A REVIEW ON BLOCKCHAIN AND ITS SECURITY

B. Ramdasu and K Kiran Prakash

ABSTRACT

Blockchain is the latest buzzwords in the field of Computer Science since the past four years. It has the potential to completely take over the traditional Financial Institutions we know since the past century and bring about Web 3.0. In order to do this the technology has to be highly secure. To understand how and why blockchain is so secure and reliable we need to first understand how the different blocks are linked together in a Blockchain Network. The blocks in a blockchain are linked with the help of a Hashing Algorithm. A hashing algorithm is a one-way mathematical function which generates a unique output for every unique input. The Bitcoin Network uses a SHA-256 hash. A basic block has a data, hash and previous hash field. The hash value of any block is dependent on the hash value of the previous block, therefore making it very difficult to alter the data as any tampering would require altering hashes of each and every subsequent block in the blockchain. A typical blockchain network can have millions of blocks on its chain. This makes it virtually impossible to alter the blockchain, thereby making it so secure. Blockchain is a decentralized technology [14]. It has a lot of power when it comes to solving business difficulties. Algorithms on the nodes validate blockchain transactions. A transaction cannot be initiated by a single entity. Finally, blockchains ensure transparency by allowing each participant to view transactions at any moment. Smart contracts ensure safe transactions, reducing the risk of third-party interruption. Decentralization and immutability are two key characteristics of blockchain. Faster transactions, transaction and validation in seconds, and so forth.

Index Terms: *Blockchain, cryptocurrency, hash, blocks, faster transaction.*

Reference *to this paper should be made as follows: B. Ramdasu and K Kiran Prakash, (2022), "A Review on Blockchain and Its Security", Int. J. Electronics Engineering and Applications, Vol. 10, No. 2, pp. 13-22.*

Biographical notes:

B. Ramdasu *is working as an assistant professor in the Department of Computer science and engineering for last 15 years. He has done his M.Tech in Computer Science and Engineering from Osmania University.*

K Kiran Prakash *is working as an assistant professor in the Department of Computer science and engineering for last 5 years.*

Published by: International Associations of Professionals and Technical Teachers (IAPATT)

I. INTRODUCTION

Blockchain has come a long way since it was first introduced in the 2008 white paper by Satoshi Nakamoto with Bitcoin. Although many people confuse Bitcoin with Blockchain the best way to think about it is that Bitcoin, a cryptocurrency was the first application of Blockchain Technology. Blockchain and Cryptocurrency are the most sought-after technology in this era of Computer Science. Other than Cryptocurrency some of the existing applications using Blockchain which are gaining popularity are –.

Crowdfunding Platform
In the last few years, crowdfunding has emerged as an alternative source of funding for various types of projects. Crowdfunding is seen as a way to reduce the funding gap in the early stage of new ventures. Funding from venture capitalists and banks is usually available only in the later development phases of start-ups [12]. The major issue of regular funding is no back transactions which can be solved by funding through blockchain.

Decentralized Voting System – Some of the problems that can occur in traditional electoral systems is with an organization that has full control over the database and system, it is possible to tamper with the database of considerable opportunities [13]. Blockchain, due to being very secure can eliminate this problem.

It has the potential to radically alter transactions, security, supply chain and other areas. Web 3.0 is possible because of this technology. Many new concepts such as NFTs (Non-Fungible Tokens), Metaverse, Cryptocurrency, etc. are based on the Blockchain Technology. It's estimated that Blockchain will generate $3.1 trillion in new business value by 2030 [8]. For the majority of time till now traditional Financial Institutions have been the central authority for managing financial transactions between two or more parties. The value of any currency is controlled by the Government of the Country. This model is also known as the Client-Server Architecture.

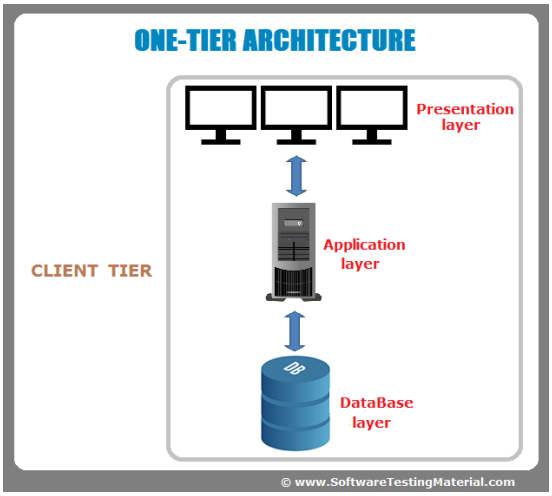

Fig 1: One Tier Client/Server Architecture [8]

One of the problems with this type of architecture is that there is a “single point of failure”, i.e., if this server is taken down due to any reason, it jeopardizes the data of all the Clients dependent on this system. The servers are often quite expensive to setup and require skilled expertise [1]. These problems can be solved using a Decentralized Architecture which is the backbone of a Blockchain Network. Large-scale distributed computing environments provide a vast amount of heterogeneous computing resources from different sources for resource sharing and distributed computing [2]. This shifts power from the Central Authority to all the peers of the network. While the Client-Server Architecture requires that all users trust in the Central Authority, a decentralized network is based on the ‘trust no one’ model.

2. DECENTRALIZED ARCHITECTURE

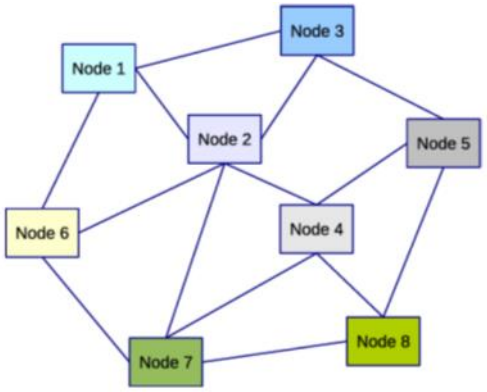

Fig 2: Decentralized Architecture

The blockchain may be defined as an application that runs on a distributed network. It is a decentralized transaction system which is transparent in the sense that any node handling blockchain software is capable of handling the entire blockchain. The corresponding data is stored in either a flat file or a relational database [3]. However, this also leads to redundancy of data storage as it stores the same data multiple times.

The Blockchain used for cryptocurrency is generally a Public Blockchain. A consensus mechanism is responsible for the decision-making process in the blockchain. Either proof-of-work (POW) or proof-of-stake (POS) is used to validate the transactions in a Blockchain Network by miners. A local copy of the transaction ledger is stored on each node(peer) part of the blockchain which ensures security and makes tampering with the blockchain virtually impossible as a hacker would have to go and alter the data on each and every node on the network. Typically, the number of nodes can be in millions

3. STRUCTURE OF A BLOCK

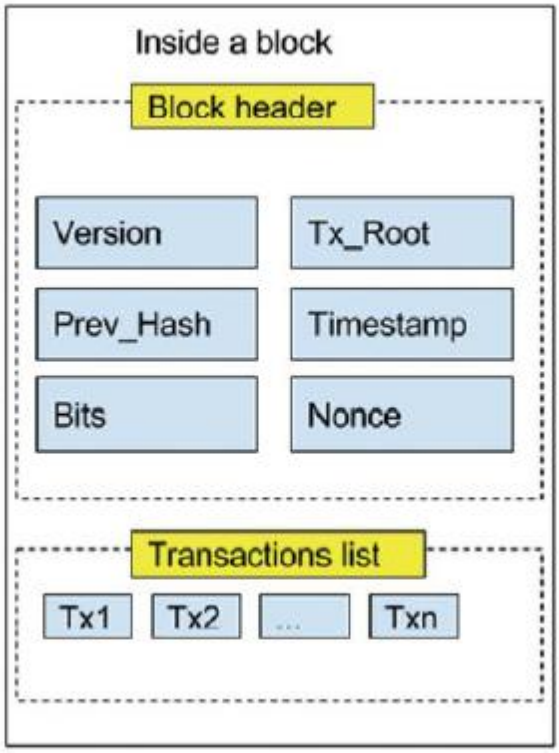

Fig 3 : The fields inside a block [7]

Blocks are part of blockchain which bunch a group of transactions and distribute them on the blockchain network. Every block consists of metadata and transactions placed by the miners. This metadata is used for verification by the nodes. Besides the list of transactions contained inside the block, the block contains some fields in the block header,

- Prev_Hash: this field can be known as reference to parents, which is a link of a block to its previous one in the chain.
- Timestamp: the time when the block was found.
- Tx_Root: this field, which is also known as the Merkle root, contains the hash value of all validated transactions of the block.
- Version: this field contains the protocol version used by the node proposing the block to the chain.
- Nonce: this field is used in PoW, which proves the efforts that a node has paid for getting the right to append this block to the chain. It is an abbreviation for 'number used once'.
- Bits: this field indicates the difficulty level of the PoW [7].

4. LINKING BLOCKS IN A BLOCKCHAIN

Blocks in a blockchain are linked together by the means of a hashing algorithm. Essential components of the block which are used in the linking process are–

- data – information stored on the block
- previous hash – hashing information of the previous block

- hash – hashing information of current block generated using “data” and “previous hash”

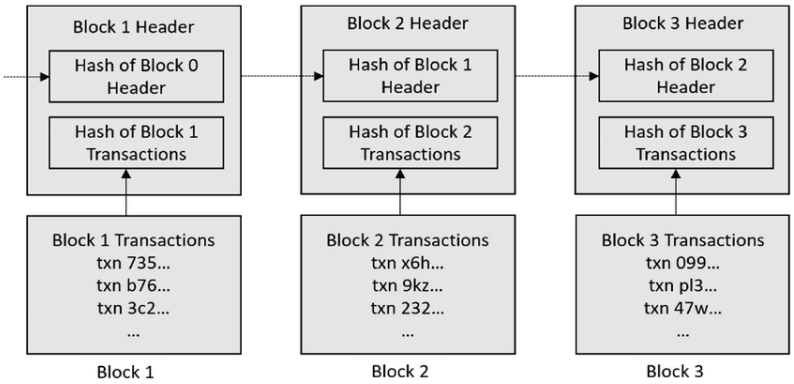

Fig 4 : Blocks in a Blockchain [5]

Every block should have the above components to be part of the blockchain network. One common question here would be what about the first block of the blockchain? It cannot possibly have a previous hash value. The first block of a network is a special block in which all the values are Hard Coded. This block is called the “Genesis Block”.

The hashing functions are special mathematical functions that are one-way i.e. the value of the input of a hash function cannot be determined with its output. This is what makes it so valuable. Digital Signature of an Account Holder is generated using the private key of that holder and with the hash function it can be ensured that the private key is not exposed. Another important property of hash functions is that for every unique input there is a unique output. This is necessary so that two accounts don’t generate the same digital signature. Even the smallest change in the input must provide an entirely different result [4]. Basically, hashing is the process of taking some readable information and converting to something that makes no sense at all [4].

An example of a popular hashing algorithm would be SHA(Secure Hash Algorithm). It is a group of cryptographic hash functions published by the NIST(National Institute of Science and Technology) [6]. In the Bitcoin system, SHA-256 Hashing algorithm is used. This algorithm always gives a 256-bit number which is represented using the hexadecimal number system.

A hash value is generated for a block using the block’s current data, nonce and the previous block’s hash. If a hacker tries to alter the data on any particular block, its hash value is altered due to the nature of hash functions. This changes the hash value of the next block as its hash is dependent on the previous block’s hash value and so on. So in order to tamper any data the entire blockchain has to be mined again which is nearly impossible on a network with millions of nodes. This is the primary reason why blockchain is such a secure technology. Even if a hacker manages to alter all the blocks, he will only be able to do so on a single copy. The decentralized nature of blockchain stores a copy on each and every node that is a part of the blockchain network. The state of that particular copy then becomes inconsistent with all copies present in the global network. This adds an additional layer of security making tampering/altering transaction data truly impossible. This is the reason Blockchain is said to be such a revolutionary technology.

Finally, the blocks are created or linked on the network using the Consensus Protocol. One of the nodes validates the transaction on the network and creates a block using a well-defined process that is dictated by the blockchain protocol. The other nodes reach a consensus on whether to include the block in the chain or reject it. This way of block creation and validation secures the network. Both Bitcoin and Ethereum currently use the Proof of Work consensus protocol. A brief description of the two most popular consensus algorithms –

Proof-of-Work(PoW) is a consensus algorithm used in permissionless Bitcoin network. PoW proves to the network server that some computational work has been performed by the nodes in the network. The network server gives problems such as Hash sequences, computational puzzles or other mathematical problems to be solved by the nodes in the network [10].

Proof-of-Stake(PoS) was conceptualized to address the issues of PoW and implemented in many systems including the Ethereum platform. In PoS, a validator can mint/forge a block or verify transactions according to the stake he puts in the network. If a validator confirms a fraud transaction, he may lose his stake in the network [10].

The mining process is incentivized to keep the network running. The account or node that validates the transaction and creates a block gets rewarded. Incentives are dictated by the protocol. Generally the reward is in the form of a fixed number of tokens and the associated transaction fee.

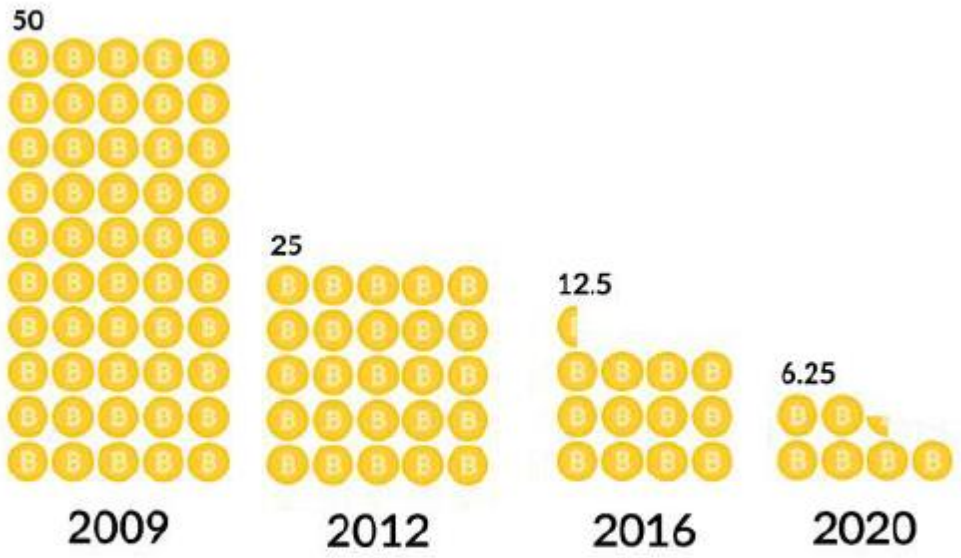

Fig 5 : Rewards for Bitcoin Mining overtime

4. DESIGN OF MODULAR MULTIPLIER

The above figure shows that the rewards for Bitcoin mining are halving every few years. On a higher level the Proof of Work generation requires to solve a mathematical puzzle. This puzzle can only be solved by either guesswork or brute force method. The first miner to find the solution validates the block and earns the reward. The difficulty in solving the puzzle i.e., the computing power required is not fixed for every block and may change. This is done to maintain a uniform average time

5. GENERATING A VALID HASH

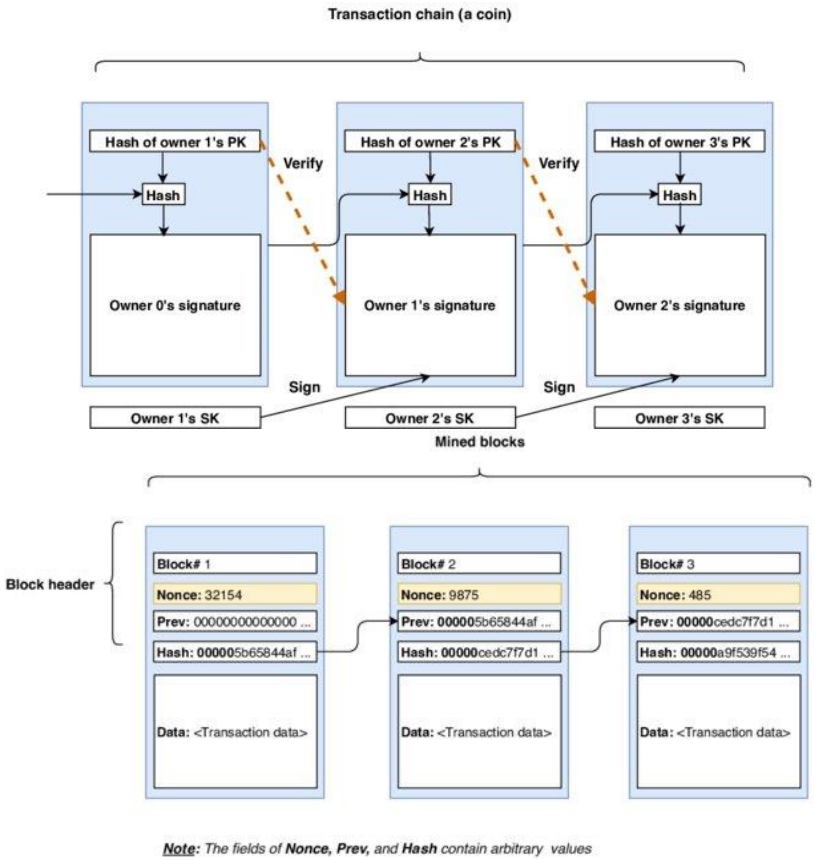

Fig 6 : Mined blocks in a blockchain. Signature is five leading zeros

We have seen in the previous section how a hash is generated to link blocks together. We however, have not yet defined when a hash is valid/invalid. On the Ethereum Blockchain in particular a hash is considered to be valid if it's value falls below a particular predefined value. The algorithm keeps altering the nonce of the block till that particular value is reached. In a 256 bit hash for example, if the value is 10,000, a nonce which generates a hash with value lesser than or equal to 10,000 for a particular data will be valid. The smaller the value chosen the longer it will take to generate the required nonce value i.e. mine the transaction.

Data	Nonce	Output Hash	Output Hash Base 10	Less than 10000?
"Hello"	0	A23042B2	2721071794	No
"Hello"	1	0BBF1491	197072017	No
"Hello"	2	0CE24258	216154712	No
"Hello"	3	0EEEEEEE	250539758	No
"Hello"	4	00014481	83073	No
"Hello"	5	00000AE1	2785	Yes

Table : Iterations to validate hash

After the hash of the block is validated, the block can be added to the Blockchain Network

6. **CONCLUSION**

The aim of this paper was to demonstrate the basic idea of the process of linking of blocks in the blockchain. Additionally, the benefits of blockchain technology i.e., a decentralized technology over traditional centralized architecture is outlined. The importance of hash function and its properties are explained. Example of popularly used hash function is given. The role of the mining process used to validate the hash for a block of a given list of transactions is analyzed. How to check whether a hash is valid or not is also explored. The different consensus protocols used to validate blocks on the Blockchain Network such as the PoW(Proof of Work) and PoS(Proof of Stake) are also studied. Blockchain is being utilized in a variety of applications, including financial transactions, healthcare, insurance, the Internet of Things (IoT), manufacturing, education, and more, with the promise of increased skills and durability. A substantial number of public announcements and news regarding its aims, collaborations, development, and execution have been made in recent years. However, the most essential features and debates about blockchain security, problems, and policies have been raised all over the world.

REFERENCES

[1] [1] Sulyman, Shakirat. (2014). Client-Server Model. IOSR Journal of Computer Engineering. 16. 57-71. 10.9790/0661-16195771.

[2] [2] Zarrin, Javad & Aguiar, Rui & Barraca, João. (2017). Resource discovery for distributed computing systems: A comprehensive survey. Journal of Parallel and Distributed Computing. 113. 10.1016/j.jpdc.2017.11.010.

[3] [3] Priyadarshini, Ishaani. (2019). Introduction to Blockchain Technology. 10.1002/9781119488330.ch6.

[4] [4] Ghimire, Suman, "Analysis of Bitcoin Cryptocurrency and Its Mining Techniques" (2019). UNLV Theses, Dissertations, Professional Papers, and Capstones. 3603.

[5] [5] Zheng, Zibin & Xie, Shaoan & Dai, Hong-Ning & Chen, Xiangping & Wang, Huaimin. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. 10.1109/BigDataCongress.2017.85.

[6] [6] Wikipedia, "Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/SHA-2. [Accessed 14 03 2019].

[7] [7] G. Nguyen and K. Kim, "A Survey about Consensus Algorithms Used in Blockchain," Journal of Information Processing Systems, vol. 14, no. 1, pp. 101-128, 2018. DOI: 10.3745/JIPS.01.0024.

[8] [8] Kumar, Santosh. (2019). A REVIEW ON CLIENT-SERVER BASED APPLICATIONS AND RESEARCH OPPORTUNITY. International Journal of Scientific Research. 10. 33857-33862. 10.24327/ijrsr.2019.1007.3768.

[9] [9] Ahmed Banafa, "1 Introduction to Blockchain," in Blockchain Technology and Applications , River Publishers, 2020, pp.1-14.

[10] [10] Yousuf, Rameez & Jeelani, Zubair & Khan, Dawood & Bhat, Owais & Teli, Tawseef. (2021). Consensus Algorithms in Blockchain-Based Cryptocurrencies. 1-6. 10.1109/ICAECT49130.2021.9392489.

[11] [11] Baiod, Wajde; Light, Janet; and Mahanti, Aniket (2021) "Blockchain Technology and its Applications Across Multiple Domains: A Survey," Journal of International Technology and Information Management: Vol. 29 : Iss. 4 , Article 4.

[12] [12] Moritz, Alexandra & Block, Joern. (2016). Crowdfunding: A Literature Review and Research Directions. 10.1007/978-3-319-18017-5_3.

[13] [13] Pathak, Prof & Suradkar, Amol & Kadam, Ajinkya & Ghodeswar, Akansha & Parde, Prashant. (2021). Blockchain Based E-Voting System. International Journal of Scientific Research in Science and Technology. 134-140. 10.32628/IJSRST2182120.

[14] [14] Remya Stephen and Aneena Alex 2018 IOP Conf. Ser.: Mater. Sci. Eng. 396 012030

[15] [15] A. Kiayias and G. Panagiotakos, “On trees, chains and fast transactions in the blockchain,” In International Conference on Cryptology and Information Security in Latin America, Springer, Cham, pp. 327-351, 2017.

[16] [16] S. Porru, et all, “Blockchain-oriented software engineering: challenges and new directions,” In 2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C), pp. 169-171, 2017.

[17] [17] D. Siegel, “Understanding the DAO Attack,” Coindesk, 2016. https://www. coindesk. com/understanding-dao-hackjournalists/, updated on, 3(28), 2018.

[18] [19] S. Sayeed, et all., “Smart contract: Attacks and protections,” IEEE Access, vol. 8, pp. 24416-24427, 2020.

[19] [20] M. Wohrer and U. Zdun, “Smart contracts: security patterns in the ethereum ecosystem and solidity,” In 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE), pp. 2-8, 2018.

[20] [21] H. Chen, et all., “A survey on ethereum systems security: Vulnerabilities, attacks, and defenses,” ACM Computing Surveys (CSUR), vol. 53(3), pp. 1-43, 2020.

[21] [22] S. Eskandari, et all., “Sok: Transparent dishonesty: front-running attacks on blockchain,” In International Conference on Financial Cryptography and Data Security, Springer, Cham, pp. 170-189, 2019.

[22] [23] B. Jiang, et all., “Contractfuzzer: Fuzzing smart contracts for vulnerability detection,” In 2018 33rd IEEE/ACM International Conference on Automated Software Engineering (ASE), pp. 259-269, 2018.

[23] [24] K. Li, “The blockchain scalability problem & the race for visa-like transaction speed,” Retrieved November 29, 2019