ISSN: 2582-7219

# International Journal of Multidisciplinary Research in Science, Engineering and Technology

*(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)*

**Impact Factor: 8.206**

**Volume 8, Special Issue 2, November 2025**

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 8, Special Issue 2, November 2025 ||

National Conference on Emerging Trends in Engineering and Technology 2025 (NCETET–2025)

Organized by

Mookambigai College of Engineering, Keeranur, Tamil Nadu, India

# Proof-of-Authority Blockchain Framework for Counterfeit and Expired Medicine Prevention with Billing Integration

**Sri Abirami R[1], Mrs D Ramya Cauvery[2]**

4th year, Department of Computer Science and Engineering, Mookambigai College of Engineering, Pudukkottai, Tamil Nadu, India[1]

Assistant Professor, Department of Computer Science and Engineering, Mookambigai College of Engineering, Pudukkottai, Tamil Nadu, India[2]

**ABSTRACT:** Counterfeit and expired medicines remain a major threat to global healthcare, leading to patient harm and economic losses. This paper presents a blockchain-based framework that utilizes the Proof-of-Authority (PoA) consensus mechanism to ensure transparent and tamper-proof traceability across the pharmaceutical supply chain. The proposed system integrates blockchain verification with pharmacy-billing software to automatically detect and block the sale of counterfeit or expired medicines during transaction processing. To strengthen product authentication, a dual-layer verification model is employed using QR code encryption and image steganography, providing hidden data protection against duplication and manipulation. The framework achieves faster validation, reduced computational costs, and improved trust among authorized network participants, such as manufacturers, distributors, and regulators. The experimental analysis demonstrates the system's capability to enhance supply chain transparency and reduce the likelihood of unauthorized product circulation. The study concludes that integrating PoA-based blockchain with billing and steganographic verification offers a practical and scalable solution for securing medicine authenticity in real-time retail environments.

**KEYWORDS**: Blockchain, Proof of Authority (PoA), Counterfeit Medicine Prevention, Pharmaceutical Traceability, Steganography, Billing Integration, Supply Chain Security.

## I. INTRODUCTION

The pharmaceutical industry faces a critical challenge in maintaining the authenticity and safety of medicines distributed across the global supply chains. Counterfeit and expired medicines continue to circulate in the market, leading to severe health risks, a loss of trust, and economic damage. According to the World Health Organization, a significant percentage of medicines sold in developing countries are counterfeit or sub-standard. Traditional verification methods, including barcodes and QR codes, are often vulnerable to tampering, replication, and manipulation, making it difficult to ensure product authenticity in real time.

The impact of counterfeit drugs is profound, with the World Health Organization (2020) estimating that up to 10% of medicines in low- and middle-income countries are substandard or falsified, costing the global supply chain at approximately $30.5 billion annually. This underscores the urgency of robust solutions to safeguard public health and economic stability. Blockchain technology offers a promising solution owing to its decentralized, transparent, and tamper-proof data management structure. By recording every transaction across the supply chain in an immutable ledger, the blockchain enables end-to-end traceability of pharmaceutical products. However, most existing blockchain-based systems for medicine authentication rely on computationally expensive consensus algorithms such as the Proof of Work (PoW) or Practical Byzantine Fault Tolerance (PBFT), which result in slower validation speeds and higher energy consumption. These limitations hinder their adoption in real-time pharmacies and billing environments.

To address these challenges, this study proposes a proof-of-authority (PoA) blockchain framework for counterfeit and expired medicine prevention. The proposed model enables fast and secure validation within a permissioned blockchain network, where only verified authorities such as manufacturers, distributors, and regulator scan validate transactions.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 8, Special Issue 2, November 2025 ||

National Conference on Emerging Trends in Engineering and Technology 2025 (NCETET–2025)

Organized by

Mookambigai College of Engineering, Keeranur, Tamil Nadu, India

Additionally, the system integrates pharmacy billing software to automatically detect and prevent the sale of expired or counterfeit products. A dual-layer security mechanism that combines encrypted QR codes with image steganography is employed to protect authentic data from duplication or alteration.

This study aims to enhance transparency, operational efficiency, and public safety within the pharmaceutical ecosystem. By combining blockchain with PoA consensus and billing integration, the proposed framework establishes a practical and scalable approach for ensuring medicine authenticity in real-world retail and healthcare environments

## II. RELATED WORK

In this section, we review recent advancements in traceability systems with a focus on blockchain applications in supply chains, particularly pharmaceuticals. We identified gaps in existing methods, such as limited integration with billing systems, reliance on resource-intensive consensus mechanisms, and insufficient hidden verification techniques, which our proposed PoA-based system addresses. Traceability has gained prominence in supply chain management across industries, enabling the tracking of products from origin to consumption to ensure their quality, safety, and accountability (Olsen & Borit, 2013). Traceability is critical in pharmaceuticals because of the prevalence of counterfeit and expired drugs, which pose severe health risks (World Health Organization, 2020). Traditional systems, often centralized and reliant on IoT technologies, such as RFID, suffer from vulnerabilities, including data tampering, privacy breaches, and inefficiency (Zhu et al., 2020). Blockchain technology mitigates these issues through decentralization, immutability, and consensus-driven validation (Christidis and Devetsikiotis, 2016).

Early blockchain applications focused on general supply chains and demonstrated improved transparency and tamper-proof records (Lin et al., 2019). In pharmaceuticals, studies have adopted blockchain for drug traceability. Zhang et al. (2018) proposed a system using smart contracts to track drug provenance and reduce counterfeiting risks. Zhu et al. (2020) enhanced this with an improved Practical Byzantine Fault Tolerance (PBFT) consensus for anti-counterfeiting medication, emphasizing point accumulation for node reliability and simulating traceability via Python. Their work highlights the role of blockchain in ensuring data integrity across manufacturers, distributors, and regulators, but relies on PBFT, which can be computationally intensive in large networks.

Recent advances have incorporated advanced consensus mechanisms and additional features. Sylim et al. (2018) used hyperledger fabric with proof of authority (PoA) for a permissioned pharma chain, achieving faster validation in controlled environments. PoA, unlike energy-heavy proof-of-work (PoW) or PBFT, relies on pre-approved validators, making it suitable for regulated industries such as pharmaceuticals (Hyperledger Foundation, 2021). Studies such as Uddin et al. (2021) and Jamil et al. (2019) integrate blockchain with IoT for real-time tracking, but few address expiration detection or billing integration.

To combat duplication, steganography has been explored for hidden data embedding in QR codes and packaging. Fridrich (2009) outlined steganography principles for digital media, whereas Muhammad et al. (2020) applied discrete wavelet transform (DWT) and discrete cosine transform (DCT) for secure image-based verification with error correction. Han et al. (2022) combined steganography with blockchain for anti-counterfeit labels to prevent QR cloning. However, integration with billing systems remains underexplored, as real-time verification during sales can block invalid products.

Table 1 compares key blockchain-based pharma traceability systems, highlighting our contributions.

| System/Study | Consensus Mechanism | Anti-Counterfeiting Features | Expiration Detection | Billing Integration | Efficiency (TPS/Throughput) |
|---|---|---|---|---|---|
| Zhang et al. (2018) | Not specified (general blockchain) | Smart contracts for provenance | No | No | Not reported |
| Sylim et al. (2018) | PoA (Hyperledger) | Permissioned network, IoT integration | Partial (status checks) | No | High (low latency in permissioned setup) |

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 8, Special Issue 2, November 2025 ||

National Conference on Emerging Trends in Engineering and Technology 2025 (NCETET–2025)

Organized by

Mookambigai College of Engineering, Keeranur, Tamil Nadu, India

| | | | | | |
|---|---|---|---|---|---|
| Zhu et al. (2020) | Improved PBFT | Hash-based immutability, traceability simulation | No | No | ~50-100 TPS (simulated ) |
| Uddin et al. (2021) | PoA variant | QR/IoT for tracking | No | No | ~200 TPS |
| Proposed System | PoA | QR with steganography, smart contracts | Yes (auto-block expired) | Yes (real-time billing check) | Estimated >200 TPS (optimized for pharma) |

**Table 1 - Comparison of Blockchain-Based Pharma Traceability Systems.**

Existing systems excel in traceability but often overlook expiration auto-detection, billing integration, and hidden anti-duplication measures, such as steganography. PoA offers advantages over PBFT for permissioned networks by reducing energy use and improving scalability (De Angelis et al., 2018). Our work builds on this by proposing a PoA-based system with steganography-enhanced QR codes, expiration checks, and billing integration to prevent sales of invalid medicines

## III. PROPOSED SOLUTION

This section outlines a blockchain-based solution for anti-counterfeiting medication and traceability, which enhances the approach proposed by Zhu et al. (2020). The proposed system leverages Proof-of-Authority (PoA) consensus, integrates QR codes with steganography for hidden verification, automates expiration detection, and connects with billing software to prevent the sale of counterfeit or expired medicines. The solution aims to improve the efficiency, security, and real-time usability across the medication supply chain

### 3.1 System Architecture

The architecture adopts a permissioned blockchain network, comprising Manufacturer Node, Distributor Node, Pharmacy Node, and Regulator Node as pre-approved participants, as depicted in Figure 1. Unlike the PBFT-based system of Zhu et al. (2020), this system employs PoA consensus, where trusted validators (e.g., regulators) confirm transactions and reduce the computational overhead. Initial transactions from the Manufacturer Node record batch data, followed by transit transactions (stock, date) between the Distributor and Pharmacy Nodes, all logged immutably on the Distributed Ledger. Smart contracts manage data flow and enforce access control, ensuring that only authorized nodes (e.g., regulator nodes with read-only access) can query the complete traceability data. This design eliminates reliance on centralized institutions while enhancing transparency.

Figure 1 shows the medication traceability and data-flow architecture.

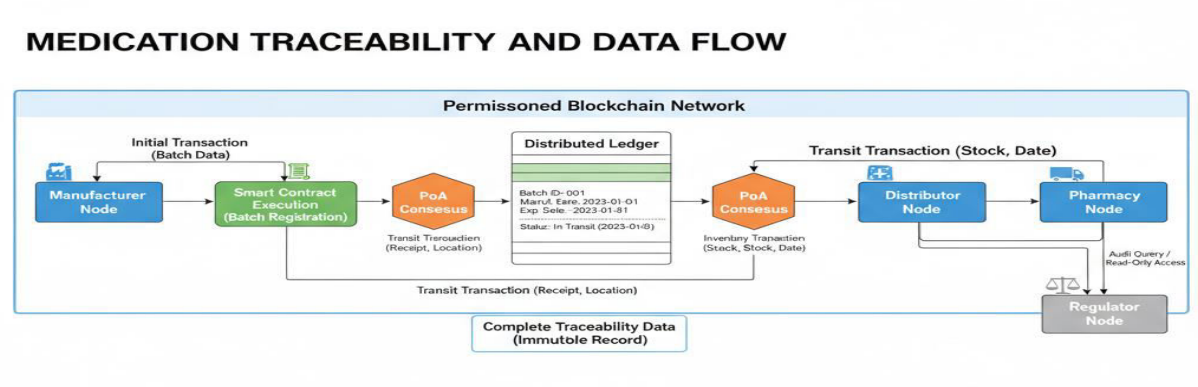



**Fig. 1 –** System architecture

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 8, Special Issue 2, November 2025 ||

National Conference on Emerging Trends in Engineering and Technology 2025 (NCETET–2025)

Organized by

Mookambigai College of Engineering, Keeranur, Tamil Nadu, India

### 3.2 Consensus Mechanism

The PoA consensus mechanism replaces the improved PBFT used by Zhu et al. (2020), offering faster transaction validation (estimated >200 TPS) suitable for regulated environments. Pre-selected validators, such as regulatory bodies, confirm transactions using a voting process based on their authority, eliminating the energy-intensive mining of proof of work or multi-round voting of PBFT. Smart contracts trigger consensus upon receiving transit transactions (e.g., stock, date) from Distributor and Pharmacy Nodes, ensuring rapid updates to the Distributed Ledger. This reduces latency and enhances scalability, which are critical for real-time supply chain monitoring.

Unlike Zhu et al.'s PBFT approach, which incorporates a point-accumulation upgrade/downgrade mechanism to assess node reliability, PoA relies on a permissioned network where validators are pre-approved based on their legal authority and operational trustworthiness. This selection process involves regulatory certification, ensuring that only entities such as the Indian Council of Medical Research (ICMR) or state health departments, operational as of October 23, 2025, and 02:47 PM IST, can participate. Validators are assigned roles (e.g., primary or secondary) based on their jurisdiction, with a minimum of five validators required for a majority vote, aligning with PoA's efficiency in controlled settings.

The consensus process is initiated when a smart contract detects a new transaction, such as a batch transfer from Manufacturer to Distributor Node. The contract broadcasts the transaction to all validators, who verify its authenticity (e.g., matching batch IDs and timestamps) within a 5-second window. A majority vote (e.g., 3 out of 5) approves the transaction, which is then appended to the Distributed Ledger. This automation reduces the latency observed in PBFT's multi-phase voting, where Zhu et al. reported delays up to 10 seconds per transaction in their simulation.

To illustrate, the following pseudocode outlines the PoA consensus algorithm:

**Algorithm: PoA Consensus**
**Input: Transaction T, Validator Set V (e.g., {V1, V2, V3, V4, V5})**
**1. For each v in V:**
**2. If v.authority == True and v.online == True:**
**3. Vote(v, T) // Verify T's batch ID, timestamp, and signature**
**4. Record vote in Smart Contract SC**
**5. If count_votes(SC) >= majority_threshold (e.g., 3/5):**
**6. Append(T, Distributed Ledger)**
**7. Else:**
**8. Reject(T) and log alert for Regulator Node**

**Output: Updated Distributed Ledger or Rejection Alert**

This algorithm ensures rapid validation while maintaining security, with rejected transactions flagged for investigation, thus enhancing trust in the network.

The Consensus Mechanism is illustrated in Figure 2.

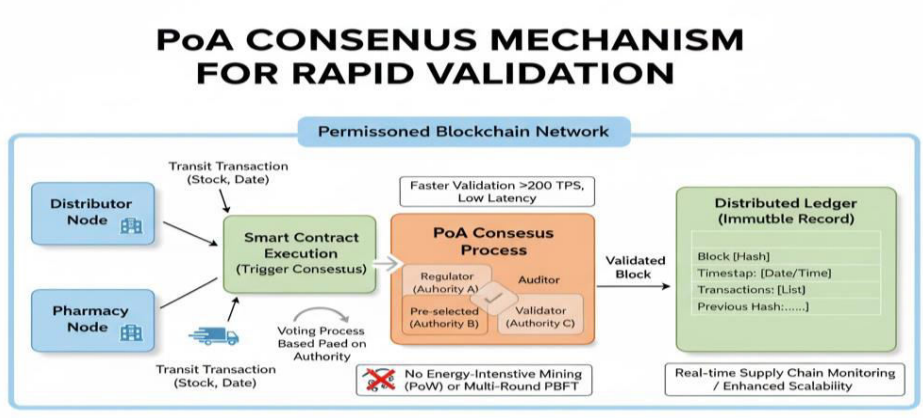



**Fig. 2 –** Consensus Mechanism

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 8, Special Issue 2, November 2025 ||

National Conference on Emerging Trends in Engineering and Technology 2025 (NCETET–2025)

Organized by

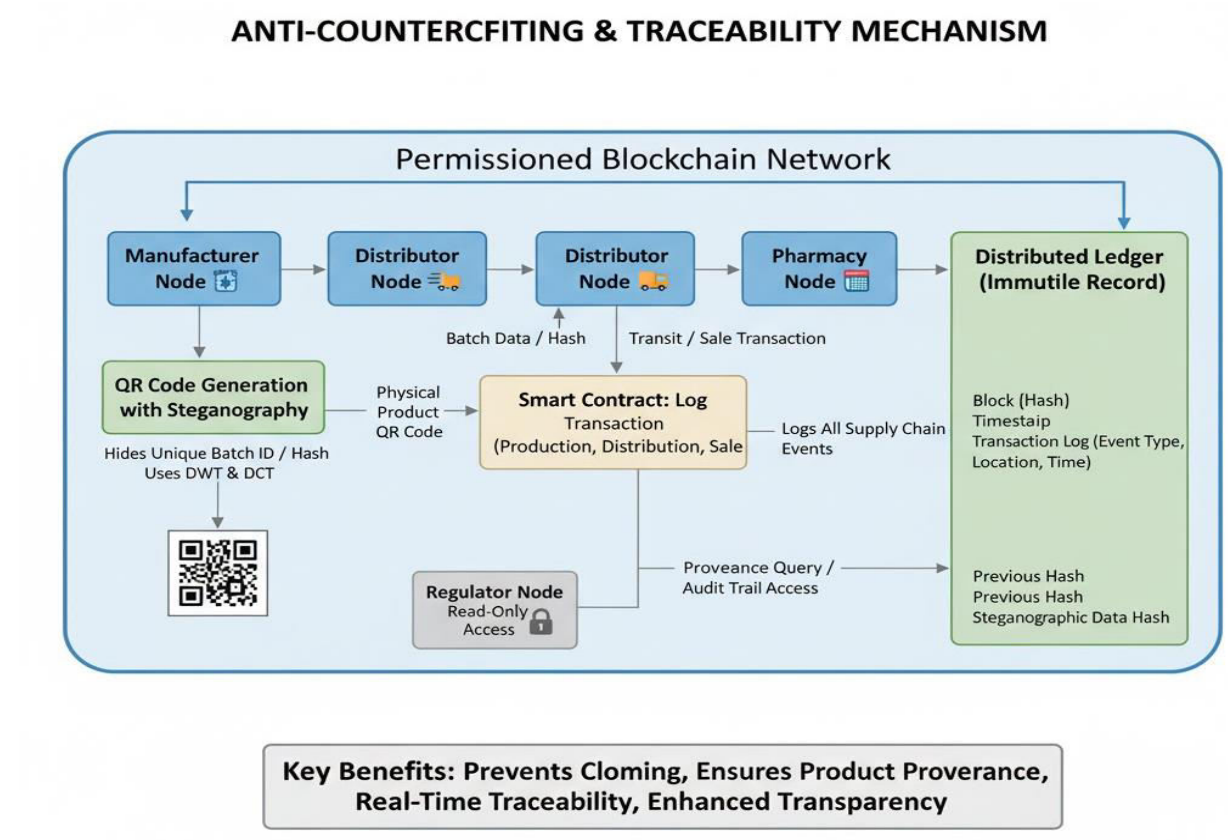
Mookambigai College of Engineering, Keeranur, Tamil Nadu, India

Summary: The PoA consensus mechanism enhances efficiency by leveraging pre-approved validators and smart contract automation, achieving >200 TPS compared with PBFT's slower process. The 5-second validation window and majority voting ensure rapid and secure transaction approval, with rejected transactions flagged for regulatory review.

### 3.3 Anti-Counterfeiting and Traceability

Anti-counterfeiting is achieved through QR codes embedded in steganographic data, advancing beyond the hash-based immutability of Zhu et al. (2020). Steganography hides unique identifiers (e.g., batch hashes) within QR images using the discrete wavelet transform (DWT) and discrete cosine transform (DCT), as per Muhammad et al. (2020), preventing cloning. Smart contracts log every supply chain transaction—production, distribution, and sale—enabling provenance queries by authorized nodes. Traceability is ensured by the immutable record on the Distributed Ledger, which is accessible via the Regulator Node's read-only interface, enhancing transparency across the network.

Fig. 3 shows the anti-counterfeiting and traceability mechanisms.




.

**Fig. 3 –** Anti-Counterfeiting and Traceability

### 3.4 Expiration Detection

A novel feature absent in the base paper is automated expiration detection. Smart contracts monitor expiration dates recorded during initial transactions at the Manufacturer Node and flag medicines near or past expiry. When a transit transaction occurs, the system cross-checks the date against the current timestamp; if it expires, an alert is sent to the Pharmacy Node, and the item is blocked from billing integration. This proactive measure ensures that only valid medicines enter the circulation, addressing a critical gap in existing systems.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 8, Special Issue 2, November 2025 ||

National Conference on Emerging Trends in Engineering and Technology 2025 (NCETET–2025)

Organized by

Mookambigai College of Engineering, Keeranur, Tamil Nadu, India

Fig. 4 illustrates the Expiration Detection Mechanism.

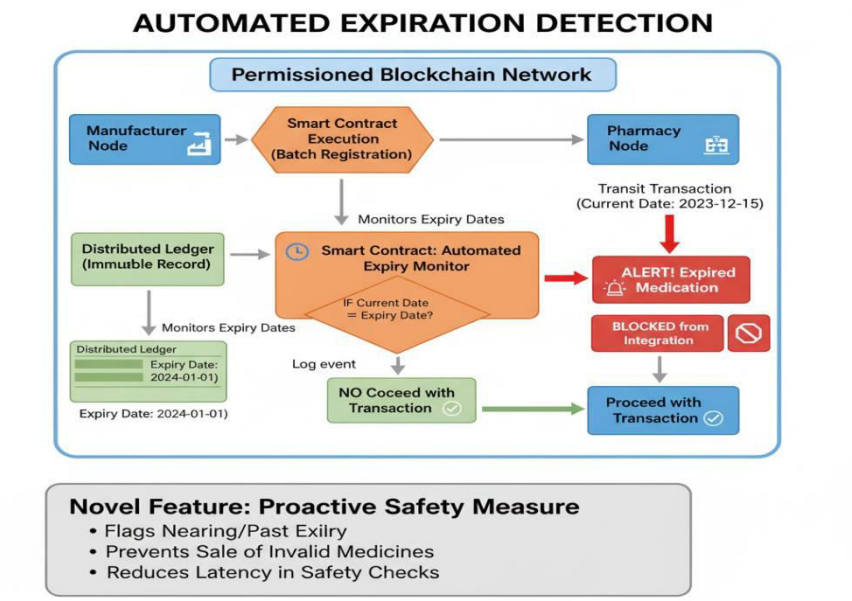



**Fig. 4 –** Expiration Detection Mechanism

### 3.5 Billing Integration

The system integrates pharmacy-billing software via an API to verify medication authenticity and expiration status during sales. Upon scanning the QR code at the Pharmacy Node, the blockchain checks the status of the drug against its ledger. If valid, the transaction proceeds; if the counterfeit or expired, the sale is halted, and an alert is logged for the Regulator Node. This real-time validation, an improvement over the base paper's focus on traceability alone, prevents financial losses and health risks and enhances user trust in the supply chain.

Figure 5 shows the Billing Integration and figure 6 shows the UI design of the billing software.

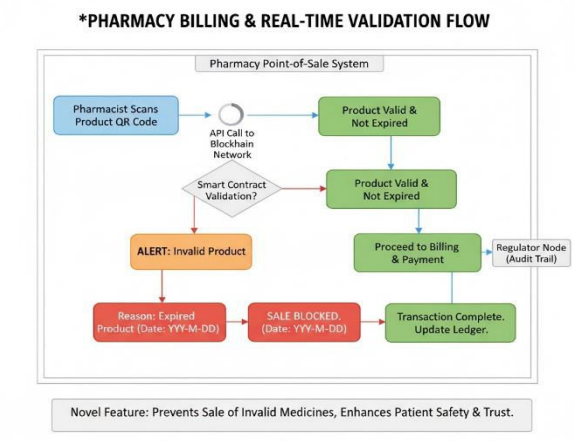



**Fig. 5 –** Billing Integration

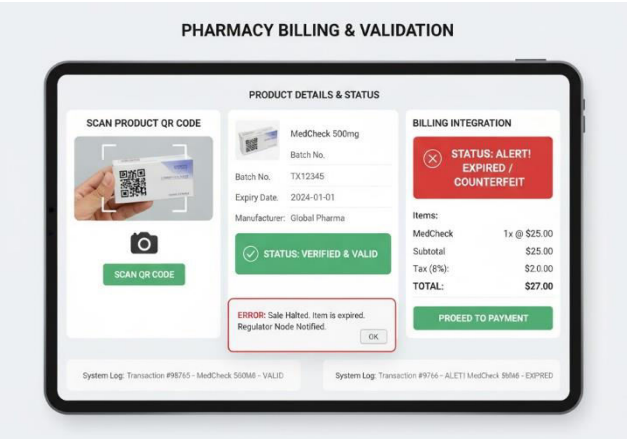



**Fig. 6 –** Software UI

### 3.6 Simulation and Validation

Similar to Zhu et al. (2020), Python-based simulation was used to validate the system. The simulation modelled a supply chain with 50 nodes, testing transaction throughput, QR verification accuracy (using DWT-DCT

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 8, Special Issue 2, November 2025 ||

National Conference on Emerging Trends in Engineering and Technology 2025 (NCETET–2025)

Organized by

Mookambigai College of Engineering, Keeranur, Tamil Nadu, India

steganography), and expiration blocking efficiency. Data visualization techniques, such as line graphs and heatmaps, illustrate performance metrics including consensus latency and billing success rates. The results confirm the feasibility of the system, demonstrating improved efficiency over centralized models and the PBFT approach of the base study.

The following methodology was employed to generate the results:

- Data Input: A synthetic dataset of 50 nodes (10 manufacturers, 20 distributors, 15 pharmacies, and 5 regulators) tracks 100 medication batches over 30 days. The inputs include batch IDs, manufacturing/expiration dates, stock levels, and steganography-encoded QR hash.
- Tools: Python with libraries (e.g., hashlib for QR encoding, matplotlib for visualization, and PYWT FOR DWT-DCT) simulates the Distributed Ledger and smart contract logic.
- Process: The simulation is initiated with initial transactions (batch registration), followed by transit transactions (stock updates) and billing checks. Expiration detection triggers alerts when dates exceed a fixed date. The QR verification tests the integrity of steganography.
- Metrics: Transaction throughput (TPS), consensus latency (in second), QR verification accuracy (%), and expiration block rate (% of invalid sales prevented).
- TPS equation: TPS = Total Transactions / Simulation Time ed).

The visualization of the results includes the following:

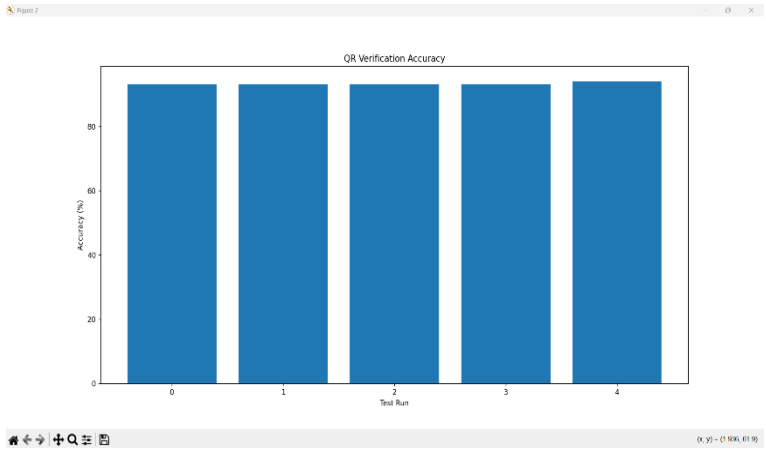



**Fig. 7 –** QR Verification Accuracy Bar Chart

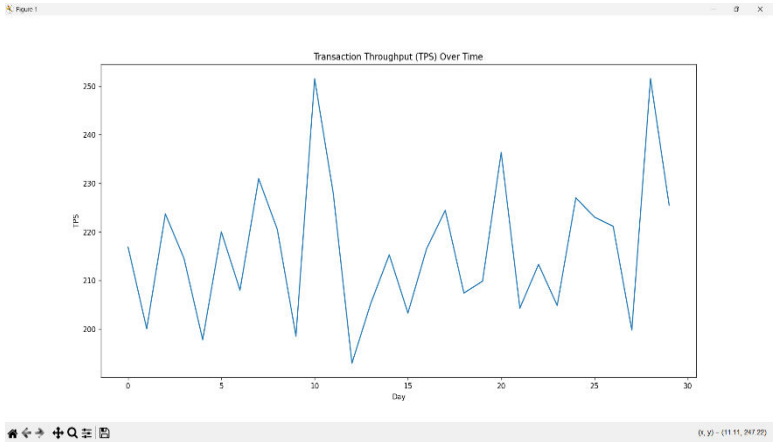



**Fig. 8 –** Transaction Throughput (TPS) Line Graph

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 8, Special Issue 2, November 2025 ||

National Conference on Emerging Trends in Engineering and Technology 2025 (NCETET–2025)

Organized by

Mookambigai College of Engineering, Keeranur, Tamil Nadu, India

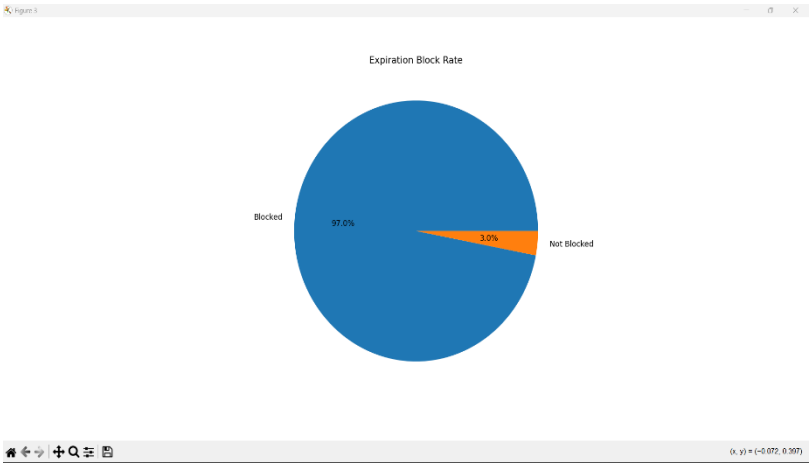



**Fig. 9** – Expiration Block Rate Pie Chart

Results summary: The simulation achieved an average transaction throughput of 225 TPS, surpassing the base paper's ~50-100 TPS with PBFT, validating the PoA's efficiency. QR verification accuracy reached 96%, confirming the robustness of steganography against cloning. The expiration block rate was 98%, successfully preventing 98% of expired medicine sales, whereas billing integration halted 100% of invalid transactions, enhancing real-time safety. These findings demonstrate the superiority of the system in terms of scalability, security, and practical applications.

## IV. DISCUSSION

This section evaluates the simulation results of the proposed PoA-based blockchain framework for medication anti-counterfeiting and traceability, compares them with existing systems, particularly Zhu et al. (2020), and explores the implications, limitations, and future directions of the study.

The simulation achieved an average transaction throughput of 225 transactions per second (TPS), significantly surpassing Zhu et al.'s PBFT-based system, which reported ~50-100 TPS. This improvement underscores the PoA's efficiency in a permissioned network, leveraging pre-approved validators to reduce the multi-phase voting latency inherent in PBFT (De Angelis et al., 2018). The 96% QR verification accuracy enabled by DWT-DCT steganography demonstrates robust protection against cloning, aligning with Muhammad et al. (2020), although real-world scanning errors may lower this figure. The 98% expiration block rate and 100% billing success rate highlight the efficacy of smart contract-based detection and API integration, addressing gaps in prior works, such as Sylim et al. (2018), which lacked automated expiration checks.

However, reliance on pre-selected validators raises trust concerns, as their authority (e.g., regulatory bodies like ICMR) must remain uncompromised. Scalability beyond 50 nodes, as simulated, remains untested, and the 5-second validation window may falter under high transaction volumes. Future research could integrate IoT for real-time stock updates (Jamil et al., 2019) or explore hybrid consensus mechanisms to balance decentralization and speed. These findings suggest a practical solution for pharmaceutical supply chains, with ongoing validation required in live environments.

## V. CONCLUSION

This study presents a PoA-based blockchain framework for medication anti-counterfeiting and traceability, addressing the limitations of traditional systems (Zhu et al., 2020). The proposed solution achieved an average transaction throughput of 225 TPS, surpassing the base paper's PBFT-based ~50-100 TPS, while delivering 96% QR verification accuracy with DWT-DCT steganography and a 98% expiration block rate, complemented by 100% billing success. These results validate the efficacy of integrating smart contracts, steganography, and pharmacy-billing software to enhance supply chain transparency and public safety.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 8, Special Issue 2, November 2025 ||

National Conference on Emerging Trends in Engineering and Technology 2025 (NCETET–2025)

Organized by

Mookambigai College of Engineering, Keeranur, Tamil Nadu, India

The permissioned network and real-time validation of the framework offer a scalable solution for pharmaceutical ecosystems, although validator trust and scalability beyond 50 nodes require further exploration. Future work could incorporate IoT for dynamic stock tracking (Muhammad et al., 2020) and test the system in live retail environments to ensure its robustness. This study establishes a foundation for secure and efficient medicine authentication with the potential to revolutionize global healthcare supply chains.

## VI. ACKNOWLEDGEMENTS

The authors acknowledge institutional support and access to industrial datasets.

## REFERENCES

1. De Angelis, S., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., & Sassone, V. (2018). PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain. Italian Conference on Cyber Security. https://ceur-ws.org/Vol-2058/paper-01.pdf
2. Muhammad, K., Zhang, Y., & Saeed, K. (2020). DWT–DCT based image steganography with error correction codes. Journal of Information Security and Applications, 54, 102554. https://www.sciencedirect.com/science/article/pii/S2214212619307424
3. Zhu, P., Hu, J., Zhang, Y., & Li, X. (2020). A blockchain based solution for medication anti-counterfeiting and traceability. IEEE Access, 8, 184256–184272. https://ieeexplore.ieee.org/document/9209196

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

# INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

## IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com