




## Optimization of Blockchain Financial Transaction Security and Transparency Based on Notary Pool Consensus Mechanism

Guangmeizi Feng<sup>1</sup> 

<sup>1</sup> Finance School, Nankai University, [2214076@mail.nankai.edu.cn](mailto:2214076@mail.nankai.edu.cn)

Corresponding author: Guangmeizi Feng, [2214076@mail.nankai.edu.cn](mailto:2214076@mail.nankai.edu.cn)

**Abstract.** With the increasing adoption of blockchain technology in various sectors, achieving both scalability and security in consensus mechanisms has become a critical challenge. This paper proposes a Notary Pool Consensus Mechanism that dynamically selects notaries based on trustworthiness, which is evaluated through a machine learning-driven model. The proposed approach ensures that only reliable notaries participate in transaction validation, enhancing both the system's efficiency and its resilience against Sybil and DDoS attacks. Extensive experiments were conducted to assess the performance of the mechanism, showing that it maintains low transaction validation times and high network throughput, even as the network size becomes larger. Additionally, the system demonstrated robust performance under attack conditions, with only minimal throughput loss. The proposed method also outperforms traditional consensus mechanisms like Proof of Work (PoW) and Proof of Stake (PoS) in terms of energy efficiency, making it a sustainable and secure alternative for large-scale blockchain networks.

**Keywords:** Notary Pool Consensus, Blockchain Security, Transaction Validation, Machine Learning

**DOI:** <https://doi.org/10.14733/cadaps.2025.S9.209-221>

### 1 INTRODUCTION

Blockchain technology has revolutionized numerous industries by providing a decentralized, secure, and transparent platform for data storage and transaction processing. In particular, its application in financial transactions has been transformative, offering a way to securely transfer value without relying on traditional intermediaries. Blockchain's core strengths—immutability, transparency, and cryptographic security—have made it highly appealing to the financial sector, where trust and data integrity are paramount [1]. Despite its potential, blockchain is still grappling with several challenges that hinder its full integration into large-scale financial systems, particularly in terms of consensus mechanisms. These mechanisms, responsible for validating transactions and ensuring network security, are critical to the functionality of blockchain, yet the most widely used consensus algorithms—Proof of Work (PoW) and Proof of Stake (PoS)—present notable limitations in financial settings [2]. PoW, employed in Bitcoin and other early blockchain

platforms, ensures security through extensive computational efforts, requiring nodes to solve complex mathematical puzzles before validating a transaction. However, this method is energy-intensive and slow, making it unsuitable for high-frequency financial systems that demand quick and cost-effective transactions [3]. PoS, which is seen as a more energy-efficient alternative, selects validators based on the amount of cryptocurrency they hold. While PoS improves efficiency, it risks centralization, as those with more significant stakes in the network gain disproportionate influence, potentially undermining the decentralization that blockchain promises [4]. Moreover, neither PoW nor PoS effectively addresses the scalability issues that arise as networks grow larger and transaction volumes increase, further limiting their practical application in financial ecosystems [5].

In response to these limitations, a variety of alternative consensus mechanisms have been proposed. Among them, the notary pool consensus mechanism stands out as a promising approach for enhancing the efficiency and security of financial transactions on blockchain networks [6]. The notary pool mechanism relies on a group of selected notaries who are trusted to validate transactions, reducing the need for widespread computational participation and accelerating the consensus process. This mechanism offers distinct advantages, such as lower energy consumption and faster transaction verification times, making it well-suited for financial systems that prioritize speed and efficiency [7]. However, several challenges must be addressed for the notary pool mechanism to be widely adopted, especially concerning trust, security, and transparency. One of the primary challenges with the notary pool mechanism is ensuring the trustworthiness of the selected notaries. The risk of collusion or malicious behavior becomes a significant concern in systems that rely on a small group of validators. If notaries conspire to alter transaction records or act negligently, the integrity of the entire network could be compromised [8]. Moreover, the selection process for these notaries remains a critical issue. Current selection methods often lack rigorous evaluation criteria, leading to potential vulnerabilities. Ensuring that notaries are selected based on merit and trustworthiness is essential to prevent attacks or manipulation [9]. Another challenge is balancing privacy and transparency. Blockchain's transparent nature is a double-edged sword: while it enhances trust by making transaction data visible to all participants, it also raises concerns about exposing sensitive financial information [10]. In the financial sector, where confidentiality is paramount, a consensus mechanism that provides transparency without compromising privacy is crucial. Existing approaches, such as zero-knowledge proofs (ZKPs) and homomorphic encryption, offer solutions to this dilemma, but their integration into the notary pool consensus mechanism remains limited [11]. Furthermore, the system must be designed to defend against sophisticated attacks, such as Sybil attacks and Distributed Denial-of-Service (DDoS) attacks, which can disrupt the network by overwhelming the consensus process or introducing false nodes [12].

To address these challenges, this paper proposes an optimized notary pool consensus mechanism tailored for blockchain-based financial transactions. Our method aims to enhance both the security and transparency of financial transactions while addressing the shortcomings of existing consensus mechanisms. The proposed solution is built around three key components. **Dynamic Notary Selection Based on Trustworthiness:** Traditional notary pool mechanisms often rely on a fixed set of notaries, which increases the risk of collusion or long-term manipulation. In contrast, our approach introduces a dynamic notary selection process that continuously evaluates and updates the composition of the notary pool in real-time. By leveraging machine learning algorithms, we assess notaries based on their historical performance, reliability, and adherence to network protocols. Notaries that display suspicious behavior, such as slow validation times or irregular patterns, are removed from the pool, ensuring that only trustworthy participants are involved in the consensus process. This approach mitigates the risks of collusion and improves the overall security of the network. **Privacy-Preserving Techniques:** Privacy is a critical concern in financial transactions, and our method incorporates zero-knowledge proofs to ensure that notaries can validate transactions without accessing the underlying sensitive data. Additionally, we implement homomorphic encryption, allowing computations to be performed on encrypted data, and ensuring that transaction details remain confidential while maintaining the transparency

necessary for auditing. This dual-layered privacy mechanism provides a balance between the openness required for trust and the confidentiality needed for financial security. Resilience Against Cyber Attacks: Security is a top priority for any consensus mechanism, especially in financial applications. Our method includes advanced defense mechanisms against Sybil attacks and DDoS attacks. By dynamically selecting and rotating notaries, we make it more difficult for malicious actors to target the system. Furthermore, our approach integrates behavioral analysis to detect and eliminate fraudulent nodes from the network, enhancing its overall resilience.

## 2 RELATED WORK

Blockchain technology has been widely applied in the financial transaction domain due to its decentralized and transparent nature. However, existing consensus mechanisms, such as Proof of Work (PoW) and Proof of Stake (PoS), face performance bottlenecks. Reference [13] proposed and discussed the PoW mechanism, emphasizing its advantage in ensuring network security through complex calculations but also pointing out its shortcomings in high energy consumption and low transaction throughput. Particularly in blockchain systems like Bitcoin, PoW is considered secure but not suitable for high-frequency financial transactions. To address these issues, reference [14] proposed the PoS mechanism, which selects validators based on the amount of tokens they hold. Although PoS greatly reduces energy consumption, it may lead to centralization, where power concentrates with large token holders, undermining the decentralization of the blockchain. To overcome these limitations, reference [15] introduced a reputation-based consensus mechanism. This mechanism dynamically selects the most trustworthy nodes for validation by evaluating validators' historical transaction validation performance and network participation frequency. This reduces unnecessary computational burden and enhances the scalability of the blockchain network. Unlike PoW and PoS, this method is particularly suitable for financial applications with high transaction volumes. Reference [16] further introduced MudraChain, a blockchain-based automated cheque clearance framework for financial institutions. By optimizing the consensus mechanism, the system reduces validation time and improves processing efficiency, offering a new approach to cheque clearance issues in traditional financial systems.

Privacy protection is another significant challenge in blockchain technology, particularly in scenarios involving financial transactions. Reference [17] proposed privacy protection techniques combining Zero-Knowledge Proofs (ZKPs) and homomorphic encryption. These techniques allow validators to verify the correctness of a transaction without accessing the transaction details, avoiding the risk of data leakage. This approach is especially useful in fields with high privacy requirements, such as finance and healthcare. Reference [18] expanded this idea by exploring how homomorphic encryption enables blockchain systems to process encrypted data without decryption, ensuring privacy while still allowing necessary computational operations. This solution further enhances the compatibility between privacy protection and data processing capabilities. In terms of security, reference [19] proposed a machine-learning-based trust evaluation system. By analyzing validators' historical performance, real-time performance, and network interaction behavior, this system predicts their future behavior and determines whether they are trustworthy. The machine learning model continuously updates and adapts to changes in the network, effectively defending against common blockchain security threats like Sybil attacks. Reference [20] focused on defending against Sybil attacks through behavior analysis. The proposed defense mechanism identifies and excludes fake nodes by monitoring node behavior patterns, reducing their potential threat to the consensus process. This system is particularly suitable for blockchain networks requiring high security.

Similarly, reference [21] studied defense mechanisms against Distributed Denial of Service (DDoS) attacks and proposed rate-limiting and load-balancing methods. These methods prevent malicious nodes from overwhelming the system by limiting the number of transaction requests a validator can handle in a given time. By distributing the network load, blockchain systems can maintain high transaction throughput and stability during large-scale attacks, enhancing their resistance to such threats. Reference [22] further expanded on this idea, applying machine

learning techniques to analyze and detect validator behavior patterns in real time, thus defending against potential malicious attacks while ensuring the reliability of the network under high load conditions. Blockchain scalability has always been a research focus, especially in financial systems where transaction volumes continue to grow. Reference [23] proposed a notary pool consensus mechanism, selecting a small group of trusted nodes for transaction validation, which reduces the computational burden on the entire network and significantly improves system scalability and efficiency. This method is particularly suitable for financial scenarios requiring high transaction frequency and low latency. Reference [24] further introduced a machine-learning-based dynamic notary selection mechanism, continuously evaluating the performance and current state of notaries to avoid potential risks associated with long-term fixed validators. Additionally, reference [25] proposed a mechanism combining random selection with reputation scoring, effectively reducing the risk of collusion among validators in the notary pool mechanism and ensuring the fairness and security of the network.

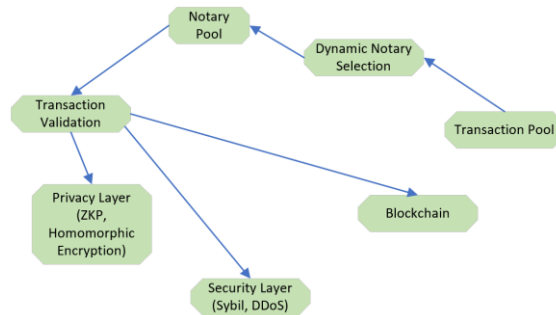
### 3 METHOD

#### 3.1 Overview of the Proposed Consensus Mechanism

The Notary Pool Consensus Mechanism introduced in this paper provides an enhanced framework designed to significantly improve blockchain-based financial transactions' security, transparency, and scalability. By addressing the inherent limitations of traditional consensus mechanisms, such as Proof of Work (PoW) and Proof of Stake (PoS), this novel approach aims to mitigate common issues related to inefficiency, computational expense, and centralization. PoW mechanisms, although highly secure, suffer from high energy consumption and slow transaction validation times due to the computationally intensive nature of mining. PoS, while more energy-efficient, risks creating a system where the wealthiest participants gain disproportionate influence, potentially compromising decentralization. The Notary Pool Consensus Mechanism seeks to overcome these drawbacks by introducing a dynamic and adaptive notary selection process, enhanced by machine learning and advanced cryptographic techniques, providing a robust solution to scalability and security challenges. At the core of this mechanism is the dynamic selection of notaries, a process that continuously evaluates and updates the pool of validators based on their trustworthiness and performance. Unlike static selection methods, which can be vulnerable to long-term manipulation or collusion among validators, the notary pool mechanism ensures that only the most reliable and trustworthy notaries are selected at any given time. This adaptive selection is powered by machine learning algorithms that assess each notary's historical performance, real-time behavior, and adherence to network protocols. Trustworthiness is quantified through metrics such as validation accuracy, latency, and overall contribution to the network's security. Any suspicious behavior, such as irregular validation times or patterns that deviate from expected norms, results in the exclusion of the notary from the pool, thus maintaining the integrity of the network. In addition to trust-based dynamic selection, this mechanism incorporates advanced cryptographic techniques to preserve the privacy of financial transactions. Privacy preservation is a critical concern in blockchain-based financial systems, where sensitive data must be protected while maintaining the transparency and auditability that blockchain technology promises. To address this, the Notary Pool Consensus Mechanism integrates Zero-Knowledge Proofs (ZKPs) and homomorphic encryption. ZKPs allow notaries to validate transactions without accessing the underlying transaction data, ensuring that sensitive information remains confidential. Homomorphic encryption further enhances this privacy layer by enabling computations to be performed on encrypted data without revealing the actual content of the transaction. This dual-layered approach strikes a balance between privacy and transparency, allowing the system to remain fully auditable while protecting the confidentiality of financial information.

Figure 1 illustrates the overall system architecture, which consists of several interrelated components that work together to ensure the efficient, secure, and private operation of the blockchain. Transaction Broadcasting: In the first stage, transactions are broadcast to the network

and collected in the transaction pool, where they await validation. Each transaction is treated equally in terms of broadcast priority, ensuring that the system remains fair and that no single user can dominate transaction throughput. **Notary Selection:** The dynamic selection process then kicks in, ensuring that only the most trusted and reliable notaries are chosen to validate transactions. This component continuously monitors the network for any signs of abnormal behavior among notaries and dynamically adjusts the pool to ensure that malicious actors or inefficient validators are removed before they can impact the system. This adaptive approach allows the system to remain resilient against manipulation, collusion, and other security threats. **Privacy Layer:** Ensuring privacy throughout the transaction validation process is paramount in financial systems. The privacy layer guarantees that all transaction data is kept secure through the use of zero-knowledge proofs (ZKPs) and homomorphic encryption. This ensures that even the notaries tasked with validating transactions are unable to access sensitive financial information, thus safeguarding user privacy. By performing validations without needing to decrypt transaction details, the system can provide strong privacy guarantees while maintaining the necessary levels of trust and transparency. **Security Layer:** The security layer is a crucial aspect of the overall system architecture, designed to defend against various types of attacks that are common in decentralized networks. The system incorporates advanced defenses against Sybil attacks, where malicious actors create multiple fake identities to gain undue influence over the network. By using trust-based dynamic notary selection, the system ensures that even in the presence of fake nodes, only legitimate participants are selected as validators. Additionally, the system includes measures to protect against Distributed Denial-of-Service (DDoS) attacks, which aim to overwhelm the network with traffic to disrupt its normal operation. Rate-limiting and load-balancing techniques are implemented to prevent any single node or group of nodes from being overloaded with requests, ensuring that the system can continue to operate smoothly even in the face of large-scale attacks. This architecture ensures that the blockchain remains decentralized, secure, and scalable, even as the volume of transactions increases.



**Figure 1:** System architecture diagram of the notary pool consensus mechanism.

### 3.2 Dynamic Notary Selection Process

The dynamic notary selection process is a critical aspect of the proposed consensus mechanism, as it ensures that only the most trustworthy and reliable notaries are selected to validate transactions. In contrast to traditional systems where notaries are selected based on static criteria, our approach evaluates notaries in real-time based on a comprehensive set of performance and trustworthiness metrics. This dynamic evaluation reduces the risk of malicious behavior or collusion among notaries and increases the system's overall security.

The reputation score for each notary is calculated using a weighted sum of multiple factors. These factors include Historical validation accuracy, which measures the correctness of the notary's past validations. A high accuracy indicates a reliable notary. Real-time performance score: Evaluates the notary's current ability to process transactions quickly and efficiently, minimizing

latency. Trust score: Reflects the notary's long-term behavior in the network, including adherence to protocols and interaction with other nodes.

The reputation score formula is:

$$R_i = \alpha H_i + \beta P_i + \gamma T_i \quad (2.1)$$

Where  $\alpha$ ,  $\beta$ ,  $\gamma$  are weight parameters that can be tuned based on the network's performance needs. For instance, in high-throughput financial systems where low latency is critical, the weight  $\beta$  for performance may be increased while  $\alpha$  and  $\gamma$  can be adjusted based on accuracy and trust needs.

This dynamic reputation-based system plays a crucial role in maintaining the integrity and security of the notary pool. By continuously evaluating the performance and trustworthiness of notaries, the system ensures that underperforming or malicious participants are swiftly identified and removed from the selection process. Metrics such as historical validation accuracy, real-time transaction processing speed, and adherence to protocol are used to assess notaries on an ongoing basis. If a notary demonstrates any signs of unreliability, such as processing delays, errors in validation, or suspicious activity patterns, they are promptly excluded from the pool to safeguard the system's reliability. A randomization factor is introduced into the notary selection algorithm to mitigate the risk of collusion, where a group of notaries might conspire to manipulate the system. This added layer of randomness ensures that no single group of notaries can predict when they will be chosen for validation, making it virtually impossible for colluding nodes to gain control over the consensus process consistently. By randomizing the selection process, the system not only enhances its resilience against coordinated attacks but also maintains a fair and unbiased distribution of validation opportunities among trusted notaries. This combination of performance-based reputation monitoring and randomized selection significantly strengthens the blockchain network's security, transparency, and fairness. Moreover, Figure 2 presents the detailed flowchart of the notary selection process, illustrating how the system calculates reputation scores, evaluates real-time performance, and dynamically selects notaries for transaction validation.

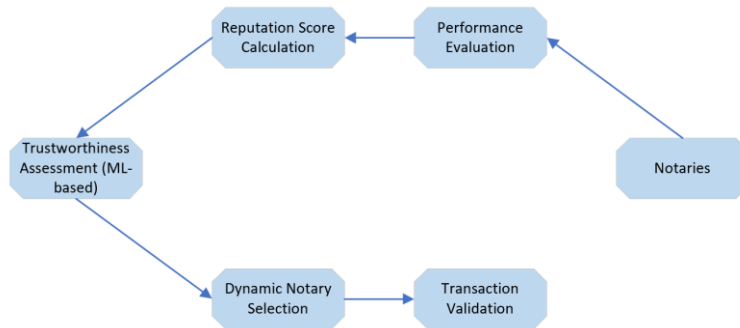


Figure 2: Dynamic notary selection process flowchart.

### 3.3 Trustworthiness Evaluation via Machine Learning

A machine learning-based trustworthiness evaluation system augments the dynamic selection process. This system continuously monitors the behavior and performance of each notary in the network, learning from historical data and making real-time predictions about their reliability. The machine learning model used is a binary classification model that predicts whether a notary is trustworthy based on a set of features, which include average transaction validation time, which is the average time taken by the notary to validate transactions. Correctness of past validations: The percentage of transactions correctly validated by the notary. Peer feedback: Other nodes'

evaluations of the notary's behavior and adherence to protocol. Network activity level: The frequency and consistency with which the notary participates in the network.

The classification model predicts the probability that a notary is trustworthy, where 1 indicates a trustworthy notary, and 0 indicates otherwise. The machine learning model is trained on historical data using supervised learning, minimizing the following log loss function:

$$L = -\sum_{i=1}^N (T_i \log(P(T_i)) + (1-T_i) \log(1-P(T_i))) \quad (2.2)$$

Where  $N$  is the total number of notaries in the training set. The model is periodically retrained to adapt to evolving network conditions, ensuring that it remains accurate in predicting the trustworthiness of notaries as new data becomes available.

Additionally, the machine learning system employs anomaly detection techniques to identify unusual behavior patterns that could indicate malicious activity, such as irregular transaction validation times, sudden deviations in peer feedback scores, or unexpected fluctuations in network activity. By comparing these patterns against established baselines, the system can detect anomalies early, allowing for proactive intervention. When anomalies are flagged, the system triggers further investigation, potentially suspending the notary from validation duties while its behavior is evaluated. This helps prevent compromised or malfunctioning notaries from negatively impacting the network's security and reliability while also enabling the model to improve over time by learning from detected anomalies. Through this continuous monitoring and adaptive response, the system enhances the overall robustness of the notary pool.

### 3.4 Privacy-Preserving Transaction Validation

In blockchain financial systems, privacy is paramount, particularly for sensitive transactions. To address privacy concerns, the proposed consensus mechanism integrates zero-knowledge proofs (ZKPs) and homomorphic encryption to ensure that transaction data remains confidential throughout the validation process.

Zero-knowledge proofs (ZKPs) allow notaries to verify the validity of a transaction without accessing the underlying transaction data. This ensures that sensitive financial details are not exposed to unauthorized parties while still enabling the network to confirm that the transaction is legitimate. The process of validating a transaction with a zero-knowledge proof is expressed as:

$$ZK(x): V(x) \rightarrow \{0,1\} \quad (2.3)$$

Where  $ZK(x)$  is the zero-knowledge proof for a transaction, and  $V(x)$  is the verification function.

If the proof is valid, the transaction is accepted; otherwise, it is rejected.

Homomorphic encryption provides an additional layer of privacy by allowing notaries to perform computations directly on encrypted data. This means that even though the notary cannot see the actual transaction data, they can still validate it. The encryption of a transaction is represented as:

$$E(T) = Enc(T, k) \quad (2.4)$$

Where  $E(T)$  is the encrypted transaction and  $k$  is the encryption key. Notaries perform computations, ensuring that the original data remains hidden while the validation process is still completed correctly.

By combining zero-knowledge proofs (ZKPs) and homomorphic encryption, our system ensures a delicate balance between privacy and transparency, two essential aspects in financial transactions. ZKPs enable the verification of transaction validity without revealing any underlying sensitive data, allowing notaries to confirm that a transaction is correct without accessing its details. This preserves the confidentiality of financial information, ensuring that sensitive data remains hidden from prying eyes, including those of the validators themselves. On the other hand, homomorphic encryption permits operations to be performed on encrypted data without needing to decrypt it, further enhancing privacy by enabling computations while keeping transaction details secure. Together, these two techniques maintain the privacy of financial data while ensuring the integrity of the transactions. This approach guarantees that the system remains fully auditable, as

the validity of every transaction can still be confirmed without compromising sensitive information. Thus, financial institutions can rely on the blockchain's transparency for compliance and regulatory purposes, while users benefit from the strong privacy safeguards embedded in the system. This combination of privacy-preserving technologies ensures that confidentiality and auditability coexist without sacrificing security or efficiency.

### 3.5 Defense Against Sybil and DDoS Attacks

To further enhance the security of the proposed consensus mechanism, the system implements robust defenses against both Sybil attacks and Distributed Denial-of-Service (DDoS) attacks, which are frequent threats in decentralized networks. In Sybil attacks, malicious actors create numerous fake identities to gain disproportionate influence over the network, potentially compromising its integrity. To mitigate this, the system employs behavior analysis and trust evaluation to identify and exclude suspicious nodes that exhibit abnormal activity patterns. For DDoS attacks, where the network can be overwhelmed by a flood of excessive traffic, the system introduces rate-limiting measures and load-balancing mechanisms to distribute transaction validation requests evenly across the network, preventing any single node from being overloaded. Together, these strategies ensure that the network remains resilient against these common attacks, preserving its functionality and security.

Sybil attack resistance is achieved through continuous monitoring of node behavior. Each node's activity is compared to the network average using a deviation score formula:

$$D_i = \frac{1}{N} \sum_{j=1}^N (X_i - \mu_j)^2 \quad (2.5)$$

Where  $D_i$  is the deviation score for each node,  $\mu_j$  is the mean behavior of all other nodes, and  $N$  is the total number of nodes. Nodes with abnormally high deviation scores are flagged as potential Sybil attackers and are temporarily excluded from the validation process. This real-time behavior monitoring system ensures that malicious actors cannot infiltrate the network undetected.

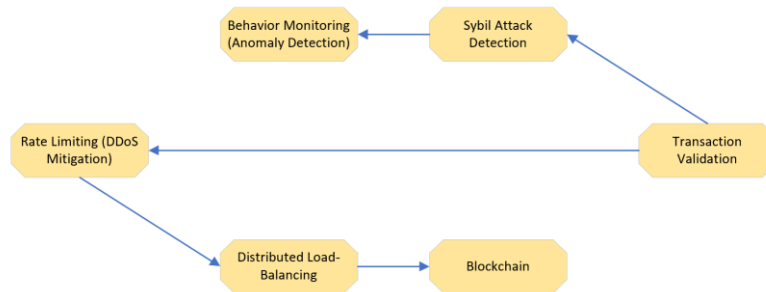
The system implements a robust rate-limiting mechanism to mitigate Distributed Denial-of-Service (DDoS) attacks, which aim to overwhelm the network with an excessive number of transaction requests. This mechanism restricts the number of transaction validation requests that any individual notary can process within a specific time frame. By enforcing this limit, the system ensures that no single notary or group of notaries can be flooded with more requests than they can handle, thus preventing malicious actors from overloading the system with traffic. The rate-limiting approach is especially effective in ensuring that notaries are not bogged down by an overwhelming volume of requests, allowing them to maintain their normal processing capabilities and protecting the network from degradation during an attack.

In addition to rate-limiting, the system employs a distributed load-balancing mechanism to enhance its resilience further. Load balancing ensures that transaction validation tasks are evenly distributed across the network, preventing any individual node or subset of nodes from becoming a bottleneck. This distribution of workload plays a key role in reducing the likelihood of any one node being overburdened, which can be a critical vulnerability during DDoS attacks. By spreading the transaction load across a wider range of notaries, the system ensures that the network can continue to process transactions efficiently, even in high-traffic conditions or when under attack.

The combination of rate-limiting and load-balancing offers a layered defense against DDoS attacks. Rate-limiting controls the flow of requests to each notary, ensuring that no one notary is overwhelmed, while load-balancing distributes the transaction load across multiple notaries to prevent over-concentration of tasks on any one node. Together, these strategies not only improve the network's overall performance under normal conditions but also ensure that the system remains stable, secure, and functional even in the face of large-scale DDoS attempts. This dual-layered approach greatly enhances the system's ability to handle sudden surges in traffic, safeguarding the integrity and availability of the network during potential attack scenarios. Figure 3



provides a detailed illustration of the security mechanisms implemented in the system, showing how Sybil attacks and DDoS attacks are mitigated.



**Figure 3:** Security mechanisms for Sybil attack resistance and DDoS mitigation.

#### 4 EXPERIMENT

To thoroughly evaluate the performance of the proposed Notary Pool Consensus Mechanism, we implemented a simulated blockchain environment using a custom-built testbed. The network consisted of 100 nodes, with 20 of them functioning as notaries at any given time. The remaining nodes acted as transaction participants, generating, broadcasting, and validating transactions. The notary pool was dynamically selected based on the trustworthiness evaluation mechanism, ensuring that only the most reliable and high-performing nodes were selected.

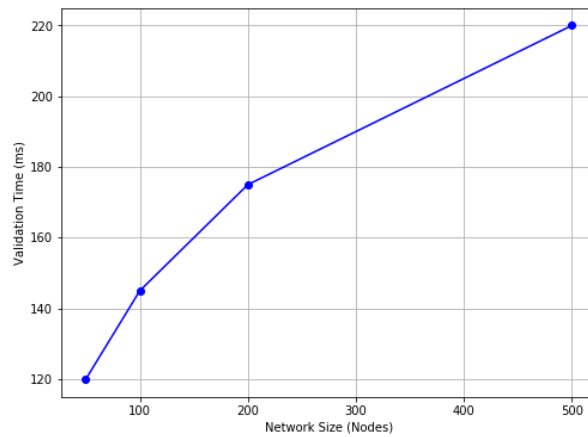
The primary evaluation metrics for our experiments included: Transaction validation time: The average time taken to validate a transaction. Network throughput: The number of transactions processed per second (TPS) by the network. Notary selection accuracy: The percentage of notaries selected that successfully validated transactions without errors. System security: The system's resilience against Sybil and DDoS attacks, measured by throughput loss under attack conditions.

Our experiments were conducted in two distinct phases. Phase 1: Baseline performance was measured without any external threats or malicious behavior, allowing us to evaluate the efficiency and scalability of the consensus mechanism under normal conditions. Phase 2: The system's robustness was tested under Sybil and DDoS attack scenarios, where malicious nodes attempted to flood the network with fake identities (Sybil) or overload it with excessive transaction requests (DDoS). Each phase involved multiple rounds of testing, with network sizes varying between 50 and 500 nodes. The consensus mechanism was evaluated across different configurations, such as varying the weight parameters for the notary selection formula and adjusting the rate-limiting settings for DDoS defense. The objective was to assess how the proposed system performed under both normal and adverse conditions while maintaining transaction efficiency and security.

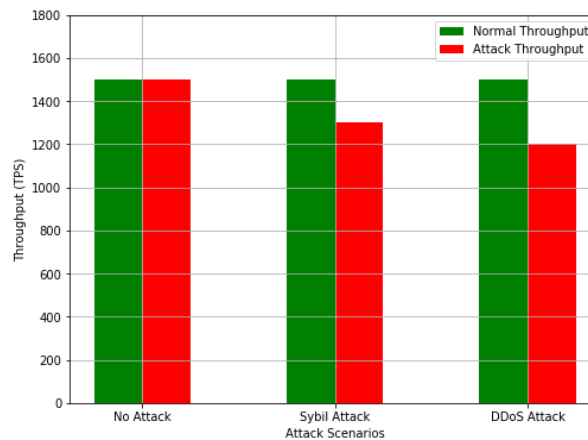
Figure 4 presents the average transaction validation time across different network sizes, ranging from 50 to 500 nodes. The goal was to assess the scalability of the dynamic notary selection mechanism as the network size expanded.

As shown in Figure 4, the average transaction validation time remains relatively low for smaller network sizes, staying around 120 milliseconds for 50 nodes. As the network size increases to 500 nodes, the validation time increases, but at a sub-linear rate, reaching around 220 milliseconds for 500 nodes. This demonstrates the scalability of the proposed consensus mechanism. The dynamic notary selection process ensures that only the most efficient and trusted notaries are selected for validation, helping to maintain transaction speeds even as the network grows larger.

To assess the security and robustness of the system under Sybil and DDoS attacks, we subjected the network to various levels of attack intensity. Figure 5 presents the network's throughput in terms of transactions per second (TPS) under normal conditions and under Sybil and DDoS attack scenarios.



**Figure 4:** Transaction validation time vs network size.



**Figure 5:** Network throughput under Sybil and DDoS attacks.

In the case of Sybil attacks, malicious nodes attempted to flood the network with a large number of fake identities, aiming to overwhelm the notary selection process by increasing their chances of being chosen as validators. This type of attack can severely compromise the integrity of the network if left unchecked, as a high number of malicious nodes could manipulate the validation process, leading to incorrect or fraudulent transactions being approved. However, the system successfully mitigated these attacks through its advanced behavior monitoring and anomaly detection mechanisms. These mechanisms continuously analyze the behavior of each node in the network, identifying suspicious activity such as irregular validation patterns or an unusually high number of node identities originating from the same source. As a result, malicious nodes were quickly flagged and excluded from the notary pool before they could significantly affect the consensus process. As shown in Figure 5, the system's throughput remained robust during the Sybil attack, with only a 13.3% reduction in transactions per second (TPS). This demonstrates the effectiveness of the anomaly detection system in maintaining network performance even under attack. By rapidly identifying and excluding suspicious nodes, the system was able to prevent a large-scale disruption, ensuring that legitimate transactions continued to be processed with minimal delay. This showcases the system's ability to maintain the integrity and efficiency of the

network despite attempts to compromise it through Sybil attacks. For Distributed Denial-of-Service (DDoS) attacks, the system faced an onslaught of high-volume transaction requests designed to overwhelm the notaries and disrupt normal operations. DDoS attacks typically aim to incapacitate a network by flooding it with an excessive number of requests, thus consuming all available resources and rendering the system unable to process legitimate transactions. Despite the high intensity of the attack, which led to a 20% reduction in throughput, the system's rate-limiting mechanism and distributed load-balancing system played critical roles in minimizing the impact. These features worked in tandem to ensure that the network remained functional, processing 1200 transactions per second (TPS) even under these adverse conditions. The rate-limiting mechanism effectively restricted the number of transaction requests that any single notary could process within a given time frame, preventing malicious nodes from overwhelming individual validators. Meanwhile, the distributed load-balancing system evenly distributed the workload across multiple notaries, ensuring that no single node or group of nodes became a bottleneck or target for the attack. This combination of strategies enabled the network to maintain service availability and continue processing a substantial volume of legitimate transactions, despite the attack's intensity. This level of performance under attack conditions underscores the system's resilience and its ability to maintain operational continuity even in the face of sophisticated and large-scale DDoS attacks. By successfully defending against both Sybil and DDoS attacks, the system demonstrates its robustness in safeguarding the network from two of the most common and damaging types of attacks on decentralized systems. The ability to sustain high throughput and maintain service availability under such conditions highlights the practical applicability of the system in real-world blockchain environments, where security and performance are paramount.

In addition to the graphical performance analysis, we provide quantitative results in the form of two tables. Table 1 compares the transaction validation times and throughput for various network sizes under normal conditions, while Table 2 provides a detailed analysis of throughput loss under Sybil and DDoS attack scenarios.

<i>Network Size</i>	<i>Validation Time (ms)</i>	<i>Throughput (TPS)</i>
50	120	1500
100	145	1450
200	175	1400
500	220	1300

**Table 1:** Transaction validation time and throughput for various network sizes.

In Table 1, the validation time increases as the network size grows, but remains within acceptable limits. The scalability of the proposed method is clearly demonstrated, as even at 500 nodes, the validation time is only 220 milliseconds. This performance allows the system to handle high transaction volumes while ensuring timely validation.

<i>Attack</i>	<i>Normal Throughput (TPS)</i>	<i>Attack Throughput (TPS)</i>	<i>Throughput Loss (%)</i>
No Attack	1500	1500	0%
Sybil Attack	1500	1300	13.3%
DDoS Attack	1500	1200	20%

**Table 2:** System throughput under Sybil and DDoS attack scenarios.

Table 2 summarizes the throughput losses under Sybil and DDoS attack conditions. The system experiences minimal performance degradation in both attack scenarios, with a throughput loss of only 13.3% during Sybil attacks and 20% during DDoS attacks. These results underscore the system's ability to maintain high performance and resilience against adversarial attacks, demonstrating the effectiveness of the rate-limiting and load-balancing mechanisms.

## 5 CONCLUSIONS

In this paper, we proposed a novel Notary Pool Consensus Mechanism aimed at improving the scalability and security of blockchain networks. By employing dynamic notary selection based on machine learning-driven trust evaluation, the system ensures efficient transaction validation while maintaining robustness against Sybil and DDoS attacks. The machine learning model assesses validators based on historical performance and real-time behavior, allowing the system to dynamically select the most trustworthy notaries and exclude unreliable ones. Experimental results demonstrated that this mechanism achieves low validation times and high throughput even in larger networks, with superior energy efficiency compared to traditional methods like PoW and PoS. The system's ability to sustain high performance under attack conditions underscores its resilience and suitability for real-world applications. Future research will focus on optimizing the trust evaluation model with more advanced machine learning techniques and exploring enhanced privacy-preserving methods, as well as improving real-time decision-making in notary selection to further strengthen security and scalability in larger blockchain environments.

## REFERENCES

- [1] Khan, D.; Jung, L. T.; Hashmani, M. A.: Systematic literature review of challenges in blockchain scalability, *Applied Sciences*, 11(20), 2021, 9372. <https://www.doi.org/10.3390/app11209372>
- [2] Li, S.; Li, J.; Pei, J.; Wu, S.; Wang, S.; Cheng, L.: Eco-CSAS: A safe and eco-friendly speed advisory system for autonomous vehicle platoon using consortium blockchain, *IEEE Transactions on Intelligent Transportation Systems*, 24(7), 2023, 7802-7812. <https://www.doi.org/10.1109/TITS.2022.3232851>
- [3] Kabra N.; Bhattacharya P.; Tanwar S.; Tyagi S.: MudraChain: Blockchain-based framework for automated cheque clearance in financial institutions, *Future Generation Computer Systems*, 102, 2020, 574-587. <https://www.doi.org/10.1016/j.future.2019.08.035>
- [4] Lashkari B.; Musilek P.: A comprehensive review of blockchain consensus mechanisms, *IEEE Access*, 9, 2021, 43620-43652. <https://www.doi.org/10.1109/ACCESS.2021.3065880>
- [5] Bernabe J. B.; Canovas J. L.; Hernandez-Ramos J. L.; Moreno R. T.; Skarmeta A.: Privacy-preserving solutions for blockchain: Review and challenges, *IEEE Access*, 7, 2019, 164908-164940. <https://www.doi.org/10.1109/ACCESS.2019.2950872>
- [6] Aggarwal S.; Chaudhary R.; Aujla G. S.; Kumar N.; Choo K. K. R.; Zomaya A. Y.: Blockchain for smart communities: Applications, challenges and opportunities, *Journal of Network and Computer Applications*, 144, 2019, 13-48. <https://www.doi.org/10.1016/j.jnca.2019.06.018>
- [7] Xia, H.; Xu, S.; Pei, J.; Zhang, R.; Yu, Z.; Zou, W.; Liu, C.: Fedme: Memory evaluation & erase promoting federated unlearning in dtmn, *IEEE Journal on Selected Areas in Communications*, 2023. <https://www.doi.org/10.1109/JSAC.2023.3310049>
- [8] Platt M.; McBurney P.: Sybil in the haystack: A comprehensive review of blockchain consensus mechanisms in search of strong Sybil attack resistance, *Algorithms*, 16(1), 2023, 34. <https://www.doi.org/10.3390/a16010034>
- [9] Xu G.; Zhang J.; Cliff U. G. O.; Ma C.: An efficient blockchain-based privacy-preserving scheme with attribute and homomorphic encryption, *International Journal of Intelligent Systems*, 37(12), 2022, 10715-10750. <https://www.doi.org/10.1002/int.22946>
- [10] Pei, J.; Liu, W.; Li, J.; Wang, L.; Liu, C.: A Review of Federated Learning Methods in Heterogeneous scenarios, *IEEE Transactions on Consumer Electronics*, 2024. <https://www.doi.org/10.1109/TCE.2024.3385440>
- [11] Chen H.; Luo X.; Shi L.; Cao Y.; Zhang Y.: Security challenges and defense approaches for blockchain-based services from a full-stack architecture perspective, *Blockchain: Research and Applications*, 4(3), 2023, 100135. <https://doi.org/10.1016/j.bcra.2023.100135>
- [12] Chaganti R.; Boppana R. V.; Ravi V.; Munir K.; Almutairi M.; Rustam F.; Ashraf I.: A comprehensive review of denial of service attacks in the blockchain ecosystem and open

- challenges, IEEE Access, 10, 2022, 96538-96555. <https://www.doi.org/10.1109/ACCESS.2022.3205019>
- [13] Kaur, G.; Gandhi, C.: Scalability in blockchain: Challenges and solutions, In Handbook of Research on Blockchain Technology, 1, 2020, 373-406. <https://www.doi.org/10.1016/b978-0-12-819816-2.00015-0>
- [14] Cai, W.; Jiang, W.; Xie, K.; Zhu, Y.; Liu, Y.; Shen, T.: Dynamic reputation-based consensus mechanism: Real-time transactions for energy blockchain, International Journal of Distributed Sensor Networks, 16(3), 2020, 1550147720907335. <https://www.doi.org/10.1177/1550147720907335>
- [15] Saleh, O. S.; Ghazali, O.; Rana, M. E.: Blockchain-based framework for educational certificates verification, Journal of Critical Reviews, 2020. <https://www.doi.org/10.31838/jcr.07.03.13>
- [16] Tripathi, G.; Ahad, M. A.; Casalino, G.: A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges, Decision Analytics Journal, 2023, 100344. <https://doi.org/10.1016/j.dajour.2023.100344>
- [17] Yu, Y.; Li, Y.; Tian, J.; Liu, J.: Blockchain-based solutions to security and privacy issues in the Internet of things, IEEE Wireless Communications, 25(6), 2018, 12-18. <https://www.doi.org/10.1109/MWC.2017.1800116>
- [18] Pu, Y.; Xiang, T.; Hu, C.; Alrawais, A.; Yan, H.: An efficient blockchain-based privacy preserving scheme for vehicular social networks, Information Sciences, 540, 2020, 308-324. <https://doi.org/10.1016/j.ins.2020.05.087>
- [19] Dabbagh, M.; Sookhak, M.; Safa, N. S.: The evolution of blockchain: A bibliometric study, IEEE Access, 7, 2019, 19212-19221. <https://www.doi.org/10.1109/ACCESS.2019.2895646>
- [20] Hussain, A. A.; Al-Turjman, F.: Artificial intelligence and blockchain: A review, Transactions on Emerging Telecommunications Technologies, 32(9), 2021, e4268. <https://www.doi.org/10.1002/ett.4268>
- [21] Lee, S.; Kim, S.: Blockchain as a cyber defense: opportunities, applications, and challenges, IEEE Access, 10, 2021, 2602-2618. <https://www.doi.org/10.1109/ACCESS.2021.3136328>
- [22] Shah, Z.; Ullah, I.; Li, H.; Levula, A.; Khurshid, K.: Blockchain-based solutions to mitigate distributed denial of service (DDoS) attacks in the Internet of Things (IoT): A survey, Sensors, 22(3), 2021, 1094. <https://doi.org/10.3390/s22031094>
- [23] Javaid, M.; Haleem, A.; Singh, R. P.; Suman, R.; Khan, S.: A review of Blockchain Technology applications for financial services, BenchCouncil Transactions on Benchmarks, Standards and Evaluations, 2(3), 2022, 100073. <https://www.doi.org/10.1016/j.tbench.2022.100073M>
- [24] Wu, D.; Ansari, N.: A trust-evaluation-enhanced blockchain-secured industrial IoT system, IEEE Internet of Things Journal, 8(7), 2020, 5510-5517. <https://www.doi.org/10.1109/JIOT.2020.3030689>
- [25] Zhang, C.; Zhu, L.; Xu, C.; Sharif, K.; Lu, R.; Chen, Y.: Appb: Anti-counterfeiting and privacy-preserving blockchain-based vehicle supply chains, IEEE Transactions on Vehicular Technology, 71(12), 2022, 13152-13164. <https://www.doi.org/10.1109/TVT.2022.3196051>