working of blockchain is demonstrated as follows.



1. A transaction is requested from a node.
2. A block that represents the transaction is created
3. The block is send to every node in the network.
4. All the node check the authencity and validates the node. Each node will get the reward points(bitcoins).
5. Block is added to the existing blockchain.
6. Transaction is completed.
7. The benefits of blockchain are increased efficiency and speed, transparency, improved traceability, and enhanced security.

III. WHY DOUBLE SPEND ATTACK A 51% ATTACK?

Its still confusing that a some miners in the network control network mining real hash rate or computing power. This attack mainly focused on half payments and block the access. They even reverse the payments and use the coin twice. As mentioned by experts if it is proved highly damaging also, it is found probably donot use destructive bitcoin or another blockchain based new currencyto be out reached . It cannot create new currency or alter the previous ones. For instance one can spend 10 bitcoins to purchase a car. Once the car is delivered logic dictates that bitcoins are to be transferred to cater for the cost of the car and this can activate the attack. Now the attacker can reverse the transaction and in the end the attacker will be the owner of the bitcoins used to purchase the car and even the car too.

As per the definition of double spend attack ,the attack happens once the attacker has the control of the network more than 50%..Hence the name 51% attack. Whenever a transaction is carried out in a blockchain by any means of cryptocurrency (bit coin), it will be into a pool of unconfirmed transactions.Miners are allowed to select the transactions of their own to form a block of transactions. If a transaction has to be added into a blockchain a miner must solve a complex mathematical puzzle. The miners will find a solution for the puzzle by using computational power. Higher the computational power, higher the person finding correct answer and add blocks to the block chain. A good miner should broadcast the answer of the puzzle in the network but a corrupt miner will not broadcast in the network.If the answer accepted and all transactions in the network blocks are valid according to the previous record on a blockchains. This always results in two versions of blockchain.

1. Original blockchain followed by a legitimate miners
2. Corrupt miners using a blockchain where the answers of the comple puzzle is not broadcasted.

Now the corrupt miner will be working from his own blockchain using his bitcoins or any other form of crypto currencies on the genuine case of the blockchain as of the original miners.

IV. JOB ON ROLE OF DOUBLE SPEND ATTACK.

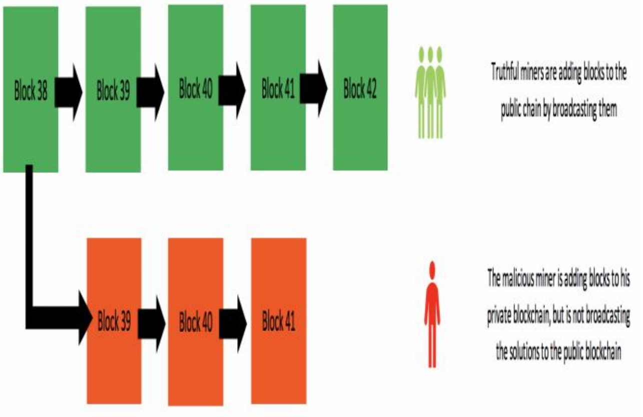
If any crypto currency owner signs off a transaction and if moves the transaction into a local pool of unconfirmed transactions, miners select the transactions from the pool to form a block of transactions. Then if they want to add this block of transaction to any blockchain, they have to solve a difficult puzzle by using computational power. This is called as hashing technique. When a miner finds a solution it will be broadcasted along with their own block to the other miners and they will verify all the transactions inside this block are valid according to the existing record of transaction on the blockchain.

To make a note on this a corrupted miner can never create a transaction for someone else because they would need the digital signature of that person that is they should know the owner's private key. So sending crypto currency from someone else's account is therefore impossible without access to their private key.

V. OFFSPRING OF THE BLOCKCHAIN IN DSA

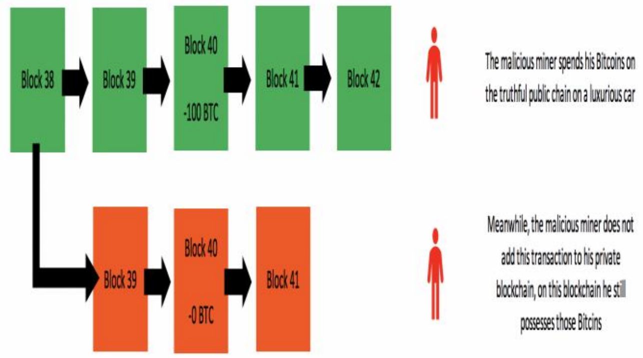
Now a days creating an offspring of the blockchain is done using stealth mining. A malicious miner can make an attempt to reverse existing transactions. Actually when a miner finds a solution it should be broadcasted to all other miners so that they can verify it whenever a block is added to the blockchain.

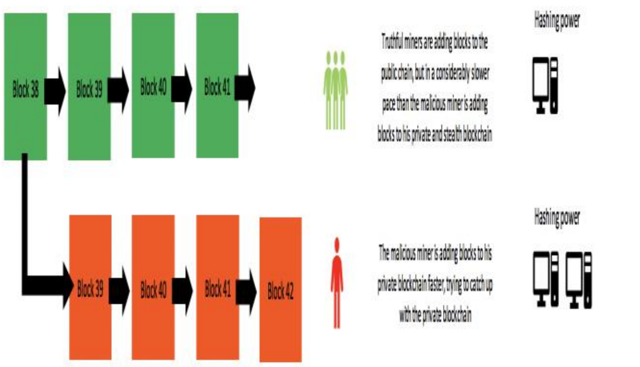
But here a corrupt miner creates an offspring of the blockchain by not broadcasting the solution. There are two versions of blockchain. One is Green blockchain and other is Red blockchain. The red blockchain is in stealth mode.


Block 38
Block 39
Block 40
Block 41
Block 42
Truthful miners are adding blocks to the public chain by broadcasting them
Block 39
Block 40
Block 41
The malicious miner is adding blocks to his private blockchain, but is not broadcasting the solutions to the public blockchain

The corrupted miner is now working on his own blockchain and is not broadcasting the information on the network.The rest of the network will not pick up this chain because it is isolated from the network. Now the corrupted miner spends all his bitcoins on the original version of the blockchain in which all the other miners are working with.

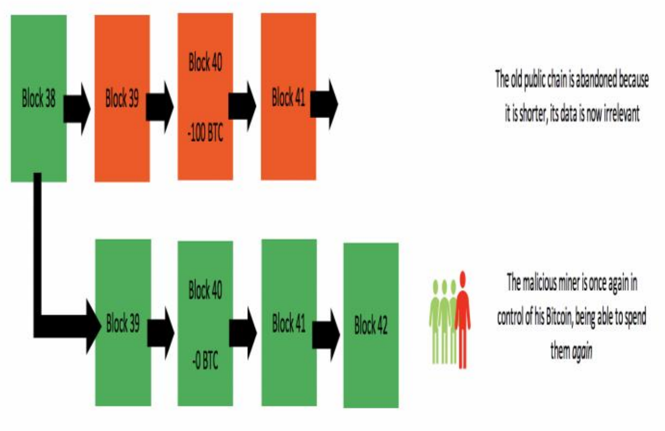
For example ,A person spends his bitcoins to purchase a luxurious car on blockchain. He doesnot include this in his isolated blockchain.so he has these bitcoins still in the isolated blockchain so he has these bitcoins in the isolated blockchain.Now the real trouble starts.The blockchain is programmed to follow a model of democratic governance.The blockchain does this by following the longest chain. Most of the miners add blocks to their version of the blockchain faster than the rest of the network.By this we can determinate which network is true.actually now the race has started between miners who has the most hashing power will add blocks to their chain faster.


Block 38
Block 39
Block 40
-100 BTC
Block 41
Block 42
The malicious miner spends his Bitcoins on the truthful public chain on a luxurious car
Block 39
Block 40
-0 BTC
Block 41
Meanwhile, the malicious miner does not add this transaction to his private blockchain, on this blockchain he still possesses those Bitcins


Block 38
Block 39
Block 40
Block 41
Truthful miners are adding blocks to the public chain, but in a considerably slower pace than the malicious miner is adding blocks to his private and stealth blockchain
Hashing power
Block 39
Block 40
Block 41
Block 42
The malicious miner is adding blocks to his private blockchain faster, trying to catch up with the private blockchain
Hashing power

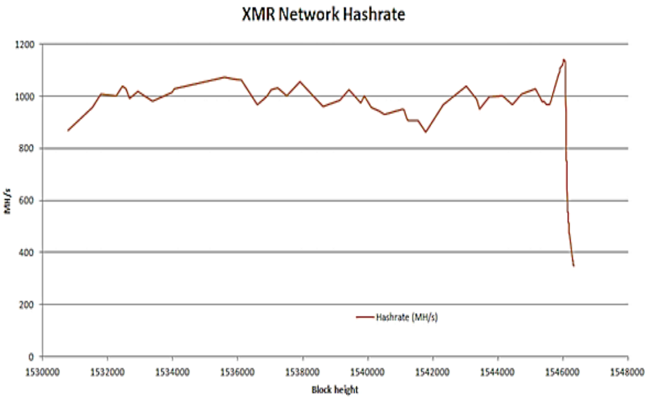
VI. REVERSING EXISTING TRANSACTIONS BY NEW LONGER CHAINS & RESULTS

The corrupted miner adds new blocks to his isolated blockchain faster than the other miners in the truthful blockchain.When this isolated blockchain becomes longer he broadcast this in the networks. As per the protocol the truthful miners switch to this chain.Now this completed blockchain is the truthful blockchain and all transactions will be reversed immediately.so the owner of the car as in example spend his bitcoins are not in stealth chain and now it is in the control of corrupted miner. He can spend this bitcoin once again. Hence it is called double spend attack.


Block 38
Block 39
Block 40
-100 BTC
Block 41
The old public chain is abandoned because it is shorter, its data is now irrelevant
Block 39
Block 40
-0 BTC
Block 41
Block 42
The malicious miner is once again in control of his Bitcoin, being able to spend them again

VII. METHODS TO SECURE BITCOINS AGAINST 51% ATTACK

These attacks are actually very difficult to perform. The Bitcoin blockchain is made up of hundreds of thousands of miners, a malicious miner would have to spend a lot on mining hardware to compete with the rest of the network. There are numerous other arguments against an attack of 51 percent. Electricity costs, the rental of mining equipment space, storage, tracking and money laundering, for example, risk being captured and traced. An operation such as this simply makes much too much effort to reimburse the attacker. A case study is that the attacker found a bug in the blockchain edge code which allowed him to produce new blocks at an extremely quick pace so that in just a short period of time the Verge blockchain can create a longer version of the blockchain. This example shows a 51% bug that is not common, but often caused by a body in the protocol code. This example shows a bug. A credible team of blockchain-developers will probably notice such a bug and stop it from being exploited. By reviewing the algorithm for ‘proof of work’, it tells us that more active hash / computer power leads to a 51-percent attack. Smaller blockchains that work on the algorithm may, however, be more vulnerable to such attacks like a small altcoin, as no way to compete with as much computer power is available. This is why 51% of attacks usually occur on small blockchains (e.g., Bitcoin Gold). A 51% attack has never occurred before on Bitcoin blockchain. Enhanced mining hardware (AISC Mining) is one of blockchain's newest hot topics recently; ASIC mining is a mining technology developed by various early mining firms in Bitcoin for improving mining hardware, making it much stronger. Many in the industry are now debating whether or not ASIC miners are overpowering some miners or groups. A protocol update that blocked ASIC mining from using its blockchain was recently implemented by the Monero (XMR) blockchain. The result is that the network's total hazard power dropped by a stunning 80%.



VIII. POTENTIAL SOLUTIONS

51% Double Spend Attacks are a threat to many evidence-of-working Blockchains. It is important that the hacker has the upper side if the attacker can collect the hacking power to control the network. However, it could actually eliminate the difficulty using completely different supreme algorithms. Evidence of play is often regarded as the best alternative because it relies on a mining knot to stake its own currencies to check transactions. Unrighteous nodes could lose the whole stake. In reality, the second most precious cryptocurrency has been changing over the next few months from a working proof algorithm to a proof-of-stake (Casper)-basis mechanism. Finally, 51% assaults are a threat that is not properly decentralized or secure to the PoW Blockchains. The most optimal solution is to fight centralisation and take a step forward against potential bad players.

IX. CONCLUSIONS

Although a 51% attack does not generate new coins or cause the collapse of the Blockchain directly, the confidentiality of participants in the cryptocurrency does have a major impact. If someone knows that a malicious miner can change the state of the Blockchain, then that creates a crisis of trust. Other network miners will either be confused or risk confirming the invalid chain. They think about the probability that their operations will not be confirmed by the malicious miner(s) and the transaction will be reversed. This could have a serious effect on trust, as a potential threat in future may arise. Fortunately, the most established Blockchains are less likely to suffer an attack for most cryptocurrency holders. This results in the costs of such an assault. A miner must attack more than 50 percent of a network to conduct a 51 percent attack. It needs a great deal of resources. The cost is electricity and hardware in terms of the proof of work mining algorithms.. The more established and progressive Blockchain, the more difficult it is for the blocks to spread, and the more expensive it is for the hash power to be gained. The attacker also has an indirect cost and that is how much the coin price drops. More people can begin dumping their own coins which will affect the value of the stolen loot, as the attack takes place. The costs of such attacks on the Bit coin network are estimated to be around $634 billion an hour. But for some newer Blockchains that have lower hazard power to protect their network, the same can not be said. This is important today because hashing power can be rented easily because hashing algorithms can be shared across chains.

REFERENCES

1. https://www.investopedia.com/terms/1/51-attack.asp
2. https://www.fxempire.com/education/article/51-attack-explained-the-attack-on-a-blockchain-513887
3. https://www.upgrad.com/blog/51-attack-in-blockchain-technology-explained/