Comparative Study of Blockchain Consensus Algorithms in Cryptocurrency

Nishitha Mohanan[1], Sudha D[2]

[1]PG Scholar, Dept. of Master of Computer Application, SCMS School of Technology and Management,Mutton, India , Email: ca-631@scmsgroup.org

[2]Assistant professor, Dept. of Computer Applications, SCMS School of Technology and Management, Mutton, India, Email: sudha@scmsgroup.org

ABSTRACT: Blockchain technology serves as a cornerstone for various cryptocurrencies, with current research primarily focusing on its security aspects due to its inherent qualities such as stability, immutability, security, and decentralization. Similar to other distributed systems, Blockchain relies on consensus algorithms to achieve agreement and safeguard its network. In recent years, diverse consensus algorithms have emerged within the Blockchain ecosystem, playing a pivotal role in upholding the security and integrity of distributed networks in blockchain technology. These algorithms are fundamental in maintaining trust within the blockchain technology realm. They can be categorized into two types: proof-based and voting-based. This paper presents some of the prominent consensus algorithms from these two categories while scrutinizing their respective strengths, weaknesses, and the specific types of blockchains to which these algorithms are applicable.

Keywords—Blockchain, consensus algorithm, PoS, Pow, DPoS, PBFT

I. INTRODUCTION

In 2008, an individual using the pseudonym Satoshi Nakamoto introduced the original concept of blockchain technology. Nakamoto applied this technology to create the first cryptocurrency, known as Bitcoin, and its associated distributed ledger. Subsequently, various other cryptocurrencies emerged, all built upon the blockchain technology. Traditional transaction processing systems rely on a central authority to oversee and process all transactions within the system. However, this centralized approach can introduce numerous issues, such as concerns regarding data privacy, security, and system efficiency. Blockchain technology, with its decentralized nature, has become a significant area of research in many fields, particularly in data privacy and security.

Cryptocurrency can be viewed as a digital asset that facilitates transactions between untrusted parties without the need for an intermediary entity like a bank. Conducting transactions within such a distributed system, where parties may not fully trust one another, necessitates a system that can establish trust among otherwise untrusted participants. Consensus algorithms in blockchain-based cryptocurrency systems ensure that only valid transactions are accepted within the system, while invalid ones are rejected.

The consensus mechanism stands as the fundamental pillar of blockchain and serves as a crucial assurance of the security of the blockchain system. As a decentralized system, blockchain relies on the consensus mechanism to enable thousands of nodes dispersed globally to reach an agreement on the creation of blocks. In essence, the blockchain consensus mechanism represents an algorithm for achieving distributed consensus on blockchain transactions. Commonly employed consensus mechanisms for public blockchain networks include

Proof of Work (POW), Proof of Stake (POS), Delegated Proof of Stake (DPOS), Practical Byzantine Fault Tolerance (PBFT), among others.

The rest of the paper is organized as follows. Section II presents an overview of the Blockchain technology . Section III discusses analysis of different consensus algorithm. Section IV gives a comparative study as findings. Finally in section V summarizes the work presented in this paper.

II. OVERVIEW ON BLOCKCHAIN TECHNOLOGY

In [1], the author asserts that the genesis of Blockchain technology can be traced back to 1991 when Haber and Stornetta conceived a solution geared towards safeguarding electronic documents. This solution hinged on the principles of timestamping and the interlinking of document hashes, thus establishing an incorruptible system. However, it wasn't until 2008 that Blockchain gained widespread recognition, thanks to its inaugural application in the form of Bitcoin. This revolutionary technology, spearheaded by Satoshi Nakamoto, underpinned the creation of the very first cryptocurrency.

Blockchain, therefore, represents a versatile technology that concurrently offers storage and data transmission capabilities. It operates on a peer-to-peer network architecture, facilitating transparent and secure communication between nodes, all without the necessity of a central controlling authority. Each node within this network maintains a copy of the database, also referred to as the ledger. Data is systematically organized into blocks, with each block intricately linked to its predecessor through a cryptographic hash.

In [3], the author delves into the five fundamental components that constitute blockchain technology: a peer-to-peer network, a distributed ledger, cryptographic mechanisms, consensus protocols, and smart contracts.

Within the realm of blockchain, three distinct types have emerged: public or permissionless blockchain, private or permissioned blockchain, and consortium blockchain. These categories primarily differ in terms of the rights and abilities granted for reading, writing, and validating blocks.

Public blockchain, the first type, finds its prominent use in cryptocurrencies like Bitcoin and Ethereum. It offers open access to anyone interested in joining the network, allowing them to read and write on the ledger while actively participating in the consensus process. Conversely, the second type, private blockchain, operates under the authority and control of a single entity. To gain entry into the network and partake in the consensus process, nodes necessitate permission from this overseeing authority. The third type represents a hybrid, combining elements from both public and private blockchains. In this scenario, multiple organizations collectively oversee the consensus process, as opposed to a singular authority.

In [6], the author explores the pivotal role of consensus algorithms within the realm of blockchain technology. These algorithms serve as the linchpin for blockchain networks, facilitating agreement among a multitude of dispersed nodes.

A consensus mechanism, such as Proof of Work (PoW) or Proof of Stake (PoS), assumes the mantle of guardian for the network, thwarting any attempts by unauthorized users to validate detrimental transactions. Importantly, these mechanisms orchestrate consensus within the network, even in the absence of a centralized authority. They wield the authority to dictate how transactions are authenticated and appended to the blockchain, thus ensuring the trifecta of security, decentralization, and scalability, each executed through distinct methodologies.

Every algorithm comes with its unique strengths and compromises, and the selection of a consensus mechanism hinges on several factors such as security prerequisites, scalability objectives, energy conservation considerations, and the precise objectives of the cryptocurrency venture.

A consensus algorithm serves as the pivotal mechanism enabling the blockchain to authenticate and affirm transactions and operations, effectively sidelining the necessity for an external third-party intermediary. The consensus algorithm takes on the pivotal role of determining which block should be

appended next to the blockchain. Furthermore, it acts as a robust defence mechanism, warding off potential disruptions, tampering attempts, or interference from rogue nodes within the blockchain network.

III. LITERATURE REVIEW

ANALYSIS OF DIFFERENT CONSENSUS ALGORITHM

Consensus, at its core, signifies the attainment of a unanimous agreement among all participating nodes or blocks within the blockchain network. It serves as the beating heart of the blockchain network. Through the application of consensus algorithms, blockchain engenders trust and reliability among the anonymous nodes in the realm of distributed computing. Essentially, these consensus algorithms act as sentinels, safeguarding the distributed ledger's integrity against any potential tampering by malicious actors.

Broadly speaking, in the realm of blockchain applications, we grapple with two fundamental challenges: double spending and the Byzantine General's problem. Double spending, in essence, involves the surreptitious reuse of coins in two separate transactions concurrently. In the blockchain domain, this predicament is averted by necessitating transaction validation from all participating nodes in the network.

Conversely, the Byzantine General's problem unfolds as a scenario where participating nodes must harmonize on a singular strategy to avert total system failure. However, this conundrum is exacerbated by the presence of corrupt nodes disseminating false information or displaying unreliability. In this section, we acquaint ourselves with some of the primary consensus algorithms in the blockchain arena.

A. Proof of Work (Pow)

Satoshi Nakamoto initially introduced Proof-of-Work (PoW) as an integral component of the Bitcoin cryptocurrency system, a process commonly known as mining, where the participating entities are referred to as miners. PoW serves as the prevailing consensus algorithm employed within the open and permissionless Bitcoin network.

The fundamental purpose of PoW is to substantiate to the network server that nodes within the network have indeed engaged in computational work. The network server presents challenges to the nodes in the form of tasks, including sequences of cryptographic hashes, computational puzzles, or various mathematical problems that necessitate resolution by the network's nodes. These nodes diligently perform the requisite computations and subsequently furnish their solutions to the network server. As a token of appreciation for their computational efforts, the network server rewards those nodes that have successfully computed the accurate solutions.

It is worth noting that the Proof of Work mechanism extends its utility beyond Bitcoin, finding application in multiple other cryptocurrencies, including but not limited to Litecoin, ZCash, Primecoin, Monero, and Vert coin, among others.

- *Pros & cons*

Main advantages of this algorithm are its high degree of decentralization, which enhances transparency and resilience by distributing control. The system's security is a standout feature, fortified by advanced cryptography and consensus mechanisms, establishing trust and data integrity. Moreover, its impressive scalability renders it versatile for diverse applications, accommodating growing user numbers and transaction volumes.

However, the algorithm's prominent drawback lies in its high energy consumption, which raises environmental concerns. Furthermore, the system's long confirmation times could prove limiting for real-time transactional requirements. Lastly, its decentralized nature, while a strength, also exposes vulnerabilities to potential malicious actors who exploit the absence of a central authority.

B. Proof of Stake (PoS)

Proof of Stake (PoS) stands out as a fundamental and environmentally-conscious alternative to the PoW consensus protocol. This innovative algorithm made its debut in 2012, courtesy of Sunny King and Scott Nadal. It effectively addresses the significant energy consumption issues associated with Bitcoin mining.

In the PoS mechanism for introducing new transactional blocks, each individual miner invests a portion of their coins as a stake in the system's currency. The number of coins at stake directly corresponds to the number of participants capable of adding fresh blocks to the blockchain. Each miner receives rewards in the form of new blocks and a share of the transaction fees, a remuneration based on their stake in the system.

PoS networks inherently boast a higher degree of decentralization when compared to PoW networks. Furthermore, they incorporate a concept known as "shredding" to enhance network scalability. Notably, cryptocurrencies like Ether, NXT, and Peercoin have adopted the PoS consensus algorithm to govern their operations.

- *Pros & cons*

Main advantages of this algorithm are its higher speed, lower energy consumption, and resource efficiency. The streamlined nature of the algorithm leads to quicker processing, reduced energy usage, and optimal resource utilization.

However, notable disadvantages of this algorithm include poor security due to complex implementation rules that can inadvertently create security vulnerabilities. Additionally, the algorithm's tendency to favour the wealthy can result in a "rich get richer" scenario where only the wealthiest participants gain control of the consensus, potentially undermining the system's democratic ideals.

C. *Delegated Proof of Stake (DPoS)*

A variant of the Proof of Stake (PoS) concept, originally proposed by Daniel Larimer, introduces a novel approach known as Delegated Proof of Stake (DPoS). DPoS relies on a reputation system and employs an election process to establish decentralized voting within the network. The core concept revolves around the selection of a group of delegates, also referred to as witnesses, tasked with safeguarding the network on behalf of other shareholders. These delegates take turns in a randomized fashion to create blocks.

In the event that a delegate encounters difficulties in appropriately generating a block, it incurs a loss to its reputation. Consequently, shareholders possess the option to retract their votes in favour of the affected delegate and, subsequently, replace it with another delegate deemed more reliable.

DPoS has gained traction in various iterations across several blockchain platforms, including Bit Shares, EOS, and Lisk, each implementing its unique version of the DPoS consensus mechanism.

- *Pros & cons*

Main advantages of this algorithm include its simplicity and efficiency, which contribute to streamlined processes. The algorithm's resource-saving nature leads to optimal resource utilization and its high scalability ensures seamless expansion to accommodate growing demands.

However, significant disadvantages of this algorithm are its susceptibility to failures caused by bribery within the main network, potentially undermining its integrity. Additionally, the algorithm's weak degree of decentralization can compromise its ability to withstand centralized control and potential vulnerabilities associated with such control.

D. *Practical Byzantine Fault Tolerance (PBFT)*

The Practical Byzantine Fault Tolerance (PBFT) algorithm, introduced by Castro and Liskov, addresses the critical issue of handling one or more nodes within a network that turn faulty and engage in malicious behaviour. Such malfeasance disrupts the smooth communication among all nodes connected to the network, leading to operational delays. In our context, time is of utmost importance, especially in an asynchronous system, where even a single fault occurrence can render the consensus problem unsolvable. Additionally, it introduces discrepancies in the responses received from various nodes.

It's essential to note that PBFT is tailored for a permissioned model. Within the Practical Byzantine Fault Tolerance framework, state machine replication is carried out across multiple nodes. The client's operation involves waiting for responses from n + 1 nodes, where n represents the number of faulty nodes. However, this approach encounters limitations as n + 1 cannot definitively ascertain the majority vote on behalf of the client. PBFT is designed to function effectively in an asynchronous system, navigating the challenges posed by such an environment.

- *Pros & cons*

Main advantages of this algorithm include its higher performance, delivering efficient processing speeds. The algorithm also boasts high security measures, incorporating advanced cryptographic techniques to ensure data integrity and user protection. Furthermore, the concept of finality within the algorithm adds an extra layer of certainty to transactions.

However, significant disadvantages of this algorithm are its weak degree of decentralization, which can impact its resistance to centralized control and decision-making. The closed node system further restricts participation and transparency, potentially limiting the diversity of the network. Additionally, the algorithm's low fault tolerance could lead to a reduced ability to handle errors and disruptions effectively.

IV. FINDINGS

The initial parameter we scrutinize relates to the computational resources required, as network nodes expend their computational power when appending data to a blockchain, earning cryptocurrency rewards in return. According to [11], it is posited that Proof of Work (PoW) necessitates the highest computational power, while Delegated Proof of Stake (DPoS) mandates the least. This distinction confers a substantial advantage upon DPoS over other algorithms in this regard.

Another pivotal parameter affecting network performance is the number of nodes engaged in the validation process for confirming the legitimacy of proposed blocks. In the context of these algorithms, only DPoS operates with a predetermined fixed set, typically around 20 nodes, while Proof of Stake (PoS) and Proof of Work (PoW) rely on the entire network.

A greater number of nodes participating in the validation process is synonymous with heightened network decentralization and, consequently, increased security. In this light, it is discerned that PoW and PoS tend to foster higher degrees of decentralization compared to DPoS.

In [14], the topic of decentralization is explored further. Decentralization and scalability are often regarded as fundamental attributes of a blockchain network. It is noteworthy that highly scalable networks often exhibit limited decentralization, with PoS being a notable exception, where the balance between the two tends to be more equitable.

PoS operates within a permissionless network, markedly distinct from PoW in terms of energy consumption. PoS boasts significantly reduced block creation times, approximately 1 minute, and commendable throughput. For instance, Peercoin effectively leverages PoS.

On the other hand, the practical Byzantine Fault Tolerance (pBFT) consensus algorithm finds its niche in permissioned networks, characterized by a more centralized structure. This setup facilitates rapid block creation and expedites transaction settlement, often within seconds.

Each of the aforementioned algorithms bears its own set of advantages and drawbacks. Therefore, the process of selecting an appropriate algorithm must be approached with meticulous consideration, tailored to the specific use case that a given blockchain seeks to address.

The comparison of consensus algorithms is given in Table 1.

Features	PoW	PoS	DPoS	PBFT
Type of blockchain	Permissio n less	Permis sioned & permis sion less	Permis sioned & permiss ion less	Permissi oned
Decentralization structure	Strong	Strong	Strong	Weak
Electing miners based on	Solving difficulty hash	Stake owned	Stake owned	Mathe matical operation
Reward	Yes	Yes	Yes	No
Speed of verification	Greater than 100 sec	Less than 100 sec	Less than 100 sec	Less than 10 sec
Speed of block creation	Low	High	High	High
Consumption of energy	High	Less than PoW	Low	Moderate
Scalability	Strong	Strong	Strong	Weak
Fees of transaction	For all miners	For all miners	For all miners	No
Properties of distributed consensus	Probabili stic	Probab ilistic	Probabi listic	Determi nistic
Crash fault tolerate	50%	50%	50%	33%
Byzantine fault tolerance	50%	50%	50%	33%

V. CONCLUSION

Blockchain technology, initially conceived as the foundational framework behind Bitcoin, the world's largest cryptocurrency, has found versatile applications across various domains, owing to its distinctive attributes. Notably, cryptocurrency represents a highly critical and sensitive manifestation of Blockchain technology, characterized by stringent requirements for security, expeditious transaction processing, and unwavering reliability. To address these imperatives, consensus algorithms play a pivotal role in reinforcing security within Blockchain-based cryptocurrency systems.

However, it's essential to acknowledge the divergence among cryptocurrencies, with some being computationally intensive and energy-demanding, while others exhibit varying degrees of centralization. The realm of consensus algorithms offers a plethora of choices, each tailored to specific use cases. In essence, the selection of a particular consensus algorithm hinges upon the unique requirements of the application. Broadly speaking, the ideal features sought in a consensus algorithm for cryptocurrency systems encompass permission lessness, energy efficiency, rapid transaction processing with minimal latency, and robust security.

Within this paper, we have provided a comprehensive overview of Blockchain technology, delving into Blockchain-based cryptocurrency systems, and have expounded upon the diverse consensus algorithms employed within these systems.

REFERENCES

[1]Kevin Wang, Cristiano Bellavitis, Carlos M. DaSilvaAn "Introduction to Blockchain, Cryptocurrency and Initial Coin Offerings" 2018

[2]Bashar Ibrahim" Blockchain and Cryptocurrencies Technology: a survey"2019

[3]Stephen Chan,Jeffrey Chu,Yuanyuan Zhang,Saralees Nadarajah "Blockchain and Cryptocurrencies"2020

[4]Cheick Tidiane Ba, Matteo Zignani, Sabrina Gaito "The role of cryptocurrency in the dynamics of blockchain-based social networks"2022

[5]Ahmed G Gad,Diana T Mosa, Laith Abualigah,Amr A Abohany " Emerging Trends in Blockchain Technology and Applications: A Review and Outlook" 2021

[6]Munish Sabharwal, Fayzullo Makhmadiyarovich Nazarov, Bunyod Eshtemirov "Effectiveness Analysis of Blockchain Mechanisms Using Consensus Algorithms"

[7]Xuesen Zhang, Qinglei Guo, Xiaoxiao Ma, Zhe Du, Shuang Sun, Desheng Bai" Research on blockchain consensus algorithm for large-scale high-concurrency power transactions" 2022 9th International Forum on Electrical Engineering

[8]Kebira Azbeg, Ouail Ouchetto, Said Jai Andaloussi, and Laila Fetjah" An Overview of Blockchain Consensus Algorithms: Comparison, Challenges and Future Directions"

[9]Qianwen Wang et al 2020" A Study of Blockchain Consensus Algorithms"

[10] Sharvani G. S.; Ruquiya Anjum" A Brief on Blockchain and cryptocurrency system" 2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)

[11] Harshini Pooja K, Ganesh Kumar S" Evolution of Consensus Algorithms in Blockchain Technology"

[12] Rameez Yousuf, Zubair Jeelani, Dawood Ashraf Khan, Owais Bhat and Tawseef Ahmed Teli" Consensus Algorithms in Blockchain-Based Cryptocurrencies"

[13] S. J. Alsunaidi and F. A. Alhaidari, A Survey of Consensus Algorithms for Blockchain Technology, 2019, ICCIS, pp. 1-6, 2019.

[14] Jannah Yusoff1, Zarina Mohamad1, Mohd Anuar2" A Review: Consensus Algorithms on Blockchain"

[15] Dejan Vujičić, Dijana Jagodić, Siniša Ranđić , Faculty of Technical Sciences in Čačak University of Kragujevac Čačak, Serbia" Blockchain Technology, Bitcoin, and Ethereum: A Brief Overview"

[16] Kevin Wang, Cristiano Bellavitis, Carlos M. DaSilvaAn "Introduction to Blockchain, Cryptocurrency and Initial Coin Offerings" 2018