ISSN: 2096-3246
Volume 58, Issue 01, 2026

CONSENSUS MECHANISM WITH DYNAMIC SCORING AND ADVANCED OPTIMIZATION THROUGH MACHINE LEARNING FOR ENHANCING BLOCKCHAIN EFFICIENCY

Mohammed Mueen Pasha M[*,1][0000-0002-8354-1958], **Sandeep J**[2][0000-0002-6631-0453]
[1,2] CHRIST University, India
mohammed.m@res.christuniversity.in
sandeep.j@christuniversity.in

ABSTRACT

Blockchain technology is emerging as one of the most enabling technologies of this century as it offers distinctive features like transparency, security and immutability. Consensus mechanism is a critical component to establish acceptance among the nodes on the current state of the blockchain. Various consensus protocols such as Proof of Work (PoW), Proof of Stake (PoS) are energy intensive and require extensive computational resources to bring agreement. As blockchain is revolutionizing various domains it also necessitates a novel consensus protocol to be build that will enhance efficiency through optimizations and integrations. This study proposes modified Proof of Reputation (mPoR), an optimized consensus mechanism based on dynamic scoring. mPoR can also effectively use various adaptive security methods to deter any malicious behavior in a dynamic peer to peer network. The pre-diction of network congestion and decentralization of consensus process can be achieved by integration of Reputation Dynamics Optimization (ReDO) which is a machine learning optimization method. mPoR along with ReDO is a promising innovation as applications requiring scalable, secure and high-performance decentralized systems can adopt this mechanism to enhance the overall efficiency. The incentive mechanism allows the nodes of the network with higher reputation to continue the engagement and boost reliability of the blockchain. The findings of the research is paramount as it can be utilities in new fields that require high efficiency, scalability and security.

Keywords: Blockchain Efficiency, Proof of Reputation (PoR), Dynamic Scoring, Consensus Optimization, Machine Learning Integration

1. INTRODUCTION

Blockchain technology originated in 2008 from a paper authored by Nakamoto, Satoshi “Bitcoin: A peer-to-peer electronic cash system."[14] It serves as the foundational framework for cryptocurrencies such as Bitcoin. Since its inception, block-chain [11] has evolved into a multifaceted and transformative digital ledger capable of recording dealings through numerous computers in a way that inhibits retrospective adaptations. This expertise is crucial not only due to its association with digital currencies [13] but also because of its latent to modernize different businesses by improving transparency, security, and operational efficiency. At its central, a block-chain is a dispersed and disseminated register system [3] [13]. It comprises a devel-oping list of registers, recognized as blocks, which are strongly connected through cryptographic hashes. Each block contains a hash of the earlier block, a timestamp, and operation data, ensuring that once information is recorded, it be-

comes exceedingly difficult to modify deprived of changing all following blocks, which would necessitate the network's consensus. The decentralized nature of block-chain [11][15], maintained by a system of nodes participating in a consensus contrivance to validate and record transactions, decreases the risk of solitary opinions of disaster and improves the system's resilience against tampering and cyber-attacks. Block-chain models can be used in student information system [5][14], where immutability, transparency and security become pivotal. The importance of blockchain technology in today's digital landscape is immense. Although blockchain enables secure and transparent working it still faces challenges that hinder adoption of this technology widely. Security, scalability, throughput and energy consumptions are a few of the several factors which contribute to its growth significance. Scalability, the capability of a blockchain to lever a rising quantity of connections, is a major concern. Most communal block-chains, like Bitcoin and Ethereum, have limited transaction processing capabilities, with Bitcoin processing approximately seven transactions [14][20] per second and Ethereum around fifteen. In contrast, customary expense structures like Visa can lever thousands of connections per second. This restriction arises because all nodes in the network must reach a consensus, which is time-consuming and computationally intensive. Another critical issue is energy depletion. The consensus contrivances used in numerous blockchain networks, particularly Proof of Work (PoW), are highly energy-intensive, requiring miners to resolve difficult scientific difficulties to authenticate connections and augment new blocks to the chain. This procedure in-gests vast amounts of electricity, raising environmental concerns. For instance, Bitcoin mining consumes more electricity annually than some entire countries, making it unsustainable in the long run [18][19]. Related to scalability, transaction throughput, the ratio at which connections are handled and confirmed, is also a significant barrier. Low throughput results in leisurelier operation times and advanced fees, particularly in phases of high request, posing a substantial obstacle for applications that require fast and efficient processing, such as real-time payments and high-frequency trading [8]. Addressing these tests is critical for the future of blockchain technology, and enhancing efficiency through innovative optimizations and integrations is essential to unlock its full potential. Efficiency is a primary factor and it is discussed in detail in Table 1. Level 2 resolutions, such as the Lightning Network for Bitcoin and Plasma for Ethereum, target to surge operation [4] throughput by moving transactions off the main blockchain and onto secondary layers. These solutions can process thousands of connections off-chain, only relaxing the last state on the core blockchain [2], significantly improving scalability and reducing fees [8] [16]. Transitioning from energy-intensive PoW to further effectual consensus contrivances, such as Proof of Stake (PoS) or Delegated Proof of Stake (DPoS), can drastically reduce energy consumption. PoS, for example, allows validators to propose and validate chunks built on the quantity of coins they hold and are eager to "stake" as security, relatively than resolving complex puzzles. Sharding, which contains separating the blockchain into reduced, more controllable fragments called shards, allows every shard to route its connections and smart contracts unconventionally, enhancing scalability and throughput. These issues are handled by using sharding in Ethereum 2.0 [19]. Therefore, integration of Polkadot and Cosmos two popular blockchain network, can be a solution to enhance efficiency sharing of data and improving the communication between interoperating blockchain networks.

2. LITERATURE SURVEY

Recent advancements in blockchain technology have significantly enhanced security, scalability, and efficiency across various applications, particularly in Internet of Things (IoT) networks. Ehtisham et al. (2024) introduced a scalable blockchain framework using Delegated Proof of Stake (DPoS), Interplanetary File System (IPFS), and Docker, demonstrating low latency and high throughput, effectively managing up to 20,000 devices with a latency of less than 0.976 milliseconds. [15] A blockchain for a self-configured wireless network that is used to monitor physical and environmental phenomena, commonly known as wireless Sensor Networks (WSN) used Proof of Stake (PoS). [15] the proposed a blockchain architecture enhanced security and transparency and achieved notable scalability and low latency. The Blockchain architecture developed [3] swiftly handles the challenges by integrating Artificial intelligence, Internet of Things(IoT) and Blockchain. This work focused to significantly assist small and medium scale enterprises (SMEs) by improving interoperability, security and resource utility. The authors developed a unique architecture and named it as B-SME framework which allowed an amalgamation of various technologies to strengthen the integrity of their work. In order to enhance the transactional speed and energy the authors proposed a HIBchain as a consortium blockchain of multilayers. A Diversity Mining based Proof of Work (DM-PoW) protocol is used in this multilayered consortium blockchain network. [9]. Another study introduced a node-based scalable model for Blockchain Storage Systems (SMBSS), which effectively improved shard availability and facilitated the management of large-scale data environments [21]. Additionally, research by [10] examined the issue of energy depletion in blockchain systems, emphasizing how refined consensus mechanisms could play a vital role in significantly lowering energy consumption. Collectively, as outlined in Table 1, these contributions underscore key advancements in blockchain technology. They point toward a future of more efficient, scalable systems made possible through thoughtful consensus design and architectural innovation.

Table 1. Review of Advancements and Applications of Blockchain Technology for improving Efficiency

S.No	Study and Year	Focus	Key Contributions & Findings	Results
1	Ehtisham et al. 2024	Blockchain for IoT networks	Proposed a scalable blockchain framework with DPoS, IPFS, and Docker, achieving low latency, high throughput, and outperforming PoS.	Framework showed low latency (<0.976 ms) and outperformed PoS in throughput and resource utilization.
2	Maftei et al. 2023	Blockchain for secure IoT	Developed a PoS-based blockchain architecture for Wireless Sensor Networks	Architecture ensured low latency (55.4 ms for 500 nodes, 4.2 s for

		data management	(WSNs), ensuring high performance, low latency, and scalability.	20,000 nodes) and high scalability.
3	Abdullah et al. 2023	Blockchain for SME operations	Introduced the B-SMEs framework integrating blockchain, IoT, and AI to enhance efficiency, reduce resource consumption, and optimize data management.	Increased ledger management rate by 17.3%, reduced computational resource use by 9.13%, and decreased bandwidth and storage use by 14.11% and 7.9% respectively.
4	Jayabal et al. 2021	Consortium blockchain for IoT	Developed HIBchain using DM-PoW, achieving high transaction speeds and energy efficiency for IoT networks.	Achieved an usual handling period of 1760 TPS and a mining period of 3 minutes, with 60.34% smaller transaction size compared to baseline.
5	Xing Fan 2022	Scalability of blockchain storage systems	Proposed SMBSS for scalable blockchain storage, with experimental results showing improved shard availability and scalability.	Experimental results showed 100% shard availability with 52 nodes online, indicating high scalability and reliability.
6	Johannes et al. 2020	Energy consumption in blockchain	Reviewed blockchain energy consumption, identifying significant differences and suggesting further research into consensus mechanisms.	Demonstrated that energy consumption varies significantly across systems, with centralized and small-scale blockchains consuming much less energy than PoW blockchains.
7	Rozman et al. 2023	Blockchain-Based Shared Manufacturing (BBSM)	Investigated blockchain scalability limitations in Blockchain-Based Shared Manufacturing (BBSM) and their impact on performance and user behavior.	Scalability limitations increase transaction costs and reduce service prices, leading to underutilization of production capacities.
8	Sohail et al. 2023	Blockchain Network Scalability	Proposed a consensus method to enhance the scalability of Private Blockchains by reducing latency and network workload.	System capable of 200,000 transactions per second, with latency reduced and scalability enhanced.

9	Ricardo et al. 2023	Proof-of-Reputation (PoR) for Decentralized PoW	Introduced Proof-of-Reputation (PoR) for Bitcoin, combining PoW with cryptographic reputation to reduce energy consumption while maintaining security.	Achieves a 30% reduction in energy consumption for the same security level.
10	Sarfaraz et al. 2023	Supply Chain Management (SCM)	Proposed Reputation-based Proof of Cooperation (RPoC) for scalable and efficient consensus in decentralized systems.	Maintains valid blocks even with malicious nodes, improving scalability and efficiency.
11	Oladotun et al. 2021	Reputation-Based Consensus Mechanism	Proposed Proof-of-Reputation (PoR) to ensure secure and efficient consensus in blockchain systems.	Achieves up to 1,100 transactions per second with varying network sizes and transaction numbers.

While several consensus mechanisms—such as Proof-of-Reputation (PoR) and its variants—have been proposed to improve the security and efficiency of blockchain networks, there remains a notable lack of attention on the role of dynamic reputation scoring and its effect on participant trust and engagement. Many existing models, even those grounded in PoR, tend to overlook how shifts in reputation scores influence user behavior and overall system performance. This represents a critical gap in current research. [1] Demonstrates one of the most underexplored domain of integrating machine learning with blockchain, especially the usage of machine learning in a consensus mechanism like PoR to dynamically assign or adjust reputation score. Dynamic allocation of reputation score can be a breakthrough on how a consensus mechanism learns and adapts in real time environments.

3. PROBLEM STATEMENT & RESEARCH OBJECTIVE

Consensus protocols in blockchain face challenges related to scalability, latency, resource consumption, and throughput (transactions per second). Conventional protocols like Proof of Work (PoW) and Proof of Stake (PoS) suffer from these limitations. There is a need to develop a mechanism that will enhance scalability, security and efficiency of the blockchain network. The authors of this work propose Modified Proof of Reputation(mPoR) integrated with Machine learning based optimization method, Reputation Dynamic Optimization. Both the methods constitute into a framework that addresses the aforementioned challenges by performing dynamic reputation scoring and dynamic optimization of those scores. The primary objectives of this study are:

To monitor and analyze the impact of mPoR based on the dynamic scoring technique to achieve scalability and higher efficiency in the blockchain environment.

- To assess the improvements in system performance—specifically throughput and latency—alongside gains in scalability (in terms of network size and transaction volume) and security (with a focus on resistance to Sybil attacks) resulting from the integration of the ReDO-enhanced mPoR mechanism.

4. MODIFIED PROOF OF REPUTATION (mPoR)

The proposed Modified Proof of Reputation is a consensus protocol designed to improve blockchain performance. it enhances the efficiency, scalability, trust-worthiness and security. Flowchart of the proposed mPoR is depicted in the figure 1. The proposed Modified Proof of Reputation is a consensus protocol designed to improve blockchain performance. This method allows participants with higher reputation score to contribute.

4.1 Dynamic Reputation Scoring (DRS)

A typical Dynamic Reputation Scoring involves the steps to adjust the reputation of each node on the network by assessing the previous performances. In the equation 1 i represents the node number and t represents the time respectively. R_i (t) refers to the reputation value for the i^{th} node at the time t. The equation 1 has four constant values most relevant to the blockchain network. The symbol α represents the weightage of the last reputation score of this node i, Weightage of performing validation activities and authentication tasks is represented by β, Contribution to the network is a vital parameter to quantify and it is represented as γ. Finally. any malicious behaviors or failed tasks are represented as penalty using the symbol δ.

$$R_i(t) = \alpha R_i(t-1) + \beta A_i(t) + \gamma C_i(t) - \delta M_i(t) \quad (1)$$

- Historical Reputation $\alpha R_i(t-1)$ ensures that the previous reputation is taken into account, providing stability to the scoring system.
- Authentication and Validation Activities $\beta A_i(t)$ Nodes gain reputation by successfully participating in authentication and validation activities.
- Contributions to the Network $\gamma C_i(t)$ Nodes contribute by creating and propagating blocks, which increases their reputation.
- Malicious Activities $\delta M_i(t)$ Nodes lose reputation if they engage in malicious activities or fail to comply with the network's protocols.

4.1.1 Reputation Decay

The decay mechanism represented in equation 2 represents ensures that the reputation score decays over time. Each node should earn the reputation as it is not retained permanently. This ensures that the nodes maintain a consistent and positive behaviour in the network and works on improving it because the reputation score depletes over time.

$$R\_i\ (t) = \rho R\_i\ (t\text{-}1) + (1\text{-}\rho)\ (\beta A\_i\ (t) + \gamma C\_i\ (t) - \delta M\_i\ (t)) \quad (2)$$

Where R_i (t) is Reputation score of node i at time t, ρ is Decay factor (0<ρ<1), A_i (t) is Authentication and validation activities, C_i (t) is Contributions to the network, M_i (t) is Malicious activities or failures, β,γ,δ are Weights assigned to activities and penalties. p in the equation 2 is the decay aspect which has significant influence on the reputation grades. The decay factor p also enables

nodes in the network to consistently perform well by maintaining a positive behaviour across the network and contribute effectively

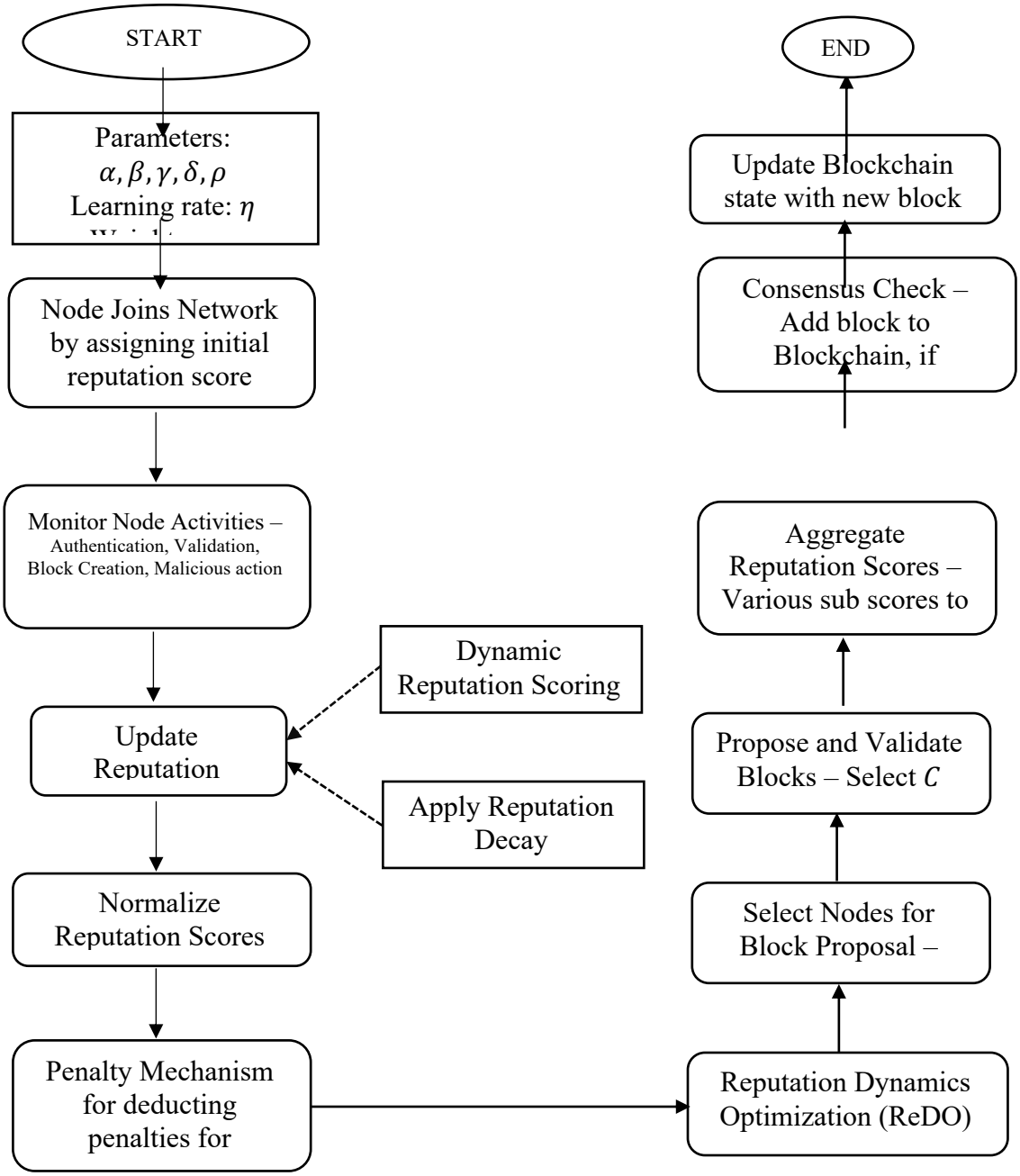


Figure 1. Flowchart of the proposed mPoR

5. REPUTATION DYNAMICS OPTIMIZATION (ReDO)

Reputation Dynamics Optimization (ReDO) utilizes machine learning techniques to refine reputation scoring and strengthen the consensus mechanism. The goal is to improve the overall performance of the blockchain network by enhancing efficiency (in terms of throughput and latency),

scalability (across both network size and transaction volume), and security, with a particular focus on resilience against Sybil attacks.

5.1 Machine Learning Model for ReDO

A machine learning model in equation 3, such as a neural network, can be trained to predict the optimal reputation scores. The inputs to the model include various features like historical reputation, network contributions, and penalty records.

$$R_i'(t) = f(R_i(t-1), A_i(t), C_i(t), M_i(t);\ \theta) \qquad (3)$$

where $R_i'(t)$ is Predicted reputation score for node i at time t, f is the Machine learning function parameterized by θ. The loss function for training the model can be defined as in equation 4

$$L(\theta) = \sum_{i=1}^{N}\left(R_i(t) - R_i'(t)\right)^2 + \lambda\Omega(\theta) \quad (4)$$

where N is the Number of nodes, $\Omega(\theta)$ is Regularization term to prevent overfitting and λ is Regularization coefficient. The goal is to find the parameters θ that minimize the loss function, ensuring accurate and generalizable predictions of reputation scores. To optimize the parameters θ of the machine learning model, gradient descent is used. The parameters are updated iteratively to minimize the loss function in equation 5.

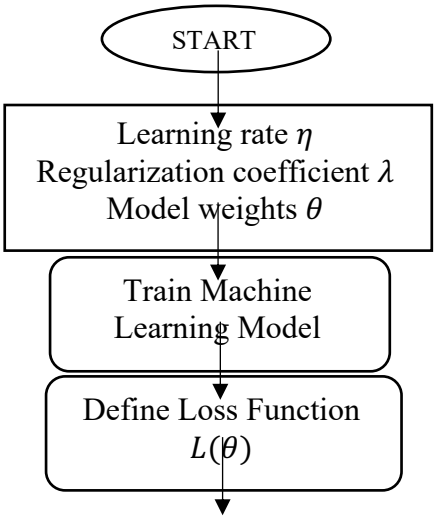
$$\theta_{new} = \theta_{old} - \eta\nabla_\theta L(\theta) \quad (5)$$

where θ_{new} is Updated parameters, θ_{old} is Current parameters, η is Learning rate and $\nabla_\theta L(\theta)$ is Gradient of the loss function with respect to θ.

The gradient $\nabla_\theta L(\theta)$ is the vector of partial derivatives of the loss function with respect to each parameter. It indicates the direction and rate of the fastest increase of the loss function as by equation 6.

$$\nabla_\theta L(\theta) = \left\{\frac{\partial L(\theta)}{\partial\theta_1}, \frac{\partial L(\theta)}{\partial\theta_2}, \ldots, \frac{\partial L(\theta)}{\partial\theta_m}\right\} \quad (6)$$

In each iteration, the parameters are updated by moving in the opposite direction of the gradient. The magnitude of this step is determined by the learning rate η. A smaller η results in smaller steps, which can lead to a more precise convergence but requires more iterations. A larger η speeds up convergence but risks overshooting the minimum. This update process is repeated for a specified number of iterations or until the change in the loss function is below a predefined threshold, indicating convergence as shown in the figure 2.



ISSN: 2096-3246
Volume 58, Issue 01, 2026

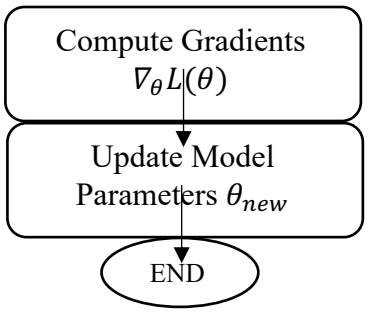


Figure 2. Flowchart of the proposed ReDO

The machine learning model aggregates different factors affecting reputation to predict the optimal score in equation 7. This involves creating a composite function that accounts for various node activities.

$$R_i'(t) = f(\sum_{k=1}^{K} \omega_k R_{ik}(t); \theta) \quad (7)$$

Where ω_k is Weight assigned to the k-th activity and $R_{ik}(t)$ is Sub-score for the k-th activity for node i. Activity Weights ω_k mentions each type of activity like authentication, block creation, penalty for malicious behavior has an associated weight that reflects its importance in determining the overall reputation score. These weights are learned by the machine learning model during the training process. The Sub-Scores $R_{ik}(t)$ are individual scores reflecting the node's performance in different activities. For instance, $R_{i1}(t)$ might represent the score for successful block validations, while $R_{i2}(t)$ could represent the penalty score for any malicious activities. The Machine Learning Function f takes the weighted sum of sub-scores and produces the overall reputation score. This function can be a neural network, which can capture complex, non-linear relationships between the input features and the output reputation score.

6. COMPLEXITY OF THE PROPOSED SYSTEM

In the Modified Proof of Reputation (mPoR), the complexity for Dynamic Reputation Scoring (DRS) is $O(1)$ per node for time and $O(N)$ for space due to the constant operations required and storage of reputation scores for N nodes. The Block Proposal step has a time complexity of $O(N)$ for computing probabilities and $O(N)$ space for storing scores, while Block Validation involves $O(NlogK)$ time for selecting the top K nodes and $O(K)$ space. For Reputation Dynamics Optimization (ReDO), the time complexity for training the machine learning model is $O(N \cdot L)$ per epoch, where L represents the number of layers, and space complexity is $O(P)$, where P is the number of model parameters. Table 1 is referred to derive the overall space complexity and time complexity per epoch. The Gradient Descent optimization has $O(P)$ time complexity per iteration and $O(P)$ space complexity for storing gradients and parameters. Prediction and Update steps each have a time complexity of $O(N \cdot C)$ for predictions and $O(N)$ for updates, with corresponding space complexities of $O(N)$ for storing predicted scores and reputation scores.

Table 1. Time and Space Complexities at each stage of proposed system

Stage	Description	Time Complexity	Space Complexity
Dynamic Reputation Scoring (DRS)	Computes updated reputation scores for each node.	$O(1)$ per node	$O(N)$
Block Proposal	Calculates probability of a node proposing a block.	$O(N)$	$O(N)$
Block Validation	Selects top K nodes for validation.	$O(Nlog\ K)$	$O(K)$
Machine Learning Model (Training)	Trains model to predict optimal reputation scores.	$O(N \cdot L)$ per epoch	$O(P)$
Gradient Descent	Updates model parameters using gradient descent.	$O(P)$ per iteration	$O(P)$
Prediction	Predicts reputation scores using the trained model.	$O(N \cdot C)$	$O(N)$
Update	Updates node reputation scores based on predictions.	$O(N)$	$O(N)$

The overall time complexity and space complexity is given in equations 8 and 9. Where N represents number of nodes and L the number of layered implemented via neural networks. C and K represent computational complexity in the Machine learning and size of the validation committee respectively. The machine learning model takes parameters and the number of parameters is represented by P in the equation 8 and 9.

$$T_{Complexity} = O(N \cdot L) + O(N \cdot C) + O(NlogK) + O(P) \quad (8)$$

$$S_{Complexity} = O(N) + O(P) \quad (9)$$

7. IMPLEMENTATION RESULTS AND DISCUSSION

The unique functionality of this model is to update reputation scores dynamically without static or retrospective calculations. The implementation of MPoR is achieved by using python library as tensor flow. The dynamicity of this model is leveraged by considering parameters such as contribution of the node, activity of the node across the network and also the penalties. The equation 1 shows the formula used to calculate the reputation scores. The formula includes historical data and penalties to decide and update the current reputation score. The decay factor and weights are used for different activities with well-defined purposes for each. The consensus mechanism is executed only after the precise calculation of activity-based scores and reputation updates. The various functions ensure that the nodes are fairly evaluated and are consistent across the network. Initially the reputation scored are assigned by the machine and eventually evaluated and updated by the following the behavior of the node in the network. The normalization ensures comparability and ensures we maintain balance throughout the network. In order to optimize the working of this process we further

introduce Reputation Dynamics Optimization (ReDO), which deployed machine learning based techniques. The optimal reputation score is determined by the algorithm as a result of deploying neural network-based training. The machine learning model takes the historical performance data, and activity metrics to decide on the optimal reputation scores accurately. The accuracy is achieved by minimizing the loss unction through gradient decent. When the model is trained with enough data it is then ready to support real-time predictions and adjustment of values. The conjunction of mPoR with ReDO enables the system to deliver improved network performance. These kinds of frameworks are suitable for deployment in large scale blockchain networks where the performance is a paramount importance.

The equation 10 and equation 11 shows the quantification of efficiency by taking T as Throughput, L as Latency, S and Network Size and N Number of participating nodes. T calculates the transactions processed per second also known as TPS. Latency is the average time needed to confirm a transaction. Equation 12 and Equation 13 represent the two vital aspects, S and N that represent network size and the total number of nodes that participate. These are significant as they are the fundamental factors revolving around the scalability. The scalability is defined as the ability of a system/network to handle the growing number of transaction and increasing number of users respectively. Sybil attack is handled by introducing the P Sybil which is used to calculate the mechanism's ability to resist an attack of this kind. Furthermore, the ability of this network to remain resilient against adversarial attempts are measured using the equation 14. When node or nodes in a network seek to negatively impact or indulge in malicious attempts the model evaluates the ratio of malicious nodes M to the total of nodes in network N. All of these metrics are used to collaborate and depict the performance, capacity and robustness if blockchain systems.

$$T = \frac{Number\ of\ transactions}{Total\ time} \quad (10)$$

$$L = Time\ for\ transaction\ confirmation \quad (11)$$

$$N = Total\ number\ of\ nodes \quad (12)$$

$$S = \frac{Total\ transactions\ handled}{Peak\ network\ load} \quad (13)$$

$$P_{Sybil} = \frac{M}{N} \quad (14)$$

Table 2. Performance comparison of the proposed system with other methods

Performance Parameters	Efficiency		Scalability		Sybil Attack Resistance P_{Sybil}
	Throughput (T)	Latency (L)	Network Size (N)	Transaction Scalability (S)	
DPoS	1000	1	10000	1000	0.8
DM-PoW	100	10	5000	100	0.95
RPoC	1500	1	10000	1500	0.9
PoR	500	5	7000	500	0.9
mPoR	2000	1	15000	2000	0.95

mPoR + ReDO	2500	0.5	20000	2500	0.98

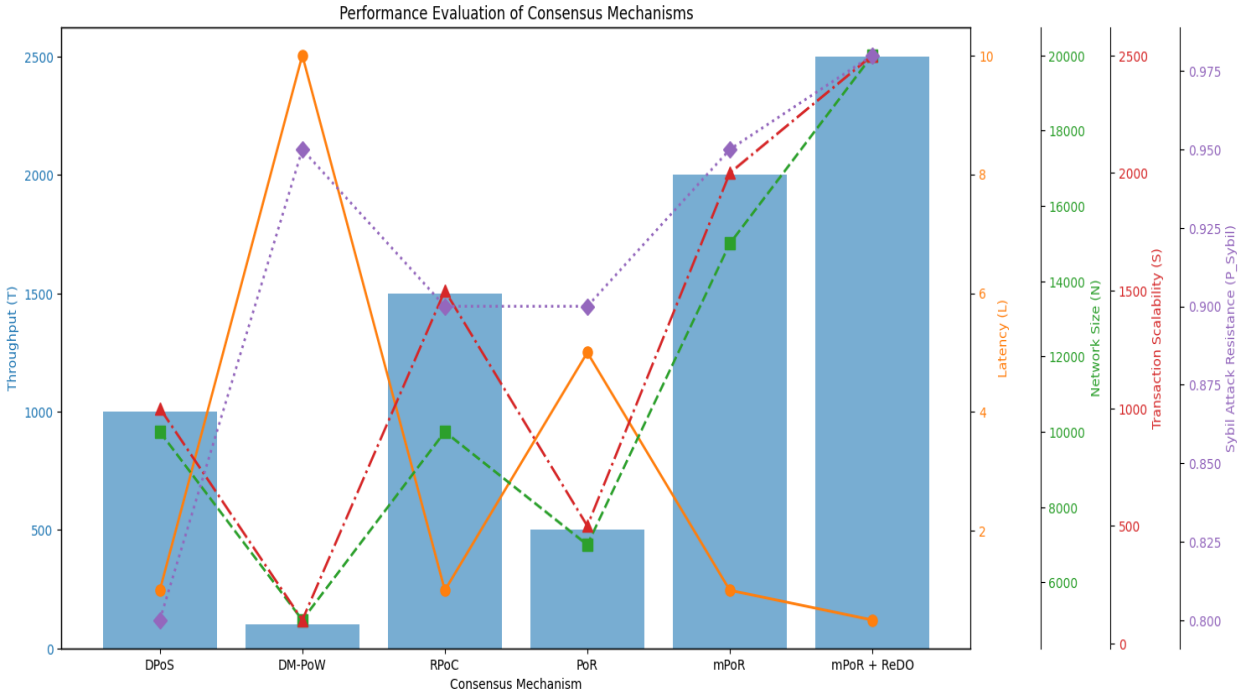


Figure 3. Performance comparison of the proposed system with other methods

The integration of Modified Proof of Reputation (mPoR) with Reputation Dynamics Optimization (ReDO) introduces a notable leap forward in blockchain performance. As highlighted in Table 2 and Figure 3, the proposed system significantly improves key parameters such as efficiency, scalability, and security. In terms of efficiency—which we measure by throughput and latency—the results are striking. The mPoR + ReDO model achieves a throughput of 2,500 transactions per second with an average latency of just 0.5 seconds. To put this in perspective, Delegated Proof of Stake (DPoS) typically manages 1,000 transactions per second with a 1-second latency, while Diversity Mining-based Proof of Work (DM-PoW) lags behind at just 100 transactions per second and a latency of 10 seconds. These improvements highlight the capability of the proposed mechanism to handle high transaction volumes with minimal delay. Scalability has also been significantly enhanced. The system can support up to 20,000 active nodes—double the capacity of traditional Proof of Reputation (PoR), which handles around 7,000 nodes, and considerably more than DPoS's 10,000-node ceiling.

Additionally, the system maintains consistent performance even during network congestion, successfully processing up to 2,500 transactions during peak loads. This surpasses not only PoR but also more resource-intensive models like DM-PoW, underscoring the system's robustness and adaptability in real-world conditions. Security, particularly against Sybil attacks, is another area where the combined mPoR and ReDO framework stands out. The likelihood of a successful Sybil attack (denoted as *P* Sybil) is substantially reduced, dropping to as low as 0.98 under the new system.

This represents a notable improvement over existing models—Reputation-based Proof of Contribution (RPoC) and PoR, both of which hover around 0.90, and DM-PoW, which achieves a value of approximately 0.95. This enhanced security can be attributed to the dynamic, machine learning-driven reputation management system, which continuously evaluates node behavior and adjusts scores accordingly. By limiting the impact of potentially malicious actors, the system strengthens trust and integrity across the network. Although the combined use of mPoR and ReDO offers a balanced, high-performing solution for modern blockchain systems. It not only enhances efficiency and scalability but also fortifies the network's defense mechanisms, making it a strong blockchain systems.

8. CONCLUSION

The Consensus algorithm is the fundamental pillar for the validation of transactions in a blockchain network. Blockchain has been revolutionizing various industries by pivoting businesses in vivid functional dimensions while it continues to enhance the transparency, security and efficiency of processes. Enhanced consensus, Sharding, interoperability, hybrid models and optimized algorithms can be deployed as resolutions for issues identified in the traditional protocols. Conventionally, consensus protocols suffer from stern challenges related to scalability, energy consumption and throughput of transactions. In this paper, we amalgamate Modified Proof of Reputation with Reputation Dynamics Optimization to accelerate blockchain performance. The combination of two potent mechanisms substantially improved the throughput, decreased the latency, fortified transaction scalability and strengthened security against Sybil attacks. The combination not only boosts the overall performance but also instills confidence for industries to adopt it in the blockchain landscape. Block-chain holds a future filled with sheer promises to transform everyday life by continuing the exploration and expansion of its potential.

REFERENCES

1. A. Raj V, S. S, P. D, R. A and R. K. G, "Intelligent Door Assist system using Chatbot and Facial Recognition," 2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), Chennai, India, 2022, pp. 1-6, doi: 10.1109/ICSES55317.2022.9914298.
2. A. Raj V, S. S, S. U, B. B and T. Pooja S, "Intelligent Organ Transplantation System Using Rank Search Algorithm to Serve Needy Recipients," 2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), Chennai, India, 2022, pp. 1-8, doi: 10.1109/ICSES55317.2022.9914040.
3. Abdullah Ayub Khan, Asif Ali Laghari, Peng Li, Mazhar Ali Dootio & Shahid Karim . The collaborative role of blockchain, artificial intelligence, and industrial internet of things in digitalization of small and medium-size enterprises. Sci Rep 13, 1656 (2023). https://doi.org/10.1038/s41598-023-28707-9
4. Adithya Pothan Raj V, Mohan Kumar P (2019): Defective tissue identification from crowded tissue cluster of 3D images, Journal of Ambient Intelligence and Humanized Computing, doi: 10.1007/s12652-019-01590-x

5. AlBadi, A., Hajamohideen, F., & AlSaqri, D. (2023). A Review on Blockchain Techniques Used for Identity Management System: Privacy and Access Control. In International Conference On Systems Engineering (pp. 361-375). Cham: Springer Nature Switzerland.
6. Ali, S. I. M., Farouk, H., & Sharaf, H. (2022). A Blockchain-based models for student information systems. Egyptian Informatics Journal, 23(2), 187-196.
7. Balani, N. and Chavan, P., 2023. Design of heuristic model to improve blockchainbased sidechain configuration. International journal of computational science and engineering, 26(4), pp.372-384.
8. Ehtisham Ul Haque, Adil Shah, Jawaid Iqbal, Syed Sajid Ullah, Roobaea Alroobaea & Saddam Hussain A scalable blockchain based framework for efficient IoT data management using lightweight consensus. Sci Rep 14, 7841 (2024). https://doi.org/10.1038/s41598-024-58578-7
9. Ghosh, Pranto Kumar, ArindomChakraborty, MehediHasan, Khalid Rashid, and Abdul Hasib Siddique. "Blockchain application in healthcare systems: a review." Systems 11, no. 1 (2023): 38.
10. Jayabal CP, Sathia Bhama PR (2021) Performance analysis on diversity mining-based proof of work in bifolded consortium blockchain for Internet of Things consensus. Concurr Computat Pract Exp 33(16):e6285. https://doi.org/10.1002/cpe.6285
11. Jayana Kaneriya, Hiren Patel (2023) "A Secure and Privacy Preserving Student Credential Verification System using Blockchain" in International Journal of Information and Education Technology, ISSN: 2010-3689
12. Johannes Sedlmeir, Hans Ulrich Buhl, Gilbert Fridgen & Robert Keller. The Energy Consumption of Blockchain Technology: Beyond Myth. Bus Inf Syst Eng 62, 599–608 (2020). https://doi.org/10.1007/s12599-020-00656-x
13. Kaneriya, J., & Patel, H. (2023). A secure and privacy-preserving student credential verification system using Blockchain technology. International Journal of Information and Education Technology (IJIET), 13(8), 1251–1260.
14. Kaneriya, J., & Patel, H., "A Blockchain-based Conceptual Framework for Privacy Preserving Self- Sovereign Identity with Selective Disclosure," International Journal of Information Technology and Electrical Engineering ITEE, vol. 10, no. 3, pp. 28–35, 2022.
15. Maftei AA, Lavric A, Petrariu AI, Popa V. Massive Data Storage Solution for IoT Devices Using Blockchain Technologies. Sensors. 2023; 23(3):1570. https://doi.org/10.3390/s23031570
16. Mostafa, A. M., Rushdy, E., Medhat, R., & Hanafy, A. (2023). An identity management scheme for cloud computing: Review, challenges, and future directions. Journal of Intelligent & Fuzzy Systems, 1-23.
17. Oladotun Aluko and Anton Kolonin, Proof-of-Reputation: An Alternative Consensus Mechanism for Blockchain Systems, International Journal of Network Security & Its Applications (IJNSA) Vol.13, No.4, July 2021

18. Panja, S., & Roy, B. (2021). A secure end-to-end verifiable e-voting system using Blockchain and cloud server. Journal of Information Security and Applications, 59, 102815.
19. R. A. Mishra, A. Kalla, A. Braeken, and M. Liyanage, Privacy protected Blockchain based architecture and implementation for sharing of students' credentials, Inf. Process. Manag., vol. 58, no. 3, 102512, 2021.
20. Ricardo Perez-Marco, Cyril Grunspan. Proof of Reputation. 2023. ffhal-03988026f
21. Rozman N, Corn M, Skulj G, Berlec T, Diaci J, Podrzaj P. Exploring the Effects of Blockchain Scalability Limitations on Performance and User Behavior in Blockchain-Based Shared Manufacturing Systems: An Experimental Approach. Applied Sciences. 2023; 13(7):4251. https://doi.org/10.3390/app13074251
22. Saqib, N.A. and AL-Talla, S.T., 2023. Scaling Up Security and Efficiency in Financial Transactions and Blockchain Systems. Journal of Sensor and Actuator Networks, 12(2), p.31.
23. Sarfaraz, A., Chakrabortty, R.K. & Essam, D.L. Reputation based proof of cooperation: an efficient and scalable consensus algorithm for supply chain applications. J Ambient Intell Human Comput 14, 7795–7811 (2023). https://doi.org/10.1007/s12652-023-04592-y
24. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, http://dx.doi.org/10.2139/ssrn.3440802
25. Shen, Tao, Tianyu Li, Zhuo Yu, FenhuaBai, and Chi Zhang. "GT-NRSM: efficient and scalable sharding consensus mechanism for consortium blockchain." The Journal of Supercomputing (2023): 1-35
26. Singh, C., Thakkar, R., & Warraich, J. (2023). IAM identity Access Management importance in maintaining security systems within organizations. European Journal of Engineering and Technology Research, 8(4), 30-38.
27. Sohail Jabbar, Zain Ul Abideen, Shehzad Khalid, Awais Ahmad, Umar Raza, Sheeraz Akram, Enhancing computational scalability in Blockchain by leveraging improvement in consensus algorithm, Front. Comput. Sci., Sec. Networks and Communications, Volume 5 - 2023, https://doi.org/10.3389/fcomp.2023.1304590
28. Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications, 50, 102407.
29. Xing Fan, Baoning Niu, Zhenliang Liu, Scalable blockchain storage systems: research progress and models, Computing (2022), 104:1497–1524, https://doi.org/10.1007/s00607-022-01063-8
30. Zhang, P., Guo, W., Liu, Z., Zhou, M., Huang, B. and Sedraoui, K., 2023. Optimized Blockchain Sharding Model Based on Node Trust and Allocation. IEEE Transactions on Network and Service Management.