Cover Page

DOI: http://ijmer.in.doi./2022/11.12.35
www.ijmer.in

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :8.017(2022); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:11, ISSUE:12(2), December: 2022
Online Copy of Article Publication Available (2022 Issues)
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd December 2022
Publication Date:10th January 2023
Publisher: Sucharitha Publication, India
Digital Certificate of Publication: www.ijmer.in/pdf/e-CertificateofPublication-IJMER.pdf

AGREEMENT PROTOCOL IN BLOCKCHAIN TECHNOLOGY

Rishi Kumar Srivastav, Dr. Devendra Agrawal, Dr. Gaurav Srivastava, and Dr. Shovona Choudhury
Research Scholar Babu Banarasi Das University, Lucknow
Dean Goel Institute of Technology & Management Lucknow
Assistant Professor Babu Banarasi Das University, Lucknow
Assistant Director Student Welfare, Amity University Jharkhand

Abstract:

The Bitcoin protocol, which is built on a peer-to-peer (P2P) network, allows transactions and blocks to be distributed in a decentralized manner to all nodes. The information is verified and kept in a Blockchain, a distributed data ledger, across the nodes. True decentralization is a feature of blockchain technology. Every block in blockchain technology consists of three major components: data, a hash block, and the previous hash block. Each block's uniqueness is controlled by the hash, which is different for every block. The previous block's hash is likewise contained in each new block, making the blocks interconnected. Three categories of blockchain exist: consortium blockchains, private blockchains, and public blockchains. In the suggested article, the blockchain consensus algorithms were compared and evaluated analytically based on specifications.

Keywords: Blockchain Technology, Bitcoin

Introduction:

Blockchain technology was first introduced in 1990 by Haber and Stornetta, and Satoshi Nakamoto utilised it for the first time in Bitcoin in 2008. The main objective of bitcoin, like any other currency system, is to simplify the exchange of goods and services by offering a product that is in high demand. No one entity or state issued bitcoin under the previous monetary system. It wasn't used often. Recently, it has been used in a number of industries, such as supply chain management, biomedicine, and registering smart contracts. The team behind the Casino et alstudy. provided a detailed analysis of the uses of blockchain in several businesses in 2019.

Using cryptography, Bitcoin allows transactions to be made among parties involved without the involvement of an escrow service or other third party. Bitcoin, on the other hand, is based on a P2P network where users can create new bitcoins [1]. Many trading marketplaces and companies are now accepting Bitcoin as a currency. Bitcoin is regarded as a trustworthy medium of exchange that enables exchange rates to be completed at the same speed as regional ones. All payments that have ever taken place can be found in a public database. Innovative payment methods like micro-payment, contractual, and escrow trades are also introduced.

As per figure 1, the Bitcoin system is based on a shared consensus mechanism that depends on the authentication and monitoring of payments being carried out by several parties. To achieve an agreement on which transfers are legitimate, all network nodes must be notified of a Bitcoin exchange via this process. In a public ledger that is accessible to the whole system, the agreed-upon position is documented in real-time. All of the transactions that were ever executed are stored in this register, which goes by the name of "blockchain" [2]. To keep track of previous blocks, each one provides a specific hash from the preceding something in its header. The genesis block would be the first block throughout the chain, but it contains no links to blocks that came before it. Blockchain technology experiences various branches and is a path out of a leaf block towards the genesis block.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :8.017(2022); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:11, ISSUE:12(2), December: 2022
Online Copy of Article Publication Available (2022 Issues)
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd December 2022
Publication Date:10th January 2023
Publisher: Sucharitha Publication, India
Digital Certificate of Publication: www.ijmer.in/pdf/e-CertificateofPublication-IJMER.pdf

DOI: http://ijmer.in.doi./2022/11.12.35
www.ijmer.in

Blockchain technology uses a completely decentralized and distributed database that is made up of an arrangement of blocks, each of which contains a list of transactions. Data, hash blocks, and prior hash blocks are the three main components of each block. Each block's uniqueness is controlled by the hash, which is different for every block. Hash indicates the information for each block. When a transaction is recorded in a block, its hash number is calculated and retrieved using mathematical formulas in an encryption block containing information. The blocks are related to one another since each block carries the hash of the one before it. A block's hash number changes whenever any modifications are made to its data. Therefore, if there are any unauthorized changes to the blocks' information, the hash value may change, making the block invalid for subsequent blocks (Zheng et al. 2019). Figure 1 shows the three-block structure of the bitcoin blockchain (Bhabendu 2019).

Figure. 1 Structure of bitcoin blockchain for three the blocks (Bhabendu 2019)

In the Fig. 1, the block 1 is 7th block it stored previous hash, next is 8th block is stored hash of 7th block and own hash, the first block is known as Genesis block and because of there is no any other block before this block, and previous hash amount is zero. Each block can cover thousands of records of transaction that are coded by a hash function before broadcasting to the network. To Generate a final hash value as a hash pointer, blockchain uses Merkle tree function (hash of current block) and each block comprises the hash code of the previous block for the reserve the connection in the blocks.

A hash-based data structure called the Merkle tree is a condensed version of the hash list. The non-leaf node in this tree is a hash of the child node, while the leaf node in this tree is a hash of a block of data. It lowers the cost of data communication and processing resources (Panarello et al. 2018). In order to identify a nonce that satisfies a predefined criteria, a cryptographic hash function must be thoroughly questioned during the process of authenticating or mining a new block by the proof of work method.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :8.017(2022); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:11, ISSUE:12(2), December: 2022
Online Copy of Article Publication Available (2022 Issues)
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd December 2022
Publication Date:10th January 2023
Publisher: Sucharitha Publication, India
Digital Certificate of Publication: www.ijmer.in/pdf/e-CertificateofPublication-IJMER.pdf

DOI: http://ijmer.in.doi./2022/11.12.35
www.ijmer.in

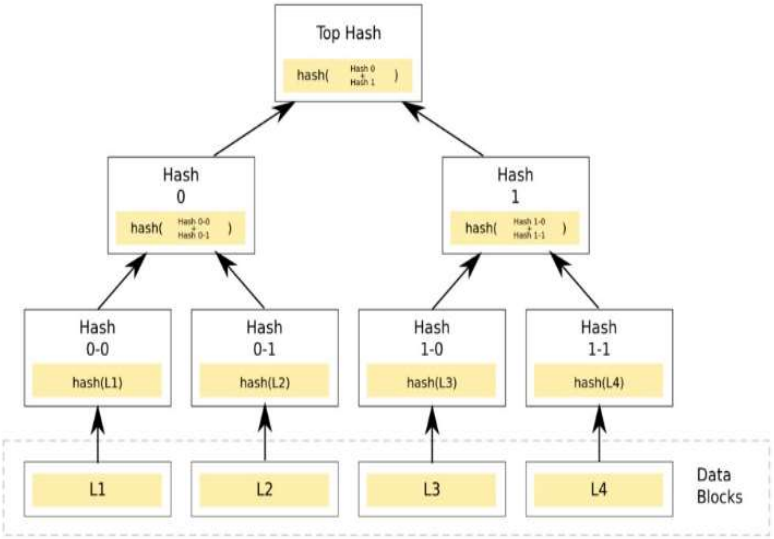

Figure 2: A Hash tree

Assume H (): hash function

x is a Merkle Root of transactions in a block.

Target hash=H(x nonce)≤D(h)

Where nonce= "number only used once" known as added number in hashed block in a blockchain to meet the predefined strain level and for about fixed span of bits L.

$D(h) = 2^{L-h}$

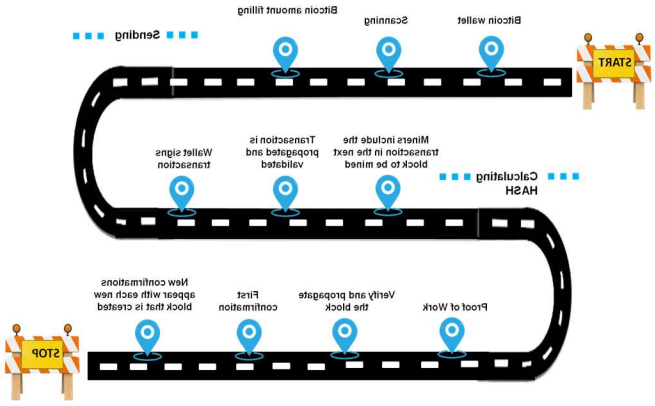

Figure3: Generalized procedure of Bitcoin transaction

Cover Page

DOI: http://ijmer.in.doi./2022/11.12.35
www.ijmer.in

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :8.017(2022); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:11, ISSUE:12(2), December: 2022
Online Copy of Article Publication Available (2022 Issues)
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd December 2022
Publication Date:10th January 2023
Publisher: Sucharitha Publication, India
Digital Certificate of Publication: www.ijmer.in/pdf/e-CertificateofPublication-IJMER.pdf

Nevertheless, the public ledger's inconsistency is blamed in part on the Bitcoin platform's information propagation delay. Our proposed solution to the issue of Bitcoin nodes agreeing on a shared history of transactions is by ramping up the propagation in the Bitcoin system.

This manuscript introduces the SAS+CAS technique to optimize the propagation delay in the P2P and Bitcoin networks. To standardize the bitcoin data, a normalization technique is used. To legalize the normalized data, smart contracts are employed. To store the validated data, a blockchain ledger is utilized. To increase the new blocks in the ledger, Proof-of-Work (PoW) approach is applied. The additional detail of this manuscript is organized as follows: topic II-related works with a problem statement, topic III-proposed work, topic IV-performance analysis, and topic V-conclusion.

Type of Blockchains
A blockchain is classified into general three categories public blockchain, consortium blockchain and private blockchain (Korpela et al. 2017):

1.1 Public Blockchain

1.2 Consortium Blockchains

1.3 Private Blockchains

2.Blockchain Consensus Algorithm
Please Reaching an agreement in a network of blockchain is a significant and a complex task. The new records of transaction would be added in blockchain since the new block is verified by all nodes in the network.

- Proof of Work (PoW)
- Proof of Stake (PoS)
- Delegated Proof of Stake
- Practical Byzantine Fault Tolerance
- Delegated Byzantine Fault Tolerance
- Proof of Weight (PoWeight)
- Proof of Burn (PoB)
- Proof of Capacity

Conclusion

The blockchain technology is truly distributed and decentralized technology. In blockchain technology, every block has consisted three main parts that is data, hash block, and the previous hash block. Hash is controlling the uniqueness of each block and it is unique for each block. Each block also contains the hash of the previous block; thus, the blocks are connected to each other. A blockchain can divided into three categories public blockchain, consortium blockchain and private blockchain. The proposed paper provided the give complete review on vulnerabilities in blockchain technology and various performance evaluation criteria of the consensus algorithms in blockchain

Cover Page

DOI: http://ijmer.in.doi./2022/11.12.35
www.ijmer.in

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :8.017(2022); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:11, ISSUE:12(2), December: 2022
Online Copy of Article Publication Available (2022 Issues)
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd December 2022
Publication Date:10th January 2023
Publisher: Sucharitha Publication, India
Digital Certificate of Publication: www.ijmer.in/pdf/e-CertificateofPublication-IJMER.pdf

REFERENCES

[1]. Lee, J.Y., 2019. A decentralized token economy: How blockchain and cryptocurrency can revolutionize business. Business Horizons, 62(6), pp.773-784.
[2]. Dai, M., Zhang, S., Wang, H., and Jin, S., 2018. A low storage room requirement framework for distributed ledger in blockchain. IEEE Access, 6, pp.22970-22975.
[3]. Franzoni, F. and Daza, V., 2022. Clover: An anonymous transaction relay protocol for the bitcoin P2P network. Peer-to-Peer Networking and Applications, 15(1), pp.290-303.
[4]. Zhang, J., Cheng, Y., Deng, X., Wang, B., Xie, J., Yang, Y. and Zhang, M., 2021. A Reputation-based Mechanism for Transaction Processing in Blockchain Systems. IEEE Transactions on Computers.
[5]. Chen, Y.H., Hu, C.C., Wu, E.H.K., Chuang, S.M. and Chen, G.H., 2017. A delay-sensitive multicast protocol for network capacity enhancement in multirate MANETs. IEEE Systems Journal, 12(1), pp.926-937.
[6]. Yadav, A.K. and Tripathi, S., 2017. QMRPRNS: Design of QoS multicast routing protocol using reliable node selection scheme for MANETs. Peer-to-Peer Networking and Applications, 10(4), pp.897-909.
[7]. Sharma, V.K. and Kumar, M., 2017. Adaptive congestion control scheme in mobile ad-hoc networks. Peer-to-Peer Networking and Applications, 10(3), pp.633-657.
[8]. Shahsavari, Y., Zhang, K. and Talhi, C., 2020. A theoretical model for block propagation analysis in bitcoin network. IEEE Transactions on Engineering Management.
[9]. Yang, W., Wu, J. and Luo, J., 2020. Effective data transmission and control based on social communication in social opportunistic complex networks. Complexity, 2020.
[10]. Klinkowski, M., 2020. Optimization of latency-aware flow allocation in NGFI networks. Computer Communications, 161, pp.344-359.
[11]. Jiang, X., 2019. Bitcoin price prediction based on deep learning methods. Journal of Mathematical Finance, 10(1), pp.132-139.
[12]. Alleema, N.N. and Kumar, D.S., 2020. Volunteer nodes of ant colony optimization routing for minimizing delay in peer to peer MANETs. Peer-to-Peer Networking and Applications, 13(2), pp.590-600.
[13]. Marzal, S., González-Medina, R., Salas-Puente, R., Figueres, E. and Garcerá, G., 2017. A novel locality algorithm and peer-to-peer communication infrastructure for optimizing network performance in smart microgrids. Energies, 10(9), p.1275.
[14]. Huang, J., Tan, L., Mao, S. and Yu, K., 2021. Blockchain Network Propagation Mechanism Based on P4P Architecture. Security and Communication Networks, 2021.
[15]. Shamshirband, S. and Soleimani, H., 2021. LAAPS: an efficient file-based search in unstructured peer-to-peer networks using reinforcement algorithm. International Journal of Computers and Applications, 43(1), pp.62-69.