Comparative Analysis and Future Directions of Consensus Algorithms in Blockchain Technology

Richard Li

School of Computer and Network Security (Oxford Brookes College), Chengdu University of Technology, Cheng Du, 610059, China
liyi1069268110@stu.cdut.edu.cn

Abstract. The essence of blockchain technology lies in the consensus algorithm, which ensures data consistency among network nodes and secures the blockchain system. As blockchain technology rapidly evolves and finds widespread application, a diverse array of consensus algorithms has emerged, each tailored to specific use cases, performance criteria, and security needs. This paper differentiates between permissionless and permissioned blockchains, provides an overview of prevalent mainstream algorithms, and introduces a classification framework based on key features of these algorithms. A systematic comparative analysis is conducted by gathering data to delve into the principles, performance metrics, and suitability of various algorithms across different application contexts. Findings indicate that while many mainstream consensus algorithms exhibit unique characteristics, they face substantial challenges in network security, performance efficiency, and system scalability. The adaptability of different consensus algorithms varies significantly across application scenarios, suggesting that no single algorithm can universally fit all types of applications. Selecting an appropriate consensus algorithm is crucial for maintaining data consistency and security in blockchain systems. Moreover, the development of more efficient and secure consensus algorithms, continuous performance optimization, and security enhancement updates are essential for existing mainstream algorithms to address growing demands and emerging challenges in the blockchain industry.

Keywords: Blockchain technology, Consensus algorithm, Security analysis.

1 Introduction

Initially developed for cryptocurrencies like Bitcoin, blockchain technology was predominantly used for financial transactions. Over time, through continuous advancements, it has been increasingly applied to diverse fields beyond finance. At the heart of this technology are consensus algorithms, which are crucial for maintaining the integrity and security of data within decentralized networks. These algorithms enable all transactions to be accurately recorded on a distributed ledger without the need for a central authority, a function that is pivotal for the reliability and efficiency of the blockchain system [1]. With the growing adoption of blockchain technology, spurred

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_34

by its capacity to secure and streamline various digital interactions, the significance of consensus algorithms is ever-expanding across multiple domains [2].

The selection and implementation of appropriate and precise consensus algorithms are vital, as they directly influence the efficiency, scalability, and integrity of blockchain systems. As the technology permeates sectors such as finance, healthcare, and supply chain management [3], understanding the impact of different consensus processes becomes essential. These methods affect not only the transaction speed and delay but also the overall trust and reliability of the blockchain network.

This study conducts a comparative analysis of blockchain consensus algorithms, focusing on the variations in their fundamental principles, performance efficiency, and system security, all tailored to meet the diverse requirements of modern blockchain applications. Through a systematic review of existing literature, the study identifies and categorizes consensus mechanisms used in various blockchain implementations. The algorithms are categorized by analyzing article information and assessing their underlying principles, performance metrics, and suitability for different use cases. A comparative analysis highlights the trade-offs between efficiency, resource consumption, and vulnerability to attacks associated with each algorithm. This approach provides a comprehensive evaluation of the current state of the technology and offers insights that could guide future advancements. The primary goal of this study is to present a clear and organized assessment of blockchain consensus algorithms, aiming to enhance understanding of their impact on the effectiveness and security of blockchain systems. This research aims to aid researchers, technologists, and industry practitioners in selecting the most suitable consensus mechanism for their specific applications, ultimately improving the performance and reliability of blockchain technology.

2 Background of Blockchain Consensus Algorithms

2.1 Permissionless vs. Permissioned Blockchains

Permissionless Blockchains: Permissionless blockchains represent a fundamental model of blockchain technology where any participant can join the network without prior approval or identity verification, this type of blockchain is epitomized by systems such as Bitcoin and Ethereum [4]. Permissionless blockchains provide for the open access of transaction records, enabling every node in the network to verify and record transactions. This ensures the transparency of the network and the unchangeability of the data. Permissionless blockchains have substantial obstacles, namely in terms of scalability and privacy, notwithstanding their advantages. Due to the transparent nature of these blockchains, they are vulnerable to many types of network attacks, such as Sybil attacks, in which an attacker undermines the network by generating a significant number of pseudonymous entities. Moreover, the scalability of permissionless blockchains is often limited by the consensus mechanism, which can require significant computational power and result in slower transaction processing times compared to centralized systems [5].

Permissioned Blockchains: In the field of blockchain technology, permissioned blockchains represent a specialised application scenario for specific scenarios where control and privacy are critical. Unlike permissionless blockchains like Bitcoin or Ether, where anyone can join and participate without prior authorisation, permissioned blockchains restrict access to a predefined group of participants, requiring the approval of one or more entities. This control mechanism ensures a higher level of privacy and system efficiency by limiting the participation of trusted entities, which is crucial in applications concerned with data sensitivity. However, this control comes at a cost. The inherent centralisation of the permissioning system introduces potential points of failure and can compromise the fundamental decentralisation of blockchain technology.

In essence, while permissioned blockchains offer advantages in terms of control, privacy, and efficiency, they do so at the expense of decentralization and some of the core benefits that blockchain technology originally promised. As such, they are best applied in scenarios where the benefits of central control and privacy outweigh the advantages of a decentralized and open system. This perspective aligns with the insights discussed by Solat et al. in their comprehensive analysis of permissioned versus permissionless blockchains, where they highlight the limitations and situational benefits of permissioned systems in ensuring data integrity and system efficiency while sacrificing some aspects of blockchain's inherent decentralization [6].

2.2 Overview of Common Algorithms

Proof of Work (PoW) is by far the most common consensus mechanism used in cryptocurrencies such as Bitcoin. The algorithm requires nodes to solve complex computational problems in order to validate transactions and create new blocks, a process that requires a large amount of computational resources. The main advantage of PoW is its security - modifying any information on the blockchain requires recomputing the answers to all subsequent blocks. However, it has also been criticised for being energy intensive and potentially leading to centralised mining. According to Meneghetti et al, PoW was originally designed to ensure that individual nodes in a network could agree without a central authority, but the algorithm's significant consumption of energy and potential risk of centralisation has also attracted widespread attention and controversy [7].

Proof-of-Stake (PoS) is a consensus mechanism that addresses the energy waste and efficiency issues of traditional Proof-of-Work (PoW) methods. Unlike PoW, which relies on computational power, PoS "mints" new blocks by selecting "verifiers" through an election mechanism, where the choice of verifiers depends on the amount of tokens they pledge in the network [8]. In PoS, in order to become a verifier, all need to pledge a certain amount of cryptocurrency for locking, the more money a node pledges, the greater the chances of being selected, this pledge behaviour is essentially a security guarantee, when there is any misbehaviour it will lead to the loss of the money they pledged. PoS significantly reduces the need for energy as it eliminates the energy-consuming process of mining. In addition, since participation in the verification process does not require high hardware costs, more users can become verifiers, which not only lowers the barrier to entry, but also increases the decentralisation and security of the network. Despite its benefits, PoS also faces challenges, such as the potential for increased wealth concentration, as nodes with a large number of tokens may become richer as a result of frequent validation opportunities, as well as potential security risks, such as the possibility of a "51% attack" if a small number of validators take control of a disproportionate amount of collateralised tokens, thus threatening the integrity and fairness of the network. ", thus threatening the integrity and fairness of the network.

Proof of Authority (PoA) is a consensus mechanism specifically designed for permissioned blockchains that relies on a certain number of trusted entities (called "authorities") to manage the network and generate new blocks. PoA can achieve consensus quickly and with low computational and energy requirements, and is particularly suited to private or licensed chain environments that require a high level of trustworthiness, as at its core it relies on a set of certified verifiers to ensure the stability and security of the network. The advantages of PoA are mainly in terms of high efficiency and energy saving, but there are also some potential disadvantages, such as the risk of centralisation. The system's over-reliance on the integrity and competence of a few authorities may lead to the concentration of power, thus to some extent violating the original intention of decentralisation of blockchain technology. In addition, the selection and management of authorities, if not handled properly, may also affect the fairness and decentralisation of the network. PoA generally outperforms other consensus mechanisms in terms of processing speed and transaction throughput, but more stringent measures may be required to ensure network consistency and security. In Ethernet's private network, PoA has been implemented in the form of Aura and Clique, both of which differ in the consensus process but are initiated by the current leader with a proposal for a new block [9]. Choosing the right PoA implementation requires a combination of factors such as network scalability, security requirements, and ease of management.

Practical Byzantine Fault Tolerance (PBFT), is a consensus algorithm that can effectively solve the Byzantine general problem in distributed systems with fault tolerance and large processing throughput. However, PBFT has some problems in application, such as bad behaviour of the master node, high network communication overhead and poor system flexibility compared to other consensus algorithms [10]. The PBFT algorithm secures the consistency of a distributed system through a structured three-phase broadcast process, encompassing pre-preparation, preparation, and commit phases. Initially, the primary node acquires a request and broadcasts a pre-prepare message to all replica nodes, thereby commencing the consensus mechanism. In the subsequent preparation phase, the replica nodes verify the received message and broadcast a preparation message to affirm their concurrence with the request. Ultimately, during the commit phase, the nodes distribute commit messages and upon receiving sufficient commit confirmations, they execute the request and update the system's state. This sequence ensures system consistency and maintains state uniformity, even when malicious nodes are present. Achieving consensus on such a three-segment broadcast is a good solution to the Byzantine general problem, but it can also cause network congestion, and random selection of master nodes can also present security risks.

3 Systematic Classification of Blockchain Consensus Algorithms

3.1 Key Feature-Based Classification

Table 1. Classification table based on key characteristics.

Consensus algorithms	PoW	Pos	PoA	PBFT
Designing Goal	Sybil-proof	Energy efficiency	Benefits of both Pos and PoW	Remove software errors
Decentralization level	Decentralized	Semi-centralized	Decentralized	Decentralized
Permission model	Permissionless	Permissionless	Permissioned	Both
verifiers Based on	Work (Hash)	Stake	Vote and work	Vote
Energy efficiency	No	Yes	No	Yes
51% Attack	Vulnerable	Vulnerable	Safe	Safe
Scalability	Strong	Strong	Strong	Low
Double Spending attack	Vulnerable	Difficult	Vulnerable	Safe
speed	Slow	Fast	Fair	Fast

This study classifies the major blockchain consensus algorithms—Proof of Work (PoW), Proof of Stake (PoS), Proof of Authority (PoA), and Practical Byzantine Fault Tolerance (PBFT)—based on several critical features that directly influence their performance, security, and suitability for different blockchain applications.

Design Objective: Each consensus algorithm targets specific goals. Proof of Work (PoW) is designed to be resistant to Sybil attacks, Proof of Stake (PoS) emphasizes reducing energy consumption, Proof of Authority (PoA) seeks to balance the strengths of PoW and PoS for better performance and security, and Practical Byzantine Fault Tolerance (PBFT) aims to minimize software faults and increase fault tolerance.

Decentralization Aspect: PoW and PBFT are highly decentralized frameworks, while PoS offers a somewhat centralized approach. PoA maintains a decentralized structure but operates on a permissioned basis, which marginally reduces its decentralization level.

Access Model: PoW and PoS are permissionless, allowing anyone to participate without prior approval. PoA, on the other hand, is permission-based, limiting access to only those who are pre-authorized. PBFT is flexible, capable of functioning in both permissionless and permissioned settings.

Basis for Verifier Selection: The criteria for verifier selection varies across consensus algorithms. Proof of Work (PoW) bases its selection on the computational effort (hash work) provided by nodes, Proof of Stake (PoS) depends on the amount of stake held by nodes, Proof of Authority (PoA) considers the identity and reputation of validators (incorporating their voting and work record), and Practical Byzantine Fault Tolerance (PBFT) selects validators through a voting system, prioritizing fault tolerance.

Energy Consumption: PoS is noted for its superior energy efficiency, markedly contrasting with the energy-intensive nature of PoW. Both PoA and PBFT offer better energy efficiency compared to PoW, though they do not reach the low energy consumption levels of PoS.

Risk of 51% Attacks: PoW and PoS are vulnerable to 51% attacks, which occur when an entity gains control over the majority of the network's mining power or staking capacity, respectively. PoA and PBFT are less susceptible to such attacks due to their distinct validator selection processes.

Scalability Concerns: PoW and PoS both provide scalability, although PoW' s scalability is limited by its substantial energy and computational demands. PoA and PBFT also support scalability; however, PBFT faces challenges in maintaining scalability under high network loads due to its consensus communication demands.

Exposure to Double Spending and Similar Threats: PoW is prone to double spending if significant control over the network's hash rate is obtained. Conversely, PoS mitigates such risks through the economic disincentives of acquiring substantial stakes. PoA offers increased security against double spending compared to PoW due to its somewhat centralized approach, while PBFT is inherently resistant to double spending and other Byzantine faults due to its design.

Transaction Processing Speed: PoW typically experiences slower transaction speeds because of the extensive computational effort required for block mining. PoS facilitates quicker transactions by eliminating the mining process. PoA achieves reasonable transaction speeds, generally faster than PoW but potentially slower than PoS. PBFT is known for its rapid transaction processing, benefiting from an efficient consensus mechanism.

3.2 A Classification Framework

Permission-Based Classification: Permissionless Algorithms: Examples include Proof of Work (PoW) and Proof of Stake (PoS), which permit any individual to engage in the consensus mechanism without prior authorization or trust. These algorithms are highly decentralized and are ideal for public blockchains that prioritize transparency and inclusivity.

Permissioned Algorithms: Proof of Authority (PoA) and specific versions of Practical Byzantine Fault Tolerance (PBFT) are categorized here, limiting consensus participation to a predefined group of nodes. This structure benefits enterprise or private blockchains that value control, privacy, and rapid consensus over complete decentralization.

Resource-Based Classification: Computationally Intensive Algorithms: PoW epitomizes this category by demanding substantial computational resources to solve cryptographic challenges, prioritizing security but sacrificing energy efficiency and scalability.

Stake-Based Algorithms: PoS utilizes the financial commitment of participants as a security measure, fostering energy efficiency and quicker transaction processing.

Identity-Based Algorithms: PoA relies on the identity and reputation of validators, reducing resource demands and fitting well into environments where participants are identifiable and trustworthy.

Fault Tolerance Approach: Classical Fault Tolerance: PBFT is designed to robustly handle malicious activities and faults within a network, ensuring continuity without single points of failure. It is particularly useful in environments that demand high reliability and security.

Probabilistic Fault Tolerance: Algorithms such as PoW and PoS are classified under this approach, where security strengthens with increased participation but is not absolutely guaranteed. These are appropriate for expansive public networks where predicting node behavior is challenging.

4 Comparative Analysis of Consensus Algorithms

4.1 Principles and Trade-offs

Proof of Work (PoW), implemented by Bitcoin, focuses on security and decentralization, though it incurs high energy usage and slower transaction processing. The extensive computational tasks required to maintain network integrity hinder scalability.

Proof of Stake (PoS), adopted by Ethereum, minimizes energy consumption by allocating mining power proportional to coin ownership. This mechanism increases transaction speed and reduces energy use compared to PoW, yet it may concentrate power among those holding larger amounts of coins, potentially leading to centralization.

Proof of Authority (PoA), utilized by networks such as DASH, speeds up transactions and cuts computational expenses by using pre-selected validators. Although this enhances efficiency and transaction speed, it compromises some decentralization due to the centralized process of validator selection.

Practical Byzantine Fault Tolerance (PBFT), seen in Ripple, aims for nearly instantaneous transactions and high fault tolerance. It is ideal for applications needing quick transaction times, though it faces challenges in scaling with increasing network size.

4.2 Performance Metrics Comparison

Based on Table 2, the following is a Performance Metrics Comparison (Table2):
Transaction Per Second (TPS) Metrics: Ripple, using a PBFT-like consensus, achieves the highest throughput at 1500 TPS, making it ideal for rapid processing applications like payment systems. Ethereum, employing Proof of Stake (PoS), offers a throughput of 15 TPS, providing a balance between reasonable speed and enhanced energy efficiency compared to Proof of Work (PoW). Bitcoin’s PoW consensus has the lowest throughput, prioritizing security and decentralization but at the expense of speed, with just 5 TPS.

Block Time Comparison: Ripple excels with near-instantaneous block times, far surpassing the average 10-minute 50 seconds block time seen with Bitcoin's PoW, positioning PBFT as highly effective for quick transactions. Ethereum’s PoS achieves a block time of approximately 12.1 seconds, offering a compromise between speed and security.

Block Size and Confirmation Requirements: Bitcoin's larger block size （730.79 Kbytes）accommodates more transaction data but necessitates longer confirmation times, posing challenges for time-sensitive transactions. In contrast, Ripple's PBFT protocol requires fewer confirmations, enabling faster transaction validations.

Mining Rewards and Transaction Fee Structures: The reward and fee systems vary widely, with Bitcoin providing significant mining rewards（ 6.25+0.3721 BTC ($422,720.29)） to offset its high computational and energy costs. Conversely, Ripple and Ethereum（2+0.6046+0+0-0.5326 ETH($7,181.34)） offer lower rewards, reflective of their reduced operational expenses.

Security and Energy Consumption: Bitcoin's PoW depends on SHA-256 hashing, resulting in high energy use. PoS and PoA are considerably less energy-demanding. PBFT maintains high security without the energy-intensive mining process, leveraging a robust fault-tolerant mechanism to safeguard the network.

Table 2. Performance comparison table based on representative cryptocurrencies.

Consensus algorithms		PoW	Pos	POA	PBFT
Cryptocurrency		Bitcoin	Ethereum	DASH	Ripple
Throughput	TPS	5	15	0.17	8
	Block time	10m 50s	12.1s	2m 37s	0.06m
	Confirmations required/Block verification time	3/40m	70/14m	2/5m	NA/Near-instant
	Block size	730.79 KBytes	76.26 KBytes	17.45 KBytes	No fixed upper limit
Profitability of mining	Mining rewards /Per Block	6.25+0.3721 BTC ($422,720.29)	2+0.6046+0+0-0.5326 ETH ($7,181.34)	2.05+0.000955 DASH ($72.84)*	NA
	Hash function /consumption	SHA-256/high	BLAKE2b/low	X11/hig	SHA-512/high
	Average Transaction fee	0.00011 BTC ($6.82)	0.0032 ETH ($10.99)	0.000047 DASH ($0.0017)	0.00233 XRP ($0.0014)
	Hardware dependency	Yes	No	Yes	No

4.3 Application Scenarios and Suitability

Proof of Stake (PoS) – Ethereum. Well-suited for decentralized applications (dApps) and smart contracts that require faster transaction speeds and enhanced energy efficiency compared to PoW. PoS is particularly advantageous in applications where stakeholder incentives align with network health and security, such as in governance tokens and decentralized finance (DeFi) platforms [14].

Proof of Authority (PoA) - Private Enterprise Blockchains. Ideal for permissioned blockchain networks where transaction privacy, control, and speed are critical. PoA is frequently used in supply chain management, private financial services [15, 16]. where a known and accountable group of validators is preferable for network integrity.

Practical Byzantine Fault Tolerance (PBFT) – Ripple. Suited for financial applications requiring rapid processing and high throughput, such as payment processing systems and cross-border transactions [17]. PBFT's quick consensus mechanism makes it excellent for applications where transaction latency is a concern and where reliability is crucial under potential fault conditions.

5 Security Analysis of Consensus Algorithms

5.1 Main Security Challenges

Table 3. Comparison of consensus algorithms in terms of security

	POW	POS	POA	PBFT
Double spending attack	Vulnerable	Difficult	Vulnerable	Safe
51% attack	Vulnerable	Vulnerable	Safe	Safe

As shown in Table 3, different consensus algorithms show different degrees of vulnerability in the face of security threats. Because of its reliance on computing power, proof-of-work (PoW) is particularly vulnerable to double spend attacks and 51% attacks (Table 3). Proof-of-stake (PoS), on the other hand, makes a double-spend attack economically impractical, although it is still vulnerable to a 51% attack if the attacker can accumulate enough equity (Table 3). At the same time, Proof of Authority (PoA) and practical Byzantine Fault Tolerance (PBFT) provide stronger defenses against these attacks. Because of its consensus mechanism, PBFT provides significant flexibility (Table 3). The following is a specific analysis of different consensus algorithms under different attacks

Proof of Work (PoW): Double Spending Attacks: Vulnerable. PoW, as employed in Bitcoin, relies heavily on miners' computational power to validate transactions. An attacker with substantial computational resources can potentially reverse transactions, making double spending feasible [18].

51% Attacks: Vulnerable. If an attacker gains control of more than 50% of the network's hashing power, they can monopolize block creation and alter the blockchain's history, enabling double-spending [19].

Proof of Stake (PoS):

Double Spending Attacks: Difficult. In PoS, the validator's influence on the consensus process is proportional to their stake. This makes it economically impractical to execute double spending as it requires owning a significant portion of the total stakes, which is typically financially prohibitive.

51% Attacks: Vulnerable. Although more challenging and costly than in PoW due to the economic stake needed, acquiring 51% of the staking power could still let an attacker have major control over the ledger.

Proof of Authority (PoA): Double Spending Attacks: Vulnerable. Despite the reliance on a limited number of validators, which theoretically reduces risk, the centralized nature of authority can make it susceptible to insider threats or targeted attacks.

51% Attacks: Safe. PoA systems generally do not face traditional 51% attacks as the validators are pre-selected and trusted entities, reducing the risk of such an attack.

Practical Byzantine Fault Tolerance (PBFT): Double Spending Attacks: Safe. PBFT is designed to handle malicious nodes up to a third of the network. Its consensus mechanism prevents any single entity from altering the transaction record unilaterally.

51% Attacks: Safe. PBFT's consensus mechanism ensures that as long as fewer than one-third of the nodes are malicious, the network can function correctly and resist majority attacks.

6 Conclusion

This study systematically evaluates various consensus mechanisms integral to blockchain architectures, highlighting their distinct applications, performance metrics, and security challenges. Specific algorithms such as Proof of Work (PoW), Proof of Stake (PoS), Proof of Authority (PoA), and Practical Byzantine Fault Tolerance (PBFT) are tailored to meet particular objectives, influencing their ideal use cases and the trade-offs among security, efficiency, and scalability. The investigation explores the vulnerabilities and performance dynamics of key blockchain consensus algorithms such as PoW, PoS, PoA, and PBFT, each presenting unique challenges and advantages. PoW is noted for its substantial energy demands and risks of centralization, whereas PoS offers a more energy-efficient alternative but with potential governance issues due to wealth concentration. PoA ensures controlled access which mitigates common security threats but could suffer from centralization challenges. PBFT is recognized for its robust defense against security breaches and its proficiency in processing high volumes, although scalability can be a limitation. As blockchain technology evolves, there is a pronounced need to develop or refine consensus algorithms to better harmonize security, efficiency, decentralization, and scalability, particularly addressing vulnerabilities like the 51% attacks and tendencies towards centralization.

In conclusion, while no single consensus algorithm ideally satisfies all criteria for diverse blockchain implementations, understanding the inherent trade-offs and specific requirements of applications is crucial in guiding the selection of the most appropriate technology. This research is positioned to make a significant contribution to the field by providing a comprehensive analysis that supports the judicious choice and implementation of consensus algorithms in blockchain applications.

References

1. Yli-Huumo, J., Ko, D., Choi, S., Park, S., Smolander, K.: Where is current research on blockchain technology? A systematic review. PLoS One 11(10), e0163477 (2016).

2. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H.: An overview of blockchain technology: Architecture, consensus, and future trends. In: 2017 IEEE International Congress on Big Data (BigData Congress), pp. 557-564. IEEE (2017).
3. Bakos, Y., Halaburda, H.: Permissioned vs Permissionless Blockchain Platforms: Tradeoffs in Trust and Performance. NYU Stern School of Business Working Paper (2021).
4. Peng, L., Feng, W., Yan, Z., Li, Y., Zhou, X., Shimizu, S.: Privacy preservation in permissionless blockchain: A survey. Digital Commun. Netw. 7(3), 295-307 (2021).
5. Monrat, A. A., Schelén, O., Andersson, K.: Performance evaluation of permissioned blockchain platforms. In: IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), pp. 1-8. IEEE (2020).
6. Solat, S., Calvez, P., Naït-Abdesselam, F.: Permissioned vs. Permissionless Blockchain: How and Why There Is Only One Right Choice. J. Softw. 16(3), 95-106 (2021).
7. Meneghetti, A., Sala, M., Taufer, D.: A survey on pow-based consensus. Ann. Emerg. Technol. Comput. Print ISSN, 2516-0281 (2020).
8. Fahim, S., Rahman, S. K., Mahmood, S.: Blockchain: A comparative study of consensus algorithms PoW, PoS, PoA, PoV. Int. J. Math. Sci. Comput. 3, 46-57 (2023).
9. Islam, M. M., Merlec, M. M., In, H. P.: A comparative analysis of proof-of-authority consensus algorithms: Aura vs Clique. In: IEEE International Conference on Services Computing (SCC), pp. 327-332. IEEE (2022).
10. Zheng, X., Feng, W.: Research on practical byzantine fault tolerant consensus algorithm based on blockchain. In: Journal of Physics: Conference Series, Vol. 1802, No. 3, p. 032022. IOP Publishing (2021).
11. Bouraga, S.: A taxonomy of blockchain consensus protocols: A survey and classification framework. Expert Syst. Appl. 168, 114384 (2021).
12. Bamakan, S. M. H., Motavali, A., Bondarti, A. B.: A survey of blockchain consensus algorithms performance evaluation criteria. Expert Syst. Appl. 154, 113385 (2020).
13. Ferdous, M. S., Chowdhury, M. J. M., Hoque, M. A.: A survey of consensus algorithms in public blockchain systems for crypto-currencies. J. Netw. Comput. Appl. 182, 103035 (2021).
14. Arslan, C., Sipahioğlu, S., Şafak, E., Gözütok, M., Köprülü, T.: Comparative analysis and modern applications of PoW, PoS, PPoS blockchain consensus mechanisms and new distributed ledger technologies. Adv. Sci. Technol. Eng. Syst. J. 6(5), 279-290 (2021).
15. An, A. C., Diem, P. T. X., Van Toi, T., Binh, L. D. Q.: Building a product origins tracking system based on blockchain and PoA consensus protocol. In: 2019 International Conference on Advanced Computing and Applications (ACOMP), pp. 27-33. IEEE (2019).
16. Huang, Z., Zheng, P., Zheng, Z., Li, Y.: Lock-based proof of authority: A faster and low-forking PoA fault tolerance protocol for blockchain systems. In: International Conference on Blockchain and Trustworthy Systems, pp. 348-361. Springer Nature Singapore (2022).
17. Hanyu, M.: Central Bank Digital Currency Cross-Border Payment Model Based on Blockchain Technology. In: International Forum on Financial Mathematics and Financial Technology, pp. 191-202. Springer Nature Singapore (2021).
18. Sayeed, S., Marco-Gisbert, H.: Assessing blockchain consensus and security mechanisms against the 51% attack. Appl. Sci. 9 (9), 1788 (2019).
19. Hasanova, H., Baek, U. J., Shin, M. G., Cho, K., Kim, M. S.: A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. Int. J. Network Manag. 29(2), e2060 (2019).