Blockchain Technology and Security

A survey on the technology used in blockchain, an overview of bitcoin, some of the security protocols and issues, and prevention techniques

Saad Ahmad
Beijing Institute of Technology
IoT Security and Privacy
Student ID: 1820182059

***Abstract*—Blockchain technologies have already changed people's lifestyle in certain aspects due to their impact in the business and industrial sectors. The importance of digital cryptocurrency and the concept of blockchain have been explored by several developers and organizations. It is assumed to be one of the secure and easy payment methods that can be used in the coming years. The security of blockchain networks have always been the focus of people's attention, and is one of the predominant reasons why blockchain technology has not yet been generally accepted worldwide.**

***Keywords*—** blockchain, security, cryptocurrency, bitcoin

I. Introduction

Blockchain technology produces a structure of data with inherent security qualities. To ensure trust in transactions, it is based on the principles of decentralization, cryptography and consensus. The data is structured into blocks in most blockchains or DLTs(Distributed Ledger Technologies), and each block either contains a single transaction or a bundle of transactions[13]. The blocks are part of a cryptographic chain, and each new block connects to all the blocks before it in a way that is impossible to tamper. All transactions within the blocks are validated and agreed upon by a consensus mechanism. Blockchain technology enables decentralization, with the participation of members across a distributed network. A single user cannot change the record of transactions, which means that there is no single point of failure. Blockchain networks can differ in who can participate and who has access to the data. Networks are typically described as either public or private, depending on who is allowed to participate, and permissioned or permissionless, depending on how participants gain access to the network.

II. Types of Blockchain

A. Public Blockchain

A public blockchain has an open network. The information is available in a public domain. Due to the permissonless nature of blockchains, the data is accesible to all and any party can read, write or view the data on the blockchain. No particular participant has control over the data in a public blockchain. Public blockchains are also decentralized and changeless. What this means that once an entry is validated on the blockchain after being entered, it cannot be deleted or modified. A public blockchain sees applications in public sectors like healthcare and education. For example, healthcare institutes can use blockchain technology to have a historical record of all their operations.

B. Private Blockchain

A private blockchain is also known as a consortium blockchain. A private blockchain is an invitation-only blockchain. The blockchain is governed by a single entity. The participating parties require permission to read, write, or audit the blockchain. The blockchain can have multiple layers of data access to keep certain pieces of data confidential. Private blockchains can be adopted in the corporate sector where the details need to be shared only between certain nodes. For example, a consortium of banks can adopt a private blockchain where financial transaction details are only shared with the concerned parties.

III. Background

The domain bitcoin.org was registered on 18 August 2008. On 31st October the same year, a link to a whitepaper authored by Satoshi Nakamoto was posted to a cryptography mailing list. On the 3rd of January 2009, the Bitcoin network came into existence. On that day, Nakamoto mined the "genesis block", in other words block 0, which had a reward of 50 bitcoins. It is speculated that Satoshi Nakamoto had mined close to a million bitcoins when it was still in its infancy. The first real-world bitcoin transaction was done by purchasing two pizzas from Papa John's for 10,000 bitcoins (the equivalent of $0.08 at that time)[11]. The growth of bitcoin in terms of USD is shown in the graph below[4].

Fig. 1. Bitcoin price over the years

Bitcoin's market cap is shown in the graph below[5].

Fig. 2. Bitcoin Market cap

IV. Satoshi Nakamoto

So who is this mysterious Satoshi Nakomoto? After Nakamoto published his famous white paper on a crypto mailing list, bitcoin came to life. His white paper described a digital currency that would allow secure, p2p transactions without any middleman involved, whether that be a corporation, a financial institution or the government. The tranasctions would be tracked using a blockchain. This digital ledger would be distributed across the entire network and the exact duplicates would be held by all the participants on the network. All of this was to be secured by cryptographic means. Satoshi Nakamoto created this currency with the goal that of taking control of currency from the elite financial institutions and giving it to the common man[2]. That is why there will never be more than 21 million bitcoin. Bitcoin is fully open source. This means that its design is public, and anyone can access it. There is no single entity that owns or controls bitcoin. As Nakamoto continued to control the development of Bitcoin, many other users and developers converged in the forums to contribute and work on the project. Throughout the history of bitcoin, efforts to unveil Satoshi Nakamoto's true identity have ended in vain. There have been all sorts of wild speculation. Some say that Nakamoto is a part of the Yakuza, whereas others say that he might be a money-launderer. In a world where anonymity is taken for granted, and is getting more and more difficult to pursue, Satoshi Nakamoto has truly succeeded in keeping his secrets.

V. How a blockchain works

A. Consensus Mechanism

A consensus mechanism is a protocol which ensures that all the members in a given blockchain are complying to the agreed rules. This ensures that all the transactions are legitimate, by having each participant consent to the state of the distributed ledger[3]. Public blockchains operate as decentralized systems without a central authority. They involve contributions from thousands of participants who work on the verification and authentication of the transactions, which effectively makes the blockchain a secure and reliable technology for digital transactions. There have been several consensus mechanisms introduced considering the requirements of secure digital transactions.

B. Functionality

A blockchain is a digital technology that records the origin of a digital asset. The digital information is stored in blocks, and any information inside those blocks cannot be modified, which is the inherent nature of this technology[14]. Each block has three basic elements, which are listed below.

- The data in the block.
- a 32-bit whole number, called nonce. It is randomly generated when a block is created, which in turn generates a block header hash.
- The hash is a 256-bit number joined to the nonce. It must start with a huge number of zeroes i.e. be extremely small.

The information enclosed within the blocks is available to the public, such as payment information and client records. Every block has a digital signature. A change to a single digit of any particular block produces a totally new digital signature. The blocks can be verified by anyone who is a part of the network. Due to this, any malice is immediately detected by the participants in the network. In the case of failure of any part of the network, the blockchain still keeps on running as usual.

C. Mining

Mining is a process that involves computing a new block to the distributed ledger. The block generation process differs for different cryptocurrencies. Computers used for mining are used in generating the correct hash values. Nodes that are involved in mining are required to solve a mathematical puzzle utilizing their machines to mine[8]. As soon as a miner successfully produces a new block, they then notify the network about it. After this is done, every miner in the network stops mining that particular block and then start solving equations for the next block. During mining, a miner takes the hash Merkle root and adds it to the nonce value. Of all the transactions in the block, The Merkle root is the hash of all hashes. It is a part of the block header. With this being said, to securely verify that a transaction jas been accepted by the network, and get the number of confirmations, all that needs to be done is download just the small block headers and the Merkle tree. It allows one to verify

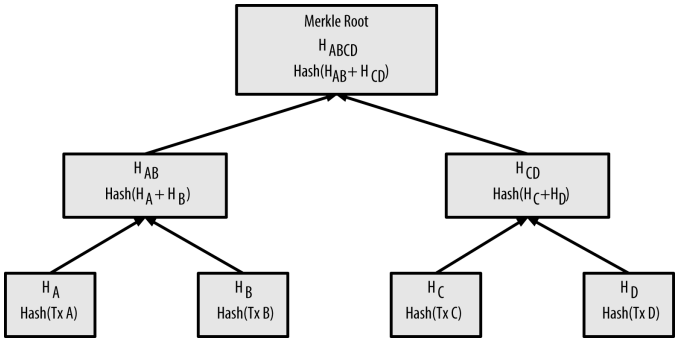

Fig. 3. Merkle Tree

transactions as needed and not include the body of every transaction in the block header, while still providing a way to test the entire blockchain and therefore proof of work on every transaction. A new hash is then generated from the amendment of the nonce value and then is compared with the target each time. If the hash value turns out to be less than the target, the mathematical puzzle is solved. Crypto mining is a painstaking process, which is intermittently rewarding. It requires a lot of processing power and electricity, which generates a lot of heat as a result.

VI. Security Problems

If not accounted for, the effects of the exposure of blockchains to their specific set of security issues can be adverse. These are discussed below.

A. Double Spending/ 51% attacks

A 51% attack refers to an attack on a blockchain, commonly Bitcoin. Such an attack is still hypothetical, that being more than 50% of the network's mining hash rate being controlled by a group of miners.[12]. Due to the hardware used, the total computational power of a decentralized PoW system the sum of the computational power of its nodes, which in turn may differ significantly. Larger computational power increases the prospect to win the mining reward for every new block mined, which creates an incentive to accumulate clusters of mining nodes, or mining pools. Any pool that achieves 51% hashing power can effectively overturn network transactions, resulting in double spending. As the name implies, a blockchain is basically a

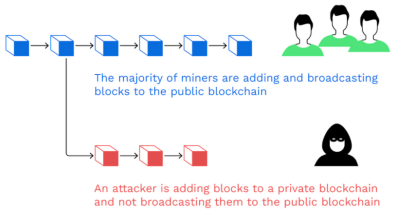

Fig. 4. A 51% attack

chain of blocks, which are bundles of data that record all completed transactions during a given period. For bitcoin, a replacement block is generated approximately every 10 minutes. Once a block is finalized or mined, it can't be altered since a fraudulent version of the general public ledger would quickly be spotted and rejected by the network's users. However, by controlling the bulk of the computing power on the network, an attacker or group of attackers can interfere with the method of recording new blocks. They can prevent other miners from completing blocks, theoretically allowing them to earn all of the rewards by monopolizing the mining of the latest blocks. The existing hashing power of the network is what determines a given cryptocurrency's susceptibility to attack, since the attacker needs to overcome it. For the attack to be viable economically, to justify the cost to rent hashing power the market cap of the currency must be adequately large.

B. Sybil Attacks

A Sybil Attack may be a sort of attack seen in peer-to-peer networks. During this kind of attack, a node within the network operates multiple identities actively at an equivalent time and undermines the authority in reputation systems. The main aim of this attack is to gain the majority of influence in the network to carry out illegal(with respect to rules and laws set in the network) actions in the system. A single entity(a computer) has the potential to make and operate multiple identities(user accounts, IP address based accounts). To outside observers, these multiple fake identities appear to be real unique identities. The model utilized in the Sybil Attack paper may be a simple one. This consists of the following:

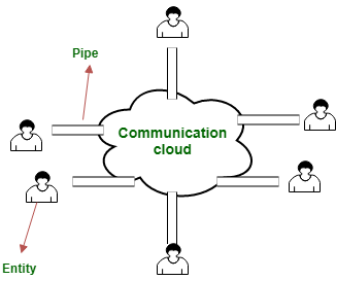

Fig. 5. A Sybil attack model

- E entities = c(correct) entities + f(faulty) entities
- correct – entities that follow the protocols and rules setup in the network honestly.
- faulty – entities whose behavior is erratic and cannot be predicted. They do not follow the protocols and rules in the network honestly.
- A communication cloud: A general purpose cloud through which messages between different entities travel.
- pipe: It connects an entity with the communication cloud.

There are two types of Sybil attacks, which are listed below:

- Direct attack - The Sybil node directly influences the honest nodes.
- Indirect attack - A node that directly communicates with the Sybil nodes attacks the honest nodes. The middle node is under the influence of the Sybil nodes and is compromised.

C. Balance Attacks

The Balance attack is a novel form of attacks that affect proof-of-work blockchains, especially Ethereum. Its novelty lies in identifying subgroups of miners of equivalent mining power and delaying messages between them instead of entering a race to mine blocks faster than others. The Balance attack demonstrates a fundamental limitation of main proof-of-work systems in that they are not immutable. The Balance attack is simple: while the attacker disrupts communications between correct subgroups of equivalent mining power, it simply issues transactions in one subgroup[10]. The attacker then mines a large number of blocks in another subgroup with the high probability that the subtree of another subgroup outweighs the transaction subgroup's. The attacker can rewrite the blocks that contain these transactions by outweighing the subtree containing this particular transaction, even though the transactions are committed. One may benefit from delaying messages only between the merchant and therefore the remainder of the network by applying the eclipse attack to Ethereum. Eclipsing one node of Bitcoin appeared, however, sufficiently difficult: it requires to restart the node's protocol so as to regulate all the logical neighbors the node will eventually try to connect to. While a Bitcoin node typically connects to 8 logical neighbors, an Ethereum node typically connects to 25 nodes, making the problem even harder. Another option would be to isolate a subgroup of smaller mining power than another subgroup, however, it might make the attack only possible if the recipients of the transactions are located in the subgroup of smaller mining power. Although possible this is able to limit the generality of the attack, because the attacker would be constrained on the transactions it can override. The Balance attack inherently violates the persistence of the main branch prefix and is enough for the attacker to double spend. The attacker has simply to identify the subgroup that contains merchants and create transactions to buy goods from these merchants. After that, it can issue the transactions to this subgroup while propagating its mined blocks to at least one of the other subgroups. Once the merchant shipped goods, the attacker stops delaying messages. Based on the high probability that the tree seen by the merchant is outweighed by another subtree, the attacker could reissue another transaction transferring the precise same coin again. an attacker has to be knowledgeable about the current settings of the blockchain system to execute a Balance attack. In fact, the attacker must have information regarding the logical or physical communication graph, the mining power of the miners or pools of miners and the current difficulty of the crypto-puzzle. The dynamic information regarding the mining power and the difficulty of nodes is generally public information and can often be retrieved online.

VII. Attack Mitigation Techniques

In this section, we shall discuss some of the recent defense techniques based on mitigating the 51% attacks.

A. Delayed Proof of Work(DPoW)

Delayed Proof of Work is a security mechanism designed by Komodo. It is basically a modified version of the Proof of labor (PoW) consensus algorithm that creates use of Bitcoin blockchain's hashpower as how to reinforce network security. Not only are the Komodo developers able to secure their own network, but also any third-party chain that joins the ecosystem made by Komodo by using dPoW[7]. The Zcash codebase implemented the dPoW security mechanism, allowing complete privacy, and by leveraging Bitcoin's hash rate, offering increased network security. At an interval of ten minutes, a snapshot of its blockchain is taken by the Komodo system. This is then written to the Bitcoin network through the process of notarization. What this means is that a backup of the entire Komodo system is saved within the Bitcoin blockchain. The reason why the notary nodes select a block hash that's about ten minutes old is to make sure that the whole network agrees the block is valid. Each blockchain's network still comes to consensus for each block[15]. A block hash from a previously-mined block is simply recorded by the notary nodes. The reason why the notary nodes select a block hash that's about ten minutes old is to make sure that the whole network agrees the block is valid. Each blockchain's network still comes to consensus for each block. One of the main goals of a PoW algorithm is to maintain network security, discouraging cyber attacks such as DDoS attacks. The mining is very demanding by design within PoW-based blockchains. Miners need to solve a complex cryptographic

puzzle in order to be able to mine a new block. Intense computational work is involved in such a process, which is very costly in terms of hardware and electricity. Therefore, one among the explanations Proof of labor blockchains are secure is that the incontrovertible fact that the mining process involves a really high financial investment and depends on network consensus. However, it's important to notice that the safety of PoW blockchains is directly associated with the quantity of computational power (hash rate) being dedicated to them. In contrast to PoW, dPoW isn't wont to achieve consensus on new blocks and, thus, isn't considered a consensus algorithm. Instead, it's a security mechanism that's implemented additionally to ordinary PoW consensus rules. The blockchains are far more secure and resistant to the 51% attacks because DPoW makes it impossible for the blocks to be reorganized once they have been notarized.

B. ChainLocks

ChainLocks is a security technique developed to secure DASH. It results from the implementation of long living masternode quorums (LLMQs) to mitigate the 51% attack. ChainLocks executes a network-wide vote process which comprises a "first-seen" policy. For each particular block, an LLMQ of an outsized number of master nodes is approved[6]. Every participant is required to sign the noticed block so that the active chain can be extended. 60% or more of the participants verify the distinct block and generate a P2P message (CLSIG) to notify every other node in the network about the event. The (CLSIG) message can't be generated unless enough members suits it. The message involves a legitimate signature for authenticity and verifiable by all the nodes within the network. The transaction gets confirmed after the first confirmation in this security protection technique. Once confirmed, it cannot be reversed back as the signed block cannot be acknowledged at a later time. This security feature lifts the six confirmation aspects and enhances a secure transaction after just one confirmation. ChainLocks also helps to mitigate other security issues in addition to the 51% attack.

C. Merged Mining

Merged mining refers to the act of mining two or more cryptocurrencies at an identical time, without the overall mining performance being sacrificed[9]. This operation can be viewed as a generalization of incremental mining. Fundamentally, computational power of a miner can be used to mine blocks on multiple chains concurrently through the utilization of what's referred to as Auxiliary Proof of labor . For merged mining to be performed, an equivalent algorithm must be used by all the involved cryptocurrencies. For instance, Bitcoin uses SHA-256, meaning that virtually the other coin that uses SHA-256 are often mined along side Bitcoin - as long because the technical implementations are properly done[1]. Notably, the parent blockchain is barely affected because it doesn't need to go under any quite technical modification. On the opposite hand, the auxiliary blockchain must be programmed to effectively receive and accept the work of the parent chain.

VIII. Conclusion

The assumption of having the majority of honest miners over the blockchain network has been underestimated resulting in realistic and practical 51% attacks to various cryptocoins. In fact, this encouraged attackers to perform the 51% attack. We have shown that the PoW consensus protocol comprises severe security risks and fails to protect against the 51% attack, uncovering that this and other consensus protocols are vulnerable. We have also identified that the weaknesses which enable the 51% attack exploitation rely on the hashing power ability of mining pools and how this attack could cause immense damage to the blockchain network. The presented security-based evaluation revealed the weaknesses of each technique. In our analysis, we showed that all the security techniques fail to provide enough protection against the 51% attack. The implemented security policies lack robustness, and a sturdy policy must be in place to conquer these challenges. By studying the limitations of the consensus protocols and the protection techniques, we revealed the fundamental weaknesses contained in them, suggesting that further research must be performed. A security policy accepting a limited number of blocks by totally ignoring the longest chain rule must be explored to mitigate the 51% attack effectively. For future work, we aim to develop an effective protection mechanism against the 51% attack by creating a robust consensus protocol without the weaknesses and limitations analyzed in this paper.

References

[1] W.G. Aref, M.G. Elfeky, and A.K. Elmagarmid. "Incremental, online, and merge mining of partial periodic patterns in time-series databases". In: *IEEE Transactions on Knowledge and Data Engineering* 16.3 (2004), pp. 332–342. DOI: 10.1109/TKDE.2003.1262186.

[2] Rebecca Baldridge. *Why The Father of Bitcoin Is Nowhere to Be Found*. URL: https://robbreport.com/lifestyle/finance/bitcoin-founder-satoshi-nakamoto-1234613022/. (accessed: 2021.05.26).

[3] A. Baliga. "Understanding Blockchain Consensus Models". In: 2017.

[4] *Bitcoin price today, BTC live marketcap, chart, and info — CoinMarketCap*. URL: https://coinmarketcap.com/currencies/bitcoin/. (accessed: 2021.05.26).

[5] *Bitcoin to USD Chart (BTC/USD) — CoinGecko*. URL: https://www.coingecko.com/en/coins/bitcoin/usd#panel. (accessed: 2021.05.26).

[6] Alexander Block. *Mitigating 51% attacks with LLMQ-based ChainLocks*. URL: https://blog.dash.org/mitigating-51-attacks-with-llmq-based-chainlocks-7266aa648ec9. (accessed: 2021.05.26).

[7] *Delayed Proof of Work Explained — Binance Academy*. 2021. URL: https://academy.binance.com/en/articles/delayed-proof-of-work-explained. (accessed: 2021.05.26).

[8] Suman Ghimire and Henry Selvaraj. "A Survey on Bitcoin Cryptocurrency and its Mining". In: *2018 26th International Conference on Systems Engineering (ICSEng)*. 2018, pp. 1–6. DOI: 10.1109/ICSENG.2018.8638208.

[9] *Merged Mining — Binance Academy*. URL: https://academy.binance.com/en/glossary/merged-mining. (accessed: 2021.05.27).

[10] Christopher Natoli and Vincent Gramoli. "The Balance Attack or Why Forkable Blockchains are Ill-Suited for Consortium". In: *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. 2017, pp. 579–590. DOI: 10.1109/DSN.2017.44.

[11] Martin Rosulek. *What is Bitcoin and How Does it Work*. URL: https://www.blockalive.com/what-is-bitcoin/. (accessed: 2021.05.26).

[12] Jimi S. *Blockchain explained: how a 51% attack works (double spend attack) — Good Audience*. 2018. URL: https://blog.goodaudience.com/what-is-a-51-attack-

or - double - spend - attack - aa108db63474. (accessed: 2021.05.27).

[13] *What is Blockchain Security — IBM*. URL: https://www.ibm.com/topics/blockchain-security. (accessed: 2021.05.25).

[14] *What is Blockchain? — Lisk*. URL: https://lisk.com/what-is-blockchain. (accessed: 2021.05.27).

[15] Xinle Yang, Yang Chen, and Xiaohu Chen. "Effective Scheme against 51% Attack on Proof-of-Work Blockchain with History Weighted Information". In: *2019 IEEE International Conference on Blockchain (Blockchain)*. 2019, pp. 261–265. DOI: 10.1109/Blockchain.2019.00041.