

A Comparative Evaluation of Blockchain Consensus Algorithms in Terms of Energy Efficiency and Performance Metrics

Doğukan Çatal¹, Mehtap Köse Ulukök^{2*}

¹Department of Computer Engineering, Cyprus Aydın University, Northern Cyprus, 99010 Mersin, Türkiye

²Department of Software Engineering, Cyprus Aydın University, Northern Cyprus, 99010 Mersin, Türkiye

*Corresponding author: Mehtap Köse Ulukök (mehtapulukok@cau.edu.tr)

Abstract – This study presents a comparative evaluation of five widely adopted blockchain consensus algorithms—Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), and Proof of Authority (PoA)—based on energy efficiency and performance metrics. As blockchain systems scale into broader applications, key indicators such as transaction throughput (TPS), latency, security, centralization risk, and scalability become increasingly critical. Each algorithm is assessed through theoretical analysis, empirical data, and simulation-based studies found in the literature. The findings indicate that Proof of Work is the most secure, but it does not environmentally sustainable due to its energy needs. Proof of Stake and Delegated Proof of Stake are more energy-efficient and have a high throughput, but it can lead to centralization. A Practical Byzantine Fault Tolerant consensus algorithm is great in permissioned networks, but it doesn't scale well. Furthermore, those networks aren't really decentralized. Proof of Authority is the most environmentally sustainable option, but that energy efficiency comes at the cost of decentralization. This research highlights the lack of sustainable consensus mechanisms, that is, consensus protocols that are both secure and scalable and environmentally sustainable—as a gap that future research can address.

Keywords: Blockchain, Consensus Algorithms, PoW, PoS, DPoS, PBFT, PoA, Scalability, Sustainability.

I. INTRODUCTION

In the last ten years, blockchain technology has developed into a change agent across many industries, especially finance, healthcare, and energy systems. Because of its basic, distributed structure, blockchain technology manages data in a secure, clear, and immutable manner—without a centralized authority [1], [2]. Once the underlying technology behind the rise of Bitcoin and other cryptocurrencies (and a few ICOs), it does far more than this. Currently, it is edging forward into use cases that are only beginning to be understood and appreciated.

The consensus algorithm is the essential mechanism that upholds the integrity of blockchain systems. These algorithms allow the distributed nodes in the network to come to an agreement on a single, shared version of the transactional history. In doing so, they allow the network to maintain trust among its participants and protect the system from malicious interference [3], [4].

Yet, the process of achieving consensus can differ quite a lot, depending on which algorithm is in, especially when it comes to energy and computing power. Take the example of how the leading crypto has imbued the world with a hefty bill for electricity. Bitcoin, as you may know, works using an algorithm called Proof of Work (PoW). In the PoW system, if you want to be a part of the Bitcoin blockchain network and earn your reward in crypto, you must solve a very hard puzzle first. This puzzle gets solved by very fast computer with very large power supplies [5], [6].

To lessen these challenges, models like Proof of Stake (PoS) have been developed as alternatives. PoS does not grant validation privileges based on how much computational power

one can muster. Instead, it gives those privileges based on how many tokens one holds. This reduction in authorization permissions cuts down energy demands substantially. But it does raise some questions about how secure the network is and whether the validators might end up being too centralized [7], [8]. Ethereum's switch over to PoS is a fine example of this new kind of trade-off [9].

PoS serves as the foundation for Delegated Proof of Stake (DPoS), which adds a layer of representation to the concept. In DPoS, token holders vote for delegates to take care of the validation chores. DPoS can handle an impressive number of transactions with 21 delegates doing their job. DPoS can handle around 2000 transactions per second. Of course, this is theoretical. In practice, DPoS has been handling around 1500 transactions per second, which is a pretty good result. However, as it is discussed in [10], [11], there are several issues associated with DPoS. For one thing, it is centralized. Especially with the 3 seconds of time that DPoS has for creating a block, it can indicate even more obvious centralization.

Practical Byzantine Fault Tolerance (PBFT) is typically applied in permissioned blockchain networks. Rephrasing services need not apply for forms of PBFT that are cited along with references. PBFT functions through a method of all participating nodes exchanging messages to achieve consensus. Though this method is highly efficient with respect to both energy, and latency it is not highly scalable. As the number of nodes increases, so does the communication overhead. [12],[13].

Proof of Authority (PoA) adopts a different approach by designating authority nodes to produce blocks. Consequently,

transaction speeds are extremely high, and energy consumption is very low. The fundamental contradiction in this respect arises from the centralization of PoA. Trust becomes an issue in open environments when there is such a centralized blockchain system. Systemic trust concerns are in fact place concerns—who gets to control what happens when [14], [15].

The primary goal of this study is to conduct a multidimensional comparison of five major consensus algorithms—PoW, PoS, DPoS, PBFT, and PoA—not only in terms of energy efficiency but also based on metrics such as transaction speed (TPS), latency, security robustness, centralization risk, and scalability. This research endeavors to offer a complete framework that promotes both technical optimization and ecological sustainability in the design of blockchain systems used for formal verification [6], [16], [17].

II. METHODOLOGY AND EVALUATION CRITERIA

In this study, an analytical comparison based on the literature to evaluate five different blockchain consensus algorithms is aimed to investigate. The criteria for evaluation are twofold: energy consumption and performance. For each algorithm, through theoretical analysis, empirical data, and simulation-based findings are introduced in this section. These findings have been rendered comparable by normalizing relevant metrics [4], [6], [12]. The performance parameters used in the comparisons are summarized in Table I.

Table 1. List of performance evaluation criteria used for consensus algorithm comparisons.

Criterion	Description
Energy Consumption (J/txn)	Average energy required to validate a single transaction.
Transaction Throughput (TPS)	Number of transactions confirmed per second, indicating overall efficiency.
Latency	The average delay between initiating and finalizing a transaction on the ledger.
Security	Resilience against known threats such as 51% attacks, Sybil attacks, and double spending.
Centralization Risk	The extent to which an algorithm is prone to validator or miner monopolization.
Scalability	The ability to maintain performance as the number of network nodes increases.

The methodology comprises three primary components:

Theoretical Analysis: The benefits of structure, the complexity of mathematics, and the types of systems each algorithm produces all were synthesized from established academic literature [3], [12].

Empirical Data: Empirical Data Values of benchmark quantities like transaction throughput (TPS), energy per transaction, and average latency were compiled from previous testnet and production network evaluations and made into comparative tables [5], [6], [13].

Simulation Studies: Simulation Studies Data from prior models were used to replicate performance fluctuations corresponding to differences in node counts for the following consensus models: PBFT and DPoS [12], [16].

The study aspires to guarantee a trustworthy and just comparison of consensus algorithms used in both

permissioned and permissionless blockchain contexts. It aspires to do so not by comparing a handful of them for the types of platforms where they serve but by evaluating them all on the same platform.

III. RESULTS

This is a comparison done at the behest of no blockchain project or platform. This section evaluates five consensus algorithms in comparison with each other: Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), and Proof of Authority (PoA). The algorithms are evaluated along six common dimensions: transaction throughput (TPS), latency, energy consumption per transaction (J/txn), security, centralization risk, and scalability. The data used for this evaluation come from a combination of experimental studies [5], [6], [13], real-world implementations (e.g., Ethereum 2.0, Solana) [9], [11], and theoretical analyses. Energy comparison of these consensus algorithms are summarized in Table 2.

Table 2. Consensus algorithms energy comparison

Algorithm	TPS	Latency	Energy (J/txn)
PoW	3–7	High	707–900 [5][6]
PoS	50–1000+	Medium	0.01–0.1 [7][8][22]
DPoS	1000+	Low	0.05–0.2 [9][23]
PBFT	200–500	Very Low	0.1–0.3 [10][12]
PoA	1500+	Very Low	0.01–0.05 [11]

Note: Throughput and latency values are generalized estimates and may vary depending on deployment architecture and network size.

As shown in the energy comparison table and multi-criteria comparison given in Table 3, every consensus algorithm has individual strengths and weaknesses that make them applicable to different blockchain scenarios.

- **PoW** offers exceptional security and resistance to attacks like double spending and Sybil manipulation, making it reliable in adversarial environments. However, its reliance on computationally intensive mining operations results in extremely high energy consumption, elevated hardware costs, and considerable environmental impact. Studies show that the Bitcoin network alone consumes as much energy annually as several mid-sized countries [6], [17], raising concerns over long-term sustainability. This makes PoW a less favorable option for future open networks.
- **PoS** emerges as a more sustainable alternative by assigning validation power based on token ownership rather than computational effort. Following Ethereum's transition to PoS in 2022, the network's energy consumption reportedly dropped by 99.95% [9]. However, PoS may introduce validator centralization, as token accumulation by a minority of participants can result in power imbalances and potential threats to the principle of decentralization [7], [8].

- **DPoS**, building on PoS, enhances throughput through a delegation model in which stakeholders vote for a limited number of validators. This approach has enabled networks like EOS and Solana to achieve high processing speeds—exceeding thousands of transactions per second [10], [11]. Nevertheless, trust is concentrated among a small set of delegates, increasing centralization risk and dependency on their integrity.
- **PBFT** is optimized for permissioned blockchain environments, offering high accuracy and ultra-low latency. It is well-suited for enterprise-level applications, such as inter-organizational data sharing and financial operations [12], [13]. Yet, the message complexity of the system scales poorly with the number of nodes, rendering it impractical for large, decentralized networks [16].
- **PoA** offers unrivaled energy efficiency and speedy transaction finality by banking on a preselected subset of trusted validators. It is thus ideal for applications with a need for high throughput and requiring almost no overhead, like government systems or supply chains [14], [15]. However, being as it is, for PoA to be workable, trustworthy validators must be in place beforehand—something that is not a condition for public networks at large.

Table 3. Consensus algorithms multi-criteria comparison

Algorithm	Security	Centralization Risk	Scalability
PoW	Very High	Low	Moderate
PoS	High	Medium	High
DPoS	Moderate –High	High	Very High
PBFT	High	Low	Limited (≤ 10 nodes)
PoA	Moderate	Very High	Limited

Note: Throughput and latency values are generalized estimates and may vary depending on deployment architecture and network size.

These findings emphasize the need to match the selection of a consensus mechanism to the network's intended architecture and operational objectives. Notably, attention is turning to hybrid consensus mechanisms—like Raft-PoW [18] and VG-Raft [18]—that hold the promise of combining security with energy efficiency. Another future research direction is the integration of AI and machine learning to dynamically adapt the consensus protocol to the "state" of the network and to performance metrics and attack vectors. This is an exciting area, particularly for future constrained environments like the IoT and smart cities, where energy efficiency and responsiveness are paramount [15].

IV. DISCUSSION

The selection of an appropriate consensus mechanism is fundamental to achieving the intended architecture and operational goals of a blockchain network. This study has provided a criterion-based evaluation of several widely adopted consensus algorithms, emphasizing their respective strengths and limitations in terms of performance, scalability,

security, and environmental sustainability. The findings underline the trade-offs involved and the necessity for context-aware consensus design—especially as blockchain expands into diverse and demanding application domains. The strengths and weaknesses of the considered consensus algorithms are separately addressed, and their performances are evaluated and summarized in the following sections.

A. Proof of Work (PoW)

PoW is held in high esteem as one of the most secure consensus protocols in the whole blockchain arena. Its uncanny knack for withstanding attacks—especially the now-infamous 51% attack—is attributed not to clever coding but to the sheer amount of diverse, extensive power that computational devices embody. But was that a good trade for security? Many people think not. Again, if PoW were a product, it ought to have some responsible corporate social outcomes. Instead, what it has is notoriety for being a change to something as simple as an unwanted digital post-it notes on every door of a building, with high carbon emissions to boot. [5], [6].

B. Proof of Stake (PoS)

PoS moves the validation mechanism away from consuming energy, to selecting validators based on the tokens they hold and are willing to "stake," making it a much more sustainable alternative to past mechanisms like PoW. This was instanced by Ethereum's shift in 2022 to using PoS instead of PoW to achieve consensus, with claimed savings in network energy consumption of 99.95% compared to what its consumption would have been had it still been using PoW [9]. Nevertheless, PoS introduces new concerns, particularly the risk of validator centralization. Large token holders may exert disproportionate influence over consensus outcomes, potentially undermining the decentralized ethos that blockchains seek to preserve [7], [8].

C. Delegated Proof of Stake (DPoS)

DPoS builds upon PoS by introducing a representative governance model where token holders vote for a small group of trusted delegates to validate transactions. This system enables high transaction throughput, as demonstrated by networks like EOS and Solana, which can process thousands of transactions per second [11]. However, while appearing democratic in structure, the delegation mechanism often results in power consolidation. As such, the security and reliability of the system become highly dependent on the integrity of a limited number of elected validators [10].

D. Practical Byzantine Fault Tolerance (PBFT)

PBFT is especially suitable for private or permission blockchain networks. It offers advantages such as low latency and minimal energy consumption, which make it appealing for enterprise-level use cases including financial services and institutional data sharing [12], [13]. Despite its operational efficiency in small networks, PBFT does not scale well. As the number of participating nodes increases, the volume of inter-node communication grows linearly, severely limiting its horizontal scalability [16].

E. Proof of Authority (PoA)

PoA departs from decentralization by relying on a set of pre-approved authority nodes to validate transactions. This design results in extremely high processing speeds and minimal energy requirements [14], [15]. Although PoA is highly efficient, it contradicts the decentralized nature of public blockchain networks. For this reason, its usage is generally confined to controlled environments such as governmental systems, inter-organizational data exchanges, or supply chain networks where validator trust can be externally enforced.

V. CONCLUSION

This study has provided a comprehensive, multi-dimensional evaluation of five widely used blockchain consensus algorithms—PoW, PoS, DPoS, PBFT, and PoA—through the lenses of energy consumption and performance metrics. As the adoption of blockchain technology expands into energy-sensitive sectors and large-scale digital infrastructures, selecting an appropriate consensus mechanism becomes a matter of balancing security, efficiency, and sustainability.

The findings reveal that no single algorithm is universally optimal. Energy sustainability is a core tenet of modern society. While security and decentralization are indeed desirable features of blockchain systems, these are hardly. In the future of blockchain design, hybrid systems and AI-driven, adaptive, consensus frameworks are expected to play a key role in addressing the growing demands for not just practical, but also environmentally responsible, money and communication systems. The consensus mechanisms of tomorrow's systems will likely prioritize energy efficiency, security, and flexibility across a spectrum of operational contexts.

VI. ACKNOWLEDGMENT

The authors would like to thank Cyprus Aydın University for providing the academic environment and research support that made this study possible. Special thanks are also extended to the conference organizers of SETSCI 2025 for offering a platform to present this work.

REFERENCES

- [1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
- [2] M. S. Alnahari and S. T. Ariaratnam, "The application of blockchain technology to smart city infrastructure," *Smart Cities*, vol. 5, no. 3, pp. 979–993, 2022.
- [3] S. M. H. Bamakan, A. Motavali, and A. B. Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," *Expert Systems with Applications*, vol. 154, Sep. 2020.
- [4] Z. Liu, S. Tang, S. S. M. Chow, Z. Liu, and Y. Long, "Fork-free hybrid consensus with flexible proof-of-activity," *Future Generation Computer Systems*, vol. 96, pp. 515–524, 2019.
- [5] J. Yun, Y. Goh, and J.-M. Chung, "Analysis of mining performance based on mathematical approach of PoW," in *Proc. Int. Conf. Electron., Inf., Commun. (ICEIC)*, 2019.
- [6] L. Shi, T. Wang, J. Li, S. Zhang, and S. Guo, "Decentralize mining power of PoW blockchain using age-of-work," *IEEE Trans. Cloud Comput.*, vol. 11, no. 3, pp. 2756–2769, 2023.
- [7] S. Leonardos, D. Reijnsbergen, and G. Piliouras, "Weighted voting on the blockchain: Improving consensus in proof of stake protocols," *Int. J. Netw. Manage.*, vol. 30, no. 5, 2020.
- [8] D. Das, P. Chatterjee, S. Banerjee, U. Ghosh, and M. S. Al-Numay, "Blockchain-enabled federated learning for security and privacy in consumer electronics devices," *IEEE Trans. Consum. Electron.*, early access, Jan. 2025.
- [9] Ethereum Foundation, "Ethereum Energy Consumption After The Merge," 2022. [Online]. Available: <https://ethereum.org/en/energy-consumption/>
- [10] A. Rejeb, J. G. Keogh, and H. Treiblmaier, "Leveraging the Internet of Things and blockchain technology in supply chain management," *Future Internet*, vol. 11, no. 7, p. 161, 2019.
- [11] Solana Foundation, "Solana Throughput Performance," 2024. [Online]. Available: <https://solana.com/performance>
- [12] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. 3rd Symp. Operating Systems Design and Implementation (OSDI)*, 1999.
- [13] D. Huang, X. Ma, and S. Zhang, "Performance analysis of the Raft consensus algorithm for private blockchains," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 1, pp. 172–181, Jan. 2020.
- [14] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
- [15] L. Al Hwaitat et al., "A blockchain-based security framework for IoT networks," *Sensors*, vol. 23, no. 1, p. 45, 2023.
- [16] D. Tan, J. Hu, and J. Wang, "VBBFT-Raft: An understandable blockchain consensus protocol with high performance," in *Proc. IEEE 7th Int. Conf. Comput. Sci. Netw. Technol. (ICCSNT)*, 2019.
- [16] W. Gorenflo, S. Lee, L. Golab, and S. Keshav, "Energy-Efficient Blockchain Systems: A Survey," *IEEE Commun. Surv. Tutor.*, vol. 22, no. 4, pp. 2096–2130, 2020.
- [17] M. K. Ulukök, I. Saryıldız, and V. Evrim, "Hybrid Raft-PoW Blockchain Consensus Algorithm," *IEEE Access*, vol. 13, 2025.
- [18] R. Zhou and W. Ying, "VG-Raft: Byzantine fault tolerance consensus protocol with verifiable gossip mechanism," *IEEE Access*, vol. 9, pp. 125161–125171, 2021.