A Next-Generation Blockchain Consensus Model for Efficient Credential Verification

Mayuri Rangari [1;] Manvi Godbole [2;] Aruna Chamatkar [3]

[1]Department of Masters in Computer Applications, G H Raisoni College of Engineering and Management Nagpur, Maharashtra, India
[2]Department of Masters in Computer Applications, G H Raisoni College of Engineering and Management Nagpur, Maharashtra, India
[3] Department of Computer Science, Kamla Nehru Mahavidyalaya, Nagpur, Maharashtra, India.

Abstract- Blockchain Technology a Powerful Solution To Securely Verify Digital Credentials Nonetheless, traditional consensus mechanisms such as Proof of Work (PoW) and Proof of Stake (PoS) also have disadvantages, such as extensive energy expenditure, scalability limitations, and possible centralization risks. In order to overcome these issues, this study proposes a hybrid consensus model combining Delegated Proof of Authority (DPoA) with sharding. This method increases efficiency, accelerates transaction speed, minimizes latency, and preserves a decentralized validation process. According to the evaluation, its empirical performance exceeds many traditional consensus methods, leading to efficient credential verification for large-scale distributed users.

Keyword:
Nature-inspired algorithm, Dominance hierarchy

1.Introduction

Credential verification is a very important and essential process in the education, employment, and professional certifications, ensuring authenticity, integrity and preventing fraud.

Traditional academic credential verification is the process of confirming the authenticity of academic qualifications, which typically involves manual checks by the issuing institution or a third-party verification service, which contacts the school or university to confirm the details of the credential, such as the degree awarded, the dates of study, and the individual's academic performance, leading to delays, high costs, and vulnerabilitytotampering.Blockchain-based credentialing offers various benefits such as decentralized alternative, provide security and immutability, transparency, reduces fraud, global access etc but there are some issues associated with the implementation such as:

1.High Gas Fees: Transaction costs associated with Ethereum-based credential verification are high. **Slow Processing Speed**: Validation time is impacted bynetworkcongestion.
Scalability Issues: Single-chain processing causes bottlenecks in the PoW and PoS algorithms.

2.Commonly used consensus mechanisms, such as Proof of Work (PoW) and Proof of Stake (PoS), have various advantages but also have many limitations. PoW requires considerable computational power, whereas PoS is vulnerable to centralization by wealthier stakeholders. To overcome these challenges, a hybrid consensus mechanism is proposed, which integrates Delegated Proof of Authority (DPoA) and sharding, thereby creating a more efficient and scalable solution for blockchain-based credential verification.

This research builds upon these findings, integrating DPoA and sharding to balance security, efficiency, and decentralization.

2. Related Work

Several studies have proposed various blockchain consensus mechanisms for credential verification.

PoW (Proof of Works) mechanism, ensures security but is highly energy-intensive [3]. PoS(Proof of Stacks) improves energy efficiency but may lead to wealth-based centralization [4]. Delegated Proof of Stake (DPoS) enhances transaction speed but requires trust in elected validators [5]. Sharding has been proposed as a method to improve blockchain scalability by partitioning the network [6].

3. Proposed Hybrid Consensus Mechanism

3.1 Delegated Proof of Authority (DPoA)

By adding a delegation structure, Delegated Proof of Authority (DPoA) improves on conventional Proof of Authority (PoA). To provide a more decentralized and democratic process, stakeholders might assign their voting power to trusted validators rather than a

DOI: https://doi.org/10.5281/zenodo.18335733

predefinedgroupofvalidators.
Validators in DPoA are in charge of keeping the blockchain up to date and confirming transactions. Network integrity can be preserved by allowing stakeholders to vote for a validator to be replaced if they behave maliciously. With its quicker transaction finality, reduced energy usage, and enhanced efficiency over PoW and PoS, DPoA is perfect for permissioned and semi-permitted blockchains

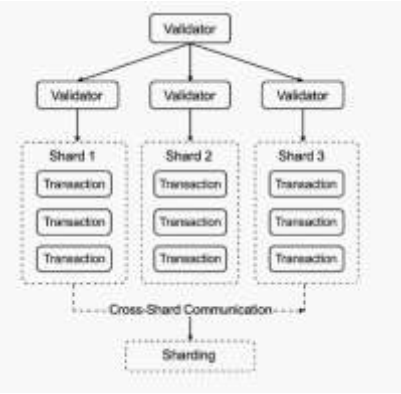
3.2 Sharding for Scalability

Blockchain supports scalability, which is possible only because of sharding. Sharding divides the entire network into smaller, autonomous shards, which handle individual transactions. This continuous and automatic processing lowers congestion and improves throughput.
Sharding is mainly divided into the following categories:

- **Network Sharding:** Nodes are divided into smaller groups, and each group manages a particular shard.
- **Transaction Sharding**: In order to execute a transaction in parallel, transactions are divided into shards.
- **State Sharding**: This technique divides blockchain data into shards to improve storage efficiency.

In the proposed hybrid consensus framework, the characteristics of DPoA and sharding are combined to create a decentralized and more scalable framework, avoiding data fragmentation through cross-shard interaction and enabling shards to function individually while validators ensure security.

Figure 1 depicts this architecture, displaying how DPoA validators coordinate shard operations to optimize blockchain productivity.

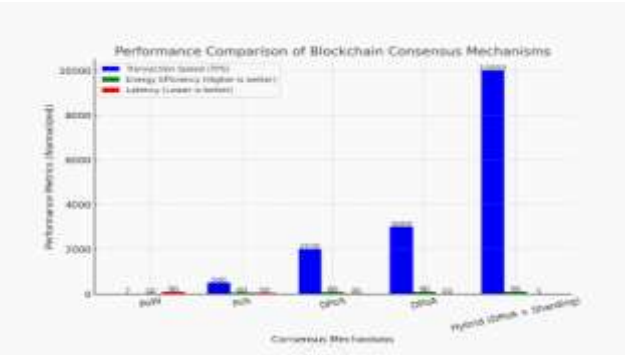


Performance Evaluation

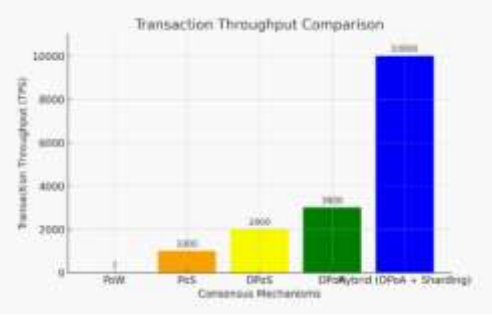
In order to evaluate the effectiveness of the proposed model, we conducted simulations comparing the approach we proposed to PoW, PoS, and DPoS-based systems. Among the primary indicators of performance studied are:

- Transaction Throughput: The number of transactions processed per second (TPS).
- Latency: The time required for a transaction to be confirmed.
- Energy Efficiency: The computational power required for validation.

Table 1 presents a comparative analysis of consensus mechanisms.



[Table 1: Performance Comparison of Consensus Mechanisms]



[Figure 2: Graph Comparing Transaction Throughput]
Security Analysis
As Delegated Proof of Authority (DPoA) and sharding reduce single points of failure, they improve security. When DPoA identifies validators based on accountability and trust, the probability of malicious activity is reduced. By further isolating security risks within distinct shards, sharding helps to stop widespread attacks [8].

6. Conclusion and Future Work

This paper demonstrates that combining DPoA and sharding offers a scalable and secure solution for blockchain-based credential verification. The proposed hybrid consensus mechanism significantly enhances transaction efficiency while maintaining decentralization and security. Future research will focus on real-world implementation and optimizing inter-shard communication to further improve performance.

DOI: https://doi.org/10.5281/zenodo.18335733

References

1. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
2. King, S., & Nadal, S. (2012). PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake.
3. Buterin, V. (2013). Ethereum Whitepaper: A Next-Generation Smart Contract and Decentralized Application Platform.
4. Larimer, D. (2014). Delegated Proof-of-Stake (DPoS) Consensus Algorithm - BitShares.
5. Zamani, M., Movahedi, M., & Raykova, M. (2018). RapidChain: Scaling Blockchain via Full Sharding. ACM CCS.
6. Wood, G. (2016). Ethereum: A Secure Decentralized Generalized Transaction Ledger.
7. Kokoris-Kogias, E., Jovanovic, P., et al. (2018). OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding. IEEE S&P.
8. Lu, Q., & Xu, X. (2019). Adaptable Blockchain-Based Systems: A Survey. Future Generation Computer Systems.
9. Wang, W., Liu, J., et al. (2020). A Survey on Consensus Mechanisms and Mining Strategies in Blockchain. IEEE Access.
10. Gupta, M., Soni, P., & Verma, A. (2021). Enhancing Blockchain Security and Scalability Using Hybrid Consensus Models. Springer.
11. Liang, J., Zhao, H., et al. (2022). An Efficient and Secure Blockchain-Based Credential Verification Model. IEEE Transactions on Network and Service Management.
12. Zhang, Y., Wang, L., et al. (2023). Sharding and Hybrid Consensus for Scalable and Secure Blockchain Applications. ACM Computing Surveys.
13. Hussain, S., Tariq, M., et al. (2023). Comparative Analysis of Blockchain Consensus Mechanisms. IEEE Blockchain Symposium.
14. Li, F., & Chen, X. (2023). The Role of Delegated Proof of Authority in Reducing Latency in Blockchain Networks. Springer Journal of Blockchain Research.

DOI: https://doi.org/10.5281/zenodo.18335733