Security Challenges in blockchain

Ankit Singh
Master's of Computer Application - Software Engineering
Guru Gobind Singh Indraprastha University
Delhi, India
ankitsigh0111000@gmail.com

Abstract

Blockchain technology is considered secure and reliable as it uses the hashing protocols to interlink the blocks, creating a tamper-resistant system. The blocks are developed and interlinked using the hash code, a 64-bit alphanumeric hexadecimal key which is locally distributed among all the peer networks, enhancing the security. Vulnerabilities present in the smart contract are another major challenge for the security in the blockchain. Flaws in the code can be exploited which may lead to unauthorized access, data breaches, or manipulation and tampering of contract terms. The immutability of transactions is a foundational blockchain feature that sometimes becomes a double-edged sword, i.e., erroneous or malicious transactions once entered then are irreversible. Research aims to analyse data, gather information and study the challenges to the blockchain, focusing on potential threats like 51majority of the network's computing power, enabling the whole network to manipulate the transactions sometimes even double-spending the currency and may such attacks, which can inject a malicious block into the network and compromise the integrity of the blockchain.

Keywords: Hashing Protocols; Blocks; Immutability, 51- majority; Double spending.

1. Introduction

Blockchain technology is a fast-growing technology as it has several functionalities and feature. Bitcoin and the other cryptocurrencies are often considered as the main reason to blockchain technology's success and growth. Understanding history of the bitcoin, Satoshi Nakamoto (an anonymous developer) in 2008 introduced a digital currency (peer to peer network) Bitcoin using Blockchain and which led to emergence of bitcoin, bitcoin was introduced in 2009 [1], resulting in the boom of cryptocurrency and blockchain technology in the world. Blockchain is considered to have a rapid rise as technologies are switching to blockchain due to its numerous advantages over the previous network "the centralised network" which had several flaws like lacked to perform better over the large data, had increased risks, in centralised network system if main server fails or gets corrupted, the entire network is likely to get shut down whereas blockchain is a decentralised public ledger that has no concept of central node system, it is a P2P network system where it aims to govern transparency and efficiency along with the enhanced security [3]. It is predicted that the annual growth rate and size of blockchain technology market in world will increase to 39 billion US Dollars by 2025. Blockchain is a series of blocks, the block contains Block number, Nonce, Data, Previous hash and Current hash [3]. The first block in the blockchain is called the genesis block [6]. Each block is linked with the other block and link between the blocks is established by the help of cryptographic hash code i.e., a 64-word alphanumeric unique hexadecimal code (also called the unique identifier) which makes the block secure and reliable [5]. As sensitive data is being passed though the block it is necessary to configure the security of node and the system and hence to understand the challenges to the security in blockchain get important. The research will delve in collection of information from e-books, researches, journals and other resources and study the blockchain, security in blockchain, security challenges and issues in blockchain, attacks that can be done or are done on a blockchain in past which may breach the integrity of the blockchain network.

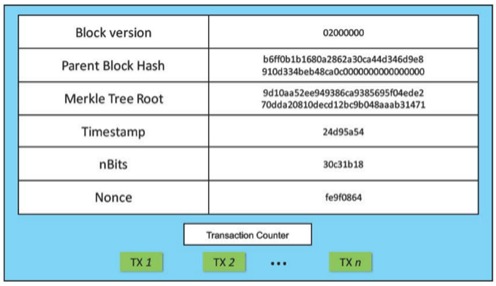

Рис. 1: **: Elements in side block in a block chain [3]**

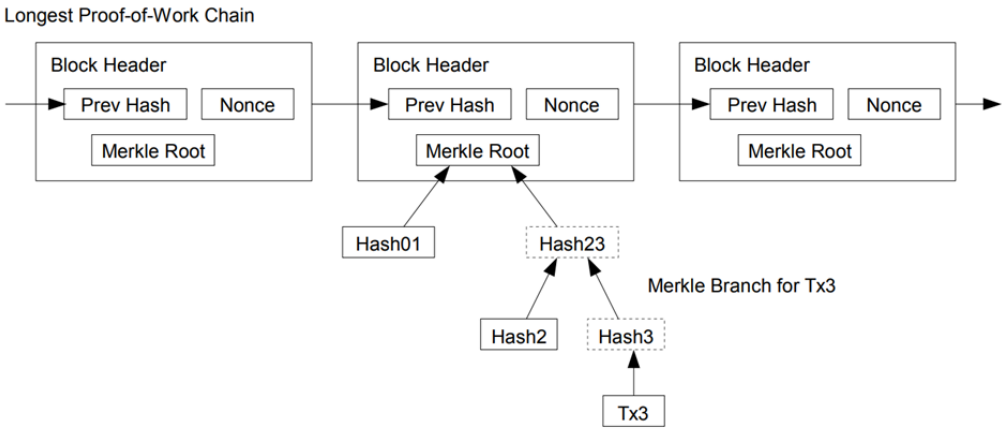

Рис. 2: **Diagrammatic representation of blocks in blockchain [1]**

2. Blockchain

Blockchain is a secure distributed public ledger, a peer-to-peer network [1][8], Blockchain is a chain of blocks that are stored over network in decentralised manner in a distributed network storing all committed transactions in a network [2]. As the system of network is distributed every participant or peer that is a member of the following network has the copy of the data over the network. In simpler terms, a local copy of transactions is distributed over the network to every participating member which ensures transparency of data among the members and integrity of the data over the network and the network chain grows continuously as when new blocks are appended to it resulting in creation of a network the growth of the network highly depends on number of participants present in the network and blocks that are being added [3]. It can help in alleviating multiple security risks that threaten traditional centralised systems such as single points of failure [6]. Blockchain is considered as leverage a secure and resilient networking architecture, a robust consensus protocol, and as a environment for building higher-level application [12].

2.1 Type of Blockchain Blockchain is categorised into 3 types: Public blockchain, Private blockchain and consortium blockchain.

2.1.1 Public blockchain: Public blockchain is an 'open to all' type of blockchain any node can read, send, verify transactions, participate without any security permission, often considered as the permissionless ledger [5]. In public blockchain network everyone has the knowledge and information about the transaction being performed in the network. This type of blockchain requires architects to consider the trade-offs between privacy and transparency in the given context [6][12]. Examples of public blockchain: Bitcoin, Dogecoin, Litecoin etc.

2.1.2 Private blockchain: Private blockchain are the permissioned, restricted and secure blockchain network which are rigorously controlled by a single authority hence it is also referred as the centralised blockchain [5][6]. Private blockchains require trust in identities, especially when the number of blocks in the

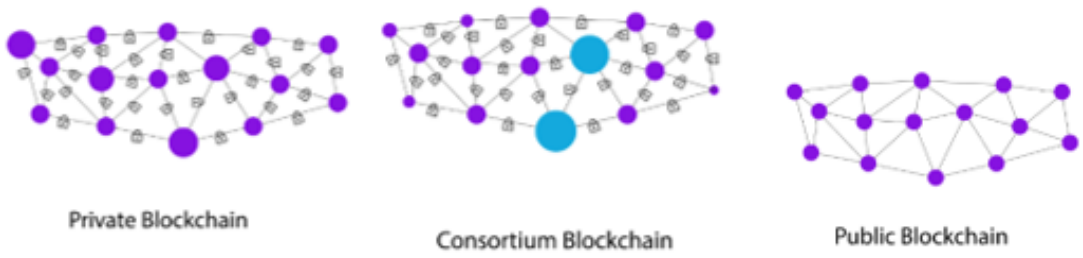

Рис. 3: Types of BlockChain

network are less as the parties sometimes act in collusion to threaten the system [12]. In this data (sensitive information) cannot be accessed by any outsider who has not been given the permission to be part of private block chain network by an organisation which makes the data only accessible to those within the organisation make it secure from outside access [5]. Example of private blockchain: ripple, Ethereum etc.

2.1.3 Consortium blockchain: Consortium blockchain also referred as federated blockchain or partially decentralised blockchain. It is considered as a balance between the both public and private blockchain in terms of reading, writing and security [6]. Generally made for when group of authorities or institutions come together to achieve a common goal. It is considered as highly distributed blockchain as it contains several organisations [5]. Example of consortium blockchain: Hyperledger.

2.2 Key features of the blockchain

Distributed ledger: Blockchain is considered as a distributed ledger every node is connected to one another making the transaction process faster and efficiently, Distributed property makes it nearly impossible to tamper the public blockchain [3].

Decentralisation and transparency: In a public blockchain, data is decentralized, eliminating the need for a central authority. Each node possesses an identical local copy of the data, ensuring security and integrity. This distributed structure fosters transparency, allowing peer nodes to observe transactions and activities on the chain. Unlike centralized systems, transactions in the blockchain occur peer-to-peer (P2P) without the need for authentication by a central agency [9]. This decentralized approach reduces trust concerns among network participants. However, in proof-of-work (POW) scenarios like Bitcoin and Ethereum, server and energy costs are comparatively high, impacting performance [2].

Immutability: As the data stored in the blockchain if written once and uploaded on the chain it cannot be altered it is implemented by the help of cryptographic principles [2]. Security: As blockchain uses cryptography, hashing techniques blocking are preferred to be much secure [2]. It is considered as a tamper resistant system i.e., any transaction information stored in the blockchain cannot be tampered during and after the process of block generation [3].

Efficiency: Fewer validators and elective consensus protocols, private and consortium blockchain can facilitate better performance and energy efficiency [2], the strong consistency and efficiency chain model means that all nodes have the same ledger at the same time [3]

3. Security in blockchain

Blockchain is considered as **immutable, secure and transparent** as it is distributed over the network. In blockchain security is governed by the several methods and algorithms such as **cryptography, consensus mechanism and transparency** [2]. Blockchain technology promises to overcome security challenges, enhance data integrity, and transform the transacting process into a decentralised, transparent, and immutable manner [6]. Blockchain comprises of blocks which are interlinked with one another. The linking of the block is established by the help of hashing codes. This is termed as a part of cryptography.

Cryptography is a method of developing protocols and techniques to hinder unauthorised access of data from sensitive information during a transaction. Blockchain uses the method of cryptography to establish a highly secured link between two blocks or nodes. Blockchain mainly uses hashing function cryptographic method to induce security in the blocks.

Hash function plays a major role defining the security and integrity of the blockchain. Any type of inconsistency or manipulation can result in discarding the chain and making it void and invalid. Use of cryptographic primitives i.e., hashing provides uniqueness integrity and quickness to the blockchain. It uses SHA-256 algorithm to generate a hash code a 64-word alphanumeric hexadecimal unique code which is responsible for maintaining the integrity of the blockchain [5]. Use of **Asymmetric-key cryptography** primitive is used to generate a digital signature also governs the security in the block chain

Use of security tools such as Oyente, remix, gasper, SmartCheck ensures the security of the network they provide the security over mishandled exception, time stamp dependencies, immutable bugs, block hash usage [9].

4. Consensus mechanism

We know that the blockchain is a **decentralised network** hence there exists no central or main authority to check and verify the nodes that are being added into the network whether they are malicious or not. Even then the blockchain performs transaction in a much safer manner with complete security, transparency and integrity. The reason behind blockchain is able to maintain transparency and security is because of consensus protocol [3], it helps decentralized networks making unanimous decisions [9]. It is considered as a backbone to the blockchain technology. Consensus mechanism is an approach in which all the member(peer) of the block chain network come to a common conclusion a consensus (an agreement) on whether a node which is being added to the network is a true node or not and who will add it that is decided by the other peers in the network. Based on whether the network is a permissioned or permission less blockchain there are several consensus algorithms that are driven to reach to a consensus.

POW (Proof of Work): POW is a consensus algorithm used by the bitcoin in order to add a new node into the network, adding a node in the network through pow requires high computational power and energy consumption. POW tries to solve the issue i.e., a new node getting added to the network, as nodes need to solve a difficult puzzle with adjusted difficulty to obtain the opportunity of appending the new block to the current chain. **Competitors** who use logics and energy computational powers are called miners [2].

Competitive miners calculate the hash value with **SHA-256 hash function** to convert all the altered or manipulated of the block until one reach to matching hash value and if reached then mutually the data and resources are compared, as a result new node gets pushed by the miner involved in finding the hash. In other terms, Miners mine the block in POW [3], once one block is added block reward is given to the miner [2]. **Miners are required to solve the hard complex mathematical puzzle in order to mine a block.** The consensus follows that the calculated hash must be smaller than or equal to the given value which is hectic task as it takes time, computational power, energy [3]. The proof-of-work also solves the problem of determining representation in majority decision making [1].

POS (proof of stake): POS is a consensus mechanism that requires very less computational power as one to validate the transaction or to become a candidate, Validator has to put a amount of cryptocurrencies on stake and authority with the highest stake is most likely to become a validator. The only problem lies with this consensus protocol is that wealthiest node may receive more chances to validate a block and becomes more dominant in the network [3][12]. In comparison with POW, proof-of-stake (POS) can be an energy efficient alternative and can be more sustainable than POW, as it saves more energy as well as provides better latency and throughput It does not require high computational power equipment and Standard equipment also can work [2], **POS majorly focuses towards the stakes and is an efficient alternative of POW** [3].

POET (Proof of Elapsed Time): Proposed by Intel, Associated with permissioned blockchain. If an individual has become a participant of the network the individual,it gets mandatory for the individual to go through verification and validation processes as an obligatory way to maintain the security and integrity of system [3]. In POET there are equal chances of win by providing random associated waiting time to a node until that the node is set to inactive state. **DPOS (Delegated Proof of Stake):** Delegated proof-of-stake (DPOS) is an elective consensus procedure where each node with a stake in the network can delegate the validation of transactions to another node by the process of voting [2]. **POS** follows a direct democratic approach whereas DPOS is a representative democratic method. The delegates get elected by the stakeholders to generate and validate a block and are known as witnesses [2]. These elected nodes then form a set that proposes blocks and validate data states. They take turns on voting for blocks on behalf of their stakeholders and validate previous blocks authenticity. Generally, most implementations employ a replacement pool with a standby validator [3].

5. Security issues and Challenges

Although blockchain is considered to be secure yet there arise several challenges and issues that may impact and compromise the integrity and security of the blockchain. As blockchain applications are connected and are available over the internet, they are vulnerable towards the various **cyber-attacks including stealing of resources [7], spy attempts, and Denial-of-Service (DoS) attacks,** which can make blockchain services unavailable and sometimes gaining whole control over the network. One of the main security concerns with blockchain is that public keys and transactions must not reveal real identities [3].

Hard fork

Hard fork is dividing of blockchain network can occur in any kind of blockchain. Their messy nature can compromise the network security, making it more susceptible to attacks. The reason behind the hard fork is correcting the security by bringing some upgrades to it, by adding new functionalities and new divisions are to be made in order to create new forks that help in creating integrity and security risk. Whenever hard fork is generated two new forks get generated on is old and other is the new one and a copy get induced leading it to become less secure. **Re-entrancy and time stamp dependency:**

Re-entrancy in a smart contract allows it to call external functions, including its own, offering flexibility. However, this feature can be exploited by malicious actors to manipulate the contract's state, posing potential vulnerabilities. Re-entrancy acts a double sword for the blockchain as it provides flexibility but also leads to creation of weak nodes vulnerable to attack. **Identity revealing attacks:**

A Sybil attack is a popular attack in terms of blockchain security threat where a large number of fake nodes are introduced into the network to anonymize client traffic and create vulnerabilities. The attack creates loop holes in the integrity of the decentralized system introducing malicious nodes to control a portion of the network, leading to potential manipulation, fraud, and disruption of various operations [12].

Selfish mining problem and Spoofing:

Selfish mining poses a significant threat to blockchain networks by compromising the integrity of the mining process. In this attack, a miner attempts to gain a competitive advantage by withholding newly mined blocks to increase their chances of collecting rewards. This strategy can lead to inconsistencies in the blockchain, undermining the reliability of the network and potentially destabilizing its operation.

Spoofing refers to the attempt on the part of an adversary to access a blockchain system, or even control the network, by using a false identity. This can be done by stealing or retrieving the private keys and the credentials of an authorised node [5].

Tampering: Tampering is a critical threat where an attacker makes unauthorized modifications to data, transactions, or blocks, whether stored or in transit, with the intent to manipulate or misuse the information.

Denial of Service:

DOS threat makes a system unavailable when legitimate users request a service. This can be accomplished by causing network congestion which interrupts the service available to the user also leading into increased retrieval time. To prevent DOS, a node can privately determine whether it is a potential leader by using Verifiable Random Function (VRF) and immediately release a block candidate.

Other major issues and challenges includes the consensus related challenges i.e. in the POW high computational power is utilised in order to mine a particular node which is not inexpensive and also is not environment friendly.

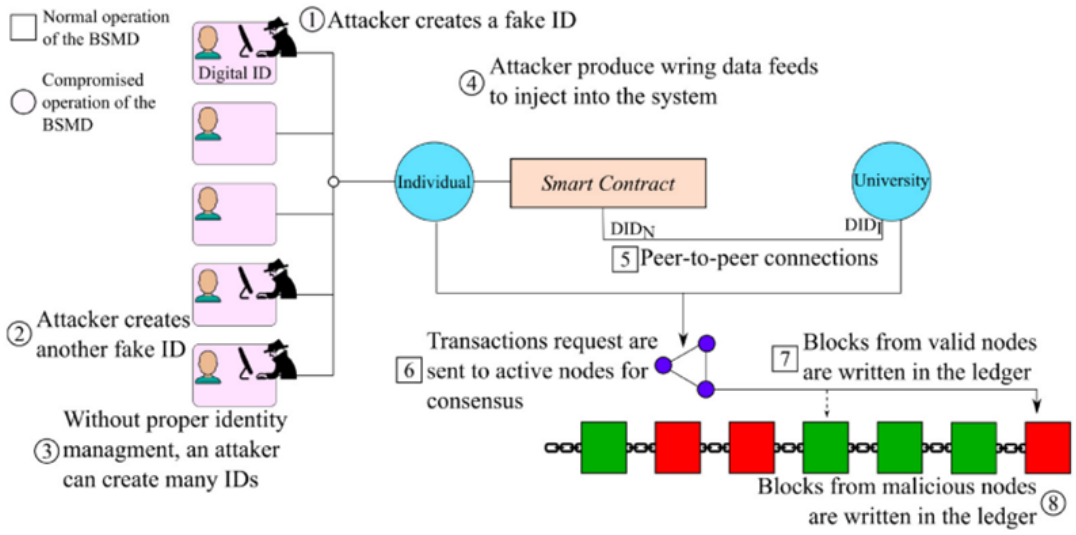

Рис. 4: Figure 4: Detailed steps of attack scenario of false data injection [7].

Other is POS which can be considered as a kind of in justice to honest nodes and dedicated miners as one with higher stakes gains higher chances to be a validator. Rest remains various attack that can be done on the network, nodes and on chain through the loop holes present and are serious threat to the security of the blockchain.

6. Attacks

Blockchain network being decentralised, immutable, scalable is still prone to attacks, one of the stealing attacks was against MtGox, a bitcoin exchange based in Tokyo, Japan, in 2014 that resulted in a loss of $600 million, another example was against Ether digital currency that values around 55$ million [2]. Threats like injection of fake data and malicious node into the network affects whole network [7].

51 percent attack

Also referred as majority attack. In this attacker gains control over more than half of the network power. Impact of this results in breach in integrity of the network by merging a malicious chain with the network trying to gain the dominance over the network to perform double spins and perform transaction multiple times [9][11], during a 51 percent attack, it is possible to redirect financial transactions and manipulate other confidential processes such as smart contracts in one's own favour – with massive consequences for affected companies and blockchain operators. 51 percent attack is one of major concern for the double-spending of money [7][12].

In this, the attacker forks a private chain from honest chain. Next, he gains 51 percent or more computing-power in blockchain and creates two conflicting transactions. The attacker sends one transaction in true chain paying a receiver some goods and another double-spend transaction to himself in his chain. The attacker starts mining blocks on his chain and generates blocks quicker than the honest nodes by using his computing-power. Once the attacker chain length is greater than the honest chain length, the attacker chain becomes valid and honest nodes adopt it based on the longest chain rule. Thus, it makes the double-spend transactions valid [3], and the attacker receives his spent funds back to himself [11].

Sybil attack

The Sybil attack is one of the majorly occurring and concerning attack on the blockchain network. It comprises of the attacker nodes honest nodes and the sybil nodes [9]. To initiate the attack, the attacker creates large number of Sybil nodes and connects with the honest nodes that disconnect genuine connections of honest nodes with other honest nodes on the P2P network. In this manner the attacker takes control over the whole P2P network when he gains a disproportionately large influence on the network. Eventually, the attacker uses Sybil nodes and attack method to trigger various threats damaging the reputation system of a P2P network [11].

```
WHILE true DO
    AttackerNode.ForkPrivateChain(AttackerChain, HonestChain)

    IF AttackerComputationalPower >= 51% THEN
        IF AttackerNode.CreateConflictingTransactions() THEN
            SendTransaction(Transaction1, HonestChain)
            SendTransaction(Transaction2, AttackerChain)

            AttackerNode.StartMining(AttackerChain)

            IF AttackerChain.Length > HonestChain.Length THEN
                ValidateChain(AttackerChain)
                HonestNodes.AdoptChain(AttackerChain)
                AttackerNode.RetrieveSpentFunds()
            END IF
        END IF
    END IF
END WHILE
```

Рис. 5: Algorithm for 51 attack

```
WHILE true
  DO
    AttackerNode.CreateSybilNodes()
    AttackerNode.ConnectSybilNodesToHonestChain()
    systemFraction = AttackerNode.GainSystemFraction()

    IF systemFraction == 1 THEN
        AttackerNode.ExecuteAttackMethod()
        AttackerNode.TriggerThreat()
        AttackerNode.DamageReputationSystem()
    END IF
END WHILE
```

Рис. 6: Algorithm for sybil attack

The DAO (Decentralised Anonymous Organisation) attack:

DAO attack or the consensus-based attack. The DAO was a medium where the transaction can be carried out by transferring Ether and receiving the tokens. Token was a key factor in approving a state of proposal. Ethereum deployed DAO as a smart contract in 2016 on a crowdfunding platform. The DAO contract was assaulted after being deployed for 20 days. It had raised approximately US120$million before the attack, and the attacker stole around 60$ million, making it the largest attack on the Ethereum consensus model [9][11]. To track down the and recover the stolen funds hard forking was done and new contract was created.

Selfish Mining Attack: Selfish mining attacks are committed by some miners to waste legitimate miners' computing power or obtain unearned rewards. Such attackers attempt to fork the private chain by making the discovered block private [9], As a result, the selfish miners gain a competitive advantage over real miners.

Eclipse attack: Eclipse attacks aim to hijack all connections of a node to its peers in a blockchain network. Eclipse attacks arise from threats on DNS and routing in the network, and they may be a result of vulnerabilities in p2p protocols. Eclipse attack can be seen generally over the public blockchains [12].

7. Strengthening Security with Diligent Oversight

Enhanced focus towards mixing techniques:

Mixing techniques are used in order to prevent users' addresses from being linked. CoinJoin was proposed in 2013 as an alternative anonymization method for bitcoin transactions. It is motivated by the idea of joint payment [2]. CoinJoin requires that users negotiate transactions with whom they wish to join payment. The first generation of the mixing services to offer this functionality. Enabling of firewalls, multiple factor authentication and enhanced security patches at every threat prone interface may improve the security of the network [3].

Remodelling and enhancing smart contracts:

Trusted Execution Environment Based Smart Contracts (An execution environment) that provides a completely isolated environment for application execution, which effectively prevents other software applications and operating system(s) from tampering with and learning the state of the application running in it [2], generally provides a security to the smart contract. Using frameworks to develop the privacy of smart contracts. The Hawk framework allows developers to write codeless private smart contracts to enhance the security system [9].

Resolving hard fork gaps:

Hard forks can introduce security vulnerabilities by splitting the chain, creating attack-prone gaps in the network. Resolving hard fork gaps and introducing upgrades in the software, smart contracts certainly would increase the integrity and increase the security [3].

Upgrading consensus protocol:

Consensus protocols play a pivotal role in ensuring blockchain security by preventing unauthorized access, tampering, and forks. Upgrading Proof-of-Work (POW) methods for block inclusion can greatly enhance the overall security of the chain [11]. Upgrading consensus models provides 1) **Consistency**- safeguarding all nodes that are vulnerable. 2) **Fault tolerance** - fault tolerance for recovery from failure nodes. 3) Better **readability and maintainability** of the application.

Decentralising:

Decentralization enhances blockchain security by reducing vulnerability, as larger chains are more resilient to attacks than smaller ones. A distributed system undergoes thorough inspections before appending any node to the chain, making it more challenging for smaller chains.

Additional Security Aspects:

Incorporating secure cryptographic primitives or biometric configurations in Proof-of-Work (PoW) and Proof-of-Stake (PoS) mechanisms enhances security when adding a node to the network. This reduces the risk of information tampering, ensuring the creation of a secure and resilient distributed network.

10. Conclusion

Blockchain is a decentralised distributed and a growing network which is transparent, maintains integrity and considered as highly secure and has many applications from medical sector to finance, from yet there are flaws in the blockchain and as blockchain is getting popular and nearly everything is switching to blockchain technology, it is highly important to understand about the security flaws that is the challenge to the blockchain security. The paper provides information about security in block chain and such challenges that were faced by the blockchain like 51 percent attack, double spending attack, sybil attack and many other and to understand the challenges in security to blockchain. There are several challenges that a network faces in blockchain for example: hard fork, scalability issues, vulnerability of the smart contract and many more.

11. References

1. S. Nakamoto et al., Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, [online] Available: http://bitcoin.org/bitcoin.pdf.
2. A. A. Monrat, O. Schelén and K. Andersson, "A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities,"in IEEE Access, vol. 7, pp. 117134-117151, 2019, doi: 10.1109/ACCESS.2019.2936094.
3. R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," ACM Computing Surveys, vol. 52, no. 3, pp. 1–34, Jul. 2019, doi: 10.1145/3316481.
4. Wang, Huaimin Zheng, Zibin Xie, Shaoan Dai, Hong-Ning Chen, Xiangping. (2018). Blockchain challenges and opportunities: a survey. International Journal of Web and Grid Services. 14. 352 - 375. 10.1504/IJWGS.2018.10016848.
5. S. Ahmadjee, C. Mera-Gómez, R. Bahsoon, and R. Kazman, "A study on blockchain architecture design decisions and their security attacks and threats," ACM Transactions on Software Engineering and Methodology, vol. 31, no. 2, pp. 1–45, Apr. 2022, doi: 10.1145/3502740.
6. S. Aggarwal and N. Kumar, "Attacks on blockchain," in Advances in Computers, 2021, pp. 399–410. doi: 10.1016/bs.adcom.2020.08.020.
7. I. Homoliak, S. Venugopalan, D. Reijsbergen, Q. Hum, R. Schumi and P. Szalachowski, "The Security Reference Architecture for Blockchains: Toward a Standardized Model for Studying Vulnerabilities, Threats, and Defenses,"in IEEE Communications Surveys Tutorials, vol. 23, no. 1, pp. 341-390, Firstquarter 2021, doi: 10.1109/COMST.2020.3033665.
8. M. N. M. Bhutta et al., "A Survey on Blockchain Technology: Evolution, Architecture and Security,"in IEEE Access, vol. 9, pp. 61048-61073, 2021, doi: 10.1109/ACCESS.2021.3072849.
9. S. Singh, A. S. M. S. Hosen and B. Yoon, "Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network,"in IEEE Access, vol. 9, pp. 13938-13959, 2021, doi: 10.1109/ACCESS.2021.3051602.
10. N. Fields, "4 types of blockchain technology explained," Komodo Academy | En, Aug. 31, 2023. https://komodoplatform.com/en/academy/blockchain-technology-types/
11. M. Iqbal and R. Matulevičius, "Exploring Sybil and Double-Spending Risks in Blockchain Systems,"in IEEE Access, vol. 9, pp. 76153-76177, 2021, doi: 10.1109/ACCESS.2021.3081998.
12. I. Homoliak, S. Venugopalan, D. Reijsbergen, Q. Hum, R. Schumi and P. Szalachowski, "The Security Reference Architecture for Blockchains: Toward a Standardized Model for Studying Vulnerabilities, Threats, and Defenses,"in IEEE Communications Surveys Tutorials, vol. 23, no. 1, pp. 341-390, Firstquarter 2021, doi: 10.1109/COMST.2020.3033665.