Turkish Journal of Computer and Mathematics Education Vol.12 No.13 (2021), 571-581

Research Article

The blockchain technology and attacks on it

Kanneganti Jahnavi[a], Gandharba Swain[b]

[a,b]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh-522502, India
[a]jahnavi.kanneganti@gmail.com, [b]gswain1234@gmail.com

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 4 June 2021

Abstract: Now a day's blockchain technology has become popular because of its decentralised, peer to peer, immutable and distributed nature. It allows us to perform transactions, and store these transactions in an immutable way. It's a kind of database in which the total data is stored in form of blocks. However due to its decentralised nature there are many challenges like scalability and security attacks. So various researchers have started their research activities in this direction. In this paper we have described the different characteristics, issues, challenges, and consensus mechanisms of blockchain. Furthermore, we have identified a number of security attacks and elaborated them with detailed discussions. There are mainly seven types of attacks identified, (i) 51% attack, (ii) distributed denial of service attack (DDoS), (iii) selfish mining attack, (iv) eclipse attack, (v) double spending attack, (vi) sybil attack and (vii) phishing attack.

Keywords: Blockchain characteristics; consensus protocols; blockchain applications; blockchain challenges; blockchain attacks

1. Introduction

Blockchain is a kind of distributed database [1]. It is said that blockchain was designed by a person named Satoshi Nakamoto or by some pseudonymous group of people in 2008. The first foundation for blockchain technology was initiated in the year 1991 by Stuart Haber and Scott Stornetta. They founded a technology in which the document timestamps cannot be tampered. Later on, Merkle tree was introduced for merging many document time stamps into a single block to increase the performance and efficiency [2]. By using all these technologies Satoshi developed the blockchain concept to avoid trust on third party. He incorporated the characteristics like immutability, and consensus. In blockchain the storage of data is done in the form of blocks in a chronological order (one after the other in a sequence) as shown in the Fig. 1.

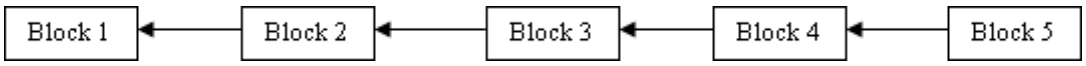

Fig 1: Blockchain structure

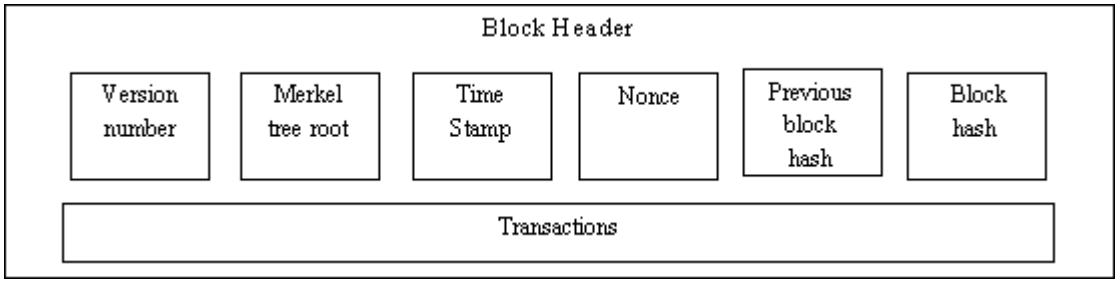

Fig 2: Block Structure

As depicted in Fig.2, there are block header and body in every block of a blockchain. The header consists of six items, (i) block version that indicates the rules to be followed [3], (ii) merkle root that is used for making the blocks immutable [4,5], (iii) timestamp for indicating the time at which the block was created [4], (iv) nonce, a random number generated by the consensus mechanism to calculate the hash value of a block [4], (v) previous block hash is the hash of the preceding block in blockchain [5], (vi) block hash is the unique identity of a block. The first block of blockchain will not have the previous block and that block is known as the genesis block. The block body consists of transactions which indicate the list of transactions that are recorded in the block. The total number of transactions that a block contains will be based on the size of the block and also on the size or transactions.

Each block in blockchain network is cryptographically connected to its previous block by using the hash value [6,7]. All the blocks in blockchain are connected to each other in a chronological order. If any changes are

done on the transactions, it will completely change the block hash. So once the transactions are added to blockchain we cannot alter them. Hence blockchain is immutable. The total process in blockchain is carried out in a decentralised way [8] (without central authority). In Fig.3 centralised and decentralised networks are shown. Because of this decentralised nature even if some nodes of the network in blockchain crashes, the rest of the nodes functions normally which avoids single point of failure. When any new blocks are to be added in blockchain, all the nodes in the blockchain should validate it. In blockchain all the transactions are broadcasted over peer to peer network. Due to this peer to peer network the users can access the network simultaneously [9].

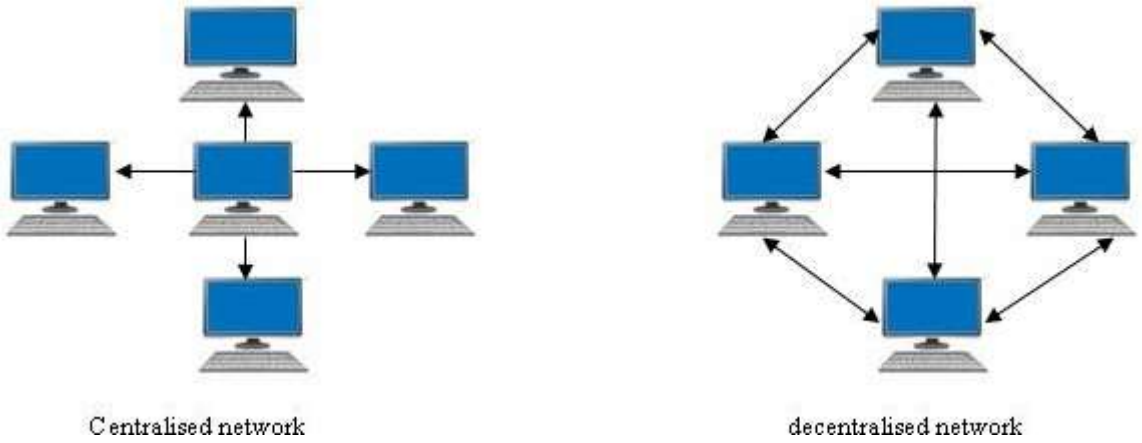

Fig 3: Centralised and decentralised network

To add a new block to existing blockchain, asymmetric cryptography technique [10] is used for authentication purpose [6]. In this method the user in the network will have two keys. One key is known as public key and other one is known as private key. These two keys are inter-twined mathematically in such a way that encryption can be done by one key, and decryption can be done by the other key [11]. The message to be sent is first signed and encrypted by using the public key of the recipient [12] and the recipient can decrypt it by his private key [13].

In the working process of blockchain first the sender will create a transaction and broadcasts it to the network [9]. This message contains the public address of the receiver and also a digital signature. When the data reaches the receiver, he will verify the data and this is kept in a block. Now the nodes which are presented in the network will validate this block by performing consensus methods like proof of work (POW) or proof of stake (POS) etc [12]. After performing these consensus activities, the block is attached to blockchain. Transactions are not valid until they are added to the blockchain.

There are mainly five characteristics of blockchain, (i) decentralized, (ii) distributed ledger (iii) anonymity (iv) immutability and (v) auditability as shown in Fig.4. These are described below.

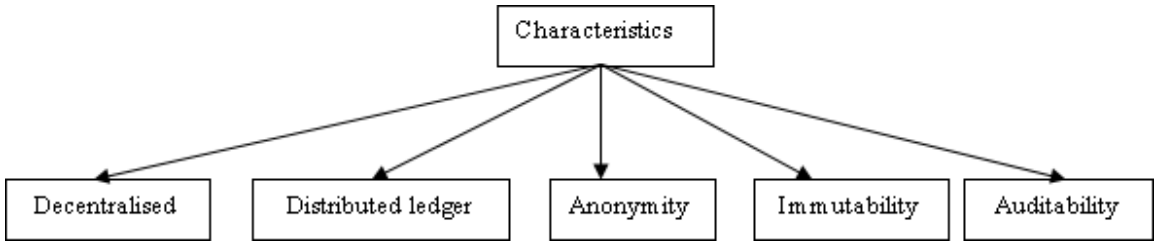

Fig 4: Characteristics of blockchain

(i) Decentralised: In centralised system [3] the total transactions are done using the central third party. But blockchain technology has decentralised nature. It does not depend on third party.

(ii) Distributed ledger: In order to add a new block to the blockchain, it is shared among all the existing nodes, that are present in that network [14].

(iii) Anonymity: The communication [15] in blockchain network is done using a generated identity or address [6]. In this blockchain technology the user will not use his original identity.

(iv) Immutability: Immutability is one of the important characteristics in blockchain. Information or data that is stored in blockchain is kept unchanged by using crypto techniques [9]. Any transactions in the blockchain network cannot be altered, if once they are added to the blockchain network [16, 17].

(v) Auditability: If any block is added to blockchain or if any transactions are performed in the blockchain network they are recorded by using a time stamp [6]. Hence if users want to see that particular block or transactions details [15] they can trace them easily and speedily by using this time stamp.

Blockchain is classified into three classes as shown in Fig.5. They are (i) Public blockchain, (ii) Private blockchain, (iii) Consortium blockchain.

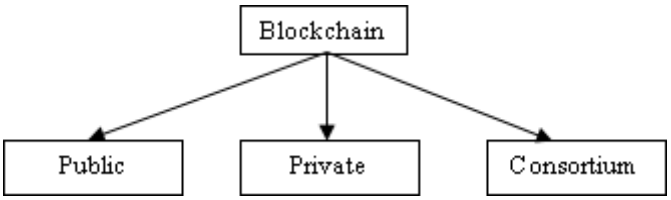

Fig 5: Types of blockchain

(i) Public blockchain is open to all the public users. If we want to access this type of blockchain we can access it very easily without having any kind of permissions [18]. Anyone can download the code or software tool and run this on their device for doing transactions in the peer to peer network [16]. Any person can join this type of blockchain and can have read and write permissions. If we are connected to this blockchain we can access this blockchain from anywhere in this world. Bitcoin [13], and Ethereum, monero [19] are examples of this type of chain.

(ii) Private blockchain is kept restricted by a particular company or community who is using it [9]. This type of chain is maintained or controlled by one single central authority. All the permissions are kept within the hand of particular company who is controlling this blockchain. Hyper ledger [13], bankchain, ripple are the main examples of this type of private chain.

(iii) Consortium blockchain is a mixture of both public and private blockchain. In this type of chain instead of single authority taking the total decision, the decisions are taken by some pre-defined authorities [18]. The validation of a block is done by many nodes but the confirmation is done by some pre-selected nodes only. As it is validated by everyone it had public blockchain characteristics and while confirmation is done by some pre-defined nodes it has the privates' chain characteristics. These types of chains are mostly used for enterprise use. Corda, hyper ledger [20] are the examples of this type of consortium blockchain.

To add a new block to existing blockchain the user should satisfy some consensus. If these consensus mechanisms are performed correctly, then the block can be added to the chain. Fig.6 shows various types of blockchain consensus mechanisms. A consensus mechanism is some sort of agreement between all the nodes present in the blockchain network for creating trustful environment [6] in the network. Because of its many good features the blockchain technology is applied in many fields like education, IOT, business, financial sector, medical, voting etc [21].

Now a days many consensus mechanisms are being used in blockchain technology. They are divided in two types. (i) Permission less consensus and (ii) Permissioned consensus. Proof of work (PoW), proof of stake (PoS), Proof of Burn (PoB), Proof of Elapsed Time (PoET) comes under permission less consensus and, Byzantine fault tolerance (BFT), Practical Byzantine Fault Tolerance (PBFT), Paxos, Raft comes under permission consensus.

(i) PoW: This is the earliest and first consensus method used in blockchain technology for providing security in blockchain network and for adding an authorised block to the chain. In this method user has to prove himself by solving some mathematical puzzle [22]. To solve this mathematical puzzle a target value will be set before. If the users solve these puzzles and reach that particular target, then he can add a new block to the blockchain. This puzzle goes on changing all the time. But this is a long time taking and resource consuming process. This consensus mechanism is firstly used in Bitcoin [23].

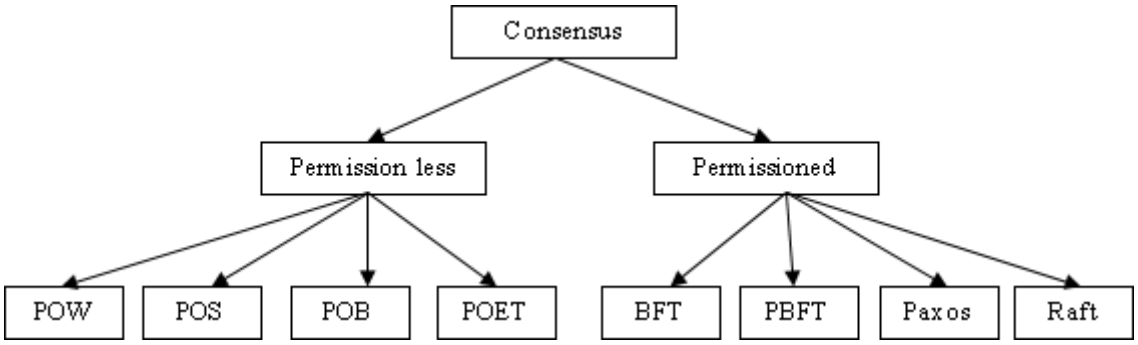

Fig 6: Blockchain consensuses

(ii) PoS: This consensus was started in 2011. As lot of time and resources are being consumed in PoS consensus [24], to solve this problem PoS is designed [25]. In this method the users are validated based on the particular amount of stake they are having [26]. The node with more stakes is given more importance in this method. This consensus also has some drawback. As the node with more stake is given more importance to validate a block and also becomes more ruling node in the network which sometimes cause inequitable distribution in the network. PoS consensus can be more vulnerable to attacks [6]. Ethereum uses PoS consensus mechanism [27].

(iii) PoB: In this consensus the participants need to burn some coins by transferring them to an eater address, which is an irretrievable address. This address will have a public key and will not have a private key. The coins which are sent to this eater address are abolished from the network which can't be used further. Due to this process the malicious users will get discouraged to mine an invalid block because they have to burn the coins [5]. In this process as the validation of block depends on burning the coins. It causes unnecessary resources wastage [11].

(iv) PoET: Intel developed this consensus in 2016. This consensus is based on trusted execution environment [29] and SGX which is abbreviated as Intel's Software Guard eXtensions. This SGX provides reliability and security by permitting applications to run important code in a trusted environment without allowing for any kind of modifications [5]. Each verifying node sleeps after producing a waiting time. The node which completes the waiting time first will win the chance to generate the block. This random waiting time is given by the code running in the trusted execution environment by utilising SGX. This algorithm prevents the more usage of networks computational power [11].

(v) PBFT: In this method all the nodes present in the network will select a particular node and they will make that node as the leader node. This leader node is like a primary node [27]. When this leader node gets the request, this node will notify the backup nodes about it and then wait for their respond. Which means any decision should depend on the majority of the votes which are present in that network [6]. Based on this the leader node will decide the validity of a block, along with the acceptance of two third nodes present in the network. Private Blockchain uses this consensus method [28].

(vi) Paxos: This consensus runs in three phases. First phase is the propose phase, next is the accept phase and the third is the commit phase. In the propose phase, a node in the network will try to become the leader node by proposing unique ballot number for its followers. The follower nodes accept the leader nodes based on the highest ballot number seen so far or they can reject ballot greater than ballot number. By receiving one rejection the node will come to know that there is other leader node with high ballot number reaching to the participants. After a node becomes a leader node it goes to the second phase. In this second phase the leader node will choose a value for this ballot. This value can be any new value or it depends on the highest ballot number in the previous stage phase. Now this leader node will send this value to the follower nodes and majority of the followers should accept this if not the leader node is cancelled and it is again sent to the first stage. If the leader node is accepted it is sent to the third phase. In this stage this leader node sends a commit message that allows the follower nodes to commit and apply the value to their state machines [30].

(vii) Raft: As per Yang's [31] view this consensus was proposed by Ongaro and Ousterhout. This consensus is used mostly for private blockchain [32], and also used in Quorum which is a blockchain development platform [5]. All the nodes this raft consensus will always be in any of three states: One is the leader phase, second is the follower phase and third is the candidate phase. In Raft time is partitioned into terms with a limited duration and these terms are assigned with consecutive numbers. All the terms start with an election process to become a leader.

If the node gets selected in this election process then that node is made as a leader node for that term. Next is the follower state. This follower node becomes candidate node if he doesn't listen for the leader node. Again to become leader this candidate node will request votes from other nodes. In this consensus there will be one leader node and others are follower nodes. The follower node periodically gets heartbeat message from the leader node for the authority purpose. During this term all the transactions goes through leader. These transactions are added to an entry. If the leader node receives transaction it is sent to the follower nodes. Leader will wait until he receives feedback from the follower nodes and accept the transactions [32].

2. Applications of blockchain

Blockchain allows us to do transactions among the nodes. The transacted things can be anything like currency, votes etc [33]. As depicted in Fig.7 the various applications of blockchain are, (i) Bitcoin, (ii) Health care management (iii) Education (iv) Voting (v) Internet of Things (IoT), and (vi) Business [34].

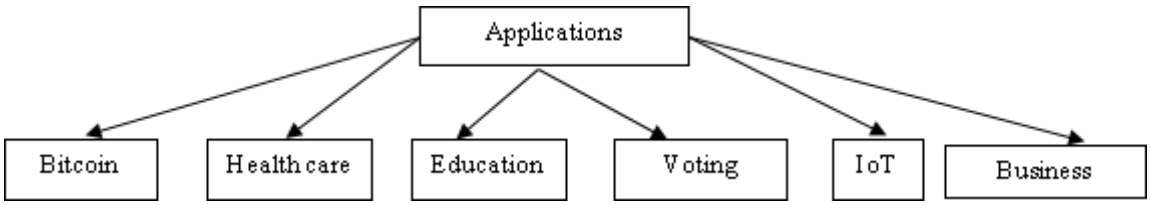

Fig 7: Applications of blockchain

2.1 Bitcoin

This is the earliest application for using this blockchain technology and was founded in 2009 as open source software [35]. It's a form of crypto currency which uses peer to peer technology and has anonymity character. This is operated in a decentralised way. Instead of normal cash some coins named bit coins are used for transactions [23]. The value of these coins varies all the time like share market. A lot of transactions will take place in this Bitcoin without using the bank [20]. It eliminates the need of third party. All the transactions took place in this Bitcoin are stored using this blockchain technology. As blockchain has the features of consensus (agreements between nodes) this feature mainly made this blockchain technology to use in Bitcoin. Bitcoin uses PoW consensus to add a user block to the blockchain and do transactions in Bitcoin.

2.2 Health care management

Blockchain technology plays a vital role in this health care sector. All the information related to the patient's data is stored using blockchain technology in a secured way [36]. It also provides the facilities like doctor connecting to the patient through online [37], providing e- health facility [38], storing the health claim issues etc. It is also used for tracing the drugs because drug counterfeiting is creating a big problem in the medical industry [6]. Many reports from health organisations say that medicines sold in some countries have counterfeited. These drugs can cause danger to the patient's health. Blockchain solves this problem. As blockchain has distributed, immutable, and time stamped features, these features provide the facilities to trace a product and make the date tamper proof [6].

2.3 Education

In education field blockchain technology is used to store huge amount of details related to educational fields like student's certificates details [37], fees details, collaborative learning environment. We can also store infrastructure details like cc camera footage details, teachers and students attendance details. Many schools like university of Nicosia [39] had already started using this blockchain technology. Software named Blockcert is started by Media lab in MIT University, this is used mainly for issuing certificates. Blockchain technology also allows many institutions to verify student certificates in a secure way [40]. Even Sony global education, and Wooly University is also using this blockchain technology.

2.4 Voting

Voting is a process done by a group of people to express their decisions in the election process. But this voting systems, lack security and transparency. Blockchain technology became a solution to this problems. The present voting process is based on ballots system which is a lot of time-consuming process because these ballots are to be gathered from all the places and then they need to be controlled, maintained and counted by a centralised administration. In this process the voters have no guarantee about their votes were added in the results or they were tampered and also there are some problems like tampering the voting machines and also single person

put votes many times in different places etc are the major problems occurring in many places. Furthermore, in the existing election process the expenditure is very high and a time-consuming process. These problems can be solved by e-voting system. Although in e-voting system the results can be declared fast, to some extent it reduces frauds by decreasing the human involvement, reducing the cost, but it lack the transparency and trust [41]. By using this blockchain technology we can solve this problem. The immutable, audit ability nature of blockchain made to use this technology in voting process [42]. If once voter's data is stored using this blockchain technology no one can tamper the data. For maximum extent we can stop fraud things like vote tampering etc. Some countries already started using blockchain technology for voting purpose.

2.5 IoT

Now a day's iot technology is playing an important role in over daily lives. Many applications like smart homes, smart cars, smart cities [27, 38], smart iot agriculture techniques etc are the examples of iot devices. As iot is a network connection of several devices [43] that can sense, store, transfer data without human interaction a lot of information is stored in these devices. But many applications of iot are based on the centralised party which cause a lot of damage if they are misused [44]. Hence by using this blockchain technology in iot we can make it as decentralised party and also can store a large amount of data in an immutable way.

2.6 Business and industry

Blockchain plays a significant role in business, and industrial fields. In business field there is always a confusion regarding the data security. Blockchain becomes a solution to this problem. In business and industrial fields blockchain technology is used for storing huge amounts of data and for performing secured transactions [45]. If once the data is added to the block no one can alter it. So, if a single person wants to change any kind of data, he cannot do it. We can also store employees and workers data, stock trading details, supply chain details, insurance matters, financial details etc in the blocks.

In addition to these, blockchain applications can also be used in real estate to store the land details, land property details, brokers details, [18], manufacturing [44], logistics and transport [44], [45], integrity verifications to store the data about products details like their manufacturing details, their life time details, their services [37], supply chain management [37], [1], [29], agriculture and food [45], robotic industry [45], digital identity [47] etc are the sectors in which blockchain technology applications are used.

3. Challenges

As shown in Fig.8, there are mainly 4 kinds of challenges in blockchain, (i) attacks, (ii) scalability, (iii) energy consumption, and (iv) awareness.

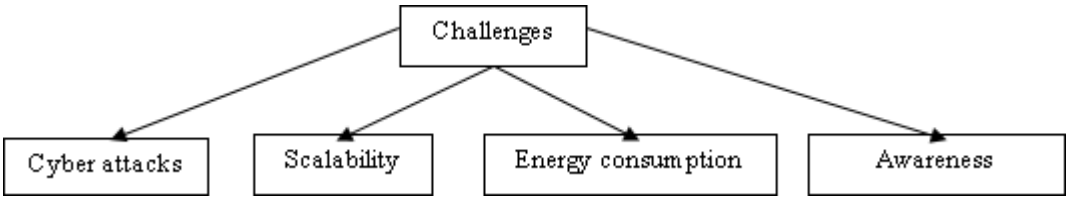

Fig 8: Blockchain challenges

(i) A**ttacks:** An attack is a kind of threat that is performed for altering or destroying the data, or for obtaining the confidential information which is present in the network without having the owner permissions. Due to the anonymous nature of blockchain technology this is mostly prone to various attacks [46] like Distributed Denial of Service (DDoS) [48], 51% attack [49], and selfish mining attacks.

(ii) Scalability: This problem is the major challenge in blockchain technology. In the recent days the people using this blockchain technology has been increased highly. Hence this blockchain technology should support many users [21]. When many people are using this for doing transactions the performance of blockchain is becoming slow down [45]. Hence the scalability should is a concern.

(iii) Energy consumption: As blockchain uses the consensus mechanisms like Pow, huge amount of power is needed. [50]

(iv) Awareness and adoption: When compared to other technologies, still there is confusion among many people about the working of blockchain, how data transactions are done using blockchain and also how consensus is used in the blockchain technology [48].

4. Blockchain attacks

An attack is a kind of threat that is performed on computer networks. These attacks are done for altering or, destroying the data, or for obtaining the confidential information which is present in the network without having the owner permissions.

As depicted in Fig.9, the various blockchain attacks are, (i) 51 %, (ii) DDoS, (iii) selfish mining attacks, (iv) eclipse attack, (v) double spending attack, (vi) sybil attack and (vii) phishing attack. Since its birth till now there is less research is being done on these attacks issues.

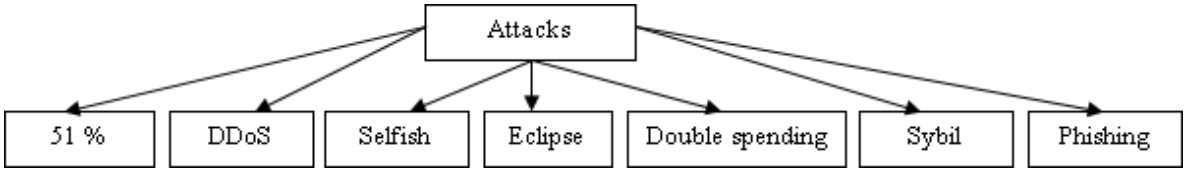

Fig 9: various types of attacks on blockchain

4.1 The 51% attack

This attack is done by the miners who are having more than fifty percent of computing resources when compared to other nodes. If this 51% attack is implemented in blockchain the attacker can control the blockchain by influencing the verification process, transactions and can also control mining power. Here the miner who is performing this attack can be a single person or it can be a group of persons. The plan or strategy of this 51 % attack differs or changes based upon the different consensus being used [22]. But this is mostly done in PoW consensus mechanism when compared to other consensus mechanisms. This attack is also called as majority attack [51]. This attack is mostly seen in crypto currency like Bitcoin [52]. If this attack is done on blockchain technology based crypto currencies the attackers can control the mining hash rate [53], and can stop the new transactions being confirmed.

4.2 The DDos attack

This is a kind of cyber-attack [51] which confuses and floods the total network or a single node with more amount of traffic by sending continuous multiple requests. Due to this the resources [22] present in the network will not be properly accessed by the users who are present in the network and also the targeted node goes offline [17] for some time due to the overload on it [54]. This attack can target the total network or only a node in it. If the attacker targets a specific node, then it continuously sends many requests [55] to that specific node. As a result, the victim node is overwhelmed and does not accept genuine requests in the network. In blockchain technology if this attack is done the total network gets struck up and sometimes it becomes invalid for transactions to be performed. Recently in github [56] website this attack has been identified. In blockchain technology this attack is done on crypto currency which uses blockchain technology like Bitcoin. This attack occurs on the mempool also known as memory pools (it's a location that stores all the transactions that are not confirmed in the network) [57] of Bitcoin.

4.3 The Selfish mining attack

This attack is a kind of malicious attack. Saad et al says [58] this attack was first identified by Eyal and Sirer. If this attack occurs in blockchain it disrepute the total networks integrity. In this attack selfish miner node will withhold a mined block that is successfully confirmed from being send to the rest of the network. Later they start to mine the next block and create their own private chain. Then this private chain looks longer [15] than the particular public blockchain and all the miners will try to add their block to this chain thinking this as a genuine chain which will waste the genuine miners computational powers [59] and resources [60]. Hence by doing this kind of mining the selfish miners will get more rewards. This attack can be performed by miners or mining pools which consists of huge network hash [22].The selfish miners can also stop other mining blocks from getting rewards because if the selfish miner chain becomes long the new joining nodes will be added to this selfish miners chain due to this these selfish miners get more amount of rewards. As the selfish miner in this attack withholds the block from being broadcasted this attack is also called as block withholding attack [61].

4.4 The Eclipse attack

In this attack a group of malevolent nodes detach its neighbour nodes by using their IP address and control their outgoing and incoming traffic [28]. In blockchain network all the nodes are connected to each other. Each and every node is aware of all the nodes IP address. This attack will isolate the truthful node and will control its outgoing and incoming traffic and also fill them with fake data and it can also block that node [54].

4.5 The Double spending attack

Double spending attack is a type of attack in which the attacker spends same amount [62] twice at a time. In physical terms this type of attack is impossible [61]. In this process the attacker will send a transaction and he will wait until the merchant accept it and release the goods. Now the attacker will block the communication with merchant [63] or reverse it and again the attacker will put that amount in other transaction. A solution named recipient-oriented transaction [64] is founded to stop this double spending attack.

4.6 The Sybil attack

This attack was bought to attention by John Douceur. In this attack the adversary will develop a huge amount of fake nodes that appear to be genuine in the network which causes disturbance and confusion [54] in the total network. These fake nodes alter the transactions or validate unauthorised transactions [22] or misguide the network opinion. If many nodes are controlled by attacker this attack becomes difficult to identify [51]. In blockchain this attack can be avoided by using the consensus properly [61]. This attack occurs more in peer to peer networks [65].

4.7 The Phishing attack

This attack is done to know the user's important details like user names, their important key passwords etc [66] for performing malicious activities. The security policies of projects using blockchain technology also became helpless for these phishing attacks and also many of the blockchain members lost their money because of this phishing attack. Many tools and methods were founded to prevent this attack. But no tool provides hundred percent securities [66].

5. Conclusion

In this paper, we explained about different characteristics, types, consensus mechanisms, and challenges of blockchain along with various major attacks like DDoS attack, 51% attacks, Selfish mining attack, Eclipse attack, double spending attack, Sybil attack and Phishing attack. As blockchain consensus mechanism are good and resistant to attacks for some level, but there is still possibility for attacks to take place and many attacks are also being happened. In the future work, we aim to solve these attacks and develop solutions for those attacks.

References

1. Y. Li, Emerging blockchain-based applications and techniques, Service Oriented Computing and Applications, 13, pp. 279- 285, 2019.
2. R. Thakore, R. Vaghashiya, C. Patel, N. Doshi, Blockchain - based IoT: A Survey, Procedia Computer Science, 155, pp.704-709, 2019.
3. Ahmed, Shilpi, M. Amjad, Blockchain technology a literature survey, International Research Journal of Engineering and Technology, 5(10), pp. 1490-1493, 2018.
4. N. Elisa , L. Yang, F. Chao, Y. Cao, A framework of blockchain-based secure and privacy-preserving E-government system, Wireless Networks, 2018, https://doi.org/10.1007/s11276-018-1883-0
5. L. Ismail, and H. Materwala, A review of blockchain architecture and consensus protocols: use cases, challenges, and solutions, Symmetry, 11(1198), pp. 1-47, 2019.
6. A.Monrat, O. Schelen, K. Andersson, A survey of blockchain from the perspectives of applications, challenges, and opportunities, IEEE Access, 7, pp. 117134-117151, 2019.
7. Aruna., A. A. Prakash, M. S. Srinija, Security analysis on blockchain using the Ecc and Sha algorithms, International Journal of Innovative Technologies and Exploring Engineering, 8(8), pp.1966-2001, 2019.
8. M. Poluri, A. Kumar, S. Allam, K.V.D. Kiran, IOT Ecosystem with Blockchain and Smart Contracts, International Journal of Recent Technology and Engineering, 7(6s), pp. 638-647, 2019.

9. Y. Perwej, A pervasive review of blockchain technology and its potential applications, Open Science Journal of Electrical and Electronic Engineering, 5(4), pp. 30-43, 2018.
10. Satya AR, B.G. Banik, A comprehensive study of Blockchain Services: Future of Cryptography, International journal of Advanced Computer Science and Applications, 11(10), pp. 279-288, 2020.
11. M. Andoni, V, Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, A. Peacock, Blockchain technology in the energy sector: A systematic review of challenges and opportunities, Renewable and Sustainable Energy Reviews, 100, pp. 143-174, 2019.
12. P. Joshi, M. Han, Y. Wang, A survey on security and privacy issues of blockchain technology, Mathematical Foundations of Computing, 1(2), pp.121–147, 2018.
13. Tandon, An empirical analysis of using blockchain technology with internet of things and its application, International Journal of Innovative Technology and Exploring Engineering, 8(9S3), pp. 1469-1475, 2019.
14. R. Chatterjee, R. Chatterjee, An overview of the emerging technology: blockchain, International Conference on Computational Intelligence and Networks, pp. 126-127, 2017.
15. Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of block chain technology: archicture, consensus, and future trends, IEEE International Congress on Big Data, pp. 557-564, 2017.
16. D. Madavi, A comprehensive study on blockchain technology, International Research Journal of Engineering and Technology, 6(1), pp. 1765- 1770, 2019.
17. J. Moubarak , E. Filiol , M. Chamoun, On blockchain security and relevant attacks, IEEE Middle East and North Africa Communications Conference, pp. 1-6, 2018.
18. D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, G. Das, Everything you wanted to know about the blockchain: its promise, components, processes, and problems, IEEE Consumer Electronics Magazine, 7(4), pp. 6-14, 2018.
19. P. Tejaswi, P. Nikitha, A. Vijaya Kumar, An Efficient Blockchain Security for Distributed Systems, International Journal of Innovative Technologies and Exploring Engineering, 8(6), pp. 1265-1269, 2019.
20. I.-C. Lin, T.-C. Liao, A survey of blockchain security issues and challenges, International Journal of Network Security, 19(5), pp. 653-659, 2017.
21. M. Niranjanamurthy, B.N. Nithya, S. Jagannatha, Analysis of blockchain technology: pros, cons and SWOT, Cluster Computing, 22, pp. 14753-14757, 2018.
22. S. Sayeed, H. Marco-Gisbert, Assessing blockchain consensus and security mechanisms against the 51% attack, Applied Sciences, 9(1788), pp. 1-17, 2019.
23. M. Rahouti, K. Xiong, N. Ghani, Bitcoin concepts, threats, and machine-learning security solutions, IEEE Access, 6, pp. 67189-67205, 2018.
24. N.S. Tinu, A survey on blockchain technology- taxonomy, consensus algorithms and applications, International Journal of Computer Sciences and Engineering, 6(5), pp.691-696, 2018.
25. M. Sinha, Block-Chain: Survey on privacy, security and challenges, International journal of computer engineering and applications, 8(2), pp. 6-12, 2019.
26. T. Nguyen, D. T. Hoang , D. N. Nguyen , D. Niyato , H. T. Nguyen , E. Dutkiewicz, Proof-of-Stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities, IEEE Access, 7, pp. 85727 – 85745, 2019.
27. S. T. Aras, V. Kulkarni, Blockchain and its applications- a detailed survey, International Journal of Computer Applications, 180(3), pp. 29-35, 2017.
28. M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, and A. Mohaisen, Exploring the Attack Surface of Blockchain: A Systematic Overview, arxiv:1904.03487v1 [cs.CR], pp: 1- 30, 2019.
29. T. A. Syed, S. Jan, M. S. Siddiqui, A. Naddem, T. Alghamdi, A comparative analysis of blockchain architecture and its applications: problems and recommendations, IEEE Access, 7, pp. 176838 – 176869, 2019.
30. Charapko, A. Ailijiang, M. Demirbas, Bridging Paxos and blockchain consensus, IEEE International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data, 2018, pp. 1545-1552.

31. F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, M. Zhou, Delegated proof of stake with downgrade: a secure and efficient blockchain consensus algorithm with downgrade mechanism, IEEE Access, 7, pp. 118541- 118555, 2019.
32. Huang, X. Ma, S. Zhang, Performance analysis of the Raft consensus algorithm for private blockchains, IEEE Transactions on Systems, Man, and Cybernetics: Systems, 50(1), pp.172-181, 2020.
33. M. Parssinen, M. Kotila , R. C. Rumin , A. Phansalkar , J. Manner, Is blockchain ready to revolutionize online advertising?, IEEE Access, 6, pp.54884-54899, 2018.
34. K. Zile, R. Strazdina, Blockchain use cases and their feasibility, Applied Computer Systems, 23(1), pp. 12–20, 2018.
35. S. Singh, N. Singh, Blockchain: future of financial and cyber security, 2nd International Conference on Contemporary Computing and Informatics, pp. 463-467, 2016.
36. P. Tasatanattakool, C. Techapanupreeda, Blockchain: challenges and applications, International Conference on Information Networking, pp. 473-475, 2018.
37. F. Casino, T. K. Dasaklis, C. Patsakis, A systematic literature review of blockchain-based applications: current status, classification and open issues, Telematics and Informatics, pp. 55-81, 2019.
38. Reyna, C. Martin, J. Chen, E. Soler, M. Diaz, On blockchain and its integration with IoT, Challenges and opportunities, Future Generation Computer Systems, 88, pp. 173-190, 2018.
39. G. Chen, B. Xu, M. Lu, N.-S. Chen, Exploring blockchain technology and its potential applications for education, Smart Learning Environments, 5(1), pp.1-10, 2018.
40. S. M. K. V Pramod Kumar, P. Kiran Kumar, R. Sai Krishna, P.S. G. Aruna Sri, Incorporation of Blockchain in Student Management System, International Journal of Innovative Technologies and Exploring Engineering, 8(6), pp. 664-668, 2019.
41. M. Pawlak, A. Poniszewska-Maranda, N. Kryvinska, Towards the intelligent agents for blockchain e-voting system, Procedia Computer Science, 141, pp. 239-246, 2018.
42. P. Yellamma, P. Anupama, K. Lakshmibhavani, U. Jhansi Siva Priya, Ch, Kazalalitha, Implimentation of E- Voting System Using Blockchain Technology, Journal of Critical Reviews, 7(6), 865-870, 2020.
43. N. Satheesh, G. R. Koteswara Rao, S. Chowdhury, K. P. Prakash, S. Sengan, Blockchain – Facilitated IoT Built Cleverer Home with Unrestricted Validation Arragment, International Journal of Advanced Trends in Computer Science and Engineeering, pp.5398-5405, 2020.
44. N. M. Kumar, P. K. Mallick, Blockchain technology for security issues and challenges in IoT, Procedia Computer Science, 132, pp.1815-1823, 2018.
45. J. Al-Jarooodi, N. Mohamed, Blockchain in industries: a survey, IEEE Access, 7, pp.36500-36515, 2019.
46. L. V. Kiran, R. B. Dinakar, P. S. Prasad, Blockchain technology-a sturdy protective shield, International Journal of Recent Technology and Engineering, 7(4), pp. 269-272, 2018.
47. P. S. G. Aruna Sri, D. L. Bhaskari, A study on blockchain technology, International Journal of Engineering and Technology, 7(2.7), pp.-418-421, 2018.
48. W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, J. Han, When intrusion detection meets blockchain technology: a review, IEEE Access, 6, pp: 10179 – 10188, 2018.
49. Meva, Issues and Challenges with blockchain: a Survey, International Journal of Computer Sciences and Engineering, 6(12), pp. 488-491.
50. Ammbika V. M, DS Rao, Limitations of Blockchain Technology with its Applications, International journal of Recent Technology and Engineering, 8(2S11), pp. 3646- 3652, 2019
51. S. Sayeed, H. Marco-Gisbert, On the effectiveness of blockchain against crypto currency attacks, The Twelfth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, pp.9-14, 2018.
52. J.J. Xu, Are blockchains immune to all malicious attacks?, Financial Innovation, 2(25), pp.1-9, 2016.
53. C. Ye, G. Li, H. Cai, Y. Gu, A. Fukuda, Analysis of security in blockchain: case study in 51%- attack detecting, 5th International conference on dependable systems and their applications, pp. 15-24, 2018.
54. N. Anita, M Vijayalakshmi, Blockchain security attack: a brief survey, 10th International Conference on Computing, Communication and Networking Technologies, pp. 1-6, 2019.
55. T. K. Kim, Analysis of spam transaction on the blockchain, International Journal of Engineering & Technology, 7 (3.34), pp. 551-553, 2018.

56. J. Dheeraj, S. Gurubharan, DDoS mitigation using blockchain, International Journal of Research in Engineering, Science and Management, 1(10), pp.622-626, 2018.
57. M. Saad , L. Njilla, C. Kamhoua, J. Kim, D. Nyang, A. Mohaisen, Mempool optimization for defending against DDoS attacks in PoW-based blockchain systems, IEEE International Conference on Blockchain and Cryptocurrency, pp. 285-292, 2019.
58. M. Saad, L. Njilla, C. Kamhoua, A. Mohaisen, Countering selfish mining in blockchains, 2019 Workshop on Computing, Networking and Communications, pp.1-5, 2018.
59. X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain systems, Future Generation Computer Systems, 107, pp. 841-853, 2020.
60. Kibet, S. M. Karume, A synopsis of blochchain technology, International Journal of Advanced Research in Computer Engineering & Technology, 7(11), pp.789-795, 2018.
61. Deirmentzoglou, G. Papakyriakopoulos, C. Patsakis, A survey on long–range attacks for proof of stake protocols, IEEE Access, 7, pp. 28712 - 28725, 2019.
62. N. Rathod, D. Motwani, Security threats on blockchain and its countermeasures, International Research Journal of Engineering and Technology, 5(11), pp.1636-1642, 2018.
63. Ramezan , C. Leung , Z. J. Wang, A strong adaptive, strategic double-spending attack on blockchains, 2018 IEEE Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics, pp. 1219-1227, 2018.
64. Lee, M. J. Shin, K. S. Kim, Y. Kang, J. Kim, Recipient-oriented transaction for preventing double spending attacks in private blockchain, 15th Annual IEEE International Conference on Sensing, Communication, and Networking, pp. 1-2, 2018.
65. D. Dasgupta, J. M. Shrein, K. D. Gupta, A survey of blockchain from security perspective, Journal of Banking and Financial Technology, 3, pp. 1-17, 2019.
66. A.A. Andryukhin, Phishing Attacks and preventions in blockchain based projects, International Conference on Engineering Technologies and Computer Science, pp. 15-19, 2019.