A Secure and Transparent Pharmaceutical Supply Chain Monitoring System Using Blockchain and On-Chain Cryptographic Verification

Thenmozhi T1, a), Arjun Rishi S1, b), Devaraj S1, c), Kavin Karkki P1, d), Keshav KV 1, e), Kannan R 2, f)

1Department of Computer Science, KGiSL Institute of Technology (Autonomous), India

2 Centre for Image and Vision Computing, Centre of Excellence for Artificial Intelligence, Multimedia University, 63100 Cyberjaya, Malaysia

*f)Corresponding author: kannan.ramakrishnan@mmu.edu.my*

*a) thenmozhithangavel74@gmail.com*

*b)arjunrishi.s2021@kgkite.ac.in*

*c)devaraj.s2021@kgkite.ac.in*

*d)kavinkarkki.p2021@kgkite.ac.in*

*e)keshav.v2021@kgkite.ac.in*

**Abstract.** The pharmaceutical supply chain is vulnerable to counterfeit drugs and lacks end-to-end transparency, posing significant risks to patient safety. This paper presents a blockchain-based system designed to enhance the security, traceability, and integrity of drug distribution. Leveraging a private Ethereum network with Clique Proof-of-Authority consensus, the system employs modular smart contracts written in Solidity to manage batch registration, stakeholder transactions, and verification processes. A React frontend facilitates role-based interactions and QR code scanning enables product verification. A key feature is the integration of Elliptic Curve Digital Signature Algorithm (ECDSA) signatures, verified on-chain using Solidity's *ecrecover* function, to authenticate critical handover points and ensure data non-repudiation. The system architecture, implementation details, and performance analysis based on gas consumption benchmarks on a private test network are discussed. The results demonstrate a robust, transparent, and verifiable framework for pharmaceutical tracking, highlighting the potential of blockchain combined with strong cryptographic verification to combat counterfeiting and enhance supply chain security.

**INTRODUCTION**

The integrity of the global pharmaceutical supply chain (PSC) is consistently threatened by methodological weaknesses in conventional tracking and verification systems. These systems, often reliant on centralized databases and technologies like barcodes or RFID, suffer from inherent vulnerabilities such as susceptibility to data manipulation, a lack of end-to-end transparency, and poor interoperability across stakeholders [6]. These shortcomings create an environment where counterfeit medicines can infiltrate the market, posing severe public health risks and eroding trust in healthcare systems [1].

To address these challenges, researchers have increasingly turned to blockchain technology for its decentralized, immutable, and transparent properties [2],[3]. Numerous studies explore its application for drug traceability, frequently utilizing platforms like Ethereum [4] or permissioned alternatives like Hyperledger Fabric [5], often integrated with QR codes, IoT, and IPFS for off-chain storage [6], [7]. Specific applications have targeted vaccine security [8] and the tracking of resellable returned drugs [9]. These works confirm the potential of blockchain to establish a secure and auditable record of a product's journey.

However, a review of existing solutions reveals that many blockchain implementations primarily focus on logging the transactional flow of products. While this improves traceability, it often overlooks the need for a more robust mechanism to establish irrefutable, cryptographically verifiable accountability for each stakeholder's actions at critical handover points [10]. Recognizing this gap, this paper proposes a novel blockchain-based monitoring system. The primary contribution lies in a secure, role-based tracking ecosystem that methodically integrates mandatory on-chain verification of off-chain Elliptic Curve Digital Signature Algorithm (ECDSA) signatures. Stakeholders cryptographically sign data off-chain, and these signatures are subsequently verified and recorded on-chain using Solidity's *ecrecover* function. This process cryptographically binds each stakeholder to their specific data attestations, ensuring strong non-repudiation and data integrity beyond conventional blockchain traceability, as demonstrated within our private Ethereum network implementation.

# PROBLEM STATEMENT

The foundational problem addressed in this research is the methodological inadequacy of both traditional and many existing blockchain-based supply chain systems to provide strong, verifiable, and granular accountability. Traditional systems, due to their centralized nature, lack mechanisms for immutable and transparent data verification, making them inherently unable to guarantee drug provenance and integrity [4], [11], [12].

While blockchain technology offers a superior framework by providing decentralization and immutability [13], [14] a more subtle methodological challenge persists. A significant portion of current blockchain solutions for supply chains focuses on creating a transactional history—logging that a product has moved from one point to another. However, this often fails to capture explicit, cryptographically proven attestation for the specific data and context of each action. This results in a gap: there is a need for a system that does not just track movement but also enforces irrefutable, signature-backed integrity for every specific event. The absence of such a mechanism limits the system's ability to provide unconditional non-repudiation and to fully secure the supply chain against sophisticated counterfeiting and data integrity violations [7],[10]. This paper addresses this specific methodological gap by implementing a system where on-chain verification of off-chain signatures is a mandatory protocol for every critical handover, thereby elevating the standard of accountability in the pharmaceutical ecosystem.

# SYSTEM ARCHITECTURE AND METHODOLOGY

The proposed system uses a multi-layered architecture integrating a private blockchain, modular smart contracts, a web frontend, and cryptographic techniques for secure pharmaceutical tracking. Figure 1 illustrates the overall architecture of the system.

## **Blockchain Network Infrastructure**

A private Ethereum network (Geth client v1.13) forms the foundation, providing a controlled environment. The Clique PoA consensus mechanism was chosen for its efficiency and fast block finality (e.g., 5 seconds), suitable for supply chain tracking. The network includes a bootnode for peer discovery and multiple processing/sealer nodes. A custom genesis block defines network parameters like a unique Chain ID and initial authorized sealers.

## Smart Contract Design

Core logic resides in three modular Solidity smart contracts (BRC, BTC, VSC) deployed on the private network:

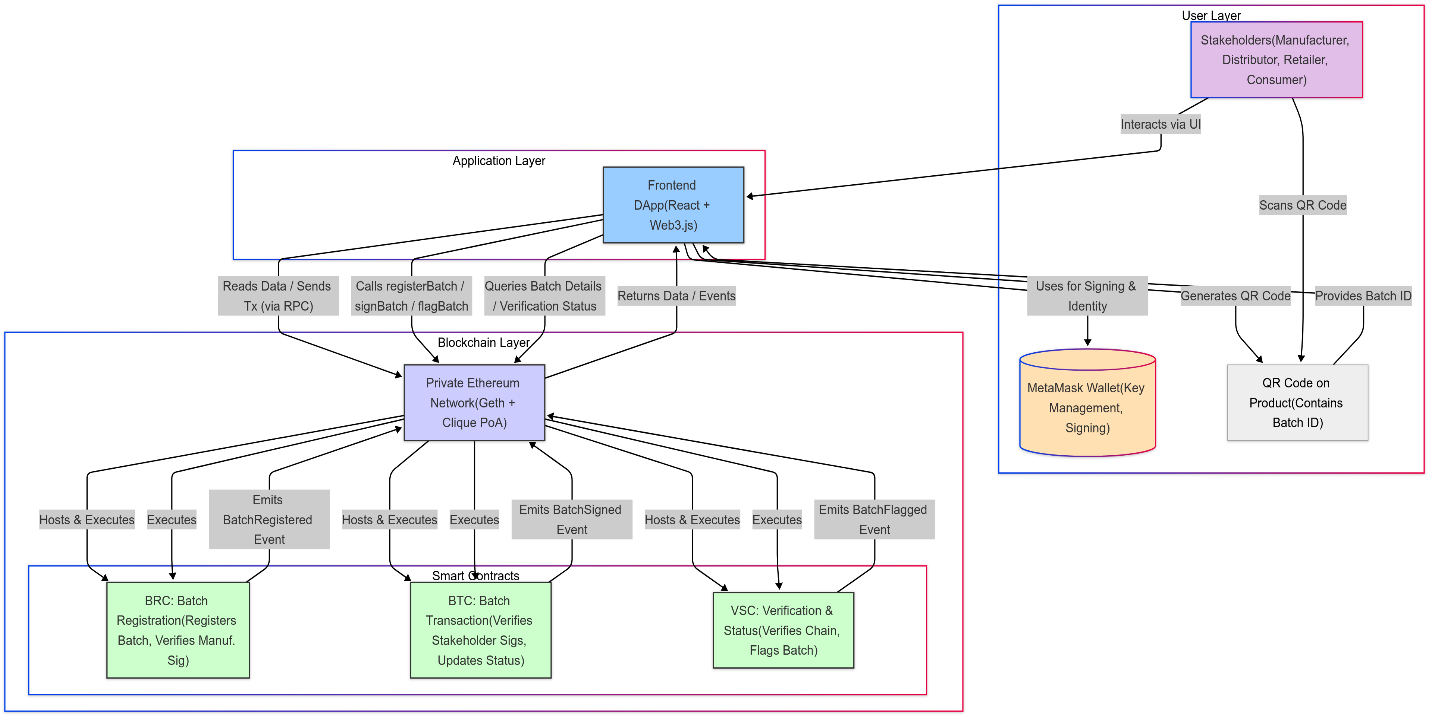
1. **Batch Registration Contract (BRC)**: Handles initial batch creation and verifies the manufacturer's ECDSA signature over batch metadata.
2. **Batch Transaction Contract (BTC):** Manages sequential signing and handover confirmations by downstream stakeholders (Distributor, Wholesaler, Retailer), verifying their ECDSA signatures.
3. **Verification and Status Contract (VSC):** Provides functions to verify a batch's signature chain integrity, check status, and handle consumer-initiated counterfeit reporting.

Key data structures include a Batch struct (holding *batchId,* metadata, *isFlagged* status, and an array of *Signature* structs) and a Signature struct (recording *signer address, role, timestamp,* and ECDSA signature components *r, s, v*). Role-Based Access Control (RBAC) is enforced using modifiers (e.g., *onlyManufacturer*) checking *msg.sender* against an on-chain role mapping. Events are emitted for significant state changes.

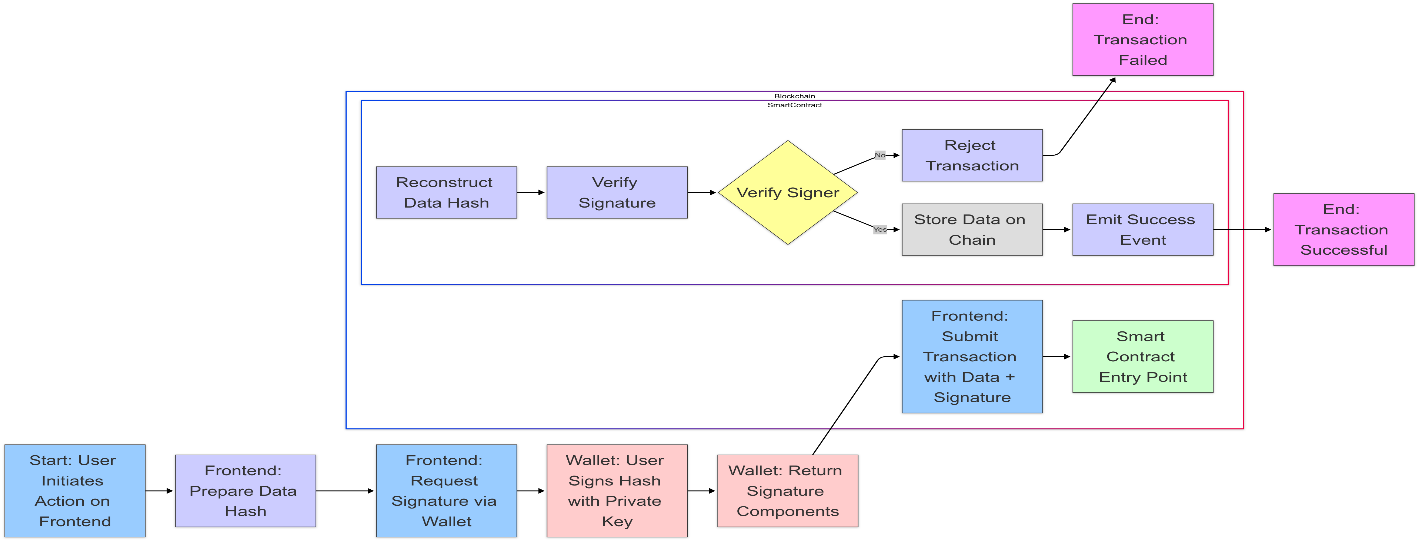
## ECDSA Signature and Verification Flow

A key contribution is the on-chain verification of ECDSA signatures for critical state changes. The process, illustrated conceptually in Figure 2, involves:

1. **Off-Chain Signing:** Stakeholders (e.g., Manufacturer, Distributor) use their private key via MetaMask (prompted by the DApp) to sign a hash of the relevant data message (e.g., batch details, handover confirmation).
2. **On-Chain Verification:** The DApp submits the original data elements and the signature components (*r, s, v*) to the appropriate smart contract function (*registerBatch* or *signBatch*).
3. ***ecrecover* Execution:** The smart contract reconstructs the data hash and uses Solidity's *ecrecover(hash, v, r, s)* to derive the signer's address.
4. **Validation & Storage:** The contract verifies that the recovered address matches *msg.sender*. If valid, the action proceeds, and the verified Signature struct (including *r, s, v*) is stored immutably on the blockchain, linked to the batch, ensuring non-repudiation and data integrity. Transactions revert if validation fails.



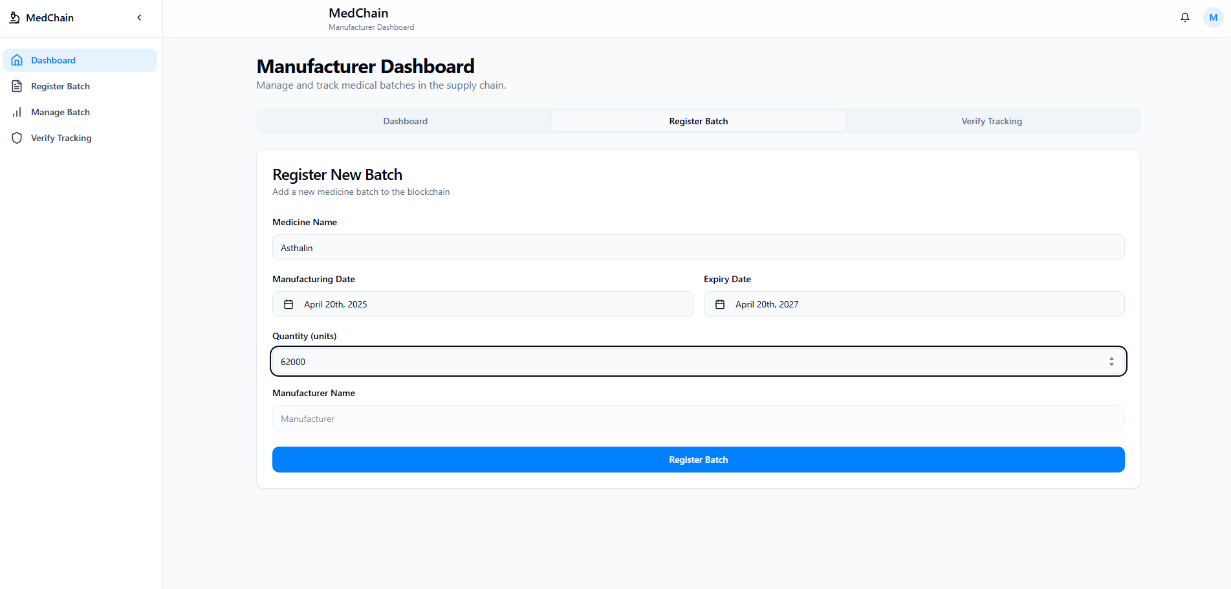
**FIGURE 1.** System architecture diagram for the Blockchain-based pharmaceutical tracking system



**FIGURE 2.** ECDSA signature verification block diagram

## **Frontend Interface and User Roles**

A React DApp using Web3.js provides the user interface. Users connect via MetaMask, which manages private keys and transaction signing. The DApp fetches the user's role (Manufacturer, Distributor, Wholesaler, Retailer, Consumer) from the smart contract and dynamically adapts the UI, presenting role-specific dashboards and functionalities (e.g., batch registration for manufacturers, Figure 3; QR scanning for consumers).



**FIGURE 3.** Manufacturer dashboard interface for registering a new batch.

For product verification, manufacturers generate QR codes encoding only the unique Batch ID after successful, signed batch registration. When a consumer or stakeholder scans this QR code using the DApp, the application extracts the Batch ID and queries the smart contracts (VSC/BRC) via Web3.js. It retrieves the full batch details and its associated signature chain from the blockchain, presenting this information for authenticity and provenance verification.

# IMPLEMENTATION AND RESULTS

## **Deployment and Testing Setup**

 Smart contracts (BRC, BTC, VSC) were compiled (Solidity) and deployed onto the private Geth network (Clique PoA, 5-second block time) using Remix IDE connected via MetaMask (Custom RPC). This controlled setup allowed seamless interaction, transaction signing, and debugging without public network latencies or real gas costs, ensuring rapid transaction confirmations.

## **Post-Scan Verification**

The system's QR code verification, implemented in the React frontend, was tested. Scanning a Batch ID successfully queried VSC and BRC contracts via Web3.js, retrieving batch metadata and stored Signature structs. Frontend logic (or VSC's *verifyBatchChain*) correctly checked the signature chain's completeness and sequential correctness (Manufacturer -> Distributor -> Wholesaler -> Retailer). Authentic batches were confirmed, and discrepancies or flagged statuses were accurately indicated, validating the QR-based verification flow.

Gas consumption benchmarks for key state-changing operations were recorded. Gas, in Ethereum, is the fee for transactions or contract execution, compensating for computational resources. Approximate gas usage ranges are in Table 1.

Batch registration was the most gas-intensive due to storage initialization and signature verification. Subsequent signing operations were moderately costly (*ecrecover* and storage updates), while flagging was the least expensive write operation. These predictable gas profiles suggest viability for private/consortium chains and amenability to Layer 2 scaling solutions for potential public deployment.

## Security Features

The system incorporates multiple security layers. Data integrity is ensured by the blockchain's immutability. Role-Based Access Control (RBAC), enforced by smart contract modifiers checking *msg.sender* against on-chain role mappings, prevents unauthorized actions. Crucially, mandatory ECDSA signature verification using *ecrecover* for *registerBatch* and *signBatch* provides strong non-repudiation. Table 2 details the specific ECDSA roles and verification points for each actor. This confirms not only transaction initiation but also cryptographic authorization of the specific data by the stakeholder, significantly enhancing security.

**TABLE 1.** Approximate gas consumption for primary smart contract operations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Operation** | **Contract** | **Function** | **Approx. Gas Used Range** | **Key Factors Affecting Gas** |
| Batch Registration (incl. Manuf. Sig) | BRC | *registerBatch* | 210,000 - 250,000 | Storing Batch struct, *ecrecover* for manuf. signature, storing signature, event emission |
| Signing a Batch (Stakeholder Sig) | BTC | *signBatch* | 85,000 - 110,000 | *ecrecover* for stakeholder sig., appending Signature struct to array, storage update, event |
| Flagging a Suspicious Batch | VSC | *flagBatch* | 65,000 - 75,000 | Updating isFlagged boolean in storage, event emission |
| On-Chain Verification (Hypothetical) | VSC | *verifyBatchChain* | 40,000 - 60,000 | Reading array data, loops, comparisons (if called within another transaction) |

**TABLE 2.** ECDSA Role Verification Table

|  |  |  |
| --- | --- | --- |
| **Supply Chain Stage** | **Actor** | **ECDSA Role** |
| Batch Registration | Manufacturer | Signs core batch metadata (e.g., batch ID, medicine name, dates, manufacturer address) off-chain. The BRC's registerBatch function receives this signature (r,s,v) and verifies it on-chain using *ecrecover* against the Manufacturer's *msg.sender*. |
| Handover/  Transfer | Distributor, Wholesaler, Retailer | Each actor, upon receiving/processing a batch, signs a confirmation message (e.g., hash of batch ID, their address, role, timestamp) off-chain. The BTC's *signBatch* function receives this signature (r,s,v) and verifies it on-chain using *ecrecover* against the actor's *msg.sender*. The verified signature is then recorded. |
| Authenticity Check | Retailer/Consumer (via *verifyBatchChain* or frontend) | The verifyBatchChain function (in VSC) checks the on-chain record for a complete and sequentially correct chain of previously verified and recorded signatures (Manufacturer, Distributor, Wholesaler, Retailer). The frontend can also retrieve individual stored signatures (r,s,v) and associated data to perform off-chain verification if needed, or rely on the status from *verifyBatchChain*. |

## Comparison with Traditional Methodologies

The proposed blockchain-based system with on-chain ECDSA signature verification offers significant advantages over traditional pharmaceutical supply chain methodologies, which often suffer from data immutability issues, opacity, and weak accountability. In contrast to traditional systems vulnerable to tampering, our approach ensures high Data Integrity through an immutable ledger and on-chain ECDSA signature verification. Where traditional methods offer limited Transparency with data silos, our system provides a shared, auditable ledger for authorized participants, enabling comprehensive Traceability and granular batch tracking, a significant improvement over the often fragmented visibility in conventional setups.

In addition to these benefits, blockchain technology has inherent trade-offs. Blockchain networks tend to have lower throughput and higher latency compared to centralized databases as a result of the consensus process. The setup, configuration, and maintenance of a multi-node private network are more involved and require expert-level expertise. On-chain data storage is also more computationally costly, with a need for precise architectural design to meet both performance and security advantages of decentralization. These factors represent key considerations for organizations planning to adopt such advanced systems.

# CONCLUSION

This project successfully demonstrated a blockchain-based pharmaceutical supply chain system using a private Ethereum PoA network, Solidity smart contracts, and a React DApp. Key achievements include robust RBAC and, critically, on-chain ECDSA signature verification via *ecrecover* for enhanced data integrity and non-repudiation. Functional testing validated core features like secure batch registration, auditable stakeholder signing, QR code verification, and counterfeit reporting, with gas benchmarking affirming private network viability. The system enhances drug traceability, combats counterfeits, and improves patient safety.

Limitations include private network governance considerations, public chain scalability (gas costs, throughput), lack of integration with existing enterprise IT systems (ERP/WMS) and comprehensive IoT data, need for DApp UI/UX refinement, and detailed regulatory mapping.

Future work will prioritize Layer 2 scaling solutions, developing standardized APIs for interoperability, comprehensive IoT integration, AI-driven data analytics, real-world pilot studies, establishing a robust governance model, creating native mobile applications, and incorporating features for specific regulatory compliance to transition this proof-of-concept to a widely adoptable solution.

# REFERENCES

1. S. Hamid, N.Z. Bawany, and K. Fatima, “A Blockchain based Framework for Verifying Drug Authenticity,” in *2023 24th International Arab Conference on Information Technology (ACIT)*, (IEEE, Ajman, United Arab Emirates, 2023), pp. 1–8.
2. M. H. Z. Hairul Nizam, M. A. Ahmad Nizam, M. H. Husaini Jummadi, N. N. M. S. Nik Mohd Kamal, and A. A. Zainuddin, “Hyperledger Fabric blockchain for securing the edge Internet of Things: A review,” Journal of Informatics and Web Engineering **4**(1), 81–98 (2025).
3. F. Mazlan, N. F. Omar, N. N. M. S. Nik Mohd Kamal, and A. A. Zainuddin, “Comprehensive insights into smart contracts: Architecture, sectoral applications, security analysis, and legal frameworks,” Journal of Informatics and Web Engineering **4**(1), 1–17 (2025).
4. 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 **9**, 9728–9743 (2021).
5. F. Jamil, L. Hang, K. Kim, and D. Kim, “A Novel Medical Blockchain Model for Drug Supply Chain Integrity Management in a Smart Hospital,” Electronics **8**(5), 505 (2019).
6. S.K. Nanda, S.K. Panda, and M. Dash, “Medical supply chain integrated with blockchain and IoT to track the logistics of medical products,” Multimed Tools Appl **82**(21), 32917–32939 (2023).
7. S. Namasudra, S. Das, R.G. Crespo, D. Taniar, and N.R. Moparthi, “DrugBlock: An Advanced System to Secure Drug Supply Chain Using Internet of Things and Blockchain-Enabled Consumer Electronics,” IEEE Trans. Consumer Electron., 1–1 (2024).
8. A. Ghadge, M. Bourlakis, S. Kamble, and S. Seuring, “Blockchain implementation in pharmaceutical supply chains: A review and conceptual framework,” International Journal of Production Research **61**(19), 6633–6651 (2023).
9. M. Debe, K. Salah, R. Jayaraman, and J. Arshad, “Blockchain-Based Verifiable Tracking of Resellable Returned Drugs,” IEEE Access **8**, 205848–205862 (2020).
10. U. Agarwal, V. Rishiwal, M. Yadav, M. Alshammari, P. Yadav, O. Singh, and V. Maurya, “Exploring Blockchain and Supply Chain Integration: State-of-the-Art, Security Issues, and Emerging Directions,” IEEE Access **12**, 143945–143974 (2024).
11. K. Wasnik, I. Sondawle, R. Wani, and N. Pulgam, “Detection of Counterfeit Products using Blockchain,” ITM Web Conf. **44**, 03015 (2022).
12. V. Lingayat, I. Pardikar, S. Yewalekar, S. Khachane, and S. Pande, “Securing Pharmaceutical Supply Chain using Blockchain Technology,” ITM Web Conf. **37**, 01013 (2021).
13. M. Rehman, I.T. Javed, K.N. Qureshi, T. Margaria, and G. Jeon, “A Cyber Secure Medical Management System by Using Blockchain,” IEEE Trans. Comput. Soc. Syst. **10**(4), 2123–2136 (2023).
14. W. Alkhader, K. Salah, A. Sleptchenko, R. Jayaraman, I. Yaqoob, and M. Omar, “Blockchain-Based Decentralized Digital Manufacturing and Supply for COVID-19 Medical Devices and Supplies,” IEEE Access **9**, 137923–137940 (2021).