Evolution of Consensus Algorithms for Scalable Blockchain Networks

Dr. H.Mohana
Assistant Professor, Department of Computer Science St Anne's Arts and Science College, Chennai, India.

Abstract: ***One of the key technologies for various cryptocurrencies is blockchain. Because of its characteristics, including stability, security, inalterability, and decentralization, blockchain is currently the subject of much research in the security domain. In blockchain technology, the transactions can be done securely with the help of consensus algorithms in a distributed system which has P2P connections of blocks, without interference of mediator [1]. Therefore, in blockchain technology, consensus algorithms are essential to maintaining the integrity and security of a distributed network. It is primarily employed to uphold blockchain technology's credibility. The algorithms used for consensus are separated into two categories: voting-based and proof-based. The primary consensus algorithms of these two categories are discussed in this paper along with their advantages, disadvantages, and the kinds of blockchains they work with.***

Keywords: Cryptocurrency, Bitcoin, Block Chain, Consensus Algorithms.

I. INTRODUCTION

A cryptocurrency is defined as a digital or virtual currency that employs cryptographic techniques for security. In our increasingly digital society, there is a significant shift towards complete digitalization, with many aspects of our lives becoming paperless. This transition includes financial transactions and investments, which is now predominantly conducted without physical documentation. Cryptocurrency represents a notable sector within this digital payment landscape.

What is Cryptocurrency?

Cryptocurrency refers to a form of digital or virtual currency that lacks a physical form and is characterized by its high level of security. In essence, it can be understood as a method of exchanging value. Bitcoin serves as the most prominent example, being the first cryptocurrency ever created. Other notable cryptocurrencies include Ethereum, Litecoin, and Zcash. Cryptocurrencies are decentralized so they operate individually of any central authority. Additionally, cryptocurrencies are not subject to taxation and lack insurance, with neither governments nor banks assuming responsibilities of their own. Several nations have imposed bans on cryptocurrency usage.

Need for Cryptocurrency?

The primary objective of cryptocurrency is to mitigate the risks associated with traditional forms of currency. Its user-friendly nature allows for accessibility at any time and from any location, requiring only a smartphone and a reliable internet connection. In cryptocurrency, power and responsibility rest with the holder, enabling them to address effectively for various real-world challenges.

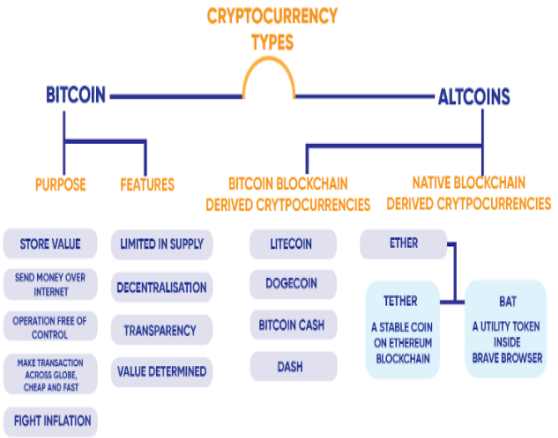

Fig 1. Types of Cryptocurrency [2]

In 2008, Satoshi Nakamoto introduced the foundational concept of blockchain technology, which was subsequently utilized for the creation of the first cryptocurrency, Bitcoin, characterized by its distributed ledger system[3]. A Bitcoin wallet serves as a device or software application for storing and transferring Bitcoins. These wallets house the private keys essential for authorizing Bitcoin transactions; possession of the private key grants control over the Bitcoins linked to that

specific address. Among the various types of wallets, hardware wallets are recognized as the most secure option.

Rank	Country	Percentage
1	Ukraine	12.73
2	Russia	11.91
3	Kenya	8.52
4	United States	8.31
5	India	7.3
6	South Africa	7.11
7	Nigeria	6.31
8	Thailand	5.2
9	United Kingdom	4.95
10	Brazil	4.88

Fig 2. Leading 10 Countries with the Highest Number of Cryptocurrency Holders[4].

This figure presents a ranking of countries with the largest populations of cryptocurrency owners globally. In India, for instance, 7.3% of the population possesses cryptocurrency.

Table 1. Difference between Crypto Coin and Crypto Token:

CRYPTO COIN	CRYPTO TOKEN
A coin is a digital asset that operates on its own blockchain.	A token is a digital asset that functions on an existing blockchain. Ownership of tokens provides specific advantages and opportunities within a project's ecosystem, while cryptocurrencies are primarily designed to serve as a medium of exchange.

How does a Cryptocurrency work?

Cryptocurrency operates through Blockchain technology, which is a sophisticated system that allows both buyers and sellers to access each other's information, thereby eliminating the need for intermediaries such as brokers. For instance, when purchasing shares in a stock market, one typically relies on a broker to facilitate the transaction. The broker confirms the order, and the shares are subsequently transferred to the buyer without any direct interaction with the seller. This reliance on brokers stems from the uncertainty regarding the seller's possession of the stock, a concept referred to as the principle of novation. In contrast, cryptocurrency transactions do not require third-party involvement, as all transaction data is recorded in a shared ledger that is accessible to all participants. While the identities of the individuals involved in the transactions are encrypted, the transparency of the Blockchain ensures that the transaction history is publicly available.

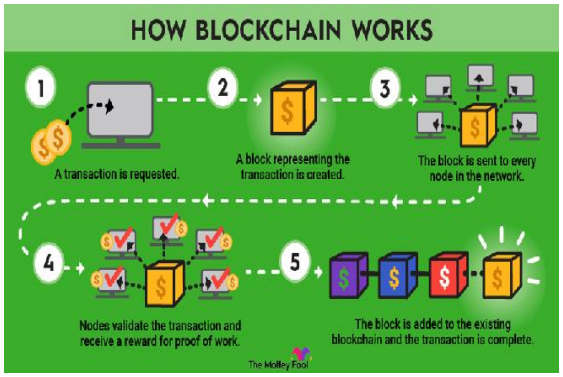

Fig 3. BlockchainWorking Methodology

Blockchain Technology: A blockchain functions as a decentralized ledger that records all transactions within a peer-to-peer network. This technology enables participants to validate transactions independently, eliminating the necessity for a central clearing authority. To ensure the blockchain security, a consensus algorithm is implemented. This algorithm facilitates the addition of new blocks to the blockchain while maintaining the integrity of the data contained within the distributed ledger. The operational methodology of blockchain[3] begins with a user initiating a transaction. A new block is generated to encapsulate the details of this transaction. This block is then disseminated to all nodes within the network, where it undergoes a verification and validation process. Upon successful verification by the node, the block is incorporated into the existing blockchain, thereby completing the transaction.

II RELATED WORK:

Qian Hu et al [15] propose the Reputation-DPoS consensus algorithm, which can select high-quality proxy nodes from a large-scale blockchain distributed network to participate in consensus.

Yang, Fan & Zhou et al [16] addresses, At present, the most common consensus algorithms are: PoW, PoS, DPoS and PBFT. From the emergence of Bitcoin to today, there are more than 30 consensus algorithms, most of which are based on the above four consensus algorithms.

S. Islamet al., [17] presents an extensive study of different types of consensus protocols used in existing blockchain solutions with the strength and limitations of each algorithm. Author provides general architecture, taxonomy of consensus algorithm and did a comparative study on all consensus algorithms.

III CONSENSUS ALGORITHM

Blockchain technology, akin to other distributed systems, depends on consensus algorithms to achieve agreement and maintain the integrity of its network. A consensus algorithm serves as a protocol that enables all participants within the blockchain network to reach a unified agreement regarding the current state of the ledger. So therefore In a distributed computing setting, this promotes confidence among peers who are unfamiliar with one another. These algorithms ensure that each new block integrated into the network represents the singular, agreed-upon version of truth, as recognized by all nodes within a decentralized computing framework. Four primary criteria have been identified that, when considered together, enhance the precision of consensus algorithm selection. These criteria include energy consumption, decentralization, security, and bandwidth [9]. The significance of consensus algorithms in blockchain technology is multifaceted. Firstly, they safeguard legitimate transactions and ensure smooth network functionality by preventing malicious actors from gaining control. Secondly, they support decentralization by ensuring that all nodes reach a consensus on the validity of transactions, thus averting centralization. Thirdly, by making every transaction visible on the blockchain, consensus algorithms promote transparency, facilitating the detection and prevention of fraudulent activities. Lastly, they enhance efficiency by allowing nodes to quickly agree on transaction legitimacy and promptly incorporate new blocks into the blockchain.

Top Blockchain Consensus Algorithms:

1. Proof Of Work (PoW)
2. Proof Of Stake (PoS)
3. Delegated Proof-of-Stake (DPoS)
4. Leased Proof of Stake (LPoS):
5. Proof of Authority (PoA)
6. Proof of Elapsed Time (PoET)

1. PoW (Proof of Work):

This concept was initially presented by Satoshi Nakamoto in relation to the Bitcoin cryptocurrency. The predominant consensus mechanism utilized in the realm of cryptocurrency is known as Proof of Work (PoW). The term "Proof of Work" was first coined by Markus Jakobsson and Ari Juels [11] in 1999. The fundamental principle of PoW is to enable miners to append new transaction blocks to the blockchain. To authenticate a transaction, miners are required to resolve a cryptographic challenge, commonly referred to as a hash puzzle. The traditional PoW consensus algorithm employs the SHA-256 hashing function, while other algorithms include those associated with SHA-3, Scrypt, scrypt-n, and scrypt-jane [5].

In this framework, the miner who successfully solves the puzzle first is granted the authority to generate a new block and is rewarded with bitcoins. The complexity of solving a PoW puzzle is considerable. Moreover, the PoW algorithm is not without its drawbacks: it necessitates substantial computational resources and is susceptible to a 51% attack. This term refers to a scenario in which a regulatory entity controls 51% or more of the nodes within the blockchain network, thereby possessing the capability to manipulate the network. Additionally, as the blockchain expands, the time and difficulty associated with resolving PoW puzzles also escalate. Given that PoW is resource-intensive, it is ill-suited for extensive and rapidly evolving networks. Cryptocurrencies such as Bitcoin, Ethereum, Monero, Litecoin, and Dogecoin employ PoW as their consensus mechanism. SHA-256 is the most widely adopted Proof of Work algorithm, having been introduced as part of Bitcoin, alongside others like SCRYPT, SHA-3, SCRYPT JANE, and SCRYPT-N [13].

Advantages:

1. PoW compels miners to engage significant computational power to tackle intricate mathematical challenges.
2. Within a PoW network, miners possessing the highest hashrate wield greater influence over the network, which may result in centralization.

2. PoS (Proof of Stake):

An alternative approach to Proof of Work (PoW) is Proof of Stake(POS). Initially proposed by Sunny King and Scott Nadal in 2012, it addresses the

significant energy consumption associated with Bitcoin mining. In a Proof of Stake (PoS) system, miners contribute a portion of their coins as a stake, which allows them to participate in the addition of new transaction blocks. The likelihood of a participant being able to add new blocks increases with the amount of coins they have staked. Upon successfully mining new blocks, each miner is rewarded with both the block reward and a share of the transaction fees. The introduction of the concept of coin age serves to address the issue of stake size within PoS [6] . In this framework, validators replace miners, as seen in PoW [12]. For instance, if an individual holds 15 coins for a duration of 25 days, their coin age would total 375. When a node successfully creates a new block, its coin age resets to zero. The relevant formula is: proofhash < currency age * target. The PoS consensus algorithm can randomly select miners for block creation, ensuring that no miner can anticipate their turn. This mechanism also mitigates the monopoly concerns associated with PoW. Furthermore, the algorithm is designed to be resilient against 51% attacks, which could occur if validators engage in fraudulent verification processes. Cryptocurrencies such as Decred, Ethereum (upcoming), and Peercoin utilize PoS as their consensus mechanism.

Advantages
1. PoS necessitates that validators merely hold cryptocurrency, rendering it more environmentally sustainable and cost-effective.
2. PoS fosters decentralization.

Disadvantage
A notable concern with PoS is the potential for a rich-get-richer dynamic, where validators with larger stakes accumulate more cryptocurrency, thereby complicating participation for smaller validators within the network.

3. Delegated Proof-of-Stake (DPoS)
Certain blockchain networks implement a consensus mechanism known as Delegated Proof of Stake (DPoS) to facilitate transaction approval and the addition of new blocks to the blockchain. In this system, a limited number of validators, commonly referred to as delegates or witnesses, are employed to authenticate transactions and extend the blockchain. Token holders within a DPoS framework elect these delegates to represent them in the validation process. The responsibilities of the delegates include the incorporation of new blocks into the blockchain and the verification of transactions. Their incentives to maintain integrity are heightened by the risk of losing both their rewards and their positions should they engage in malicious activities or endorse fraudulent transactions.

Advantage
1. The DPoS model allows only the selected delegates to engage in the validation process, resulting in enhanced speed and efficiency.
2. Token holders in a DPoS environment have the opportunity to influence the selection of delegates, potentially fostering a more decentralized network.

Disadvantage
A notable concern regarding DPoS is the potential for power to become concentrated among a limited number of delegates. If a small faction of delegates possesses a substantial share of voting power, there exists the risk of collusion to manipulate the network.

4. Leased Proof of Stake (LPoS):
Certain blockchain networks utilize a consensus mechanism referred to as Leased Proof of Stake (LPoS) to validate transactions and add new blocks to the blockchain. In this system, smaller token holders can engage in the validation process by leasing their tokens to larger validators. This approach allows them to participate in LPoS, which is a variation of the traditional Proof of Stake (PoS) model. In LPoS networks, token holders lease their tokens to validators, who then leverage these tokens to enhance their stake, thereby increasing their likelihood of being selected to append new blocks and validate transactions. In addition to keeping ownership of the tokens they have leased, token holders get a fraction of the rewards produced by the validators, which is based on how many tokens they have leased.

Advantages
A significant advantage of LPoS is that it enables smaller token holders to engage in the validation process and earn rewards without the necessity of possessing a large number of tokens. This feature fosters decentralization and encourages a more varied participant base within the network. 2. Additionally, LPoS has the potential to enhance the overall security of the network.

Disadvantage
A notable disadvantage of LPoS is its complexity compared to other consensus algorithms. Token holders need to comprehend the associated risks and rewards of leasing their tokens to a validator, while validators are required to manage the leased tokens responsibly.

5. Proof of Authority (PoA)
Certain blockchain networks implement a consensus mechanism known as Proof of Authority (PoA) to validate transactions and add new blocks to the blockchain. Unlike other consensus methods such as Proof of Work (PoW) and Proof of Stake (PoS), which rely on a decentralized network of nodes, PoA is predicated on a select group of trusted validators. These validators are in charge of block addition and transaction validation in a PoA framework.
Their selection is typically based on their expertise and established reputation, which incentivizes them to maintain integrity, as their credibility is on the line.

Advantages:
1. A primary advantage of PoA is its enhanced efficiency compared to other consensus mechanisms.
2. Additionally, PoA is often more appropriate for private or enterprise-level blockchain networks.

Disadvantage:
A notable disadvantage of PoA is its comparatively lower security relative to other consensus algorithms. The reliance on a limited number of validators increases the network's susceptibility to attacks, particularly if any of the validators are compromised or engage in malicious behavior.

6. Proof of Elapsed Time (PoET)
Intel developed the Proof of Elapsed Time (PoET) consensus algorithm specifically for permissioned blockchain environments. The primary aim of PoET is to offer a more secure and energy-efficient alternative to the traditional Proof of Work (PoW) mechanisms utilized in public blockchains, such as Bitcoin. PoET functions similarly to a lottery in that each player is given a waiting period at random.
The individual who completes their wait time first earns the privilege to initiate the next block, leading to a competitive environment among participants. This process is commonly referred to as "leader election."

Advantage:
One of the key strengths of PoET is its high level of security. The random assignment of wait times makes it exceedingly challenging for any single participant or coalition of participants to exert control over the network.

Disadvantage:
However, a notable limitation of PoET is its dependency on Intel's hardware, which may restrict its broader adoption. Furthermore, as PoET is tailored for permissioned networks, it may not be appropriate for public blockchains that allow unrestricted participation.

IV CONCLUSION

Selecting the most suitable consensus algorithm is critical in the development of a blockchain network. Each consensus mechanism provides its own advantages and disadvantages, and an inappropriate choice can significantly impact the network's performance, decentralization, and security. Therefore, it is essential to evaluate the specific requirements of the blockchain application and consider factors such as scalability, efficiency, security, and decentralization. A carefully chosen consensus algorithm can yield numerous benefits, including improved decentralization, quicker transaction processing, enhanced efficiency, and greater security. Conversely, an ill-suited consensus algorithm may result in less secure transactions, higher costs, and slower processing times. The choice of consensus algorithm ultimately determines the success of a blockchain application, so choosing wisely is essential. Staying updated and informed is crucial for making the best choice for each unique blockchain application.

REFERENCE

[1] B. K. Mohanta, D. Jena, S. S. Panda and S. Sobhanayak, Blockchain technology: A survey on applications and security privacy challenges, 2019. https://doi.org/10.1016/j.iot.2019.100107.
[2] https://www.jaroeducation.com/blog/cryptocurrency-market-guide/

[3] S. Nakamoto et al., Bitcoin: A peer-to-peer electronic cash system, 2008.
[4] https://www.fool.com/terms/b/blockchain/
[5] S. Zhanga and J.-H. Lee, Analysis of the main consensus protocols of blockchain, https://doi.org/10.1016/j.icte.2019.08.001, 2019.
[6] S. J. Alsunaidi and F. A. Alhaidari, A Survey of Consensus Algorithms for Blockchain Technology, 2019, ICCIS, pp. 1-6, 2019.
[7] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei and C. Qijun, A review on consensus algorithm of blockchain, ICSMC), (2007), 2567-2572
[8] Kebira Azbeg, Ouail Ouchetto, Said Jai Andaloussi, "An Overview of Blockchain Consensus Algorithms: Comparison, Challenges and Future Directions", Oct 2020, October 2020, Advances in Intelligent Systems and Computing, DOI:10.1007/978-981-15-6048-4_31
[9] Viktoriia zhebka, Serhii Zhebka, Tetiana Bazhan, "Methodology for Choosing a Consensus Algorithm for Blockchain Technology", April 2024, Conference: Digital Economy Concepts and Technologies, At: Kyiv, Ukraine.
[10] C. Gupta and A. Mahajan, "Evaluation of Proof-of-Work Consensus Algorithm for Blockchain Networks," 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2020, pp. 1-7, doi: 10.1109/ICCCNT49239.2020.9225676.
[11] M. Swan, Blockchain: Blueprint for a New Economy (O'Reilly Media, Newton, MA, USA, 2015); A.M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies (O'Reilly Media, Newton, MA, USA, 2014)
[12] F.B. Crane, Proof of work, proof of stake and the consensus debate. Cointelegraph, 20 Dec. 2014. https://www.cointelegraph.com/news/proof-of-work-proof-of-stake-and-the-consensusdebate
[13] Sriman, B. & Kumar, s & Prabakaran, Shamili. (2020). Blockchain Technology: Consensus Protocol Proof of Work and Proof of Stake. 10.1007/978-981-15-5566-4_34.
[14] S. M. S. Saad, R. Z. R. M. Radzi and S. H. Othman, "Comparative Analysis of the Blockchain Consensus Algorithm Between Proof of Stake and Delegated Proof of Stake," 2021 International Conference on Data Science and Its Applications (ICoDSA), Bandung, Indonesia, 2021, pp. 175-180, doi: 10.1109/ICoDSA53588.2021.9617549.
[15] Qian Hua , Biwei Yanb, Yubing Hana , Jiguo Yua,c,d , "An Improved Delegated Proof of Stake Consensus Algorithm", International Conference on Identification, Information and Knowledge in the internet of Things, 2020, Procedia Computer Science 187 (2021) 341–346
[16] Yang, Fan & Zhou, Wei & Wu, Qingqing & Long, Rui & Xiong, Naixue & Zhou, Meiqi. (2019). Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism. IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2935149.
[17] S. Islam, M. J. Islam, M. Hossain, S. Noor, K. -S. Kwak and S. M. R. Islam, "A Survey on Consensus Algorithms in Blockchain-Based Applications: Architecture, Taxonomy, and Operational Issues," in *IEEE Access*, vol. 11, pp. 39066-39082, 2023, doi: 10.1109/ACCESS.2023.3267047.