Comparative Analysis of Blockchain Consensus Algorithms

Zhihao Lin

School of Computer & Communication Engineering, University of Science and Technology Beijing, Beijing, 100083, China
u202141838@xs.ustb.edu.cn

Abstract. Over the past decade, blockchain technology has undergone remarkable growth, largely driven by its versatility across various applications, which has garnered significant attention from multiple sectors. This technology has facilitated the shift from traditional, centralized ledgers controlled by single entities to decentralized, trustworthy systems managed collaboratively by numerous participants. This transformation has notably increased the complexity and criticality of achieving consensus within blockchain networks, a challenge commonly referred to as the "consensus problem." Consensus algorithms are crucial for maintaining the operational efficacy of blockchain frameworks. This paper presents a comprehensive review of prevalent consensus algorithms and introduces a structured set of criteria for their assessment and comparison. These criteria are categorized into three primary groups: Performance, Scalability, and Security. Employing the proposed evaluation framework, this research conducts an extensive examination and comparison of the specific advantages and disadvantages associated with each consensus algorithm. This endeavor not only aids in the development and enhancement of robust blockchain architectures but also establishes a clear pathway for future academic inquiry into this dynamic field.

Keywords: Blockchain, Consensus algorithm, Metrics, Evaluation framework.

1 Introduction

Blockchain technology, originally developed for Internet finance, emerged as a decentralized, immutable ledger designed to mitigate the risks associated with commercial transactions. It has since become one of the most significant technological breakthroughs, heralding a promising future. This decentralized system provides transparent and secure record-keeping. Over recent years, its applications have broadened to include supply chain management, healthcare, and privacy protection, attracting attention from government and industry leaders due to its extensive utility and transformative potential.

Blockchain was first conceptualized by researchers but only achieved widespread adoption after Satoshi Nakamoto introduced Bitcoin in 2008. Bitcoin addressed trust

Y. Wang (ed.), *Proceedings of the 2024 2nd International Conference on Image, Algorithms and Artificial Intelligence (ICIAAI 2024)*, Advances in Computer Science Research 115,
https://doi.org/10.2991/978-94-6463-540-9_28

issues inherent in conventional payment systems, which relied heavily on centralized third parties often criticized for potential exploitation and deception of consumers [1]. The central problem was the centralization of verification processes under a single entity, creating significant trust deficits [2]. The proposed solution shifted from centralized to decentralized verification, where multiple independent entities confirm transactions, significantly altering the digital transaction landscape by diminishing the trust issues associated with centralized systems. Achieving consensus in distributed systems through the validation of transactions by multiple independent organizations is managed via specific mechanisms known as consensus algorithms. The complexity of these systems is exemplified by the Byzantine Generals' Problem, which illustrates the challenge of reaching unanimous agreement among multiple autonomous parties despite potential misinformation [3]. In blockchain, which operates without a central authority, reaching consensus is crucial. The decentralized nature of blockchain necessitates a consensus mechanism that ensures a tamper-proof environment where all nodes agree on a consistent truth. Consequently, consensus algorithms are vital for maintaining the integrity and uniformity of blockchain's distributed framework.

Selecting the appropriate consensus algorithm is crucial for developing blockchain solutions, given the diversity of available options, each with unique advantages and disadvantages. This variety creates a complex landscape that can be daunting and error-prone when selecting the most suitable consensus algorithm for specific applications. This paper provides an extensive review and comparative analysis of major blockchain consensus algorithms, highlighting their strengths and weaknesses. It introduces a comparison framework based on Performance, Scalability, and Security, designed to optimize and refine blockchain systems. This structured approach aims to guide the selection of consensus algorithms effectively.

The paper is organized as follows: Section 2 defines blockchain technology and discusses its operational mechanisms, including a review of studies on blockchain consensus algorithm design and analysis. Section 3 provides an overview, analysis, and comparison of well-known blockchain consensus algorithms, introducing the proposed comparative framework. Section 4 explores the challenges faced by consensus algorithms and suggests directions for future research. Section 5 offers a critical evaluation of the study. Section 6 concludes the paper with final observations and insights.

2 Relevant Theories

2.1 Definition of Blockchain

Blockchain is a decentralized, distributed database that consists of a sequence of blocks linked together in a chain-like manner [4]. As depicted in Fig. 1, every block on the blockchain contains three primary components: the data, the hash value, and the hash value of the previous block. Each block's distinct hash value encodes its information, anchoring the block securely within the blockchain's immutable ledger. The inclusion of the previous block's hash in each subsequent block ensures the continuity and

interconnectedness of the blockchain structure. Hash values represent not only the transactional information in each block but also its sequential position within the chain. Owing to the characteristics of hash functions, any modification of a block's data results in a change in its hash value, thus maintaining the blockchain's integrity and immutability [5].

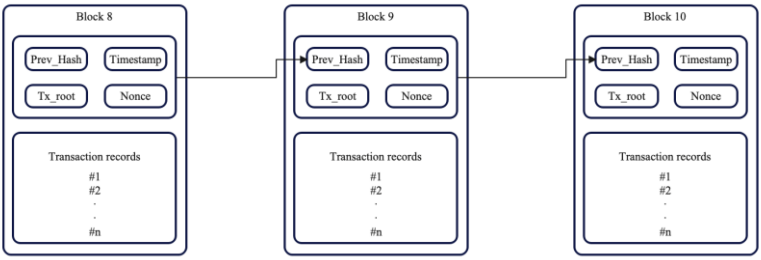

Fig. 1. The blockchain structure.

The Tx_ root, or Merkle root, is integral to blockchain technology, encapsulating the hash values of all verified transactions in a block. This root is produced through the Merkle tree function, a hierarchical data structure used to efficiently summarize and verify transaction integrity. As illustrated in Fig. 2, each transaction within a block is hashed into individual hash values. These values are then paired and hashed again. Iteratively repeating this method produces a single hash that is called the Merkle root [6]. This method enables swift and safe verification of large data sets, enhancing the blockchain's efficiency and security.

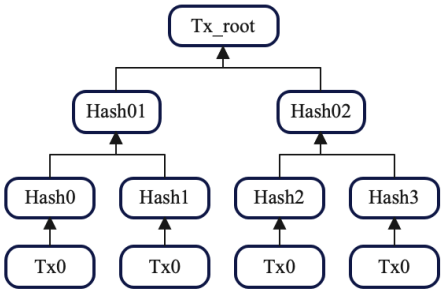

Fig. 2. An example of Merkle root.

2.2 Blockchain System

Modern blockchain systems differ in their applications and functionalities, generally falling into two categories: permissionless and permissioned blockchains [7]. These two distinct types of blockchains exhibit significant differences in their consensus mechanisms.

Permissionless blockchains are recognized for their decentralized nature, enabling anyone to engage in submitting and confirming transactions without the need for special permissions. To submit transactions, users must pay transaction fees. Furthermore,

every participant is allowed to verify transactions. In addition, all information within the blockchain system is accessible and made public to all network members.

Permissioned blockchains operate as a more centralized form of blockchain technology, where participation in the submission or verification of transactions is restricted [8]. To send transactions on these networks, users must obtain specific permissions.

Blockchain technology presents notable advantages over traditional distributed databases. Blockchain systems are designed to reduce both manual and time-related costs and operate independently of third-party intermediaries, thereby enhancing asset security. By utilizing robust consensus mechanisms, blockchain technology ensures verifiability and security, effectively eliminating the need for intermediaries. This addresses many of the challenges faced by traditional distributed databases, such as inefficiencies, vulnerabilities to fraud, and the high costs associated with managing and securing transactions.

2.3 Comparisons of Consensus Algorithms

Five well-known consensus algorithms are thoroughly compared in the paper referenced in reference: Practical Byzantine Fault Tolerance, Proof of Work, Delegated Proof of Stake, Proof of Stake, and Reliable, Replicated, Redundant, And Fault-Tolerant (RAFT). This analysis highlights their capabilities in terms of throughput, scalability, verification speed, and Byzantine and crash fault tolerance [9]. Reference provides a focused comparison and analysis of PoW, PoS, Byzantine Fault Tolerance (BFT), Proof of Elapsed Time (PoET), and Federated BFT, emphasizing qualitative performance metrics. Similarly, the reference research performs a qualitative evaluation of various hybrid consensus algorithms [10,11]. Additionally, reference explores PoW-based mechanisms compared with BFT state machine replication methods, paying special attention to the following aspects: energy consumption, resilience against adversaries, network synchronicity, consensus finality, scalability, operational efficiency, and node identity management [12]. Collectively, this body of work significantly enriches the discourse on consensus mechanisms, offering a wide range of analytical perspectives and evaluation criteria that help comprehend and improve blockchain's foundational structures.

Despite the extensive research conducted on consensus algorithms, a noticeable gap exists due to the absence of clear classification and selection criteria. To address this gap, this paper carries out a focused comparative analysis by collecting relevant data on cryptocurrencies that utilize specific consensus algorithms. The analysis is guided by evaluation criteria that include performance, scalability, and security. The objective is to develop a framework that facilitates the comparison of blockchain consensus algorithms. This framework is intended to serve as a reference, assisting stakeholders in making informed decisions about the most appropriate consensus algorithm for their specific blockchain application.

3 System Analysis and Comparison Research

This section examines the consensus algorithms that are frequently employed in blockchain networks in this section. The discussion and analysis focus on their benefits and drawbacks based on established evaluation criteria. Building on this analysis, an analytical and classification framework is proposed. This framework will help clarify the distinctions among different consensus algorithms and provide a systematic approach for evaluating their suitability for various blockchain applications.

3.1 Overview of Various Consensus Algorithms

Proof of Work. PoW stands as the most renowned consensus algorithm, introduced by Satoshi Nakamoto and employed within Bitcoin. Miners in the PoW must use a hash function to solve a mathematical puzzle in order to discover a nonce that satisfies certain conditions. This process is often referred to as mining [13].

$$H(x\ nonce) \leq D(h) \tag{1}$$

In essence, the task involves searching for a string, known as the nonce, such that when it is concatenated with a given string x, the Merkle root of the block, the hash value of this concatenation, as computed by the hash function $H()$, satisfies the condition of being less than a target value $D(h)$.

Upon discovering a nonce that meets the target criterion, a node broadcasts this block across the entire network. The block is added to the end of the blockchain when it has been validated by additional nodes.

Proof of Elapsed Time. PoET is a consensus mechanism created by Intel, which shares some procedural elements with Proof of Work (PoW) in that it involves each participant solving a problem [14]. Unlike PoW, which requires intensive computational effort to find a nonce, PoET gives each node a random waiting time. This waiting period is determined through a random number generator and is implemented within a Trusted Execution Environment (TEE) [15]. The node that receives the shortest designated waiting time is granted the right to publish the subsequent block. Following this selection, other nodes in the network are responsible for verifying that the newly proposed block is legitimate, thus maintaining the blockchain's accuracy and reliability.

Proof of Stake. PoS is a consensus mechanism that provides an option for the computationally intensive PoW. PoS introduces the concept of "coin age" as a critical element in determining who gets to construct the new block [16]. Coin age is calculated by multiplying the amount of cryptocurrency a participant holds by the length of time since those coins were last spent. In PoS, the process of selecting the creator of the next block is influenced by both the participant's stake—the quantity of cryptocurrency held—and the age of that stake. This selection is made through a pseudo-random process, which effectively ties the likelihood of creating the next block to both the

amount of the stake and the time it has been held. This mechanism aligns the incentives of blockchain participants with the network's overall longevity and security, reducing the energy demands associated with PoW systems.

Delegated Proof of Stake. DPoS builds upon the fundamental concepts of the PoS model by introducing a representative-based system. In DPoS, nodes cast votes to elect a limited number of witnesses—essentially representatives—based on the voting nodes' stake in the network [17]. These elected witnesses are tasked with the duty of adding new blocks to the blockchain and doing so in a scheduled round-robin manner. The DPoS system provides a mechanism for accountability and efficiency; if a witness does not produce a block within their assigned time or commits errors, the stakeholders can quickly respond by voting to replace them with a more reliable witness.

Proof of Activity. PoA is a consensus algorithm that merges features from both PoW and PoS [18]. In the PoA framework, the process begins like PoW, with miners competing to solve a challenging mathematical puzzle. When a miner successfully solves this problem, a set of validators is selected through a pseudo-random process that considers their stake in the cryptocurrency.

Proof of Importance. PoI assigns an "importance score" to each node, which serves as a more comprehensive measure of a node's value to the network than merely the amount of cryptocurrency it holds. This importance score is calculated not only based on the number of coins a node possesses but also takes into account the frequency and volume of the node's transactions. These transaction metrics are used to assess the node’s active participation and its contribution to the network’s overall health and growth [19]. Higher-importance nodes are given a better chance of being selected to create the next block.

Practical Byzantine Fault Tolerance. PBFT utilizes a voting process among nodes to establish fault tolerance within a network [20]. PBFT involves several stages in the creation process of a new block, with the key phase being the voting by all participating nodes. Each node engages in this vote, and a new block is deemed valid and successfully added only when it receives approval from over two-thirds of the network's nodes.

Delegated Byzantine Fault Tolerance. DBFT modifies the PBFT model by incorporating delegation elements akin to those in DPoS. In DBFT, a specific group of nodes, referred to as witnesses, are chosen via a voting mechanism to engage in the consensus and block creation processes.

3.2 Consensus Algorithms Evaluation Criteria

This section details the criteria used for evaluating and analyzing consensus algorithms in this paper, focusing on performance, scalability, and security.

Performance. Performance is a crucial aspect of blockchain networks, primarily reflected through its throughput, which is affected by various factors [21]:

Transactions per second (TPS) gauges the volume of transactions processed by the blockchain each second. A higher TPS suggests quicker block verification and confirmation times.

Block time denotes the duration required for transactions to be included in a block, from the moment they are broadcast to the network until consensus is achieved [22].

Block size specifies the maximum amount of transactions that can fit in a single block.

Scalability. Scalability is a critical issue for blockchain technology, reflecting the capacity of a blockchain network to manage an increasing volume of transactions efficiently as the network expands [23]. This capability is essential for blockchain applications that require processing a high volume of transactions, supporting a large user base, or executing complex business operations.

Security. In blockchain systems, double-spending attacks and 51% attacks represent the most prevalent security threats. These attacks not only jeopardize the security of funds but also affect user trust and system reliability, crucial factors for widespread adoption. A double-spending attack refers to an attacker successfully spending the same digital currency multiple times. On the other hand, a 51% attack happens when a single entity or group acquires more than half of the network's mining capacity, giving them the ability to interfere with the recording of new blocks and potentially reverse transactions to double-spend coins.

3.3 Comparative Analysis of Consensus Algorithms

In this segment, data regarding specific cryptocurrencies that utilize particular consensus algorithms has been compiled, as presented in Table 1. Additionally, based on the previously outlined evaluation criteria—Performance, Scalability, and Security—a focused comparative analysis is conducted.

PoW offers substantial benefits including robust security, a high level of decentralization, and considerable scalability. However, it also comes with significant drawbacks. The mining process in PoW is energy-intensive and demands substantial computational resources. This dependence on hardware capabilities results in lower throughput and elevated computational costs. Consequently, PoW may be less suitable for blockchain networks that need to process a large volume of transactions per second.

PoET provides a notable improvement over PoW by significantly reducing computational demands and energy consumption. It achieves a satisfactory level of

scalability and promotes fairness by ensuring that each participant has an equal opportunity to create a block. However, PoET also presents its own set of limitations. Its reliance on a Trusted Execution Environment (TEE) makes it highly dependent on specific hardware capable of supporting this feature, potentially limiting its applicability and raising concerns about the security and integrity of the TEE.

Table 1. Comparison of consensus algorithms based on representative cryptocurrencies.

Algorithm	Cryptocurrency	Transactions per second	Block time	Block size	Scalability	Vulnerabilities
PoA	Bitcoin	5	10m 50s	730.79 KBytes	Strong	51% Attack Double Spending attack
PoS	Ethereum	5	12.1s	112.69 KBytes	Strong	51% Attack Long-range attack
DPoS	EOS	2000	0.5m	NA	Strong	51% Attack Double Spending attack
PoA	DASH	0.17	2m 37s	17.45 KBytes	Strong	Double Spending attack
PoI	NEM	10000	1m	No fixed upper limit	Strong	Cyclic attacks
PBFT	Ripple	8	0.06m	No fixed upper limit	Low	Replay attack
DBFT	NEO	10000	0.25m	1KBytes	Medium	51% Attack Double Spending attack

PoS offers a distinct advantage over PoW by eliminating the need for solving complex hash problems, which reduces energy consumption and increases throughput. PoS also enables shorter block creation times and does not depend on specific hardware, enhancing operational efficiency. Still, while PoS may slightly lag in scalability compared to PoW if a single node or a small group of nodes gains a substantial share of the total cryptocurrency, it could lead to increased centralization, making it vulnerable to various attacks, including long-range attacks.

DPoS builds on the security features of traditional PoS by adding a democratic governance layer. In DPoS, the consensus process involves a voting mechanism that typically leads to enhanced efficiency, faster transaction processing speeds, and reasonable scalability. This system permits a more efficient and less energy-intensive block creation compared to the computationally heavy PoW and the wealth-

concentrating tendencies of PoS [22]. However, DPoS introduces a semi-centralized structure within the network. By limiting the number of witnesses who can produce blocks and concentrating this ability among a selected few, DPoS can inadvertently centralize power within a smaller group of nodes. Therefore, DPoS may be especially suitable for permissioned blockchains, where governance can be more tightly controlled and the potential centralization is less of a concern given the network's closed nature.

PoA combines the methodologies of PoW and PoS, reducing security vulnerabilities found in each when used alone. PoA significantly lowers the chance of a 51% attack, as attackers must overcome challenges in both mining and staking components. While it reduces energy consumption by limiting the number of miners, PoA still requires significant computational resources and human oversight, especially during mining. Additionally, incorporating elements of PoS makes PoA vulnerable to bribery-based attacks, like double-spending.

PoI employs several strategies to bolster its security and counteract Sybil attacks, where attackers create numerous fake identities to disproportionately influence the network. Unlike PoW, PoI doesn't involve solving complex mathematical problems, making it more energy-efficient and eliminating the need for specialized hardware. Additionally, PoI is scalable. However, despite these advantages, PoI can be vulnerable to cyclic attacks, where nodes may participate in artificial or illegitimate transactions to artificially boost their importance scores.

PBFT is highly effective in environments prone to Byzantine faults, managing to operate reliably even with up to one-third of the nodes being defective or malicious. This resilience ensures that the consensus regarding the blockchain's state is maintained securely and dependably. Another significant benefit of PBFT is its high throughput, which allows it to process a large volume of transactions efficiently once consensus is reached. However, PBFT necessitates extensive message exchanges among nodes to achieve consensus, involving multiple communication rounds. This extensive communication not only consumes significant network resources but also limits the system's scalability [23].

Delegated Byzantine Fault Tolerance (DBFT) reduces the communication overhead typical of traditional PBFT systems, thereby enhancing throughput and reducing latency in the consensus process, which in turn improves scalability. However, despite these advantages, DBFT faces potential challenges concerning network centralization, particularly if the number of witnesses involved is too small, which can centralize control and influence within the network [24].

Based on the analysis conducted, this paper introduces a comparative framework for blockchain consensus algorithms, which is detailed in Table 2.

This framework acts as a reference and guide to help in selecting suitable consensus mechanisms for different blockchain applications.

4 Discussion and Challenges

In the past few years, blockchain technology has extended its reach beyond the realm of digital cryptocurrencies, capitalizing on its high security, consistency, and decentralized characteristics to find utility in a variety of domains and scenarios. The essence of blockchain technology resides in its consensus algorithms, which are crucial for achieving agreement among network participants. There has been substantial research focused on analyzing these algorithms in terms of efficiency, scalability, security, and practical applicability.

Table 2. Comparison framework of blockchain consensus algorithm.

Consensus algorithms	Designing Goal	Decentralization level	Energy efficiency	Hardware dependency	Scalability	Vulnerability	Speed
PoW	Sybil-proof	Decentralized	No	Yes	Strong	51% Attack Double Spending attack	Slow
PoET	Fairness	Semi-centralized	Yes	No	Strong	51% Attack	Fast
PoS	Energy efficiency	Semi-centralized	Yes	No	Strong	51% Attack Long-range attack	Fast
DPoS	effective PoS	Semi-centralized	Yes	No	Strong	51% Attack Double Spending attack	Fast
PoA	Benefits of Pos and PoW	Decentralized	Yes	Yes	Strong	Double Spending attack	Medium
PoI	Improve PoS	Decentralized	Yes	No	Strong	Cyclic attacks	Fast
PBFT	Remove software errors	Decentralized	Yes	No	Low	Replay attack	Slow
DBFT	Faster PBFT	Semi-centralized	Yes	No	Medium	51% Attack Double Spending attack	Slow

Looking ahead, blockchain technology is set to expand into even broader applications. For example, blockchain-based cloud computing and artificial intelligence applications can leverage blockchain to enhance resource allocation efficiency significantly [25]. Furthermore, the integration of blockchain with smart grids could greatly facilitate the energy transition and boost energy efficiency [26]. These advancements are merely a glimpse of the potential uses of blockchain technology in various fields.

5 Critical Evaluation

5.1 Contributions

This paper establishes an analytical framework by systematically categorizing and comparing different consensus mechanisms, effectively evaluating each mechanism's performance in terms of security, efficiency, scalability, and decentralization. This framework offers developers and researchers clear guidance, facilitating the selection of the appropriate consensus algorithm tailored to specific application requirements. Adopting such an approach is crucial for designing blockchain systems that align precisely with the necessary functionalities and operational demands.

5.2 Limitations

This paper does not analyze, evaluate, or categorize several nonmainstream but effective consensus algorithms, nor does it cover variants of mainstream consensus mechanisms. Additionally, there is an opportunity to further explore and analyze the strengths and weaknesses of each algorithm within specific application scenarios and domains. Moreover, further research could be conducted to demonstrate the relevance of the evaluation criteria to practical applications, enhancing the framework's applicability and accuracy in guiding the selection of consensus algorithms tailored to real-world uses.

6 Conclusion

While this paper provides a robust evaluation framework and practical tools for comparing consensus algorithms, it omits an exploration of several non-mainstream but potentially impactful consensus mechanisms, as well as variations of established consensus methods. There is a considerable opportunity to deepen the exploration and analysis of each algorithm's strengths and weaknesses within specific application scenarios and domains. Furthermore, enhancing the relevance of the evaluation criteria to practical applications could significantly improve the framework's utility and precision in guiding the selection of consensus algorithms suited to real-world contexts. This would broaden its applicability and enhance its effectiveness in addressing distinct technological needs. The rapid evolution of blockchain technology underscores the significant potential for further exploration. Newly emerging consensus mechanisms

and their variants offer fresh opportunities for future research to assess their performance and security aspects. Moreover, exploring more complex scenarios, such as cross-chain operations and multi-chain integration, becomes increasingly important as blockchain technology seeks broader applicability. Additionally, given the global application of blockchain, future studies should also explore the adaptability and compliance of consensus mechanisms within various legal and cultural contexts. This broader perspective is crucial to ensure that blockchain technologies can be effectively and ethically integrated across diverse global environments, thereby facilitating their widespread adoption and utility.

References

1. S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system. (2008).
2. A. Lovejoy, The great chain of being: A study of the history of an idea, Routledge. (2017).
3. L. Lamport, R. Shostak, & M. Pease, The Byzantine Generals Problem, ACM Trans. Program. Lang. Syst., 4 (1982) 382-401.
4. M. Muzammal, Q. Qu, & B. Nasrulin, Renovating blockchain with distributed databases: An open source system, Future Gener. Comput. Syst., 90 (2019) 105-117.
5. M. Wang, M. Duan, & J. Zhu, Research on the Security Criteria of Hash Functions in the Blockchain, 47-55. (2018).
6. A. Mizrahi, N. Koren, & O. Rottenstreich, Optimizing Merkle Proof Size for Blockchain Transactions, 2021 International Conference on COMmunication Systems & NETworkS (COMSNETS), 299-307. (2021).
7. T. Neudecker & H. Hartenstein, Network Layer Aspects of Permissionless Blockchains, IEEE Communications Surveys & Tutorials, 21 (2019) 838-857.
8. D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, & C. Qijun, A review on consensus algorithm of blockchain, 2017 IEEE international conference on systems, man, and cybernetics (SMC), 2567-2572. (2017).
9. A. Baliga, Understanding blockchain consensus models, Persistent, 4(1) (2017) 14.
10. G.T. Nguyen & K. Kim, A survey about consensus algorithms used in blockchain, Journal of Information processing systems, 14(1). (2018).
11. M. Vukolić, The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication, Open Problems in Network Security: IFIP WG 11.4 International Workshop, iNetSec 2015, Zurich, Switzerland, October 29, 2015, Revised Selected Papers, 112-125. (2016).
12. X. Zhu, H. Xu, Z. Zhao, & others, An Environmental Intrusion Detection Technology Based on WiFi, Wireless Personal Communications, 119(2) (2021) 1425-1436.
13. M. Bowman, D. Das, A. Mandal, & H. Montgomery, On Elapsed Time Consensus Protocols, 559-583. (2021).

14. J. Lind, I. Eyal, F. Kelbert, O. Naor, P. Pietzuch, & E. Sirer, Teechain: Scalable Blockchain Payments using Trusted Execution Environments, ArXiv, abs/1707.05454. (2017).
15. H. Gurram, H. Mohamad, A. Sriram, & A. Endurthi, A Strategy to Improvise Coin-age Selection in the Proof of Stake Consensus Algorithm, 2023 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), 1-4. (2023).
16. F. Yang, W. Zhou, Q. Wu, R. Long, N. Xiong, & M. Zhou, Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism, IEEE Access, 7 (2019) 118541-118555.
17. Z. Liu, S. Tang, S. Chow, Z. Liu, & Y. Long, Fork-free hybrid consensus with flexible Proof-of-Activity, Future Gener. Comput. Syst., 96 (2019) 515-524.
18. V. Kuchkovsky, BLOCKCHAIN SYSTEM CONSENSUS ALGORITHMS, HERALD OF KHMELNYTSKYI NATIONAL UNIVERSITY. (2021).
19. X. Zheng & W. Feng, Research on Practical Byzantine Fault Tolerant Consensus Algorithm Based on Blockchain, Journal of Physics: Conference Series, 1802. (2021).
20. F. Ma & R. Fan, Queuing Theory of Improved Practical Byzantine Fault Tolerant Consensus, Mathematics. (2022).
21. C. Fan, S. Ghaemi, H. Khazaei, & P. Musílek, Performance Evaluation of Blockchain Systems: A Systematic Survey, IEEE Access, 8 (2020) 126927-126950.
22. C. Pinzón, C. Rocha, & J. Finke, Algorithmic Analysis of Blockchain Efficiency with Communication Delay, in FASE (2020) 400-419.
23. J. Xie, F. Yu, T. Huang, R. Xie, J. Liu, & Y. Liu, A Survey on the Scalability of Blockchain Systems, IEEE Network, 33 (2019) 166-173.
24. BitInfoCharts, Home page, Retrieved April 12, 2024, from https://bitinfocharts.com/ (n.d.).
25. C. Murthy, M. Shri, S. Kadry, & S. Lim, Blockchain Based Cloud Computing: Architecture and Research Challenges, IEEE Access, 8 (2020) 205190-205205.
26. M. Waseem, M. Khan, A. Goudarzi, S. Fahad, I. Sajjad, & P. Siano, Incorporation of Blockchain Technology for Different Smart Grid Applications: Architecture, Prospects, and Challenges, Energies (2023).