Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

A Distributor-Centric Blockchain Framework for Regulatory-Aware Pharmaceutical Supply Chain Verification

Deepa B
Associate Professor
Computer Science and Engineering
Rajalakshmi Engineering College
Chennai, India

Sowbarnigaa Sridharan
Student
Computer Science and Engineering
Rajalakshmi Engineering College
Chennai, India

Soundarylakshmi S
Student
Computer Science and Engineering
Rajalakshmi Engineering College
Chennai, India

Siva Bharathi K
Student
Computer Science and Engineering
Rajalakshmi Engineering College
Chennai, India

Abstract - The pharmaceutical supply chain faces significant challenges from counterfeit, expired, recalled, and regulatory-prohibited medicines reaching patients. Existing verification systems mainly rely on centralized databases and conventional record-keeping, which may provide limited traceability, fragmented information, and delayed regulatory enforcement. This paper proposes a Distributor-Centric, Regulatory-Aware Blockchain Enforcement System for Pharmaceutical Verification to improve medicine traceability and regulatory compliance across the distributor–pharmacy–patient workflow. Each medicine is identified using a unique QR code and verified based on product and batch existence, expiry status, ownership, regulatory status, and supply-chain history. A dedicated regulatory database maintains the current status of medicines and batches, while blockchain provides a tamper-resistant record of critical events such as receiving, transferring, blocking, and dispensing. Smart contracts enforce predefined rules to prevent expired, unauthorized, recalled, prohibited, or invalid medicines from progressing through the supply chain. Pharmacies can perform additional verification, while patients can independently scan the QR code to check medicine information. The proposed framework provides an auditable and transparent approach to pharmaceutical verification and can be evaluated using valid, counterfeit, expired, duplicate, and prohibited medicine scenarios.

Keywords - Blockchain, pharmaceutical supply chain, counterfeit drug detection, smart contracts, QR code verification, regulatory compliance, CDSCO, traceability.

I. INTRODUCTION

The pharmaceutical supply chain is one of the most safety-critical logistics networks in existence, directly determining patient health outcomes. In India, ensuring that only genuine, valid, and regulatory-compliant medicines reach patients remains a persistent challenge, as counterfeit, expired, recalled, and prohibited drugs continue to surface within distribution networks, sometimes reaching pharmacies and patients before enforcement action takes effect. These failures stem from structural weaknesses in how pharmaceutical movement is tracked and enforced across independent stakeholders, each typically operating with its own records and limited visibility into others' data.

Current traceability approaches rely predominantly on centralized databases and manual record-keeping, which present a single point of failure vulnerable to tampering, propagate regulatory updates slowly since no automated link exists between CDSCO notifications and inventory status, and leave information fragmented across participants including patients, who have no independent way to verify a medicine's authenticity at purchase.

Blockchain technology offers a tamper-resistant, shared ledger for supply-chain traceability, but many existing pharmaceutical proposals store all data on-chain and treat regulatory status as static rather than continuously updated, failing to reflect how a medicine's status can change abruptly after a recall.

This paper proposes a Distributor-Centric, Regulatory-Aware Blockchain Enforcement System built on three principles: (1) verification spans the distributor–pharmacy–patient workflow, checking every custody transition; (2) regulatory decision-making is separated from blockchain storage — a continuously updatable database tracks each batch's status (permitted, restricted, prohibited, recalled, or unknown) from CDSCO notifications, while the blockchain records and enforces supply-chain events; and (3) smart contracts automate enforcement, validating transactions against expiry, ownership, and regulatory status, and halting movement of any batch whose status changes after entering the chain.

Each medicine carries a unique QR code enabling verification at every stage: distributors check incoming stock, pharmacies verify before dispensing, and patients can independently scan a code to view a medicine's status, extending transparency to the final link in the chain.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

II. LITERATURE REVIEW

Counterfeit and substandard medicines remain one of the most serious unresolved threats to global healthcare. According to the World Health Organization, an estimated one in ten medical products circulating in low- and middle-income countries is either substandard or falsified, costing health systems close to US$30.5 billion annually in wasted spending and, more critically, contributing to treatment failure, antimicrobial resistance, and preventable deaths [9], [10]. WHO's global surveillance data further shows that the majority of reported cases involve antimalarials and antibiotics, and that reporting itself remains inconsistent across regions, with large gaps in detection technology and regulatory follow-through even after a problematic product has been identified [11], [12]. Disease-specific studies reinforce this pattern: research on anti-tuberculosis medicines found that weak post-market surveillance repeatedly allows substandard or unregistered drugs to remain in circulation well after regulatory bodies have acted against them [13]. Taken together, this body of evidence establishes an important point that motivates the present work — the problem of unsafe medicines is not confined to the manufacturing stage. A product can be legitimate when it enters the supply chain and still become dangerous or non-compliant later, once a recall, ban, or safety alert is issued. Any verification system, therefore, needs to treat compliance as something that is checked continuously, not something confirmed only once.

Blockchain technology has become the dominant technical response to this problem over the past several years, largely because its immutability and decentralized structure make it well suited to recording tamper-proof supply-chain history. Early implementations combined blockchain with QR-code-based product identification to trace a medicine's movement from manufacturer to consumer, allowing any deviation in the recorded chain of custody to be detected [6]. This general pattern — pairing a distributed ledger with a scannable product identifier — has since been repeated and refined across a wide range of systems. Some frameworks emphasize ownership-transfer logging between manufacturers, distributors, and retailers to prevent unauthorized alteration of transaction records [1], [2], while others extend the same underlying idea into full provenance-verification pipelines that track a drug continuously from production through to dispensing [4]. A parallel line of work has adapted this architecture to permissioned blockchain networks such as Hyperledger Fabric, prioritizing controlled access among known pharmaceutical industry participants over open public verification [3]. Complementary systems have also integrated IoT sensor data into the blockchain layer, extending counterfeit detection to cover cold-chain violations for temperature-sensitive drugs and vaccines [5]. More recent work has pushed the QR-code layer itself further, embedding cryptographic protection directly into pharmaceutical packaging to resist cloning and duplication of physical identifiers, and combining this with patient-facing authentication interfaces broadly similar to the role-based verification model adopted in the proposed system [23], [24].

What becomes clear across this cluster of work is a shared architectural assumption: verification is treated as validating a product against its own recorded transaction history. A scanned medicine is checked to see whether its batch, serial number, and ownership chain are internally consistent — and if they are, the product is considered trustworthy. Broader surveys of the field confirm that this is the prevailing design pattern rather than an isolated choice, and several explicitly flag it as a limitation: a tamper-resistant ledger can prove that a product's recorded history has not been altered, but it cannot, on its own, tell you whether that product is still legally permitted to be sold today [7], [8]. In other words, traceability and regulatory compliance are treated as separate concerns in most existing systems, even though a fully trustworthy verification result depends on both.

This gap is echoed in systematic reviews of blockchain applications across the wider healthcare domain. Reviews spanning patient-record management, data integrity, and drug traceability consistently find that most blockchain-healthcare implementations remain prototype-stage deployments rather than production systems integrated with authoritative external data sources [14], [15]. More recent reviews of blockchain-based health information systems reach a similar conclusion, and further identify machine-learning-based anomaly detection as a promising but still underexplored direction for strengthening verification beyond fixed, rule-based checks [16]–[18]. This observation is directly relevant to the proposed system's future-work trajectory, since anomaly detection over serial-number usage and transaction patterns is identified as a natural next step once the core regulatory-synchronization architecture is established.

Because the proposed system, like the works discussed above, relies on Solidity smart contracts to enforce supply-chain operations such as batch registration and blocking, the reliability of the contract layer itself is also a relevant design concern. Security surveys of Ethereum smart contracts catalogue recurring vulnerability classes — reentrancy, integer overflow, and access-control flaws among them — and the static and dynamic analysis techniques developed to detect them before deployment [19]–[22]. These surveys are useful less as verification solutions in themselves and more as a checklist of failure modes to guard against when designing enforcement-critical contract logic, since a compromised smart contract would undermine the trust the rest of the system depends on.

Finally, on the regulatory side, the Central Drugs Standard Control Organisation's Drugs Rules mandate QR-code and barcode labelling for pharmaceutical products under Schedule H2 [25]. This regulation is significant because it establishes the compliance basis for using QR-based identification in the Indian context — but it defines only a labelling requirement, not a technical architecture for how that QR code should be verified against evolving regulatory status once a product is in the market.

Synthesizing across these strands of literature reveals a consistent pattern rather than a set of unrelated gaps: the scale-of-problem studies [9]–[13] show that danger persists after market entry; the blockchain traceability systems [1]–[8], [23], [24] verify identity and history but not current legal status; the systematic reviews [14]–[18] confirm this is a field-wide tendency rather than an isolated oversight; the smart contract security literature [19]–[22] addresses a necessary but separate layer of trust; and the regulatory framework [25] defines the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

labelling obligation without specifying how it should be enforced dynamically. The proposed system is positioned directly at the intersection of these gaps. By pairing a Regulatory Data Synchronization Module — which continuously ingests updated prohibition, recall, and alert information — with a multi-factor Verification and Enforcement Engine that checks serial validity, expiry, ownership, supply-chain history, and regulatory status together, the system extends the blockchain traceability model reviewed above into one capable of flagging a medicine that was valid yesterday but has since become non-compliant, closing the specific gap that recurs throughout the surveyed literature.

III. METHODOLOGY

The proposed system implements a distributor-centric, regulatory-aware blockchain framework for verifying pharmaceutical products at any point after they enter the market. Unlike traceability-only systems, it re-evaluates a product's regulatory and supply-chain status every time it is scanned, allowing previously valid medicines to be flagged if they later become expired, recalled, or prohibited, as illustrated in Fig. 1.

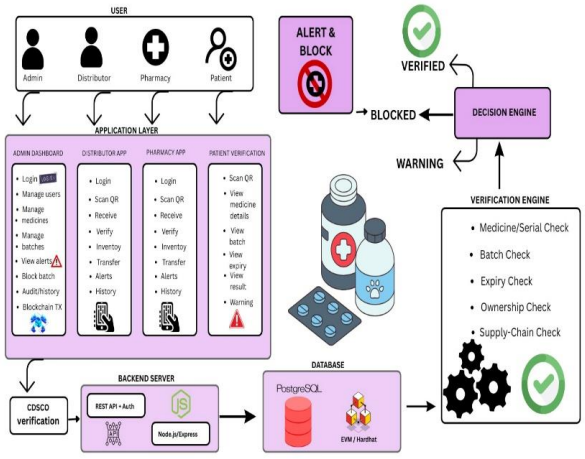

Fig. 1. Architecture diagram of the proposed distributor-centric, regulatory-aware blockchain verification system.

A. System Architecture The architecture involves four entities — distributor, pharmacy, patient, and administrator — connected through a centralized backend. Each medicine is identified via QR/barcode data (medicine name, batch number, serial number, manufacturing/expiry date). Scans are sent to a Verification and Enforcement Engine, which returns one of three outcomes: VERIFIED, WARNING, or BLOCKED.

B. Regulatory Data Synchronization A dedicated module maintains a regulatory knowledge base sourced from authoritative bodies (e.g., CDSCO), covering prohibited/banned drugs, recalls, and alerts. Data passes through collection, extraction, normalization, and storage stages before being stored in PostgreSQL, with statuses such as APPROVED, RESTRICTED, PROHIBITED, RECALLED, or UNKNOWN.

C. Medicine Registration and QR Verification Each medicine/batch is linked to a QR or barcode. On scanning, the identifier is decoded and matched against PostgreSQL records. This enables repeated verification at multiple lifecycle stages: receiving, transferring, dispensing, and patient-level checks.

D. Verification and Enforcement Engine The engine applies the following sequential checks:

1) Medicine/Serial Check — validity and duplication of serial numbers
2) Expiry Check — comparison with current date
3) Regulatory Check — cross-reference with the regulatory database
4) Ownership/Inventory Check — authorization of the requesting organization
5) Blockchain Traceability Check — consistency with recorded transaction history

A decision function combines these checks, as shown in (1):

$$Decision = f(Serial, Expiry, Regulatory, Ownership, Blockchain) \quad (1)$$

Critical failures (regulatory violation, expiry) yield BLOCKED; minor inconsistencies yield WARNING; passing all checks yields VERIFIED.

E. Regulatory Enforcement Mechanism If a regulatory authority later prohibits or recalls a batch already in circulation, the updated regulatory status takes precedence over prior supply-chain approval on the next scan, triggering a BLOCKED result and alert — independent of blockchain history.

F. Blockchain Traceability Module An Ethereum-compatible network (Hardhat for local testing) with a Solidity smart contract records batch registration, receipt, transfer, blocking, and dispensing events. Only minimal traceability data (batch ID, hash, sender/receiver, event type, timestamp) is stored on-chain; sensitive data remains off-chain. The backend interacts with the contract via ethers.js, storing resulting transaction hashes in PostgreSQL.

G. Alert and Enforcement Module Alerts are generated for conditions such as prohibited/recalled products, expired medicines, duplicate serials, ownership mismatches, and supply-chain inconsistencies. Administrators can review and investigate flagged records through a centralized dashboard.

H. Role-Based Application Module Role-based access control (RBAC) governs access: distributors and pharmacies manage receiving, transferring, dispensing, and inventory; patients get a simplified public verification view; administrators manage regulatory records, users, alerts, and blockchain monitoring.

I. Security and Audit Mechanism JWT-based authentication, hashed password storage, RBAC, input validation, and audit logging secure the application layer. Blockchain private keys are isolated from user-facing components, and every verification/enforcement action is logged for accountability.

J. End-to-End Workflow The complete verification cycle proceeds as follows:

Medicine in Market → QR/Barcode Scan → Product Identification → Regulatory Lookup → Expiry Check → Serial Check → Blockchain Check → Decision Engine → VERIFIED/WARNING/BLOCKED → Alert & Audit Record

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

IV. RESULTS AND ANALYSIS

The implementation results confirm that the proposed system successfully performs multi-parameter pharmaceutical verification rather than relying on a single QR-code identifier. Test scenarios covering valid medicines, expired products, invalid and duplicate serial numbers, and supply-chain transactions demonstrated that the Verification and Enforcement Engine correctly classified outcomes into VERIFIED, WARNING, and BLOCKED states. The blockchain layer reliably recorded all supply-chain events — registration, receiving, transfer, blocking, and dispensing — with each transaction producing a verifiable hash stored alongside the corresponding PostgreSQL record, as shown in Fig. 3. This confirms that the hybrid architecture, combining off-chain application data with on-chain traceability, functions as intended without imposing unnecessary storage overhead on the blockchain.

Overall, the analysis shows that integrating QR-based identification, rule-based verification logic, and blockchain traceability provides a more comprehensive and tamper-resistant mechanism for detecting counterfeit, expired, or inconsistent pharmaceutical products compared to conventional QR-only systems. However, since testing was limited to a controlled environment with a small dataset and transaction volume, the results primarily validate functional correctness rather than real-world scalability. Further evaluation involving larger datasets, concurrent multi-organization transactions, and performance metrics such as latency, throughput, and gas consumption is necessary before the system can be considered ready for production deployment.

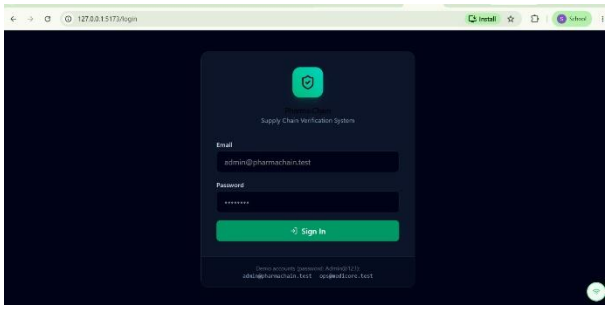

Fig. 2. Sign-in interface of the PharmaChain supply-chain verification application.

The application was evaluated across its distributor, administrator, and patient-facing interfaces. Fig. 2 shows the sign-in interface used to authenticate registered distributor and administrator accounts before any inventory or verification action can be performed. Fig. 4 shows the CDSCO Regulatory Data module, which synchronizes prohibited fixed-dose combinations, Not-of-Standard-Quality (NSQ) alerts, and gazette notifications into the regulatory knowledge base used by the Verification and Enforcement Engine. Fig. 5 shows the Scan & Verify interface used by distributor staff to read a product's QR code and check its authenticity, regulatory status, and supply-chain history before processing a shipment, while Fig. 6 shows the corresponding QR-code generation interface used to issue unique, scannable identifiers for each inventory package.

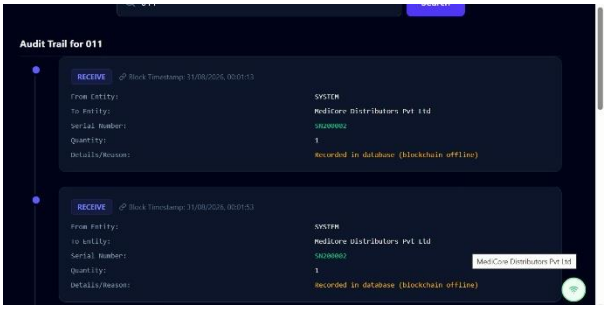

Fig. 3. Blockchain-recorded audit trail showing successive RECEIVE events logged for a medicine batch.

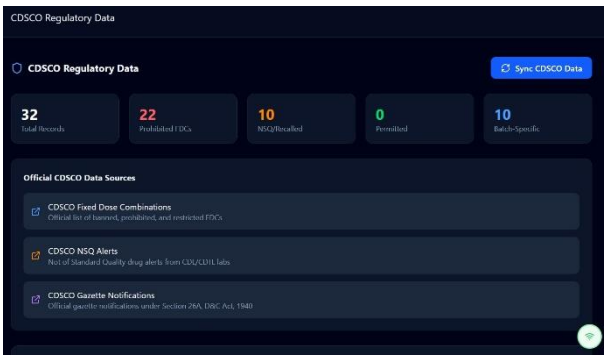

Fig. 4. CDSCO Regulatory Data module synchronizing prohibited, NSQ/recalled, and gazette-notified drug records.

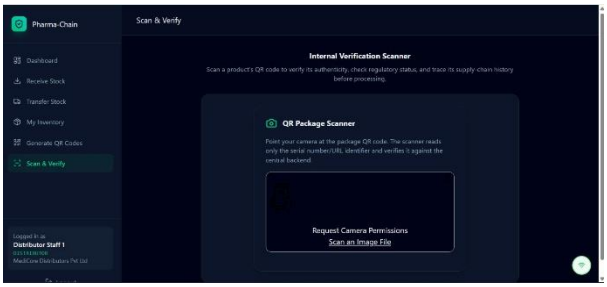

Fig. 5. Scan & Verify interface used to check a product's authenticity, regulatory status, and supply-chain history via its QR code.

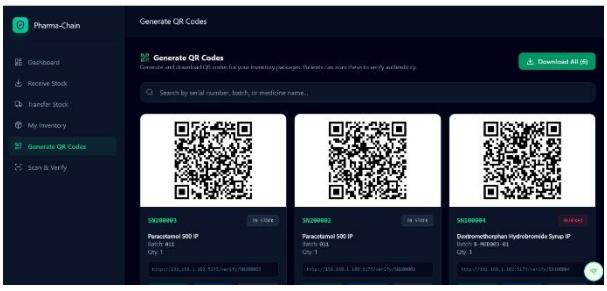

Fig. 6. QR-code generation interface for issuing unique, scannable identifiers to inventory packages.

Fig. 7 shows the administrator dashboard, which summarizes system-wide metrics — total medicines, total batches, open alerts, and system status — alongside recent regulatory alerts and recent batch activity, giving administrators a consolidated view for audit and investigation. Fig. 8 shows the Manage Medicines interface used to register and maintain the master list of pharmaceutical products recognized by the system.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

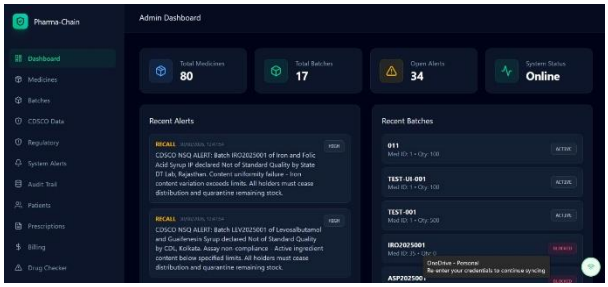

Fig. 7. Administrator dashboard showing system-wide medicine, batch, and alert statistics with recent activity.

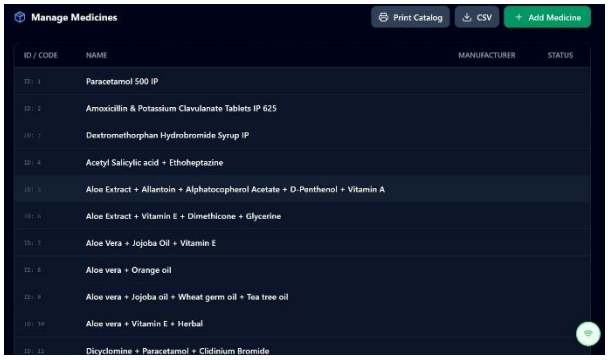

Fig. 8. Manage Medicines interface listing registered pharmaceutical products recognized by the system.

Figs. 9–11 show representative outcomes returned by the patient-facing verification page for three distinct scenarios. Fig. 9 shows a medicine classified as AUTHENTIC & SAFE, confirming that its regulatory status is PERMITTED and that its record is consistent with the official supply-chain ledger. Fig. 10 shows a PRODUCT EXPIRED result, in which the system legally prohibits dispensing despite the medicine's underlying regulatory status remaining permitted, demonstrating that the expiry check operates independently of regulatory approval. Fig. 11 shows a REGULATORY BLOCK result for a batch that has since been prohibited or recalled by drug authorities, illustrating the enforcement mechanism described in Section III-E, whereby an updated regulatory status overrides prior supply-chain approval on the very next scan.

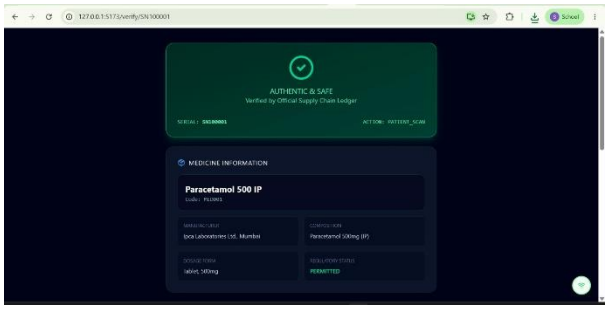

Fig. 9. Patient-facing verification result for an authentic medicine with PERMITTED regulatory status.

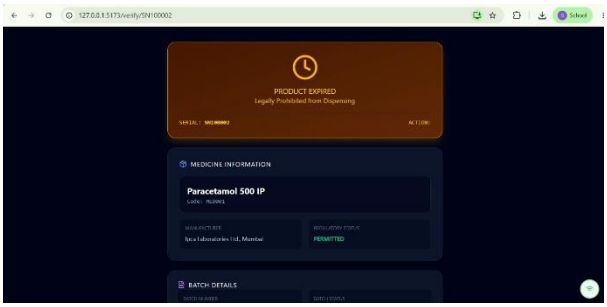

Fig. 10. Patient-facing verification result flagging an expired medicine as legally prohibited from dispensing.

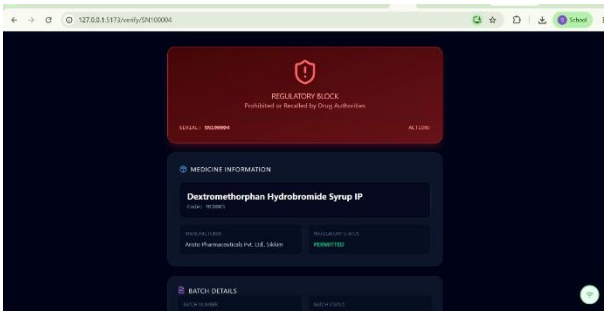

Fig. 11. Patient-facing verification result showing a regulatory block for a batch prohibited or recalled by drug authorities.

V. CONCLUSION

This paper presented a Distributor-Centric, Regulatory-Aware Blockchain Enforcement System to curb counterfeit, expired, recalled, and prohibited medicines in India's pharmaceutical distribution network, verifying medicines at the distributor level and extending checks through the pharmacy–patient workflow to overcome the limited visibility and tampering risks of conventional centralized record-keeping. Its key contribution is separating regulatory decision-making from blockchain storage: a continuously updatable database tracks CDSCO-sourced status, while the blockchain records supply-chain events and a smart contract automatically blocks the transfer or dispensing of expired, unauthorized, or prohibited medicines, with QR-code identification extending this verification to distributors, pharmacies, and patients alike. Evaluation across counterfeit, expired, prohibited, duplicate, and valid medicine scenarios shows reliable detection and near real-time blocking, with verification latency, processing time, and detection accuracy suitable for practical use, and future work will focus on IoT/RFID-based tracking, automated regulatory-data ingestion, offline operation, and integration with larger healthcare supply-chain infrastructures.

REFERENCES

[1] S. Patil, V. Sawant, A. Kanaji, V. Kadukar, and I. Patade, "Counterfeit pharmaceutical product detection using blockchain technology," in Proc. Int. Conf. Computing, Communication and Networking Technologies (ICCCNT), IEEE, 2024, doi: 10.1109/ICCCNT61001.2024.10725331.

[2] A. Mohindra, S. Singh, and D. Agrawal, "Counterfeit medicine detection through blockchain," in Proc. 16th Int. Conf. Contemporary Computing (IC3-2024), Noida, India, Aug. 2024, doi: 10.1145/3675888.3676066.

[3] M. A. Uddin, "Blockchain Medledger: Hyperledger Fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry," Int. J. Pharmaceutics, 2021.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

[4] "PharmaChain: Blockchain-based drug supply chain provenance verification system," Heliyon, Cell Press, 2023.

[5] "Internet of Things based blockchain for temperature monitoring and counterfeit pharmaceutical prevention," NCBI PMC, 2020.

[6] "Traceability of counterfeit medicine supply chain through blockchain," presented at an IEEE conference, IEEE Xplore doc. 8711418.

[7] "Blockchain technology in pharmaceutical industry to prevent counterfeit drugs," ResearchGate, 2018.

[8] "Leveraging blockchain for combatting drug counterfeiting," Cogent Engineering, Taylor & Francis, 2025, doi: 10.1080/23311975.2025.2551811.

[9] World Health Organization, "Substandard and falsified medical products," WHO Fact Sheet, 2024.

[10] World Health Organization, "1 in 10 medical products in developing countries is substandard or falsified," WHO News, Nov. 2017.

[11] World Health Organization, "Report of existing technologies used to screen and detect substandard and falsified medical products," WHO, May 2025.

[12] World Health Organization, "Global surveillance and monitoring system for substandard and falsified medical products: Activity report, August 2017–December 2021," WHO, Dec. 2024.

[13] T. Akpobolokemi, R. T. Martinez-Nunez, and B. T. Raimi-Abraham, "Tackling the global impact of substandard and falsified and unregistered/unlicensed anti-tuberculosis medicines," 2022, doi: 10.1177/23992026211070406.

[14] H. Saeed et al., "Blockchain technology in healthcare: A systematic review," PLOS ONE, 2022, doi: 10.1371/journal.pone.0266462.

[15] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, "Blockchain technology in healthcare: A systematic review," Healthcare, vol. 7, no. 2, p. 56, 2019, doi: 10.3390/healthcare7020056.

[16] "Blockchain in health information systems: A systematic review," Int. J. Environ. Res. Public Health, NCBI PMC11593537, 2024.

[17] "Blockchain in healthcare systems: A systematic review," IEEE Xplore doc. 10489533.

[18] "Systematic review on AI-blockchain based e-healthcare," IEEE Xplore doc. 9868006.

[19] N. F. Samreen and M. H. Alalfi, "A survey of security vulnerabilities in Ethereum smart contracts," arXiv:2105.06974, 2021.

[20] "A survey of Ethereum smart contract security: Attacks and detection," ACM Comput. Surv., 2024, doi: 10.1145/3643895.

[21] "Ethereum smart contract security: Vulnerabilities, analysis techniques, challenges and research directions," Comput. Electr. Eng., ScienceDirect, 2025.

[22] "Smart contract vulnerability detection technique: A survey," arXiv:2209.05872.

[23] M. A. Aulia, N. Saha, et al., "Protected QR code-based anti-counterfeit system for pharmaceutical manufacturing," arXiv:2404.07831, 2024.

[24] "A framework for enhancing pharmaceutical integrity and patient safety," Scientific Reports, Nature, 2026.

[25] Central Drugs Standard Control Organisation (CDSCO), Ministry of Health and Family Welfare, Government of India, Drugs Rules, 1945 — Rule 96(5)–(7), Schedule H2: QR-code and barcode labelling requirements for pharmaceutical products.