International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(1s) 2026 pp. 1-16
https://doi.org/10.70917/ijcisim-2026-2033
Article

PoAV-Based QR Code Blockchain Technique for Counterfeit Medicine Detection and Performance Validation

Yogesh Arjun Shinde1, Shrinivas. K. Sonkar2

1Department of Computer Engineering, MET's Institute of Engineering Nashik. (SPPU, Pune), Maharashtra India, yogeshshinde599@gmail.com
2 Department of Computer Engineering Amrutvahini College of Engineering, Sangamner, (SPPU, Pune), Maharashtra India, sonkar83@gmail.com

Abstract: — The problem of counterfeit drugs remains a constant threat in the pharmaceuticals industry due to identity, handoff, and record fragmentation across various organizations. Also hard for the end users to verify their identities instantly. In this paper, a new blockchain framework is proposed with QR-coded identity of medicines and Proof of Authentic Validation (PoAV) as a custom consensus along with a Trans-Evaluator layer for mutual validation of the block. The system will be recording on-chain events related to registration of products, transfer of ownership, compliance event occurrence, and drug recall notices while keeping an extendable metadata of the medicines off-chain via a content hash link mechanism. Contrary to existing approaches based on centralizing metadata storage or costly public blockchain validation, the proposed architecture stresses on instant verification, efficient computation power, and access for end users. The implementation of the framework uses smart contracts for registration, roles, auditing, quality assurance of products, and drug recalls. Validator selection is made via scoring policy that is dependent on the reputation score, compliance score, role importance, and efficiency of validators for forming the PoAV approval set. The developed framework was prototyped on a permissioned testbed using scalable virtual nodes. The experiment results show perfect QR authentication accuracy for Different scenarios and better validation execution throughput compared to the reference Ethereum, DApp, and BCoT implementations. Besides, our approach shows significantly less CPU consumption and faster confirmation times compared to PoW and PoS mechanisms.

Keywords: —Blockchain, Counterfeit Medicine Detection, Healthcare Supply Chain, Permissioned Ledger, PoAV, QR Code, Smart Contract, Security.

1. Introduction

The existence of counterfeit and substandard drugs threatens the safety of patients and the integrity of health care organizations, and creates unnecessary financial burden in the supply chain. The issue becomes more significant when the records of medicines are dispersed among various parties such as manufactures, distributors, pharmacies, logistics operators, and regulatory agencies without the availability of an auditable and tamper-resistant trail. It is evident from recent blockchain research that blockchain technology could enhance provenance, transparency, and trust in the supply chain management especially when multi-parties require a synchronized event history [1]– [4].

However, there still exist several drawbacks in practice. Firstly, previous works have paid more attention to optimizing traceability within institutional participants, and the authentication process from the patients' side has been viewed as a secondary objective instead of a primary concern [2], [3]. Secondly, some blockchain-based schemes suffer from latency, storage expansion, or computation complexity of the inherent blockchain platform, making them less appropriate for timely drug verification in small-scale and medium-scale systems [4], [7], [8]. Lastly, existing blockchain-based traceability frameworks do not include duplicate scan detection, time window check, validator reliability evaluation, and mutual validation between block proposers and smart contracts.

To overcome these limitations, this study develops a permissioned QR code-oriented framework in which the identity information of medicines is registered on QR codes via blockchain, product transactions are managed by smart contracts, and block production is regulated by a specialized proof-of-auth validation (PoAV) consensus protocol. In addition, a trans-evaluator component is proposed to conduct mutual validation between the block proposer and the smart contract prior to block creation. This research does not seek for a higher level of decentralization at the expense of security, transparency, user-friendly experience, and computation overhead in regulated pharmaceutical sectors.

2. Related Work And Research Gap

Traceability of drugs via blockchain in healthcare is a well-established research topic, although the solutions implemented by previous authors diverge greatly in their design. First, in [1] Omar et al. used smart contracts to automatically manage procurement contracts and found that automation may eliminate some time-consuming stages in healthcare supply chain. Second, in [2] Musamih et al. suggested a smart contract platform based on Ethereum to facilitate tracking of provenance in a specific lot of medicine. At the same time, in [3] Crypto Pharmacy provided a mobile app which uses blockchain in a somewhat different setting and emphasized the importance of user visibility in the purchase process.

In addition to medicine-focused research, the literature in blockchain for supply chain in general explores the aspects of optimization, digital twins, proof of delivery, privacy and data governance, and off-chain storage. Optimization and implementation for digital twins shows that the design of consensus protocol heavily influences energy and time costs [4]. In [5] and [9], inventory sharing and proof-of-delivery contracts show that the use of smart contracts in the context of inter-organizational communication allows automating some operations in a reliable manner. Also, the research dedicated to vaccines and IoT-assisted management of the quality of drugs reveals the benefits of the combination of off-chain storage and on-chain digest anchoring [7], [11].

However, in their surveys of the literature, authors frequently point out obstacles such as lack of interoperability between platforms, ambiguity of governance rules, developer shortage, storage growth, and difficulties with reconciling technological design with regulatory requirements [8], [12], [13]. The above obstacles become especially important in the case of pharmaceutical systems because the end-user trust is determined by the mathematical properties of the ledger, as well as the possibility of instant verification provided by the last-mile scanning. The research conducted by Pattanayak et al. [15] discussed the application of blockchain technology based on dynamic capabilities and explained the ways in which blockchain makes supply chains resilient via increased transparency, traceability, and disruption response. Hsiao and Sung [16] created an information sharing model using blockchain technology to increase the level of security and trust within supply chain operations. Hawashin et al. [17] have come up with a blockchain technology solution for the problem of overproduction and underconsumption of medical products due to poor supply-demand synchronization in the field. Saranya and Maheswari [18] presented a proof of transaction method of creating a traceable agricultural supply chain. Zhu et al. [19] researched applications of blockchain technology and smart contracts in fresh product supply chains and found them beneficial when it comes to resource management and supply chain effectiveness. In summary, these articles prove that blockchain could be used to increase transparency, traceability, resilience, and automation in various industries; however, domain-specific validation mechanisms should be applied to make healthcare supply chains more secure.

Blockchain technology has received considerable attention when it comes to enhancing transparency, traceability, security, and efficiency in supply chain operations. Dutta et al. [21] considered blockchain technology's relevance regarding immutability of records, prevention of fraud, provenance, and secure data sharing in the pharmaceutical, food, and manufacturing industries. Paliwal et al. [22] examined how blockchain technology could aid sustainable supply chains by improving the utilization of resources, ethical sources, and minimizing wastage. On the other hand, Jordan et al. [23] explored how blockchain could be useful in increasing the transparency of fashion supply chains. Vistro et al. [24] and Hussain et al. [25] pointed out the usefulness of the combination of blockchain and IoT technologies in ensuring real-time monitoring, quality control, compliance, and provenance of products. Pradeep et al. [26] conducted a review on blockchain's application in supply chains, the issues involved, and future directions of using the technology for SCM. Deepa et al. [27] identified blockchain as a technology that could enhance secure and scalable big data analytics in supply chains, whereas Kassen [28] talked about the possibilities of blockchain technology in e-government and automated provision of public information.

Table I. Representative blockchain studies related to medicine and supply-chain traceability.

Study	Core focus	Strength	Gap motivating this work
Omar et al. [1]	Healthcare procurement automation	Multi-stakeholder smart-contract coordination	No patient-side QR verification emphasis
Musamih et al. [2]	Drug-lot traceability	Event-based provenance and authenticity lookup	Limited duplicate/replay awareness
Subramanian et al. [3]	Mobile pharma blockchain	Direct user visibility of medicine history	Different chain model and purchase orientation
Garcia et al. [10]	Privacy-preserving governance	Consent and access tracking	Focuses on data governance, not QR authenticity
Cui et al. [7]	Storage-efficient vaccine blockchain	Off-chain scaling with on-chain evidence	Not tailored to medicine QR validation
Agarwal et al. [8]	Comprehensive review	Clear taxonomy of benefits and barriers	Highlights need for lightweight, interoperable designs

The analysis of this literature results in a clear research gap which needs to be addressed. There exist multiple approaches which provide one of the following advantages: smart-contracts tracing; mobile interaction; privacy-preserving access control; digital certification; and off-chain data support. At the same time, there exists a need for the implementation of the comprehensive end-to-end system providing all of the following features: traceability with smart contracts, mobile interaction, privacy protection, reputation checking, and real-time feedback.

3. Problem Formulation And Design Objectives

The problem that needs addressing here is how to ensure that the identity of medicine can be securely validated through the whole journey between manufacturer and consumer. Each batch of medicine will have its own identity that will include details like medicine name, composition, producer, batch number, lot number, production date, expiration date, and regulations it complies with. For each batch of medicine there will be generated a QR code that will serve to identify this particular batch. A good system needs to have five guarantees: 1) medicine identity cannot be altered; 2) any change of ownership is recorded; 3) any copy of the code or its replay will be discovered; 4) only authorized participants should be able to add new information to the ledger; and 5) end users can get a timely answer of validity of the batch.

Using an authentication system that would check the scanned QR code against data stored in centralized database is not sufficient since the system can be manipulated or compromised in many ways. Pure use of public ledger will provide immutable data and will ensure that no party other than medicine manufacturer can tamper with the ledger. It will provide immutability of data but also may cause high fees due to heavy validation process or high latency. Therefore, the solution we seek here should involve permissioned ledger with some elements of decentralization where validators will be added following the certain criteria.

In order to address the issues described above, we want our system to have the following features: 1) low-latency for QR-based authentication; 2) low computing power in contrast to heavy-weight consensus algorithms; 3) regulator aware governance for drug ecosystem; 4) extension capabilities for recalls, audits, and compliance; and 5) protection against forgery and replay attacks.

4. Proposed Qr-Centric Blockchain Framework

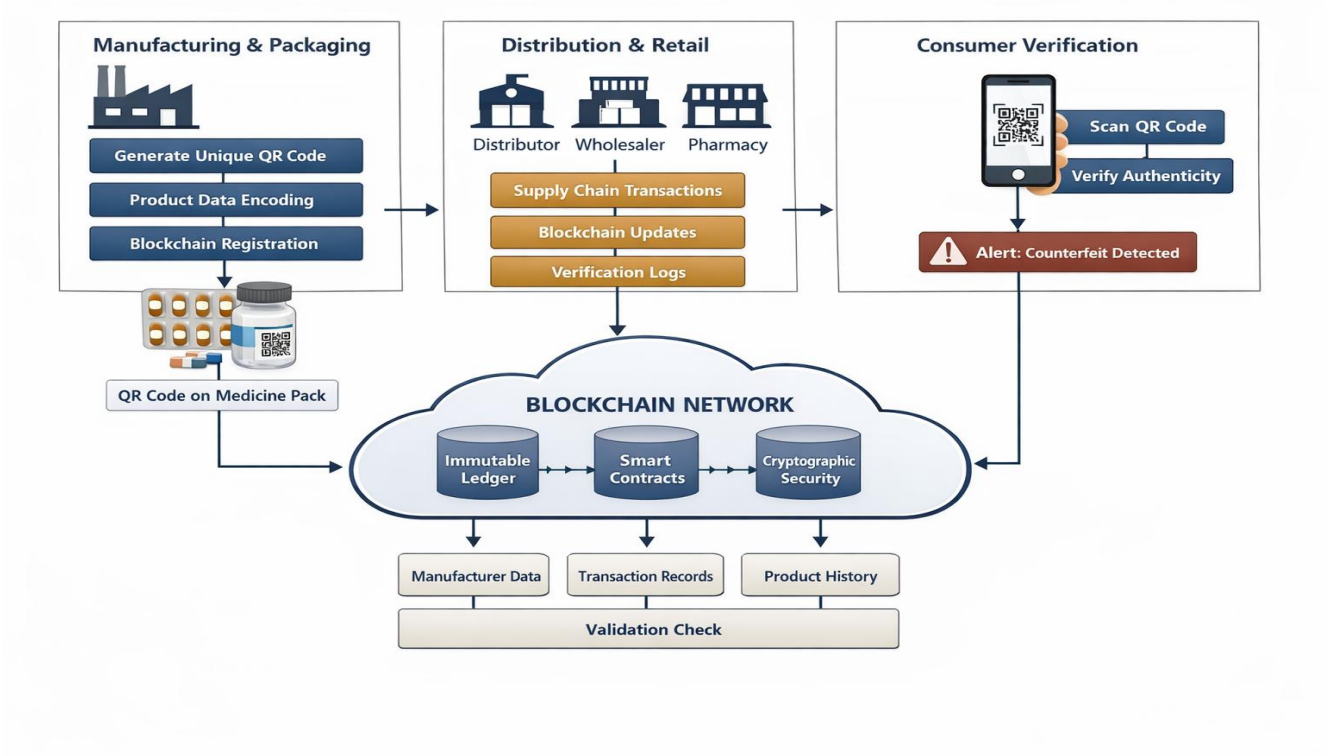

Fig. 1. Proposed QR-centric pharmaceutical traceability architecture.

A. Architectural Overview

As seen in Figure 1, the system architecture deliberately blends both on-chain and off-chain components. The manufacturers, distributors, pharmacies, and regulatory authority communicate with the permissioned blockchain ledger using smart contract services. The off-chain storage of medicine data metadata is done via a content-addressed repository, which contains the corresponding hash pointer, ownership status, approval, and audit trail on the blockchain ledger. In contrast, the QR reader or verifier acts as the user interface on the left side of the architecture.

This architecture allows the blockchain to remain small and yet maintain evidence-based strength. Everything that is needed for origin, authorization, and auditability is kept on-chain, while richer data like formulation data, certificate, or documentation can be maintained off-chain. This architecture aligns with the trajectory established in previous research on vaccine tracking and IoT logistics. [7], [11].

B. Smart-Contract Modules

Smart contracts consist of six functional modules. The registration contract holds information about batch identification, manufacturer identification, date of manufacturing, date of expiry, regulatory status, and the off-chain hash of the content. The transfer contract handles custody transfer at each step in the supply chain. The access control contract provides role-based authentication for manufacturers, distributors, pharmacies, and regulators. Quality and Compliance ContractThe quality and compliance contract is responsible for the recording of the inspection records and certificates. Finally, the audit contract provides a trace operation that reconstructs a timeline of events for the medicine batch from registration to the most recent verified ownership.

The architecture thus encompasses a broader scope than just being able to detect counterfeits. In this sense, the framework constitutes an auditable medicine event system, in which authentication, compliance, and recalls are tightly coupled. Such an outlook is relevant since counterfeit detection can be greatly enhanced by integrating it as part of the regular business record keeping process.

Table II. Smart-contract decomposition of the proposed framework.

Module	**Core function**	**Recorded state**	**Benefit**
Registration	Create batch and QR identity	Batch, lot, manufacturer, dates, CID hash	Unique product anchor
Transfer	Update authorized ownership	Current owner, transfer history	Traceable handoffs
Access control	Admit and revoke participants	Role, permissions, status	Restricted writes
Quality/compliance	Store inspection outcomes	Certificates, compliance flags	Regulatory visibility
Recall/alert	Publish incident or recall notice	Batch alert, recall reason	Rapid containment
Audit	Reconstruct chain of custody	Chronological event log	External verification

C. Hash Anchoring and QR Identity

SHA-256 is utilized in the PoAV scheme to hash medicine metadata as well as QR codes, producing unique blocks. SHA-256 produces a fixed-length hash output of 256 bits. This hashing algorithm provides high collision resistance and can easily identify any changes in the input message as the new hash output would be entirely different from that of the initial input message.

A hash of the medicine entry D is then generated and anchored on the blockchain. If H(·) represents the hash function chosen, the digest for registration will be $h = H(D)$.

For block i, the chained block hash is computed as

$h_i = H(h_{i-1} \| D_i \| metadata_i)$.

The QR code does not have to store the entire medicine entry. Rather, it stores the identity of the product, a digest pointer signature, and a token that leads to the blockchain storage location. This way, the QR code remains small in size yet fully verifiable. Any modification made to an entry after registration makes its hash value mismatch.

D. Trans-Evaluator Mutual Validation

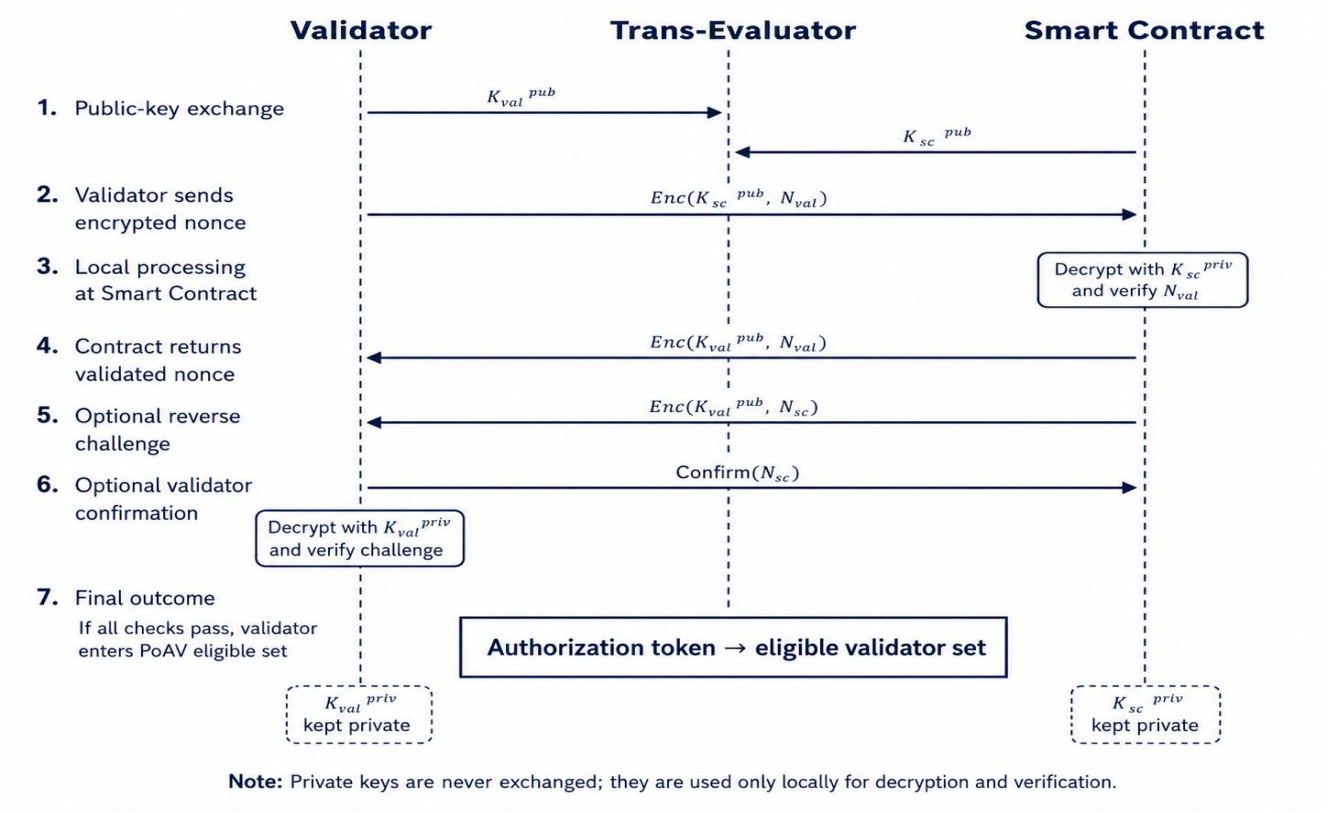

Fig. 2. Trans-Evaluator mutual-validation sequence used before block authorization.

One of the important elements of the new framework is the Trans-Evaluator, which allows carrying out a mutual validation process of the block proposer and the smart contract before creating a new block. The purpose of this approach is to ensure the involvement in the process only authorized and synchronized participants. At the stage of validators' onboarding, each of them publishes its public key but keeps the respective private key confidential. Any type of traditional public key cryptography (RSA) be used within the proposed framework.

This mutual verification process is based on the challenge-response protocol, which includes the generation of a cryptographic nonce and its encryption. The initial step of this protocol consists in generation by the validator of a nonce and its subsequent encryption with the smart contract's public key. After that, the smart contract uses its private key to decrypt the nonce and encrypts it using the validator's public key. This technique ensures validation of participants and excludes possible replay attacks. Besides, it is also possible for the smart contract to send a nonce and request validation from the proposer.

After successful authentication of both parties, block creation will be carried out. This simple but efficient method guarantees participation in the consensus process only by authorized, synchronized, and active validators. Compared to the heavyweight cryptographic handshakes, the Trans-Evaluator ensures sufficient security along with performance optimization.. The high-level interaction sequence is illustrated in Fig. 2.

E. Proof of Authentic Validation (PoAV) Validator Selection

Within the semi-centralized authority model, validators verify transactions and blocks before adding them to the blockchain. The proposed PoAV method selects them using reputation, role importance, and performance efficiency.

1) Reputation Score

The reputation score R reflects a validator’s past reliability based on successful validations, penalties, and availability. It is defined as:

$R = ((V - P) / V) \times U$ ……..**(1)**

where: V = number of successful validations P = number of penalties U = uptime (0–1)

A higher R value means the validator is more trustworthy.

2) Role Importance

The importance factor I shows how significant a validator's role.

Predefined values are assigned as follows:

- **Manufacturer: I = 0.9**
- **Distributor: I = 0.7**
- **Pharmacy: I = 0.6**

3) Efficiency Score

The efficiency score E evaluates a validator's performance based on speed and resource usage:

$E = 1 / (T \times RU)$ ……..**(2)**

where: T = average validation time RU = resource usage

Higher E values show better efficiency.

4) Composite Validator Score

The final validator score is calculated using a weighted combination:

$VS = W_r \times R + W_i \times I + W_e \times E$ ……..**(3)**

where: $W_r = 0.4$, $W_i = 0.3$, $W_e = 0.3$

5) Validator Selection Policy

Validators with the highest composite scores are selected. Only compliant validators are eligible, and the top-k validators from this group take part in each consensus round.

Algorithm : QR verification routine

Input: scanned QR token q

1. Extract (ID, Hs, Ts, Sigs) from QR token q
2. Fetch ledger state (Hb, Tb, owner, approvals) using ID
3. If Hs ≠ Hb then
4. return INVALID
5. If |Tnow − Ts| > ΔT then
6. return INVALID
7. If DuplicateScan(ID) = true then
8. return INVALID
9. If approvals < k then
10. return INVALID
11. If Verify(Sigs) = false then
12. return INVALID

13. return VALID

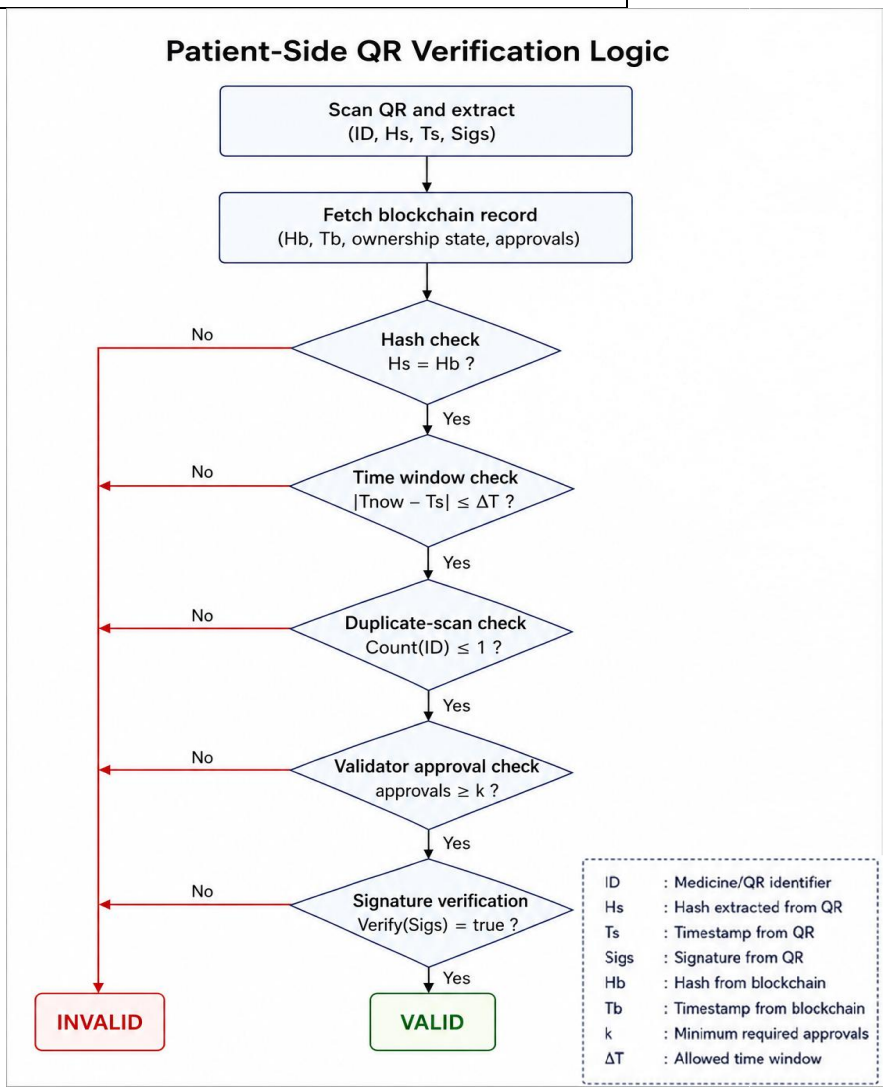

Fig. 3. Patient-side QR verification logic for medicine authenticity.

This approach targets the main vulnerability vectors in QR codes identified through prototypes: duplicated codes, replay attacks, falsified codes on counterfeit packaging, and state alteration. Using both static and dynamic analysis, the model goes beyond mere hashing validation methods.

G. Threat Model

In the threat model, it is considered that the attackers can duplicate a legitimate QR code, create an illegitimate QR token for an illegitimate package, or launch a replay attack by reusing an earlier successful scan. Another category of the attackers tries to take advantage of any possible vulnerabilities or flaws in the consensus/block authorization process by injecting stale or unauthorized validator state into it. The PoAV algorithm and Trans-Evaluator are not intended to be a panacea against all blockchain-based threats; they specifically defend against the described threats.

5. Experimental Design

A. Dataset And Prototype Setup

The prototype involves meta-data from medicines that comes from the A–Z Medicine Dataset of India. The dataset contains information about allopathy medicines like the name of the medicine, composition, manufacturing

company, price, batch, and other attributes. In the case of experiments, suitable attributes from those datasets were selected for creating structured information about the medicines along with batch attributes such as product name, manufacturer name, batch number, lot number, manufacturing date, expiration date, manufacturer location, and regulatory status.

The prototype is implemented using Java (JDK 1.8). Permissioned blockchain supports virtual nodes that can be configured between the range of 4 to 100 in number. The benchmarks include three different configurations like Ethereum, DApp, and BCoT. In addition to that, PoW and PoS protocols serve as the consensus algorithm for CPU usage, execution time, and block creation studies.

B. Evaluation Metrics and Workloads

Four sets of metrics were chosen to evaluate the implementation. First, scalability was evaluated by calculating validation requests made and processed per second for increased numbers of virtual machines. Second, the quality of QR authentication was evaluated based on direct detection results and controlled use cases of true and false uses. Third, the computational overhead was measured by using CPU usage and execution time at growing transaction numbers. Fourth, consensus response was evaluated by measuring block creation time depending on the number of validators.

There were two types of workloads chosen for analysis. One of them was a controlled-use-case workload with a known number of both true and false medicine instances that would allow evaluating the effectiveness of the QR-validation pipeline. Another one was a stress workload with a growing number of transactions and VMs to measure scalability and evaluate the real advantages of low overhead PoAV.

6. Results And Discussion

A. Scalability Under Increasing Virtual Nodes

Table III and Fig. 4 summarize the executed validation throughput for the four benchmark configurations as the number of virtual machines increases. The proposed framework starts below BCoT at the smallest scale, but its growth pattern is substantially steeper and more stable as the environment scales. At 20 virtual machines, the proposed framework executes 257 validation requests per second, already outperforming Ethereum and DApp. At 50 virtual machines, it reaches 369 executed requests per second, and at 100 virtual machines it achieves 372 executed requests per second, exceeding Ethereum (342), DApp (274), and BCoT (197).

Table III. Executed validation requests per second under increasing virtual machines.

VMs	Ethereum	DApp	BCoT	Proposed
10	98	92	201	119
20	145	141	202	257
30	215	201	198	326
40	301	226	199	355
50	302	246	198	369
100	342	274	197	372

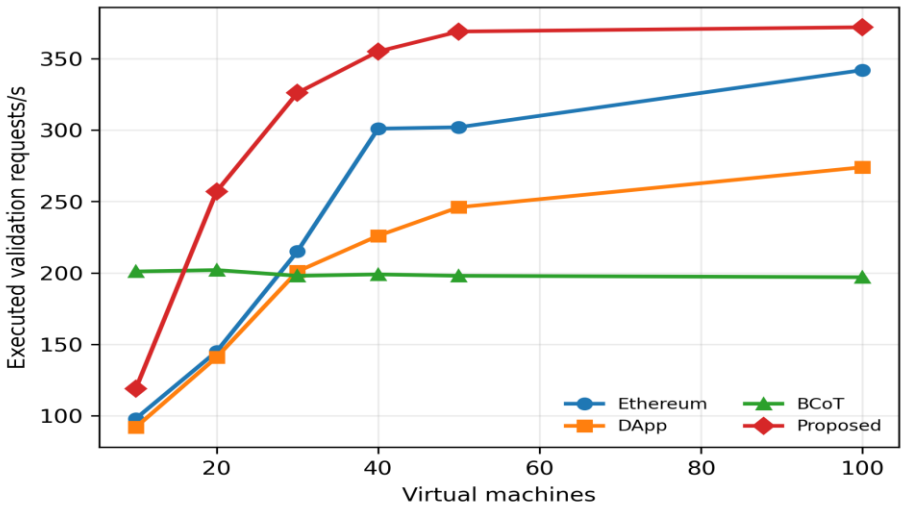

Fig. 4. Executed Validation Requests vs. Number of Virtual Machines

The result has two implications. First, the permissioned design avoids the bottleneck associated with heavyweight public-chain validation for last-mile medicine authentication. Second, the new architecture does not only gain from reduced overhead but also maintains scaling efficiency when new validator nodes are introduced. BCoT, on the other hand, has a nearly flat graph and hence performs closer to a bounded baseline than an efficient execution engine.

B. Controlled Use Cases and Direct Fake-QR Detection

In table 4, Controlled-use case analysis was done over 10-100 cases with real drugs and fake drugs. In this case, the framework was successful in detecting both real drugs and fake drugs, achieving an accuracy rate of 100%. This indicates that the checks on hashes, timestamps, duplicate scans, approval and signatures are logically consistent.

Table IV. Controlled-use-case QR validation results for genuine and counterfeit medicines.

Use cases	Genuine	Detected	Fake	Detected	Accuracy
10	9	9	1	1	100%
20	18	18	2	2	100%
50	45	45	5	5	100%
80	65	65	15	15	100%
100	90	90	10	10	100%

Another experiment was conducted to test the detection performance of the framework in comparison to the Ethereum benchmark, DApp benchmark, and BCoT benchmark under the number of transactions set to 10, 50, 100, 200, and 500. In table 5 & fig. 5 all cases with 50, 100, and 200 transactions, the proposed framework is capable of detecting all fake QR codes. The detection rate is still 98.8 percent even when the number of transactions rises to 500.

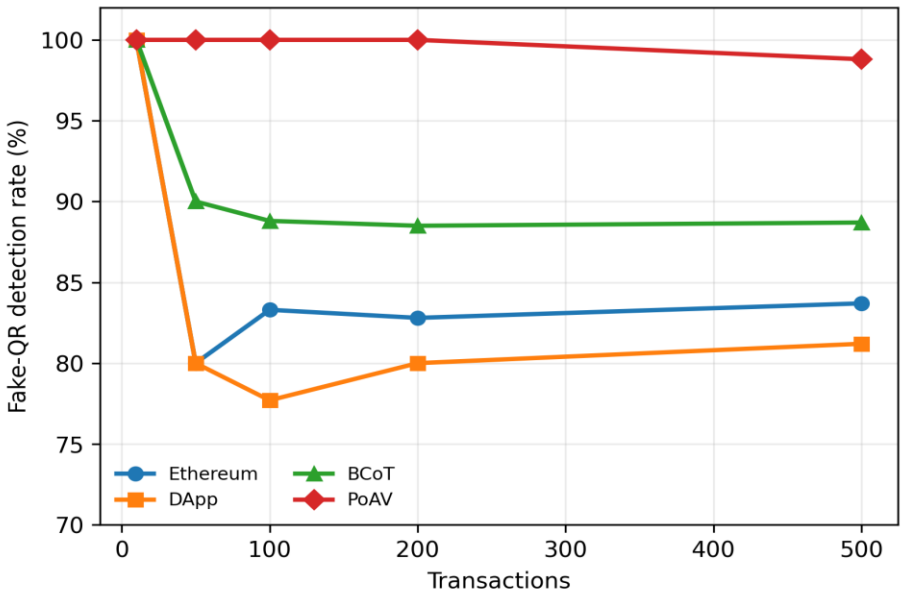

Fig. 5. Detection rate of Fake-QR with increasing transaction rates.

Table V Direct fake-QR detection rate across benchmark configurations.

Transactions	**Ethereum**	**DApp**	**BCoT**	**PoAV**
10	100%	100%	100%	100%
50	80%	80%	90%	100%
100	83.3%	77.7%	88.8%	100%
200	82.8%	80%	88.5%	100%
500	83.7%	81.2%	88.7%	98.8%

This superiority compared to other techniques is noteworthy because detecting fake QR codes is more important than merely processing the transactions. From the data provided, it is apparent that introducing duplicate-scan checks and status conditions would significantly enhance the robustness of the framework as the number of transactions grows. In layman's terms, the new framework will not just become more efficient in handling transactions, but it will also be less prone to identifying a fraudulent or duplicated QR code.

C. Resource Efficiency and Responsiveness to Consensus Changes

This is because the validation of PoAV algorithm doesn't require the use of GPU since its processes will mainly involve QR hash check, timestamp check, duplicate check, validator verification, and digital signature verification which aren't resource intensive and easily carried out using CPU.

Another set of tests conducted involved comparing PoW, PoS, and PoAV while varying the number of transactions processed from 10 to 500(in table 6 and fig. 6). It becomes evident from the data that PoAV performs better than its competitors with regard to CPU consumption and transaction execution time. For instance, PoW starts with 80% CPU usage and 10 seconds per transaction at 10 transactions and rises to 95% and 20 seconds respectively at 500 transactions. On the other hand, PoAV remains within the range of 10% to 30% CPU usage and 2 seconds to 4 seconds per transaction. PoS falls between those two.

Table VI. CPU usage and execution time across consensus baselines.

Transactions	Consensus	CPU (%)	Time (s)
10	PoW	80	10
10	PoS	40	5
10	PoAV	10	2
100	PoW	85	12
100	PoS	50	6
100	PoAV	15	2.5
200	PoW	90	15
200	PoS	55	7
200	PoAV	20	3
500	PoW	95	20
500	PoS	60	8
500	PoAV	30	4

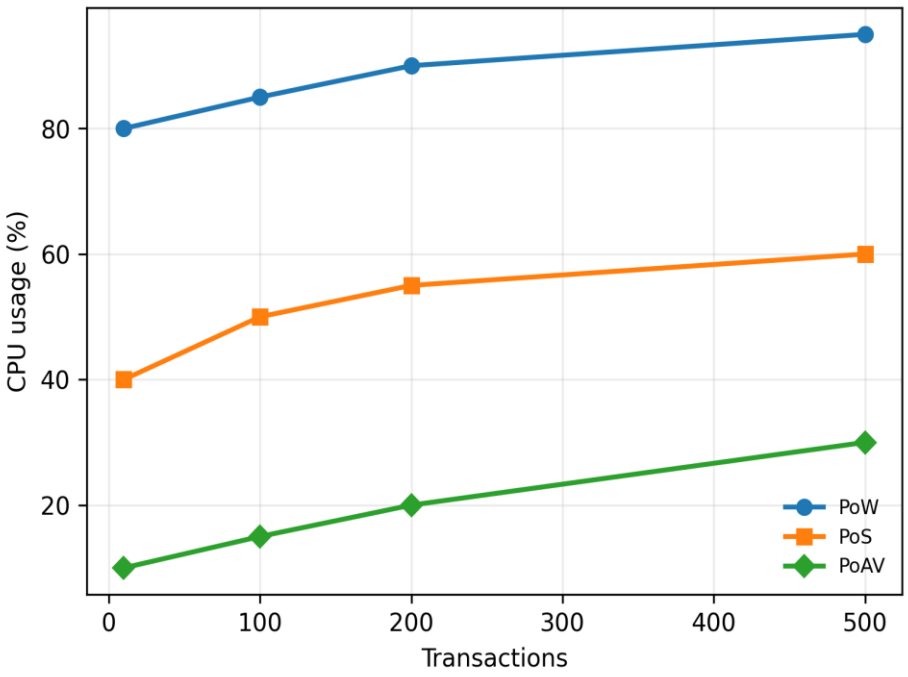

Fig. 6. CPU usage comparison across PoW, PoS, and PoAV.

In fig. 7, The validator-count experiment shows a similar result. With 10 validators, PoW, PoS, and PoAV take about 60 s, 20 s, and 5 s to create a block. With 100 validators, times reduce to 20 sec, 10 sec, and 3 sec. This

shows that PoAV has low block-creation latency even as the validator increased.

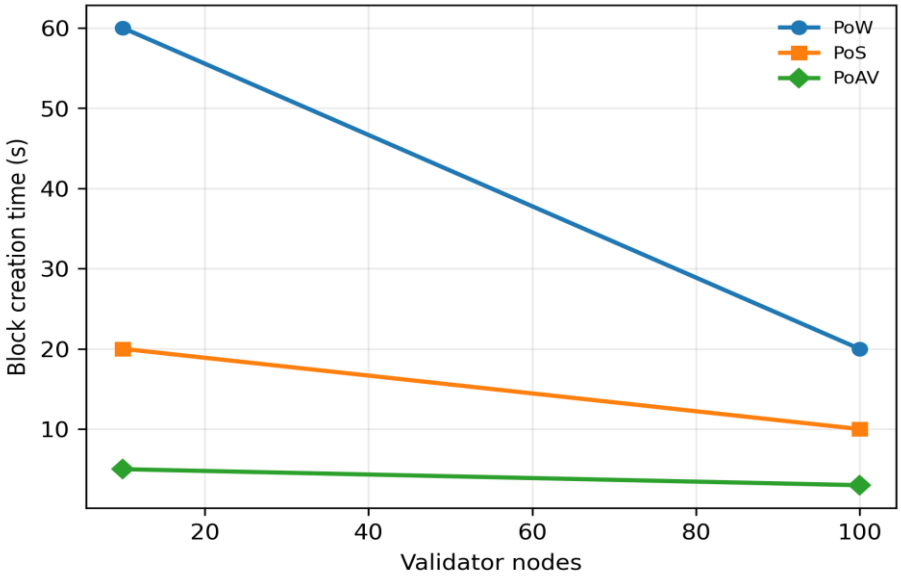

Fig. 7. Block creation time across validator-set sizes.

D. Security Interpretation

Quantitative findings are consistent with the qualitative security design. Hash anchoring defends against silent record manipulation. Timestamp intervals discourage replay attacks. Duplicate scanning increases scrutiny when QR identity reuse occurs for incompatible transactions. Role-specific contracts and regulator inclusion prevent malicious writings. Lastly, the Trans-Evaluator mitigates the threat of an unverified proposer engaging in block generation without establishing cryptographic liveness within the existing trust zone.

Operationally, the framework also enhances auditability. As all registration, transfer, quality incident, approval, and recall records are available through an immutable ledger, regulators and pharmacies may investigate disputes more efficiently than in distributed database systems. This is congruent with general supply chain research that highlights transparency, provenance, and automated verification as blockchain advantages.[8], [12], [14].

Table VII. Threats addressed by the proposed framework.

Threat	**Primary control**	**Expected effect**
Copied QR code	Duplicate-scan history + ownership lookup	Raises anomaly flag when the same identity appears in incompatible contexts
Replay attack	Timestamp window check	Rejects late or repeated reuse of previously valid QR payloads
Forged QR token	Hash anchoring + digital signature verification	Invalidates codes that do not match the registered on-chain state
Unauthorized ledger update	Role-based access control	Prevents writes from non-admitted participants
Stale or malicious proposer	Trans-Evaluator mutual validation	Allows block proposal only after cryptographic liveness is proven

7. Managerial, Regulatory, And Deployment Implications

The practical relevance of the proposed framework stems from its ability to shift the responsibility of verification throughout different links in the pharmaceutical supply chain. Pharmaceutical companies receive tamper-evident product anchors upon creating a batch, distributors and pharmacies benefit from standardized and

traceable transfer records instead of disjointed paper-based or even database-driven procedures. Patients can access their own product verification without resorting to opaque third-party services. Regulatory agencies, finally, have access to an audit trail of events to facilitate their operations of recall management and dispute resolutions. All these benefits are in line with other blockchain supply chain papers that highlight transparency, shared data visibility, accountability, and lower search costs as main sources of operational value [8], [12], [19].

Three governance-related aspects deserve special attention when deploying the framework in practice. First, admission to the network needs to be policy-driven since unlike public blockchain systems, regulated healthcare settings cannot afford the luxury of fluid validators' identity. Hence, the proposed PoAV protocol is intended to assume an admission layer that allows only authorized parties such as manufacturers, distributors, pharmacies, and even authorized quality institutions to participate in the validation process. Second, a policy for handling alerts must be designed since duplicated or replayed scans of QRs do not necessarily imply counterfeiting especially with regards to situations when connectivity may be inconsistent. Thus, it is reasonable to introduce graded alert levels such as warning, suspicious, and high-risks alerts to increase interpretability. Third, the new solution must interoperate with regulatory workflows to ensure that exported audit trails and structured alerts are available for managing recall actions, monitoring adverse reactions, and ensuring compliance.

From the cost side, the proposed framework has many practical benefits. According to the results obtained in the experiments, it is possible to achieve efficient confirmation times without excessive computational costs typical for PoW systems. It is particularly useful for organizations such as hospitals or small pharmacy networks that may struggle with maintaining high computational power. In addition, the proposed solution enables phased deployment where initial batch registration and transfer tracking may be deployed first and followed by patient verification and automated recalls later.

A separate area of consideration is the user experience. Patients and pharmacists should not be expected to understand the specifics of consensus algorithms to make sense of verification results. Therefore, the application UI must reflect the status of a product as simple states such as valid, expired, suspiciously duplicated, and regulator-alerted. It is one of those cases when the separation of backend complexity and frontend simplicity is extremely important.

Lastly, it is necessary to point out that there is a regulatory trade-off in the proposed framework. While permissioned blockchains are much better in terms of improved governance and faster responses, they require reaching consensus and designing explicit policies of validators' participation, conflict resolution, and system maintenance. However, it is a perfectly acceptable move for pharmaceutical supply chains in which regulation is an integral part anyway.

8. Limitations And Future Work

The current paper has several limitations. First of all, the evaluation is limited to a prototypical environment and not a real-world deployment of the system involving multiple pharmaceutical stakeholders. Second, even though the benchmarks include Ethereum, DApp, and BCoT, internal configuration details of BCoT are not specified. Finally, while use-case simulations were used to evaluate performance, real-world deployment would have been more informative.

Possible future work includes:

1. Performing formal security analysis of the proposed Trans-Evaluator protocol;
2. Conducting tests in a production-ready permissioned blockchain network with independent validator organizations;
3. Incorporating advanced anomaly detection techniques based on geo-temporal QR scan patterns;
4. Maintaining large-scale content-addressed off-chain storage; and
5. Ensuring interoperability with regulatory reporting systems and mobile healthcare applications.

9. Conclusion

The paper introduces a light-weight QR-based blockchain system for counterfeit pharmaceutical detection. In addition to smart-contract-based traceability, permissioned ledger, patient-facing QR verification, Trans-Evaluator algorithm, and custom PoAV consensus mechanism, the system enables a practical and scalable alternative to centralized verification services and costly public blockchain systems.

The experimental results prove three main facts about the proposed solution. First, the validation throughput is quite scalable as more virtual nodes are added to the network. Second, high performance in counterfeit detection is demonstrated when validation load grows with perfect accuracy achieved under controlled-use-case scenarios. Finally, CPU usage, execution times, and latency of block creation is substantially lower compared to PoW and PoS baselines. All together, it proves that permissioned, regulator-aware blockchain systems are technically feasible and efficient in terms of operations for pharmaceuticals' real-time authentication.

In conclusion, QR pharmaceutical traceability cannot be treated just as an innovation for package labeling. When combined with a permissioned blockchain that captures events of product identity, ownership, validation, and recall, QR verification becomes an advanced and clinically actionable safety measure.

References

1. I. A. Omar, R. Jayaraman, M. S. Debe, K. Salah, I. Yaqoob, and M. Omar, “Automating procurement contracts in the healthcare supply chain using blockchain smart contracts,” IEEE Access, vol. 9, pp. 37397–37409, 2021.
2. A. Musamih, K. Salah, R. Jayaraman, J. Arshad, M. Debe, Y. Al-Hammadi, and S. Ellahham, “A blockchain-based approach for drug traceability in healthcare supply chain,” IEEE Access, vol. 9, pp. 9728–9743, 2021.
3. G. Subramanian, A. S. Thampy, N. V. Ugwuoke, and B. Ramnani, “Crypto Pharmacy – Digital Medicine: A Mobile Application Integrated With Hybrid Blockchain to Tackle the Issues in Pharma Supply Chain,” IEEE Open Journal of the Computer Society, vol. 2, 2021, doi: 10.1109/OJCS.2021.3049330.
4. K. Gai, Y. Zhang, M. Qiu, and B. Thuraisingham, “Blockchain-Enabled Service Optimizations in Supply Chain Digital Twin,” IEEE Transactions on Services Computing, vol. 16, no. 3, pp. 1673–1685, 2023.
5. I. A. Omar, R. Jayaraman, M. S. Debe, H. R. Hasan, K. Salah, and M. Omar, “Supply Chain Inventory Sharing Using Ethereum Blockchain and Smart Contracts,” IEEE Access, vol. 10, pp. 2345–2356, 2022.
6. A. Musamih, I. Yaqoob, K. Salah, R. Jayaraman, M. Omar, and S. Ellahham, “Using NFTs for Product Management, Digital Certification, Trading, and Delivery in the Healthcare Supply Chain,” IEEE Transactions on Engineering Management, early access, 2022.
7. L. Cui, Z. Xiao, F. Chen, H. Dai, and J. Li, “Protecting Vaccine Safety: An Improved, Blockchain-Based, Storage-Efficient Scheme,” IEEE Transactions on Cybernetics, vol. 53, no. 6, pp. 3588–3598, 2023.
8. U. Agarwal, V. Rishiwal, S. Tanwar, R. Chaudhary, G. Sharma, P. N. Bokoro, and R. Sharma, “Blockchain Technology for Secure Supply Chain Management: A Comprehensive Review,” IEEE Access, vol. 10, pp. 85493–85517, 2022.
9. Y. Madhwal, Y. Borbon-Galvez, N. Etemadi, Y. Yanovich, and A. Creazza, “Proof of Delivery Smart Contract for Performance Measurements,” IEEE Access, vol. 10, pp. 69147–69159, 2022.
10. R. D. Garcia, G. S. Ramachandran, R. Jurdak, and J. Ueyama, “Blockchain-Aided and Privacy-Preserving Data Governance in Multi-Stakeholder Applications,” IEEE Transactions on Network and Service Management, vol. 19, no. 4, pp. 3781–3793, 2022.
11. C. Yang, S. Lan, Z. Zhao, M. Zhang, W. Wu, and G. Q. Huang, “Edge-Cloud Blockchain and IoE-Enabled Quality Management Platform for Perishable Supply Chain Logistics,” IEEE Internet of Things Journal, vol. 10, no. 4, pp. 3264–3277, 2023.
12. P. M. Reyes, M. J. Gravier, P. Jaska, and J. K. Visich, “Blockchain Impacts on Global Supply Chain Operational and Managerial Business Value Processes,” IEEE Engineering Management Review, vol. 50, no. 3, pp. 123–140, 2022.
13. R. Z. Rasi, U. S. B. Rakiman, R. Z. Raja Mohd. Radzi, N. R. Masrom, and V. P. K. Sundram, “A Literature Review on Blockchain Technology: Risk in Supply Chain Management,” IEEE Engineering Management Review, vol. 50, no. 1, pp. 186–200, 2022.
14. H. R. Hasan, K. Salah, I. Yaqoob, R. Jayaraman, S. Pesic, and M. Omar, “Trustworthy IoT Data Streaming Using Blockchain and IPFS,” IEEE Access, vol. 10, pp. 17707–17721, 2022.
15. S. Pattanayak, R. M. Arputham, M. Goswami, and N. P. Rana, “Blockchain Technology and Its Relationship With Supply Chain Resilience: A Dynamic Capability Perspective,” IEEE Transactions on Engineering Management, early access, 2023.
16. S.-J. Hsiao and W.-T. Sung, “Blockchain-Based Supply Chain Information Sharing Mechanism,” IEEE Access, vol. 10, pp. 78875–78886, 2022.
17. D. Hawashin, K. Salah, R. Jayaraman, I. Yaqoob, and A. Musamih, “A Blockchain-Based Solution for Mitigating Overproduction and Underconsumption of Medical Supplies,” IEEE Access, vol. 10, pp. 71669–71682, 2022.
18. P. Saranya and R. Maheswari, “Proof of Transaction (PoTx) Based Traceability System for an Agriculture Supply Chain,” IEEE Access, vol. 11, pp. 10623–10636, 2023.

19. Q. Zhu, Y. Sun, S. K. Mangla, S. Arisian, and M. Song, “On the Value of Smart Contract and Blockchain in Designing Fresh Product Supply Chains,” IEEE Transactions on Engineering Management, early access, 2023.
20. Shudhanshu Singh, “A–Z Medicine Dataset of India,” Kaggle dataset. [Online]. Available: https://www.kaggle.com/datasets/shudhanshusingh/az-medicine-dataset-of-india/data
21. Dutta, P.; Choi, T.M.; Somani, S.; Butala, R. Blockchain Technology in Supply Chain Operations: Applications, Challenges and Research Opportunities. Transp. Res. Part E Logist. Transp. Rev. 2020, 142, 102067. [PubMed]
22. Paliwal, V.; Chandra, S.; Sharma, S. Blockchain Technology for Sustainable Supply Chain Management: A Systematic Literature Review and a Classification Framework. Sustainability 2020, 12, 7638.
23. Patil, S. S., & Rosemaro, E. (2025). Blockchain-Based Smart Contracts: Implementation and Security Considerations. International Journal on Advanced Computer Engineering and Communication Technology, 12(2), 8–13. https://doi.org/10.65521/ijacect.v12i2.138
24. Vistro, D.M.; Farooq, M.S.; Rehman, A.U.; Sultan, H. Applications and Challenges of Blockchain with IoT in Food Supply Chain Management System: A Review. In Proceedings of the 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021), Bangalore, India, 6–7 August 2021; Volume 4, pp. 596–605.
25. Hussain, M.; Javed, W.; Hakeem, O.; Yousafzai, A.; Younas, A.; Awan, M.J.; Nobanee, H.; Zain, A.M. Blockchain-Based IoT Devices in Supply Chain Management: A Systematic Literature Review. Sustainability 2021, 13, 3646.
26. Pradeep, V.; Yajnesh, R.; Moolya, S.; Yash, S.; Thirtha. A Review of Blockchain-Based Supply Chain Management: Applications, Challenges and Research Opportunities. Int. J. Adv. Res. Sci. Commun. Technol. 2023, 3, 106–109.
27. Deepa, N.; Pham, Q.V.; Nguyen, D.C.; Bhattacharya, S.; Prabadevi, B.; Gadekallu, T.R.; Maddikunta, P.K.R.; Fang, F.; Pathirana, P.N. A survey on blockchain for big data: Approaches, opportunities, and future directions. Future Gener. Comput. Syst. 2022, 131, 209–226.
28. Kassen, M. Blockchain and e-government innovation: Automation of public information processes. Inf. Syst. 2022, 103, 101862.