

Design and Analysis of the Improved Consensus Algorithm of the Blockchain Technology

Kolli Lalitha Kumari, P Lalitha Surya Kumari*

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Hyderabad-500075, Telangana, India.

*Corresponding Author's Email: vlalithanagesh@gmail.com

Abstract

Blockchain is a progressive technology that considerably impacts current technology due to its transparency, decentralization, and security features. In any blockchain application, the critical and core part is the consensus algorithms. Consensus algorithms are crucial for ensuring that all transactions are validated before being added to a blockchain, which serves as a primary function of the blockchain. Maintaining a good performance in different consensus algorithms is essential in blockchain technology. This paper presents an improved consensus algorithm for Proof of Authority-Practical Byzantine Fault Tolerance, incorporating validation, voting, and authentication concepts. The proposed method enhances PBFT with an authorisation module to provide confidentiality in blockchain applications. The results are implemented using Spyder, a Python IDE, and the Ethereum platform, precisely the Remix IDE. The performance is analyzed through the experimental results of PBFT and PoA-PBFT algorithms based on computational resources, including gas cost, transaction cost, execution cost, latency, and transactional throughput. Experimental results have demonstrated that an improved consensus algorithm requires fewer computational resources. The proposed algorithm is applicable in various fields, including healthcare, supply chain management, and the Internet of Things. Based on the experimental results examined, this work presents a potential future approach that serves as a helpful framework for researching the expansion of blockchain system functionality.

Keywords: Bitcoin, Blockchain Applications, Hybrid-Consensus Algorithms, PoA, PoP.

Introduction

Blockchain technology is the latest innovation to revolutionise the IT industry, boasting some of the most robust security features. Bitcoin and Blockchain are becoming the chosen technologies for implementing numerous business solutions in the current technological era. Bitcoin is a cryptocurrency that enables online payments, whereas blockchain is the technology and platform that facilitates transparent and immutable transactions (1). Blockchain can deliver the required levels of more excellent privacy and trust. The verification task is carried out by applying a consensus algorithm. Since no cooperation among peers, the consensus process can identify incorrect information if a peer has forwarded it to others (2). Because all blocks are chained together, and each created block contains information about prior blocks, if one block in a chain is altered, all preceding blocks must also be changed, as shown in Figure 1. The blockchain's structure is depicted in the diagram, which illustrates how blocks are

linked to form a secure and immutable ledger. A cryptographic nonce used in PoW consensus, the hash of the previous block, current block, and Merkle root—a cryptographic hash that summarises the transactions of the block—are among the crucial metadata included in the header of each block, which is represented as a cube. Successively connecting the blocks using the previous block's address maintains the chain's integrity, and any changes made to one block render the hashes of the subsequent blocks incorrect. A consensus algorithm is essential to the blockchain as a transparent and efficient system.

Validation-Based Consensus

Algorithms

Validation-based algorithms are PoW, PoS, PoA, PoR and PoET. In the PoW technique, miners solve the algorithm's cryptographic puzzle. A successful miner adds each block to the blockchain and will receive payment for their work. In a PoS system,

This is an Open Access article distributed under the terms of the Creative Commons Attribution CC BY license (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted reuse, distribution, and reproduction in any medium, provided the original work is properly cited.

(Received 13th December 2024; Accepted 17th April 2025; Published 30th April 2025)

miners are chosen based on their contributions to a decentralised system rather than processing power resources. It refers to the number of digital tokens, such as cryptocurrency coins, that an entity owns or deposits in a PoS consensus mechanism. Spending minimal energy on mining, miners were selected based on the stakes they held. The PoR consensus process generates the block according to its applicability. Each block containing private data and its adjacent blocks has been generated to determine relevance. This algorithm helps maintain the original and secure information by preventing false data attacks on the blockchain. In authorised blockchains, PoET is a widely utilised algorithm. On the network, each miner has an equal opportunity to generate a block. If the consensus mechanism succeeds and no network

forks occur, then every node's last-closed ledger will be identical. PoA relies on the reputation of trustworthy participants in a blockchain network. In the PoA framework, authenticators offer their identities and reputations as stakes rather than tangible resources. The reason is that the PoA consensus mechanism is built on the integrity and credibility of the network participants. Therefore, corroborating arbitrary nodes are considered reliable parties for PoA blockchain networks. The PoA method is an easily scalable blockchain system, as it only requires a limited number of block validators, and transactions are verified by network users who have already been authorised. The PoA consensus method can be effectively applied in various fields, such as supply chain management.

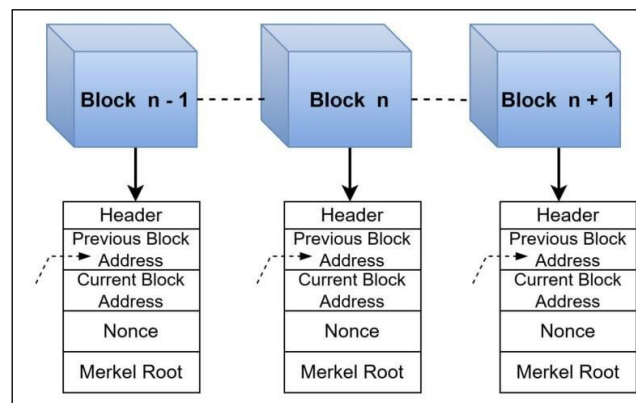


Figure 1: Simple Blockchain

Voting-Based Consensus Algorithm

The agreement achieved through voting in the PoV consensus mechanism is "evidence of vote". In this context, core nodes serve as the central logical hub of the network, responsible for voting to oversee and validate the production of blocks. PoV aims to achieve eventual consistency and limited partition tolerance by evaluating its correctness and security theoretically. For PoV to function effectively, it is essential that more than half of the core nodes, along with at least one accounting node, remain reliable and diligent, all while minimising energy consumption. Initially, the PoT consensus employs a reputation-based approach grounded in subjective logic to select nodes that exhibit high trustworthiness. Only these chosen nodes are granted this opportunity to create blocks, participate in verification processes, and claim jobs through crowdsourcing. Additionally, the unpredictable characteristics of timestamps

and digital signatures significantly enhance the selection process for node generating blocks.

Authentication-Based Consensus Algorithms

The proof-of-authentication process employs a simplified version of standard blockchain block verification. While this method aims to authenticate blocks using the same transaction techniques as blockchain, the first task for a miner in the network is to validate the block and then assess its hash value. A new hardware security concept, known as Physical Unclonable Functions (PUFs), is being thoroughly explored. For hardware-assisted security protocols, the technical aspects of logic-based events are expanded, and a method is proposed to utilise event logic to abstract hardware security attributes for PUF-enhanced identity verification protocols. The fundamental execution order is established, and the successful authentication property within the protocol interaction process is

confirmed through the interaction of a PUF-based mutual authentication protocol, as defined by the event logic in Figure 2. According to the diagram, three primary categories of consensus algorithms are used in blockchain systems: voting-based, validation-based, and authentication-based. Examples of validation-based methods include PoW, PoS, PoA, PoR, and PoET. Voting-based

consensus algorithms, such as Ripple, PoV, and PoT, rely on nodes voting to achieve agreement. Lastly, PoAh and PoP focus on identity verification or validated participation in the consensus process and fall under the Authentication-Based category. These classifications illustrate the diverse methods available for achieving distributed consensus in blockchain networks.

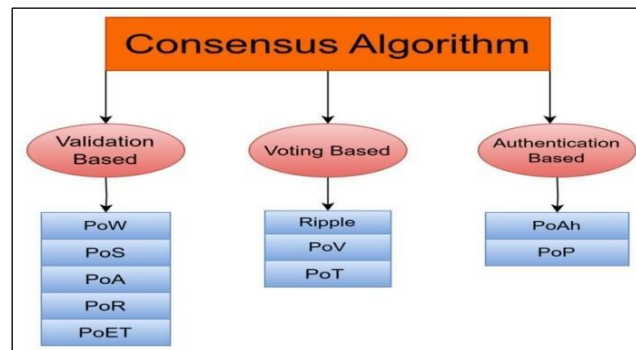


Figure 2: Categories of Consensus Algorithms

Proof of Authority

Permitted blockchain networks can utilise a PoA consensus, which offers distinct advantages. Anytime a new transaction proposal is made, all authenticators are notified. These authorities independently verify that the transaction meets validity requirements and network rules. As more authenticators agree the transaction is valid, it is added to a new block. In PoA, the most crucial part is the authenticator chosen to create the block. A consensus algorithm, such as round-robin or weighted random selection, determines the authenticator. The new block is then shared with all network nodes. Each node independently verifies the block's integrity by checking if it contains valid transactions and is correctly linked to the previous block. Once most nodes agree the block is valid, it is added to the blockchain.

Practical Byzantine Fault Tolerance

To make BFT accessible on large networks, an optimisation known as pBFT was developed. This is accomplished in several ways by eliminating connections between every linked node in the blockchain network. pBFT enhances network performance by implementing a primary node and backup node ordering. The pBFT approach can withstand node failures since it is purposefully designed to be fault tolerant. This is particularly significant in systems like blockchain consensus, where nodes can suddenly go offline. Since Blockchain consensus techniques, such as PoW or PoS, only have a probabilistic conclusion, an

accepted block may be removed from the distributed ledger after a reconfiguration (3). pBFT's finality guarantees that it's unchangeable once a transaction secures approval from a defined quorum of nodes. An Algorithm designed to withstand Byzantine Fault Tolerance is pBFT, which withstands a threshold of malicious nodes within the blockchain network. A designated leader node orchestrates the approval process and determines the content of the next block, which will be included in the subsequent block on the blockchain. This results in a level of centralisation that can violate the core principles of blockchain. pBFT is communicated from a particular set of the network's nodes to finalise a block's contents. It suggests that the network's scalability is constrained since the number of messages increases with network size. Parallel to scalability, pBFT faces difficulties with network bandwidth usage. Hence, more bandwidth is required when more nodes communicate with one another. If the system receives a large number of votes, an attacker may be able to approve malicious blocks and control a significant portion of the nodes. pBFT is now utilized with other blockchain consensus techniques due to its scalability challenges. For instance, a consensus process may combine PoS with DPoS to restrict the number of nodes participating in PoS to the number of delegates elected via DPoS.

pBFT is a powerful BGP alternative that enables network nodes to reach consensus even in the

presence of malicious nodes. Blockchains using a BFT version, such as pBFT, usually integrate it with another algorithm to restrict the number of voting nodes. It might be a decentralised consensus system, such as DPoS, or a permissioned blockchain with a centralised authority selecting the delegates. Regardless of the approach used, ensuring that the consensus algorithm is carefully considered and adequately implemented to achieve consensus and maintain functionality even in the presence of rogue nodes is crucial. This article proposes an enhanced consensus algorithm to address the scalability challenges associated with computational resources in current blockchain technology. The subsequent sections focus on relevant research in consensus algorithms, comparing the proposed approach with existing methodologies and evaluating the outcomes of the enhanced algorithm through the implementation of smart contracts. The article concludes by discussing future directions for blockchain consensus algorithms.

A game-theory-based analysis was proposed to select mining pools to investigate the balance between the effectiveness of transparency and the exposure to adversarial actions in a PoW-driven blockchain framework (4). This study meticulously examines the trade-offs related to block size and its effect on overall latency to provide a thorough and perceptive analysis of the optimization of PoW blockchain performance (5). A comprehensive analysis of modifiable signatures was provided, and their implementations in the PoS blockchain were analyzed (6). Investigation focused on proof-of-stake mechanisms, which ranged from basic understanding to sophisticated PoS-based protocols and performance analysis, including energy expenditure, latency, and security, as well as their encouraging implementations, specifically in vehicular networking (7). Existing studies were assessed, and analysis outcomes were compiled to evaluate the performance of both methodologies, reaching a consensus on one or both approaches to implementing Blockchain for data storage (8).

A new cryptocurrency protocol, PoA, was proposed to expand on the Bitcoin system by combining a PoS model with its PoW element (9). A novel consensus framework was introduced based on the PoA and game theory (10). By evaluating parameters such as decentralization, which is minimal in PoA compared to other

mechanisms, and the scalability limitations of PoW, facilitation of choosing the most suitable protocol based on prioritized performance aspects is achieved (11). A defense mechanism based on the idea that multiple witnesses should verify authentic information is presented (12). By using a Proof-of-Relevance through consensus, security and reliability in VANETs are aimed to be enhanced, making them more resilient to false data injection attacks. A low-complexity consensus method was proposed that utilizes minimal resources in a lightweight blockchain-enabled architecture for 5 G-enabled Internet of Things (IoT) networks. (13).

A hybrid approach known as TF-RC (Two Fish with Ripple Consensus Algorithm) was presented, and efficient data transmission within the decentralized network was leveraged to increase security and detection speed (14). An electronic voting system that utilizes blockchain technology and a robust Proof-of-Vote (POV) consensus mechanism was developed. Legal issues with conventional procedures were assessed in this study along with how blockchain technology can resolve them (15). Blockchain and distributed ledger technology were presented in voting systems (16). Blockchain and distributed ledger technology were presented in voting systems (17). Blockchain and distributed ledger technology were presented in voting systems (18). An enhanced PoT consensus model, developed using the foundational technology of blockchain suitable for crowdsourcing applications, was introduced (19). The fundamental features of blockchain, such as decentralization and immutability, were highlighted to create a reliable foundation of trust, eliminating the need for intermediaries. Increased control over data and transactions within blockchain-based systems was provided to users through this trust (20). The principle of PoAh for the efficient deployment of blockchains in the IoT was presented, which can substitute conventional consensus algorithms for resource- and energy-optimized systems, such as IoT (21). Present the principle of PoAh for the efficient deployment of blockchains in the IoT. It can substitute conventional consensus algorithms for resource- and energy-optimized systems, such as IoT (22). A consensus mechanism combining PBFT with PoS was proposed, which can effectively handle dishonest nodes, including both leaders and

individual validators, while maintaining optimal performance (23, 24).

A novel group-to-group (G2G) verification method was introduced, leveraging Physical Unclonable

Functions (PUFs) and blockchain technology to address existing challenges. Categories of different blockchain consensus algorithms based on the available literature were explained in Table 1.

Table 1: Categories of Different Consensus Algorithms

Category	Reference	Consensus Mechanism	Mainly Focuses on	Performance and Scope	Applications
Validation Based	(4-6)	POW	Mining competition based on cryptographic puzzles to add the block to a blockchain.	Low	Smart contracts Cryptocurrency
	(7-8)	POS	Random Block Selection Method based on the stakes	Medium	Smart contracts Cryptocurrency
	(9-11)	POA	A limited number of block validators	High	Cryptocurrency
	(12)	POR	computational complexity	High	Cryptocurrency
	(13)	POET	Random Timer System	High	Cryptocurrency
	(14)	Ripple	Correctness and agreement of the network	Medium	Cryptocurrency
Voting Based	(15-18)		Controllable security, convergence reliability, and a single block of corroboration are sufficient to validate a transaction's correctness, along with a short verification time for transactions.	High	Real World
	(19-21)	POT	Selecting validators according to their percentage of ratings and fixed stakes	Medium	Cryptocurrency
		PoAh	Cryptographic authentication mechanism	High	Cryptocurrency
	(22-24)	POP	Utilise PUFs to integrate hardware security primitives, addressing bandwidth, integration, scalability, latency, and energy requirements.	High	Real World and General Applications.

Methodology

It is essential to have a brief idea of consensus algorithms to continue research in blockchain-related aspects. Every consensus algorithm focuses on validating block data, authenticating access to the data, and performing mining operations on transactions before adding them to the main chain, as shown in Figure 1. However, to perform all these tasks efficiently, a single consensus will not yield accurate results in a public blockchain, as it fails to address scalability issues concerning performance. The improved consensus algorithm is crucial for enhancing the performance of a public blockchain. PoW will take more energy to solve the mathematical challenge with everyone's cooperation. People with the highest stakes can only operate blockchain nodes, and PoS energy consumption is lower than PoW. In contrast to PoW and PoS, however, the energy usage in PBFT and Ripple is low, as shown in Table 1 (17). By this comparison, improved consensus algorithms are more efficient than single consensus algorithms. The consensus blockchain architecture has reduced the average processing time of intensive transactions by approximately 26.3% compared to traditional blockchain designs. The proposed work focuses on integrating PoA with PBFT to compare results in terms of computational energy, latency, and transaction throughput with existing work.

Existing PoA-PBFT Methodology

Existing work focuses on a few key parameters, such as time consumption and transactions per second. The PoA-PBFT algorithm outperforms the PBFT algorithm by 51.8% to 64.7% (25). In addition, when compared to PBFT, the PoA-PBFT method can significantly reduce the time required for consensus.

$$C(txn) = C_{intrinsic}(txn) + C_{execution}(txn) + C_{deploy}(txn) \quad [1]$$

Equation [1] does not account for a gas return because it occurs after execution is complete and is unrelated to an exceptional transaction due to running out of gas. It should be noted that while Ethereum offers a gas reimbursement technique that reimburses a portion of the consumed energy at the time of transaction implementation, this process occurs after the transaction is

Proposed PoA-PBFT Methodology

The proposed work enhanced the PoA and PBFT consensus algorithms for improved computational efficiency, latency, and transaction throughput. This proposed methodology mainly concentrates on observing and measuring computational resources in pBFT and PoA-pBFT. Results were evaluated based on the following parameters: computational energy, latency, and transaction throughput. Computational resources as evaluated by gas cost, transaction cost, and execution cost.

Gas Cost

The amount of computing labour necessary to carry out an operation on the Ethereum network is measured in gas. On the Ethereum network, a specific amount of gas is required to complete each transaction and execute each smart contract. You must specify the amount of gas you are willing to pay when sending transactions for them to be processed.

Transaction Cost

In a blockchain network, users must pay transaction fees to engage with a smart contract. Although the term "gas fees" can refer to transaction costs on any blockchain, it is most commonly used to describe the transaction fees for the Ethereum network. Small portions of the native coin of the network are used to pay transaction fees.

Execution Cost

A blockchain's execution cost refers to the amount of resources (computing power, storage, and possibly other resources) required to perform specific actions on the blockchain network. These tasks often involve verifying transactions, executing smart contracts, and operationalising the blockchain. The execution cost is a crucial component of blockchain networks since it has a direct impact on the network's usability, efficiency, and scalability.

implemented and is not covered by the definition given above. Furthermore, regardless of the potential refunded gas, since this reimbursement occurs after execution is complete, any single out-of-gas execution will still induce state reversion. Intrinsic costs as outlined in Equations [2], [3], [4], and [5] only apply to external transactions. Internal transactions incur no fees. In other words,

Ethereum costs just an external transaction basis for its inherent gas cost. The deployment cost, as outlined in equations [6] and [7], only applies to transactions that create new contracts. If the gas is

exhausted, the entire transaction will fail, even if a preceding operation is completed using the remaining gas.

$$C_{intrinsic}(tx) = C_{input}(tx) + C_{create}(tx) + C_{basic}(tx) \quad [2]$$

$$C_{input}(tx) = \sum_{byte \in tx.input} \{4 \quad \text{if byte is zero} \quad 68 \quad \text{Otherwise} \} \quad [3]$$

$$C_{creation}(tx) = \{32000 \quad 0 \quad \} \quad [4]$$

$$C_{basic}(tx) = 21000 \quad [5]$$

$$C_{deploy}(tx) = \sum_{INS} C(INS) \quad [6]$$

$$C_{deploy}(tx) = \begin{cases} 200 \times |o| & \text{if tx.to is empty} \\ 0 & \text{Otherwise} \end{cases} \quad [7]$$

Table 2: Performance Analysis of pBFT and PoA-pBFT in terms of computational energy

Consensus Algorithm	Gas Cost	Transaction Cost	Execution Cost
PBFT	1394373	1212838	1079942
PoA-PBFT	546390	475247	392969

Results and Discussion

The existing pBFT and proposed PoA-pBFT results mentioned above were implemented in Python and deployed on the Ethereum blockchain platform using the Remix IDE. The results demonstrated that the proposed methodology outperforms the existing one. In this contribution, the gas cost, transaction cost, and execution cost in PoA-PBFT were reduced to 39.1853%, 39.1847%, and 36.3879%, respectively, as shown in Table 2, Figures 3, 4, 5, 6, and 7. Additionally, 0.1225 blocks were reduced in latency in PoA-PBFT. Transaction throughput improved to 13.534 transactions per

second in PoA-pBFT, as shown in Figures 7, 8, 9, and 10. Here, the proposed work focused on adding additional parameters, specifically computational resources, to measure the scalability of a blockchain. The proposed methodology was measured with the help of smart contracts. The outcome of this contribution is to strengthen the network and improve its scalability, leveraging various parameters such as computational resources, latency, and transactional throughput. PoA will enhance the entire network by eliminating unauthorised or faulty nodes.

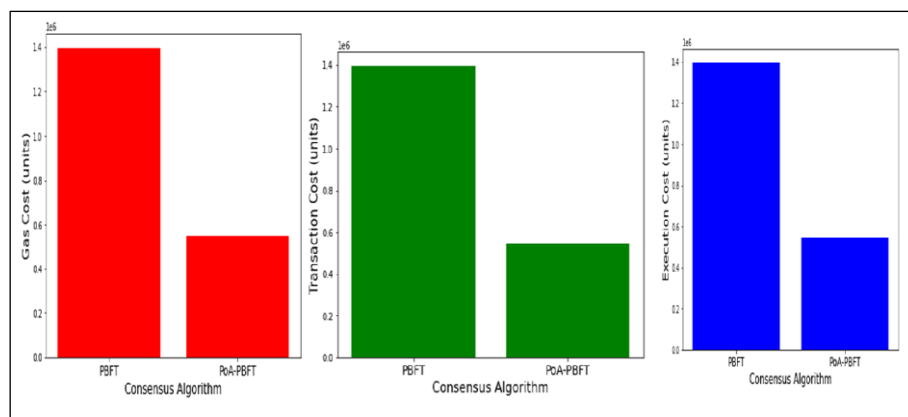
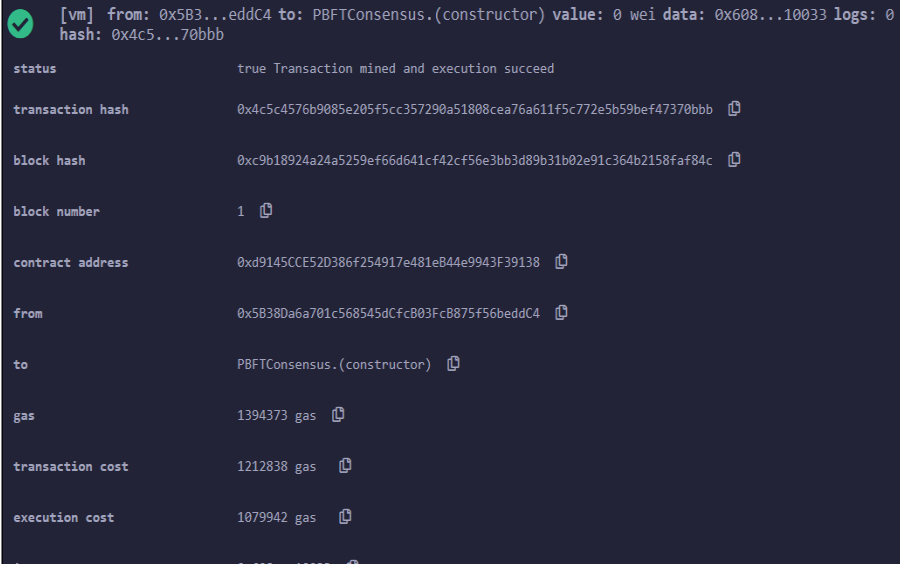


Figure 3: Performance Analysis of pBFT and PoA-pBFT in Terms of Computational Resources

In this observation of these two algorithm executions, PBFT consumes more computational energy compared to an improved model, i.e., PoA-PBFT (Table 2 and Figure 3). The overall performance of a blockchain is based on the factor

of scalability, specifically energy consumption. The cost of transaction completion is also based on the energy it consumes. Figures 4, 5, 6, and 7 are the platform-related proofs for the mentioned values in terms of energy consumption.



```

[vm] from: 0x5B3...eddC4 to: PBFTConsensus.(constructor) value: 0 wei data: 0x608...10033 logs: 0
hash: 0x4c5...70bbb

status      true Transaction mined and execution succeed

transaction hash  0x4c5c4576b9085e205f5cc357290a51808cea76a611f5c772e5b59bef47370bbb

block hash      0xc9b18924a24a5259ef66d641cf42cf56e3bb3d89b31b02e91c364b2158faf84c

block number    1

contract address 0xd9145CCE52D386f254917e481eB44e9943F39138

from           0x5B38Da6a701c56854dCfcB03FcB875f56beddC4

to             PBFTConsensus.(constructor)

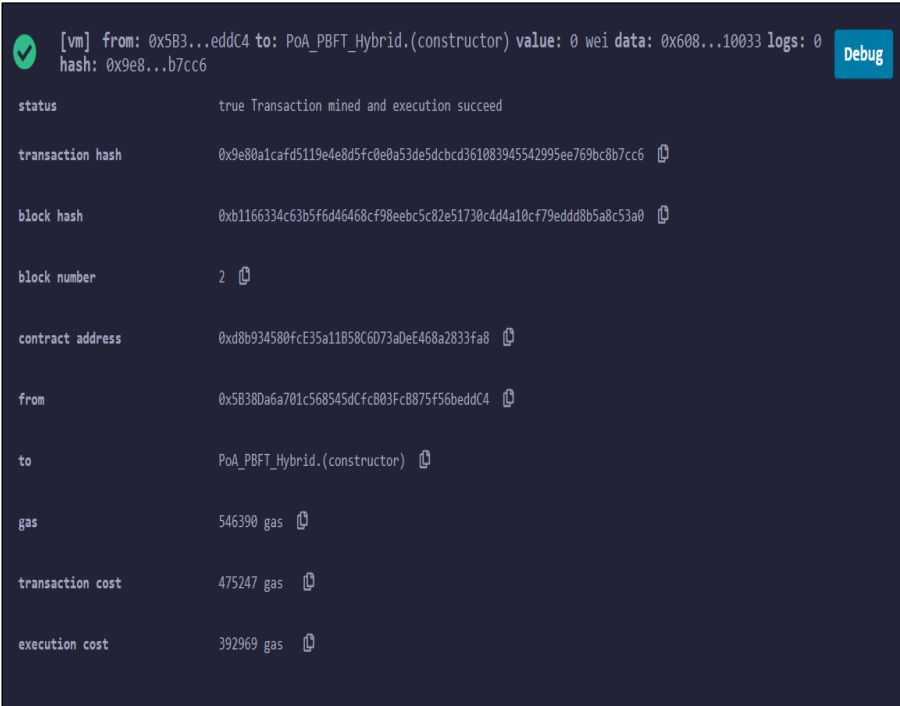
gas            1394373 gas

transaction cost 1212838 gas

execution cost  1079942 gas

```

Figure 4: pBFT Consensus Algorithm Computational Resources



```

[vm] from: 0x5B3...eddC4 to: PoA_PBFT_Hybrid.(constructor) value: 0 wei data: 0x608...10033 logs: 0
hash: 0x9e8...b7cc6

status      true Transaction mined and execution succeed

transaction hash  0x9e80a1cafd5119e4e8d5fc0e0a53de5dcbcd361083945542995ee769bc8b7cc6

block hash      0xb1166334c63b5f6d46468cf98eebc5c82e51730c4d4a10cf79eddd8b5a8c53a0

block number    2

contract address 0xd8b934580fcE35a11B58C6D73aDeE468a2833fa8

from           0x5B38Da6a701c56854dCfcB03FcB875f56beddC4

to             PoA_PBFT_Hybrid.(constructor)

gas            546390 gas

transaction cost 475247 gas

execution cost  392969 gas

```

Figure 5: PoA-PBFT Consensus Algorithm

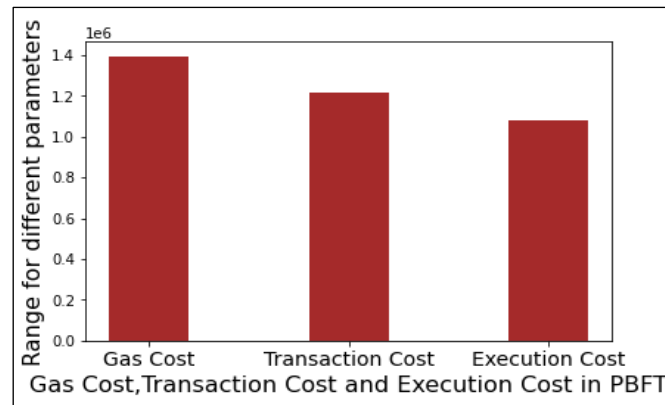


Figure 6: pBFT Consensus Algorithm in Terms of Gas Cost, Transaction Cost, and Execution Cost

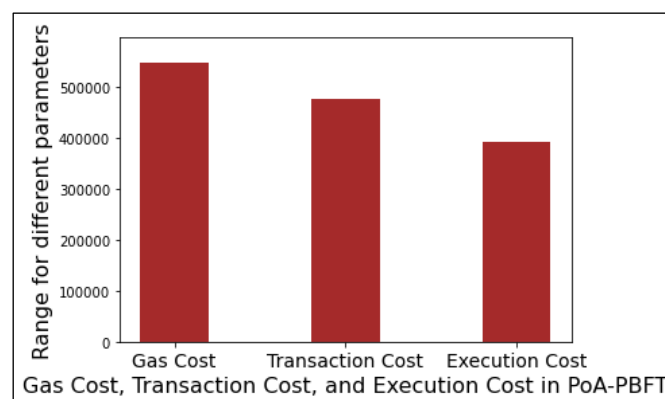


Figure 7: PoA-pBFT Consensus Algorithm in Terms of Gas Cost, Transaction Cost, and Execution Cost

Latency in pBFT

Figure 8. Considering five block data in a smart contract based on pBFT, which is a single consensus algorithm that achieves a latency of 1.3205 seconds and a transaction throughput of 50.74 transactions per second. Latency and transaction throughput are key scalability parameters that are essential for improving the overall performance of a blockchain. From Figures 10 and 11, the performance of a blockchain is illustrated graphically.

Latency in PoA and pBFT

Figure 8 considers five block data in a smart contract based on PoA-pBFT. This improved consensus algorithm achieves a latency of 1.1980 seconds and a transaction throughput of 64.27 transactions per second. When compared to the existing consensus algorithm, improvements are seen in PoA-pBFT. Figures 9 and 10 also depict the latency and transaction throughput performance based on the retrieved values. The individual consensus algorithm pBFT exhibits higher latency and lower transaction throughput compared to the proposed consensus algorithm, PoA-pBFT.

```

Processing Block 1 with 20 transactions.
Block 1: Pre-Prepare phase started.
Block 1: Prepare phase started.
Block 1: Commit phase started.
Block 1: Consensus reached in 0.2701 seconds.

Processing Block 2 with 20 transactions.
Block 2: Pre-Prepare phase started.
Block 2: Prepare phase started.
Block 2: Commit phase started.
Block 2: Consensus reached in 0.2568 seconds.

Processing Block 3 with 12 transactions.
Block 3: Pre-Prepare phase started.
Block 3: Prepare phase started.
Block 3: Commit phase started.
Block 3: Consensus reached in 0.2529 seconds.

Processing Block 4 with 6 transactions.
Block 4: Pre-Prepare phase started.
Block 4: Prepare phase started.
Block 4: Commit phase started.
Block 4: Consensus reached in 0.2803 seconds.

Processing Block 5 with 9 transactions.
Block 5: Pre-Prepare phase started.
Block 5: Prepare phase started.
Block 5: Commit phase started.
Block 5: Consensus reached in 0.2603 seconds.

PBFT Blockchain Simulation Results:
Block 1: 20 transactions, Latency = 0.2701 seconds.
Block 2: 20 transactions, Latency = 0.2568 seconds.
Block 3: 12 transactions, Latency = 0.2529 seconds.
Block 4: 6 transactions, Latency = 0.2803 seconds.
Block 5: 9 transactions, Latency = 0.2603 seconds.

Total Latency: 1.3205 seconds
Transaction Throughput: 50.74 transactions/second

```

Figure 8: Latency and Transaction Throughput in Pbft

```

In [13]: runfile('C:/Users/srira/untitled131.py', wdir='C:/Users/srira')
Block 1: Authority node Authority_Node_1 proposes the block.
Block 1: Consensus reached in 0.2340 seconds.
Block 2: Authority node Authority_Node_1 proposes the block.
Block 2: Consensus reached in 0.2324 seconds.
Block 3: Authority node Authority_Node_2 proposes the block.
Block 3: Consensus reached in 0.2021 seconds.
Block 4: Authority node Authority_Node_2 proposes the block.
Block 4: Consensus reached in 0.2346 seconds.
Block 5: Authority node Authority_Node_1 proposes the block.
Block 5: Consensus reached in 0.2950 seconds.

--- Blockchain Consensus Results ---
Block 1: 20 transactions, Latency = 0.2340 seconds.
Block 2: 13 transactions, Latency = 0.2324 seconds.
Block 3: 19 transactions, Latency = 0.2021 seconds.
Block 4: 11 transactions, Latency = 0.2346 seconds.
Block 5: 14 transactions, Latency = 0.2950 seconds.

Total Latency: 1.1980 seconds
Transaction Throughput: 64.27 transactions/second

```

Figure 9: Latency and Transaction Throughput in PoA-pBFT

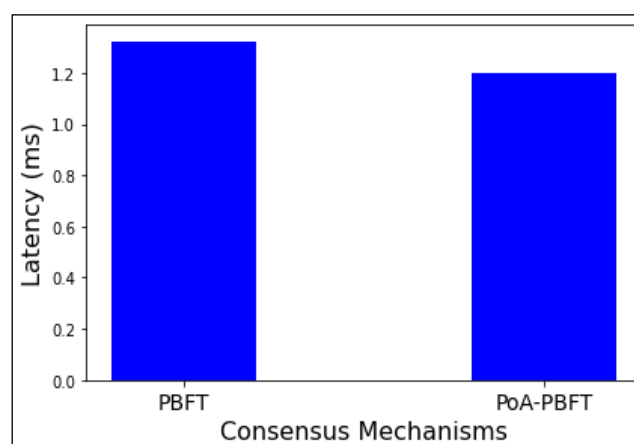


Figure 10: Latency in PoA and PoA-pBFT

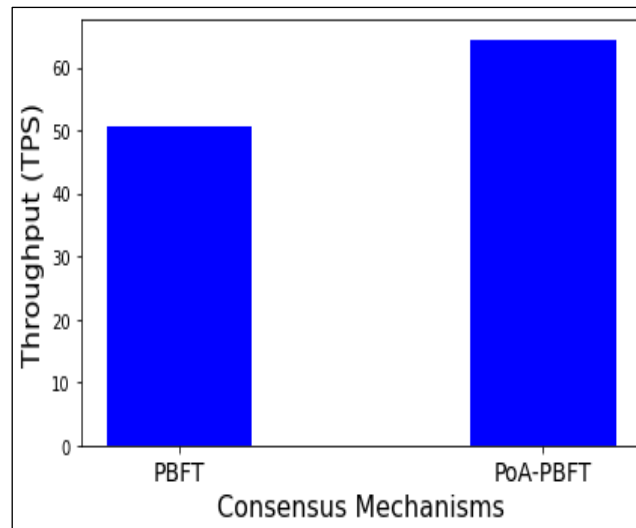


Figure 11: Transaction Throughput in PoA and PoA-pBFT

Conclusion

In this paper, the importance of blockchain consensus, its categories, and an improved consensus working methodology are demonstrated using relevant literature and experimental results. The proposed method primarily focuses on analysing different consensus algorithms in terms of their performance. Based on the observations, the improved consensus algorithm yields significantly lower gas, transaction, and execution costs for pBFT and PoA-pBFT. Computational energy was reduced in the enhanced model when compared to PBT. A change in consensus can avoid scalability and blockchain trilemma problems. Efficiency in consensus ultimately leads to satisfying the scalability parameters. Along with the performance, it concentrates on the authorisation, and providing security to the blockchain network is essential. Ultimately, this paper offers improvements in scalability, along with reduced costs for gas, transactions, execution, and authorisation.

Abbreviations

G2G: Group-to-group, DPOS: Delegate Proof of Stake, pBFT: Practical Byzantine Fault Tolerance, PoA: Proof of Authority, PoAh: Proof of Authority Hybrid, PoET: Proof of Elapsed Time, PoP: Proof of Participation, PoR: Proof of Reputation, PoS: Proof of Stake, POT: Proof of Trust, PoV: Proof of Vote, PoW: Proof of Work, PUFs: Physical Unclonable Functions, VaaP: Votes-as-a-Proof.

Acknowledgment

None.

Author Contributions

Each author contributed equally.

Conflict of Interest

No conflict of interest.

Ethics Approval

Not applicable.

Funding

None.

References

1. Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, Qiaoyan Wen. A survey on the security of blockchain systems. *Future Generation Computer Systems*. 2020;107:841- 853.
2. Cali U, Cakir O. Energy policy instruments for distributed ledger technology empowered peer-to-peer local energy markets. *IEEE access*. 2019 Jun 19;7:82888-900.
3. Shahaab A, Lidgey B, Hewage C, Khan I. Applicability and appropriateness of distributed ledgers consensus protocols in public and private sectors: A systematic review. *IEEE access*. 2019 Mar 21;7:43622-36.
4. Wang Y, Tang C, Lin F, Zheng Z, Chen Z. Pool strategies selection in pow-based blockchain networks: Game-theoretic analysis. *IEEE Access*. 2019 Jan 2;7:8427-36.
5. Wilhelmi F, Barrachina-Muñoz S, Dini P. End-to-end latency analysis and optimal block size of proof-of-work blockchain applications. *IEEE Communications Letters*. 2022 Jul 28;26(10):2332-5.
6. Li X, Xu J, Fan X, Wang Y, Zhang Z. Puncturable signatures and applications in proof-of-stake blockchain protocols. *IEEE Transactions on Information Forensics and Security*. 2020 Jun 11;15:3872-85.
7. Nguyen CT, Hoang DT, Nguyen DN, Niyato D, Nguyen HT, Dutkiewicz E. Proof-of-stake consensus

- mechanisms for future blockchain networks: fundamentals, applications and opportunities. *IEEE access*. 2019 Jun 26;7:85727-45.
8. Nair PR, Dorai DR. Evaluation of Performance and Security of Proof of Work and Proof of Stake using Blockchain. *IEEE Xplore*. 2021;279-83. 10.1109/ICICV50876.2021.9388487
 9. Bentov I, Lee C, Mizrahi A, Rosenfeld M. Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake. *Association for Computing Machinery*. 2014;42(3):34-7.
 10. Boreiri Z, Azad AN. A Novel Consensus Protocol in Blockchain Network based on Proof of Activity Protocol and Game Theory. *8th International Conference on Web Research (ICWR)*. 2022;82-7. <https://ieeexplore.ieee.org/abstract/document/9786224>
 11. Kaur M, Khan MZ, Gupta S, Noorwali A, Chakraborty C, Pani SK. MBP: Performance analysis of large scale mainstream blockchain consensus protocols. *Ieee Access*. 2021 May 31;9:80931-44.
 12. Cao Z, Kong J, Lee U, Gerla M, Chen Z. Proof-of-relevance: Filtering false data via authentic consensus in vehicle ad-hoc networks. In *IEEE INFOCOM Workshops 2008*. IEEE. 2008 Apr 13:1-6. <https://ieeexplore.ieee.org/abstract/document/4544650>
 13. Maroufi M, Abdolee R, Tazekand BM, Mortezaei SA. Lightweight Blockchain-Based Architecture for 5G-Enabled IoT. *IEEE Access*. 2023; 11:60223-39.
 14. Baseera A, Alsadhan AA. Enhancing Blockchain Security Using Ripple Consensus Algorithm. *Computers, Materials & Continua*. 2022;73(3):4713-26.
 15. Chaudhari KG. E-Voting System Using Proof of Voting (PoV) Consensus Algorithm. *SSRN Electronic Journal*. 2018; 7:4051-5.
 16. Killer C, Rodrigues B, Scheid EJ, Franco MF, Stiller B. Blockchain-Based Voting Considered Harmful? *IEEE Transactions on Network and Service Management*. 2022;19(3):3603-18.
 17. Fu X, Wang H, Shi P. Votes-as-a-Proof (VaaP): Permissioned Blockchain Consensus Protocol Made Simple. *IEEE Transactions on Parallel and Distributed Systems*. 2022;33(12):4964-73.
 18. Oprea SV, Băra A, Andreescu AI, Cristescu MP. Conceptual Architecture of a Blockchain Solution for E-Voting in Elections at the University Level. *IEEE Access*. 2023; 11:18461-74.
 19. Zhu X, Li Y, Fang L, Chen P. An Improved Proof-of-Trust Consensus Algorithm for Credible Crowdsourcing Blockchain Services. *IEEE Access*. 2020; 8:102177-87.
 20. Ali V, Norman AA, Azzuhri SRB. Characteristics of Blockchain and Its Relationship with Trust. *IEEE Access*. 2023; 11:15364-74.
 21. Zou J, Ye B, Qu L, Wang Y, Orgun MA, Li L. A Proof-of-Trust Consensus Protocol for Enhancing Accountability in Crowdsourcing Services. *IEEE Transactions on Computing Services*. 2019;12(3):429-45.
 22. Puthal D, Mohanty SP. Proof of Authentication: IoT-Friendly Blockchains. *IEEE Potentials*. 2019;38(1):26-9.
 23. Qushtom H, Mišić J, Mišić VB, Chang X. A Two-Stage PBFT Architecture with Trust and Reward Incentive Mechanism. *IEEE Internet of Things Journal*. 2023;10(13):11440-52.
 24. Liu B, Chen Z, Zhang Y, Xiong L, Yang X, Chen S. A New Group-to-Group Authentication Scheme Based on PUFs and Blockchain. *IEEE 6th International Conference on Signal and Image Processing (ICSIP)*. 2019;279-83. <https://ieeexplore.ieee.org/abstract/document/8868807>
 25. Zhang J, Tian R, Cao Y, Yuan X, Yu Z, Yan X. A Hybrid Model for Central Bank Digital Currency Based on Blockchain. *IEEE Access*. 2021; 9:53589-601.