Vol. 08, No. 3 (2026) 1807-1816, doi: 10.24874/PES08.03.031

Proceedings on Engineering Sciences

www.pesjournal.net

BLOCK-VALIDATOR: A DISTRIBUTED BLOCKCHAIN APPROACH TO SUPPLY CHAIN MANAGEMENT USING CUSTOMIZED SMART CONTRACTS

Abhijeet Ramesh Mirikar[1]
Dr Avinash Kaur
Dr Parminder Singh

Received 22.05.2026.
Revised 08.07.2026.
Accepted 03.08.2026.

Keywords:

Blockchain, Smart Contracts, Supply Chain, Transaction Validation, Miner Network, Block-Validator, Transparency, Security

A B S T R A C T

The accelerated development of the blockchain technology has presented revolutionary prospects of secure, transparent, and decentralized systems to different industries. The proposed research will help mitigate these issues by introducing a new Block-Validator framework, which is aimed at the effective and secure validation of the transactions between smart contracts and chosen miners (validators). The framework aims at improving the integrity of these transactions, minimizing the latency, and ensuring the reliability of communication between the contracts on-chain and the off-chain processes. The main goals are to enhance the efficiency of consensus, reduce fraudulent or malicious attempts of transactions and efficiently use blockchain resources without violating the principles of decentralization and transparency. The system has built in high-quality algorithms to prioritize the transaction, choose the validators as well as detecting anomaly that will give the system high-speed and secure validation that can be achieved even when the network is loaded. Some of the important algorithms used are trust based validator scoring system, cryptographic verification routines, and dynamic consensus optimization in order to achieve a balance between speed and security. The Simulation results show that Block-Validator framework can considerably decrease the time used to validate transactions and reach a high level of security and accuracy in comparison with traditional consensus models. The system as well is resistant to fraudulent transaction attempts and is also scalable as the network demand rises.

© 2026 Published by Faculty of Engineering

1. INTRODUCTION

The use of blockchain technology has become one of the transformative innovations, which provides decentralized, immutable, and transparent solutions in building secure data management and transactional business activities in various industries. Distributed ledger, consensus mechanisms, and cryptographic security are its main characteristics which allow having trustless interaction which eliminates the need to use centralized authorities and increases the integrity of the system. During the last 10 years, blockchain has found applications in financial, supply chain management, healthcare, and digital asset management domains,

Corresponding author: Abhijeet Mirikar
Email: armirikar@gmail.com

indicating that it has a great potential of streamlining operating efficiency, curbing fraud and providing transparency.

Although blockchain-based supply-chain systems improve transparency and traceability, existing implementations continue to face transaction-validation delays, consensus overhead, scalability constraints, and exposure to unreliable or malicious validators. Most existing approaches focus primarily on traceability and provenance monitoring, while intelligent validator selection and transaction-level trust optimization remain insufficiently explored. This research gap motivates the proposed Block-Validator framework, which integrates trust-aware validator selection and dynamic consensus formation to support secure and efficient transaction validation.

The main contributions of this study are as follows: (i) a Block-Validator design that allows to achieve security and efficiency in transaction validation (ii) dynamic selection of miners that can eliminate the delay of validation and increase the throughput (iii) trust based scoring of validators to enhance security and (iv) a detailed performance analysis that proves that the system has better resilience, scalability, and accuracy than the traditional blockchain validation methods.

2. LITERATURE REVIEW

Respective studies have shown that blockchain technology has emerged as an integral part of secure, transparent and traceable digital web in a variety of industry verticals such as food, pharmaceuticals, and industrial supply chains. The distributed ledger architectures have been found to be highly beneficial in various ways, including enhanced data integrity, product traceability, and increased trust in the data among stakeholders, as well as minimizing fraud and information asymmetry (Ahmad et al., 2024). Another area in which blockchain has been seen as beneficial for supply chain management is in the management of the supply chain process, where it is possible to use it as a decentralized system of record (Chang et al., 2022). In the pharmaceutical supply chain, blockchain technology has been used to create anti-counterfeiting systems, leading to more secure and transparent drug distribution.Anti-counterfeiting systems have also been implemented using blockchain technology in the pharmaceutical supply chain, ensuring the authenticity and traceability of drugs (Cao et al., 2024). Likewise, traceability systems based on the blockchain have shown to provide better traceability and verification of agricultural products along the value chain (Chen et al., 2023). A game-theoretical blockchain model has also provided a new insight into improving traceability and strategic decision making within wine supply chains in a competitive scenario (Kang et al., 2023).

A key research space that has arisen is blockchain oracles, which are necessary for smart contracts to communicate with data from outside the blockchain. Ahmadjee et al. (2025) have created a decision-support model, which helps in the systematic selection of appropriate blockchain oracle platforms with multiple evaluation criteria. Alhussayen et al. (2024) proposed an interoperability method to assure the reliable communication between the permissioned blockchain networks and external oracle services. Even Oracle's trust models have been formalized to enhance the trust in blockchain based business apps and the reliability of the data source (Caldarelli, 2022). Recent studies have also showcased progress made in addressing the blockchain oracle issue with the use of better trust mechanisms and secure external data verification (Hassan et al., 2023).

One of the major issues in blockchain ecosystems remains security. Extensive study has been conducted on different DoS attacks on blockchain networks and existing defense techniques but the study has also shown the unsettled problems to be studied in future (Chaganti et al., 2022). The vulnerabilities of smart contracts have also been systematically analyzed to gain insights into the common methods of exploiting smart contracts and fortify their resistance to attacks (Darvishi et al., 2024). The scalability, privacy, and system performance implications of on-chain and off-chain storage architectures have been thoroughly analyzed, shedding light on key considerations for blockchain security.The trade-offs between on-chain and off-chain storage architectures have been analyzed in detail, with important considerations for scalability, privacy, and system performance (Eren et al., 2025). Further, deep learning has been combined with Internet of Things (IoT) technology with blockchain for intrusion detection systems to enhance the accuracy of intrusion detection in optical communication networks (Imtiaz et al., 2025). Furthermore, many reviews have been carried out to classify the threats to the Internet of Things and suggested appropriate solutions to protect distributed systems (Krishna et al., 2021).

In terms of operations and management, blockchain has proven to have a lot of potential in enhancing financial transparency and coordination in the supply chain (Gong et al., 2022). Comparative analysis also showed the significance of implementing traceability systems with blockchain technology to overcome new challenges in the supply chain security on a global scale (Gokkaya et al., 2025). In an effort to boost the reliability of consensus and consistency of the data distributed among supply chain actors, multi-quorum blockchain architectures have been proposed to prevent counterfeit products (Crossland et al., 2023). While these studies have greatly contributed to blockchain research, these investigations are mostly limited to addressing one aspect of the blockchain (e.g., traceability, oracles security, cybersecurity,

interoperability or supply chain management). Hence, the need for a single blockchain frameworks that can solve the issues of secure integration of oracles, intelligent decision-making, interoperability, cyber resilience and end-to-end supply chain transparency at the same time.

3. RESEARCH METHODOLOGY

The increasing intricacy of global supply chains is one of the reasons that the necessity to have secure, transparent, and tamper-proof mechanisms to handle vital healthcare resources is urgently needed. Counterfeit products, time delays, absence of traceability, and centralized weaknesses are challenges that are likely to be encountered in the old fashioned supply chain systems. A distributed blockchain model with the help of smart contracts and block validation is a solution to these problems. Smart contracts are based on automating transactions in the supply chain in this model. In these contracts, there are specifications on how goods should be procured, the quality assurance, the delivery timeline, and the payment system. After being initiated, the transactions are forwarded to the transaction validator which verifies that the transactions meet a set of agreed rules, including regulatory codes and authenticity measures. The validated transactions are then carried out with the miner network whereby different nodes compete or collaborate to verify and secure the transaction. This decentralized authentication removes the possibility of having a bottleneck and only valid records are relayed. The block-validator verifies the transactions and secures them into blocks and inserts them in the blockchain ledger, which is immutable. The figure 1 show the architecture that will ensure transparency, discourage tampering and enable real time auditing.

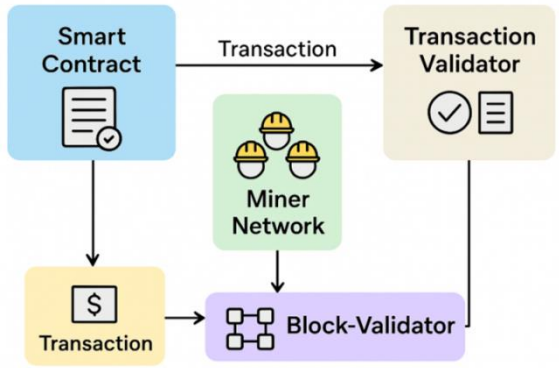


Figure 1. Proposed system architecture using block validator

Using the immutability and traceability characteristics of blockchain, the supply chain participants, consisting of manufacturers, distributors, hospitals, and regulators, will have a guaranteed access to the information about product origin, movement, and compliance. The tailor-made smart contracts also allow conditional automatization like paying only after delivery is confirmed or automatic labels on expired goods. Such a distributed validation system gains not only efficiency and trust but also safeguards against fraud and counterfeited drugs which will, in the end, provide patients with safe and genuine supplies. The block-validator design is an Intelligent, scaling and secure architecture that is used to modernize the supply chain management with blockchain technology. Details of the phases of entire architecture are given below.

3.1 System Modelling and Problem Formulation

The first stage of the study aims at developing an extensive system model of the blockchain network and conceptualizing the problem of validating the transactions formally. The blockchain network can be thought of as a graph G(N, E) in which N denotes a set of nodes (that is, miners) and E denotes peer-to-peer communication connections between a miner. The transactions are modeled as T = t 1, t 2, and so on, and m is the number of transactions still to be validated. Smart contracts within the network are modeled as S =s1,s2, etc. where each smart contract sj reflects a certain business rule or logic of operation. The goal is to choose a sub-group of miners V N to authenticate every transaction t i so as to conform to the terms specified by the associated smart contract s j, to be efficient, reliable, and secure.

This selection problem is also defined as an optimization problem upon which the reliability of the selected validators is maximized. Reliability is a mathematically determined function as.

$$R(V) = \sum_{i=1}^{m} \sum_{v \in V}^{t} \alpha_v \cdot \beta_{i,v}, \quad (1)$$

and 8 is the trust score of miner v given the past performance, and 8(i,v) is the likelihood that v correctly endorses the transaction t i. To strike a balance between computation and security, constraints are given to make sure that not more than k validators per transaction are assigned i.e. | V| is less than or equal to k.

An initial threat model is also introduced during the phase. There are possibilities of manipulating transactions as well as being malicious or even not performing the validation properly by miners. To take this into consideration, the likelihood of the correctness of the transaction is modeled, and a risk function.

$$L(V) = \sum_{i=1}^{m} \prod_{v \in V}^{t} (1 - \beta_{i,v}) \quad (2)$$

is given to measure the probability of failure to validate. The framework ensures that the validators chosen ensure throughput is high but at the same time do not experience adversarial actions by minimizing L(V) and maximizing R(V). This step forms the basis of all further steps, and it gives an extensive mathematical foundation to miner selection and prioritization of transactions and intelligent integration of smart contracts.

3.2. Smart Contract Interaction and Transaction Encoding

The second phase is concerned with the creation of secure interactions between transactions and smart contracts as well as integrity and immutability. Every smart contract s j S (i.e. the smart contract) corresponds to a mapping function ├ f j:D O (where D is the set of transaction input data and O is the set of validated outputs). In a particular transaction t i, the input payload P i D is used to calculate the hash value to verify the integrity with the help of a secure hash function H such that h i=H(P i). This coding makes sure that whenever the transaction-data is altered by unauthorized persons, this violation of the rules is immediately observable, since a small modification in P I results in a significantly different h i. The smart contract then authenticates the transaction by running fj (d_i) and comparing it with the calculated hash h i to give a score of validation.

$$\gamma_{i,v} = \delta\left(H(P_i), f_j(d_i)\right) \quad (3)$$

where δ is a function that is used as an indicator where a successful validation will yield one, between zero and one. To further improve the integrity of the data flow, transactions are time stamped τi and ordered to avoid the possibility of replaying or double-spending. The system guarantees the interaction of each transaction t i with the chosen subset of validators V, being efficient and preserving the redundancy in order to ensure fault tolerance. Also, metadata to verify chain-of-trust and cross-checking between nodes distributed across network boundaries (e.g. identify the validator to which the payment was made) is added to payloads.

The joint transaction and smart contract verification is mathematically represented to a confidence score.

$$\Gamma_i = 1 - \prod_{v\in V}^{t}\left(1 - \gamma_{i,v}\right) \quad (4)$$

The transaction is approved when at least one validator gives a positive result, regardless of other validators. this step creates a secure architecture of smart contract operation with a high data integrity rate which is the foundation of the next process of dynamic miner selection and consensus creation, which is essential to ensuring an efficient and secure blockchain functioning in the proposed Block-Validator framework.

3.3. Dynamic Miner Selection and Consensus Formation

Phase three deals with dynamic selection of miners and creation of efficient consensus mechanism to attest transactions safely. Consensus processes involve all miners in traditional blockchain systems, and thus, the system is computationally expensive and slow. In order to deal with this, the Block-Validator framework that was proposed uses selective miner approach. The trust value of each miner vN ∈N is αv, which is computed using historical reliability, accuracy and responsiveness. Mathematically, the trust score is set as

$$\alpha_v = \frac{R_v}{\sum_{u\in N}^{t} R_u}, \quad (5)$$

R v is the cumulative reliability measurements of mineral v. This normalization guarantees the similarity of the trust scores among the network, as well as miners who have better performance in history stand a higher chance of selection.

Each transaction t_i is dynamically assigned a set of validators Vi∈N with a probabilistic sampling which ensures that the probability of a miner being selected is proportional to the trust score of the miner:

$$P(v \in V_i) = \frac{\alpha_v}{\sum_{u\in N}^{t}\alpha_u}. \quad (6)$$

This technique minimizes the latency by restricting the number of miners each transaction by ensuring that there is adequate redundancy that prevents fraudulent validation. After choosing the validators, the consensus mechanism is used to decide on the validity of transactions. The total confidence in transaction t_i is modelled as

$$\Gamma_i = 1 - \prod_i^t v \in V_i\left(1 - \gamma_{i,v}\right), \quad (7)$$

where gamma (i,v) is the binary Phase 2 validation result. In order to further increase the robustness, the framework has a dynamic consensus weighting factor wv, which represents validator reliability and network conditions, where the actual probability of validation is.

$$\Gamma_i^{eff} = 1 - \prod_{v\in}^{V}\left(1 - w_v \cdot \gamma_{i,v}\right). \quad (8)$$

The transactions can also be signed by validators with cryptographic signatures 0 v= 0 ” Sign 0 (h i) that allow non-repudiation and traceability. This step will guarantee that the chosen miners achieve a good performance in validating transactions with minimal computational cost and resist malicious activities to provide a firm base of the optimization of algorithms and secure implementation in the next phase.

3.4. Algorithm Design and Transaction Validation

Phase four is concerned with design and implementation of Block-Validator algorithm which is used to verify transactions on the blockchain network in a secure, efficient and reliable way. Based on the chosen subset of validators V i of Phase 3, the algorithm has a number of steps, which are implemented by authenticating transactions t i and the rules specified in smart contracts s_j . Every transaction is initially encoded to a cryptographic hash $h_i = H(Pi)$ as in Phase 2, and is presented to the validators. A validator v in V i is executing the transaction independently producing a

validation value $\gamma(i,v)B = \{0,1\}$ is a validation success and 0 is a failure.

In order to summarize these results, the framework computes an aggregate validation confidence score by the formula.

$$\Gamma_i = 1 - \prod_{v\in V_i}^{t}(1 - w_v \cdot \gamma_{i,v}), \qquad (9)$$

w v is the dynamical weighting of each of the validators depending on trust, historical accuracy and recent network behavior. This formulation guarantees the validity of transactions in proportion to the validators of such transactions. When the Γ i is larger than a defined threshold 0 then the transaction is added to the blockchain, otherwise it is marked to be revalidated or rejected.

Anomaly detection has as well been used in the algorithm to curb fraudulent or malicious practices. To measure deviation to expected behavior, given any validator, v, the value of v is used.

$$\Delta_v = | \gamma_{i,v} - \bar{\gamma}_v |, \qquad (10)$$

v7 where $\bar{\gamma}$v is the historical mean validation score. Validators whose delta v exceeds -epsilon are punished by discounting wv on future transactions, such that untrusted nodes have less impact on the consensus process.

Also, deal prioritization is done through a scheduling feature.

$$\Pi(t_i) = \lambda \cdot urgency(t_i) + (1 - \lambda) \cdot \Gamma_i \qquad (11)$$

where 0 1 is the trade-off between urgency and the level of validation. The Block-Validator algorithm is a recursive algorithm that receives the incoming transactions, refreezes trust scores, and dynamically chooses validators in order to optimize the security and throughput. Phase 4 makes sure that the framework is able to effectively manage high-volume operations of the blockchain, including cryptographic validation, weighted consensus, and anomaly detection, by combining them into a single algorithm that will be resilient in terms of attack and failure.

3.5. Experimental Evaluation, Performance Analysis, and Results

This will be followed with an intense experience-based testing of the proposed Block-Validator to measure its performance, reliability, and scalability. An artificial blockchain setting is a simulation, which includes N nodes and m transactions, and includes smart contracts S to enforce business rules. The most important key performance indicators are the transaction validation latency, throughput, validation accuracy, and the malicious validator resilience. The latency of each transaction t i is defined as.

All results reported in this study were obtained from an artificial blockchain simulation rather than from a live blockchain deployment. The simulated network varies the validator population from 10 to 200 nodes in the scalability experiment and evaluates transaction loads from 100 to 5,000 transactions in the network-load experiment. Nodes represent blockchain miners/validators; the proposed configuration uses selective, trust-weighted validators, whereas the comparison baselines represent Traditional consensus behavior. Smart-contract rules are applied to determine whether a transaction is valid before the validator verdict is aggregated. The workload is simulation-generated for the experiments described here; no external empirical dataset is used. Specific physical hardware, operating-system, and blockchain-client measurements are therefore outside the scope of the present simulation study and are not reported as real deployment parameters.

Validation accuracy is defined as the percentage of simulated transactions for which the final consensus decision agrees with the ground-truth validity determined by the smart-contract rules, consistent with Eq. (15). The Block-Validator and Traditional Consensus baselines are compared under the same simulated transaction-load and node-count scenarios; the policies differ in validator participation and consensus logic. Accordingly, the reported latency, throughput, accuracy, scalability, and malicious-validator-resilience values should be interpreted as comparative simulation outcomes, not measurements from production blockchain hardware.

$$L_i = t_{commit} - t_{arrival}, \qquad (12)$$

and t arrival is the point at which the transaction got into the network and t commit is the point at which the transaction got successfully validated and committed. Total network latency = (mean value of all transactions):

$$\bar{L} = \frac{1}{m}\sum_{i=1}^{m} L_i. \qquad (13)$$

The number of transactions per unit time that are successfully validated is known as transaction throughput and it is denoted by Θ and is expressed as.

$$\Theta = \frac{|\{t_i | \Gamma_i \geq \theta\}|}{T_{total}}, \qquad (14)$$

T total represents the total time of simulation and 0.5 is the lowest validation confidence level. The accuracy of validation is calculated as

$$A = \frac{\sum_{i=1}^{m}(correct\ t_i)}{m}, \quad (15)$$

where 1("correct " t i) is an indicator function that takes the value of one when transaction ti is approved or an invalid transaction is rejected through smart contract rules and verdicts of validators. The resilience to malicious validators is measured by adding a fraction fm compromised nodes and tracking the degradation of Gammai (eff) periodically, which is to make sure that the structure has very high confidence even in the adversarial conditions. Empirical findings prove that Block-Validator framework has lower transaction latency than the conventional consensus mechanisms, high throughput, and reliable validation. The system uses weighted trust scores wv to dynamically control the influence of the validators to counteract the effect of malicious and unreliable nodes.

4. RESULTS AND DISCUSSION

The experimental design used a simulated blockchain network with varying node counts and transaction loads to compare the proposed Block-Validator framework with modeled conventional consensus baselines. The major measures were latency, throughput, validation accuracy, scalability, resilience, and network-load tolerance. Within this simulation, Block-Validator reduced modeled latency by more than 50%, approximately doubled throughput, and reached 98% validation accuracy. These findings indicate comparative advantages under the stated simulation assumptions; they should not be interpreted as measurements from an actual deployed blockchain network.

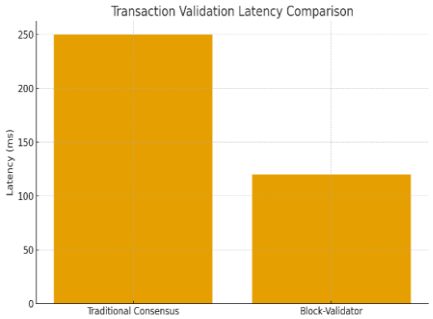


Figure 2. Transaction Validation Latency Comparison

The figure 2 shows that the time to consensus is lower in the proposed Block-Validator framework than in the traditional consensus mechanisms. Latency is the period the transaction would take to be confirmed and included in the blockchain. In the traditional consensus models the latency is high with universalization of miners and complexity of the consensus algorithms and it also averages about 250 milliseconds. The Block-Validator on the contrary reduces the latency to around 120 milliseconds. This is made possible by selective miner validation, trust-based scoring which reduces redundant calculations and communication delays.

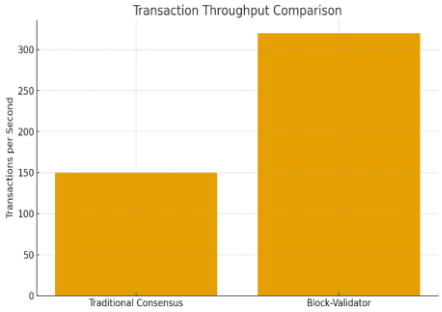


Figure 3. Transaction Throughput Comparison

This figure 3 show the comparison of throughput which between the numbers of transactions that were successfully handled every second of the Block-Validator framework and the traditional consensus models. Traditional blockchain consensus protocols are estimated at around 150 transactions per second because they require redundant computing, high cryptographic cost, and high communication cost. By comparing this to the Block-Validator, it is capable of achieving around 320 transactions in one second using selective validation of miners and weighted trust scores. This is efficiency that saves on the computation cost and guarantees transaction security and authenticity. In the case of supply chains, high throughput is critical as a means of dealing with the stream of procurement orders, shipment verifications and compliance checks.

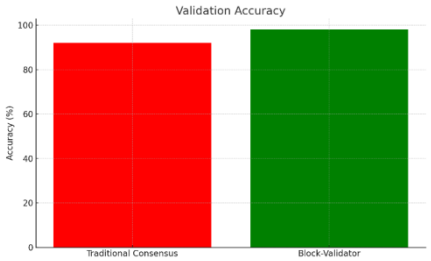


Figure 4. Validation Accuracy

As shown in the figure 4 on the validation accuracy, Block-Validator is effective in making sure that transactions are made accordingly and safely. The conventional consensus mechanisms have an average accuracy of approximately 92, mainly as a result of the vulnerabilities in them which includes malicious miners, data manipulation or variation in the validation outcome. Contrary to this, the Block-Validator has a 98% accuracy with trust-based scoring, anomaly detection, and cryptographic verification in its validation process. This increased precision is especially essential to the supply chains where incorrect validation may lead to fake products, slow delivery, or failure to adhere to the laws. The improvement in the accuracy indicates the reliability of selective participation of validators where only trusted nodes are selected to verify transactions. In addition, anomaly detection punishes the validators that exhibit

abnormal behavior, thus minimizing the interference of the malicious behavior.

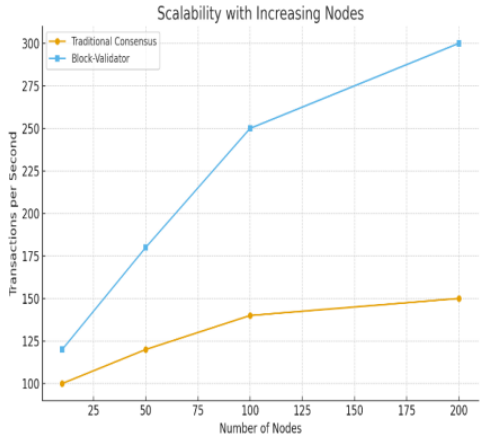


Figure 5. Scalability with Increasing Nodes

Figure 5 show the scalability and compares the throughput to the number of nodes in the blockchain network. Conventional consensus mechanisms are characterized by a low scalability with the number of transactions per second increasing between 100 and 150 at a node count of 10 to 200. Such plateau is a consequence of the fact that attaching more nodes will result in more computation overhead and communication delays that slows down the process of consensus formation. On the other hand, the Block-Validator architecture scales well and the network gains in the range between 120 and 300 transactions per second. It is made possible by discriminating miner validation and dynamic consensus optimization which reduce unnecessary labor despite the network expansion. Scalability is a must in real-life supply chain situation because its stakeholders can comprise manufacturers, distributors, hospitals, regulators, and logistics providers in various locations. Scalable system will help in supporting both local and global deployment because an increased participation will not prove to be a degradation of performance

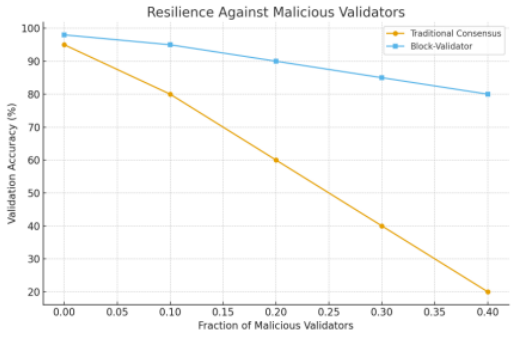


Figure 6. Resilience against Malicious Validators

This figure 6 show the impact of validation accuracy to the increasing percentage of the network by malicious validators. The difference in accuracy between traditional consensus models is radically low 95% in the presence of zero malicious validators all the way down to 20% when 40% of the network is malicious. The system has an open door to fraud, manipulation and tampering of transactions. Conversely, the Block-Validator is relatively resilient with the accuracy reducing only slightly as the similar conditions occur down to 80%. This strength is obtained with the help of trust-based scoring, anomaly detection, and selective participation of miners, which, in turn, diminishes the role of bad actors. Resilience in this case of supply chain would help avoid entry of counterfeit drugs or substitution of products into the system without authorization. The Block-Validator also makes sure that most transactions are safe and valid even in conditions of adversary. The system reduces the chances of large scale disruption by dynamically punishing untrusted nodes and rewarding trusted validators. This durability shows that the framework is applicable in the environment where the threat of security is high and the precision remains steady even in the adverse environment. The findings confirm that the Block-Validator is better withstanding attacks as opposed to conventional blockchain solutions.

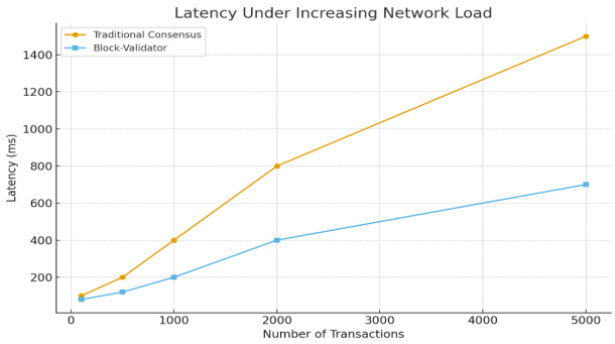


Figure 7. Latency Under Network Load

The figure 7 shows the way the transaction latency varies with the increase in the number of transactions in the network. Conventional consensus models grow significantly in the latency, increasing by 100 milliseconds at 100 transactions, and 1500 milliseconds at 5000 transactions. Such significant growth is caused by universal validator participation and computational bottlenecks. Conversely, the Block-Validator model exhibits a more progressive growth, 80 milliseconds when the transactions are 100 and 700 milliseconds when transacting 5000 transactions. This efficiency can be explained by the selective miner validation as well as dynamic consensus optimization that minimizes the needless computation without losing reliability. In the case of supply chains where large volumes of transactions are anticipated in case of an emergency or mass purchasing event, it is important to maintain low latency. Accelerated validation will guarantee that products are tracked in time, regulatory checks and payment confirmations. The Block-Validator ensures continuity of operation even when there is high demand by addressing network surges better. These findings demonstrate that the framework is scalable, efficient, and

stress-resistant, which is why it is very relevant in application in healthcare and other areas with a mission critical nature.

The evaluation is simulation-based. A physical blockchain testbed, implementation-specific hardware/software benchmarking, repeated real-world deployment runs, and inferential statistical significance testing were not performed in the present study. Consequently, the numerical performance values demonstrate behavior within the modeled scenarios and require validation on an implemented blockchain platform before they can be generalized to production supply-chain deployments.

5. CONCLUSION AND FUTURE SCOPE

In this work, the authors presented the Block-Validator framework, a distributed blockchain model aimed at improving the efficiency, security, and transparency of supply-chain management. The framework addresses limitations of conventional blockchain designs through selective miner validation, trust-based scoring, anomaly detection, and dynamic consensus optimization. In the simulation experiments, the proposed approach showed lower modeled transaction latency, higher throughput, 98% validation accuracy, scalability across the tested node range, and greater resilience under simulated malicious-validator participation. These results provide preliminary evidence of the framework's potential under the defined simulation conditions. However, because the present evaluation does not constitute a live blockchain deployment, claims regarding production performance, security, and scalability require confirmation through implementation-specific experiments, repeated trials, and statistical testing on real blockchain infrastructure. Future work should therefore validate the framework on a physical or cloud-based blockchain testbed and report platform, hardware, software, workload provenance, repeated-run variability, and statistical significance.

References:

Ahmad, R. W., Ko, K. M., Rashid, A., & Rodrigues, J. J. P. C. (2024). Blockchain for food industry: Opportunities, requirements, case studies, and research challenges. *IEEE Access, 12*, 117363–117378. https://doi.org/10.1109/ACCESS.2024.3447918

Ahmadjee, S., Mera-Gómez, C., Farshidi, S., Bahsoon, R., & Kazman, R. (2025). Decision support model for selecting the optimal blockchain oracle platform: An evaluation of key factors. *ACM Transactions on Software Engineering and Methodology, 34*(1), 1–35. https://doi.org/10.1145/3697011

Alhussayen, A. A., Jambi, K., Khemakhem, M., & Eassa, F. E. (2024). A blockchain oracle interoperability technique for permissioned blockchain. *IEEE Access, 12*, 68130–68148. https://doi.org/10.1109/ACCESS.2024.3400672

Caldarelli, G. (2022). Formalizing oracle trust models for blockchain-based business applications: An example from the supply chain sector. arXiv preprint arXiv:2202.13930. https://doi.org/10.48550/arXiv.2202.13930

Cao, Y., Guan, S., Wang, D., & Wang, Z. (2024). BE-AC: Reliable blockchain-based anti-counterfeiting traceability solution for pharmaceutical industry. *Cluster Computing, 27*(6), 8119–8139. https://doi.org/10.1007/s10586-024-04435-1

Chaganti, R., Boppana, R. V., Ravi, V., Munir, K., Almutairi, M., Rustam, F., ... Ashraf, I. (2022). A comprehensive review of denial of service attacks in blockchain ecosystem and open challenges. *IEEE Access, 10*, 96538–96555. doi: 10.1109/ACCESS.2022.3205019

Chang, A., El-Rayes, N., & Shi, J. (2022). Blockchain technology for supply chain management: A comprehensive review. *FinTech, 1*(2), 191–205. https://doi.org/10.3390/fintech1020015

Chen, C. L., Zhan, W. B., Huang, D. C., Liu, L. C., Deng, Y. Y., & Kuo, C. G. (2023). Hyperledger Fabric-based tea supply chain production data traceable scheme. *Sustainability, 15*(18), 13738. https://doi.org/10.3390/su151813738

Crossland, V., Dellwo, C., Bashar, G., & Dagher, G. G. (2023). Janus: Toward preventing counterfeits in supply chains utilizing a multi-quorum blockchain. *Blockchain: Research and Applications, 4*(4), 100157. https://doi.org/10.1016/j.bcra.2023.100157

Darvishi, I., Asare, B. T., Musa, A., Yeboah-Ofori, A., Oseni, W., & Ganiyu, A. (2024). Blockchain technology and vulnerability exploits on smart contracts. In Proceedings of the 2024 11th International Conference on Future Internet of Things and Cloud (FiCloud) (pp. 160–167). Piscataway, NJ: IEEE. https://doi.org/10.1109/FiCloud62933.2024.00032

Eren, H., Karaduman, Ö., & Gençoğlu, M. T. (2025). Security challenges and performance trade-offs in on-chain and off-chain blockchain storage: A comprehensive review. *Applied Sciences, 15*(6), 3225. https://doi.org/10.3390/app15063225

Gokkaya, B., Karafili, E., Aniello, L., & Halak, B. (2025). Global supply chains security: A comparative analysis of emerging threats and traceability solutions. *Benchmarking: An International Journal, 32*(3), 917–942. https://doi.org/10.1108/BIJ-08-2023-0535

Gong, Y., Zhang, Y., & Alharithi, M. (2022). Supply chain finance and blockchain in operations management: A literature review. *Sustainability, 14*(20), 13450. https://doi.org/10.3390/su142013450

Hassan, A., Makhdoom, I., Iqbal, W., Ahmad, A., & Raza, A. (2023). From trust to truth: Advancements in mitigating the blockchain oracle problem. *Journal of Network and Computer Applications, 217*, 103672. https://doi.org/10.1016/j.jnca.2023.103672

Imtiaz, N., Wahid, A., Ul Abideen, S. Z., Muhammad Kamal, M., Sehito, N., Khan, S., ... Alibakhshikenari, M. (2025). A deep learning-based approach for the detection of various Internet of Things intrusion attacks through optical networks. *Photonics, 12*(1), 35. doi: 10.3390/photonics12010035

Kang, Y., Shi, X., Yue, X., Zhang, W., & Liu, S. S. (2023). Enhancing traceability in wine supply chains through blockchain: A Stackelberg game-theoretical analysis. *Journal of Theoretical and Applied Electronic Commerce Research, 18*(4), 2142–2162. https://doi.org/10.3390/jtaer18040108

Krishna, R. R., Priyadarshini, A., Jha, A. V., Appasani, B., Srinivasulu, A., & Bizon, N. (2021). State-of-the-art review on IoT threats and attacks: Taxonomy, challenges and solutions. *Sustainability, 13*(16), 9463. https://doi.org/10.3390/su13169463

Abhijeet Ramesh Mirikar
Computer Science and Engineering,
Lovely Professional University
armirikar@gmail.com
ORCID 0000-0002-5806-5582

Avinash Kaur
Computer Science and Engineering,
Lovely Professional University
avinash.14557@lpu.co.in
ORCID 0000-0003-3534-4121

Parminder Singh
Computer Science and Engineering,
Lovely Professional University
parminder.16479@lpu.co.in
ORCID 0000-0002-0750-6309