JOURNAL
Of Universal Applied Research

ISSN (Online): XXX
Vol. 01, Issue 02 (2026)
https://universalappliedresearch.com/index.php/JUAR/issue/archive

A Blockchain-Based Framework for Transparent Pharmaceutical Supply Chains: Development, Implementation and Performance Evaluation

Mythreya Savaram

Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India,Email: sri.mythreya@gmail.com

Received:- 09/06/2026 Revised:- 09/07/2026 Accepted:- 16/07/2026
Published:- 24/07/2026

Abstract

This study developed and evaluated a Python-based blockchain framework for improving transparency, traceability, integrity and security in pharmaceutical supply chains. A design-science and simulation-based approach was applied to 10,000 synthetic transactions covering manufacturers, distributors, retailers and customers. The framework integrated stakeholder-specific ledgers, SHA-256 hashing, block-link validation, role-based access control, batch retrieval, counterfeit detection, cold-chain monitoring and performance analysis. Results showed 100% stage-specific traceability completeness, 96.29% QR verification and 100% hash-link validity. All controlled tampering attempts and counterfeit incidents were detected, 99.68% of unauthorized access attempts were blocked, and all recorded Sybil attacks were neutralized. Among cold-chain transactions, temperature and humidity violations occurred in 5.87% and 3.67% of cases, respectively, and all environmental violations generated alerts. Mean transaction latency was 2.157 seconds, processing latency was 51.74 milliseconds, and the transaction-success rate was 96.62%. Batch retrieval averaged 0.90 milliseconds, while complete ledger validation required 78.71 milliseconds, indicating efficient record access and integrity checking within Python. The proposed PoA+FBA mechanism achieved mean CPU utilisation of 37.81%, compared with 60.99% for PBFT, representing a 38% reduction. These findings demonstrate the framework's technical feasibility under simulated conditions, while real-world deployment requires validation using operational pharmaceutical data, multiple blockchain nodes, IoT sensors and production-grade distributed-ledger platforms.

Keywords: Blockchain, pharmaceutical supply chain, traceability, cold-chain monitoring, performance evaluation

1. Introduction

Pharmaceutical supply chains involve manufacturers, distributors, logistics providers, retailers, healthcare institutions, customers and regulatory authorities. The journey medicines take from manufacturer to patient is organised and geographically complex, requiring the medicines to be accurately identified, information to be secure and monitored throughout the journey. Traditional supply-chain models typically involve a number of different databases, and cause end-to-end visibility to be limited, making it more challenging to ensure the origin and ownership of a medicine, along with storage and regulatory status. These weaknesses could allow for possible counterfeit insertion, modification of unauthorized records, and slow detection of irregularities and poor monitoring of temperature sensitive medicines.

Falsified and substandard medicines continue to be a priority issue as they can be introduced at various points in the distribution chain and they can be indistinguishable from the authentic medicine. The blockchain technology could be a solution that will present a shared, distributed and cryptographically secured transaction ledger. Sylim et al. (2018) demonstrated the potential of blockchain-based records for verification of medicine origin and tracing in the regulatory, manufacturing, wholesaling, retailing and consumer movement. Authorised parties will be able to detect suspicious products and irregularities in the supply chain in a better way as the transaction history will remain consistent.

Each block of the blockchain stores the transactions and links to the previous block using a cryptographic hash function. If the block is modified in any way, then it will affect the hash of that block and make it easier to detect the change in the hash of the corresponding block and the change in the connected blocks with each other. Bocek et al. (2017) showed an early use case application of pharmaceutical product movement tracking using the blockchain along with temperature monitoring, which demonstrates how distributed ledgers can be used for supply-chain transparency and logistics monitoring. Blockchain can also contribute to better regulatory visibility. As proposed by Tseng et al. (2018), a governance model would allow regulators to obtain information on all drug transactions in a transparent manner and shift from periodic inspection to more continuous supervision.

Access control is also significant because different activities are carried out by the pharmaceutical stakeholders and they shouldn't have the same system permissions. Manufacturers can register and transfer medicine batches, distributors and retailers can check and transfer products, customers can verify authenticity, and regulators can verify compliance. Jamil et al. (2019) showed the potential of blockchain to enable controlled interaction and transaction integrity in healthcare stakeholders' interaction in drug-supply-chain management. By using role-based validation, you can therefore limit unauthorized actions while maintaining an audit trail of accepted/rejected and suspicious transactions.

Another important requirement is cold-chain monitoring. Vaccines, insulin and other temperature-sensitive drugs can be degraded by adverse environmental conditions. To combat the risk of counterfeit drugs, Singh et al. (2020) combined blockchain, Internet of Things sensors and QR verification to track pharmaceutical temperatures. It can help track a violation by relating environmental measurements to transaction data that cannot be altered by anyone. While not directly applicable to this context, Abbas et al. (2020) also illustrated the viability of integrating blockchain with machine-learning capabilities for pharmaceutical tracking and decision support, which may require specialized infrastructure and technical expertise.

Later, this study has been extended in a number of different directions for pharmaceutical traceability through blockchain. Musamih et al. (2021) demonstrated that blockchain and smart contracts can enhance transparency, track of the product history, and assist in detecting counterfeit products. Bali et al. (2021) proposed a solution called PharmaChain which utilized role-based permissions and blockchain records to monitor medicine ownership, but the use of Hyperledger and associated tools could potentially limit the availability of the solution for researchers who are working in simpler environments. To track and monitor drugs in real-time, Liu et al. (2021) combined blockchain and IoT technologies while pointing out that the performance of the system is affected by the configuration of the system, how resources are stored, and how resources are consumed.

There have been other researchers who have looked at other security and traceability options. Chiacchio et al. (2022) suggested an NFT-based method where each pharmaceutical product was uniquely tokenized to further bolster ownership verification and allow consumers to get product information through QR codes. To enhance the confidentiality and trust, Zoughalian et al. (2022) integrated a zero-knowledge proof with a reputation system, which resulted in a higher implementation complexity. Humayun et al. (2022) pointed out the need for regulatory oversight by delegating monitoring and authentication of drugs to authorities to enhance coordination and authenticity in drug-distribution activities. Zakari et al. (2022) conducted a systematic review and found that the blockchain technology can solve the issues of counterfeit medicines, disjointed records, lack of trust and poor traceability but also noted that numerous pharmaceutical blockchain solutions are still conceptual models or prototypes.

In general, the results of previously studied blockchain applications have shown that it has the potential to be used for pharmaceutical traceability, security, cold-chain monitoring, and regulatory supervision. But most of the research is limited to a specific platform or function, and few studies evaluate the integrity of hash-chain, role-based access, counterfeit detection, etc. in the same reproducible framework, to consider environmental anomalies and computational performance. So this study aims at developing and testing a Python based blockchain framework that incorporates: SHA-256 hashing, block-link validation, batch retrieval, role based transaction rules, security event monitoring and cold chain assessment. It is tested based on transaction latency, processing latency, success rate, throughput, bandwidth overhead, anomaly-response time and CPU utilisation, and the proposed PoA+FBA indicators are compared with the PBFT baseline under simulated conditions.

2. Methods

2.1 Research Design and Dataset

A design-science and simulation method are employed in this research to design and test a transparent blockchain framework for pharmaceutical supply-chain management implemented with Python.In this work, a design-science and simulation method are used to design and test a Python-based blockchain framework for a transparent pharmaceutical supply-chain management. The framework was developed for the purposes of transaction recording, access control for stakeholders, batch traceability, cold-chain monitoring and security-event validation. The study was carried out in three phases: preparation of dataset, implementation of the framework and assessment of framework performance.

The data for the analysis was the medicine_scm_10k_simulation_transactions.csv dataset with 10,000 simulated transactions and 62 variables (Saha, n.d.). They were the records of manufacturers, distributors, retailers, and customers at four points in the supply chain – batch creation, stock transfer, retail sale and customer verification. The data set also featured four chains dedicated to the four stakeholders, namely ManufacturerChain, DistributorChain, RetailerChain and CustomerChain, along with consensus mechanism proposed as PoA+FBA.

Product and Batch details, stakeholder identifiers, blockchain metadata, temperature and humidity measurements, regulatory status, security incidents and performance indicators were all included in the variables. Security events consisted of blockchain tampering, counterfeit products, unauthorized access, temperature abuse, humidity abuse and Sybil attacks. The performance metrics were transaction latency, processing latency, success rate, CPU usage of the proposed mechanism and for PBFT baseline, and bandwidth overhead.

The study did not test the effectiveness of a live pharmaceutical blockchain network but the technical feasibility and simulated performance of the Python based framework. The PoA+FBA and PBFT measurements were therefore considered as synthetic values instead of the values from independently run consensus systems.

2.2 Data Preparation and Preprocessing

The data was loaded into the Python 3 environment using pandas.The data was imported into Python 3 using Pandas library. The initial pre-processing included checking that the data had the correct dimensions, data types, missing data, duplicate records and distinctness of transaction and blockchain identifiers. To identify duplication, tx_id, block_hash, merkle_root and ipfs_cid fields were checked, and block_index was checked separately in each of the stakeholder-specific blockchains.

All the timestamp variables, such as transaction time, submission time, confirmation time, anomaly-injection time and anomaly-detection time were converted to datetime. The following numerical variables were converted to an appropriate numeric type: transaction value, temperature, humidity, latency, CPU utilization and bandwidth overhead. The values for categorical variables were coded, and binary "Yes" and "No" variables were translated into numbers for statistical purposes as needed.

The values that were missing were treated appropriately to the situation. No customer identifiers were missed in non-customer transactions, these were regarded as structurally missing. The fields which were not present in the anomaly were considered as normal if the security indicators did not indicate any anomaly. Records where no detection-time information was available were kept for analysis of the frequencies of anomalies, but these were not used in calculating response time.

The completeness of traceability was evaluated based on the completeness of each stage of a transaction. Most batch identifiers were observed only once, so batch traceability was considered as a process to retrieve all available records and observed stages on a batch instead of assuming that it was observed from the manufacturer to the customer. All preprocessing was applied to a copy of the original data, and the original data set was not changed.

2.3 Proposed Blockchain Framework

The suggested model comprised four elements: blockchain ledger, role-based transaction validation, batch traceability, and security and cold-chain monitoring.

The blockchain ledger was divided into four stakeholder chains namely ManufacturerChain, DistributorChain, RetailerChain and CustomerChain. Records were retrieved by block_index - the first block in each chain was considered the genesis block. Each block had an index, timestamp, transaction payload, previous hash and current hash. Python's hashlib library was then used to hash the transaction data in SHA-256 hash to ensure that it is consistently ordered and stored in JSON format.

The integrity of blockchain was checked by verifying that every block other than the genesis block has the same previous_hash as the previous block and by recalculating block hashes during validation. The integrity of the tampering was verified by changing the copies of the selected blocks without changing the hash values stored in the

blocks. If the hash that was recalculated was not equal to the one stored or there was an issue with the link to the next block, then the block was considered invalid.
Using Python rules, access to the different operations was granted to manufacturers, distributors, retailers, customers and regulatory users, respectively, through role-based access control. Functions verified stakeholder permissions, transaction identifiers, batch identifiers, QR status, blockchain linkage, cold-chain conditions, regulatory information – smart-contract like functions. When there was no validation required, transactions were accepted when there was an unbalanced transaction, it was rejected, and when a counterfeit, environmental, or security issue was detected, it was flagged.
Batch traceability was carried out by taking the medicine batch ID to get all records for the medicine batch and then arranging them in chronological order. Product, stakeholder, blockchain, QR-verification, environmental and regulatory information were included in the output. The framework used only the available stages in the reported dataset, as most batch identifiers were only a single instance of each batch.
The cold_chain_required, temperature_c, humidity_pct, temp_violation, humidity_violation and cceif_alert variables are used for cold-chain monitoring. Security monitoring was performed on the counterfeit products, tampering attempts, unauthorized access and Sybil attacks, with their respective detection and prevention indicators. Response-detection time was measured by the response time measured from the recorded response time and the anomaly timestamp.
The IPFS and the consensus and zero-knowledge-proof fields were kept as verification and performance data. It was not however seen as a live IPFS network nor a full zero-knowledge-proof protocol or multi-node PoA+FBA blockchain deployment within the framework.

2.4 Python-Based Framework Implementation

The proposed framework has been implemented entirely using Python, modular classes and functions. Each pharmaceutical transaction block was represented by a Block class with the block index, timestamp, transaction payload, previous hash and current hash. The blocks were hashed with SHA-256 with the content of the blocks in a consistent ordered JSON representation.
A Blockchain class oversaw the Manufacturer, Distributor, Retailer and Customer chains. It was responsible for generating the genesis block, adding transactions and verifying block hashes and links. Other modules responsible for stakeholder authorisation, transaction validation, batch tracking, cold chain monitoring, security event analysis and performance measurement.
All the information related to a selected batch_id was returned by the batch-tracing function and information on temperature, humidity and alert indicators was provided by the cold-chain module. The security module evaluates counterfeit products, tampering attempts, unauthorized access and Sybil attacks. The performance measures such as transaction latency, processing latency, success rate, throughput, CPU utilisation, bandwidth overhead, batch-retrieval time and blockchain-validation time were evaluated.
Data was processed with pandas and numpy, hashes and transactions were serialized by hashlib and json, temporal analysis was performed using datetime and time, statistical testing was done with scipy, and visualisation was done using matplotlib and seaborn. This was implemented as a Python-based system to simulate and validate a blockchain-based system instead of a production distributed ledger.

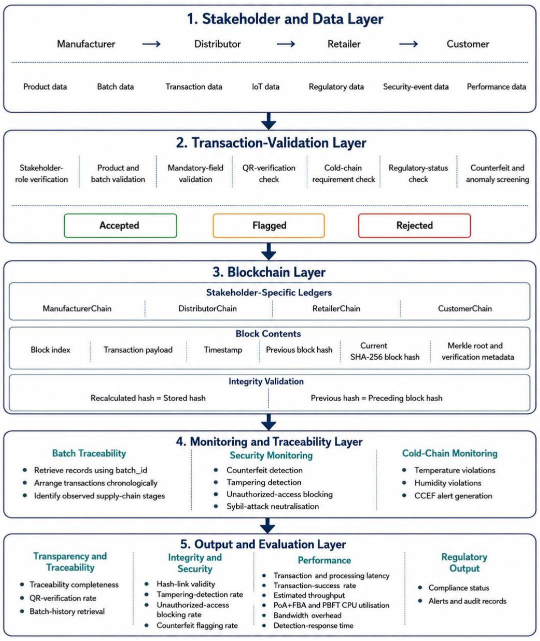

Figure 1. Proposed Python-based pharmaceutical supply-chain framework.

2.5 Performance Metrics and Statistical Analysis

The framework was tested in three aspects: traceability and blockchain integrity, security and cold-chain monitoring, and transaction performance.

Stage-specific completeness, QR-verification rate, the validity and the time of blockchain-link retrieval were used to assess traceability. A transaction was complete once all the product, batch and stakeholder, stage, timestamp and blockchain fields that were required for the transaction stage were available.

Blockchain integrity was assessed by checking whether the previous_hash of each block other than the genesis block was equal to the hash of the previous block. Both set of data indicators and modified versions of the prototype blocks were used to test tampering detection.

Security evaluation comprised of counterfeit flagging, blocking unauthorized accesses, neutralising Sybil-attack and anomaly-response-time. The performance of the cold chain was measured based on the number of temperature violations, humidistat violations and medicines that trigger an alert on the CCEIF for medicines requiring controlled storage.

Confirmation latency, processing latency, success rate, estimated throughput, CPU utilisation and bandwidth overhead were the metrics used to measure the performance of transactions.

Frequencies and percentages were used to summarize categorical variables, and means, medians, standard deviations, interquartile ranges and confidence intervals to summarize numerical variables. Proposed CPU utilisation and the PBFT CPU utilisation were compared using a paired-samples t-test or Wilcoxon signed-rank test depending on normality. Using Welch's t-test or Mann-Whitney U test, the difference in latency of normal and anomalous transactions was analyzed. The comparisons of anomalies and/or environmental-violation status with regulatory outcome were done by the chi-square test or Fisher's exact test.

The criteria for statistical significance was set at ($p < 0.05$). Results were reported using the appropriate test statistic, p-value, 95% confidence interval and effect-size measure. The data set was kept as is and all analyses were performed using reproducible python scripts.

3. Results and Discussion

3.1 Dataset and Framework Implementation

The Python-based blockchain framework successfully imported and processed all 10,000 transactions in the supply-chain of the pharmaceutical industry. The role of stakeholders and the status of transactions and the type of anomalies are summarized in Table 1.

Table 1. Characteristics and transaction distribution

Category	Frequency	Percentage
Manufacturertransactions	1,376	13.76%
Distributor transactions	2,048	20.48%
Retailer transactions	2,752	27.52%
Customer transactions	3,824	38.24%
Normal transactions	7,571	75.71%
Anomalous transactions	2,429	24.29%
Blockchain tampering	855	8.55%
Unauthorized access	500	5.00%
Humidity abuse	356	3.56%
Counterfeit products	336	3.36%
Temperature abuse	286	2.86%
Sybil attacks	96	0.96%

The framework has successfully accomplished the following tasks in block creation, generation of hash using the SHA-256 cryptography, validation of blocks and transactions, role-based access control, retrieval of blocks, and monitoring the cold-chain, as illustrated in Fig.1. Every transaction was "unnaturally" structured into a "structured block" and allocated to the corresponding Manufacturer-Distributor-Retailer or Customer chain. The most frequent anomalies found were blockchaining, unauthorized access and humidity abuse.

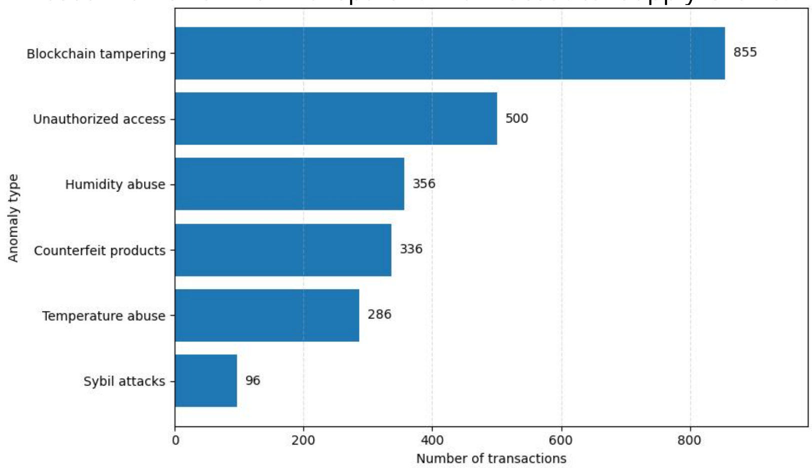

Figure 1. Distribution of security and environmental anomalies.

The successful carrying out of the core functions illustrates that blockchain-based pharmaceutical tracking can be done in a normal Python environment without having to install the whole Ethereum and Hyperledger. This will enhance the accessibility and replicability of the framework. The outcome is, however, not a product of a distributed blockchain of independent organizational nodes, but a technical simulation of the process of operation of a centralized simulation.

3.2 Traceability, Integrity and Security

All 10,000 transactions had the product, batch, stakeholder, and timestamp and blockchain data necessary at each stage of the transaction, resulting in a 100% traceability completeness for each stage of the transaction. 9,629 transactions were successfully verified using QR codes. Each of the 9,996 non-genesis blocks, were completely internally hash-chain consistent with the hash of the previous block. Table 2 provides an overview of the principal traceability, integrity and security outcomes.

Table 2. Traceability, integrity and security performance

Indicator	Result
Stage-specific traceability completeness	100.00%
QR-verification rate	96.29%
Stored hash-link validity	100.00%
Mean batch-retrieval time	0.90 ms
Mean complete-ledger validation time	78.71 ms
Prototype tampering-detection rate	100.00%
Dataset tampering-detection rate	100.00%
Counterfeit-flagging rate	100.00%
Unauthorized-access blocking rate	99.68%
Sybil-attack neutralisation rate	100.00%
Mean anomaly-response time	0.702 s

The results show that the framework was able to keep transaction logs transparent and verifiable internally. When all the intentionally altered prototype blocks are fully validated and identified, it is clear that with the aid of hash-linking and hashing of the prototype blocks, SHA-256 can be used to detect unauthorized changes. It validates earlier research on the pharmaceutical Blockchain to suggest mechanisms such as immutable records and product tracking as crucial for enhancing the trust of the supply chain and lowering counterfeit products (Kayhan, 2022; Bapatla et al., 2023).

A total of 9974 unique_batch_id were available. Of these, 9,955 happened at 1 stage in the supply chain, and 19 at 2 stages, with none of the 4 stages present. Therefore, the framework was successful in recovering all batch records available but was not able to show full manufacturer-to-customer provenance. This result points to a practical problem; blockchain can only secure information once it has been stored, but it won't help if there are missing transactions or incorrect batch identifiers between organizations.

The security analysis revealed that there were 968 tampering attempts recorded, all of which were spotted, and 336 counterfeit transactions were identified. The 626 total unauthorized accesses were blocked (624) and all 140 Sybil attacks were neutralized. The above findings suggest that the simulated performance of the systems was good for authentication, transaction integrity and access control. Their capabilities align with prior systems that rely on immutable historical records of transactions, authentication of stakeholders and permissions based on roles to stop counterfeit products and unauthorized pharmaceutical transactions (Islam & Islam, 2024; Nawaz et al., 2024).

2,427 anomalous transactions were available for detection-response time. The mean response time was 0.702 seconds, the median was 0.493 seconds and the 95th percentile was 1.263 seconds. The detection of tampering and unauthorized-access and Sybil events took about 0.40 seconds, while the detection of counterfeit and environmental anomalies took about 1.15 seconds. The increased response time for these events might be due to the extra product, environmental and regulatory fields to be validated.

3.3 Cold-Chain Monitoring

A total of 235 cold-chain transactions were identified as having temperature violations and 147 as having humidity violations. In total, 377 transactions had at least one environmental violation, with all the violations triggering a CCEIF alert. All the transactions with temperature or humidity violations have also been given flagged regulatory outcomes.

This indicates that integrating environmental data and blockchain transaction logs can enhance the traceability and transparency of cold-chain operations. The framework could help pinpoint a particular product, transaction and supply-chain level and connect it to an environmental violation. This aligns with other research that has indicated that blockchain and IoT can enhance the continuous monitoring of pharmaceuticals and minimize logistics losses (Dash et al., 2024).

The outcomes of the transactions were widely divergent for normal transactions and anomalous transactions. There were 2,429 anomalous transactions, of which 984 were flagged, and 7,571 normal transactions, 22 of which were flagged. The relationship was statistically significant, $\chi^2 (1,N=10,000)=3283.41$, $p<0.001$, with Cramér's $V=0.573$. This is a large association, suggesting that anomaly indicators were well represented in regulatory classifications. However, the measurements of the environment were simulated instead of taken from actual IoT devices (Wen et al., 2025). Calibrated sensors would have to be deployed and security measures would have to be put in place to prevent tampering with the sensors. The results of the cold-chain monitoring are shown in Table 3.

Table 3. Cold-chain monitoring results

Cold-chain indicator	Transactions	Rate
Transactions requiring cold-chain handling	4,006	—
Temperature violations	235	5.87%
violations	147	3.67%
Any environmental violation	377	9.41%
Violations generating CCEIF alerts	377	100.00%

3.4 Transaction Performance and Statistical Analysis

The framework had a transaction-success rate of 96.62%, and mean end-to-end latency of 2.157 seconds, and mean internal processing latency of 51.74 milliseconds (ms). The estimated throughput was found to be 1.38 transactions per second and the mean bandwidth overhead was 15.05% for the simulated observation period. The results suggest that the Python simulation model has a stable transaction processing rate, but in a large national pharmaceutical network, the throughput of the observed results might need to be enhanced. The summary of overall transaction-performance results is shown in Table 4.

Table 4. Performance of the proposed framework

Performance indicator	Result
Mean transaction latency	2.157 s
Median transaction latency	2.161 s
Standard deviation of latency	0.216 s
Mean processing latency	51.74 ms
Transaction-success rate	96.62%
Estimated throughput	1.38 transactions/s
Mean proposed CPU utilisation	37.81%
Mean PBFT CPU utilisation	60.99%
Mean CPU reduction	38.00%
Mean bandwidth overhead	15.05%

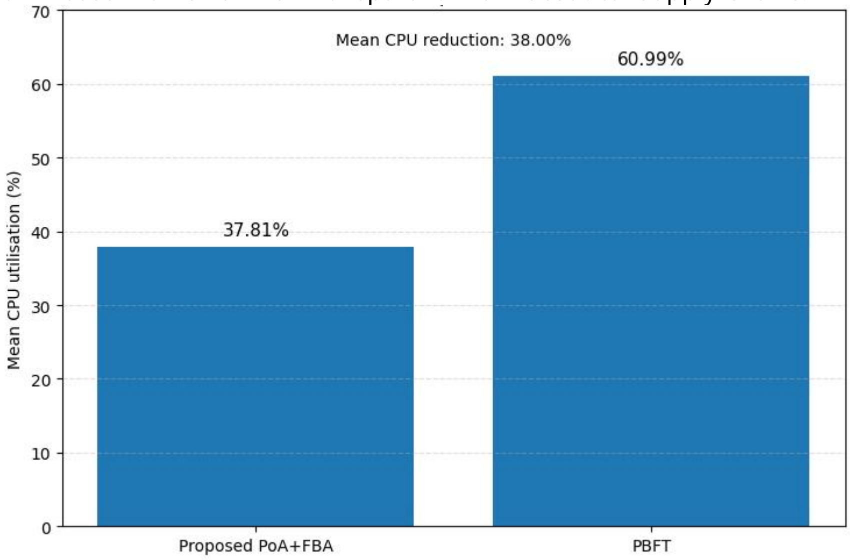

Figure 2. CPU utilisation of the proposed mechanism and PBFT

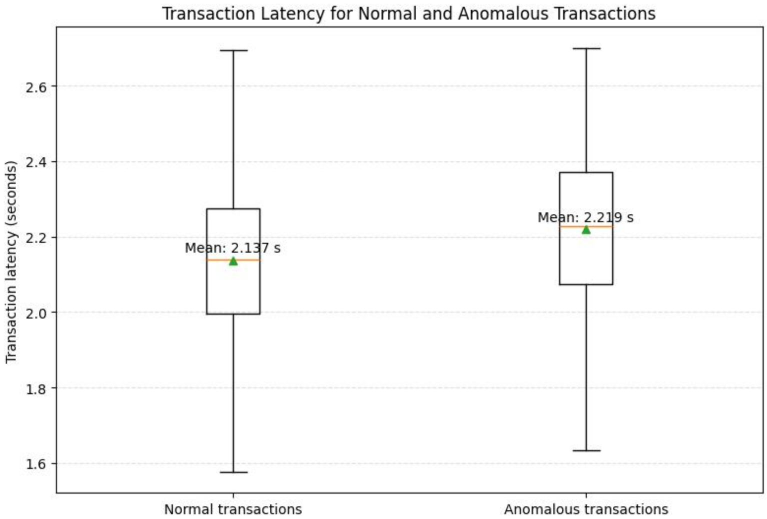

Figure 3. Transaction latency for normal and anomalous transactions.

The mean CPU utilisation for the proposed PoA+FBA mechanism was 37.81% as compared to 60.99% for PBFT, which equates to a 38% reduction as shown in Fig 2. The comparison of CPU utilisation under the proposed mechanism was then compared with the usage level under the default mechanism and a paired-samples t-test was used, with $t(9999) = 1258.85$ and $p<0.001$. The mean difference was 23.18 percentage points, 95% CI [23.14, 23.21] and $d_z=12.59$ standardized effect size. This finding indicates that the proposed simulated mechanism has significantly reduced computational requirements, and aligns with prior studies that show that the resource utilization of a blockchain system depends on the choice of the architecture and consensus method (Naga Sudha & Nayahi, 2024).

The mean latency for normal transactions was 2.137 seconds while for anomalous transactions it was 2.219 seconds. This difference of 0.082 seconds was statistically significant ($t = -16.13$, $p< 0.001$) and there was an effect size of $d = 0.39$. This was supported by a Mann–Whitney U test as shown in Fig 3. The slight rise indicates that the security and environmental validation added a bit more processing requirement, but not a significant delay in operation.

The framework exhibited overall good simulated traceability, integrity, security and computational performance. It may provide a way for manufacturers to register batches, for distributors to validate transfers, for retailers to verify medicines authenticity and for regulators to review compliance information and for customers to confirm medicines with QR records. The data set, however, was synthetic and the performance measures were not actually a test of the implementation as a live multi-node blockchain. The metadata was defined by neither IPFS nor zero-knowledge-proof fields, and the management of cryptographic keys, network failures, privacy, and large-scale deployment were not tested. Future work needs to be done to validate the framework using real pharmaceutical transactions, live IoT sensors, consistent batch identifiers and production blockchain platforms, like Hyperledger Fabric, Hyperledger Sawtooth or Ethereum.

4. Conclusion

In this study, the authors created and tested a blockchain framework for the pharmaceutical supply chain (PSC), which improves transparency, traceability, integrity and security in PSCs using Python. The framework combined role based access control, batch retrieval, cold-chain monitoring and performance analysis, counterfeit detection, and stakeholder specific ledger using a SHA-256 hashing function. The framework had a stage-specific traceability completeness of 100%, a QR verification of 96.29% and a validity of hash link of 100%, using 10000 simulated transactions. It has also identified all the known cases of tampering, counterfeiting, and blocked out 99.68% of unauthorized login attempts, making all the Sybil attacks inert. The cold-chain monitoring system detected the temperature and humidity violations and alerted for all environmental violations. The results of the performance test were a mean transaction latency of 2.157 seconds, a success rate of 96.62% and the estimated number of transactions per second of 1.38. The proposed PoA+FBA mechanism was shown to improve the computational efficiency under the simulated scenarios as mean CPU utilisation was reduced by 38% compared to PBFT. The results, however, are constrained by the synthetic dataset, the batch histories being incomplete in each of the stages of the batch and the lack of an existing distributed blockchain, of IPFS storage and full implementation of the zero-knowledge-proof. Overall, the technical feasibility of the framework was demonstrated, but further research is required to test it with real pharmaceuticals data, several blockchain nodes and production platforms like Hyperledger Fabric or Ethereum before its broad incorporation in a real supply chain of pharmaceutical products.

References

2. Abbas, K., Afaq, M., Khan, T. A., & Song, W.-C. (2020). A blockchain and machine learning-based drug supply chain management and recommendation system for smart pharmaceutical industry. Electronics, 9(5), 852. https://doi.org/10.3390/electronics9050852
3. Bali, V., Soni, P., Khanna, T., Gupta, S., Chauhan, S., & Gupta, S. (2021). Blockchain application design and algorithms for traceability in pharmaceutical supply chain. International Journal of Healthcare Information Systems and Informatics, 16(4). https://doi.org/10.4018/IJHISI.289460
4. Bapatla, A. K., Mohanty, S. P., Kougianos, E., Puthal, D., & Bapatla, A. (2023). PharmaChain: A blockchain to ensure counterfeit-free pharmaceutical supply chain. IET Networks, 12(2), 53–76. https://doi.org/10.1049/ntw2.12041
5. Bocek, T., Rodrigues, B. B., Strasser, T., & Stiller, B. (2017). Blockchains everywhere—A use-case of blockchains in the pharma supply-chain. In 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM) (pp. 772–777). IEEE. https://doi.org/10.23919/INM.2017.7987376
6. Chiacchio, F., D'Urso, D., Oliveri, L. M., Spitaleri, A., Spampinato, C., & Giordano, D. (2022). A non-fungible token solution for the track and trace of pharmaceutical supply chain. Applied Sciences, 12(8), 4019. https://doi.org/10.3390/app12084019
7. Dash, S., Ghugar, U., Godavarthi, D., & Mohanty, S. N. (2024). HCSRL: Hyperledger composer system for reducing logistics losses in the pharmaceutical product supply chain using a blockchain-based approach. Scientific Reports, 14, 13528. https://doi.org/10.1038/s41598-024-61654-7
8. Humayun, M., Jhanjhi, N. Z., Niazi, M., Amsaad, F., & Masood, I. (2022). Securing drug distribution systems from tampering using blockchain. Electronics, 11(8), 1195. https://doi.org/10.3390/electronics11081195
9. Islam, I., & Islam, M. N. (2024). A blockchain based medicine production and distribution framework to prevent medicine counterfeit. Journal of King Saud University—Computer and Information Sciences, 36(1), 101851. https://doi.org/10.1016/j.jksuci.2023.101851
10. Jamil, F., Hang, L., Kim, K. H., & Kim, D. H. (2019). A novel medical blockchain model for drug supply chain integrity management in a smart hospital. Electronics, 8(5), 505. https://doi.org/10.3390/electronics8050505
11. Kayhan, H. (2022). Ensuring trust in pharmaceutical supply chains by data protection by design approach to blockchains. Blockchain in Healthcare Today, 5, 232. https://doi.org/10.30953/bhty.v5.232
12. Liu, X., Barenji, A. V., Li, Z., Montreuil, B., & Huang, G. Q. (2021). Blockchain-based smart tracking and tracing platform for drug supply chain. Computers & Industrial Engineering, 161, 107669. https://doi.org/10.1016/j.cie.2021.107669
13. Musamih, A., Salah, K., Jayaraman, R., Arshad, J., Debe, M., Al-Hammadi, Y., & Ellahham, S. (2021). A blockchain-based approach for drug traceability in healthcare supply chain. IEEE Access, 9, 9728–9743. https://doi.org/10.1109/ACCESS.2021.3049920
14. Naga Sudha, C. M., & Nayahi, J. J. V. (2024). TrackChain: Hyperledger based pharmaceutical supply chain—Resource utilization perspective. Heliyon, 10(1), e23250. https://doi.org/10.1016/j.heliyon.2023.e23250
15. Nawaz, A., Wang, L., Irfan, M., & Westerlund, T. (2024). Hyperledger Sawtooth based supplychain traceability system for counterfeit drugs. Computers & Industrial Engineering, 190, 110021. https://doi.org/10.1016/j.cie.2024.110021
16. Saha, B. M. (n.d.). Blockchain-based medicine supply chain management [Data set]. Kaggle. from https://www.kaggle.com/datasets/bidyutmalasaha/blockchain-based-medicine-supply-chain-management

17. Singh, R., Dwivedi, A. D., & Srivastava, G. (2020). Internet of Things based blockchain for temperature monitoring and counterfeit pharmaceutical prevention. Sensors, 20(14), 3951. https://doi.org/10.3390/s20143951
18. Sylim, P., Liu, F., Marcelo, A., & Fontelo, P. (2018). Blockchain technology for detecting falsified and substandard drugs in distribution: Pharmaceutical supply chain intervention. JMIR Research Protocols, 7(9), e10163. https://doi.org/10.2196/10163
19. Tseng, J.-H., Liao, Y.-C., Chong, B., & Liao, S.-W. (2018). Governance on the drug supply chain via Gcoin blockchain. International Journal of Environmental Research and Public Health, 15(6), 1055. https://doi.org/10.3390/ijerph15061055
20. Wen, Y., Wei, Y., & Liu, L. (2025). Research on operation strategy of multiple channels pharmaceutical supply chain based on blockchain technology. Scientific Reports, 15, 17033. https://doi.org/10.1038/s41598-025-00727-7
21. Zakari, N., Al-Razgan, M., Alsaadi, A., Alshareef, H., Al Saigh, H., Alashaikh, L., Alharbi, M., Alomar, R., & Alotaibi, S. (2022). Blockchain technology in the pharmaceutical industry: A systematic review. PeerJ Computer Science, 8, e840. https://doi.org/10.7717/peerj-cs.840
22. Zoughalian, K., Marchang, J., & Ghita, B. (2022). A blockchain secured pharmaceutical distribution system to fight counterfeiting. International Journal of Environmental Research and Public Health, 19(7), 4091. https://doi.org/10.3390/ijerph19074091