Security threats on Blockchain and its countermeasures

Nidhee Rathod[1], Prof. Dilip Motwani[2]

[1]*Dept. of Computer Engineering, Vidyalankar Institute of Technology, Maharashtra, India*
[2]*Dept. of Computer Engineering, Vidyalankar Institute of Technology, Maharashtra, India*

---***---

Abstract - *Blockchain, the foundation of Bitcoin, has become one of the most popular technologies to create and manage digital transactions recently. It serves as an immutable ledger which allows transactions take place in a decentralized manner. This expeditiously evolving technology has the potential to lead to a shift in thinking about digital transactions in multiple sectors including, Internet of Things, healthcare, energy, supply chain, manufacturing, cybersecurity, and principally financial services. However, this emerging technology is still in its early stage of development. Despite the huge opportunities blockchain offers, it suffers from challenges and limitation such as scalability, security, and privacy, compliance, and governance issues that have not yet been thoroughly explored and addressed. Although there are some studies on the security and privacy issues of the blockchain, they lack a systematic examination of the security of blockchain systems. This paper conducted a systematic survey of the security threats to the blockchain systems and reviewed the existing vulnerabilities in the Blockchain. These vulnerabilities lead to the execution of the various security threats to the normal functionality of the Blockchain platforms.*

Key Words: **Blockchain, Digital Ledger, Security and Privacy, Scalability, Security Threats.**

1. INTRODUCTION

A Blockchain is a distributed, decentralized ledger or database that facilitate the process of recording transaction in the business network. In other words, A Blockchain is a distributed, transactional database that is shared across all the nodes participating in the network. Every transaction in the public ledger is verified by consensus of a majority of the participants in the network. Once the transaction is verified in the block and added to the blockchain, it is nearly impossible to erase or mutate the records. Bitcoin is the first implementation of Blockchain, introduced in 2009. Bitcoin is a cryptographically secure electronic payment system, or cryptocurrency, that uses peer-to-peer (P2P) technology, and it operates without any trusted third-party authority such as a bank, or any other centralized institutes. The owner of Bitcoin can use it anywhere, at any time without involving any centralized authority. Since the introduction of Bitcoin, Blockchain has shown promising application prospects and attracted a lot of attention from both academia and industry. The reason for interest in the Blockchain is its features that provide security, anonymity, and data integrity, without any third-party involvement in the transaction control.

2. LITERATURE REVIEW

Lloyd's London presents a report called “Emerging Risk Report 2015” [3] (Beecroft, 2015) and this report discussed different risk factors specifically in Bitcoin. Lloyd's report studies risk in various domain of Bitcoin such as operational risks, technological risks, market risks and a minor report on security risks in Bitcoin. Cambridge Centre for Alternative Finance conducted a global blockchain benchmarking Study (Hileman & Rauchs, 2017). This benchmarking study discusses the state of the blockchain ecosystem from the finance perspective and very slight attention to the privacy factors of Blockchain.

The Gervais et al. (2016)[4] paper introduced a novel quantitative framework to analyze the security and performance implications of various consensus and network parameters of Proof of Work (PoW) blockchains. This paper formulates adversarial strategies for double-spending and selfish mining while taking into account real-world constraints such as network propagation, different block sizes, block generation intervals, information propagation mechanism, and the impact of eclipse attack.

Apostolaki, Zohar, and Vanbever (2017) [5] discuss the Bitcoin's Hijacking. This paper provides a taxonomy of routing attacks and their impact on Bitcoin, considering both small-scale attacks, targeting individual nodes, and large-scale attacks, targeting the network as a whole. The paper discusses two general network attacks, partitioning attack and delay the attack.

3. BLOCKCHAIN OVERVIEW

Blockchain is a public electronic ledger, similar to the relational database, that can be openly shared among the different users and that creates an unchangeable record of their transactions, each is time-stamped and linked to the previous one. Each digital record or transaction in the thread is called a block, and it allows either an open or specific set of users to participate in the digital ledger. Blockchain can only be updated by consensus between the participants in the network, and when new data is entered, it can never be changed or erased which provides high data integrity in the blockchain. The blockchain contains a verifiable record of each and every transaction ever made in the system.[2]

Bitcoin is the first application of Blockchain and the Bitcoin based Blockchain is a public ledger system that maintain the integrity of transaction. Satoshi Nakamoto the founder of Bitcoin defines Bitcoin as a peer-to-peer electronic cash that allows online payments to be sent directly from one party to another without going through a financial institute.

From network perspective, Blockchain is distributed file system where participants keep copies of the file and agree on the changes by consensus. The file is composed of blocks and each block includes a set of transactions plus main data that includes, timestamp and a cryptographic signature (hash) of the previous block, hash of the current block, and some other information. The hash of the previous block ties the current block to the previous block and also the subsequent blocks will require the hash of the current block, so these all block are chained together. If anything in the block is modified, one could compute its hash and will find a different value as the stated one and will not accept the block. Thus, including the previous block's hash in the current block integrates the entire system history into the current block.[8]

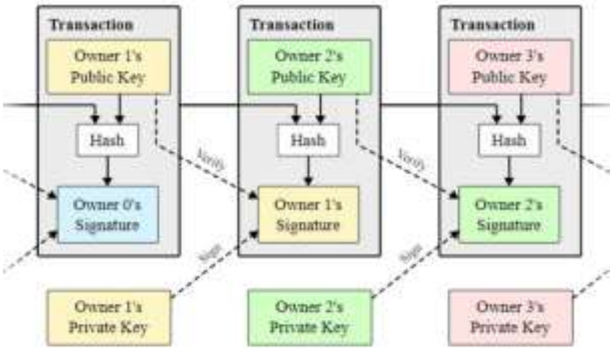

Fig -1: Blockchain Structure

3.1 Key Characteristics of blockchain

- Digital: All the information on blockchain is digitized, eliminating the need of manual documentation.
- Distributed: Transactions are grouped into blocks for processing and standard network protocol ensures every node (participant) receives every transaction in near real-time and applies the same rules.
- Decentralization: All participants (nodes) have own copy of all data in the system and no need for a central authority. This helps to obtain no single point of vulnerability or failure. In conventional centralized transaction system, each transaction needs to be validated through a central authority (e.g., bank) which requires some service fees, time and performance bottlenecks at the central servers. However, there is no central authority in the blockchain network, and no middle man/authority service fees are required, and also make the transaction faster. Consensus algorithms is used to maintain data consistency in decentralized, distributed network.
- Immutability: Data is immutable in the blockchain. Once the participants agreed on a transaction and recorded, it is nearly impossible to delete or rollback transactions once they are included in the blockchain.
- Consensus: There are standard algorithm/mechanism used to ensure all nodes agree on the integrity of transaction data in the system, replacing the need for a trusted third party. Before one can execute a transaction, there must be an agreement between all the participants that the transaction is valid. This process is known as "consensus" and it helps keep inaccurate or fraudulent transactions out of the blockchain. Blocks that includes invalid transactions could be revealed immediately.
- Anonymity: Each user can interact with the blockchain with a generated address, which does not reveal the real identity of the user, but participants can see the transaction. It is arguable the bitcoin blockchain cannot guarantee the perfect privacy preservation due to its intrinsic constraints but there are some other alternative blockchain protocols that claims for providing highest privacy.
- Traceable: Every transaction added to a public or private blockchain is digitally signed and timestamped, which means that organization can trace back to a specific time for each transaction and identify the corresponding party (through their public address) on the blockchain. So, every block is immutably and verifiably linked to the previous block. A full history can always be reconstructed right back to the beginning.
- Smart Contracts: Blockchain provides the functionality of smart contracts, or scripts that automatically execute when certain conditions are met. For instance, users of Ethereum– Ether (alt-cryptocurrency) exchange must meet the pre-defined conditions that prove someone owns the cryptocurrency and have authority to send the money they claim to own. It is also possible to develop smart contracts that require more than one set of inputs to trigger a transaction.

3.2 Working

Let us suppose A wants to send money to B. First, a block is created online and represents the transaction. Then this block is broadcasted to every participant in the blockchain network and set of participants approves the transaction and validates it. Once the block is validated, it is added to the chain which provides a permanent, non-reputable and transparent record of the transaction. Finally, B receives the money from A. The above steps are shown clarified in Figure 2.

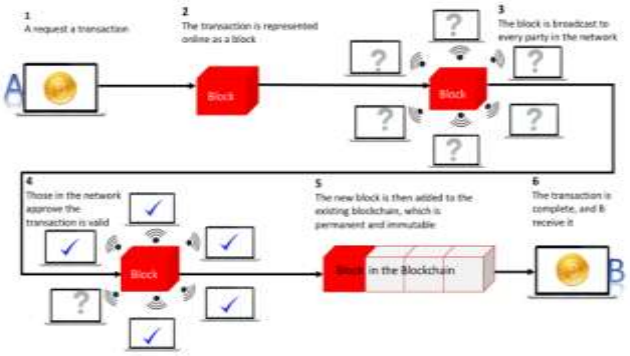
1
A request a transaction
2
The transaction is represented online as a block
3
The block is broadcast to every party in the network
A
Block
Block
?
4
Those in the network approve the transaction is valid
5
The new block is then added to the existing blockchain, which is permanent and immutable
6
The transaction is complete, and B receive it
Block
Block in the Blockchain
B

Fig -2: How blockchain works simplified.

3.3 Types

- Public blockchain: A public blockchain as its name suggest is the blockchain of public, i.e., anyone can participate in reading, writing and auditing the blockchain without permission. Public blockchain is open and transparent hence anyone can review the transaction at a given point of time. Eg: Bitcoin, Ethereum, Litecoin and many others.
- Private Blockchain: In private block chain the write permissions are kept centralized to one organization. Read permissions may be public or restricted to an arbitrary extent. Private blockchains are a way of taking advantage of blockchain by setting up groups and participants who can verify transactions internally. This create the risk of security breaches like a centralized system, as opposed to public blockchain secured by game theoretic incentive mechanisms. Eg: MONAX, MultiChain.
- Consortium or federated blockchain: Consortium is sometimes considered as third type of blockchain platform, but typically it a special type of private blockchain. This type of blockchain removes the individual autonomy which is responsible for bringing changes in the blockchain as in private blockchain. In consortium or federated blockchains operate under the control of a group of institutions. As opposed to public blockchains, consortium blockchain does not allow everyone to participate in the process of verifying transactions. Eg: R3 (banks), EWF (Energy), and B3i (Insurance)

3.4 Consensus Algorithm

- PoW (Proof of Work): PoW is currently the most common and one of the most robust consensus mechanism for blockchain technology. The miner has to solve mathematically complex puzzles on the new block before approving the block to the ledger. After solving the puzzle, the solution is then forwarded to other miners and verified by them before being accepted to their respective copies of the ledger. Blockchain core network protects against double-spending by the verification of each transaction with the use of Proof-of-Work (PoW) mechanism.
- PoS (Proof of Stack): In case of PoW, a miner is rewarded by resolving mathematical problems and creating new blocks, in Proof-of- Stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake. This means that in the PoS mechanism, there is no block reward. So, the miners take the transaction fees.
- SIEVE: SIEVE consensus mechanism is being used by Hyperledger Fabric which allows the network to detect and remove possible non-deterministic requests, and also achieve consensus on the output of the suggested transactions.
- Proof-of-Activity (PoA): In PoA, miners start with a PoW approach to solve the puzzle. If the blocks mined don't contain any transactions, the system switches to PoS. Based on the header information, a group of validators is assigned to sign the new block. If a validator owns more coin, he has the highest chance to be chosen. As soon as all the selected validators sign the template becomes a block. If the validators failed to complete the block, a new group of validators are being chosen, and this process goes on until a block receives the correct amount of signatures. Rewards are been divided between the miner and the validators. PoA requires too much energy like PoW, PoS
- Practical byzantine fault tolerance (PBFT): PBFT is a replication algorithm to tolerate byzantine faults. Hyperledger Fabric utilizes the PBFT as its consensus algorithm since PBFT can handle up to 1/3 malicious byzantine replicas.
- DPOS (Delegated proof of stake): Similar to POS, miners get their priority to generate the blocks according to their stake. The major difference between POS and DPOS is that POS is a direct democratic while DPOS is representative democratic. Stakeholders elect their delegates to generate and validate a block.
- Ripple: Ripple is a consensus algorithm that utilizes collectively-trusted subnetworks within the larger network.
- Tendermint: Tendermint is a byzantine consensus algorithm. A new block is determined in a round. A proposer will be selected to broadcast an

unconfirmed block in this round. So all nodes need to be known for proposer selection.

4. TECHNICAL CHALLENGES AND ADVANCES

- Scalability: Almost all existing Blockchain systems including the Bitcoin, Ethereum, Ripple and their associated consensus protocols have a scalability limitation. The challenging restriction is due to the decentralized nature of the blockchain system- every node on the network processes every transaction and maintains a copy of the entire state of the ledger. The main scalability problem is the time take to put a transaction in a block, and the time taken to reach a consensus.
- Throughput: Bitcoin manages around 7 transactions per second, Ethereum does about 20 transactions per second. Other transaction processing network such as VISA controls 1667 transactions per second and PayPal does 193 transactions per second. So, for the Bitcoin and Ethereum to compete with the more mainstream system like VISA and PayPal, they need to increase their throughput. In general, when the frequency of transactions in Blockchain rises to a similar level of VISA, the throughput of the blockchain networks need to be improved.
- Latency: It takes currently roughly 10 minutes in Bitcoin network to create or mine a block which contains transaction, for Ethereum it's around 14 seconds ("Bitcoin, Litecoin, Namecoin, Dogecoin, Peercoin, Ethereum stats,"). To achieve efficiency in the security, more time has to be spent on a block creation and validation, to ensure that the inputs for the transactions have not been previously used, which lead to double-spending attacks. Existing blockchain systems need to improve the block creation and validation time, to complete a transaction while maintaining the security.
- Size and bandwidth: The current size of the Bitcoin blockchain is 190.65 GB, and Ethereum blockchain size is 330.61 GB . When the throughput increases to the level of VISA network, bitcoin blockchain could multiply. The current average block size of Bitcoin is 1 MB. Ethereum uses gas limit mechanism rather than the block size. The time to create a Bitcoin 1 MB block which contains on average 500 transactions takes on average 10 minutes. If the Bitcoin blockchain needs to control more transactions, the size and bandwidth issues have to be resolved.

5. SECURITY THREATS TO BLOCKCHAIN

- Double-spending Security Threats: A double-spending attack is an attack where a consumer uses the same cryptocurrency multiple times for transactions, i.e., the given set of coins is spent in more than one transaction. For instance, Bob sends money to Alice (merchant) to get some product, Alice then ships the product to Bob, now since nodes always adopt the longer tail as the confirmed transactions, if Bob cloud generate a longer tail that contains a reverse transaction with the same input reference, Alice would be out of her money and her product.[9]

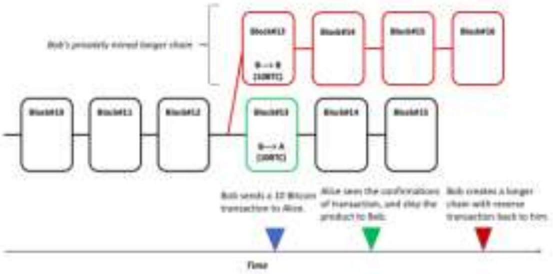
Bob's privately mined longer chain
Block#13
B→B
(10BTC)
Block#14
Block#15
Block#16
Block#10
Block#11
Block#12
Block#13
B→A
(10BTC)
Block#14
Block#15
Bob sends a 10 Bitcoin transaction to Alice.
Alice sees the confirmations of transaction, and ship the product to Bob.
Bob creates a longer chain with reverse transaction back to him.
Time

Fig -3: Double-spending attack simplified

There are various double-spending attack vectors or various ways to perform a double spending attack, such as Race attack, Finney attack, Vector76 attack, Alternative history attack, 51% attack.

- Race attack: Race attack happened when an attacker sends two conflicting transactions in rapid succession into the Bitcoin network. This type of attack is relatively easy to implement in PoW-based blockchains. Merchants who accepts a payment immediately with 55 "0/unconfirmed" are exposed to the transaction being reversed. Possible countermeasures: The three detection techniques are:
  Listening period: In the "listening period", the vendor associates a listening period with each received transaction, and it monitors all the receiving transactions during this period. The vendor only delivers the product, or provide the service, if he does not see any attempt of doublespending during the listening period.
  Inserting observers : In which the vendor inserts a node or couple of nodes that it controls within the Bitcoin network called "observer" that would directly relay all the transactions that it receives to the vendor. This helps the vendor to detect a double-spending attempt within seconds by him or by its observers.
  Forwarding double spending attempts: This technique is considered an efficient countermeasure to combat double-spending on fast Bitcoin payment. In this technique, the Bitcoin network peers propagate alerts whenever they receive two more transactions that share common inputs and different outputs.

- Finney attack: An attacker, pre-mined one transaction into a block and spend the same coins before releasing the block to public network to invalidate that transaction. This is called a 58 Finney attack. The Finney attack is a fraudulent double-spend that requires the participation of a miner once a block has been mined. An adversary can only perform a double-spending in the presence of oneconfirmation vendors.

  Possible countermeasure: Since a Finney attack can only be performed against a one confirmation vendor. In order to avoid the Finney attack, the vendor should wait for multiple confirmations before releasing the product or providing a service to the client. The waiting for multiple confirmation, will not prevent the doublespending attack, but will mitigate the risk and makes it harder for the attacker to spend the same coins more than once.

- Vector76 attack: Vector76 is also called a one-confirmation attack, in which attacker uses the privately mined block to perform a double-spending attack on the exchanges. It is a combination of the race attack and the Finney attack such that a transaction that even has one confirmation can still be reversed. A vector76 attack is possible when a wallet service such as cryptocurrency exchange runs a node that accepts direct (incoming) connections. Assuming that this node is using a static IP address, which will not be difficult for the attacker to find the IP address.

  Possible countermeasure: The protective actions could be, waiting for multiconfirmation, no incoming connections, explicit outgoing connections to a well-connected nodes, inserting observers in the network, notify the merchant about the on-going double-spend.

- Alternative history attack: The alternative history attack is still possible in case of multiple confirmations but requires high hash-rate and risk of significant expense in wasted electricity to the attacking miner.

  Possible countermeasure: The possible protective measures could be, no incoming connections, explicit outgoing connections to a well-connected nodes, inserting observers in the network, notify the merchant about the on-going double-spend.

- Fifty-one percent or >50% attack or majority hash rate attack : The blockchain relies on the distributed consensus mechanisms to maintain mutual trust in the network. However, the consensus mechanisms themselves have 51% vulnerability which can be exploited by the attackers to control the entire blockchain network. Though, the blockchain is designed with the assumption that honest nodes control the network. But when a user or group of users (miners) able to take control of more than 50% of the hash power in Proof-of-Work, then the 51% attack may be launched. The 51% attack or >50% is considered the most threatening attack on the blockchain network. It gives power to the attacker to destroy the stability of the whole network including actions such as double spending attack, exclude, modify, and self-reverse transactions and prevent some or all mining of valid blocks for their benefits.

  Possible countermeasures: The 51% attack is considered the most worst-case scenario as the adversary can do anything with the network. No amount of confirmation can prevent such attack; however, waiting for the confirmations does increase the aggregated resource cost of performing the attack. As the Bitcoin's security model relies not on a single coalition of miners controlling more than half of the network hash-rate. So, a miner or a mining pool with more than 50% hash power is an incentive to reduce their mining power and reframe from attacking. Therefore, the primary precaution is that no single miner or mining pool should have more than half of network hash-rate.

- Block-withholding attack (BWH): In block withholding attacks, blocks are discarded, and dishonest miners never publish a mined block to sabotage the pool revenue. However, in selfish mining, dishonest miners just kept the mined block secret until the right time to release them. Block withholding attack is usually made by infiltrating another pool.

  Possible countermeasure : The paper by Courtois, Bahack & Lear suggests a solution for block withholding attack, that pool manager should only allow trusted miners to register who are personally known to him or her. Also, if the pool revenue goes down than expected from its computational effort the pool should be closed.

- Fork-After-Withholding attack (FAW): FAW isanother variant of BWH attack. In case of the FAW attack, the attacker's reward is always equal to or greater than that for a BWH attacker, and it is four times more practical per pool than the BWH attack.

Possible countermeasures: There is no efficient solution so far reported and finding a cheap and efficient countermeasure remains an open problem.

Table-1: Major attacks on blockchain system and its POW based consensus protocol

Attack	**Description**	**Primary target**	**Adverse effects**	**Possible counter-measures**
Doube spending or Race attack	spent the same bitcoins in multiple transactions, send two conflicting transactions in rapid succession	sellers or merchants	sellers lose their products, drive away the honest users, create blockchain forks	inserting observers in network, communicating double spending alerts among peers, nearby peers should notify the merchant about an ongoing double spend as soon as possible, merchants should disable the direct incoming connections.
Finney attack	dishonest miner broadcasts a pre-mined block for the purpose of double spending as soon as it receives product from a merchant	sellers or merchants	facilitates double spending.	wait for multiconfirmations for transactions.
Brute force attack	privately mining on blockchain fork to perform double spending	sellers or merchants	facilitates double spending, creates large size blockchain forks	inserting observers in the network , notify the merchant about an ongoing double spend
Vector 76 or oneconfirmation attack	combination of the double spending and the finney attack.	Bitcoin exchange services.	facilitates double spending of larger number of bitcoins.	wait for multiconfirmations for transactions.
> 50% hashpower or Goldfinger	adversary controls more than > 50% Hashrate	Bitcoin network, miners, Bitcoin exchange centers, and users	drive away the miners working alone or within small mining pools, weakens consensus protocol, DoS.	inserting observers in the network , communicating double spending alerts among peers , disincentive large mining pools, TwinsCoin , PieceWork .
Block discarding or Selfish mining	abuses Bitcoin forking feature to derive an unfair reward	honest miners (or mining pools)	introduce race conditions by forking, waste the computational power of honest miners, with > 50% it leads to Goldfinger attack	ZeroBlock technique, timestamp based techniques such as freshness preferred , DECOR+ protocol
Block withholding	miner in a pool submits only PPoWs, but not FPoWs	honest miners	waste resources of fellow miners and decreases the pool revenue.	include only known and trusted miners in pool, dissolve and close a pool when revenue drops from expected, cryptographic commitment schemes.
Fork after withholding (FAW) attack	improves on adverse effects of selfish mining and block withholding attack	honest miners (or mining pools)	waste resources of fellow miners and decreases the pool revenue	no practical defense reported so far.

5. CONCLUSION

Blockchain is extremely appraised and supported for its suburbanised infrastructure and peer-to-peer nature. However, several researches regarding the blockchain area unit is protected by Bitcoin. But blockchain is been applied to a range of fields way on the far side Bitcoin. Blockchain has shown its potential for remodeling ancient trade with its key characteristics: decentralization, persistency, anonymity and auditability. This paper, explores the depth of comprehensive survey on blockchain. We initially offer an outline of blockchain technologies together with blockchain design and key characteristics of blockchain. We then discuss the standard agreement algorithms employed in blockchain. Furthermore, we have listed some challenges and issues that may hinder blockchain development and summarize some existing approaches for finding these issues.

REFERENCES

[1] Blockchains & distributed ledger technologies. (n.d.). Retrieved February 27, 2018, https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/. Bonneau, J. (n.d.).

[2] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008

[3] Lloyd's London presents a report called “Emerging Risk Report 2015”

[4] Gervais et al Retrieved February 27, 2018, “Novel quantitative framework to analyze the security and performance implications of various consensus and network parameters of Proof of Work (PoW) blockchains”

[5] Apostolaki, Zohar, and Vanbever, 2017 “Bitcoin's Hijacking”

[6] Conti, M., E, S. K., Lal, C., & Ruj, S. (2017). A survey on security and privacy issues of Bitcoin. ArXiv:1706.00916 [Cs]. Retrieved from http://arxiv.org/abs/1706.00916.

[7] Ellervee, A. (2017). A reference model for Blockchain-based distributed ledger technology. (Unpublished master's thesis), University of Tartu.

[8] Mearian, L. (2018, January 18). What is blockchain? The most disruptive tech in decades. Retrieved February 23, 2018,https://www.computerworld.com/article/3191077/security/what-is-blockchain-the-most-disruptive-tech-in-decades.html

[9] Halpin, H., & Piekarska, M. (2017).Introduction to security and privacy on the Blockchain. In Security and Privacy Workshops (EuroS&PW), 2017 IEEE European Symposium on (pp. 1–3). IEEE.