4th Indian International Conference on Industrial Engineering and Operations Management
Hyderabad, Telangana, India, November 07-09, 2024
Publisher: IEOM Society International, USA DOI: 10.46254/IN04.20240107
Published: November 07, 2024

Efficient Consensus Algorithm for Split-Join Blockchain Framework: A Comparative Analysis of PoW, PoS, and PoA

Vemula Harish
Research Scholar, Jawaharlal Nehru Technological University
Hyderabad, India

Dr. R. Sridevi
Professor in Dept. of CSE, JNTUH College of Engineering
Hyderabad, India

Dr. K S Sadasiva Rao
Professor in Dept. of CSE, Dean R&D, Sri Indu College of Engineering and Technology,
Hyderabad, India

Abstract

Blockchain is the decentralized technology which is changing the way businesses operate traditionally, due to its peer to peer characteristic and distributed consensus algorithms it is exhibiting low transaction throughput. Consensus algorithms play an important role in analyzing the performance of blockchain platforms. This study applies and analyzes three consensus protocols named Proof of Work (PoW), Proof of Authority (PoA) and Proof of Stake (PoS) on Split-Join Blockchain Framework. The Split-Join blockchain framework processes the block of transactions in parallel thus allowing more blocks to be committed to the decentralized ledger. Experiments are conducted in five rounds for all three consensus algorithms and with different transaction volumes starting with 50 transactions, then 100 txns, 500 txns, 1000 txns, 5000 txns in an increasing fashion. Observed the transaction latency over all rounds of experiment and considered the average latency and throughput to determine the efficient consensus algorithm. During the experiments it is observed that the PoA outperformed the PoW, PoS algorithms.

Keywords
Consensus Algorithms, Split-Join Blockchain, Blockchain Performance, Scalability

1. Introduction
Blockchain was introduced in the year 2008 by an anonymous author named Satoshi Nakamoto (2008**)** .Initially the blockchain technology is used for cryptocurrency, later it has developed rapidly and become a popular choice for applications such as healthcare (Hasselgren 2020), supply chain (Queiroz 2020), and the Defi (Werner 2022). The blockchain technology offers a distributed ledger, which is a database of all transactions that are happening in the network and is tamper-proof i.e., nobody can modify the record of transactions once they are stored to the blockchain ledger. Consensus protocols are used for agreeing upon a block of transactions by all network participants (Harish Vemula et al. 2020). Performance of the blockchain platforms plays an important role while promoting widespread adoption of blockchain technology (Harish Vemula, R. Sridevi 2023). Depending on the blockchain platform, application requirements there are various consensus algorithms available such as Proof of Work. It consumes a lot of energy in order to solve the cryptographic puzzle, validators who ever solve the puzzle first get the chance of publishing the block which is verified and approved by other network participants. The alternative consensus mechanisms that avoid excess energy consumption are PoS, PoA etc. PoS reduces the energy consumption through the selection of validators depending on the number of tokens they have and they are willing to "mint" as collateral.

Consequently, PoA is another alternative consensus that relies on the feedback of validators and their past performance to reach a consensus, thereby reducing the overall computational burden unlike PoW.

The objective of this study is to analyze the performance of these consensus mechanisms under a split-join blockchain (Vemula Harish et al. 2024a) in which blocks of transactions are processed in parallel. This study will help to examine their efficiency by comparing PoW, PoS and PoA. This paper is organized as follows: Section II covers the related study. Section III, the experimental methodology and evaluation metrics. Section IV discusses the results, Section V concludes and provides potential areas for future research.

2. Literature Review

The consensus algorithms play a crucial role in blockchain, many researchers have studied several aspects of consensus algorithms. Proof of Work consensus, which was introduced by Nakamoto in the Bitcoin whitepaper, is widely accepted, and became popular for its security and decentralization. However, the huge energy consumption requirement for its operations has significantly limited its transaction processing efficiency. Lasla et al. introduced the Green-PoW consensus algorithm, for mitigating the high energy consumption, which proposes a more energy-efficient approach by optimizing the computational overhead of traditional PoW while maintaining its security properties (Lasla et al. 2022). Similarly, Todorović et al. (2022) introduced an approach to blockchain mining called Proof-of-Useful-Work (PoUW), which requires miners to solve real-world optimization problems, making the computational effort more useful, reduce the environmental impact of blockchain mining by utilizing the resources meaningful applications, such as logistics and machine learning optimization. Todorović et al. also addressed the challenges of integrating PoUW with existing blockchain technologies, ensuring that essential characteristics like decentralization and security are maintained. Their research aims to make blockchain mining meaningful by utilizing computational power for real-life problem-solving. These improvements, Bitcoin is suffering from the inefficiency of the PoW consensus. It remains the most significant challenge, especially its environmental impact.

The PoS emerged as an alternative consensus for PoW, The validators are selected to publish the block of transactions based on their stake in the network instead of solving the cryptographic puzzle that requires high energy consumption. Li et al. (2017) improved the security of PoS. They analyzed the vulnerabilities associated with PoS systems and proposed solutions to address the security concerns such as long-range attacks and nothing-at-stake problems, which threaten the integrity and reliability of PoS-based blockchains. Li et al. proposed modifications and improvements to the existing PoS mechanisms to enhance resistance to these types of attacks. Similarly, Abbasi et al. (2023) proposed a new consensus mechanism called Aging-Based Proof of Stake (ABPoS). This approach enhances the traditional PoS by introducing an aging factor which increases the fairness of the staking process. In ABPoS approach, probability of the node getting selected to validate the next block increases with the amount of stake and also with the age of the stake. This ensures that the long-term participants have a better chance of getting selected, this helps in enhancing the overall reliability of the network trust. Although centralization remains a valid concern regarding large stake holders, these issues must be addressed.

PoA uses the identity and reputation of nodes to reach the consensus, it requires less computational overhead when compared to PoW, PoS. De Angelis et al. (2018) compared the Practical Byzantine Fault Tolerance (PBFT) and PoA consensus mechanisms to permissioned blockchains. They have used the CAP theorem to deal with the trade-offs between consistency, availability. De Angelis et al. highlighted that while PBFT emphasizes fault tolerance and consistency it is suitable for systems requiring strong security guarantees, PoA focuses on efficiency and performance by relying on trusted authorities for block validation. However, concerns about the need for reliable validators raise issues about PoA security, as pointed out by Ekparinya et al. (2019) in their paper The Attack of the Clones Against Proof-of-Authority, highlighting the challenges in the PoA trust model. Matthias Fitzi et al.(2018) introduced a Parallel Chains model for transaction processing, which was developed to improve the throughput by enabling parallelism in transaction execution. This method significantly enhances throughput and minimizes latency for both PoS and PoW. M. Zamani et al. (2018) proposed a solution called RapidChain, which also facilitates parallel transaction processing, showing significant improvements in throughput while reversing latency issues in sharded blockchains. However, despite these research efforts, the problem of scalability remains still open as the increase in parallel processing introduces new challenges, particularly in synchronizing parallel blocks and ensuring effective parallel execution.

3. Methodology

Split-Join blockchain is designed to process blocks of transactions in parallel to enhance throughput and reduce the latency. Vemula Harish et al. (2024b) Implemented the load balancer within the split-join architecture, and conducted a performance study. The results demonstrated enhanced throughput compared to the system without the load balancer. The split-join blockchain structure consists of the following components (Figure 1).

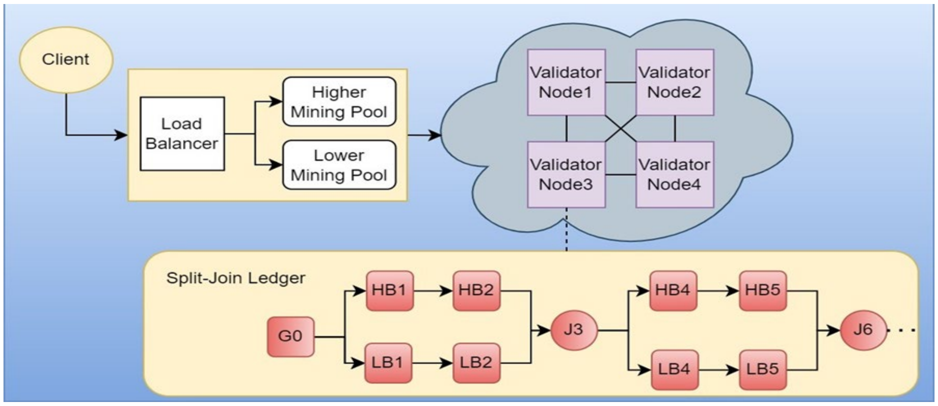

Figure 1. Split-Join Blockchain Framework Architecture

An empirical study is conducted by integrating consensus algorithms and comparing the throughput and latency of PoW, PoS, and PoA. The experimental setup uses a split-join framework for evaluating these consensus mechanisms, offering practical insights into their performance in a parallel processing environment. This study is useful in understanding the impact of parallel transaction processing on different consensus algorithms. Each block consists of a set of transactions, timestamp, previous block hash, and a random number known as nonce. The transactions are generated with random values and added to mining pools. Inorder to allow parallel block processing Transactions from the mining pools are distributed across both the validator node sets. Each validator set processes a subset of transactions simultaneously. Blocks are created and validated in parallel, with mechanisms in place to ensure consistency and prevent double-spending. It uses a Merkle tree structure to organize transactions within blocks, facilitating efficient verification.

4. Results and Discussion

To evaluate the performance of various consensus algorithms in split-join blockchain, conducted a series of experiments by considering three consensus mechanisms PoW, PoS, and PoA. Each of these algorithms was integrated into the spit-join blockchain framework to evaluate their performance in a parallel processing environment. The performance metric parameter used for experiments is number of transactions processed per second (TPS) and time taken to process the transactions (Latency).

Throughput (TPS) = Total Transactions/Total Time (seconds)

Based on the empirical study conducted the PoW algorithm showed the lowest throughput, with an average of 8.33 TPS, due to the computational requirement of solving cryptographic puzzles and the PoS algorithm achieved a 16.67 TPS, reducing block creation time and transaction processing by eliminating computationally expensive puzzles, fair selection through stake distribution among validators. Finally PoA achieved the highest throughput at 25.00 TPS, using predefined validators, absence of complex cryptographic puzzles, and periodic rotation of validators, which ensured faster block creation and validation.

The Table 1, Table 2 and Table 3 below displays the throughput and latency observed while sending 50 transactions to the split-join blockchain framework in 5 rounds for each PoW, PoS, and PoA algorithms.

4.1 50 transaction Arrival Rate

Table 1 summarizes the performance metrics of a PoW algorithm, conducted in five rounds. The key metrics evaluated are latency measured in milliseconds and throughput i.e., transactions per second (Figure 2, 3, 4, 5, 6, 7, 8, 9, 10, 11)

Table 1. PoW Consensus Algorithm

Rounds	Algorithm	Latency (ms)	Throughput (TPS)
1	PoW	49.12	1017.91
2	PoW	44.12	1133.34
3	PoW	52.84	946.18
4	PoW	61.23	816.64
5	PoW	53.37	936.81
Average		52.74	970.17

Table 2 summarizes the performance metrics of a PoS algorithm, conducted in five rounds.

Table 2. PoS Consensus Algorithm

Rounds	Algorithm	Latency (ms)	Throughput (TPS)
1	PoS	20.48	2441.36
2	PoS	25.31	1975.27
3	PoS	22.77	2195.58
4	PoS	23.49	2128.16
5	PoS	21.53	2322.33
Average		22.52	2212.34

Table 3 summarizes the performance metrics of a PoA algorithm, conducted in five rounds.

Table 3. PoA Consensus Algorithm

Rounds	Algorithm	Latency (ms)	Throughput (TPS)
1	PoA	25.65	1949.61
2	PoA	22.73	2199.65
3	PoA	21.62	2313.19
4	PoA	24.92	2006.32
5	PoA	19.91	2511.36
Average		22.96	2294.02

The results are summarized in Table 4. The highest average latency for PoW is observed at 52.74 ms, and the lowest average throughput observed for PoW is 970.17 transactions per second (TPS).

Table 4. Average Throughput and Latency 50 Arrival Rate

Algorithm	Proof of Work	Proof of Stake	Proof of Authority
Average Throughput (50 txns)	970.17	2212.34	2294.02
Average Latency in ms (50 txns)	52.74	22.52	22.96

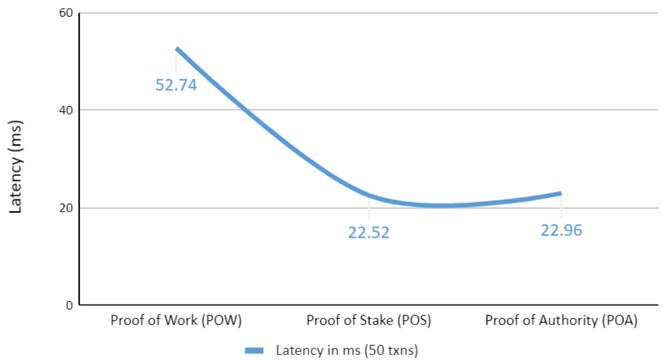

Figure 2. Average Latency 50 Arrival Rate

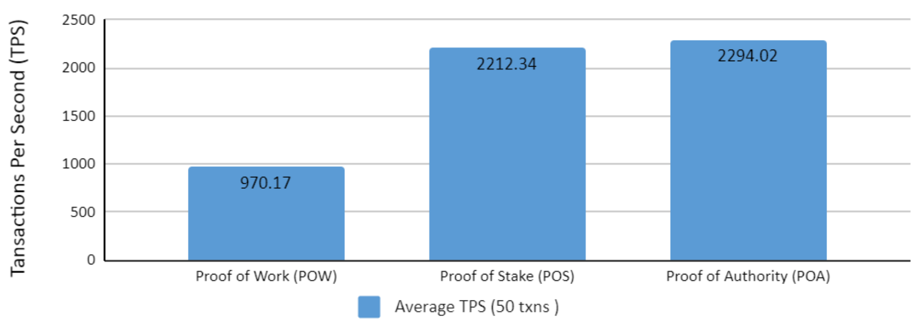

Figure 3. Average Throughput 50 Arrival Rate

Among all three consensus algorithms POA outperformed POS and POW for 50 transaction arrival rate.

4.2 100 transaction Arrival Rate

Average Throughput and Latency 100 Arrival Rate is presented in Table 5.

Table 5. Average Throughput and Latency 100 Arrival Rate

Algorithm	Proof of Work	Proof of Stake	Proof of Authority
Average Throughput (100 txns)	1108.49	2438.52	2373.39
Average Latency in ms (100 txns)	91.36	41.43	42.89

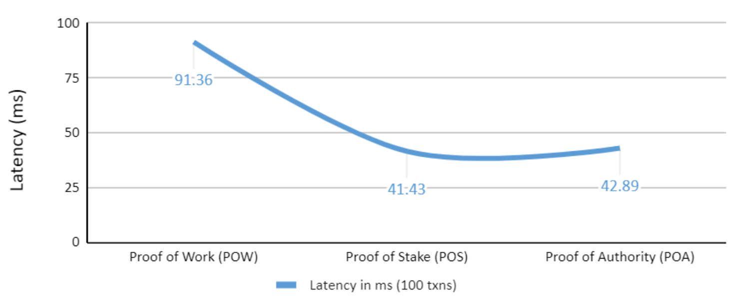

Figure 4. Average Latency 100 Arrival Rate

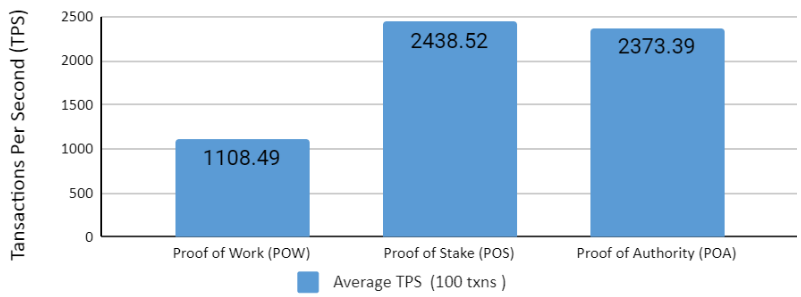

Figure 5. Average Throughput 100 Arrival Rate

Among all three consensus algorithms POS could achieve high TPS for 100 transaction arrival rate.

4.3 500 transaction Arrival Rate

Transaction arrival rate are presented in Table 6, Table 7, Table 8, Table 9.

Table 6. Average Throughput and Latency 500 Arrival Rate

Algorithm	Proof of Work	Proof of Stake	Proof of Authority
Average Throughput (500 txns)	1091.37	2433.18	2399.48
Average Latency in ms (500 txns)	459.72	211.98	216.84

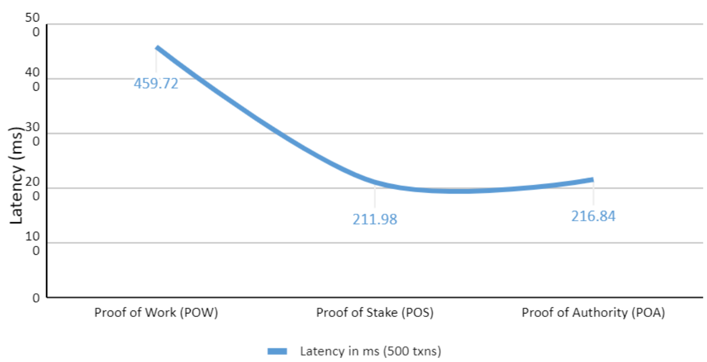

Figure 6. Average Latency 500 Arrival Rate

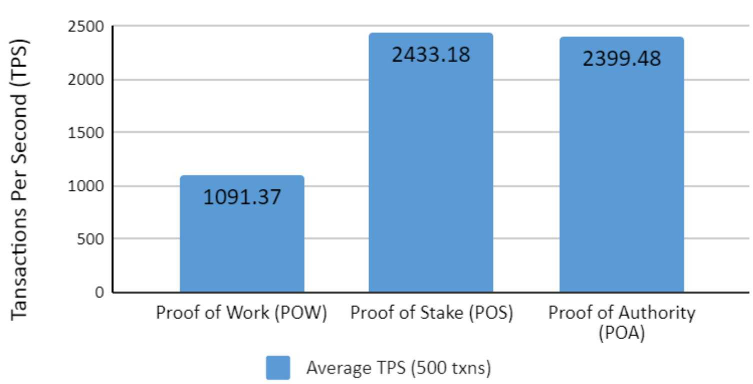

Figure 7. Average Throughput 500 Arrival Rate

Among all three consensus algorithms POS could achieve high TPS for 500 transaction arrival rate.

4.4 1000 transaction Arrival Rate

Table 7. Average Throughput and Latency 1000 Arrival Rate

Algorithm	Proof of Work	Proof of Stake	Proof of Authority
Average Throughput (1000 txns)	1023.30	2012.66	2570.33
Average Latency in ms (1000 txns)	977.77	506.99	391.31

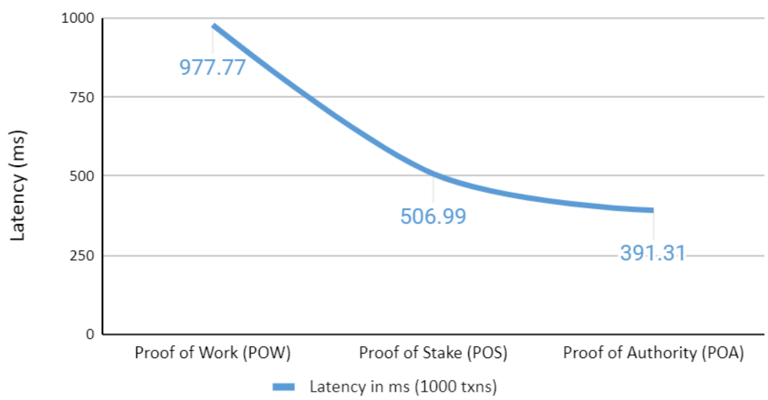

Figure 8. Average Latency 1000 Arrival Rate

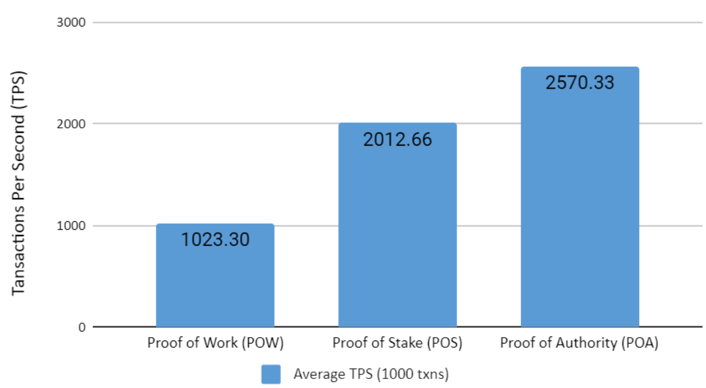

Figure 9. Average Latency 1000 Arrival Rate

Among all three consensus algorithms POA could achieve high TPS for 1000 transaction arrival rate.

4.5 5000 transaction Arrival Rate

Table 8. Average Throughput and Latency 5000 Arrival Rate

Algorithm	Proof of Work	Proof of Stake	Proof of Authority
Average Throughput (5000 txns)	974.46	1970.82	2442.21

Average Latency in ms (5000 txns)	5131.27	2544.40	2048.93

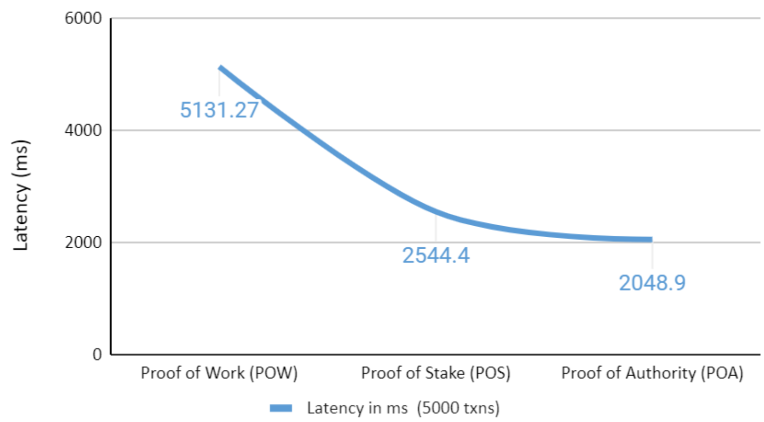

Figure 10. Average Latency 5000 Arrival Rate

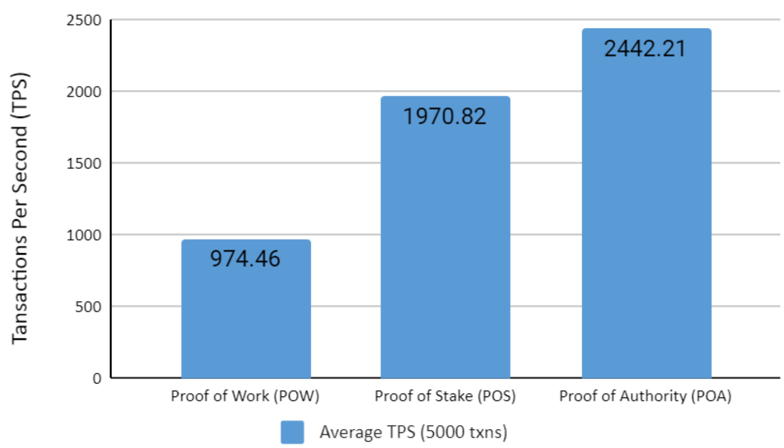

Figure 11. Average Throughput 5000 Arrival Rate

Among all three consensus algorithms POA could achieve high TPS for 5000 transaction arrival rate.

4.6 Overall Throughput

Table 9. Overall throughput for all transaction arrival rates

Transaction Volume	Proof of Work	Proof of Stake	Proof of Authority
50 txns	970.17	2212.34	2294.02
100 txns	1108.49	2438.52	2373.39
500 txns	1091.37	2433.18	2399.48
1000 txns	1023.3	2012.66	2570.33
5000 txns	974.46	1970.82	2442.21

The empirical study reveals that PoA offers the highest throughput with respect to the increasing transaction arrival rate, while PoS offers a balanced approach with lower energy consumption. whereas PoW is secure but is less efficient in terms of throughput and energy consumption.

5 Conclusion

The study examines the performance of consensus algorithms Proof of Work , Proof of Stake and Proof of Authority in a split-join blockchain environment. The results show that PoW provides robust security but has limitations in performance and scalability due to high energy consumption and computational requirements. PoS offers a balanced approach with better performance and energy efficiency, but also carries risks of centralization. PoA delivers the highest throughput and scalability, making it ideal for specific use cases where throughput is critical and validators can be trusted. Future research includes a focus on optimizing parallel processing techniques in blockchain and exploring hybrid consensus models. It is possible to build more efficient, scalable, and secure blockchain systems that meet the diverse needs of various applications. Need for further research to optimize parallel processing techniques is essential.

References

Abbasi, M Prieto, J Plaza-Hernández, M & Corchado, J. M, A Novel Aging-Based Proof of Stake Consensus Mechanism. *In Sustainable Smart Cities and Territories International Conference* (pp. 49-61). Cham: Springer Nature Switzerland, 2023.

De Angelis, Stefano, Leonardo Aniello, Roberto Baldoni, Federico Lombardi, Andrea Margheri, and Vladimiro Sassone., PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain, *In CEUR workshop proceedings*, vol. 2058. CEUR-WS, 2018.

Ekparinya, Parinya, Vincent Gramoli, and Guillaume Jourjon., The attack of the clones against proof-of-authority, arXiv preprint arXiv:1902.10244, 2019.

Fitzi, Matthias, Peter Ga, Aggelos Kiayias, and Alexander Russell., Parallel chains: Improving throughput and latency of blockchain protocols via parallel composition, *Cryptology ePrint Archive* 2018.

Hasselgren, Anton, Katina Kralevska, Danilo Gligoroski, Sindre A. Pedersen, and Arild Faxvaag., Blockchain in healthcare and health sciences—A scoping review, *International Journal of Medical Informatics* 134, 2020.

Harish Vemula, and R. Sridevi., A brief survey on blockchain technology, *In Proceedings of the Third International Conference on Computational Intelligence and Informatics: ICCII 2018*, pp. 249-258. Springer Singapore, 2020.

Harish Vemula, and R. Sridevi, Performance Analysis of Public and Private Blockchains and Future Research Directions, *In International Conference on Network Security and Blockchain Technology*, pp. 397-408. Singapore: Springer Nature Singapore, 2023.

Lasla, Noureddine, Lina Al-Sahan, Mohamed Abdallah, and Mohamed Younis., Green-PoW: An energy-efficient blockchain Proof-of-Work consensus algorithm, *Computer Networks* 214: 109118, 2022.

Li, Wenting, Sébastien Andreina, Jens-Matthias Bohli, and Ghassan Karame., Securing proof-of-stake blockchain protocols, In Data Privacy Management, Cryptocurrencies and Blockchain Technology: *ESORICS 2017 International Workshops, DPM 2017 and CBT 2017, Oslo, Norway, September 14-15, 2017, Proceedings*, pp. 297-315. Springer International Publishing, 2017.

Nakamoto, Satoshi., Bitcoin: A peer-to-peer electronic cash system, *Satoshi Nakamoto* (2008).

Queiroz, Maciel M., Renato Telles, and Silvia H. Bonilla. "Blockchain and supply chain management integration: a systematic review of the literature." Supply chain management: An international journal 25, no. 2: 241-254. 2020.

Todorović, Milan, Luka Matijević, Dušan Ramljak, Tatjana Davidović, Dragan Urošević, Tatjana Jakšić Krüger, and Đorđe Jovanović., Proof-of-useful-work: Blockchain mining by solving real-life optimization problems, *Symmetry* 14, no. 9 (2022): 1831.

Vemula Harish, R. Sridevi, K.S. Sadasiva Rao., Split-Join: A Blockchain Framework for Improving Scalability and Performance, *SSRG International Journal of Electronics and Communication Engineering,* vol. 11, no. 3, pp. 31-40, 2024. Crossref, https://doi.org/10.14445/23488549/IJECE-V11I3P104

Vemula Harish, R. Sridevi., Enhancing Split-Join Blockchain Performance through Load Balancing, *SSRG International Journal of Electrical and Electronics Engineering,* vol. 11, no. 7, pp. 124-133, 2024. Crossref, https://doi.org/10.14445/23488379/IJEEE-V11I7P110

Werner, Sam, Daniel Perez, Lewis Gudgeon, Ariah Klages-Mundt, Dominik Harz, and William Knottenbelt. "Sok: Decentralized finance (defi)." In Proceedings of the 4th ACM Conference on Advances in Financial Technologies, pp. 30-46. 2022.

Zamani, Mahdi, Mahnush Movahedi, and Mariana Raykova., Rapidchain: Scaling blockchain via full sharding, *In Proceedings of the 2018 ACM SIGSAC conference on computer and communications security*, pp. 931-948. 2018.

Biographies

Mr. Vemula Harish is a researcher, with 9 years of experience. He has served as Assistant Professor for 4 years in the Department of Computer Science and Engineering at Vardhaman College of Engineering and also served as Assistant Professor in CSE for 2 years at VNR Vignana Jyothi Institute of Engineering and Technology Hyderabad, India. He is a Professional in blockchain technology, having 3 years of research and development experience. He holds a masters degree (M.Tech) in Software Engineering from Kakatiya University Warangal, He has authored or co-authored several publications in international journals and conference proceedings. His research interests include Blockchain Scalability, Performance and Interoperability.

Dr. R. Sridevi is a Professor of CSE with 23 years of teaching experience. Presently working as Professor, Director, Directorate of Entrepreneurship, Innovation and Start-ups, JNTUH & Co.ordinator, Centre of Excellence in Cyber Security, JNTUH. Lead various roles as Head of the CSE Department for nearly 3 years, Additional Controller of Examinations(EDEP), Additional Controller of Examinations(Result Processing). Worked as Chairman, Board of Studies for Department of CSE, JNTUHUCEH, Hyderabad. During the tenure of Head, organized several Workshops,FDPs, curricular and extra-curricular events and 3 international conferences .Established three Research Labs IoT Lab, Digital Forensics Lab & Big Data Analytics Lab and one smart classroom under TEQIP in the department. Network security and information security are the research domains. Guided 7 Ph.Ds & Published very good number of research papers in various national and international conferences and reputed journals with high indexing factor.

Dr. K S Sadasiva RaO is a Professor in the Department of CSE and also Dean R&D at Sri Indu College of Engineering Technology (A), Ibrahimpatnam, Hyderabad. He has 23 Years of Teaching Experience at the level of Head of the Department, Principal and Dean-Academics. He has rich experience in organizing seminars, workshop in Computer Science Engineering topics. He is Convener for the International Conference ICICSET'24. He also worked as principal for the period of 8 years at Sri Indu PG College. He published 24 papers in several National as well as International Journals with high indexing factor and presented 6 papers in International Conferences. He is a Lifetime Member in the professional societies CSI, IETE, ISTE. He is also serving as a reviewer member for many international journals.