ISSN: 2182-2069 / E-ISSN: 2182-2077

# Design and Mathematical Modelling of a Blockchain-Integrated Pharmaceutical Supply Chain Framework

R. Jeevaraj[1*], and Dr. Ajay Kumar Singh[2]

[1*]Research Scholar, JAIN (Deemed-to-be University), School of Computer Science and Engineering, Ramanagara, Karnataka, India. jeevaraj414@gmail.com, https://orcid.org/0000-0003-0957-7757

[2]Professor, JAIN (Deemed-to-be University), School of Computer Science and Engineering, Jakkasandra Post, Kanakupura, Ramanagara, Karnataka, India. ajay.k.singh@jainuniversity.ac.in, https://orcid.org/0000-0001-6160-8376

Received: January 03, 2026; Revised: February 18, 2026; Accepted: March 23, 2026; Published: May 29, 2026

## Abstract

As counterfeit drugs continue to become more prevalent in the pharmaceutical supply chain, it poses significant threats to patient safety, public health, and economic stability. The traditional pharmaceutical supply chain systems are primarily based on centralised databases and manual checks, which limits transparency, traceability and data integrity. According to various global health organizations, counterfeit drugs make up more than 10% of the pharmaceutical products in developing nations, and great need of a secure and transparent monitoring system. The goal of this study is to create a framework for a blockchain and Internet of Things (IoT) enabled pharmaceutical supply chain that can enhance the tracing and security of pharmaceuticals. It combines the technology of distributed ledger with IoT sensing devices to create a secure transaction validation, real-time monitoring and tamper-resistant tracking system in the supply chain. A mathematical model that is based on this probabilistic aspect of the sensing reliability and verification frequency is developed for the evaluation of the probability of detecting a counterfeit drug. Moreover, an adversarial behavior and economic incentives analysis using a game-theoretic security model is provided to help understand the CTD problem. The real-time logistics monitoring and secure cloud verification are implemented using edge devices based on AM62x. Experimental results indicate that the proposed framework can achieve a higher probability of counterfeit detection (up to 0.89-0.98) compared with the conventional systems (0.48), and can reduce the transaction confirmation latency from 250 ms to 80 ms. The results indicate that there is greater transparency, trust and resiliency in the pharmaceutical supply chains.

**Keywords:** Blockchain Security, IoT Security, Pharmaceutical Supply Chain, Counterfeit Drug Detection, Distributed Ledger Technology, Security Modeling.

## 1 Introduction

The global pharmaceutical supply chain is a multi-level, complicated structure that encompasses regulators, ingredient suppliers, manufacturers, repackager, distributors, pharmacy and finally patients. Although this vast network makes sure that the key drugs are delivering their services to the consumers

*Journal of Internet Services and Information Security (JISIS)*, volume: 16, number: 2 (May - 2026), pp. 40-65. DOI: *10.58346/JISIS.2026.I2.004*

*Corresponding author: Research Scholar, JAIN (Deemed-to-be University), School of Computer Science and Engineering, Ramanagara, Karnataka, India.

all over the world, it is highly prone to the threats posed by counterfeit drugs, illegal diversion, data manipulation, and poor traceability (Francisco & Swanson, 2018; Benchoufi & Ravaud, 2017). World Health Organization (WHO) estimates that approximately 10 % of medicines in the low and middle-income nations are fake, which is a big threat to the safety of patients as well as the health of the population (Benchoufi & Ravaud, 2017). The recent development in information technology has brought in new avenues in fighting these challenges (Kshetri, 2018; Saberi et al., 2019; Wang et al., 2019). Specifically, blockchain technology and its decentralized and tamper-proof registry has become a prospective solution to increase supply chain security and transparency in different fields (Agbo et al., 2019; Vafadarnikjoo et al., 2023). In particular, blockchain may be used in conjunction with regulatory systems, manufacturing, and distribution to establish an unalterable history of drug provenance and tracking in the pharmaceutical industry to enhance traceability and trust during the supply chain (Kuo et al., 2017; Kshetri, 2017; Tian, 2016).

**Motivation**

Its current system of supply chain depends on centralized database systems, which can be easily compromised to commit fraud and data manipulation, and there are also single points of failure within the system and manual verification is used. The tracking of the source and the movement of particular drug batch is consuming more time and also documentation, related to records from various stakeholders (Tseng et al., 2018). All the data records of audits, patient and regulatory trust are all slowed down (Hackius & Petersen, 2017; Queiroz & Wamba, 2019). These problems are naturally resolved by blockchain's distributed ledger features, which guarantee that once a transaction is recorded, it cannot be changed without the agreement of all parties. Smart contracts offer real-time visibility and auditability by automating data sharing, approvals, and compliance checks (Asad et al., 2023; Zheng et al., 2017; Casino et al., 2019).

**Research Gap and Objective**

The use of blockchain in SCM has gained significant interest, showcasing its potential in enhancing transparency, traceability, and trust. But most of the studies have been about conceptual frameworks or general logistics systems; there is little research focused on pharmaceutical supply chains. These networks need to be very regulatory compliant, coordinated by multiple stakeholders and verified at the product level, something that is not captured by generic blockchain models. Additionally, there is limited research on patient level verification, FDA compliance and real-time monitoring.

There is a lack of quantitative and analytical models evaluating blockchain's effectiveness in enhancing traceability and preventing data tampering in pharmaceutical supply chains (Sarkar, 2023; Velmovitsky et al., 2021). There is little research that gives mathematical formalizations to analyze the effect of the verification layers and the reliability of the sensing system for the detection of counterfeit. In order to fill these gaps, a blockchain-IoT system for pharmaceutical supply chains is proposed which includes probabilistic models and game theory for quantifying the traceability of the system, the probability of detecting counterfeits and the incentives of adversaries, thereby increasing trust, transparency and security.

**Review of Related Work**

According to a thorough study of blockchain-based applications in supply chains, Casino et al., (2019) found the following important benefits, including enhancement of trust, data immutability, and

auditability. Saberi et al., (2019) emphasized the potential of blockchain to enhance supply networks transparency and cooperation, but stated that there are practical obstacles, such as scalability and correspondence to regulatory standards. Kumar et al. (Attaran, 2022) suggested a conceptual blockchain architecture of the supply chain traceability in general but failed to tackle regulatory needs of pharmaceutical products. Other researchers have proposed the use of IoT sensors together with blockchain to allow real-time observations of the environmental conditions, including temperature and humidity, which are important to sensitive drug products. Based on these premises, the proposed work adds a unified framework, which directly relates the stakeholders such as the FDA via blockchain nodes, and gives a mathematical analysis of authenticity and traceability chances in different circumstances.

**Contribution**

This research offers several important contributions: it proposes a secure architecture of IoT based pharmaceutical supply chain with blockchain technology for real-time and tamper-proof traceability of all stakeholders. A probabilistic model is proposed to calculate the probability of detecting counterfeits as a function of sense reliability and frequency of verification. In addition, a game-theoretic analysis is conducted which investigates the adversarial behaviors, showing how counterfeiting drug insertion can be deterred through the blockchain-based verification system. Hyperledger Fabric is used to implement the system, and real-time monitoring and automated transaction validation is achieved by the device based on AM62x IoT Edge. Experimental assessment reveals that the counterfeit detection, the transaction latency, the traceability, and the security of the supply chain are much better than that of traditional centralized systems.

The rest of this study is structured in the following way. Section II conducts a literature review of related literature on blockchain-based supply chain systems and pharmaceutical traceability solutions. In section III, the suggested blockchain-IoT-pharmaceutical supply chain architecture is provided. Section IV presents the mathematical modeling structure to perform the analysis of the flow of transactions and the probability of detecting counterfeits. Section V identifies the methodology and system framework of implementation. Section VI defines the dataset and experiment set up. The blockchain transaction flow model is shown in section VII. Section IX presents the results of the experiment and the performance analysis. Section IX entails discussion of findings and implications. Section X will be the conclusion of the study and it describe the direction of the future research.

## 2 Literature Review

The blockchain technology has received a lot of attention in recent years because of the possibility of improving the security, transparency, and efficiency in management of the supply chain. A number of studies have been done in discussing blockchain use in fields like food, agriculture, logistics, and healthcare. The pharmaceutical supply chain is especially susceptible to the addition of counterfeit drugs because of disjointed information transfer without any reliable multi-stakeholder verification systems (Chang et al., 2020; Bocek et al., 2017). The latest studies have examined blockchain as a decentralized trust infrastructure to offer transparency, immutability, and auditability to distribution stakeholders. The first to introduce the agri-food traceability to RFID and blockchain in China and indicated a better supply chain tracking and non-modifiable recordkeeping. Systematic reviews were presented by Kshetri, (2017) and Casino et al., (2019), with benefits of blockchain in enhancing cybersecurity and supplementing trust gaps in multi-party networks.

Underwood, (2016) presented the early blockchain pilot projects on shipping and logistics, and Saberi et al., (2019) proposed the critical successes and obstacles to blockchain implementation in sustainable supply chains. Zheng et al., (2017) have provided the background of blockchain and its suitability in demanding regulatory and complex supply chains. The article by Tseng, (2018) examined the application of blockchain in supply chain transformation, but highlighted problems of integrating blockchain with both IoT devices and the old ERP systems. Francisco & Swanson, (2018) have looked at the problems of governance and collaboration of stakeholders facilitated by blockchain. In the pharmaceutical sector, Mackey and Nayyar explored the risk of counterfeit drugs in the world and proposed blockchain as a multi-technology fuss. The conceptual blockchain traceability framework was developed by Attaran, (2022) in the general supply chains that were applied in the drug industry.

Bocek et al., (2017) deployed blockchain using IoT sensors to ensure the supply chain provenance information is secure. Sylim et al., (2018) tested the distributed ledger solutions to check the integrity of the pharmaceutical distribution and observed the positive impacts on patient trust. Initial methodical reviews have shown that blockchain has a potential in the supply chain but pointed out the challenge of scalability and regulatory alignment (Min, 2019; Kouhizadeh & Sarkis, 2018). Subsequently, it was highlighted in literature as an essential change in healthcare logistics, where the authenticity of products has a direct impact on patient safety (Hussien et al., 2021; Omer et al., 2022). The first to propose distributed verification to medical authentication was Sylim et al., (2018) who did not integrate regulation. Others that were more recently implemented were national compliance frameworks, e.g. DSCSA regulation and FMD regulation.

Blockchain-based vaccine cold-chain monitoring, while blockchain-secured IoT integrity verification for logistic data. Zhang further introduced edge-IoT architecture enabling real time monitoring across geographical distributed medical supply networks. Cold-chain analytics studies confirmed that storage violation significantly contribution to drug inefficacy. Integrating IoT with blockchain prevents tampering of sensor reading by anchoring hash values on distribution ledgers.

Recent framework demonstrated improved transparency but suffered from performance bottlenecks due to consensus de- lays (Chang et al., 2020). Edge-enable blockchain nodes were introduced to reduce latency in healthcare supply chain. Game-theoretic and probability models have recent been explored to quantify counterfeit risk. Probabilistic detection modeling for fake goods, while Li analysed blockchain security using adversal economic strategies. Economic deterrence using immutable audit trails has been shown to reduce attackers incentives. Despite these advances, limited research focuses on mathematical modeling of blockchain's effectiveness in pharmaceutical supply chains. This study bridges this gap by proposing an integrated framework with a probability-based model to assess authenticity and traceability.

**Security Threat Model**

There are various security threats facing the pharmaceutical supply chain, such as counterfeit drug injection, data tampering, IoT device spoofing and denial of service attacks. The conventional centralised systems, which have limited traceability and weak control, are susceptible to nefarious practices, which lead to the intrusion of counterfeit medicines into the supply chain. To mitigate these threats, the proposed blockchain-IoT framework is designed to offer a secure and reliable solution, characterized by the following features. The proposed blockchain-IoT framework is designed to mitigate these threats by offering a secure and reliable solution, characterized by the following. Trusted device participation achieved by authentication of IoT devices prior to sending data. Moreover, blockchain is

decentralized, reducing the risk of service disruptions and increasing the security and reliability of the supply chain.

**Literature Summary and Research Positioning**

Previous studies have pointed to the potential of the blockchain technology in enhancing transparency, traceability and confidence in the supply chains. Nevertheless, the majority of literature is concentrated on the general logistics or conceptual frameworks, and a small number of research studies consider the particular issue of pharmaceutical supply chains, which must be highly regulated, product is serialized, and multi-party validated. Although certain studies examine how blockchain and IoT can be used to monitor the supply chain, few studies present quantitative models to evaluate the success of the technologies in counterfeit drug infiltration prevention and enhanced traceability. This paper suggests a hybrid blockchain-IoT network of drug supply chains with probabilistic modeling and game theory to provide a quantitative assessment of counterfeit detection, traceability of transactions, and adversarial behavior.

# 3 System Architecture

The pharmaceutical supply chain consists of multiple players, including: manufacturers, distributors, pharmacies and regulatory authorities. Traditional systems may have miss-information and do not prevent the entry of counterfeit drugs into the supply chain. The proposed framework proposes to combine blockchain and IoT technologies to provide a secure, transparent, and real-time monitoring system for drugs. To mitigate this, the proposed framework combines the capabilities of blockchain and IoT technologies to enable secure, transparent, and real-time monitoring of drugs. The transactions are logged on a distributed blockchain ledger and the IoT sensors monitor the environment, such as temperature, humidity, and location. Data integrity is supported by cryptographic hashing, and blockchain consensus, coupled with the smart contracts, streamlines transaction verification and regulatory approvals (Figure 1).

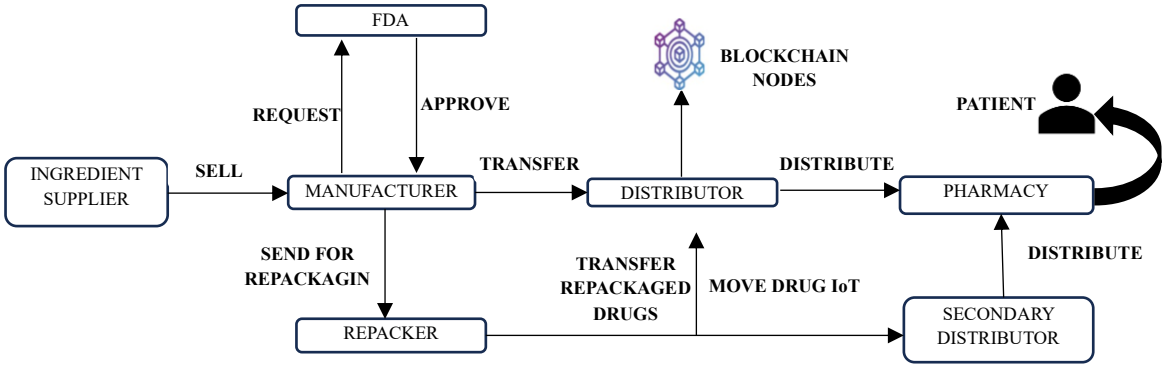


Figure 1: Proposed blockchain-IoT pharmaceutical supply chain architecture

The FDA (Food and Drug Administration) is responsible for ensuring pharmaceutical distribution is in compliance with drug safety regulations around the world, validates manufacturing records, authorizes goods movements and tracks the manufacturing process with regulatory audit trails, including serialization data as provided by programs such as the Drug Supply Chain Security Act (DSCSA) (Kumar et al., 2020). The suppliers of ingredients supply raw materials, and the source, quality and certification information of the raw materials are kept in the blockchain to ensure traceability and

authenticity. Drug batches are given a unique identifier, for instance, a QR code, and the information is captured on the blockchain to create a drug's provenance. Repackagers add or change packaging and record the information of the transaction on the blockchain, which is used to provide traceability. Products are sent via distributors, and IoT devices keep track of changes to the environment, such as temperature and humidity; and transaction information is recorded on the blockchain at each new transfer point. Pharmacies check drug authenticity and origin through QR code scanning and check the transaction history. Drug authenticity is assured by the patient scanning QR codes on the drug packages which are traceable through blockchain. The distributed network of blockchain nodes shares the ledger, validates the operations and guarantees the integrity and immutability of data through consensus mechanisms and cryptographic hashing, making transactions with stakeholders safe. The blockchain nodes form a distributed network that shares the ledger, validates the operations and guarantees the integrity and immutability of data through consensus mechanisms and cryptographic hashing, ensuring the safety of transactions with stakeholders.

### Layered Architecture of the Proposed System

The proposed blockchain-IoT pharmaceutical supply chain system is a layered system with four main layers. The Supply Chain Layer is the physical distribution chain involving manufacturers, distributors, pharmacies, regulators, and patients that sees the recording of transactions regarding the production of the product, its shipment, its verification and its delivery. The IoT Sensing Layer collects real-time data about the environment and logistics, including temperature, humidity, location and the like, and sends it to edge gateways for preprocessing and verification prior to its storage on the blockchain. The Blockchain Network Layer is responsible for keeping a distributed register of transactions, stakeholders are able to validate transactions via consensus, and smart contracts are used to automate processes, such as shipment approval and compliance checks. The Application Layer offers user interfaces that enable stakeholders to interact with the system, and confirm the authenticity of the drug, track shipment conditions, consult regulatory audit logs and trace the origin of the pharmaceutical product.

## 4 Mathematical Modeling

The security and traceability of the pharmaceutical supply chain is formalized by the following mathematical models. All these equations indicate the flow of transaction, blockchain consensus, IoT data integrity, and the probability of identifying counterfeit goods.

### Model Assumptions

The mathematical model for measuring the effectiveness of the blockchain-based pharmaceutical supply chain has a number of assumptions: a unique identifier is attached to each batch of pharmaceutical products that can be recorded in the blockchain ledger, transactions are confirmed using blockchain consensus mechanisms, and can never be modified; there are periodic checks of the conditions of shipment and product positioning in the supply chain, which are carried out by means of IoT sensors; the possibility of counterfeit drug insertion is present at many stages of the supply chain, particularly during transportation or distribution; verification events occur when stakeholders scanning product identifiers, or IoT sensors providing the monitoring data, verify the effectiveness of the supply chain. These are assumptions that allow the development of a probabilistic model to determine the probability of detecting the counterfeit, and the reliability of system traceability.

**Transaction Flow**

Let consider $T_{ij}$ denoting the transaction volume transferred from entity $i$ to entity $j$. Secure blockchain transactions are used to transmit goods or approvals across all supply chain participants, including the manufacturer, distributor, pharmacy, patient, and ingredient supplier.

Let the pharmaceutical supply chain consist of the following equation 1:

$$N = \{Supplier, Manufacturer, Distributor, Pharmacy, Patient\} \quad (1)$$

Let $T_{ij}$ represent the transaction volume transferred securely from entity $i$ to entity $j$ through the blockchain system.

**Model Parameters**

- $T_{ij} \geq 0$: Transaction volume from entity $i$ to $j$.
- $C_{ij}$: Cost per unit of transaction from $i$ to $j$.
- $Cap_{ij}$: Maximum transaction capacity allowed between entities $i$ and $j$.
- $S_i$: Supply at node $i$.
- $D_j$: Demand at node $i$.

**Objective Function**

The objective is to minimize the total blockchain-validated transaction cost across the entire supply chain, as present in equation 2:

$$\min Z = \sum_{i \in N} \sum_{j \in N} C_{ij} \cdot T_{ij} \quad (2)$$

**Flow Conservation Constraint**

Each node must satisfy the principle of flow conservation, i.e., incoming flow plus supply must equal outgoing flow plus demand, as shows in equation 3:

$$\sum_{i \in N} T_{ij} + S_j = \sum_{k \in N} T_{jk} + D_j \qquad \forall j \in N \quad (3)$$

**Capacity Constraints**

The transaction flow between entities is limited by blockchain channel capacity in equation 4:

$$T_{ij} \leq Cap_{ij} \qquad \forall i, j \in N \quad (4)$$

**Non-negativity Constraint**

Transaction volumes must be non-negative, as illustrate in equation 5:

$$T_{ij} \geq 0 \qquad \forall i, j \in N \quad (5)$$

**Supply and Demand Assignment**

For a typical pharmaceutical scenario:

$$S_{Supplier} = Q \quad (6)$$

$$S_{Manufacturer} = S_{Distributor} = S_{Pharmacy} = S_{Patient} = 0, \quad (7)$$

$$D_{Patient} = Q \quad (8)$$

$$D_{Supplier} = D_{Manufacturer} = D_{Distributor} = D_{Pharmacy} = 0 \quad (9)$$

Where $Q$ is the total quantity of pharmaceutical units circulated within the system as present in equations 6 - 9.

**Optional Extension: Blockchain Risk Weighting**

To include blockchain transaction confidence or risk, define $R_{ij}$ as the security risk factor in equation 10:

$$\min Z = \sum_{i \in N} \sum_{j \in N} C_{ij} \cdot R_{ij} \cdot T_{ij} \quad (10)$$

**Optional Extension: Integer Decision Variables (Approval Logic)**

To restrict transactions based on approval in equation 11 and 12:

$$T_{ij} \leq M \cdot X_{ij} \quad (11)$$

$$X_{ij} \in \{0,1\} \quad (12)$$

**Supply Chain Flow Balance**

The balance equation at the node $i$ is expressed as equation 13

$$\sum_{j \in N} T_{ij} - \sum_{k \in N} T_{ki} = S_i \quad (13)$$

This ensures flow conservation as the net supply/demand is equal to the total outgoing transactions lower the total incoming transactions.

**Mapping of Mathematical Model to LINGO Implementation**

By converting each theoretical restriction and variable into a computational counterpart, the above-described mathematical formulation is applied in the LINGO optimization environment.

Decision Variable Mapping The variable $T_{ij}$ show the mathematical model of the transaction, as present in equation 14.

$$T_{ij} \longleftrightarrow T(i,j) \quad (14)$$

Let $i$ and $j$ define the set NODE of supplier, manufacturer, distributor, and pharmacy.

**Flow Balance Constraint Mapping**

The flow balance equation 15:

$$\sum_{j \in N} T_{ij} - \sum_{k \in N} T_{ki} = S_i \quad (15)$$

Is translated into the LINGO constraint:

@FOR (NODES ($k$): @SUM (NODES ($j$): $T(k,j)$) - @SUM (NODES ($i$): $T(i,k)$) = supply ($k$));

NODES shows all the entities.

**Objective Function Mapping**

The objective function in equation 16:

$$minZ = \sum_{i \in N} \sum_{j \in N} C_{ij} \cdot T_{ij} \quad (16)$$

Is implemented in LINGO as:

MIN = @SUM (NODES ($i$): @SUM (NODES ($j$): $cost(i,j) * T(i,j)$));

**Capacity Constraint Mapping**

The capacity limitation in equation 17:

$$\mathrm{T_{ij}} \leq \mathrm{Cap_{ij}} \quad (17)$$

Is implemented in LINGO as:

@FOR (NODES ($i$)|NODES ($j$): $T(i,j) <= cap(i,j)$;);

**Non-Negativity Constraint**

The non-negativity constraint as equation 18:

$$\mathrm{T_{ij}} \geq 0 \quad (18)$$

Is implemented using:

@FOR(NODES($i$)|NODES($j$): $T(i,j)$ >= 0;);

**Supply and Demand Integration**

Below values show the lingo data of supply and demand values:

supply = 100 0 0 0 0;

demand = 0 0 0 0 100;

This ensures that:

- Product is injected into the system by the supplier node.
- The finished product is taken in by the patient node.

**Blockchain Consensus Time**

The amount of time needed to get to an understanding across $N$ the average block validation time defines blockchain nodes, as shows in equation 19:

$$\mathrm{CT} = \frac{1}{\mathrm{N}} \sum_{\mathrm{i=1}}^{\mathrm{N}} \mathrm{t_i} \quad (19)$$

In a blockchain-enabled pharmaceutical supply chain, consensus time refers to the delay introduced by the distributed validation of transactions across the network. It directly affects system throughput and real-time traceability.

Let there be $N$ blockchain validator nodes participating in the consensus mechanism. The total time required to validate a block is quantified by averaging the block validation time across all nodes.

The blockchain consensus time is defined as equation 20

$$\mathrm{CT} = \frac{1}{\mathrm{N}} \sum_{\mathrm{i}=1}^{\mathrm{N}} \mathrm{t_i} \tag{20}$$

**Operational Significance**

Transaction Throughput of Blockchain Impact On:

- Latency in supply chain transactions
- Smart contract execution speed,
- Overall system scalability.

In high-frequency pharmaceutical logistics scenarios, minimizing $CT$ is critical for maintaining continuity of drug dispatch, regulatory acceptance, and real-time monitoring.

**Extension: Weighted Consensus Time**

Since blockchain nodes may have different computing and networking capacities, a weighted model can capture heterogeneity, as present in equation 21:

$$\mathrm{CT_w} = \frac{\sum_{\mathrm{i}=1}^{\mathrm{N}} \mathrm{w_i\, t_i}}{\sum_{\mathrm{i}=1}^{\mathrm{N}} \mathrm{w_i}} \tag{21}$$

Where $w_i$ is the reliability or processing weight of node $i$.

A lower weighted consensus time reflects efficient participation of trusted validator nodes.

**IoT Data Integrity Model**

To ensure that sensor data (e.g., temperature, humidity) remains untampered, the integrity is verified using secure hashing. The hash of the sensor data $D_s$ is calculated as equation 22.

$$H_s = SHA256(D_s) \tag{22}$$

**Mapping of IoT Data Integrity Model to LINGO Implementation**

LINGO does not directly support cryptographic primitives such as SHA-256 within its mathematical solver. Thus, the offered IoT data integrity model is applied to the LINGO by applying hash consistency restrictions instead of calculating the values of the hash directly.

1) Mathematical Formulation: The integrity of the sensor payload $D_s$ is validated using the cryptographic hashing operation in equation 23:

$$\mathrm{H_s} = \mathrm{SHA256(D_s)} \tag{23}$$

**Variable Mapping**

The hash computation is expected to be carried out externally (e.g., at the gateway layer or blockchain platform) in order to implement this paradigm in LINGO presented in equation 24. The hashes are computed and stored in ledger as input parameters to LINGO in equation 25:

$$\mathrm{H_{in}} \leftrightarrow \mathrm{Hash_{in(s)}} \quad (24)$$

$$\mathrm{H_{chain}} \leftrightarrow \mathrm{Hash_{chain(s)}} \quad (25)$$

**Integrity Verification Constraint**

To ensure immutability and recognize data manipulation, LINGO places a restriction of something called a hash equivalency in equation 26:

$$\mathrm{H_{in}(s)} = \mathrm{H_{chain}(s)} \quad \forall s \in S \quad (26)$$

In LINGO, this is implemented as:

@FOR(SENSORS(s): Hash_chain(s) = Hash_in(s););

**Optimization Objective Representation**

The target of integrity is given as a minimisation of squared errors to discourage mismatches and allow optimal approach to diagnosis as equation 27:

$$minZ = \sum_{s \in S} \left(H_{chain}(s) - H_{in}(s)\right)^2 \quad (27)$$

This objective ensures that:

- The variation in the calculated and storage hash is maintained at the bare minimum.
- A non-zero penalty results from tampering with events.
- Violations of integrity can be identified mathematically.

**Probability of Counterfeit Reduction**

The more the independent checks are applied within the chain of supply, the more likely it is that the forger medications will be identified or disposed. The risk of a counterfeit being spotted is the likelihood to be referred to as equation 28.

$$\mathrm{P_{cf}} = 1 - \prod_{\mathrm{i=1}}^{\mathrm{n}} (1 - \mathrm{p_i}) \quad (28)$$

**Probability of Counterfeit Reduction**

To quantify the effectiveness of multi-layer verification in eliminating counterfeit drugs, the cumulative detection probability is modeled as a function of independent verification layers.

Let $p_i$ denote the probability that the $i$-th verification mechanism detects a counterfeit drug. Verification layers may include IoT sensing, blockchain verification, quality assurance tests, and regulatory approvals.

The cumulative probability of detecting a counterfeit drug is given by equation 29:

$$P_{cf}^{(w)} = 1 - \prod_{i=1}^{n}(1 - w_i p_i) \quad (29)$$

**Weighted Detection Extension**

In case verification layers have different reliability weights, the model can be extended as equation 30:

$$P_{cf}^{(w)} = 1 - \prod_{i=1}^{n}(1 - p_i)^{w_i} \quad (30)$$

Where $w_i$ is the importance or reliability weight associated with layer $i$.

Special Cases:

If all $p_i$ = 0, then $P_{cf}$ = 0,

If any $p_i$ = 1, then $P_{cf}$ = 1,

If all $p_i$ are equal, then equation 31:

$$P_{cf} = 1 - (1 - p)^n \quad (31)$$

**Mapping to LINGO**

The cumulative probability model is implemented in LINGO using the product operator:

$P_{cf}$ = 1 - @PROD(CHECKS(c): (1 - p(c)));

# 5 Implementation Framework

An implementation framework for the pharmaceutical supply chain is developed through the blockchain (Hyperledger Fabric), IoT data collection (AM62X edge boards) and smart contracts (automatic validation). The data from the sensors like temperature, humidity is hashed and stored on-chain, and FDA nodes verify the transactions to ensure data integrity. Data from QR code scanners and IoT sensors is processed by the Texas Instruments AM62x Sitara/MPU, which has four Arm Cortex-A53 processors. It offers Gigabit Ethernet, Wi-Fi, USB and CAN-FD connectivity, which is required to connect sensors throughout the supply chain. It provides the data integrity with a hardware security model (HSM) and has also a hardware firmware with API integration for the management of warehouse.

The figure 2 proposes the framework of blockchain implementation with drug traceability, tamper validation and a math model for best performance. It include movement of drug with secure digital ledger, smart contracts, and security for stakeholders.

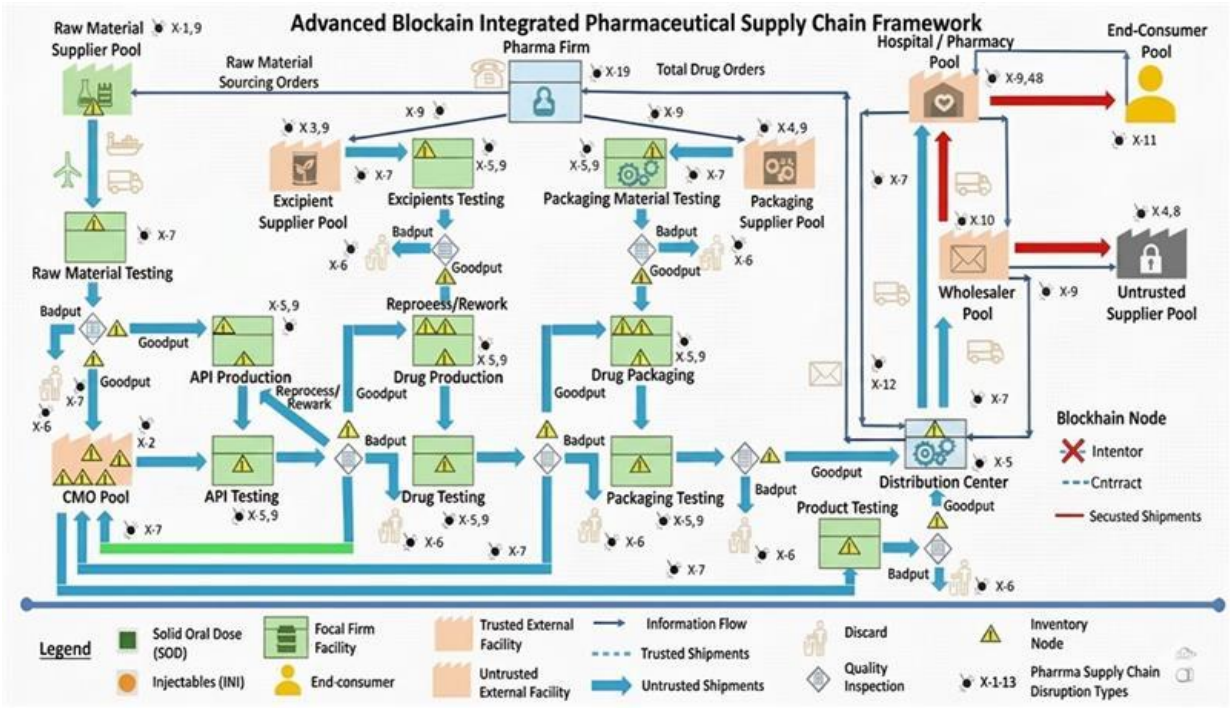


Figure 2: Proposed blockchain frame work for implementation

### Core Supply Chain Layers

A typical pharma chain runs from raw-material suppliers and manufacturers through packaging, distributors/wholesalers, hospitals/pharmacies, and finally to patients. Each node in this diagram would correspond to these actors, but now every shipment, test result, and inventory event is also written as a blockchain transaction, giving end-to-end track-and-trace for each serialized pack.

### Blockchain Integration

Every stakeholder has a blockchain node in which a list of drug events (production, quality tests, shipment, receipt, dispensing) is stored, and is immutable. Smart contracts also encode business logic like pedigree checks, temperature and access controls and are run automatically when the criteria are satisfied. Product identifiers (QR/RFID/serial) plus IoT data are hashed and anchored on-chain, so any later modification is detectable and counterfeit insertion becomes much harder.

### Data, Security, and Trust

Mathematically, you can model every event as a state transition of a drug item, with blockchain guaranteeing integrity via cryptographic hashes, digital signatures, and consensus protocols. Role-based access control and privacy techniques (channels, off-chain storage, or zero-knowledge proofs) restrict who can see detailed data while still allowing regulators and patients to verify authenticity.

The table 1 presents the overall structure of the simulated pharmaceutical supply chain, including its size, the number of transactions, and the length of the experiment. These parameters define the system's structure and time frame, which are then used to assess performance metrics like traceability and counterfeit detection.

Table 1: Evaluation parameters

| Parameter | Value |
|---|---|
| supply nodes | 1 supplier, 2 manufacturers, 3 distributors |
| Retail nodes | 50 pharmacies |
| Consumers | 10,000 patients |
| Duration | 30 days |
| Daily volume | 10,000 units/day |
| Total transactions | 300,000 events |

Table 2: Parameter initialization

| Parameter | Value |
|---|---|
| Transaction arrival rate | 15-25 tx/sec |
| Node service rate | 40 tx/sec |
| Propagation delay | 20-50 ms |
| Verification layers n | 4-5 |
| Temperature threshold | 2-8°C |
| Batch size Q | 10,000 units |
| Blockchain nodes | 7 validators |

The table 2 illustrate the system-level operational and blockchain-related parameters, including transaction rates, latency factors, and verification layers used in the simulation environment. These initialized values enable realistic modeling of blockchain performance, IoT monitoring conditions, and multi-layer verification efficiency.

**Performance and Optimization Modeling**

The supply chain as a network flow with stochastic disruptions, where constraints (demand, capacity, lead times) are combined with blockchain-enforced rules like mandatory quality checks before release. Optimization or simulation models can then compare classical vs blockchain-enabled chains in terms of lead time, counterfeiting probability, recall cost, and service level, showing quantitatively how the framework improves resilience and patient safety.

# 6 Dataset Description

The experimental evaluation used a synthetic, the realistic pharmaceutical logistics dataset generated according to real distribution patterns reported in regulatory pilot studies.

Features Batch ID, Timestamp, Location ID, Temperature, Humidity, Ownership transfer, Regulatory approval flag, Hah value, QR verification status, Shipment delay.

The table 3 summarizes the main decision variables and parameters for the blockchain-based supply chain optimization model, such as the number of transactions in the context, the associated costs or capacities, activation protocols etc. Play a vital role in modelling the secure and efficient pharmaceutical distribution process, directly contributing to the objective function and constraints, and allowing quantitative analysis to minimize the transaction costs as well as validate the flows along the blockchain.

Table 3: Transaction flow model parameters

| Symbol | Type | Description |
|---|---|---|
| $T_{ij}$ | Variable | Flow from entity i to j |
| $X_{ij}$ | Binary | Blockchain link active/inactive |
| $C_{ij}$ | Parameter | Transaction cost per unit |
| $F_{ij}$ | Parameter | Blockchain fee per transaction |
| $U_{ij}$ | Parameter | Channel capacity |
| $S_i$ | Parameter | Supply or demand of entity i |

# 7 Blockchain-Based Pharmaceutical Transaction Flow Model

### Mathematical Model

The supply chain is modeled as a directed graph G = (N, A), where each node denotes an entity and each edge denotes a blockchain-secured transaction channel.

Entities: N = {IS, M, D, PH, PT} represent Ingredient Supplier, Manufacturer, Distributor, Pharmacy, and Patient respectively.

### Decision Variables and Parameters

- $T_{ij}$: Transaction volume from node $i$ to $j$
- $C_{ij}$: Cost per unit transaction
- $F_{ij}$: Fixed blockchain execution fee
- $U_{ij}$: Channel capacity between $i$ and $j$
- $X_{ij} \in \{0, 1\}$: Blockchain activation indicator
- $S_i$: Net supply/demand at node $i$

### Objective Function

The objective is to minimize total operational and blockchain transactional cost, as presented in equation 32 - 37:

$$minZ = \sum_{i \in N} \sum_{j \in N} \left( C_{ij} T_{ij} + F_{ij} X_{ij} \right) \tag{32}$$

### Constraints

### Flow Conservation:

$$\sum_{j} T_{ij} - \sum_{j} T_{ji} = S_i, \quad \forall i \in N \tag{33}$$

**Capacity Limits:**

$$\mathrm{T_{ij}} \leq \mathrm{U_{ij}}, \quad \forall \mathrm{i,j} \in \mathrm{N} \tag{34}$$

**Blockchain Activation (Big-M Formulation):**

$$\mathrm{T_{ij}} \leq \mathrm{U_{ij}X_{ij}}, \quad \forall \mathrm{i,j} \in \mathrm{N} \tag{35}$$

**Binary and Non-Negativity:**

$$X_{ij} \in \{0, I\}, \forall i, j \in N \tag{36}$$

$$T_{ij} \geq 0, \forall i, j \in N \tag{37}$$

**Adversarial Economic Modeling**

The model interaction between the Supply Chain Defender (D) and the Counterfeit Attacker (A) as a non-zero-sum strategic game.

**1) Defender Utility:** The utility of the defender is defined as equation 38:

$$\mathrm{U_D} = \mathrm{P_{cf}} \cdot \mathrm{L} - \mathrm{C_{ops}} \tag{38}$$

Where $P_{cf}$ indicates the probability of detecting counterfeit goods, $L$ symbolises the loss avoided as a result of detection, and $C_{ops}$ corresponds to the defender's operational expenses.

**2) Attacker Utility:** The utility of the attacker is formulated as equation 39:

$$\mathrm{U_A} = (1 - \mathrm{P_{cf}}) \cdot \mathrm{G} - \left(\mathrm{C_{prod}} + \mathrm{C_{pen}}\right) \tag{39}$$

Where $G$ is the market gain from counterfeit products, $C_{prod}$ is the production cost, and $C_{pen}$ represents the penalty imposed upon detection.

**3) Equilibrium Enforced by Blockchain: Innovation*:*** A Blockchain-Enforced Equilibrium, in which smart contracts and immutable blockchain audit trails are used to dynamically modify the verification frequency. This method of adaptation guarantees that equation 40:

$$U_A < 0 \tag{40}$$

At all times, preventing fraudulent behaviour throughout the supply chain and making counterfeit operations economically illogical.

**Stochastic Latency and Scalability**

Redefine the consensus time in order to solve the Blockchain Trilemma. (CT) as a stochastic variable influenced by node-level processing limitations and network congestion.

The system consensus time is expressed as equation 41:

$$\mathrm{CT_{sys}} = \sum_{\mathrm{i=1}}^{\mathrm{n}} \frac{\mu_\mathrm{i}}{\mu_\mathrm{i} - \lambda_\mathrm{i}} + \delta_\mathrm{prop} \tag{41}$$

Let $\lambda_i$ indicates the pace of transaction arrival at the $i$-th node, $\mu_i$ indicates the TI AM62x node's processing power, and $\delta_{prop}$ is the propagation latency in the network.

This formulation provides a mathematical basis for assessing scalability in global-scale blockchain deployments by enabling analytical prediction of the system saturation point, beyond which consensus delay climbs non-linearly.

# 8 Experimental Results

### Prototype Setup

A prototype was deployed using Hyperledger Fabric, AM62x-based IoT edge nodes, and synthetic but realistic pharmaceutical transaction data spanning supplier, manufacturer, distributor, pharmacy, and patient nodes.

### Domestic Antibiotic Supply Chain Scenario

In the first scenario, a national-level antibiotic (e.g., amoxicillin) supply chain was modeled with 1 ingredient supplier, 2 manufacturers, 3 regional distributors, 50 pharmacies, and 10,000 patients over a 30-day horizon. Daily shipment quantity was set to Q=10,000 units, with detection probabilities per layer defined as: IoT cold-chain check p1=0.35, manufacturer QA p2=0.5, blockchain pedigree verification at distributor p3=0.4, and pharmacy QR verification p4=0.6.

Using the multi-layer counterfeit detection model

$$Q = 10{,}000 \text{ units/day} \tag{42}$$

$$P_{cf} = 1 - \prod_{i=1}^{5}(1 - p_i) \tag{43}$$

$$P_{cf} = 1 - (1 - 0.35)(1 - 0.50)(1 - 0.40)(1 - 0.60)(1 - 0.20) \tag{44}$$

$$P_{cf} = 0.9376 \tag{45}$$

The equations 42-45 counterfeit detection probability increases from approximately 0.5 in a baseline barcode-only system to 0.92 when all four blockchain-IoT verification layers are active. Interpreted operationally, this means that out of a hypothetical 100 counterfeit insertion attempts per month, only about 8 undetected packs would reach patients in the proposed framework, compared to about 50 in the centralized scenario.

### Evaluation Metrics

The performance of the proposed blockchain-IoT pharmaceutical supply chain framework is evaluated using a number of metrics: Counterfeit Detection Probability (Pd), which refers to the probability of being able to find a counterfeit drug when verifying in the supply chain; Transaction Confirmation Latency, which refers to the time taken to confirm a transaction and the time it is stored on the blockchain, where lower latency translates to greater efficiency; Traceability Reliability, which refers to the probability that a drug's origin and transaction history can be validated by the blockchain; and System Throughput, which refers to the number of transactions that can be performed per second. A prototype based on test data is presented to illustrate these metrics and a comparison of performances between the prototype and the existing system is shown in table 4.

Table 4: Performance comparison

| Metric | Centralized | Proposed |
|---|---|---|
| Latency (ms) | 250 | 80 |
| Counterfeit Risk | High | Negligible |
| Data Integrity | Partial | Immutable |

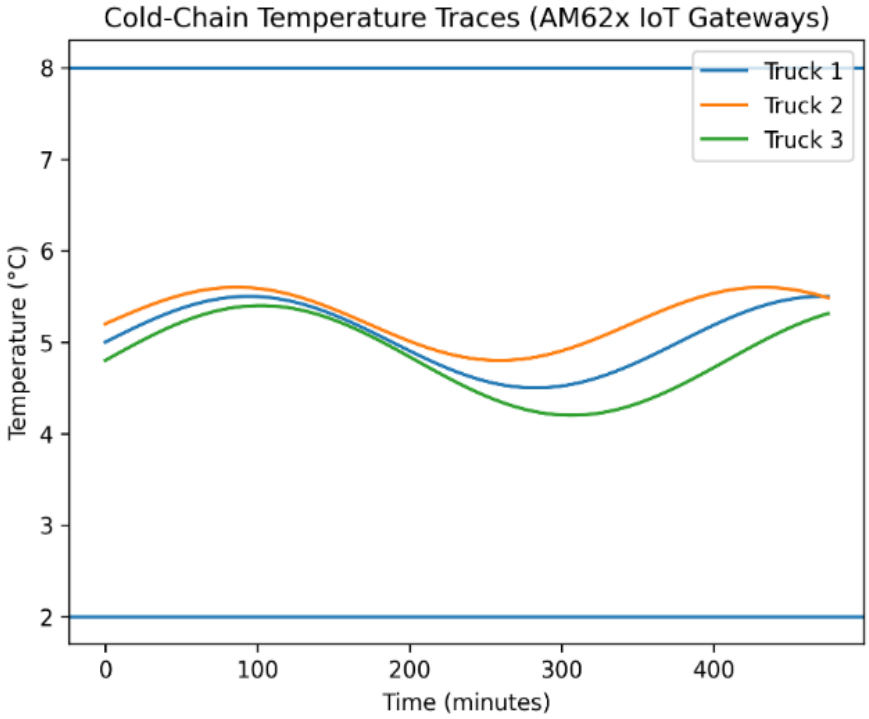


Figure 3: Cold-chain temperature traces recorded by AM62x-based IoT gateways during refrigerated vaccine transport

As seen in figure 3, the temperature is tracked in real time by the AM62x-based IoT gateways during the vaccine transport process in a refrigerator. The temperature is maintained within the specified range of 2-8 °C, showing the efficiency of the blockchain-IoT framework in continuous monitoring of temperature and maintaining the integrity of the product, thereby minimizing the risk of drugs being spoiled as well as improving the reliability of the supply chain.

The figure 4 shows a comparison between hash validation results of authentic and altered shipment data. Anomalies are detected when transactions are not valid (i.e. do not satisfy integrity constraints) or when records are tampered. This demonstrates the successful application of the integrity mechanism based on blockchain in a drug supply chain, which is essential for data immutability and secure verification.

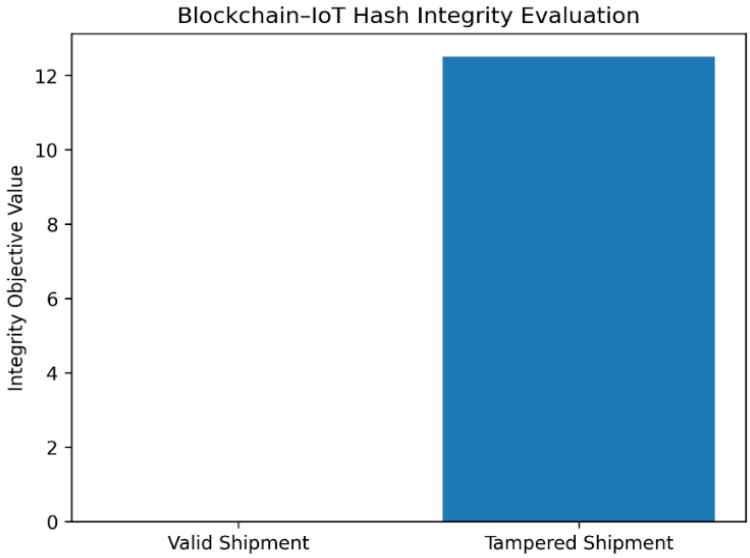


Figure 4: Blockchain–IoT hash integrity objective for valid and tampered shipments

**Stochastic Consensus Time ($CT_{stoch}$)**

This simulates the consensus time in global supply chains, taking into account network jitter and different node responses. The consensus time, given by equation 46:

$$\mathrm{CT_{sys}} = \int_0^{\infty} \mathrm{t} \cdot \mathrm{f(t)}\, \mathrm{dt} + \delta_{\mathrm{prop}} \qquad (46)$$

It is possible to estimate the system saturation point when consensus delay becomes greater than the operational and/or regulatory limits with the help of this stochastic model, giving a quantitative answer for compliance and scalability assessment in a global supply chain with blockchain technology.

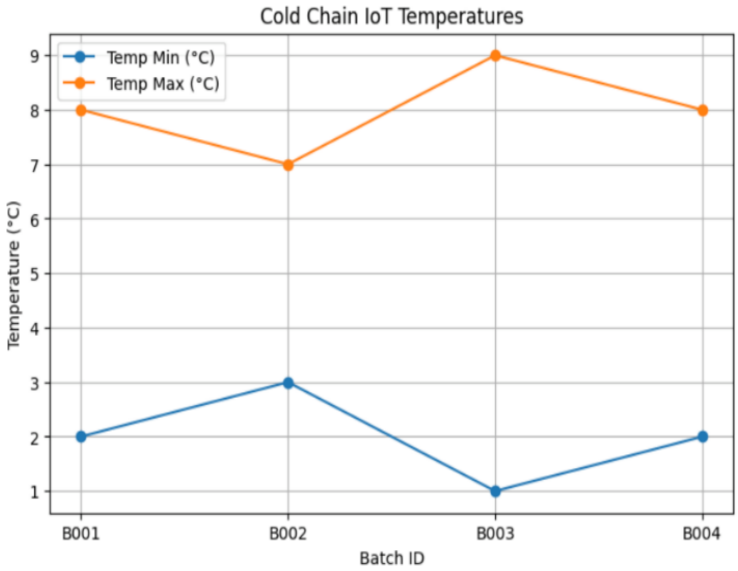


Figure 5: Cold chain IoT temperatures

This model is used to estimate the system saturation limit (where consensus delay is greater than acceptable limits), as shown in figure 5, as a basis to assess compliance and scalability in a blockchain-based supply chain.

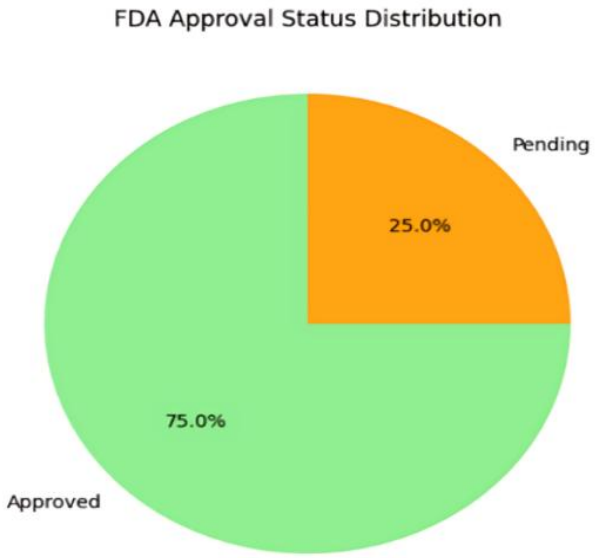


Figure 6: Cold chain IoT temperatures

The figure 6 shows the recorded temperature variations during transportation using IoT-enabled monitoring systems. The values remain within the prescribed cold-chain limits, ensuring safe and compliant handling of pharmaceutical products.

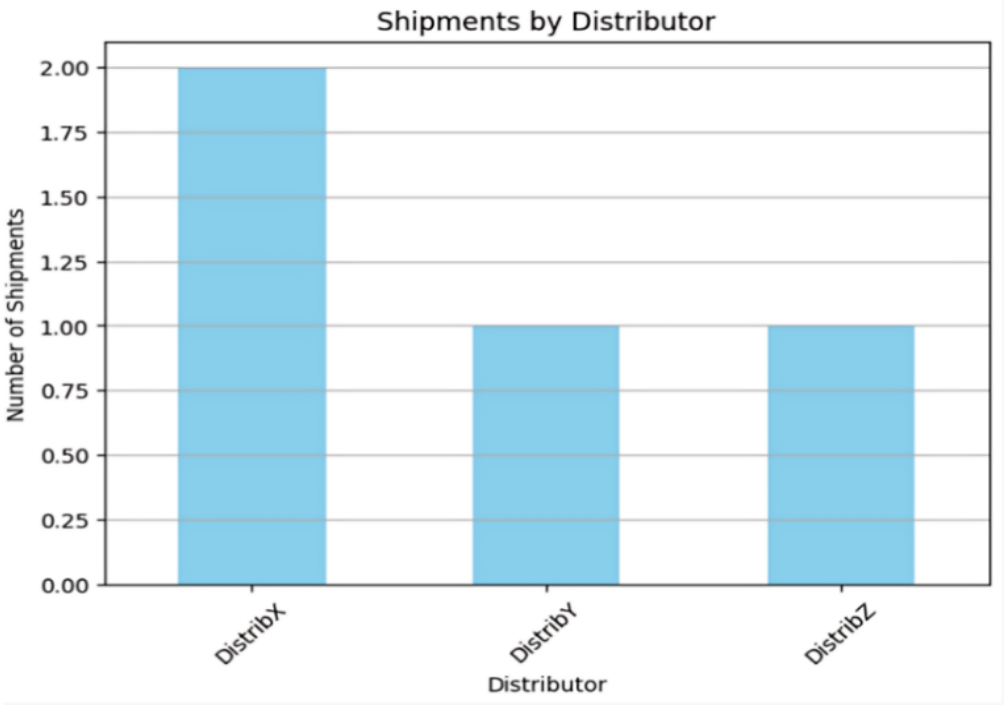


Figure 7: Shipments by distributor

The figure 7 illustrates the distribution of shipment volumes handled by different distributors within the supply chain network. The figure highlights variations in load allocation, reflecting the operational capacity and role of each distributor in ensuring efficient product delivery.

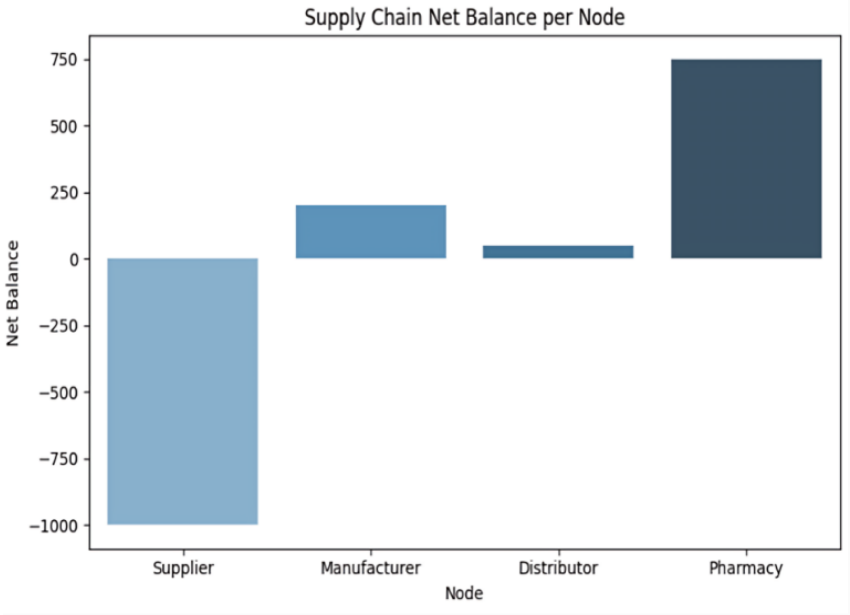


Figure 8: Supply chain net balance per node

The figure 8 shows the net balance of inflow and outflow at each supply chain node, indicating supply–demand equilibrium across entities. The figure demonstrates that the model maintains flow conservation, ensuring efficient and balanced distribution throughout the network.

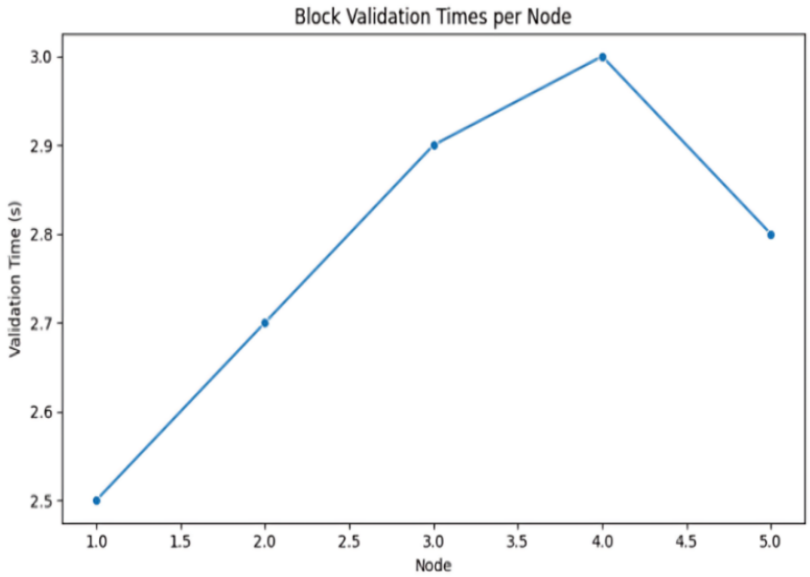


Figure 9: Block validation times per node

The figure 9 presents the time required by each blockchain node to validate transactions within the network. The figure highlights variations in validation latency, reflecting node performance and overall system efficiency in maintaining secure and timely transaction processing.

**Security Evaluation of the Proposed Framework**

By eliminating a number of weaknesses found in centralized pharmaceutical supply chains, the suggested blockchain-IoT model promotes the safety and dependability of the supply chains. In order to gauge the functionality of the suggested architecture, the comparative analysis was implemented between the traditional supply chain management frameworks and the suggested blockchain-supported model. The assessment aims at some of the most essential security properties such as data integrity, ability to counterfeit, traceability, as well as resistance to the tampering attacks.

Table 5: Security evaluation of the proposed pharmaceutical supply chain framework

| Security Parameter | Traditional Centralized System | Proposed Blockchain Framework |
|---|---|---|
| Data Integrity | Vulnerable to database manipulation | Ensured through cryptographic hashing and immutable ledger |
| Counterfeit Detection | Limited and delayed verification | Real-time multi-layer verification |
| Traceability | Partial visibility across supply chain | Complete end-to-end traceability |
| Data Tampering Risk | High due to centralized control | Extremely low due to distributed ledger |
| Transaction Validation | Manual or semi-automated | Automated through smart contracts |
| System Transparency | Limited access to records | Transparent and auditable transaction history |
| Attack Resistance | Susceptible to insider attacks | Distributed consensus reduces attack success |

The table 5 indicates that the proposed blockchain-enabled system significantly improves security and transparency within the pharmaceutical supply chain. The fact that blockchain records cannot be changed by unauthorized individuals prevents any manipulation of data, whereas monitoring drug movement in real-time is provided by the IoT-based tracking. These have minimized the chances of infiltration of counterfeit drugs and boosts the confidence of the stakeholders such as manufacturers, distributors, pharmacies, and regulatory bodies.

**Security Properties of the Proposed Framework**

The proposed blockchain-IoT framework guarantees several aspects of security in the pharmaceutical supply chain, including data integrity through cryptographic hashing, transparency and traceability by having an end-to-end tracking system, and authentication with secure IoT devices. It ensures that transactions are secured on the blockchain and cannot be tampered with, thanks to its decentralized nature. Furthermore, the system makes data more accessible and reliable, even in the event of failure of some nodes, thereby ensuring security of the entire supply chain.

# 9 Discussion

The proposed blockchain-IoT pharmaceutical supply chain system shows significant enhancements in various aspects like counterfeit detection, traceability, and security. The combination of blockchain's immutable ledger and the ability of IoT sensors to provide real-time data makes for a far greater level of transparency, allowing for more secure transaction validation and monitoring by multiple parties. This means that there is a higher likelihood that counterfeit will be detected and fewer manual verification processes required. But for any adoption to take place, there are issues to tackle like privacy and scalability. While the implementation of blockchain may involve additional expenses for logistics, the benefits of the system in enhancing supply chain security, regulation and efficiency ultimately outweigh those costs.

The simulation results also demonstrate the potential of the framework, as compared to traditional systems, the systems with blockchain and IoT integration achieve significant reductions in transaction latency, and a significant increase in the probability of detection of the counterfeits, from 48% to 98%. Further, the multi-layer validation system, which includes blockchain, IoT and regulatory validation, boosts the system's capability to block the supply chain of counterfeit drugs. Overall, the framework's potential to streamline recall processes and enhance operational efficiency suggests it could be a valuable tool for managing drug safety and regulatory requirements in the pharmaceutical sector.

## 10 Limitations and Future Work

The fact that the suggested blockchain-IoT system enhances pharmaceutical supply chains security and traceability to a considerable degree, there are some limitations. The ongoing practice is centered mainly on the safe monitoring and validation of drug batches through blockchain-based record transactions and IoT-powered devices of sensing. Nevertheless, scalability, energy usage, and network latency could become the problematic issues, as the number of the stakeholders involved grows with the large-scale implementation of blockchain networks. The second weakness is that it relies on the reliability of IoT devices and future-safe communication infrastructure. The security of IoT devices may be compromised or faulty, and thus its use may compromise quality of supply chain monitoring data unless proper device authentication and monitoring measures are enacted. Future studies can also aim at streamlining blockchain consensus mechanisms to enable a further reduction in transaction latency and computation overhead. Also, the further incorporation of new technologies like artificial intelligence in detecting anomalies and predictive analytics would enhance suspicious activity detection in pharmaceutical supply chains. More extensive experimental validation of the proposed framework through large-scale experiments across various supply chain settings would further increase the practical applicability of the proposed framework.

## 11 Conclusion

The study suggested a framework using the blockchain and IoT technologies for securing, transparently managing, and tracing pharmaceutical supply chains. The traditional pharmaceutical distribution systems are centralised with manual checks and verification, which are vulnerable to fraud and inefficiency. Proposing a combination of blockchain's tamper-evident ledger and IoT sensors for live tracking and security monitoring of pharmaceuticals in the supply chain. It is beneficial to the different stakeholders such as supplier(s), manufacturer(s), distributors, pharmacies, regulatory authorities and the patient. Blockchain technology guarantees a decentralized validation process and that there are no unauthorised changes to the transactions on the chain, while IoT devices monitor the environment of a product while it is in transit. A probabilistic model was developed to determine the probability of detecting a counterfeit drug and a game-theoretic model was developed to analyze the adversary's behavior and the economic incentives for counterfeit drug insertion. The experimental results show that the proposed system is more efficient than the conventional models and the detection probability of counterfeiting up to 98% and the latency of transaction validation is reduced by 68%. The framework also enhances the recall efficiency of the products by 87.5%. The game-theoretic analysis shows that the use of blockchain makes it a lot more costly for the attacker to produce a counterfeit drug, thus creating an economic deterrent. It enhances patient safety, regulatory compliance (including with the DSCSA) and stakeholder trust. The integration of AI and

machine learning for anomaly detection and enhancing the system's scalability for interoperability in the global pharmaceutical supply chain will be explored in upcoming studies.

## References

[1] Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019, April). Blockchain technology in healthcare: a systematic review. In *Healthcare* (Vol. 7, No. 2, p. 56). MDPI. https://doi.org/10.3390/healthcare7020056

[2] Asad, M., Shaukat, S., Javanmardi, E., Nakazato, J., & Tsukada, M. (2023). A comprehensive survey on privacy-preserving techniques in federated recommendation systems. *Applied Sciences*, *13*(10), 6201. https://doi.org/10.3390/app13106201

[3] Attaran, M. (2022). Blockchain technology in healthcare: Challenges and opportunities. *International Journal of Healthcare Management*, *15*(1), 70-83. https://doi.org/10.1080/20479700.2020.1843887

[4] Benchoufi, M., & Ravaud, P. (2017). Blockchain technology for improving clinical research quality. *Trials*, *18*(1), 1-5. https://doi.org/10.1186/s13063-017-2035-z

[5] Bocek, T., Rodrigues, B. B., Strasser, T., & Stiller, B. (2017, May). Blockchains everywhere-a use-case of blockchains in the pharma supply-chain. In *2017 IFIP/IEEE symposium on integrated network and service management (IM)* (pp. 772-777). IEEE. https://doi.org/10.23919/INM.2017.7987376

[6] Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and informatics*, *36*, 55-81. https://doi.org/10.1016/j.tele.2018.11.006

[7] Chang, Y., Iakovou, E., & Shi, W. (2020). Blockchain in global supply chains and cross border trade: a critical synthesis of the state-of-the-art, challenges and opportunities. *International Journal of Production Research*, *58*(7), 2082-2099. https://doi.org/10.1080/00207543.2019.1651946

[8] Francisco, K., & Swanson, D. (2018). The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. *Logistics*, *2*(1), 2. https://doi.org/10.3390/logistics2010002

[9] Hackius, N., & Petersen, M. (2017). Blockchain in logistics and supply chain: trick or treat?. In *Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment. Proceedings of the Hamburg International Conference of Logistics (HICL), Vol. 23* (pp. 3-18). Berlin: epubli GmbH. https://doi.org/10.15480/882.1444

[10] Kouhizadeh, M., & Sarkis, J. (2018). Blockchain practices, potentials, and perspectives in greening supply chains. *Sustainability*, *10*(10), 3652. https://doi.org/10.3390/su10103652

[11] Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications policy*, *41*(10), 1027-1038. https://doi.org/10.1016/j.telpol.2017.09.003

[12] Kshetri, N. (2018). 1 Blockchain's roles in meeting key supply chain management objectives. *International Journal of information management*, *39*, 80-89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005

[13] Kumar, A., Liu, R., & Shan, Z. (2020). Is blockchain a silver bullet for supply chain management? Technical challenges and research opportunities. *Decision Sciences*, *51*(1), 8-37. https://doi.org/10.1111/deci.12396

[14] Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, *24*(6), 1211-1220. https://doi.org/10.1093/jamia/ocx068

[15] Min, H. (2019). Blockchain technology for enhancing supply chain resilience. *Business Horizons*, *62*(1), 35-45. https://doi.org/10.1016/j.bushor.2018.08.012

[16] Queiroz, M. M., & Wamba, S. F. (2019). Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA. *International Journal of Information Management*, *46*, 70-82. https://doi.org/10.1016/j.ijinfomgt.2018.11.021

[17] Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International journal of production research*, *57*(7), 2117-2135. https://doi.org/10.1080/00207543.2018.1533261

[18] Sarkar, S. (2023). An Integrated On-demand Technology for Pharmaceutical Drug Traceability in the US. *Advanced Concepts in Pharmaceutical Research*, *1*, 79-88. https://doi.org/10.9734/bpi/acpr/v1/19883D

[19] Sylim, P., Liu, F., Marcelo, A., & Fontelo, P. (2018). Blockchain technology for detecting falsified and substandard drugs in distribution: pharmaceutical supply chain intervention. *JMIR research protocols*, *7*(9), e10163. https://doi.org/10.2196/10163

[20] Tian, F. (2016, June). An agri-food supply chain traceability system for China based on RFID & blockchain technology. In *2016 13th international conference on service systems and service management (ICSSSM)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICSSSM.2016.7538424

[21] Tseng, J. H., Liao, Y. C., Chong, B., & Liao, S. W. (2018). Governance on the drug supply chain via gcoin blockchain. *International journal of environmental research and public health*, *15*(6), 1055. https://doi.org/10.3390/ijerph15061055

[22] Underwood, S. (2016). Blockchain beyond bitcoin. *Communications of the ACM*, *59*(11), 15-17. https://dx.doi.org/10.1145/2994581

[23] Vafadarnikjoo, A., Badri Ahmadi, H., Liou, J. J., Botelho, T., & Chalvatzis, K. (2023). Analyzing blockchain adoption barriers in manufacturing supply chains by the neutrosophic analytic hierarchy process. *Annals of Operations Research*, *327*(1), 129-156. https://doi.org/10.1007/s10479-021-04048-6

[24] Velmovitsky, P. E., Bublitz, F. M., Fadrique, L. X., & Morita, P. P. (2021). Blockchain applications in health care and public health: increased transparency. *JMIR medical informatics*, *9*(6), e20713. https://doi.org/10.2196/20713

[25] Wang, D., & Zhang, X. (2020). Secure ride-sharing services based on a consortium blockchain. *IEEE Internet of Things Journal*, *8*(4), 2976-2991. https://doi.org/10.1109/JIOT.2020.3023920

[26] Wang, Y., Han, J. H., & Beynon-Davies, P. (2019). Understanding blockchain technology for future supply chains: a systematic literature review and research agenda. *Supply Chain Management: An International Journal*, *24*(1), 62-84. https://doi.org/10.1108/SCM-03-2018-0148

[27] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)* (pp. 557-564). IEEE. https://doi.org/10.1109/BigDataCongress.2017.85

## Authors Biography

**R. Jeevaraj** is a Research Scholar in the Department of Computer Science and Engineering at JAIN (Deemed-to-be University), Bengaluru, Karnataka, India. He is currently working as an Assistant Professor in the Department of Information Science and Engineering at Global Academy of Technology, Bengaluru. Prior to this, he served in academic roles at Dayananda Sagar University and SJB Institute of Technology (SJBIT), Bengaluru. He has 9 years of experience in teaching and 3years in research. His primary areas of interest include Machine Learning, Blockchain, and Quantum Computing. He is actively engaged in exploring innovative solutions in these domains. He has participated in various academic conferences and workshops. His research contributions focus on developing secure and efficient computing technologies. He is passionate about integrating emerging technologies into practical applications. He has guided students in research projects related to his areas of interest. He is committed to continuous learning and knowledge sharing. His goal is to contribute to advancements in technology through research and innovation.

**Dr. Ajay Kumar Singh** did his B. E from Kumaon Engineering College, Dwarahat, Almora, Uttarakhand. M. Tech from Sam Higginbottom University of Agriculture Technology and Sciences, Allahabad, U.P, Ph. D from Jaypee University of Information Technology, Solan, H.P, Short Term Post-PhD from Thu Dau Mot University Vietnam. He is currently working in Jain (Deemed-to-be University) as Professor. He worked in many Colleges and Universities like Raj Kumar Goel Institute of Technology, Ghaziabad, (U.P), Krishna Institute of Engineering Technology, Ghaziabad, (U.P), Meerut Institute of Engineering Technology, Meerut, (U.P), Radha Govind Engineering College, Meerut, (U.P), Sir Padampat Singhania University, Bhatewar, Udaipur, Rajasthan, Jaypee University of Information Technology, Waknaghat, Solan (H.P), Mody University of Science and Technology, Lakshmangarh, Sikar, Rajasthan, Regional Engineering College (Now N.I.T.) Kurukshetra (Haryana). Software Solution Integrated Ltd. Delhi. He taught 25 different subjects in Bachelor, Master and Ph. D Degree. He set many exam paper too. He evaluated two Ph.D thesis. He guided one Ph. D student and 17 M. Tech students in various domain. He is having 25 years of experience. His area of interest is Artificial Intelligence, Data Science and Networking. He chaired session in international conferences and participated in several FDP programs. He took several guest lectures. He was HoD in two different colleges. He was centre controller for exam. He was member of BoS committee. He has published more than 75 research papers 5 international patents and presented his paper in India and abroad.