BLOCKCHAIN'S CONSENSUS ALGORITHM: A REVIEW

Dr. Shambhu Bhardwaj*

*Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, INDIA
Email id: shambhu.bhardwaj@gmail.com

DOI: 10.5958/2249-7137.2021.02562.3

ABSTRACT

A consensus algorithm is a computer science technique that allows dispersed processes or systems to agree on a single data value. Consensus algorithms are intended to ensure dependability in a network containing many faulty nodes. Bitcoin's foundational technology is blockchain. With bitcoin's rising value and consistent functioning, blockchain is gaining traction in a variety of fields. Decentralization, stability, security, and non-modifiability are all features of blockchain. It has the capability of altering network architecture. The consensus algorithm is critical for preserving blockchain's security and efficiency. The use of the correct algorithm may significantly improve the performance of a blockchain application. We examined the fundamental concepts and features of consensus algorithms in this paper, as well as the performance and application scenarios of several consensus mechanisms. We also provided technical advice on choosing an appropriate consensus algorithm, as well as a summary of blockchain technology's limits and future developments.

KEYWORDS: *Bitcoin, Blockchain, Consensus, Digital Currency, Distributed System.*

1. INTRODUCTION

Satoshi Nakamoto originally mentioned the blockchain in his book "Bitcoin: A peer-to-peer electronic currency system" in 2008(1). It is bitcoin's fundamental technology. Traditional transactions need the use of a centralized, trustworthy organization. The trust institution is solely responsible for the validation and recording of transactions, which may lead to a slew of issues with transaction cost, efficiency, and security. Blockchain's fundamental characteristic is decentralization, which may be utilized to address these issues(2). The blockchain's nodes all share the same status. These nodes establish consensus by adopting the majority dominance principle and agreeing on the rules in advance. In the event that the other nodes are not completely trusted, they implement data dispersed storage and transaction information recognition. As a result, we will be able to properly address the transaction issues(3).

Bitcoin is the first blockchain-based financial application. The government, financial institutions, and technical companies have all shown interest in blockchain technology as it has developed. In January 2016, the British government, for example, released a study on blockchain to encourage its use in centralized digital money and government affairs (4). All of the world's top banks are actively investigating the use of blockchain technology. UBS, Deutsche Bank, Bank of Santander, and Bank of New York Mellon collaborated on a digital currency system based on blockchain technology in August 2016 to assist financial markets increase payment speed. The biggest bank in Spain, Bank of Santander, thinks that if all banks in the world used blockchain, they could save $20 billion each year. By 2027, the World Economic Forum estimates that 10% of global GDP would be held on the blockchain network (5).

Blockchain technology is also gaining popularity among academics. Blockchain research may be split into three areas. To begin, research digital currencies based on blockchain technology, including both decentralized and centralized digital currencies(6). Second, research into the use of blockchain technology in non-digital currency situations, such as smart city applications and medical information security management(7). Finally, research the blockchain technology that underpins it. Researchers are increasingly recognizing that the blockchain may be separated from the digital money to build a new technological architecture in other fields. Some academics have started to look at the underlying technologies, such as mining difficulty management, consensus algorithm scalability, and smart contracts.

1.1. The Consensus Algorithms:

We must address two issues in blockchain applications: double spending and the Byzantine Generals Problem (8). The term "double spending" refers to the practice of using the same money in two different transactions at the same time. Because conventional money is an entity, we will not have to worry about double spending when we use it. With centralized trustworthy institutions, we can also address the issue of double spending in Internet transactions(9). The technique of validating transactions by multiple distributed nodes together in blockchain overcomes this issue. The Byzantine Generals Issue is a distributed system problem. Peer-to-peer connections may be used to transmit data between various nodes. However, certain nodes may be deliberately targeted, resulting in communication content alterations(10). Normal nodes must be able to identify manipulated information and provide consistent results with other normal nodes. This necessitates the development of a consensus algorithm.In distributed systems, the consensus algorithm has been researched for many years. In blockchain, several transplantable consensus algorithms are used. In this part, we go through the fundamentals of these consensus methods in depth(11).

1.1.1. PoW (Proof of Work):

Bitcoin's consensus algorithm is known as PoW. Its fundamental concept is to distribute accounting rights and rewards across nodes based on hashing power competition. The various nodes compute the particular answer to a mathematical problem based on the input from the preceding block. The arithmetic issue is tough to solve(12). The first node to answer this math problem will be able to produce the next block and will be rewarded with a specific amount of bitcoin. This bitcoinmaths challenge was designed by Satoshi Nakamoto usingHashCash. The following are the exact stages in the calculation:

i. Get the difficulty:

Following the generation of every 2016 blocks, the bitcoin mining algorithm will dynamically change the difficulty value based on the network's hash rate.

ii. Collect transactions:

After the final block is produced, collect all outstanding transactions on the network. Then put in the block version number, the preceding block's 256-bit hash value, the current target hash value, the Nonce random number, and other information to calculate the Merkle Root of these transactions(13).

iii. Calculating:

In step 2, traverse the Nonce from 0 to 232 and compute the double SHA256 hash value. The block may be published if the hash value is less than or equal to the desired value. After the other nodes have been verified, the node completes its accounting(14).

iv. Restarting:

If the node is unable to calculate the hash value at a particular point in time, it returns to step two. If any other node completes the computation, it returns to step 1 and repeats the process(15)(16).

The workload is used as a precaution in PoW. The blocks in front of it are connected to the newly formed block. The quantity of effort is proportional to the length of the chain. The longest chain is trusted by all nodes. If someone wishes to tamper with the blockchain, he has to have more than half of the world's hashing power in order to be the first to create the most recent block and dominate the longest chain. The benefits of tampering may far outweigh the costs. As a result, the PoW can efficiently ensure the blockchain's security(17).

1.1.2. PoS(Proof of Stake):

PoS was discussed in the original bitcoin project, but it was not utilized for a variety of reasons, including robustness. PPCoin is the first PoS implementation(18). The notion of coin age exists in PoS digital money. A coin's age is calculated by multiplying its value by the time since it was minted. The longer a node keeps the money, the more network privileges it may get. Coin owners will also get a monetary incentive based on the coin's age. Mining is also required in the architecture of PPCoin in order to get accounting rights. Proofhash * coin age * goal is the formula. The proofhash is a hash value that combines the weight factor, the unspent output value, and the current time's fuzzy sum. Each node's hashing power is limited by PoS. The difficulty of mining is related to the age of the currency.

PoS encourages coin holders to keep their coins for longer periods of time. The blockchain is no longer completely reliant on proof of work thanks to the idea of coin age. In PoW, this successfully addresses the resource waste issue. With growing value on the blockchain, the security of the blockchain utilizing PoS increases. To assault the blockchain, the attackers must amass a significant amount of currencies and keep them for a long time. The attack difficulty is also significantly increased as a result of this.

Many other currencies, like as Nxt and BlackCion, use PoS in addition to the PPCoin. They do, however, take into consideration the rights of the nodes and assign accounting rights using a random method.

1.1.3. DPoS (Delegated Proof of Stake):

Satoshi Nakamoto believed that everyone who wanted to mine bitcoin could do so using their computer's CPU. As a result, the hashing power of the nodes may be matched, and each node can participate in the blockchain's decision-making process(19). Machines specifically intended for mining have been developed as technology has progressed and the value of bitcoin has increased.

Participants with a high number of mining rigs are grouped together in terms of hashing power. Ordinary miners are seldom given the chance to generate a block.

DPoS is exemplified by BitShares. Each node on the DPoSblockchain may choose the witnesses depending on its stake. The top N witnesses who participated in the campaign and received the most votes have the accounting right throughout the whole network. The number N of witnesses is chosen such that at least 50% of voting stakeholders feel decentralization is enough. The chosen witnesses are rewarded for creating new blocks one by one as directed. Witnesses must set up enough time to be online. If a witness is unable to produce the block for which they were allocated, the activity for that block will be shifted to the next block, and stakeholders will vote for a new witness to take its place. DPoS is a more efficient and power-saving blockchain than PoW and PoS.

1.1.4. PBFT(Practical Byzantine Fault Tolerance):

Byzantine Fault Tolerance may be a useful way to address transmission problems in distributed systems. Early Byzantine systems, on the other hand, require exponential processes. The PBFT (Practical Byzantine Fault Tolerance) system was proposed till 1999, and the algorithm complexity was lowered to a polynomial level, significantly increasing efficiency. The PBFT procedure is divided into five states:

i. Request:

The client makes a request to the master server node, which assigns a timestamp to the request.

ii. Pre-prepare:

The request message is recorded and assigned an order number by the master server node. The master node then broadcasts a pre-prepare message to the other server nodes in the chain. The other server nodes must first decide whether or not to accept the request.

iii. Prepare:

If a server node accepts the request, it sends out a prepare message to all other server nodes and gets prepare messages from the others. If a majority of nodes opt to accept the request after collecting 2f+1 messages, it will reach the commit state.

iv. Commit:

Each node in the commit state sends a commit message to the rest of the server's nodes. At the same time, if a server node gets 2f+1 commit messages, it may think that the request has been accepted by the majority of nodes. The node then follows the instructions in the request message and executes them.

v. Reply:

The client receives a response from the server nodes. The request is reissued to the server nodes if the client does not get a response due to a network latency. If the request has been fulfilled, the server nodes need simply transmit the reply message over and over again.

1.1.5. Raft:

In 1990, Lamport developed the Paxos algorithm to address the consistency issue under specific circumstances after the Byzantine Generals Problem was stated. However, the paper was not approved since the material was difficult to comprehend. The Paxos was temporarily revived in 2001 when Lamport reprinted the paper in 1998(20). Paxos, on the other hand, has a commanding lead in the area of consistency algorithms. It's the basis for a slew of additional algorithms. Paxos' algorithm, on the other hand, is much too theoretical. People have a hard time comprehending it and engineering its execution. In 2013, Ongaro and colleagues from Stanford University released a paper that introduced the Raft algorithm(21). Raft has the same impact as Paxos but is easier to build and comprehend in terms of engineering. In most cases, a Raft cluster consists of 5 server nodes. It is possible for up to two nodes to crash at the same time. There are three states for the server node: leader, follower, and candidate. In each term, there is only one leader who is in charge of addressing all customer demands.

2. LITERATURE REVIEW

Nguyen et al. provide an overview of Blockchain consensus algorithms that have been studied and are now being used in a number of well-known applications(22). According to them, Blockchain has addressed the issue of converting a low-trust centralized ledger maintained by a single third-party to a high-trust decentralized ledger owned by many organizations, or verifying nodes(23). The consensus method, which determines how all nodes in the validating network agree to add a new block, is a significant contribution to Blockchain's work. Blockchain algorithms are divided into two categories. The first is proof-based consensus, which requires nodes entering the verifying network to demonstrate that they are more equipped to perform the adding job than the others. The second kind of consensus is voting-based consensus, which requires network nodes to share their results of validating a new block or transaction before reaching a final decision(24).

L. M. Bach et al. compare and contrast traditional consensus algorithms with some of its contemporaries presently in use in contemporary blockchains(25). Their investigation focuses on the algorithmic processes performed by each consensus algorithm, the system's scalability, the manner by which validators are compensated for their time spent confirming blocks, and the algorithm's security concerns. Finally, they discuss their findings as well as some potential future trends in blockchain consensus algorithms.

3. DISCUSSION

3.1. Analysis of the Consensus Algorithms:

Each consensus algorithm has its own set of features. In this chapter, we examine the consensus algorithms' safety, verification speed, throughput (transactions per second, TPS), fault tolerance, scalability, and limitations, as well as their use in various situations.

3.1.1. Limitation:

PoW has other flaws, such as resource waste, transaction verification speed, and hashing power concentration:

i. Waste of Resources:

Nodes with a lot of hashing power may receive bitcoins as a reward. This is the primary method of obtaining bitcoin, which requires users to update their gear. Participants must pay a significant amount of money to purchase the specialized mining equipment, and the devices must use a significant quantity of power throughout the computation process. These features also impose certain restrictions on the use of PoW.

ii. The Slow Speed of Transactions:

The calculation time of each block must not be too short in order to minimize the creation of a single block or branch of the chain. The block's average calculation time is 10 minutes. The time gap between the two blocks, however, is unknown. The longest gap in history is almost an hour, while the shortest is less than a second. The use of immediate payment has a significant time restriction at this moment.

3.1.2. Application Scenarios:

Public blockchains, private blockchains, and permissioned blockchains are the three types of blockchains. According to the preceding section, under certain situations, it is preferable to apply the appropriate consensus method.

A public blockchain is one that is available to everyone in a public space. Anyone may join the nodes and contribute in order to get the benefits if they follow the rules. There are no node-to-node trust connections. The public blockchain is fully decentralized and accessible. On the public blockchain, no transaction can be altered or canceled. Public blockchains often use the PoW, PoS, and DPoS consensus algorithms.

4. CONCLUSION

Decentralization, stability, security, and non-modifiability are all features of blockchain. With the advancement of technology, the blockchain is gaining traction in a variety of fields. This paper does a thorough examination of the most common blockchain consensus algorithms. Although the consensus algorithm is at the heart of blockchain, current research on the process is still in its early stages. It's still uncommon to find a consensus method that's tailored to certain situations. What can be done to improve the performance of the blockchain in a certain scenario? More research is still required.The consensus algorithm has been studied in distributed systems for many years. Several transplantable consensus methods are utilized in blockchain. These consensus algorithms' principles are well explained in this paper.

REFERENCES

1. Nakamoto S. A. The Bitcoin Whitepaper by Satoshi Nakamoto - Mastering Bitcoin, 2nd Edition [Book]. www.bitcoin.org. 2018.

2. Ghai W, Kumar S, Athavale VA. Using gaussian mixtures on triphone acoustic modelling-based punjabi continuous speech recognition. In: Advances in Intelligent Systems and Computing. 2021.

3. Sharma K, Goswami L. RFID based Smart Railway Pantograph Control in a Different Phase of Power Line. In: Proceedings of the 2nd International Conference on Inventive Research in Computing Applications, ICIRCA 2020. 2020.

4. Walport M. Distributed ledger technology: Beyond block chain. Gov Off Sci. 2015;

5. Spring J. The World Economic Forum. In: Economization Of Education. 2018.

6. Solanki MS, Sharma DKP, Goswami L, Sikka R, Anand V. Automatic Identification of Temples in Digital Images through Scale Invariant Feature Transform. In: 2020 International Conference on Computer Science, Engineering and Applications, ICCSEA 2020. 2020.

7. Xia H, Jia Z, Li X, Ju L, Sha EHM. Trust prediction and trust-based source routing in mobile ad hoc networks. Ad Hoc Networks. 2013;

8. The byzantine generals problem. Dr Dobb's J. 2008;

9. Goel S, Mamta. GA based trip attraction model for DUA. In: 2015 International Conference on Computing for Sustainable Global Development, INDIACom 2015. 2015.

10. Sharda V, Agarwal RP. Analysis of Graphene Nanoribbon (GNR) interconnects with multi-gate device technology for VLSI applications. In: 2015 IEEE UP Section Conference on Electrical Computer and Electronics, UPCON 2015. 2016.

11. Walia A, Singhal N, Sharma AK. A novel e-learning approach to add more cognition to semantic web. In: Proceedings - 2015 IEEE International Conference on Computational Intelligence and Communication Technology, CICT 2015. 2015.

12. Kumar S, Kumar K, Pandey AK. Dynamic Channel Allocation in Mobile Multimedia Networks Using Error Back Propagation and Hopfield Neural Network (EBP-HOP). In: Procedia Computer Science. 2016.

13. Verma KG, Kaushik BK, Singh R. Propagation Delay Variation due to Process Induced Threshold Voltage Variation. In: Communications in Computer and Information Science. 2010.

14. Kishore N, Singh S. Torque ripples control and speed regulation of Permanent magnet Brushless dc Motor Drive using Artificial Neural Network. In: 2014 Recent Advances in Engineering and Computational Sciences, RAECS 2014. 2014.

15. Goel AR, Ranjan A, Wajid M. VLSI architecture and implementation of statistical multiplexer. In: Proceedings of the International Conference on Innovative Applications of Computational Intelligence on Power, Energy and Controls with Their Impact on Humanity, CIPECH 2014. 2014.

16. Rai MK, Khanna R, Sarkar S. Control of tube parameters on SWCNT bundle interconnect delay and power dissipation. Microelectron Int. 2014;

17. Khanna R, Verma S, Biswas R, Singh JB. Implementation of branch delay in Superscalar processors by reducing branch penalties. In: 2010 IEEE 2nd International Advance Computing Conference, IACC 2010. 2010.

18. Kiayias A, Russell A, David B, Oliynykov R, Bentov I, Lee C, et al. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. Proc 2016 ACM SIGSAC Conf Comput Commun Secur - CCS'16. 2017;

19. Bitshares. @# Delegated Proof-of-Stake Consensus. bitshares.org. 2017.

20. Leslie Lamport. Paxos Made Simple. ACM SIGACT News. 2003;

21. Ongaro D, Ousterhout J. In Search of an Understandable Consenus Algorithm (Extended Version). Proc USENIX ATC ’14. 2014;

22. Nguyen GT, Kim K. A survey about consensus algorithms used in Blockchain. J Inf Process Syst. 2018;

23. Sharma S, Bansal M. Real-time sentiment analysis towards machine learning. Int J Sci Technol Res. 2020;

24. Tyagi VK, Goel R, Singh M, Kumar S. Modeling and analysis of a closed loop supply chain with uncertain lead time in the perspective of inventory management. Int J Sci Technol Res. 2020;

25. Bach LM, Mihaljevic B, Zagar M. Comparative analysis of blockchain consensus algorithms. In: 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2018 - Proceedings. 2018.