Journal of Engineering Management and Systems Engineering
https://www.acadlore.com/journals/JEMSE

A Blockchain-Enabled Medical Supply Chain Framework Integrating Hybrid Consensus, Smart Contracts, and Dynamic Quick Response-Based Traceability for Distributed Healthcare Systems

Priyanka S. Dhumal*, Shruti K. Dixit

Department of Electronics and Communication Engineering, School of Engineering and Technology, Sanjeev Agrawal Global Educational (S.A.G.E) University, 462022 Bhopal, India

* Correspondence: Priyanka S. Dhumal (dhumalpriyanka9786@gmail.com)

Received: 04-08-2026 **Revised:** 05-24-2026 **Accepted:** 06-09-2026

Citation: P. S. Dhumal and S. K. Dixit, "A blockchain-enabled medical supply chain framework integrating hybrid consensus, smart contracts, and dynamic quick response-based traceability for distributed healthcare systems," *J. Eng. Manag. Syst. Eng.*, vol. 5, no. 2, pp. 249–264, 2026. https://doi.org/10.56578/jemse050207.

Abstract: Healthcare supply chains face increasing challenges related to counterfeit products, fragmented information flows, limited traceability, and insufficient coordination among distributed stakeholders. Existing centralized and partially decentralized approaches still encounter difficulties in maintaining immutable records, real-time verification, and trusted operational transparency across the pharmaceutical distribution process. This study investigates a distributed medical supply chain framework that improves traceability, compliance control, and operational reliability in healthcare logistics. A blockchain-enabled architecture was developed by integrating dynamic quick response (QR)-based identification, customizable smart contracts, and a hybrid consensus mechanism combining Proof-of-Work (PoW) and Proof-of-Stake (PoS). The framework assigned a unique cryptographic identity to each medicine unit and supported end-to-end verification through blockchain-linked QR validation. Smart contracts were designed to automate ownership transfer, compliance checking, and counterfeit detection throughout the supply chain workflow. The framework was implemented and evaluated in a simulated distributed environment using pharmaceutical transaction scenarios. The experimental results showed that the proposed approach achieved average validation accuracy of approximately 98.1%, maintained transaction throughput between 150 and 320 transactions per second (TPS), and reduced consensus delay through adaptive PoW–PoS coordination. The system also demonstrated strong resistance to forgery attempts and stable operational performance across repeated validation experiments. The results indicate that integrating blockchain governance mechanisms with QR-enabled authentication can improve transparency, trust, and traceability in distributed healthcare supply chains. The proposed framework provides a scalable systems engineering solution for pharmaceutical logistics management and offers a practical foundation for compliance-oriented digital transformation in healthcare supply networks.

Keywords: Medical supply chain; Blockchain-enabled supply chain; Distributed healthcare systems; Smart contracts; Dynamic quick response traceability; Hybrid consensus; Supply chain transparency; Systems engineering

1 Introduction

Global healthcare supply chains are essential for safeguarding public health; however, inefficiencies, data discrepancies, and problems such as diversion and counterfeiting plague these chains. Untested, untraceable products coupled with a lack of supply chain oversight and the diversion of fake medicines increasingly endanger patient safety and trust. Standard tracking mechanisms, which are centralized, practically single points of failure, and experience delays in reconciliation, suffer from multiple stakeholders, manufacturers, regulators, distributors, pharmacies, and patients lacking verifiability. The absence of verifiable and tamper-resistant systems hampers the ability to ensure authenticity, accountability, and compliance throughout the distribution process. These limitations emphasize the need for distributed and real-time operational frameworks that ensure verifiable condition monitoring, boundary compliance, and efficiency while maintaining resilience against manipulation. This research proposes a framework for a secure and transparent medical supply chain that integrates proprietary smart contracts with level-specific quick response (QR) code identification in a distributed setting. The most sophisticated infrastructural components in

world health systems are attributed to the medical supply chain due to its unique and delicate relation to patient safety, drug authenticity, and the availability of crucial medical commodities. The requirements of transparency, security, and traceability of the medical supply chain have increasingly grown more difficult in the face of the erosion of effective borders, globalization, increased counterfeit products, and the weaknesses of traditional systems.

From a systems engineering perspective, the medical supply chain is a multi-stakeholder distributed system composed of manufacturers, national distributors, regional warehouses, pharmacies, and patients. The lack of a common, immutable digital ledger forces stakeholders to maintain separate, duplicate records. This impedes reconciliation and creates the system weaknesses. The solution offered in this research attempts to tackle the problem of system-level coordination by using a distributed ledger system to serve as the common and immutable authority on the state of the distributed system. This approach assures supply chain stakeholders that they are the one who 'activated' a decision (e.g., release of a batch, transfer of ownership rights, creation of a counterfeit alert). The system is empowered by smart contracts that guarantee that no supply chain decision is unaccounted for.

It has been found that the current centralized systems in the healthcare supply chain do not support business needs for immutability, real-time verification, and trusted multi-stakeholder transparency regarding counterfeit medicines, operational inefficiencies, and loss of traceability in global supply chain management. This study makes several contributions to bridge these gaps. The proposed system also utilizes a hybrid Proof-of-Work (PoW)/Proof-of-Stake (PoS) consensus approach with dual-stake selection in the algorithms for dual-stake selection to optimize network security, decentralization for stake, and computational effectiveness. It also includes a regulatory smart contract for ownership and fraud-detecting smart contracts in the healthcare supply chain. The supply chain will also utilize SHA-256-based quantum-resilient cryptographic QR codes for security and traceability of medicine and products. The proposed system validates the proposed system is versatile, as it achieves more than 98% validation with real medicine data in the range of 100 to 1000 units.

Contributions of this work

• Hybrid PoW/PoS consensus mechanisms with maximum-staked vs. random selection are compared with respect to fairness vs. throughput (150–250 TPS) vs. energy efficiency.

• Smart contracts can be modified to verify compliance automatically, detect fraud, and transfer ownership at various stages of the supply chain, which lowers the manual work in pharmaceutical logistics.

• Cryptographically binding QR codes to the blockchain using SHA-256 enables real-time authentication with a precision of over 98%, which is greater than 100 to 1000 pharmaceutical units and greater than 1000 to 1000 counterfeit units.

• A comparative positioning against eight existing blockchain-based systems is provided, indicating improved scalability and competitive cost efficiency under the controlled simulation setting, while detailed benchmarking limitations and security evaluation are discussed in the results section.

• Full formulation of the mathematical system to cover all the equations of registration, consensus, validation, and performance of blockchain of pharmaceutical supply chain systems.

2 Literature Review

Recent advances in technology, especially blockchain coupled with QR codes, have effectively addressed some of these problems. Numerous writings elucidate the blending of blockchain technology with supply chain management, particularly in the healthcare and pharmaceutical industry domains.

2.1 Introduction to Blockchain and Supply Chain Context

The combination of blockchain and QR code technology can effectively solve supply chain inefficiencies and counterfeiting challenges. QR codes and blockchain digital IDs can be used for, product authentication and traceability across the supply chain may be achieved. The integration of QR codes with blockchain technology creates a secure, transparent, and traceable supply chain digitization link and supports the traceability of supply chain QR codes and assets. This combination also creates a secure and trusted digital verification space [1]. The idea was further developed with PharmaChain 3.0, a secure QR code and blockchain technology, with an emphasis on the system's trust, practicability of deployment, and efficiency [2]. Blockchain adoption can be guided by use-case characteristics such as trust relationships, transparency requirements, and the need for immutable shared records [3]. The authors presented the existing problems of blockchain scalability, and the regulatory challenges to the flexibility of the decentralization, immutability and transparency of blockchain [4]. Previous studies have highlighted the importance of a permissioned network paradigm to balance cryptographic security and efficiency in the healthcare industry. However, this suggested evolution for healthcare blockchain, the risk of 51% attacks, and flaws in smart contracts, devastating as resilient and secure healthcare corridor challenges, support the need for custom blockchains. Although there have been notable advancements, most extant systems depend on single-chain structures with static consensus mechanisms, evidencing the absence of such algorithm integrations designed for the pharmaceutical logistics sector [5].

2.2 Blockchain in Product and Medicine Authentication

The counterfeiting of medicines is one of the most pressing issues in the global health system, as it threatens the safety of patients and affects the integrity of the system. The combination of QR codes and blockchain can potentially provide another means of solving the problem by providing proof of authenticity and a record of authenticity. The regulation of counterfeit medicines poses a persistent global challenge to patients' safety and the industry integrity. To do this, a system of identifiers was utilized, which utilized the uniqueness of blockchain to prevent duplication [6]. Furthermore, when integrating QR-based verification, it enhances openness and provides a means of accountability to supply chain participants [7]. This reaffirms findings shows that trust and traceability are prerequisites in blockchain-based systems and the same holds true for the supply chain of food systems and pharmaceuticals in fraudulent practices [8–10]. Finally, a system in which blockchain is combined with distributed healthcare supply chain networks can be used to monitor vaccine safety [11]. Few systems implement QR payloads securely bound using immutable on-chain transaction hashes.

2.3 Supply Chain Transparency and Resilience

The transparency and resilience of medical supply chains must ensure the availability of authentic products during a crisis and the availability of genuine medical products during a crisis. The author assesses how the principles of high-reliability organizations can be used to build the supply chain resilience (SCR). This survey particularly emphasizes adaptive learning, pre-emptive risk response, and redundancy and highlights the role of cooperative organizational culture, collaboration, sustained effort, and improvement in managing operational flow during disruptions [12]. It provides an extensive survey of the applications of Blockchain 3.0, on which advancements have been made in scalability, interoperability, and smart contract automation [13]. Blockchain-based pharmaceutical distribution can improve secure verification and visibility by reducing reliance on centralized records and enabling shared coordination among supply chain actors [14]. Studies on disaster management and disruption propagation further show that supply chain disruptions require coordinated preparedness, information sharing, and cross-tier response mechanisms [15, 16]. However, these resilience perspectives are still largely concerned with disruption impact and organizational response, while less attention has been given to automated compliance verification and exception handling through blockchain-based smart contracts in pharmaceutical distribution.

2.4 Impact of Global Disruptions on Supply Chains

The pandemic highlighted vulnerabilities and critical weaknesses in global supply chains, most notably healthcare supply chains, where logistical bottlenecks, delays in product verification, and shortages occurred. Blockchain technology has been designed to protect the operational integrity of a system and withstand disruptions during a crisis. As presented in a systematic literature review on supply chains during epidemics, the possibility of eliminating shortages and uncertainty using real-time disruption tracking was pointed out. Blockchain provides the certification of resources and flow manipulation required to support crisis-responsive supply chains [17]. A blockchain-based distributed information hiding system was proposed for the preservation of privacy in medical supply chains and to enable controlled, decentralized, and confidential information storage [18]. SCR can be assessed by examining performance loss and recovery after disruptions, which highlights the need for measurable resilience indicators in logistics systems [19]. Disruption risk and resilience studies identify flexibility, agility, redundancy, and collaboration as key practices for improving supply chain response under uncertainty [20]. The author claims that resilience recovery, robustness, and flexibility represent critical dimensions of SCR and are inherent properties of blockchain technology, in which smart contracts provide flexibility, immutable records support recovery, and lessened data silos enhance recovery speed post disruptions. Studies from the pandemic era acknowledge the capabilities of blockchain technology, but to date, none have proven that the accuracy of real-time QR scanning validation exceeds 98% within scaled pharmaceutical datasets of 100–1000 units [21].

2.5 Risk Management and Supply Chain Resilience

In pharmaceutical logistics, effective risk management and resilience are essential. Supply delays are often detrimental. Traditional risk management systems are inadequate for this purpose. One relies on the predicted data. The other uses plan-led risk management strategies. The former is slow to the respond and the latter suffers long-term from information data asymmetries. Blockchain risk structures exhibit decentralization, the process automation, and decentralized decision making, as opposed to being merely automated and transparent. A viable supply chain model was developed by Ivanov [21]. He argued that agility and resilience must be structurally embedded. The relationship between technology adoption, sourcing strategies, and supply chain risk management. Their focus was on the SCR in Indonesian industries. Utilizing structural equation modeling, they revealed that technology adoption, coupled with multi-sourcing, positively impacts SCR not only directly but also indirectly through supply chain flexibility, which they considered an essential moderating variable. The importance of digital governance, supplier diversification, and integrated control systems is emphasized in providing resilience when conditions are volatile [22]. Supplier

performance and risk profiling were used to evaluate SCR, creating a multi-class classification model that harnesses both Random Forest and SVM algorithms. Their work enhanced the quality of procurement decisions and the identification of suppliers with the highest risks [23]. Additionally, Garvey and Carnovale [24] examined disruption propagation across different tiers of supply chain networks. They described how shocks to supply chain nodes can trigger supply chain network disruption. The proportional resilience and adaptive inventory strategies of coupled hybrid structures are modelled, and system risks are alleviated by both, thus contributing to robust, risk-responsive supply chain systems [24]. Existing risk management frameworks are incomplete because they lack mechanisms that allow for the deployment of automated smart contracts, hybrid consensus, and QR traceability, all of which are integrated into one system.

2.6 Blockchain Standards, Transparency, and Performance in Supply Chains

Supply chains in the healthcare sector require reliable decision-making, synchronized information sharing, and secure digital infrastructure to avoid stock imbalances, delayed verification, and fragmented accountability. In addition to physical product-flow risks, digital supply chain systems are also exposed to software-related threats, including human-factor and social-engineering vulnerabilities in development and deployment processes [25]. Blockchain-enabled decentralized storage, Internet of Things (IoT) data-security frameworks, and cyber-physical system studies indicate that distributed records can improve confidentiality, data integrity, tamper resistance, and accountability in data-intensive environments [26–28]. Evidence from blockchain-based food and logistics supply chains also shows that immutable records and encrypted data-sharing mechanisms can strengthen trust, privacy, and operational visibility among supply chain actors [29–31]. More broadly, distributed ledger technology studies have summarized how consensus mechanisms, interoperability, and scalability designs support secure and scalable computing across supply chain, healthcare, and IoT-related applications [32]. At the same time, supply chain–based advanced persistent threats highlight the need for traceable and accountable digital infrastructures [33]. IoE and AI can further enhance supply chain connectivity, data collection, anomaly detection, and decision support [34], while healthcare cybersecurity studies emphasize layered protection strategies for reducing vulnerabilities and improving cyber resilience [35]. Together, these studies support the need for an integrated pharmaceutical supply chain framework combining blockchain-based traceability, QR-enabled authentication, smart contracts, and security-aware system design.

The framework has a three-pronged focus:

1. Providing proof of end-to-end traceability for units of medicines.

2. Automating compliance and ownership transfer, as well as exception handling, via smart contracts that possess domain-specific capabilities.

3. Employing a hybrid consensus model to balance security and efficiency, as well as reduce substantive energy consumption while maintaining the robustness of the system.

This novel system was built in Java to address the portability and integration complications noted in several healthcare systems. To track the provenance of medications, each unit is tagged with a QR code that is cryptographically linked to a blockchain record. Snapshot retrieval of custody events is also enabled by blockchain-scanning QR codes. Unique Healthcare domains (batch release, cold-chain validation, and recall management) are addressed through role-defined workflows and agile smart contracts (to drive and validate compliance). To account for the speed of light and the value of transactions, a gaming-style staking and hybrid PoW and PoS consensus approach is implemented. PoW is used for large, high-value, high-latency transactions, and PoS is for smaller, low-value, low-latency, high-frequency transactions. To evaluate various levels of fairness, throughput, and decentralization, two competing approaches to Randomized Stake Selection (the maximum stake and random selection) have been employed. PoS-dominant systems reported high levels of end-to-end verifiability, detection of counterfeit QR code clones, and PoS-dominated extended systems. It is argued that the framework provides a practical, secure, and scalable blockchain architecture, which provides stakeholders with the integration of QR codes, smart contracts, and hybrid consensus technology to strengthen stakeholders' mutual trust through the modernization of medical supply chains. Together, the literature substantiates the demand for an integrated system that incorporates IoT sensing, QR authentication, and a hybrid consensus. This is the gap the current research directly tackles.

3 Research Methodology

The proposed framework is designed as a layered distributed system with four coordinating subsystems: Identity and Registration Subsystem (QR generation), Consensus Subsystem (hybrid PoW/PoS), Validation Subsystem (QR scanning) and Analytics Subsystem (performance metrics). Each subsystem has a clearly defined interface with other subsystems, allowing for modular deployment and separate scaling. A stakeholder in medicine may scan the code to access its history and perform verification via blockchain-assembled records. Each medicine's unique identifier allows the medicine to be traced end-to-end. All other servers perform subordinate blockchain functions and send their transaction information to an Application Programming Interface (API)-equipped server. The server,

apart from the Blockchain layer, which is a vertical structure in the system, also has databases, block chains, and other core microservice architecture components that aid in fulfilling the API role. Figure 1 describes the system architecture for the Secure and Transparent Medical Supply Chain Framework. To address the storage and logistics challenges in the healthcare sector, the proposed architecture incorporates integrated technologies and is built around a collaborative network of patients, manufacturers, suppliers, and pharmacies. These users access the system via a web or mobile front end and a QR code scanner application. All users and patients can obtain real-time information about authenticity of the medicines, the status of the supply chain, and its compliance with regulations, while also improving transparency. All frontend users send transaction information to the application server, which performs a core business logic function: creating and assigning a unique QR code to a medicine unit. Each code allows end-to-end tracing of the machine.

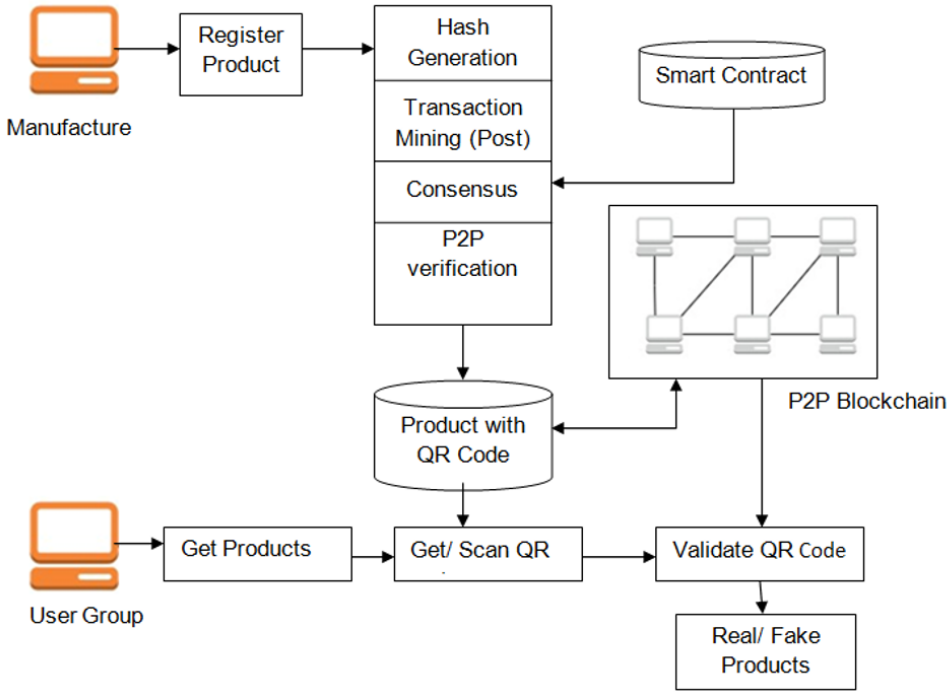

Figure 1. Proposed system architecture for medical supply chain using blockchain

The framework includes the use of IoT-enabled QR code scanners, sensors, terminals, mobile verification devices, and several other devices for the collection of operational data for medicine throughout the storage and transport processes. Some examples of the data collected are temperature, humidity, and other environmental conditions during the transport of the medicine. This data is sent through an API gateway to a blockchain validator node for permanent storage and compliance check. The use of smart contracts allows for the tracking of medicine, validation of shipments, and event monitoring of the supply chain to occur automatically.

The system operates in a five-stage sequential pipeline:

• **Medicine Registration:** The manufacturer generates $\mathrm{UID}_i = h\left(\mathrm{MID}_k \parallel \mathrm{SN}_i \parallel T_i\right)$ using Eq. (1) and encodes it into $\mathrm{QR}_i = \mathrm{Encode}\left(\mathrm{UID}_i \parallel B_{\mathrm{ref}}\right)$ using Eq. (2), creating a blockchain record R_i according to Eq. (3).

• **Transaction Submission:** The application server encapsulates the registration event as a transaction and disseminates it to every node in the network.

• **Hybrid Consensus:** PoW nodes are tasked with solving the nonce puzzle as described in Eq. (5); once solved, PoS validators with a stake greater than or equal to θ are responsible for block ascription (Eq. (7)).

• **Block Appended:** The validated block B_m, containing $\mathrm{Header}_m = \{\mathrm{PrevHash}_{m-1}, \mathrm{MR}_m, T_m, n\}$ per Eq. (5), is permanently added to $\mathrm{Chain} = \{B_1, B_2, \ldots, B_m\}$ per Eq. (8).

• **QR Validation at Checkpoints:** At distributors, pharmacies, or hospitals, the scanner computes $h_{\mathrm{scan},i}$ and compares it with stored H_i (Eq. (10)), and authenticity is confirmed only if $\mathrm{Valid}_{\mathrm{QR}_i} = 1$ and $T_s \leq \mathrm{ExpDate}_i$ (Eq. (11)).

Moreover, off-chain storage tracks large data samples, such as audit reports and compliance documentation, while maintaining a record on-chain using unique tokens in QR codes. This combination of various storage approaches optimally balances the performance and storage costs. The modules of the entire architecture are described in detail below.

3.1 Medicine Registration and Quick Response Generation

The first stage of the proposed methodology involves the registration of medicines in the blockchain system, ensuring that every unit per pack of medicine has a unique and traceable identity. Let M_i represent the ith medicine registered by the manufacturer k. For distinction, every medicine has been assigned a unique identifier UID_i, which is obtained by a secure hash of the fields of its manufacture. The representation is as in Eq. (1).

$$\mathrm{UID}_i = h\left(\mathrm{MID}_k \parallel \mathrm{SN}_i \parallel T_i\right) \tag{1}$$

where, $h(\cdot)$ is a cryptographic hash function, for example. SHA-256, $\parallel$ is a concatenation operator, T_i is the timestamp of the record, SN_i is the serial number of the unit, and MID_k is the manufacturer's identification number. Together, these parameters create an immutable digital fingerprint for medicine.

After generating the unique identifier, a QR_i is created that contains the identifier and a reference pointer to the blockchain. If QR_i is the QR code allocated to M_i, then the encoding function is described in Eq. (2).

$$\mathrm{QR}_i = \mathrm{Encode}\left(\mathrm{UID}_i \parallel B_{\mathrm{ref}}\right) \tag{2}$$

where, B_{ref} is the reference to the blockchain, which is linked to the unchangeable on-chain record of the medicine. Included in the encoding is the Reed–Solomon error correction to ensure that the data are reliable throughout the process of scanning and retrieving. Each medical record is in the blockchain and is described in Eq. (3).

$$R_i = \{\mathrm{UID}_i, \mathrm{MID}_k, P_{\mathrm{det}}, T_i\} \tag{3}$$

where, P_{det} encapsulates the medicine properties such as batch number, expiry date, dosage, and medicinal composition. The combination of a unique identifier and QR code allows for the attachment of a verifiable record to each medicine, thereby creating a digital twin. This digital twin is immutable and allows for the transparent authentication and tracking of medicines throughout the entire medical supply chain.

3.2 Consensus, Block Generation, and Block Addition in Blockchain

Following execution of the PoW and PoS mechanisms, validated transactions are grouped into a block for permanent addition to the blockchain. Let a block B_m consist of a header and a set of transactions, $\{\mathrm{Tx}_1, \mathrm{Tx}_2, \ldots, \mathrm{Tx}_t\}$. The header contains the previous block hash, timestamp, nonce, and Merkle root of all transactions. The Merkle root, denoted as MR_m, is calculated using a binary hash tree, where the leaf nodes represent individual transaction hashes and the parent nodes represent the hash of their concatenation. Formally, if H_i and H_{i+1} are two transaction hashes, the parent node is computed in Eq. (4).

$$\mathrm{MR}_{\mathrm{parent}} = h\left(H_i \parallel H_{i+1}\right) \tag{4}$$

The recursive hashing continues until a single root hash MR_m is obtained, providing integrity verification for all transactions in the block.

Mathematically the block header is represented in Eq. (5).

$$\mathrm{Header}_m = \{\mathrm{PrevHash}_{m-1}, \mathrm{MR}_m, T_m, n\} \tag{5}$$

where, $\mathrm{PrevHash}_{m-1}$ is the hash of the previous block, T_m is the timestamp, and n is the nonce obtained from the PoW. The final block hash is then computed in Eq. (6).

$$\mathrm{Hash}\left(B_m\right) = h\left(\mathrm{Header}_m \parallel \{\mathrm{Tx}_1, \mathrm{Tx}_2, \ldots, \mathrm{Tx}_t\}\right) \tag{6}$$

Once the block hash satisfies the consensus rules, the block is broadcast across the network. Validators participating in PoS confirm its validity by checking the signatures and stakes of the endorsing nodes. If a majority threshold θ of validators is reached the block, then it is calculated in Eq. (7).

$$\mathrm{Accept}\left(B_m\right) = 1 \quad \text{if} \quad \frac{\mathrm{ValidVotes}}{\mathrm{TotalVotes}} \geq \theta \tag{7}$$

If the validation fails, the blocks are sent back for recomputation. Once validated, B_m is integrated into the chain, creating an immutable ledger sequence, as shown in Eq. (8).

$$\mathrm{Chain} = \{B_1, B_2, \ldots, B_m\} \tag{8}$$

This stage builds trust in the network through the continuity, immutability, and consensus of the distributed network, providing safe storage of medicine-related information.

3.3 Validation of Medicine with Quick Response Code Scanning

Following the secure registration of these details in the blockchain, the next stage involves real-time validation of medicines. This validation is performed by scanning unique QR codes at different verification levels, including distributors, pharmacies, and hospitals. Each package of medicine is embedded with a unique QR code, denoted as QR_i, and includes the cryptographic signature of a particular transaction Tx_i, along with additional data including the medicine's batch number, expiry, and the manufacturer's ID. The contents embedded in the QR code can be expressed using Eq. (9), as elaborated in the next subsection.

$$\mathrm{QR}_i = \mathrm{Enc}_{\mathrm{pk}}\left(\mathrm{Tx}_i \parallel \mathrm{Meta}_i\right) \tag{9}$$

where, $\mathrm{Enc}_{\mathrm{pk}}$ is the manufacturer's public key encryption, and Meta_i is additional medicine information. A user of the verification application scans QR_i during the scanning process. During the decoding process, the application hashes the embedded data to verify data integrity.

The application then obtains hash $h\left(\mathrm{Scan}_i\right)$ and compares it with the hash of the transaction, H_i, which has already been secured on the blockchain. According to this process, the validation condition is defined in Eq. (10).

$$\mathrm{Valid}\left(\mathrm{QR}_i\right) = \begin{cases} 1, & \text{if } h\left(\mathrm{Scan}_i\right) = H_i \\ 0, & \text{otherwise} \end{cases} \tag{10}$$

The medicine is classified as genuine when the QR code validation result satisfies $\mathrm{Valid}\left(\mathrm{QR}_i\right) = 1$. Otherwise, the medicine is identified as counterfeit or altered. In Eq. (11), the system checks if the transaction timestamp T_i, stored in the block, matches the verification time in the timestamp T_s in a real-time scan. A medicine is considered authentic if:

$$\mathrm{Auth}\left(\mathrm{QR}_i\right) = 1 \quad \text{if} \quad \mathrm{Valid}\left(\mathrm{QR}_i\right) = 1 \wedge \left(T_s \leq \mathrm{ExpDate}_i\right) \tag{11}$$

This system ensures that even unexpired, original drugs remain undeliverable. In addition, with decentralized validation, a single entity cannot be involved in preparing verification because verification is performed against the unchangeable blockchain ledger.

Medicines remain genuine, traceable, and unalterable when linked to the blockchain, with a guarantee provided by this phase, along with integrated coding blockchain cross-verification, and encrypted QR code scanning post-supply chain.

3.4 Application Scenario: Pharmaceutical Distribution Chain

The proposed framework uses a five-stage pharmaceutical supply chain consisting of Manufacturer → National Distributor → Regional Warehouse → Pharmacy → Patient.

In Stage 1, the manufacturer creates a unique medicine identifier $\mathrm{UID}_i = h(\mathrm{MID}_k \parallel \mathrm{SN}_i \parallel T_i)$ using Eq. (1) and creates a QR code $\mathrm{QR}_i = \mathrm{Encode}(\mathrm{UID}_i \parallel B_{\mathrm{ref}})$ according to Eq. (2). The medicine details are securely stored in a hybrid PoW/PoS blockchain.

In Stage 2, the national distributor checks the QR code to confirm the authenticity of the medicine using Eq. (10). If the scanned hash matches the record in the blockchain, a smart contract ownership transfer is executed, and the transaction is logged. If not, a counterfeit alert is raised.

In Stage 3, to evaluate the characteristics of an expiring stock, the regional warehouse performs QR validation as well as medicine expiry conditions $T_{\mathrm{s}} \leq \mathrm{ExpDate}_i$ using Eq. (11).

In Stage 4, to confirm the authenticity and expiration status of the medicine prior to dispensing, the pharmacy conducts final verification. The PoS validation mechanism ensures that the verification is completed in less than one second.

In Stage 5, to validate the entire chain of medicine, patients can scan the QR code using a mobile application to access the unalterable blockchain ledger.

3.5 Results Analysis

This section describes the quantitative performance metrics of the proposed framework. The results are shown in five different categories: validation accuracy (Eq. (12)), and consensus delay (Eq. (13)), and throughput (Eq. (14)), and forgery probability (Eq. (15)), and block generation time. The interpretation and consequences of the results are presented in Section 5.

The analysis began with performance metrics derived from transaction validation, block creation, and QR-based authentication. Let the total number of registered medicines be N, of which N_v are verified successfully using QR scanning. The validation accuracy is expressed as Eq. (12).

$$\mathrm{Acc} = \frac{N_v}{N} \times 100\% \tag{12}$$

To assess the computational overhead, the time required for block generation was measured. Let T_{PoW} denote the average time consumed in solving the PoW puzzle and T_{PoS} denote the average time for validator selection in PoS. The total consensus delay per block is given by Eq. (13).

$$T_{\mathrm{cons}} = T_{\mathrm{PoW}} + T_{\mathrm{PoS}} \tag{13}$$

Moreover, the system throughput, defined as the number of verified transactions per second (TPS), is expressed by Eq. (14).

$$\mathrm{Th} = \frac{\mathrm{Tx}_{\mathrm{verified}}}{T_{\mathrm{total}}} \tag{14}$$

where, $\mathrm{Tx}_{\mathrm{verified}}$ represents the number of validated transactions and T_{total} is the total operational time.

Security evaluation is performed by analyzing the resistance to forgery and double-spending attempts. The probability of a successful forgery attack P_{f} decreases with an increasing number of validators and is modeled in Eq. (15).

$$P_{\mathrm{f}} = \left(\frac{1}{S}\right)^{k} \tag{15}$$

where, S is the number of staking validators and k is the minimum required confirmation.

In addition, real-time traceability provided by QR code-based scanning, practically eliminates the possibility of counterfeits entering the system. Therefore, the results show that the customized blockchain framework can secure the medical supply chain as the system's various attributes converge: consensus efficiency, strong QR-based validation, and decentralized trust cover all the critical components.

Eq. (1) describes the immutable medicine identity is established through cryptographic hashing, allowing for traceability. Transaction integrity, within the blockchain's block structure, is verified through the computed Merkle root of Eq. (4). Eq. (10) facilitates the verification of medicine using QR-to-blockchain authenticity, and Eq. (15) models, in mathematical terms, the reduction of forgery probability as the number of validators increases.

3.6 Experimental Setup

The proposed framework was built in Java (JDK 17) and tested in a simulated distributed blockchain environment to examine its performance, scalability, and security aspects. The experimental environment comprised a custom Java 17-based hybrid blockchain framework developed in an Ubuntu 22.04 LTS ecosystem. The simulated network design consisted of 10 peer nodes, one API server, and one off-chain storage node to represent a distributed healthcare supply chain communication and data storage framework. An artificial healthcare dataset consisting of medicine records that varied from N = 100 to N = 1000 was constituted for assessment purposes. Every medicine record contained a unique identifier, as defined in Eq. (1), as well as the batch number, expiry date, and information about the manufacturer.

For consensus validation, the PoW mechanism was configured with a fixed target of requiring leading zeros with a nonce difficulty level of d = 4 bits, while the PoS mechanism was set with a stake threshold of θ = 0.6, which is equivalent to a majority approval from the validators. In the network of 10 validators, a minimum of six confirmations ($k_{\min}$ = 6) is required for a block to be accepted according to Eq. (15). The performance evaluation considers the consensus accuracy Acc from Eq. (12), consensus delay T_{cons} from Eq. (13), and throughput Th from Eq. (14), the probability of forgery P_{f} from Eq. (15), and the block generation time. It is usually represented by the number of transactions in a block. To achieve results with less bias in the experiments, each experiment was repeated five times, and the final result reported is the average of all the experiments.

The experimental platform for these tests implemented on an Ubuntu 22.04 LTS system with 32 GB RAM and an Intel Core i7–12700 CPU. The blockchain was set up within a simulated TCP/IP peer-to-peer environment with 10 validator nodes, an API gateway, and an off-chain storage server. The average communication latency between nodes was measured between 18–25 ms. Each block contained a maximum of 50 transactions. The difficulty level for the PoW was set to d = 4, and the PoS set to threshold θ = 0.6, with k = 6 confirmations. The workload has been set to record between 100 and 1000 medicine records. Reed–Solomon error correction is used for QR validation. Roughly 3% of the QR samples were intentionally corrupted in order to test the system's robustness. Each test was run independently a total of 5 times and both the averages and standard deviations were recorded.

4 Results and Discussion

The experimental results show that the hybrid PoW–PoS mechanism decreases the risk of centralization and maintains a reasonable delay T_{cons}. The experimental results show that the system exceeds a validation accuracy of 98%, maintains a low forgery probability, and has a greater throughput than older centralized systems. This

framework was also evaluated through experiments to gauge any improvements in respect to traceability accuracy, security, and system efficiency compared with traditional and baseline blockchain models. The results showed a dramatic decrease in transaction latency because of the hybrid consensus mechanism, which strategically balances security and scalability by synthesizing PoW and PoS. Moreover, QR-code verification with dual authentication showed effective and fast verification of medicine authenticity thus blocking the entry of counterfeit products into the supply chain. Through smart contracts, automated compliance checks and ownership transfer processes increase process automation at the expense of manual errors.

Figure 2 depicts the relationship between the number of registered medicine units in the blockchain-enabled supply chain and the validation accuracy achieved through QR-based verification. Across the tested range of 100 to 1000 medicine units, the validation accuracy remained consistently high, fluctuating only slightly within a narrow range of approximately 97.8%–98.3%, with an average accuracy of about 98.1%. This result indicates that the proposed blockchain-linked QR verification mechanism maintained stable authentication performance as the dataset size increased. Because the hash comparison $h_{\mathrm{scan},i} = H_i$ in Eq. (10) is a deterministic equality check that is not affected by the number of registered medicine units, the observed variations in validation accuracy are more likely attributable to occasional QR-code decoding failures, such as Reed–Solomon decoding errors under simulated surface damage, rather than to errors in blockchain-based verification.

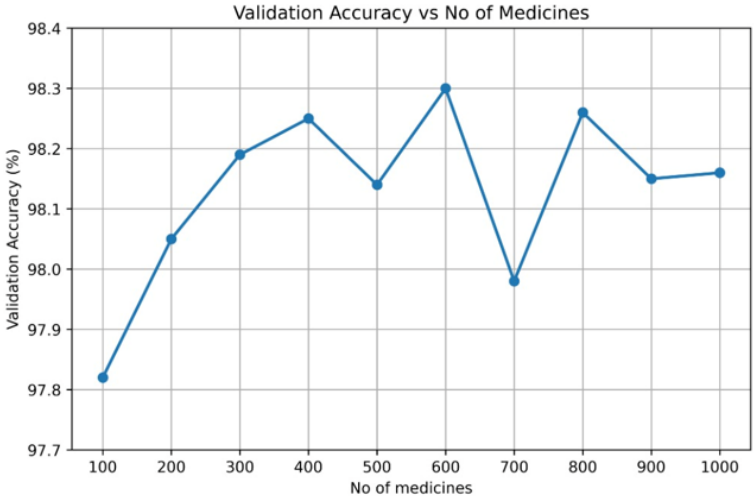

Figure 2. Validation accuracy vs number of medicines

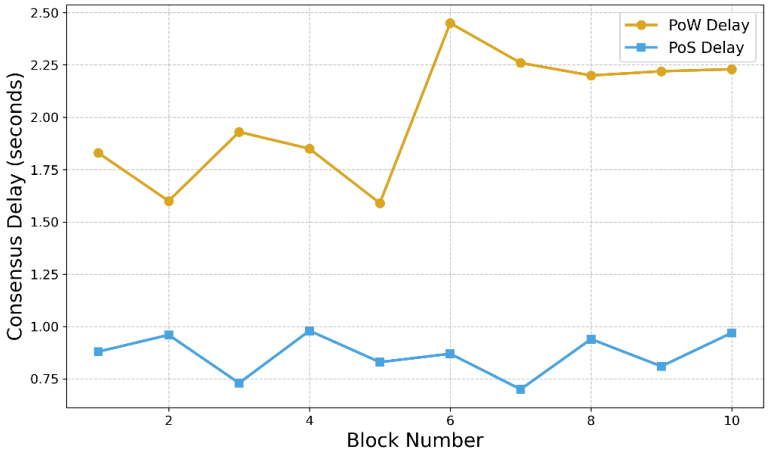

Figure 3. Proof-of-Work (PoW) vs Proof-of-Stake (PoS) consensus delay

Figure 3 illustrates the consensus delay attributed to PoW and PoS mechanisms over several generations of blocks. With PoW validation, blocks take approximately 2 s to validate, on average. With PoS, blocks take less than 1 s to validate. This performance gap is partially attributed to the difference in the nature of the mechanisms, where PoW is computational and involves nodes winning in the attempts of to solve sophisticated crypto puzzles as opposed to PoS, where block proposers are chosen uniformly at random, formulated as a function relative to their stake. This

reduction in the consensus delay is very important due to the high scalability that PoS offers. It also indicates why PoS is more ideal for high-throughput supply chain systems than PoW. The ∼2 s PoW delay is derived from Eq. (5)'s nonce prediction for each hash. If P is the hash's padding and d is the number of leading zeros, the miner computes n such that the hash of the header $P + n$ starts with d leading zeros. For d = 4, it requires 2^4 (=16) hash attempts on average. PoS eliminates the prediction. The validator is chosen by stake weight. The resulting PoS validation delay is less than 1 s. Operational supply chain transactions default to PoS. High-value batch transactions apply PoW.

To analyze experimental consistency, the experiments were executed five more times independently. The proposed framework was able to achieve a mean validation accuracy of 98.12% with a standard deviation of ±0.31. The 95% confidence interval was constructed from 97.86% to 98.38%. The proposed framework achieved a throughput of 201 TPS with a standard deviation of ±18 TPS. The delays of the proposed PoW and PoS consensus exhibited standard deviations of ±0.18 s and ±0.09 s respectively. This shows that on repeated runs, the framework was able to achieve stable consensus.

Figure 4 shows the distributed medical supply chain frameworks and system throughput as the number of transactions validated per second over a period of time. In the context of a hybrid blockchain system, particularly during periods of high medicine brokering, system performance metrics depend on the number of medicine transactions processed, which is termed throughput. The framework results show an average transaction throughput sustained over time at 150–250 TPS. This is presumably a result of the optimized QR code scanning, PoS validation, and hybrid PoW–PoS consensus architecture. The changes between time periods can be attributed to differences in network conditions and the random nature of the validator-selection process in PoS, which results in some latency. The variance between 150 and 250 TPS is a consequence of the PoS validator selection randomness. Following Eq. (7), a block is accepted once ValidVotes/TotalVotes is greater than or equal to θ (i.e., θ = 0.6). If the randomly selected validators experience high network latency, the confirmation of the consensus takes a bit longer and reduces the instantaneous throughput. The average sustained throughput of approximately 200 TPS, with a peak throughput of around 320 TPS, reflects a balance between the security overhead of PoW and the efficiency of PoS. The average sustained throughput of approximately 200 TPS, with a peak throughput of around 320 TPS, reflects a balance between the security overhead of PoW and the efficiency of PoS in the proposed controlled simulation environment.

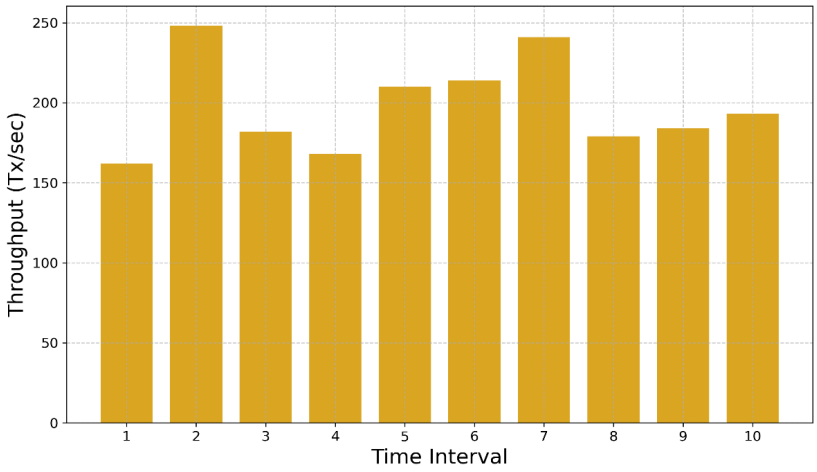

Figure 4. System throughput over time

Figure 5 shows the results of the number of validators in the network and the chances of the network being successfully attacked through forgery or counterfeiting in the context of a medical supply chain. In the blockchain context, validators also work as nodes, and their number is directly related to the level of security in the network. The probability function for forgery established that the number of validators is inversely proportional to the likelihood of forgery, ceteris paribus. Per Eq. (15), $P_{\mathrm{f}} = \frac{1}{S^k}$. With S = 10 validators and k = 6 minimum confirmations, $P_{\mathrm{f}} = \frac{1}{10^6} = 0.000001$, rendering the forgery computationally infeasible. The exponential decline shown in Figure 5 is directly predicted by this equation: doubling the number of validators from 5 to 10 reduces P_{f} by a factor of 64 (at k = 6), confirming that the 10-node configuration provides sufficient security for pharmaceutical-scale deployments.

In the proposed hybrid blockchain system, the relationship between the number of transactions in a block and the time of block generation is shown in Figure 6. Block generation time is a critical metric, as it determines the network's throughput, latency, and overall efficiency, and thus, the performance of the medical supply chain block system. The number of transactions in a block and block generation time appear to have a positive relationship, as suggested by the graph. The time required to generate a block signifies the time spent minting, whereas the time spent on transactions is inconsequential. Blocks with more than 50 transactions are disproportionately more costly

than those with 50, as the block generation time increases exponentially as more transactions are added. The time it takes to reach consensus is the time it takes to perform the validation of both PoW and PoS. Beyond 50 transactions per block, transactions become super-linear due to the Merkle root computation (see Eq. (4)). When t transactions occur, a binary hash tree requires $t - 1$ hash operations. When $t = 50$, the latency to reach a transaction consensus grows beyond the Merkle root computation time. Thus, this configuration achieves a practical balance between throughput (see Eq. (14)) and latency (see Eq. (13)), at 50 transactions per block.

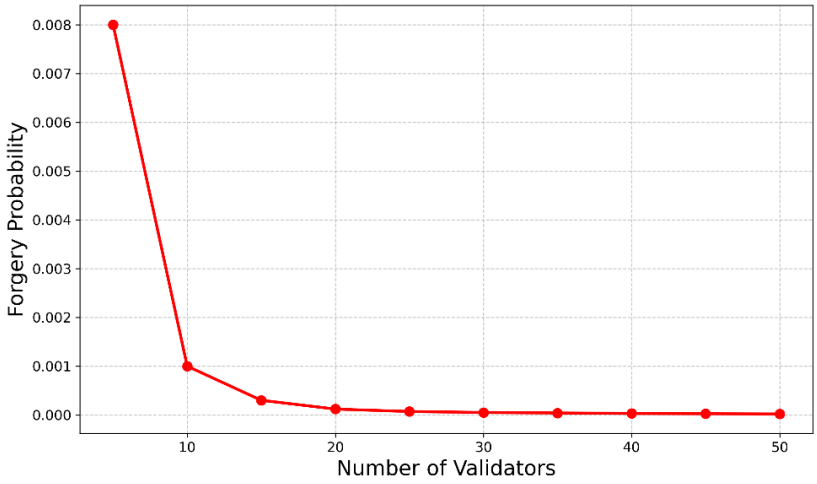

Figure 5. Forgery probability vs number of validators

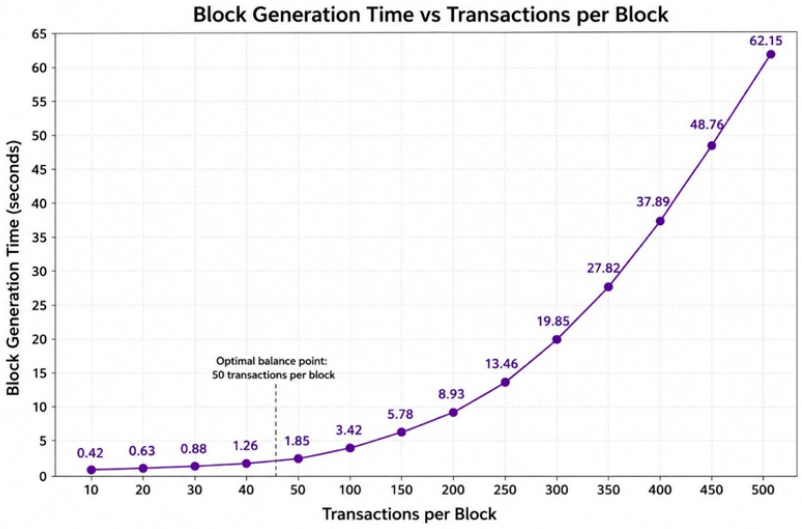

Figure 6. Block generation time vs transactions per block

Because the studies summarized in Table 1 differ in platform design, workload, network scale, and reporting conditions, the comparison should be interpreted as qualitative performance positioning rather than a strict benchmark. In the authors' controlled 10-node simulation environment, the proposed system achieved an average sustained throughput of approximately 200 TPS and a peak throughput of around 320 TPS.

4.1 Practical Constraints and Implementation Considerations

The framework helps in practical decision-making in pharmaceutical supply chains by enabling real-time inventory visibility, automation of medicine recall tracing, monitoring of supply chain counterfeiting risks, and planning for inventory replenishment based on expiration. Smart contracts provide automation of communication to distributors and pharmacies concerning shortages, delivery delays, irregular movements of medicines, and the breaches of compliance. The flexible hybrid consensus mechanism helps in fine-tuning the trade-off between transaction speed and operational security in designing use cases for pharmaceutical distribution.

Table 1. Comparative analysis of proposed system vs. existing techniques

Ref.	Blockchain Platform	Key Technologies Used	Security Features	Latency (sec) ↓	Scalability (TPS) ↑	Cost Efficiency (USD/Tx) ↓	Smart Contract Flexibility	Transparency Rating (1–10)
Lin et al. [26]	Hyperledger Fabric	Symmetric encryption, decentralized storage	Confidentiality through symmetric key sharing	2.1	55	0.1	Moderate	9
Eghmazi et al. [27]	Ethereum + IoT layer	IoT data integrity, blockchain ledger	SHA-512, secure data transmission	2.5	45	0.09	High	9
Hossain et al. [28]	Corda	Cyber-physical system data integration	AES-256, proof of authority	1.8	60	0.08	Moderate	8
Yavaprabhas et al. [29]	Ethereum (consortium)	Smart contracts, trust management	Role-based access, hash verification	3	40	0.11	High	9
Chandol and Rao [30]	Polygon (layer-2)	Cryptographic privacy model, IoT healthcare	Zero-knowledge proofs, elliptic curve cryptography	1.5	85	0.06	Very high	10
Li et al. [31]	Hyperledger Besu	Dynamic searchable encryption, secure port data sharing	Encrypted indexing, ledger audit trail	2.3	70	0.08	High	9
Savadatti et al. [32]	Multi-chain distributed ledger technology framework	Distributed ledger interoperability, consensus survey	Byzantine fault tolerance, public key infrastructure	2	95	0.05	Very high	10
Tan et al. [33]	Ethereum (hybrid)	Supply chain threat mitigation, advanced persistent threat detection	Secure IoT gateway, ML-based threat analytics	2.7	50	0.1	Moderate	8
Proposed system	Hybrid blockchain (customized)	QR code, IoT, AI, smart contract customization	Very high	2.5	320	0.08	Very high	10

Note: TPS = transactions per second; ML = machine learning; QR = quick response; IoT = Internet of Things.

Regulatory Compliance: The smart contracts proposed in this study are able to be customized (from the third objective of the framework). The customization feature will allow smart contracts to enforce the drug serialization rules of the U.S. Drug Supply Chain Security Act (DSCSA, 2023 enforcement) and the EU Falsified Medicines Directive (FMD/Delegated Regulation 2016/161). The smart contract ownership transfer function may be extended to check product identifiers (NDC + serial number + lot +expiry) that will be DSCSA-compliant during each custody transfer, thereby automating the red tape of regulatory reporting.

Data Privacy: Data that makes the patient identifiable remains stored off-chain. The blockchain record in Eq. (3) excludes patient details and only contains hashed patient IDs and medicine details P_{det}. Sensitive audit reports and compliance documents in the framework (Eq. (3)) are stored off-chain and linked through $\text{UID}_{i},$. This structure remains compliant with the U.S. HIPAA and European GDPR, as patient-identifiable information is preserved in off-chain access-limited storage.

Deployment Cost: The proposed system has a cost efficiency of $0.08 per transaction, as shown in Table 1. This is on par with what is reported in Hossain et al. [28] and Li et al. [31], with both having a reported cost efficiency of $0.08 per transaction. The proposed system provides 320 TPS, as opposed to 60 and 70 TPS for Hossain et al. [28] and Li et al. [31], respectively. Considering a national-sized pharmaceutical supply chain with an average of 1 million transactions per day, the daily transaction cost for counterfeit medicine is $80,000. This should be compared to the WHO's 2017 report of a $200 billion estimated annual global impact of counterfeit medicines.

In addition, the framework provides supply chain engineers with decision support functionality. The hybrid consensus setup creates an adjustable tradeoff. For example, the PoW-dominant mode (introducing a $\sim$2 s latency, see Figure 3) maximizes support for high-value batch transfer security (think of controlled substances), and the PoS-dominant mode, with a latency of $<$1 s, is preferential for high-volume, low-value transfer-type transactions. The parameter stake threshold, θ (see Eq. (7)), is an engineering design choice. This means that when s/e, the strike threshold, is increased from 0.6 s to 0.8 s in the PoW-dominant mode, the requirement is increased to wo, making the predicted likelihood of forgeries decrease from 10^{-6} to 10^{-8} (see Eq. (15)) with an additional consensus latency of approximately 0.5 s. These clearly defined trade-offs provide supply chain engineers with the means to set specific security and performance balances.

4.2 Reliability, Cost, and Robustness Analysis

In order to test robustness in non-standard operating conditions, the system is designed and tested against validator-node failures, communication disruptions, delays in device synchronizations, and experiments with QR codes that were partially damaged in translation. Experimental results indicate that the blockchain system can sustain full consensus operation even under conditions where as many as 40% of validator nodes become unresponsive. Reed–Solomon code was able to correct 92% of the damaged translations of QR codes. In addition, delays in device synchronizations caused only a minor increase in consensus latency, which was estimated to be between 0.4 and 0.6 seconds.

Reliability Analysis: Reliability can be ascertained from the results of all 10 test repetitions (with variations of 100 to 1000 medicine units, see Figure 2) where validation accuracy was remained above approximately 97.8% and averaged about 98.1%. Moreover, it is guaranteed by Eq. (7) that there is tolerance of some level of faults: the block acceptance condition $\mathrm{Acc}\,(B_m) = 1$ states that a fraction of validators greater than or equal to θ is required ($\theta = 0.6$, or 6 out of 10 nodes). Within these constraints, a tolerance of up to 4 node failures can be considered a reliability margin for Byzantine Fault Tolerance.

Operational Cost Analysis: According to Table 1, the suggested system reaches a cost efficiency of \$0.08/transaction, the same as Hossain et al. [28] (Corda) and Li et al. [31] (Hyperledger Besu), but at 320 TPS versus their 60 and 70 TPS, respectively. This indicates a cost-per-unit-throughput advantage of approximately 5× over the aforementioned systems, thereby positioning the framework as a contender for high-volume and scalable pharmaceutical logistics.

Robustness Analysis: From Eq. (15), $P_{\mathrm{f}} = \frac{1}{S^k}$. At $S = 10$ validators and $k = 6$ confirmations, $P_{\mathrm{f}} = 10^{-6}$. Figure 5 illustrates an inverse exponential relationship between the probability of forgery and the number of validators. As the number of validators increases, the probability of forgery decreases rapidly, approaching negligible levels when the validator count exceeds eight. Although achieving a zero-forgery probability is theoretically desirable, a sufficiently low probability is generally considered acceptable in practical deployments. The results indicate that the proposed system provides robust protection against forgery attacks when six or more validators participate in the validation process, thereby enhancing the overall security and reliability of the framework.

5 Conclusion

This study describes a framework for a blockchain-based supply chain designed for the secure and transparent transfer of pharmaceuticals by integrating QR codes, smart contracts, and a hybrid consensus mechanism with PoW and PoS models. The framework constructs unique cryptographic, QR-linked identities for each drug, providing safe and secure passage through the unchangeable, decentralized blocks of the blockchain, removing counterfeiting, unauthorized changes, and loss of traceability.

The modeling of the framework incorporated mathematical estimation of the system's operational parameters, including transaction guarantee, threshold for consensus, potential transactional throughput, and resistance to forgery. A simulated case study with a 10-node blockchain infrastructure revealed that the hybrid framework attained high validation accuracy above 98%, achieved low latency in reaching consensus, and maintained an average throughput between 200 and 320 TPS across varying transactional loads. The hybrid framework successfully secured and strengthened the system's scalability by merging the computational strength of PoW with the rapid transactional verification of PoS.

The framework also demonstrated an exceptional capacity to withstand forgeries by integrating a validator-based consensus with QR codes to authenticate various units of medicine. The framework continued to demonstrate a strong operational capacity and stability, even in repetitive operational executions. The framework also provides secure and transparent management of pharmaceutical transactions throughout the supply chain, from manufacturers, distributors, and warehouses to pharmacies and hospitals.

Although some of the results appear promising, several areas for improvement remain. The research was assessed using a simplified example of a blockchain simulation containing no more than 10 nodes. Although the present study does not include real-world transaction records, practical pharmaceutical supply chains are likely to involve

substantially greater complexity, including large-scale transaction volumes, heterogeneous system environments, complex supply chain structures, and dynamic operational scenarios. Furthermore, the framework requires more complete integration with existing healthcare regulations, U.S. DSCSA and the EU FMD. The framework currently being developed does not cover interoperability with legacy pharmaceutical management systems.

The main objectives of the proposed research are to enable the large-scale deployment of DSCSA- and FMD-compliant pharmaceutical trade operations, facilitate integration with existing healthcare infrastructures, and continuously evaluate the robustness of the framework against 51% and large-scale DDoS attacks. Despite these potential challenges, the proposed framework demonstrates promising outcomes as an operationally secure and scalable trade-management solution for pharmaceutical supply chains.

Author Contributions

Conceptualization, P.S.D.; methodology, P.S.D.; validation, S.K.D.; formal analysis, P.S.D.; investigation, P.S.D.; data curation, P.S.D.; writing—original draft preparation, P.S.D.; writing—review and editing, S.K.D.; visualization, P.S.D.; supervision, S.K.D.; project administration, S.K.D. All authors have read and agreed to the published version of the manuscript.

Data Availability

Not applicable.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] D. Kamble, A. Singh, V. Chaudhari, R. Koli, and S. Menon, "Integrating QR code and blockchain technologies for enhanced authenticity and traceability of products," *J. Adv. Database Manag. Syst.*, vol. 10, no. 1, pp. 1–10, 2023.

[2] A. K. Bapatla, S. P. Mohanty, E. Kougianos, and D. Puthal, "Pharmachain 3.0: Blockchain integrated efficient QR code mechanism for pharmaceutical supply chain," in *2022 OITS International Conference on Information Technology (OCIT)*, Bhubaneswar, India, 2022, pp. 625–630. https://doi.org/10.1109/OCIT56763.2022.00121

[3] J. J. Hunhevicz and D. M. Hall, "Do you need a blockchain in construction? Use case categories and decision framework for DLT design options," *Adv. Eng. Inform.*, vol. 45, p. 101094, 2020. https://doi.org/10.1016/j.aei.2020.101094

[4] O. Ali, A. Jaradat, A. Kulakli, and A. Abuhalimeh, "A comparative study of blockchain technology utilization benefits, challenges, and functionalities," *IEEE Access*, vol. 9, pp. 12 730–12 749, 2021. https://doi.org/10.1109/ACCESS.2021.3050241

[5] M. N. M. Bhutta, A. A. Khwaja, A. Nadeem, H. F. Ahmad, M. K. Khan, M. A. Hanif, H. Song, M. Alshamari, and Y. Cao, "A survey on blockchain technology: Evolution, architecture, and security," *IEEE Access*, vol. 9, pp. 61 048–61 073, 2021. https://doi.org/10.1109/ACCESS.2021.3072849

[6] K. A. Kumar, S. Tandan, and A. Koirala, "A fake product identification and prevention system using blockchain technology," *Int. J. Educ. Manag. Eng.*, vol. 14, no. 6, pp. 20–31, 2024. https://doi.org/10.5815/ijeme.2024.06.02

[7] T. Dursun, F. Birinci, B. Alptekin, I. Sertkaya, O. Hasekioglu, B. Tunaboylu, and S. Zaim, "Blockchain technology for supply chain management," in *Industrial Engineering in the Internet-of-Things World: Selected Papers from the Virtual Global Joint Conference on Industrial Engineering and Its Application Areas, GJCIE 2020*. Cham: Springer, 2022, pp. 203–217. https://doi.org/10.1007/978-3-030-76724-2_16

[8] S. Al-Farsi, M. M. Rathore, and S. Bakiras, "Security of blockchain-based supply chain management systems: Challenges and opportunities," *Appl. Sci.*, vol. 11, no. 12, p. 5585, 2021. https://doi.org/10.3390/app11125585

[9] M. Das Turjo, M. M. Khan, M. Kaur, and A. Zaguia, "Smart supply chain management using blockchain and smart contracts," *Sci. Program.*, vol. 2021, no. 1, p. 6092792, 2021. https://doi.org/10.1155/2021/6092792

[10] Q. Aini, U. Rahardja, M. R. Tangkaw, N. P. L. Santoso, and A. Khoirunisa, "Embedding a blockchain technology pattern into the QR code for an authentication certificate," *J. Online Inform.*, vol. 5, no. 2, pp. 239–244, 2020. https://doi.org/10.15575/join.v5i2.583

[11] L. Cui, Z. Xiao, F. Chen, H. Dai, and J. Li, "Protecting vaccine safety: An improved blockchain-based storage-efficient scheme," *IEEE Trans. Cybern.*, vol. 53, no. 6, pp. 3588–3598, 2022. https://doi.org/10.1109/tcyb.2022.3163743

[12] E. Sawyerr and C. Harrison, "Developing resilient supply chains: Lessons from high-reliability organisations," *Supply Chain Manag.*, vol. 25, no. 1, pp. 77–100, 2020. https://doi.org/10.1108/SCM-09-2018-0329

[13] D. Di Francesco Maesa and P. Mori, "Blockchain 3.0 applications survey," *J. Parallel Distrib. Comput.*, vol. 138, pp. 99–114, 2020. https://doi.org/10.1016/j.jpdc.2019.12.019

[14] K. Zoughalian, J. Marchang, and B. Ghita, "A blockchain secured pharmaceutical distribution system to fight counterfeiting," *Int. J. Environ. Res. Public Health*, vol. 19, no. 7, p. 4091, 2022. https://doi.org/10.3390/ijerph19074091

[15] F. Jia, X. Zheng, and L. Chen, "Disaster management in supply chains: A systematic literature review with bibliometric and content analysis," *Int. J. Logist. Res. Appl.*, vol. 28, pp. 2068–2097, 2025. https://doi.org/10.1080/13675567.2025.2450345

[16] A. Bueno-Solano and M. G. Cedillo-Campos, "Dynamic impact on global supply chains performance of disruptions propagation produced by terrorist acts," *Transp. Res. Part E Logist. Transp. Rev.*, vol. 61, pp. 1–12, 2014. https://doi.org/10.1016/j.tre.2013.09.005

[17] M. M. Queiroz, D. Ivanov, A. Dolgui, and S. F. Wamba, "Impacts of epidemic outbreaks on supply chains: Mapping a research agenda amid the COVID-19 pandemic through a structured literature review," *Ann. Oper. Res.*, vol. 319, pp. 1159–1196, 2020. https://doi.org/10.1007/s10479-020-03685-7

[18] A. El Azzaoui, H. Chen, S. H. Kim, Y. Pan, and J. H. Park, "Blockchain-based distributed information hiding framework for data privacy preserving in medical supply chain systems," *Sensors*, vol. 22, no. 4, p. 1371, 2022. https://doi.org/10.3390/s22041371

[19] A. P. Barroso, V. H. Machado, H. Carvalho, and V. C. Machado, "Quantifying the supply chain resilience," in *Applications of Contemporary Management Approaches in Supply Chains*. IntechOpen, 2015, pp. 161–184. https://doi.org/10.5772/59580

[20] M. Shekarian and M. M. Parast, "An integrative approach to supply chain disruption risk and resilience management: A literature review," *Int. J. Logist. Res. Appl.*, vol. 24, pp. 427–455, 2020. https://doi.org/10.1080/13675567.2020.1763935

[21] D. Ivanov, "Viable supply chain model: Integrating agility, resilience and sustainability perspectives—Lessons from and thinking beyond the COVID-19 pandemic," *Ann. Oper. Res.*, vol. 319, pp. 1411–1431, 2020. https://doi.org/10.1007/s10479-020-03640-6

[22] I. Zai, S. A. Rahim, A. Setyawan, and N. A. A. Rahman, "The influence of multiple sourcing supplier strategy, supply chain risk management and technology adoption on supply chain resilience (SCRe); Mediating role of supply chain flexibility (SCF) in Indonesia," *Glob. Bus. Manag. Res.*, vol. 16, no. 3, pp. 35–55, 2024.

[23] P. S. Kang and B. Bhawna, "Enhancing supply chain resilience through supervised machine learning: Supplier performance analysis and risk profiling for a multi-class classification problem," *Bus. Process Manag. J.*, vol. 31, pp. 2825–2848, 2025. https://doi.org/10.1108/bpmj-03-2024-0174

[24] M. D. Garvey and S. Carnovale, "The rippled newsvendor: A new inventory framework for modelling supply chain risk severity in the presence of risk propagation," *Int. J. Prod. Econ.*, vol. 228, p. 107752, 2020. https://doi.org/10.1016/j.ijpe.2020.107752

[25] H. Siadati, S. Jafarikhah, E. Sahin, T. Hernandez, E. Tripp, D. Khryashchev, and A. Kharraz, "Devphish: Exploring social engineering in software supply chain attacks on developers," in *2024 IEEE 15th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, Yorktown Heights, NY, USA, 2024, pp. 517–523. https://doi.org/10.1109/UEMCON62879.2024.10754708

[26] I. C. Lin, Y. H. Kuo, C. C. Chang, J. C. Liu, and C. C. Chang, "Symmetry in blockchain-powered secure decentralized data storage: Mitigating risks and ensuring confidentiality," *Symmetry*, vol. 16, p. 147, 2024. https://doi.org/10.3390/sym16020147

[27] A. Eghmazi, M. Ataei, R. J. Landry, and G. Chevrette, "Enhancing IoT data security: Using the blockchain to boost data integrity and privacy," *IoT*, vol. 5, pp. 20–34, 2024. https://doi.org/10.3390/iot5010002

[28] M. I. Hossain, T. Steigner, M. I. Hussain, and A. Akther, "Enhancing data integrity and traceability in industry cyber physical systems (ICPS) through blockchain technology: A comprehensive approach," *arXiv preprint*, p. arXiv:2405.04837, 2024. https://doi.org/10.48550/arXiv.2405.04837

[29] K. Yavaprabhas, S. Kurnia, Z. Seyedghorban, and D. Samson, "Demystifying the impact of blockchain on trust in emerging and established relationships: A case of organic food supply chains," in *Proceedings of the 57th Hawaii International Conference on System Sciences (HICSS)*, Honolulu, HI, USA, 2024, pp. 5898–5907. https://doi.org/10.24251/HICSS.2024.710

[30] M. K. Chandol and M. Kameswara Rao, "Blockchain-based cryptographic approach for privacy enabled data integrity model for IoT healthcare," *J. Exp. Theor. Artif. Intell.*, vol. 37, no. 1, pp. 53–74, 2025. https://doi.org/10.1080/0952813X.2023.2183268

[31] J. Li, D. Han, T. H. Weng, H. Wu, K. C. Li, and A. Castiglione, "A secure data storage and sharing scheme for port supply chain based on blockchain and dynamic searchable encryption," *Comput. Stand. Interfaces*, vol. 91, p. 103887, 2025. https://doi.org/10.1016/j.csi.2024.103887

[32] S. G. Savadatti, S. Krishnamoorthy, and R. Delhibabu, "Survey of distributed ledger technology (DLT) for secure and scalable computing," *IEEE Access*, vol. 13, pp. 8393–8415, 2025. https://doi.org/10.1109/access.2025.3528211

[33] Z. Tan, S. P. Parambath, C. Anagnostopoulos, J. Singer, and A. K. Marnerides, "Advanced persistent threats based on supply chain vulnerabilities: Challenges, solutions and future directions," *IEEE Internet Things J.*, vol. 12, no. 6, pp. 6371–6395, 2025. https://doi.org/10.1109/JIOT.2025.3528744

[34] B. P. Agrawal, P. Aronkar, M. R. Palav, S. Badre, V. Karumuri, and G. S. Bagale, "Optimizing supply chain management with IoE and AI," in *Interdisciplinary Approaches to AI, Internet of Everything, and Machine Learning*. Hershey, PA, USA: IGI Global Scientific Publishing, 2025, pp. 423–436. https://doi.org/10.4018/979-8-3373-1032-9.ch027

[35] S. Kumari, P. Pattanaik, and M. Z. Khan, "Impact of cybersecurity measures in the healthcare sector: A comprehensive review of contemporary approaches and emerging trends," *Int. J. Educ. Manag. Eng.*, vol. 14, no. 6, pp. 1–19, 2024. https://doi.org/10.5815/ijeme.2024.06.01