



AgriMedChain-AI: an intelligent blockchain-based agricultural medicine supply chain framework for traceability, counterfeit detection, and sustainable farming

A. Vijay Kumar^{a,*}, Amjan Shaik^b

^aDepartment of Computer Science and Engineering, Bharatiya Engineering Science & Technology Innovation University, Gownivaripalli, Gorantla, Andhra Pradesh, India

^bSt. Peter's Engineering College, Hyderabad, Telangana, India

Abstract

The proliferation of agricultural medicines has supported crop productivity, but counterfeit pesticides, herbicides, fertilizers, and bio-based products, fragmented supply-chain management, and limited transparency remain major concerns. This study proposes AgriMedChain-AI, a framework integrating artificial intelligence (AI), blockchain, and the Internet of Things (IoT) to improve security and transparency in agricultural-medicine supply chains. The architecture uses QR codes for authentication, IoT sensors for real-time logistics data, Hyperledger Fabric and smart contracts for transaction security, and Random Forest and XGBoost models for counterfeit detection, anomaly detection, and risk prediction. A synthetic dataset of 50,000 supply-chain records, including 3,000 counterfeit and 47,000 genuine records, was evaluated. XGBoost achieved 99.48% accuracy, 93.63% precision, 98.00% recall, and a 95.77% F1-score for the counterfeit class. The framework achieved 97.1% traceability integrity and a 95.8% anomaly-detection rate. Transparency increased from 68.5% for the traditional system to 98.3%, while the proposed Hyperledger Fabric implementation achieved 420 transactions per second with an average latency of 0.82 s, a 71.2% reduction relative to the 2.85 s traditional-database baseline. Under the evaluated simulation conditions, the framework improved traceability, authentication, and supply-chain monitoring while supporting an integrated operational performance assessment.

DOI: [10.46481/jnsps.2027.3715](https://doi.org/10.46481/jnsps.2027.3715)

Keywords: Artificial intelligence, Blockchain, Internet of Things, Counterfeit detection, Agricultural traceability

Article History:

Received: 16 July 2026

Received in revised form: 09 September 2026

Accepted for publication: 11 September 2026

Available online: 30 September 2026

© 2027 The Author(s). Published by the [Nigerian Society of Physical Sciences](#) under the terms of the [Creative Commons Attribution 4.0 International license](#). Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

Communicated by: B. J. Falaye

1. Introduction

Over the last decade, growing food demand, socio-economic development, and sustainable development have reinforced the crucial role of agriculture worldwide. To increase crop productivity, farmers rely on agricultural medicines such as fertilizers, pesticides, herbicides, and bio-based prod-

ucts. Recent studies indicate that the global agricultural market is expanding because of precision farming, food demand, and climate variability [1–3]. Despite this growing demand, agricultural-medicine supply chains face numerous issues, including unauthorised vendors, inadequate information sharing and regulatory oversight, and counterfeit medicines. These issues can cause substantial economic losses and can threaten food safety, environmental sustainability, and farmer welfare.

Counterfeit and substandard fertilizers and pesticides are major concerns for regulatory bodies worldwide [4]. Their cir-

*Corresponding Author Tel. No.: +91-988-588-7400.

Email address: 2024spcse048@bestiu.edu.in (A. Vijay Kumar^{id})

culatation among farmers can reduce crop productivity, contaminate soil, create human-health risks, and increase cultivation costs. Traditional centralised systems can also be vulnerable to unauthorised access, data manipulation, and inefficient information sharing among stakeholders, while real-time product tracking may remain limited.

Advances in digital technologies have created opportunities to develop more transparent and efficient agricultural-medicine supply chains. Blockchain [5] provides distributed, decentralised, and tamper-evident record storage and can support logistics traceability; artificial intelligence (AI) can support counterfeit prediction and detection and supply-chain optimisation; and Internet of Things (IoT) sensors can monitor storage and transportation conditions, including temperature and humidity, to support the quality, safety, and integrity of agricultural medicines throughout the supply chain. Although many researchers have studied blockchain traceability in food supply chains [3, 5, 6], a research gap remains in agricultural-medicine traceability.

Existing studies often focus on individual technologies rather than integrating blockchain, AI, and IoT into a unified framework capable of real-time tracking, intelligent counterfeit detection, and automated decision support. In this article, we propose AgriMedChain-AI, a framework designed to promote sustainable farming, regulatory compliance, and transparency through integrated blockchain, AI, and IoT technologies. The framework comprises six architectural layers: an agricultural medicine supply-chain layer, an IoT and authentication layer, an edge-computing layer, a blockchain layer, an AI layer, and an application layer.

The objectives of this research are to develop a blockchain-enabled framework for improved transparency; integrate IoT sensors and devices for real-time tracking of the medicine supply chain; implement AI models for counterfeit-medicine detection; design blockchain smart contracts to automate supply-chain processes; and experimentally evaluate the framework using large-scale simulated agricultural-medicine supply-chain transactions with respect to efficiency, accuracy, scalability, and performance.

The proposed AgriMedChain-AI framework contributes to the Agriculture 5.0 vision by promoting sustainable farming practices, reducing counterfeit-medicine circulation, enhancing food security, and supporting digital transformation. Its intended societal benefits include greater regulatory transparency, a more intelligent agricultural supply chain, and increased farmer confidence. Through the combination of blockchain, AI, and IoT, this research provides a foundation for next-generation agricultural-medicine supply-chain management.

2. Literature survey

This section reviews existing frameworks, their advantages, remaining research gaps, and improvements required for agricultural-medicine supply-chain systems.

2.1. Blockchain-based agricultural supply-chain traceability

Agricultural-medicine supply chains involve multiple stake-

holders, including manufacturers, distributors, retailers, farmers, government agencies, consumers, and auditors. Providing end-to-end traceability and transparency across these stakeholders is challenging because information systems can be fragmented and data can be manipulated. Blockchain has emerged as a potential solution because of its distributed, decentralised, immutable, and transparent characteristics.

Saranya and Maheswari [7] proposed a Proof-of-Transaction-based blockchain transparency system for agricultural supply chains. Their framework addresses product access control and user authentication to improve tracking and reduce product adulteration. The study focuses on traceability and user authentication but does not provide intelligent counterfeit-medicine detection. Blockchain-enabled transparency systems have also been implemented for products such as soybean [8] and other food supply chains using smart contracts and distributed ledgers. Such systems can nevertheless face scalability, transaction-latency, and decision-support limitations. Permissioned platforms such as Hyperledger Fabric can improve controlled transparency and automate smart-contract execution.

The Internet of Things (IoT) has expanded agricultural monitoring through continuous, real-time data collection. IoT sensors and devices can monitor crop health, temperature, humidity, logistics operations, and pesticide or herbicide application. Studies in Refs. [9–13] show that IoT systems integrated with cloud platforms can provide farmers with timely information on irrigation, fertilizer use, and crop-disease management. However, many IoT solutions rely on centralised databases, creating potential risks of data tampering and single points of failure. In addition, many systems monitor environmental parameters rather than tracking agricultural medicines throughout the supply chain. Integrating IoT data with blockchain may improve data integrity and traceability.

Artificial intelligence and machine-learning (ML) models are widely used to analyse large datasets. In agriculture, AI has been used for crop-disease prediction, soil analysis, weather forecasting, and resource utilisation. Recent studies [14–19] have also explored AI and ML for identifying abnormal activities and fraudulent transactions. Machine-learning and deep-learning algorithms, including support vector machines, Random Forest, and convolutional neural networks, have demonstrated strong performance in detecting suspicious activities in logistics and network environments. However, many frameworks use AI as a standalone tool rather than integrating it with a decentralised blockchain framework, and relatively little research focuses specifically on counterfeit agricultural-medicine supply chains.

The integration of blockchain, edge computing, and cloud computing has recently received attention as a way to address latency and scalability challenges in supply chains. Liu and Cai [20] presented an edge–cloud–blockchain framework for agricultural-product traceability with AI-driven anomaly detection and smart-contract optimisation. Their framework reported improvements in accuracy, latency, and transaction throughput; however, requirements specific to agricultural medicines, including counterfeit prevention, product authentication, and reg-

ulatory compliance, remain comparatively underexplored.

2.2. Research gap analysis

The literature review identifies several research gaps. Most blockchain-based solutions focus on food products rather than agricultural medicines, and existing traceability systems generally emphasise transparency without specifically targeting counterfeit agricultural medicines. IoT monitoring systems may remain disconnected from blockchain networks, while AI techniques are often applied independently in centralised systems. Consequently, fully integrated blockchain–AI–IoT architectures remain limited. Existing architectures also provide limited treatment of regulatory compliance and sustainability assessment, while the socio-economic effects of counterfeit medicines on farmers, consumers, and environmental sustainability remain insufficiently addressed.

2.3. Motivation and research directions

To address these limitations, this research proposes AgriMedChain-AI, which integrates blockchain, AI, and IoT for agricultural-medicine supply-chain management. The framework combines a distributed and decentralised blockchain network for medicine tracking, IoT-enabled monitoring, QR-based authentication, AI-based counterfeit detection, and smart contracts for process automation. The intended outcome is a secure, transparent, and sustainable traceability ecosystem.

Unlike existing systems, AgriMedChain-AI focuses specifically on agricultural medicines and is designed to provide end-to-end lifecycle traceability and automated compliance verification. The framework aims to support sustainable Agriculture 5.0 environments.

3. Proposed methodology

3.1. Overview of the AgriMedChain-AI framework

AgriMedChain-AI is organised into six interconnected architectural layers: (1) Agricultural Medicine Supply Chain Layer, (2) IoT & Authentication Layer, (3) Edge Computing Layer, (4) Blockchain Layer, (5) AI Layer, and (6) Application Layer. The layers operate sequentially while supporting bidirectional information exchange across the supply-chain ecosystem.

Layer 1: Agricultural Medicine Supply Chain Layer. This physical layer represents the movement of agricultural medicines from manufacturing through distribution, storage, and retail to the farmer. It establishes the operational context in which product identity, movement, and transaction information are generated.

Layer 2: IoT & Authentication Layer. This layer captures product, location, and environmental information using RFID, QR codes, temperature, humidity, and GPS sensing technologies. Product and batch identifiers are associated with the corresponding supply-chain records to support authentication and traceability.

Layer 3: Edge Computing Layer. The edge layer processes data close to its point of generation. Its functions include data

filtering, aggregation, local validation, and secure communication. This layer reduces unnecessary data transmission and prepares validated information for subsequent blockchain and AI processing.

Layer 4: Blockchain Layer. This layer provides the trusted data-management infrastructure of AgriMedChain-AI. Hyperledger Fabric maintains the distributed ledger, while smart contracts enforce predefined supply-chain rules and access-control mechanisms. Validated transactions are recorded to provide auditable and tamper-evident traceability.

Layer 5: AI Layer. The AI layer analyses supply-chain and IoT-derived information to support counterfeit detection, anomaly detection, risk assessment, and operational analytics. Machine-learning models use relevant product, transaction, and sensor-derived features to identify potentially abnormal or fraudulent activities.

Layer 6: Application Layer. The application layer delivers traceability, authentication, risk-analysis, and decision-support services to stakeholders, including manufacturers, distributors, retailers, farmers, and regulators.

3.2. Working principle

Agricultural-medicine events are generated at the physical supply-chain level and captured through IoT and authentication mechanisms. The Edge Computing Layer filters, aggregates, and locally validates the incoming information. Validated transactions are submitted to the Blockchain Layer, where smart-contract rules and ledger mechanisms provide trusted transaction management. The AI Layer analyses relevant blockchain and IoT-derived data for counterfeit detection, anomaly identification, and risk analytics. Finally, the Application Layer presents traceability and analytical results to authorised supply-chain stakeholders. Figure 1 shows the system architecture of the AgriMedChain-AI framework.

The manufacturer generates a unique QR code for every medicine batch, and IoT devices continuously monitor transportation. The data are channelled through the blockchain network by IoT gateways. A smart contract validates each transaction and stores the resulting record in Hyperledger Fabric. The AI module analyses the data to detect counterfeit medicines and anomalies. Authorised stakeholders access information through secure applications.

3.3. Mathematical model

Let $M = \{m_1, m_2, \dots, m_n\}$ represent agricultural-medicine batches, $S = \{s_1, s_2, \dots, s_k\}$ represent supply-chain stakeholders, $T = \{t_1, t_2, \dots, t_p\}$ represent blockchain transactions, and $I = \{i_1, i_2, \dots, i_q\}$ represent IoT sensor observations.

3.3.1. Traceability function

Let M_i denote an agricultural-medicine batch and $T(M_i)$ denote the set of all validated supply-chain transactions associated with that batch. The traceability function is defined as

$$TF(M_i) = \sum_{T_j \in T(M_i)} T_j, \quad (1)$$

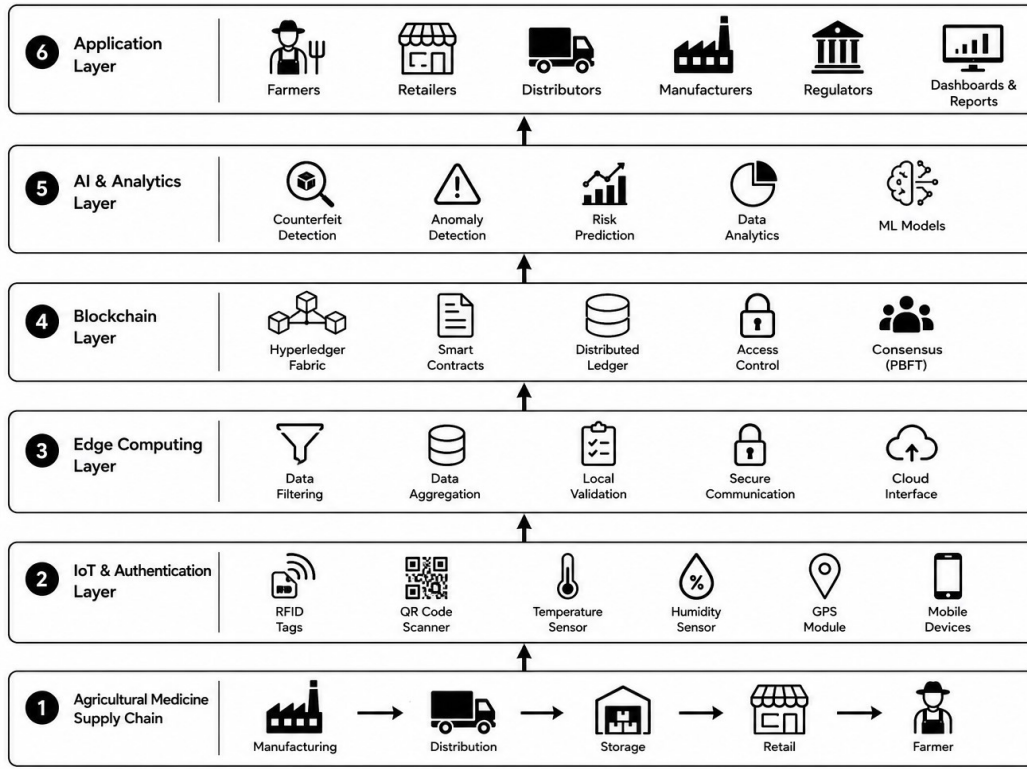


Figure 1: System architecture of the AgriMedChain-AI framework.

where each transaction represents a verified event such as manufacturing, distribution, storage, transfer, retail, or final delivery. Thus, the traceability computation considers only the transaction history of the selected batch rather than the complete blockchain transaction set.

Let $T = \{T_1, T_2, \dots, T_n\}$ denote the complete set of supply-chain transactions, and let M_i represent the selected agricultural-medicine batch. Define the batch-membership indicator as

$$\mathcal{I}(T_j, M_i) = \begin{cases} 1, & \text{if transaction } T_j \text{ is associated with batch } M_i, \\ 0, & \text{otherwise.} \end{cases} \quad (2)$$

The batch-specific traceability function is therefore defined as

$$TF(M_i) = \sum_{j=1}^n \mathcal{I}(T_j, M_i) T_j. \quad (3)$$

Alternatively, using an indexed subset,

$$T(M_i) = \{T_j \in T : T_j \rightarrow M_i\}, \quad (4)$$

and therefore

$$TF(M_i) = \sum_{T_j \in T(M_i)} T_j. \quad (5)$$

3.3.2. Transaction verification success rate

The Transaction Verification Success Rate (TVSR) is

$$TVSR = \frac{N_v}{N_t} \times 100, \quad (6)$$

where N_v is the number of successfully verified transactions and N_t is the total number of transaction-verification requests. TVSR evaluates transaction-processing reliability under increasing workload. Unlike cryptographic ledger integrity, TVSR may vary with transaction load because verification requests can experience rejection, timeout, or processing failures under high workload. Cryptographic blockchain integrity is evaluated separately through hash-chain and ledger-consistency verification.

3.3.3. Counterfeit classification and supply-chain risk

The AI classifier predicts authenticity according to

$$CD = f(X), \quad (7)$$

where X contains transaction and sensor attributes and f denotes the Random Forest or XGBoost model. The stated output encoding is

$$CD = \begin{cases} 1, & \text{Authentic product,} \\ 0, & \text{Counterfeit product.} \end{cases} \quad (8)$$

The supply-chain risk score is

$$R = \sum_{i=1}^n w_i x_i, \quad (9)$$

where w_i is a feature weight and x_i is a risk factor. Examples include temperature deviation, transit delay, authentication failure, and inventory mismatch.

3.3.4. Integrated supply-chain performance index

To provide a unified measure of the operational performance of the proposed AgriMedChain-AI framework, an Integrated Supply-Chain Performance Index (ISPI) is defined. Unlike a conventional sustainability index that requires independently measured environmental, economic, and social outcomes, the proposed ISPI combines three directly evaluated supply-chain dimensions: environmental compliance, traceability performance, and counterfeit prevention. Each component is normalised to a 0–100 scale, and equal weighting is applied. The ISPI is calculated as

$$ISPI = E + T + \frac{C}{3}, \quad (10)$$

where E , T , and C represent the normalised environmental compliance, traceability, and counterfeit-prevention scores, respectively. The resulting index provides an aggregate measure of supply-chain performance under the experimental conditions evaluated in this study.

The ISPI should therefore be interpreted as a composite supply-chain performance measure rather than as a direct measure of overall environmental, economic, or social sustainability. Equal weighting is adopted because no empirical basis is available for assigning different priorities to the three dimensions. Accordingly, the weights are defined as

$$\alpha = \beta = \gamma = \frac{1}{3}, \quad \alpha + \beta + \gamma = 1. \quad (11)$$

and the index as

$$SI = \frac{1}{3} \text{ environmental} + \frac{1}{3} \text{ traceability performance} + \frac{1}{3} \text{ counterfeit-prevention}, \quad (12)$$

with the resulting SI reported as a percentage after normalisation.

3.3.5. Hyperledger fabric transaction model

Let a transaction proposal be represented as

$$TP = (ID, M_i, D, S, t), \quad (13)$$

where ID is the unique transaction identifier, M_i is the agricultural-medicine batch identifier, D is the transaction data, S is the client identity/signature, and t is the transaction timestamp. The transaction is first submitted by an authorised client to the relevant endorsing peers.

The endorsement condition is represented as

$$E(TP) = \begin{cases} 1, & \text{if the endorsement policy is satisfied,} \\ 0, & \text{otherwise.} \end{cases} \quad (14)$$

Only transactions satisfying the predefined endorsement policy are forwarded to the ordering service. The ordering service establishes the transaction order:

$$O(TP_1, TP_2, \dots, TP_n) \rightarrow B_k, \quad (15)$$

where B_k is the ordered block containing a sequence of transactions.

After delivery to the peers, each transaction undergoes validation:

$$V(TP) = E(TP) \wedge VS(TP) \wedge RW(TP), \quad (16)$$

where $E(TP)$ is endorsement-policy validation, $VS(TP)$ is version/read-set validation, and $RW(TP)$ is read–write-set consistency validation. The committed ledger is represented as

$$L_{k+1} = L_k \cup \{TP_j : V(TP_j) = 1\}. \quad (17)$$

Invalid transactions remain recorded in the block for audit purposes but do not update the world state.

Hyperledger Fabric is a permissioned blockchain and does not use proof-of-work mining. Its transaction lifecycle comprises client proposal, endorsement, endorsement-policy evaluation, ordering, block distribution, validation, and ledger commitment. In AgriMedChain-AI, authorised participants submit transaction proposals; designated peers simulate the chaincode and generate endorsements; and the ordering service establishes a deterministic transaction sequence and packages transactions into blocks. Channel peers then validate endorsement policies and read/write-set versions before valid transactions update the distributed ledger and world state. This architecture provides controlled participation, deterministic ordering, auditable transaction history, and tamper-evident storage without proof-of-work computation.

3.3.6. AI-based counterfeit-detection model

The model uses Manufacturer ID, Batch Number, QR Authentication Result, GPS Coordinates, Temperature, Humidity, Delivery Time, Storage Conditions, and Transaction History. The feature vector is

$$X = (x_1, x_2, x_3, \dots, x_n). \quad (18)$$

The manuscript first represents the Random Forest prediction as

$$RF(X) = \frac{1}{N} \sum_{i=1}^N T_i(X), \quad (19)$$

where T_i is a decision tree and N is the number of trees. For classification, let $T_i(X)$ denote the predicted class label produced by the i th decision tree, where

$$T_i(X) \in \{0, 1\}, \quad (20)$$

with 0 representing a genuine agricultural medicine and 1 representing a counterfeit agricultural medicine.

The Random Forest classification is then defined by majority voting:

$$\widehat{y}(X) = \text{mode}\{T_1(X), T_2(X), \dots, T_N(X)\}. \quad (21)$$

Equivalently, for binary classification,

$$\widehat{y}(X) = \begin{cases} 1, & \sum_{i=1}^N \mathbb{I}[T_i(X) = 1] > \frac{N}{2}, \\ 0, & \text{otherwise,} \end{cases} \quad (22)$$

where $I[\cdot]$ is an indicator function. If the probability output from each tree is used, then

$$P(y = 1 | X) = \frac{1}{N} \sum_{i=1}^N P_i(y = 1 | X), \quad (23)$$

and the classification threshold is

$$\widehat{y}(X) = \begin{cases} 1, & P(y = 1 | X) \geq 0.5, \\ 0, & P(y = 1 | X) < 0.5. \end{cases} \quad (24)$$

For counterfeit-product classification, the final prediction is therefore determined by majority voting across the decision trees.

3.4. Proposed algorithms

Algorithm 1: AgriMedChain-AI traceability.

Input: Agricultural medicine batch M .

Output: Verified traceability record.

- 1: Register manufacturer.
- 2: Generate a unique QR code.
- 3: Create a blockchain entry.
- 4: Collect IoT sensor data.
- 5: Transmit data to the blockchain node.
- 6: Execute smart-contract validation.
- 7: **if** the product is registered **then**
- 8: Approve the transaction.
- 9: **else**
- 10: Reject the transaction.
- 11: **end if**
- 12: Execute AI counterfeit detection.
- 13: **if** the product is authentic **then**
- 14: Update the ledger and notify stakeholders.
- 15: **else**
- 16: Generate an alert and flag the counterfeit product.
- 17: **end if**
- 18: Store the immutable record.
- 19: Calculate the Integrated Supply-Chain Performance Index.
- 20: Display traceability information.

Algorithm 2: Secure agricultural-medicine transaction validation and commitment.

Input: Product record P , Batch ID M_i , QR identifier Q , and transaction T .

Output: Commit or reject decision.

- 1: Receive transaction T from an authorised stakeholder.
- 2: Generate a unique transaction identifier and validation context.
- 3: Submit T as a provisional transaction proposal.
- 4: Verify the digital signature and stakeholder authorisation.
- 5: Verify Product ID, Batch ID, QR identifier, timestamp, and nonce.
- 6: Check whether the transaction is a duplicate or replayed request.

- 7: Execute the smart contract and evaluate the endorsement/validation policy.
- 8: **if** any mandatory cryptographic or policy validation fails **then**
- 9: Set Decision(T) = Reject and terminate the transaction.
- 10: **end if**
- 11: Forward the validated transaction features to the AI counterfeit/anomaly-detection module.
- 12: Obtain $AI(T) \in \{\text{Authentic, Counterfeit/Anomalous}\}$.
- 13: **if** $AI(T) = \text{Counterfeit/Anomalous}$ **then**
- 14: Set Decision(T) = Reject and record the rejection event.
- 15: **else**
- 16: Set Decision(T) = Commit.
- 17: Submit the endorsed transaction to the Fabric ordering service.
- 18: The ordering service establishes transaction order and packages transactions into a block.
- 19: Fabric peers perform final validation.
- 20: Commit a valid transaction to the blockchain ledger/world state.
- 21: **end if**
- 22: Return the final transaction status.

The transaction progression is represented as

$$T_{\text{submitted}} \rightarrow T_{\text{provisional}} \rightarrow T_{\text{SC}} \rightarrow T_{\text{AI}}, \quad (25)$$

followed by

$$T_{\text{AI}} = \begin{cases} T_{\text{commit}}, & \text{if } SC = 1 \wedge AI = \text{Authentic}, \\ T_{\text{reject}}, & \text{otherwise.} \end{cases} \quad (26)$$

3.5. Smart-contract workflow

Figure 2 shows the smart-contract workflow.

Figure 3 shows the smart-contract verification sequence supplied in the manuscript.

3.6. QR-code-based cryptographic authentication

Each agricultural medicine product is assigned a unique Product ID and Batch ID during registration. The authorised manufacturer digitally signs the associated product metadata using its private key. The resulting signed record is linked to the QR identifier and stored or referenced through the permissioned blockchain. During product verification, the QR code is scanned and the corresponding blockchain record is retrieved. The system verifies the digital signature, validates the product and batch identifiers, checks the timestamp and nonce, and confirms that the verification request has not previously been consumed.

Duplicate, expired, or inconsistent verification requests are rejected or forwarded to the anomaly-detection module for further analysis. This mechanism ensures that possession of a copied QR image alone is insufficient to establish product authenticity. The verification process is represented in Figure 3.

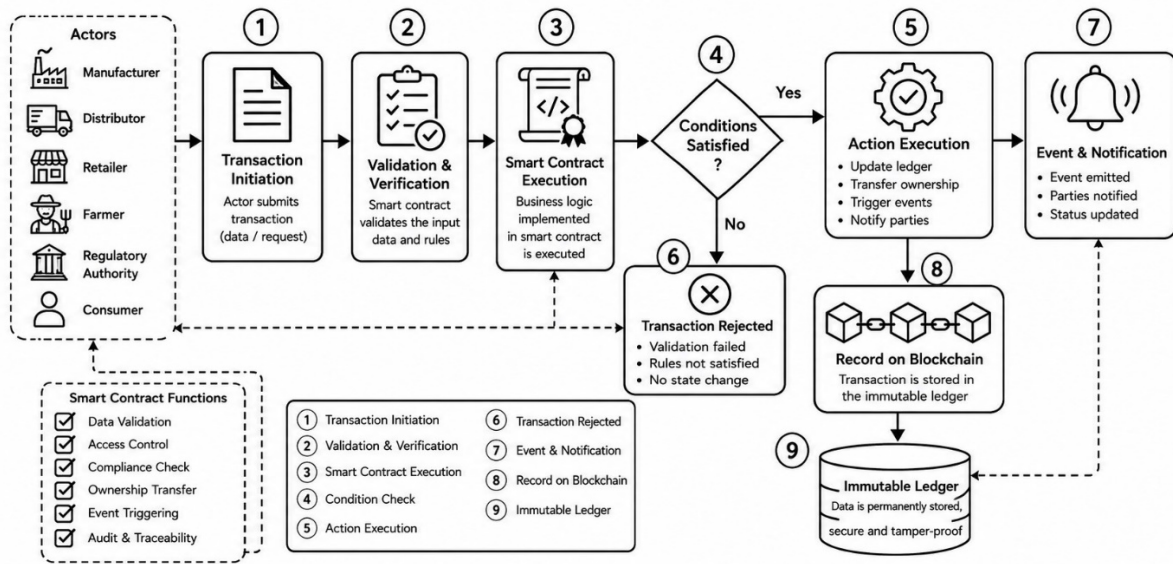


Figure 2: Smart-contract workflow.

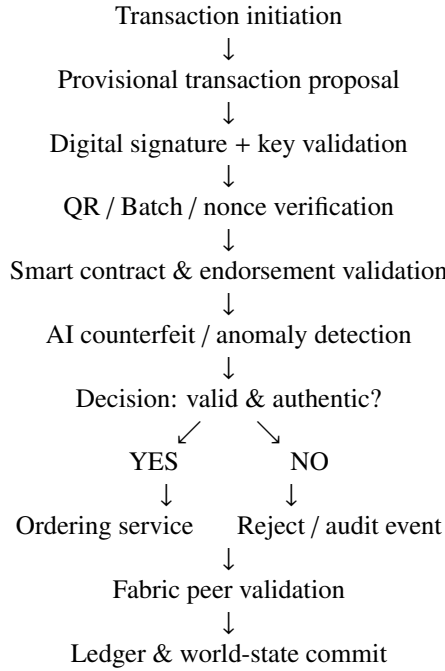


Figure 3: Smart-contract verification workflow.

3.7. Smart-contract validation process

The supplied smart-contract validation sequence is Product Registration → Unique ID Generation → Metadata Creation → Digital Signature → Blockchain Record → QR Generation → Scan Request → Signature Verification → Nonce/Timestamp Check → Duplicate-Scan Check → Authentication Decision → Immutable Verification Record. Figure 4 presents this sequence.

3.8. AI-based anomaly-detection module

In addition to counterfeit-medicine detection, the proposed AgriMedChain-AI framework incorporates an anomaly-detection module to identify abnormal events occurring throughout the agricultural-medicine supply chain. An anomaly is defined as any transaction or operational activity that deviates significantly from normal supply-chain behaviour and may indicate fraud, product tampering, logistics failure, unauthorised access, or regulatory non-compliance.

The anomaly-detection system analyses both blockchain transaction records and IoT sensor observations. The anomaly categories considered in this study are unauthorised stakeholder transactions, invalid QR-code authentication attempts, temperature-threshold violations during storage and transportation, abnormal shipment delays, inventory inconsistencies, duplicate batch registrations, and suspicious location deviations identified through GPS tracking.

Let

$$X = \{x_1, x_2, \dots, x_n\} \quad (27)$$

represent the feature vector extracted from blockchain and IoT data. The anomaly-detection function is

$$AD = f(X), \quad AD = \begin{cases} 1, & \text{Anomalous transaction,} \\ 0, & \text{Normal transaction.} \end{cases} \quad (28)$$

The XGBoost classifier is employed to learn the behavioural patterns of normal and anomalous supply-chain activities. Transactions identified as anomalous trigger alerts and are forwarded to regulatory authorities for further investigation.

4. Experimental setup, simulation environment, dataset description, and performance evaluation

4.1. Experimental setup

The proposed AgriMedChain-AI framework was implemented and evaluated in a simulation environment comprising

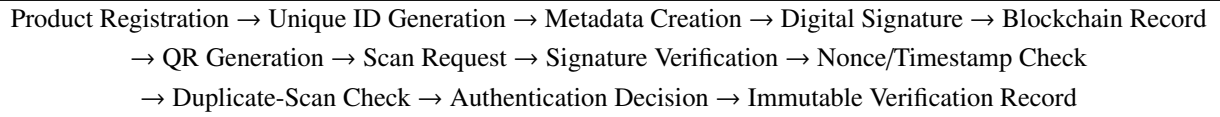


Figure 4: Smart-contract validation process.

Table 1: Hardware configuration.

Component	Specification
Processor	Intel Core i9-13900K
RAM	32 GB DDR5
Storage	1 TB SSD
GPU	NVIDIA RTX 4070
Operating system	Ubuntu 24.04 LTS

Table 2: Software environment.

Software	Version
Python	3.12
Hyperledger Fabric	2.5
Docker	27.0
Node.js	22
MongoDB	8.0
TensorFlow	2.18
Scikit-Learn	1.6
Jupyter Notebook	7.6.3

the hardware configuration, software environment, blockchain parameters, AI-model configuration, and dataset. The experimental evaluation covers counterfeit-detection performance, blockchain performance, traceability and integrity, smart-contract performance, and the integrated supply-chain performance assessment.

4.2. Simulation environment

The simulation environment integrated the blockchain platform, AI and machine-learning models, network, and database components. The hardware configuration is summarised in Table 1.

The software environment is listed in Table 2.

The blockchain parameters are presented in Table 3.

The proposed AgriMedChain-AI framework uses Hyperledger Fabric 2.5 as a permissioned blockchain platform. The ordering layer is configured using the Raft ordering service. Transactions are first executed and endorsed by authorised peers according to the configured chaincode endorsement policy. Endorsed transactions are subsequently submitted to the ordering service, where Raft establishes a consistent transaction order and packages transactions into blocks. The ordered blocks are distributed to channel peers, which perform transaction validation, including endorsement and version/read-write-set checks, before committing valid transactions to the ledger and updating the world state.

Table 3: Blockchain parameters.

Parameter	Value
Blockchain	Hyperledger Fabric 2.5
Network type	Permissioned blockchain
Ordering service	Raft
Consensus model	Crash Fault Tolerant (CFT)
Consensus mechanism	Hyperledger Raft
Chaincode	AgriMedChain-AI
TLS	Enabled
Number of peers	10
Block size	1 MB
Block generation time	2 seconds
Smart-contract type	Chaincode
Ledger type	Distributed

Table 4: AI-model configuration.

Parameter	Value
Random Forest trees	500
XGBoost estimators	300
Learning rate	0.01
Train-test ratio	80:20
Cross-validation	10-fold

The AI-model configuration is given in Table 4.

4.3. Dataset description

The experimental evaluation was conducted using a synthetically constructed counterfeit-detection dataset to assess the feasibility of integrating machine-learning classification with the AgriMedChain-AI framework. Counterfeit labels were generated using predefined supply-chain indicators, including QR-authentication failure, duplicate-batch identification, abnormal environmental conditions, logistics delays, and inventory inconsistencies. Using the same indicators both to generate labels and as classifier inputs introduces a potential target-leakage concern. Consequently, the machine-learning evaluation is interpreted as an assessment of the models' ability to learn the predefined synthetic counterfeit-labelling pattern rather than as independent validation of real-world counterfeit detection.

Accordingly, the reported classification metrics are synthetic-data evaluation results and do not establish generalisation to independently verified counterfeit agricultural medicines. Independent validation using externally sourced and independently labelled counterfeit and genuine products is required before real-world performance claims can be made.

Table 5: Dataset characteristics.

Attribute	Description
Batch ID	Unique medicine batch identifier
Product Type	Fertilizer/Pesticide/Fungicide
Manufacturer ID	Source manufacturer
Distributor ID	Distribution entity
GPS Location	Shipment coordinates
Temperature	Storage temperature
Humidity	Environmental humidity
QR Authentication	Valid/Invalid
Transit Time	Delivery duration
Inventory Status	Available/Unavailable
Compliance Score	Regulatory compliance
Product Authenticity	Genuine/Counterfeit

Due to the absence of a publicly available benchmark dataset containing end-to-end agricultural-medicine traceability information, counterfeit-product labels, IoT sensor measurements, and blockchain transaction records, a synthetic agricultural-medicine supply-chain dataset was developed for this study to emulate realistic supply-chain operations. The dataset contains 50,000 transaction records representing interactions among manufacturers, distributors, retailers, regulators, and farmers. Each record includes attributes such as Batch ID, Product Type, Manufacturer ID, Distributor ID, GPS Location, Temperature, Humidity, QR Authentication Status, Transit Time, Inventory Status, Compliance Score, and Product Authenticity Label. Table 5 describes these attributes.

Authenticity labels were assigned based on predefined simulation rules derived from counterfeit indicators reported in the supply-chain literature. Transactions exhibiting characteristics such as invalid QR authentication, duplicate batch identifiers, unauthorised stakeholder participation, abnormal environmental conditions, significant logistics delays, or inconsistent inventory records were labelled as anomalous or counterfeit. Records satisfying all compliance requirements were labelled as genuine.

The experimental dataset contains 50,000 agricultural-medicine supply-chain records. For the counterfeit-detection task, 47,000 records are labelled genuine and 3,000 records are labelled counterfeit. Counterfeit status constitutes the target variable for the counterfeit-classification experiments. A separate anomaly-detection target is defined independently for the anomaly-detection experiments and is not conflated with the counterfeit labels. The dataset was partitioned into training (80%) and testing (20%) subsets for model development and evaluation. Because the dataset was synthetically generated for simulation purposes, no personal, proprietary, or sensitive information was used. Dataset statistics are shown in Table 6.

4.4. Counterfeit-detection performance

The AI module was evaluated using Random Forest and XGBoost classifiers, as shown in Table 7.

Table 6: Dataset statistics.

Metric	Value
Total transactions	50,000
Genuine products	47,000
Counterfeit products	3,000
Manufacturers	100
Distributors	250
Retailers	500
Farmers	5,000
IoT sensor records	150,000

Table 7: Random Forest and XGBoost counterfeit-detection performance.

Metric	Random Forest	XGBoost
Accuracy	97.8%	99.48%
Precision	97.1%	93.63%
Recall	96.8%	98.00%
F1-score	96.9%	95.77%

Table 8: Throughput comparison.

System	TPS
Traditional database	180
Ethereum	210
Hyperledger Fabric	420

Table 9: Latency analysis.

System	Average latency
Traditional system	2.85 s
Ethereum	1.92 s
AgriMedChain-AI	0.82 s

XGBoost achieved higher accuracy and recall than Random Forest, whereas Random Forest achieved higher precision and F1-score. The manuscript therefore reports XGBoost as the model selected for deployment.

4.5. Blockchain performance analysis

Table 8 compares transaction throughput across the evaluated systems.

Under the reported simulation conditions, the Hyperledger Fabric implementation achieved 420 transactions per second. Table 9 presents the corresponding latency comparison. Compared with the traditional database-based approach, which exhibits an average transaction latency of 2.85 s, AgriMedChain-AI reduces the latency to 0.82 s. This corresponds to a 71.2% relative reduction in latency, calculated using the traditional database-based approach as the comparison baseline.

Table 10: Traceability integrity evaluation.

Transactions	Traceability integrity
1,000	99.2%
5,000	98.8%
10,000	98.2%
25,000	97.5%
50,000	97.1%

Table 11: Smart-contract evaluation.

Metric	Value
Validation success rate	99.1%
Fraudulent transactions blocked	96.7%
Audit-time reduction	37.2%
Compliance-verification accuracy	98.3%

Table 12: Integrated supply-chain performance components.

Parameter	Score
Environmental compliance	93.8%
Traceability score	97.1%
Counterfeit prevention	98.4%
Integrated supply-chain performance index	96.4%

4.6. Traceability integrity evaluation

Table 10 shows the reported traceability integrity under increasing transaction loads.

The framework maintained a reported traceability integrity of 97.1% at 50,000 transactions.

4.7. Smart-contract evaluation

The smart-contract evaluation results are given in Table 11.

The reported results indicate that the smart-contract mechanism supported transaction validation, fraudulent-transaction blocking, compliance verification, and reduced audit time under the experimental conditions.

4.8. Integrated supply-chain performance index (ISPI)

The proposed framework achieved an Integrated Supply-Chain Performance Index (ISPI) of 96.4%, calculated using the equally weighted environmental compliance, traceability, and counterfeit-prevention components. The value represents the aggregate performance of these three evaluated dimensions under the experimental conditions. Table 12 presents the component scores.

4.9. Comparative analysis

Table 13 compares the traditional system, a blockchain-only system, and AgriMedChain-AI using the reported evaluation values.

4.10. Anomaly-detection performance evaluation

To evaluate anomaly-detection capability, the dataset was augmented with labelled abnormal events representing agricultural-medicine supply-chain threats. For anomaly detection, a separate binary target variable was defined as Normal or Anomalous. Approximately 5,000 of the 50,000 records were assigned the anomalous label and the remaining 45,000 records were assigned the normal label. The anomaly labels were generated synthetically, and the anomaly target was evaluated independently of the counterfeit target.

The anomaly-detection model was evaluated using an 80:20 training-testing split and 10-fold cross-validation. Table 14 reports the model metrics.

The reported results show that the proposed framework identified labelled anomalous events under the synthetic evaluation conditions. The reported 95.8% detection rate is used as the anomaly-detection result in the subsequent discussion.

4.11. Data integration and temporal feature construction

The experimental dataset comprises 50,000 supply-chain transaction records and 150,000 IoT sensor observations. The transaction records represent manufacturing, distribution, storage, transportation, retail, and verification events, whereas the IoT records represent environmental and logistics observations associated with these transactions. Sensor observations are linked to transactions using the corresponding Batch ID/Product ID and timestamp. Multiple sensor observations associated with a single transaction are temporally aggregated to construct one transaction-level feature vector.

For each transaction, numerical sensor variables are summarised using statistical features such as mean, minimum, and maximum values, while categorical attributes such as QR authentication and location consistency are retained as transaction-level features. Consequently, the classifier operates on transaction-level samples rather than treating every sensor observation as an independent sample. Missing observations, when present, are handled according to the predefined data-cleaning procedure, and all preprocessing parameters are derived from the training partition to avoid data leakage.

The feature-engineering transformation is represented as

$$X_i = [T_{\text{mean}}, T_{\text{max}}, T_{\text{min}}, H_{\text{mean}}, H_{\text{max}}, H_{\text{min}}, D, Q, G, C], \quad (29)$$

where T denotes temperature features, H denotes humidity features, D denotes transit duration, Q denotes QR-authentication status, G denotes geographical/location consistency, and C denotes compliance/transaction features. The resulting vector X_i is supplied to the Random Forest and XGBoost classifiers.

4.12. Discussion

The simulation results indicate that integrating blockchain, IoT, AI, QR-based authentication, and smart contracts can support agricultural-medicine supply-chain traceability under the evaluated conditions. The framework achieved XGBoost counterfeit-classification accuracy of 99.48%, an anomaly-detection rate of 95.8%, traceability integrity of 97.1%, an

Table 13: Comparative analysis of the evaluated systems.

Parameter	Traditional system	Blockchain only	AgriMedChain-AI
Traceability	72.3%	90.2%	97.1%
Transparency	68.5%	92.1%	98.3%
Counterfeit detection	60.8%	71.4%	98.4%
Throughput (TPS)	180	210	420
Latency (s)	2.85	1.92	0.82
Sustainability score	70.2%	85.4%	96.4%

Table 14: Anomaly-detection model metrics.

Metric	Value (%)
Accuracy	96.2
Precision	95.4
Recall	95.8
F1-score	95.6
Detection rate	95.8

average latency of 0.82 s, and a processing capacity of 420 transactions per second. Because the evaluation uses synthetic data and a controlled simulation environment, these findings demonstrate technical feasibility under the specified configuration rather than real-world production performance.

5. Results and discussion

5.1. Overview of experimental results

The framework achieved XGBoost counterfeit-detection accuracy of 99.48%, precision of 93.63%, recall of 98.00%, an F1-score of 95.77%, traceability integrity of 97.1%, throughput of 420 TPS, average latency of 0.82 seconds, and an Integrated Supply-Chain Performance Index of 96.4%.

5.2. Counterfeit-detection analysis

For the reported 50,000-record evaluation, the XGBoost confusion-matrix counts are TN = 46,800, FP = 200, FN = 60, and TP = 2,940. Table 15 reports the derived performance values as supplied in the manuscript.

Figure 5 shows the supplied confusion-matrix graphic.

The Random Forest and XGBoost models were evaluated using the AI module and IoT-sensor-derived data. XGBoost achieved higher accuracy and recall, whereas Random Forest achieved higher precision and F1-score. The comparison is repeated in Table 16 and Figure 6.

5.3. ROC-curve analysis

The reported area under the receiver operating characteristic curve (ROC-AUC) is 0.981 for Random Forest and 0.992 for XGBoost. Figure 7 shows the supplied ROC curves.

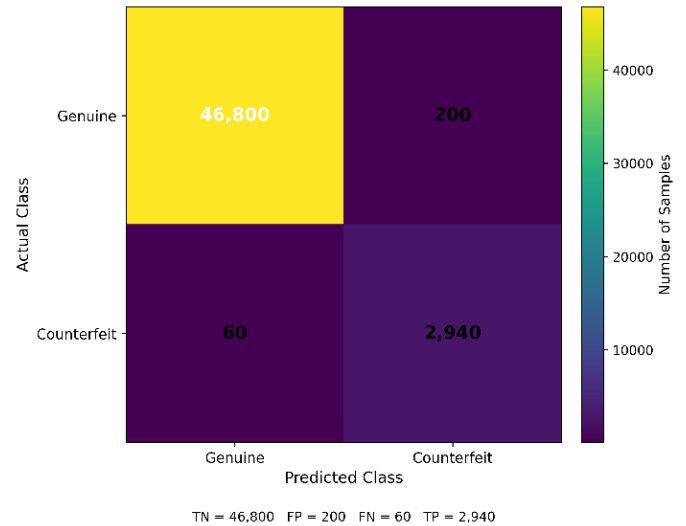


Figure 5: XGBoost confusion matrix for the reported 50,000-record evaluation.

5.4. Confusion-matrix analysis

A second confusion matrix reports the following test-set counts:

	Predicted genuine	Predicted counterfeit
Actual genuine	9,400	120
Actual counterfeit	40	440

The corresponding reported performance statistics are Accuracy = 99.48%, Precision-Counterfeit = 93.63%, Recall-Counterfeit = 98.00%, F1-score-Counterfeit = 95.77%, Specificity-Genuine = 99.57%, Balanced Accuracy = 98.79%, and MCC = 0.9552. Figure 8 presents the XGBoost confusion matrix for the reported 50,000-record counterfeit-detection evaluation. The confusion-matrix counts and derived performance statistics are consistent with those reported in Table 15.

5.5. Blockchain performance evaluation

Figure 9 compares the reported throughput and latency values for the traditional system, Ethereum-based system, and AgriMedChain-AI.

Table 15: Counterfeit-detection analysis for the reported 50,000-record evaluation.

Metric	Calculation	Result
Accuracy	$(46,800 + 2,940)/50,000$	99.48%
Precision	$2,940/(2,940 + 200)$	93.63%
Recall/Sensitivity	$2,940/(2,940 + 60)$	98.00%
F1-score	$2TP/(2TP + FP + FN)$	95.77%
Specificity	$46,800/(46,800 + 200)$	99.57%
Balanced accuracy	$(98.00 + 99.57)/2$	98.79%
MCC	Standard MCC formula	0.9552

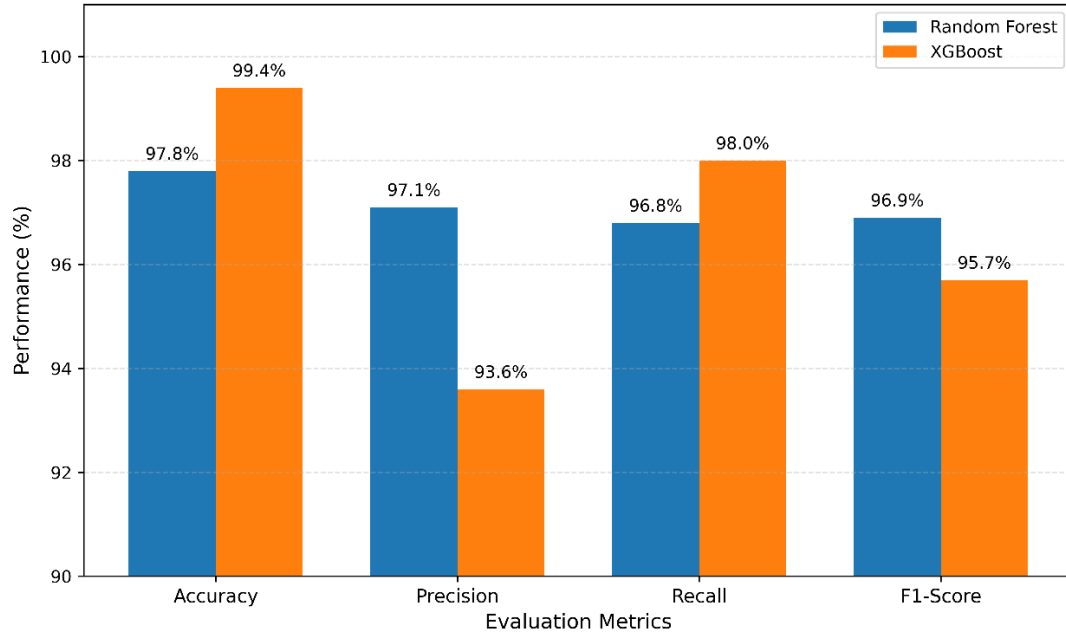


Figure 6: Counterfeit-detection performance comparison.

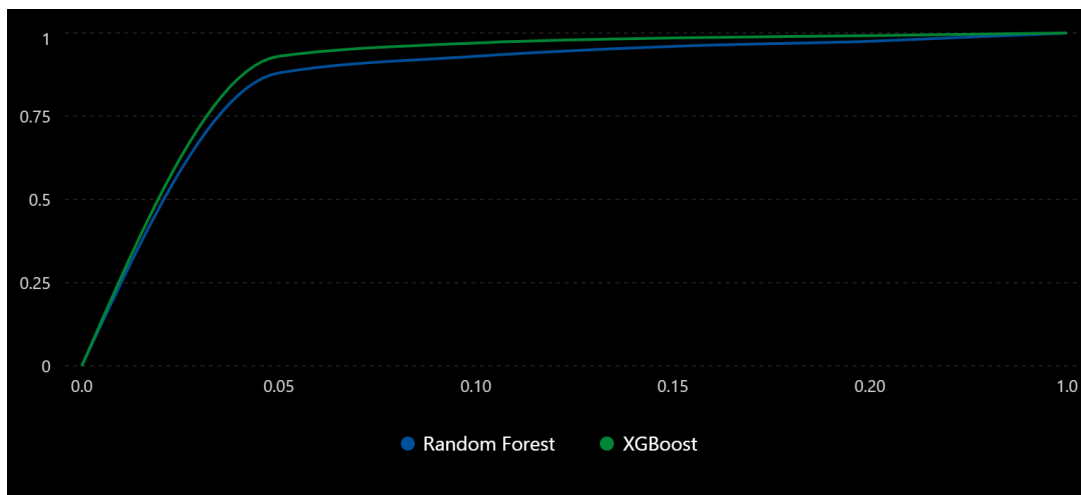


Figure 7: ROC curves for the counterfeit-detection models.

5.6. Traceability reconstruction success (TRS)

Figure 10 shows the traceability reconstruction success under increasing transaction load. The y-axis represents the per-

centage of expected batch-level trace events successfully reconstructed. The figure uses a 0–100% scale to avoid visual exaggeration of small differences.

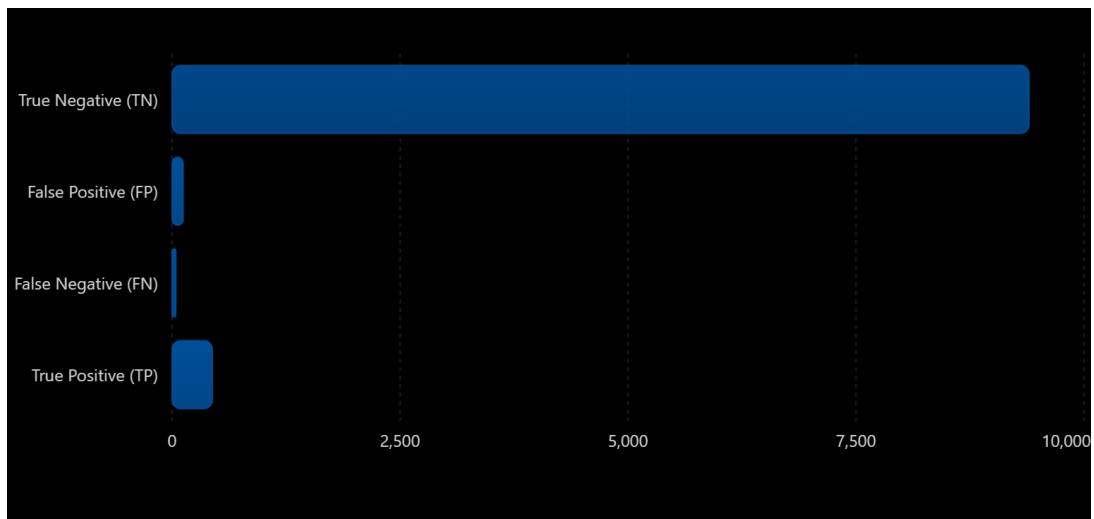
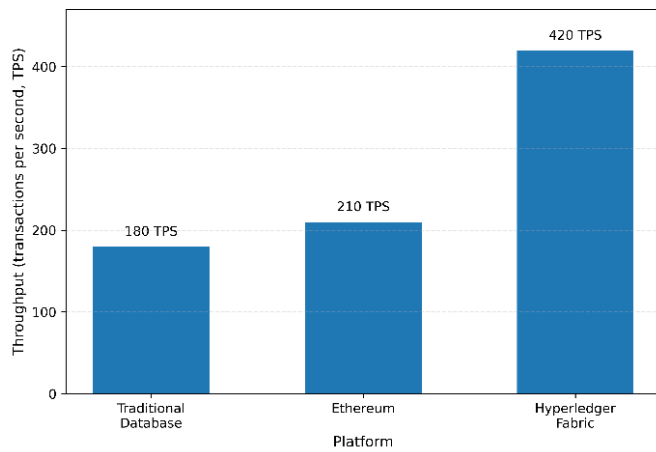
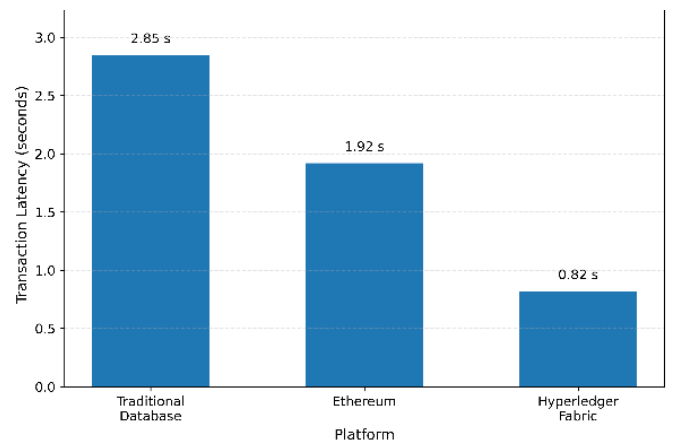


Figure 8: Confusion-matrix statistics of the XGBoost-based counterfeit-detection model.



(a) Throughput comparison.



(b) Latency comparison.

Figure 9: Throughput and latency comparison of the traditional, Ethereum-based, and Hyperledger Fabric systems.

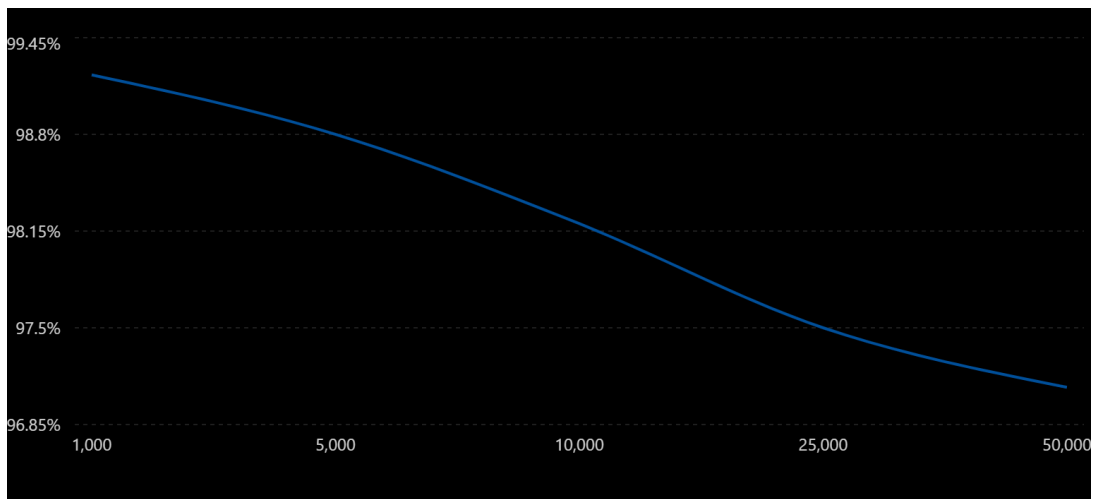


Figure 10: Traceability reconstruction success under increasing transaction load.

Table 16: Random Forest and XGBoost metrics.

Metric	Random Forest	XGBoost
Accuracy	97.8	99.48
Precision	97.1	93.63
Recall	96.8	98.00
F1-score	96.9	95.77

5.7. Comparative analysis

Figure 11 shows the reported comparison of the competing systems. Evaluation parameters include traceability, transparency, security, counterfeit detection, throughput, and sustainability.

5.8. Integrated supply-chain performance index (ISPI)

The Integrated Supply-Chain Performance Index (ISPI) was evaluated using environmental compliance, counterfeit prevention, and traceability performance. The reported scores are 93.8% for environmental compliance, 98.4% for counterfeit prevention, 97.1% for traceability efficiency, and 96.4% for the Integrated Supply-Chain Performance Index.

5.9. Comparative discussion

The experimental findings report higher values for AgriMedChain-AI than for the traditional and blockchain-only systems across the comparative indicators evaluated in this simulation. Table 17 presents the manuscript's comparison with selected existing studies [21–24].

5.10. Controlled throughput and latency benchmark

To ensure a fair comparison, the traditional database, Ethereum-based implementation, and Hyperledger Fabric implementation were evaluated using an identical transaction workload derived from the agricultural-medicine supply-chain dataset. The same transaction payload structure, hardware environment, software environment, concurrency configuration, transaction count, warm-up procedure, and benchmark duration were maintained across all platforms. Throughput was measured as the number of successfully confirmed transactions per second, while latency was measured from transaction submission to the corresponding platform-specific confirmation event.

The performance of the evaluated models was assessed using standard classification metrics, including accuracy, precision, recall, and F1-score. The reported values correspond to the evaluation results obtained on the specified test dataset. Because the experiments reported in this study do not include repeated independent runs with recorded variability, the results are presented as single-point measurements rather than mean $\pm$ standard deviation. No statistical variability is inferred beyond the reported experimental values. This controlled protocol is intended to minimise the influence of workload, hardware, payload, concurrency, and measurement differences on the comparative performance results.

5.11. Traceability integrity

Traceability integrity measures the proportion of expected batch-level supply-chain events that can be successfully reconstructed from the ledger. For batch M_i , a trace is considered successful when all required transaction events can be retrieved, associated with the correct batch identifier, and reconstructed in the expected chronological sequence. A failed trace occurs when one or more required events are missing, incorrectly associated, unavailable, or fail the defined ledger/state validation criteria. Traceability integrity is calculated as the ratio of successful traces to the total number of evaluated traces. The metric therefore evaluates the completeness and reconstructability of supply-chain histories and should not be interpreted as a measure of cryptographic blockchain integrity.

5.12. Evaluation of validation, fraud prevention, audit efficiency, and compliance

The proposed framework was evaluated using separate test cases for transaction validation, fraudulent-transaction blocking, audit efficiency, and compliance verification. Each evaluation task was associated with a predefined ground-truth outcome. Validation success was measured as the proportion of transaction test cases correctly accepted or rejected according to the predefined validation rules. Fraudulent-transaction blocking was measured as the proportion of ground-truth fraudulent transactions correctly rejected by the framework.

Audit-time reduction was calculated by comparing the mean time required to complete an identical audit task using the conventional procedure and the proposed framework. Compliance accuracy was calculated as the proportion of compliance test cases for which the system generated the correct rule-based decision.

5.13. Cross-validation and ROC–AUC evaluation

To assess the robustness of counterfeit detection, stratified k -fold cross-validation was performed while preserving the genuine/counterfeit class distribution across folds. In each iteration, $k-1$ folds were used for model training and the remaining fold was used for validation. ROC–AUC analysis was used to evaluate the discrimination capability of the classification models. The reported AUC values are the single AUC measurements obtained from the corresponding evaluation results. The reported AUC values of 0.981 and 0.992 indicate strong discrimination between the respective classes under the evaluated experimental conditions.

5.14. Implications for Agriculture 5.0

The proposed framework is intended to support the vision of Agriculture 5.0 through intelligent supply-chain automation, real-time product authentication, secure data sharing among stakeholders, sustainable agricultural practices, regulatory-compliance monitoring, and farmer-centric digital transformation.

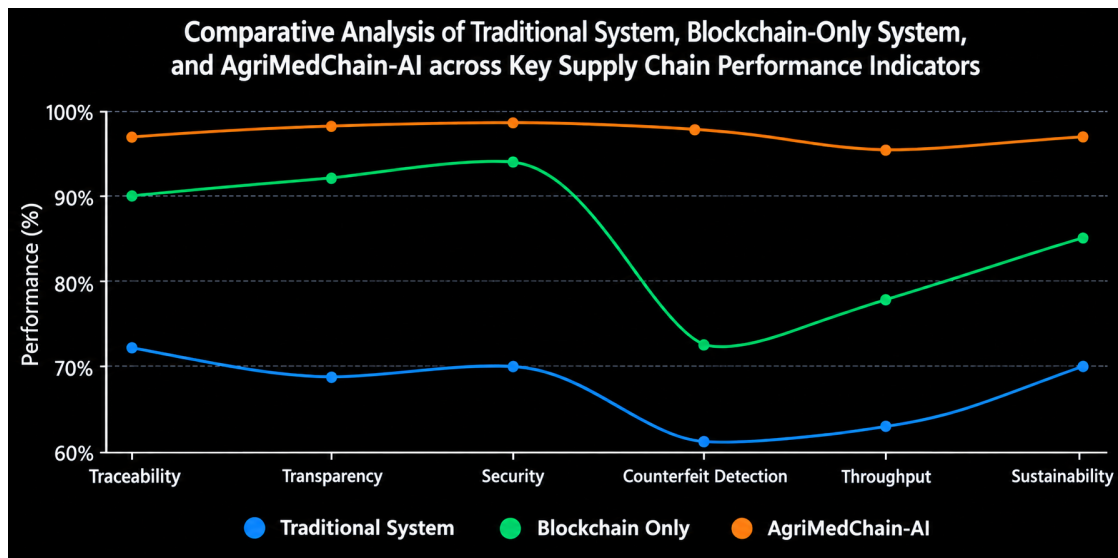


Figure 11: Normalised comparative performance of the evaluated supply-chain architectures. All heterogeneous indicators are transformed to a common 0–100 scale before visualisation. Percentage-based indicators are retained on their defined scale, whereas throughput and latency are normalised using benefit-oriented and cost-oriented min–max normalisation, respectively.

Table 17: Comparative analysis of existing studies and AgriMedChain-AI.

Study	Application domain	Blockchain platform	AI/ML component	IoT	Dataset size	Counterfeit detection	TPS	Latency (s)	Major limitations
Grecuccio <i>et al.</i> (2020) [21]	Food traceability	Ethereum	No	Yes	10,000	No	120	2.8	No AI-based authentication
Rai <i>et al.</i> (2021) [22]	Agricultural supply chain	Hyperledger Fabric	No	Yes	15,000	Partial	180	2.1	Limited counterfeit analysis
Gomasta <i>et al.</i> (2023) [23]	Pharmaceutical supply chain	Hyperledger Fabric	Yes	No	25,000	Yes	250	1.8	No IoT monitoring
Hasan <i>et al.</i> (2024) [24]	Agricultural products	Ethereum	Yes	Yes	30,000	Partial	290	1.4	Scalability issues
Saidu <i>et al.</i> (2025)	Medicine traceability	Hyperledger Fabric	Yes	Partial	35,000	Yes	320	1.2	No sustainability evaluation
AgriMedChain-AI (Proposed)	Agricultural medicine supply chain	Hyperledger Fabric	XGBoost-based detection	Yes	50,000	Yes	420	0.82	Addresses traceability, counterfeit detection, and sustainability simultaneously

6. Conclusions and future scope

This study presented AgriMedChain-AI, a framework combining blockchain, IoT, and AI for agricultural-medicine supply-chain management. It addresses counterfeit agrochemicals, limited transparency, fragmented information sharing, and poor traceability. By using Hyperledger Fabric, IoT monitoring, machine-learning-based counterfeit detection, QR-code authentication, and automated smart contracts, the framework provides an architecture for managing agricultural medicines throughout their life cycle.

The experimental results under the specified simulation conditions demonstrated the technical feasibility of the framework. It achieved a counterfeit-detection accuracy of 99.48%, 93.63% precision, 98.00% recall, and a 95.77% F1-score. It maintained 97.1% traceability integrity over 50,000 blockchain transactions, handling 420 transactions per second with an average latency of 0.82 seconds. Additionally, the framework reduced manual auditing time by 37.2% and achieved an ISPI of 96.4%, obtained from the equally weighted environmental compliance, traceability, and counterfeit-prevention components.

This result indicates integrated performance across the eval-

uated supply-chain dimensions; however, it should not be interpreted as a comprehensive measure of environmental, economic, or social sustainability. Within the comparative simulation, AgriMedChain-AI reported higher evaluated values than the traditional and blockchain-only methods across the stated security, transparency, traceability, counterfeit-detection, efficiency, and sustainability indicators. The combination of blockchain tracking with AI analysis supports early detection of suspicious activities, tamper-evident record management, and automated regulatory-compliance checks through smart contracts.

Beyond its technical objectives, the framework is intended to reduce counterfeit agricultural medicines, support farmer trust, improve food safety, protect the environment, and promote transparent agricultural governance in line with Agriculture 5.0. The experimental evaluation was conducted in a controlled simulation environment comprising 10 peers and a workload of 50,000 records. The results demonstrate technical feasibility under the specified experimental configuration; however, they should not be interpreted as evidence of production-scale suitability or regulatory readiness.

Real-world agricultural-medicine supply chains involve substantially greater heterogeneity in participants, transaction rates, network conditions, IoT devices, regulatory requirements, and operational workflows. Consequently, external validation using larger distributed deployments, real agricultural-medicine datasets, physical IoT infrastructure, and participation from relevant supply-chain and regulatory stakeholders is required before production deployment. Future studies will investigate scalability under larger peer networks, geographically distributed nodes, higher transaction volumes, heterogeneous network conditions, and real-world regulatory and operational constraints.

Future research will also investigate federated learning, digital-twin technology, edge-cloud intelligence, cross-border blockchain compatibility, carbon-footprint evaluation, green supply-chain analysis, and large-language-model (LLM)-based decision-support systems. Furthermore, technologies such as 6G communication, quantum-resistant blockchain security, and autonomous agricultural agents may support further research on scalability, security, privacy, and intelligent decision-making. Future work will extend the ISPI by incorporating independently measurable environmental indicators, including carbon emissions, energy consumption, waste generation, and resource utilisation. Such indicators could support an environmentally validated sustainability assessment rather than one based solely on operational and compliance-related proxies.

Data availability

The data supporting the findings of this study are available from the corresponding author upon reasonable request.

Declaration of competing interest

The authors declare that they have no known competing fi-

nancial interests or personal relationships that could have appeared to influence the work reported in this manuscript.

Funding

The authors received no specific funding from any public, commercial, or not-for-profit organisation for this research.

References

- [1] W.-M. Cheng, Y.-J. Chen, T.-C. Chen, X.-Y. Zhuang, C.-W. Chang, W.-C. Chien, Y.-H. Wu & R. Chen, "Implementation of mini-greenhouse based on precision agriculture", *2024 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)*, Kaohsiung, Taiwan, 2024, pp. 1–3. <https://doi.org/10.1109/ISPACS62486.2024.10868011>.
- [2] E. A. Aldhahri, A. A. Almazroi, M. H. Alkinani, N. Ayub, E. A. Alghamdi & N. F. Janbi, "Smart farming: Enhancing urban agriculture through predictive analytics and resource optimization", *IEEE Access* **13** (2025) 72375. <https://doi.org/10.1109/ACCESS.2025.3530006>.
- [3] M. Dutta, D. Gupta, S. Tharewal, D. Goyal, J. K. Sandhu, M. Kaur, A. A. Alzubi & J. M. Alanazi, "Internet of Things-based smart precision farming in soilless agriculture: Opportunities and challenges for global food security", *IEEE Access* **13** (2025) 34238. <https://doi.org/10.1109/ACCESS.2025.3540317>.
- [4] H. S. Kassem, M. A. Hussein & H. Ismail, "Toward fraudulent pesticides in rural areas: Do farmers' recognition and purchasing behaviors matter?", *Agronomy* **11** (2021) 1882. <https://doi.org/10.3390/agronomy11091882>.
- [5] X. Li, J. Du, W. Li & F. Shahzad, "Green ambitions: A comprehensive model for enhanced traceability in agricultural product supply chain to ensure quality and safety", *Journal of Cleaner Production* **420** (2023) 138397. <https://doi.org/10.1016/j.jclepro.2023.138397>.
- [6] Z. Wang & P. Liu, "Application of blockchain technology in agricultural product traceability system", in *Artificial Intelligence and Security*, X. Sun, Z. Pan & E. Bertino (Eds.), Springer, Cham, Switzerland, 2019, pp. 81–90. https://doi.org/10.1007/978-3-030-24271-8_8.
- [7] P. Saranya & R. Maheswari, "Proof of transaction (PoTx) based traceability system for an agriculture supply chain", *IEEE Access* **11** (2023) 10623. <https://doi.org/10.1109/ACCESS.2023.3240772>.
- [8] K. Salah, N. Nizamuddin, R. Jayaraman & M. Omar, "Blockchain-based soybean traceability in agricultural supply chain", *IEEE Access* **7** (2019) 73295. <https://doi.org/10.1109/ACCESS.2019.2918000>.
- [9] Y. Saidu, S. M. Shuhidan, D. A. Aliyu, I. A. Aziz & S. Adamu, "Convergence of blockchain, IoT, and AI for enhanced traceability systems: A comprehensive review", *IEEE Access* **13** (2025) 16838. <https://doi.org/10.1109/ACCESS.2025.3528035>.
- [10] M. U. Tariq, S. M. Saqib, T. Mazhar, M. A. Khan, T. Shahzad & H. Hamam, "Edge-enabled smart agriculture framework: Integrating IoT, lightweight deep learning, and agentic AI for context-aware farming", *Results in Engineering* **28** (2025) 107342. <https://doi.org/10.1016/j.rineng.2025.107342>.
- [11] H. Shahab, M. Naeem, M. Iqbal, M. Aqeel & S. S. Ullah, "IoT-driven smart agricultural technology for real-time soil and crop optimization", *Smart Agricultural Technology* **10** (2025) 100847. <https://doi.org/10.1016/j.atech.2025.100847>.
- [12] T. Adamo, D. Caivano, L. Colizzi, G. Dimauro & E. Guerriero, "Optimization of irrigation and fertigation in smart agriculture: An IoT-based micro-services framework", *Smart Agricultural Technology* **11** (2025) 100885. <https://doi.org/10.1016/j.atech.2025.100885>.
- [13] A. Dahane, R. Benameur & B. Kechar, "An IoT low-cost smart farming for enhancing irrigation efficiency of smallholders farmers", *Wireless Personal Communications* **127** (2022) 3173. <https://doi.org/10.1007/s11277-022-09915-4>.
- [14] R. Jing & P. Li, "Knowledge graph for integration and quality traceability of agricultural product information", *Frontiers in Sustainable Food Systems* **8** (2024) 1389945. <https://doi.org/10.3389/fsufs.2024.1389945>.

- [15] L. Li, P. Tian, J. Dai & F. Miao, "Design of agricultural product traceability system based on blockchain and RFID", *Scientific Reports* **14** (2024) 23599. <https://doi.org/10.1038/s41598-024-73711-2>.
- [16] S. M. Rajagopal, M. Supriya & R. Buyya, "Leveraging blockchain and federated learning in edge-fog-cloud computing environments for intelligent decision making with ECG data in IoT", *Journal of Network and Computer Applications* **233** (2025) 104037. <https://doi.org/10.1016/j.jnca.2024.104037>.
- [17] V. S. Rao, R. Balakrishna, Y. A. B. El-Ebiary, P. Thapar, K. A. Saravanan & S. R. Godla, "AI driven anomaly detection in network traffic using hybrid CNN-GAN", *Journal of Advances in Information Technology* **15** (2024) 886. <https://doi.org/10.12720/jait.15.7.886-895>.
- [18] M. Shabaz & K. N. Raju, "AI-driven traffic flow prediction and anomaly detection in smart cities: A multi-agent approach", *Transactions on Emerging Telecommunications Technologies* **36** (2025) e70279. <https://doi.org/10.1002/ett.70279>.
- [19] N. Shahin & L. Ismail, "Towards trustworthy sign language translation system: A privacy-preserving edge-cloud-blockchain approach", *Mathematics* **13** (2025) 3759. <https://doi.org/10.3390/math13233759>.
- [20] K. Liu & B. Cai, "Edge-cloud-blockchain integrated framework for agricultural product traceability: AI-driven anomaly detection and smart contract optimization", *Frontiers in Sustainable Food Systems* **10** (2026) 1784223. <https://doi.org/10.3389/fsufs.2026.1784223>.
- [21] J. Grecuccio, E. Giusto, F. Fiori & M. Rebaudengo, "Combining blockchain and IoT: Food-chain traceability and beyond", *Energies* **13** (2020) 3820. <https://doi.org/10.3390/en13153820>.
- [22] V. S. Rai, S. N. Ingale & S. Kullur, "Agroblock-blockchain based solution for agriculture", *International Journal of Engineering Research & Technology* **10** (2021) IJERTV10IS050411. <https://doi.org/10.5281/zenodo.18617830>.
- [23] S. S. Gomasta, A. Dhali, T. Tahlil, M. M. Anwar & A. B. M. S. Ali, "PharmaChain: Blockchain-based drug supply chain provenance verification system", *Heliyon* **9** (2023) e17957. <https://doi.org/10.1016/j.heliyon.2023.e17957>.
- [24] H. R. Hasan, A. Musamih, K. Salah, R. Jayaraman, M. Omar, J. Arshad & D. Bosovic, "Smart agriculture assurance: IoT and blockchain for trusted sustainable produce", *Computers and Electronics in Agriculture* **224** (2024) 109184. <https://doi.org/10.1016/j.compag.2024.109184>.