IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Consensus Protocols in Blockchain Technology

[1]Bhavika Aggarwal
[2]Bhavika Mathur
[3]Prachi Prajapati
[1,2,3]Rajasthan College of Engineering for Women, Rajasthan-302021, India

Abstract

Blockchain technology is decentralized in nature. So, it uses consensus protocols to validate the transactions. These consensus mechanisms impose a set of rules for all the nodes in the network to achieve distributed agreement about the state of the ledger. This paper provides a detailed analysis of several blockchain consensus protocols, including Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT). This study evaluates these protocols based on critical criteria including security, scalability, energy efficiency. This work aims to give a practical understanding of the important role played by consensus mechanisms in the context of blockchain.

Introduction

Blockchain technology is a decentralized distributed ledger system which records transactions across a network. Every time a transaction is completed, it gets added to a block. These blocks are added to a chain in a chronological order. A block cannot be removed or altered after getting added to blockchain. This ensures integrity of data. The use of cryptography techniques makes this possible. Blockchain cannot be fully controlled by one organization due to its' decentralized structure. It offers excellent security and transparency and is hence impervious to manipulation. A distributed database system called blockchain maintains a record of every transaction made inside a network through full replication. All of the transactions are stored on each contributing node or in the network [1]. Blockchain technology changed the way we handle transactions in decentralized systems. It's like a big shift in how things are done. The special thing about it is how all the computers in the network agree on what's a valid transaction. They use something called consensus protocols to do this. These protocols are like the glue that holds everything together and makes sure the records in the

blockchain are reliable. The spectrum of consensus protocols reflects a dynamic interplay between security, scalability, and resource efficiency. Examples of this include the more energy-efficient Proof of Stake (PoS) model, which employs ownership stakes to safeguard the network, and the revolutionary Proof of Work (PoW) algorithm, which is well-known for its computational intensity and resistance against Sybil assaults.

Types of Consensus Protocols

1. Proof of Work (PoW)

To secure and confirm transactions in blockchain networks, Proof of Work (PoW) is a consensus process employed. Satoshi Nakamoto introduced it as an important component of the Bitcoin system in 2008 [2]. Network users known as miners compete to solve complex mathematical riddles in Proof of Work system. The solving of these problems calls for a substantial amount of processing power and is intended to be computationally demanding.

A collection of pending transactions is gathered by miners from the network. A block is created by grouping these transactions collectively. Subsequently, the miner merges these transactions with additional data, such as a timestamp and a reference to the blockchain's previous block [3]. This creates a block of candidates. What's important in this procedure is the "nonce." The miner inserts a random number called the nonce into the candidate block. The miner's job is to locate the correct nonce that, when hashed with the other block data, yields a hash value that satisfies predetermined standards. This criterion usually entails the hash falling below a predetermined threshold. Miners compute the hash value and modify the nonce in their candidate block iteratively until they find a hash that satisfies the predetermined requirements. This procedure is frequently called "mining" because of the significant amount of computer work involved. A miner broadcasts the solution to the network after they find a valid nonce. Other nodes in the network can rapidly verify that the solution is correct by using the nonce to recompute the hash and see whether it meets the requirements. The first miner who finds a valid nonce adds the block to the network. This process is called "mining a block". Miner gets a reward for adding the block in the form of certain amount of cryptocurrency from transaction fees of the included transactions.

2. Proof of Stake (PoS)

An alternate consensus method called Proof of Stake (PoS) is employed by blockchain networks for transaction validation and security. Validators, often known as "stakers," are selected to build new blocks and approve transactions in a proof of stake (PoS) system according to the quantity of bitcoin they own and are prepared to "stake" as collateral [4]. A validator's chances of getting chosen to create a new block increase with the amount of cryptocurrency they stake. Validators take turns creating blocks and validating

transactions. Every round, the number of cryptocurrency that validators own, how long they have been staking, and a pseudo-random selection method are commonly used to determine which validators are chosen. A specific quantity of cryptocurrency must be "locked up" as collateral by validators, and this collateral is put at danger if they approve fraudulent transactions or make an attempt to undermine the network's security. Validators are motivated to operate truthfully by this collateral since they stand to lose anything.

3. Delegated Proof of Stake (DPoS)

Delegated Proof of Stake (DPoS) is a variation on the Proof of Stake (PoS) consensus protocol. Distributed Proof of Stake (DPoS), developed by Daniel Larimer of BitShares and Steem, has been adopted by networks like EOS. In a decentralized point of sale (DPoS) system, the network users cast votes to select a predefined number of block producers (sometimes called "delegates" or "witnesses"). These producers of blocks are in charge of validating transactions and generating new blocks. Apart from the amount of staked cryptocurrency, members with voting rights are picked through election and replacement [5]. Block producers serve in a rotational manner, with a set schedule for when each producer is responsible for creating blocks. This regular rotation ensures that different validators have the opportunity to participate in block creation. Block producers are rewarded for their role in creating blocks and validating transactions. These rewards come in the form of transaction fees and, in some cases, newly created cryptocurrency. If some block producers act maliciously or attempt to compromise the network's security, they can face penalties, which may include losing their position as a block producer.

4. Practical Byzantine Fault Tolerance (PBFT)

The goal of the Practical Byzantine Fault Tolerance (PBFT) consensus mechanism is to enable distributed systems to come to an agreement even when there are malicious or broken nodes present. It was presented by Miguel Castro and Barbara Liskov in 1999. Applications where some level of participant trust is expected, such as distributed databases and permissioned blockchain networks, are particularly well-suited for PBFT. Based on the Byzantine Fault Tolerance (BFT) model, which is the foundation for PBFT, it is assumed that malicious or other flaws may be present in up to one-third of a network's nodes [6]. PBFT guarantees unanimity as long as the number of malicious nodes stays below this limit.

5. Other Consensus Mechanisms

In addition to the widely recognized consensus mechanisms there are several other consensus mechanisms that have been proposed or implemented in various blockchain networks. These are Raft, Hashgraph, Proof of Authority (PoA), Proof of Burn (PoB), Proof of Space, Proof of Time, Simplified Byzantine Fault Tolerance (SBFT), etc.

Evaluation of different consensus protocols based on key criteria

1. Security

PoW is thought to be extremely safe because it involves a lot of calculation. Miners have to invest a significant amount of computing power to these tasks to validate transactions and create new blocks. As a result, miners cannot afford to take control of the network. Sybil attacks, in which a hacker creates multiple identities in an attempt to take over the network, cannot harm PoW. Nevertheless, Proof of Work (PoW) is susceptible to a 51% assault, in which the blockchain can be altered by a party holding more than 50% of the network's processing power [7].

By requiring validators to stake cryptocurrency as collateral, PoS offers security. If validators approve fraudulent transactions, then they can lose money. Thus, they have financial incentive to operate honestly. An attacker cannot obtain more than 50% supply of cryptocurrency. So, Proof of Stake (PoS) is immune to a 51% attack. DPoS seeks to strike a compromise between security and efficiency by reducing the number of block producers [8]. This might lead to a more centralized network since only a select group of reliable nodes are in charge of generating new blocks. PBFT handles situations prone to byzantine faults; it can achieve consensus even when up to one-third of the nodes are malevolent or failing.

2. Scalability

PoW faces scalability challenges, especially in large networks. The computational requirements for mining and the limited block size can lead to slower transaction processing times during high demand. PoS generally offers better scalability compared to PoW. PoS networks have higher throughput because they can process transactions faster because block building doesn't require a lot of resources. The goal of DPoS is to increase scalability by reducing the quantity of block producers. Improved network efficiency and quicker transaction confirmation times may result from this. PBFT can handle a moderate number of nodes efficiently [9]. It is known for its low message complexity, making it suitable for systems with a relatively small number of participants.

3. Energy Efficiency

PoW is renowned for requiring a lot of computation, which uses a lot of energy. Miners compete to find solutions to challenging mathematical riddles, which call for a lot of processing power. This can lead to high energy consumption, especially in large-scale networks [10]. PoS is generally considered more energy-efficient compared to PoW. Since block creation is not resource-intensive, PoS networks consume significantly less energy. Validators are chosen on the basis of amount of cryptocurrency they hold and are willing to stake as collateral. DPoS aims to balance efficiency and security. By limiting the number of block producers, DPoS can achieve higher energy efficiency compared to PoW, as only a fixed number of trusted nodes are responsible for block creation. PBFT is known for its relatively low message complexity, which

can lead to efficient communication. While it doesn't involve the energy-intensive computations of PoW, its energy efficiency depends more on network communication and message processing.

References

1.Zou, J.; Ye, B.; Qu, L.; Wang, Y.; Orgun, M.A.; Li, L. A Proof-of-Trust Consensus Protocol for Enhancing Accountability in Crowdsourcing Services. IEEE Trans. Serv. Comput. 2019

2.Berentsen, A. Aleksander Berentsen Recommends “Bitcoin: A Peer-to-Peer Electronic Cash System” by Satoshi Nakamoto. In 21st Century Economics; Springer International Publishing: Cham, Switzerland, 2019

3.Kingslin, S.; Zahra, R. An Effective Randomization Framework to POW Consensus Algorithm of Blockchain (RPoW). Int. J. Eng. Adv. Technol. 2019

4.Leonardos, S.; Reijsbergen, D.; Piliouras, G. Weighted Voting on the Blockchain: Improving Consensus in Proof of Stake Protocols. In Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea, 14–17 May 2019

5.Luo, Y.; Chen, Y.; Chen, Q.; Liang, Q. A New Election Algorithm for DPos Consensus Mechanism in Blockchain. In Proceedings of the 2018 7th International Conference on Digital Home (ICDH), Guilin, China, 30 November–1 December 2018

6.Castro, M.; Liskov, B. Practical byzantine fault tolerance and proactive recovery. ACM Trans. Comput. Syst. 2002

7. Sayeed, S.; Marco-Gisbert, H. Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack. Appl. Sci. 2019

8.Ogawa, T.; Kima, H.; Miyaho, N. Proposal of Proof-of-Lucky-Id(PoL) to Solve the Problems of PoW and PoS. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018

9.Cho, H. ASIC-Resistance of Multi-Hash Proof-of-Work Mechanisms for Blockchain Consensus Protocols.IEEE Access 2018

10. Sharkey, S.; Tewari, H. Alt-PoW: An Alternative Proof-of-Work Mechanism. In Proceedings of the 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON), Newark, CA, USA, 4–9 April 2019