future internet

MDPI

Article

A Blockchain and IoT-Enabled Framework for Ethical and Secure Coffee Supply Chains

John Byrd [1], Kritagya Upadhyay [1,*], Samir Poudel [2], Himanshu Sharma [3] and Yi Gu [1]

[1] Department of Computer Science, Middle Tennessee State University, Murfreesboro, TN 37132, USA; jkb8d@mtmail.mtsu.edu (J.B.); yi.gu@mtsu.edu (Y.G.)
[2] Computational and Data Science, Middle Tennessee State University, Murfreesboro, TN 37132, USA; sp2ai@mtmail.mtsu.edu
[3] Department of Computer Science and Engineering, University of North Texas, Denton, TX 76203, USA; himanshusharma@my.unt.edu
* Correspondence: kritagya.upadhyay@mtsu.edu

Abstract

The global coffee supply chain is a complex multi-stakeholder ecosystem plagued by fragmented records, unverifiable origin claims, and limited real-time visibility. These limitations pose risks to ethical sourcing, product quality, and consumer trust. To address these issues, this paper proposes a blockchain and IoT-enabled framework for secure and transparent coffee supply chain management. The system integrates simulated IoT sensor data such as Radio-Frequency Identification (RFID) identity tags, Global Positioning System (GPS) logs, weight measurements, environmental readings, and mobile validations with Ethereum smart contracts to establish traceability and automate supply chain logic. A Solidity-based Ethereum smart contract is developed and deployed on the Sepolia testnet to register users and log batches and to handle ownership transfers. The Internet of Things (IoT) data stream is simulated using structured datasets to mimic real-world device behavior, ensuring that the system is tested under realistic conditions. Our performance evaluation on 1000 transactions shows that the model incurs low transaction costs and demonstrates predictable efficiency behavior of the smart contract in decentralized conditions. Over 95% of the 1000 simulated transactions incurred a gas fee of less than ETH 0.001. The proposed architecture is also scalable and modular, providing a foundation for future deployment with live IoT integrations and off-chain data storage. Overall, the results highlight the system's ability to improve transparency and auditability, automate enforcement, and enhance consumer confidence in the origin and handling of coffee products.

Keywords: coffee supply chain; blockchain; Internet of Things (IoT); smart contracts; traceability; ethereum; ethical sourcing; decentralized ledger

Academic Editor: Qiang Qu

Received: 7 July 2025
Revised: 22 July 2025
Accepted: 23 July 2025
Published: 27 July 2025

Citation: Byrd, J.; Upadhyay, K.; Poudel, S.; Sharma, H.; Gu, Y. A Blockchain and IoT-Enabled Framework for Ethical and Secure Coffee Supply Chains. *Future Internet* **2025**, *17*, 334. https://doi.org/10.3390/fi17080334

1. Introduction

1.1. Modern Coffee Supply Chain in a Global Context

Coffee is known to be one of the most significant commodities after crude oil and plays a crucial role in a country's economy, especially for coffee producing countries [1]. A coffee supply chain is an extremely complex multi-stakeholder process that includes farm-level production and harvesting, cooperative sorting, export and import logistics, roasting, retail distribution, and finally consumer delivery. Under contemporary conditions of globalization, a single bag of coffee can easily pass through at least five or more independent entities before finally reaching the end consumer [2]. In spite of this long and complex

supply chain process, most transactions and quality checks remain opaque and/or paper-based [3]. As a result of this lack of transparency, questions regarding the origin of coffee beans, ethical sourcing, bean quality, and handling necessary conditions are difficult to answer with certainty, especially from the consumer's perspective.

For example, a consumer purchasing a bag of "single-origin organic Ethiopian coffee" has no way to confirm if it was actually manufactured from a certified organic farm in Ethiopia, or if the beans were mixed with other lower-quality batches along the way. Likewise, exporters have little or no transparency into whether the beans were properly stored before roasting. Similarly, farmers may never receive a fair compensation due to a lack of proper coffee data lineage and due to the absence of the traceable documentation. These kinds of pressing issues pose ethical, operational, and financial risks to all the parties involved in the supply chain, from coffee farmers to end consumers.

These issues make us aware of how the current generation of supply chain system lacks real-time monitoring, auditability, interoperability, and accountability at each stage of the supply chain. Today, emerging technologies such as blockchain and the Internet of Things (IoT) offer powerful tools and features as solutions, allowing these supply chain issues and limitations to be addressed immediately [4]. When these two technologies are used together synergistically, they allow for an entirely new class of supply chain solutions that are verifiable, automated, and mainly transparent from one end to another.

1.2. Problem Motivation

Despite ongoing advancements in logistics and information systems, several unresolved challenges still persist within the coffee supply chain [5]. As can be seen in Figure 1, the following problem areas illustrate the limitations of the existing model and the opportunities for synergy using blockchain and IoT technologies [6].

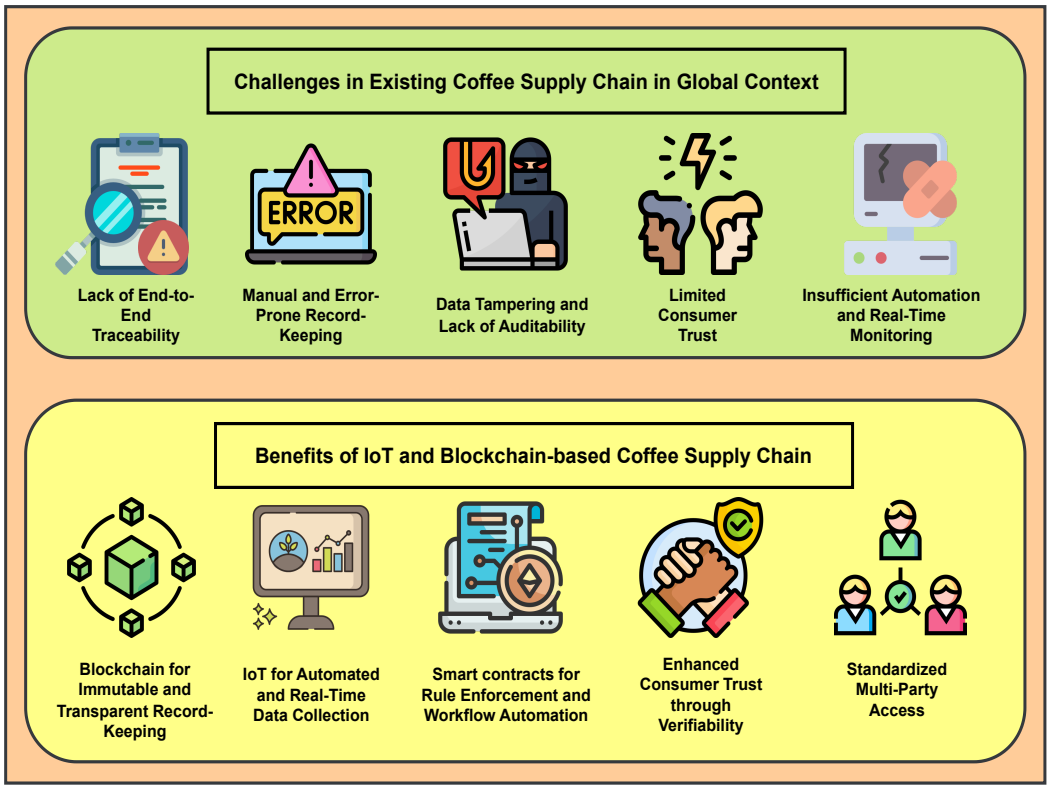

Figure 1. Comparative illustration of coffee supply chain challenges and proposed blockchain–IoT enhancements, emphasizing improvements in traceability, data integrity, transparency, and automated enforcement.

1.2.1. Lack of End-to-End Traceability

Current systems rarely capture the whole journey of a coffee batch from production and harvesting to consumption [7]. For instance, coffee beans collected from multiple farms are usually pooled and repackaged without adequate tracking. When the beans are blended or repackaged, the ability to trace them back to a specific region, farm, or even harvest season is lost. This lack of granular tracking limits the ability of stakeholders to verify ethical sourcing claims, support fair trade certifications, and ensure compliance with quality assurance protocols.

1.2.2. Manual and Error-Prone Record-Keeping

Especially in low-resource countries, paper logs remain a very common method during the farming and export stages [8]. These records are vulnerable to human error, misplacement, and even fabrication. For example, a farm might overstate the quantity of beans harvested to meet export quotas or under-report losses to avoid scrutiny. These inaccuracies introduce discrepancies that spread throughout the supply chain and ultimately erode the reliability of exported data.

1.2.3. Data Tampering and Lack of Auditability

Even in digitized systems, the absence of tamper-proof mechanisms leaves records vulnerable to unauthorized modifications. Stakeholders with privileged access can alter shipping dates, moisture levels, or origin declarations without detection. Because most existing systems are centralized, they depend on individual entities to maintain honesty, without a shared audit trail to verify actions; this undermines the credibility of traceability platforms and increases the risk of fraud, particularly when high-value certifications or pricing premiums are at stake.

1.2.4. Limited Consumer Trust

Modern consumers are increasingly concerned about the sustainability, origin, and ethical implications of their purchases [9]. However, the information available to end consumers in the current supply chain setup is often generic, unverifiable, or marketing-driven. For instance, QR codes or labels may direct users to static web pages with pre-written narratives rather than providing a real-time and authenticated view of the product's journey. This lack of transparency prevents consumers from making truly informed decisions and weakens brand trust.

1.2.5. Insufficient Automation and Real-Time Monitoring

Without the integration of real-time monitoring tools, key logistical and environmental parameters such as temperature, humidity, location, and transit times are often delayed or not tracked at all [10]. This is particularly critical during the storage and transport phases where poor handling conditions can degrade bean quality. For instance, prolonged exposure to high humidity during shipping can cause mold growth; however, without sensors or alerts such conditions may go unnoticed. Furthermore, the absence of automated event recording means that stakeholders cannot intervene proactively, leading to both quality losses and accountability gaps.

1.3. The Need for Blockchain and IoT in the Coffee Supply Chain

The synergy between blockchain [11] and Internet of Things (IoT) [12] technologies offers a compelling framework for addressing persistent inefficiencies and trust deficits within the coffee supply chain. When combined, these technologies can transform the current fragmented and opaque system into a transparent, data-driven, secure, and automated infrastructure, as presented in Figure 1. IoT devices serve as the interface between physical

events and digital records, while blockchain ensures that these records are tamper-proof, verifiable, and shared among all stakeholders. This convergence bridges the gap between real-world processes and reliable digital documentation, enabling end-to-end traceability, operational accountability, and consumer trust.

Below, we discuss the essential reasons why the synergy of blockchain and IoT is suitable for addressing the above-mentioned issues with the existing coffee supply chain.

1.3.1. Blockchain for Immutable and Transparent Record-Keeping

Blockchain technology provides a decentralized and append-only ledger, guaranteeing that every transaction or data entry is permanently recorded and resistant to tampering [13]. In the context of coffee supply chains, this allows critical events such as harvest registration, processing milestones, quality assessments, and shipment details to be captured in a format that is verifiable by all stakeholders. Because blockchain records are immutable, they cannot be modified or deleted after submission. This feature is essential for maintaining the integrity of claims regarding origin, certifications, and trade documentation.

1.3.2. IoT for Automated and Real-Time Data Monitoring and Collection

IoT devices such as RFID tags, GPS modules, digital weighing scales, and environmental sensors can be installed throughout the supply chain to collect data continuously and automatically. These devices reduce reliance on manual entry, which helps to eliminate human error and delays in data reporting. For example, GPS modules can monitor transit routes in real time, temperature sensors can alert handlers to spoilage risks, and RFID tags can preserve identity records for individual coffee batches. This automation provides the foundation for real-time visibility and enables proactive decision-making across the supply chain.

1.3.3. Smart Contracts for Rule Enforcement and Workflow Automation

Smart contracts are self-executing programs that enforce predefined business rules on the Ethereum blockchain [14,15]. Within a coffee supply chain, they can validate sensor inputs and enforce quality or compliance thresholds. For instance, a smart contract can prevent the transfer of ownership if a shipment's temperature exceeds an acceptable range or automatically release payment once verified delivery is confirmed. By replacing manual verification with autonomous logic, smart contracts improve fairness, accuracy, and efficiency across the system.

1.3.4. Enhanced Consumer Trust Through Verifiability

By linking IoT-generated data with blockchain storage, consumers can gain access to trusted and tamper-proof information about the coffee's journey. Scanning a QR code on the product package can reveal details such as farm origin, harvest date, processing steps, and storage conditions. These data are anchored in the blockchain, assuring consumers that there has been no alteration [16]. This level of transparency allows brands to differentiate themselves through verifiable ethical practices and quality assurance, thereby increasing customer loyalty and trust.

1.3.5. Standardized Multi-Party Access

Conventional supply chain systems often operate in silos, where each party maintains separate records and data inconsistencies are common. Blockchain provides a shared and synchronized ledger that allows all authorized participants to access the same set of information in real time. Farmers, cooperatives, exporters, auditors, and retailers can each interact with the system according to their role, with custom access controls in place to

protect sensitive information. This shared infrastructure minimizes reconciliation delays, increases transparency, and fosters better coordination among supply chain actors.

1.3.6. Enables Ethical Impact Assessment

The integration of blockchain and IoT allows for verifiable tracking of transactions, ownership, and environmental conditions, enabling both qualitative and quantitative assessments of ethical outcomes. This includes supporting farmer empowerment through transparent payment logs, enhancing digital inclusion via mobile wallet access, and facilitating fair trade compliance through auditable batch-level data. Such capabilities provide a concrete foundation for labeling the system as an "ethical supply chain".

1.4. Our Contributions

This paper present a practical framework for enhancing coffee supply chain transparency using blockchain and simulated IoT integration. This framework represents a simulation-based prototype in which realistic sensor outputs were modeled to test blockchain integration and smart contract functionality. Our key contributions are as follows:

- We propose a blockchain and IoT-based system architecture that enables secure and traceable transactions across all stages of the coffee supply chain.
- We design and implement Ethereum smart contract to handle ownership transfers, quality assurance, and environmental compliance, demonstrating how real-world data can trigger on-chain actions.
- We provide a unified role-based interaction model that aligns farmers, cooperatives, exporters, roasters, and retailers through transparent smart contract interactions.
- We simulate IoT sensor data, including RFID, GPS, weighing systems, environmental sensors, and mobile validation, then integrate these into blockchain-based smart contract workflows for end-to-end traceability testing.
- We evaluate performance using 1000 transactions and provide transaction fee, time distribution, and administrative cost insights, demonstrating low overhead and smart contract efficiency.
- We outline a future-ready system architecture by identifying the IoT hardware and platforms (e.g., Raspberry Pi, Node-RED) suitable for transitioning from simulation to real-world deployment.

1.5. Paper Organization

Our paper is structured as follows: Section 1 introduces the challenges in the existing coffee supply chain and motivation behind the need to integrate blockchain and IoT technologies. It also outlines key limitations such as lack of traceability, data tampering, and limited consumer trust to present the rationale for blockchain–IoT synergy. Section 2 reviews the relevant literature to highlight recent advancements in IoT-based monitoring, RFID tagging, communication protocols, and blockchain integration within agricultural and supply chain contexts. Section 3 details the proposed system architecture, including the simulated IoT dataset design, smart contract development, on-chain ledger structure, and stakeholder interaction model. Section 4 presents the results and discussion based on 1000 simulated blockchain transactions, focusing on transaction fees, completion times, and administrative overhead. Section 5 concludes the paper by summarizing contributions and practical implications. Finally, Section 6 outlines the challenges encountered and proposes future extensions, including real-world IoT integration, enhanced scalability, and interoperability with external certification systems.

2. Existing Studies and Literature Review

The integration of IoT and blockchain technologies presents significant opportunities for addressing the challenges discussed in the previous section. This review section examines key technical implementations across four critical domains that form the foundation of our proposed dual-layer architecture for coffee supply chains.

2.1. IoT Sensor Technologies for Coffee Environment Monitoring

Environmental monitoring constitutes a fundamental component in modern coffee supply chains. Rutayisire et al. (2017) pioneered an architecture utilizing pH, moisture, temperature, and humidity sensors connected to WiFi microcontrollers, demonstrating effective environmental data transmission with minimal power consumption [17]. Building on this foundation, Tippayawong et al. (2021) implemented DHT22 temperature and humidity sensors with Raspberry Pi 4 IoT gateways and LoRaWAN modules to achieve transmission ranges exceeding 10 km while maintaining 24-month battery life, which is particularly valuable for remote coffee-growing regions [18].

Addressing sensor calibration challenges, Morales and Castillo (2019) employed XBee-Pro S2C modules on ZigBee protocols, achieving measurement accuracy between 96–99% compared to laboratory-grade instruments while implementing self-healing mesh networks that are essential for dense plantation environments [19].

2.2. RFID and Tagging Technologies in Coffee Traceability Systems

RFID implementation offers robust physical traceability capabilities. Varriale et al. (2021) developed UHF RFID solutions operating in the 902–928 MHz range with 3–5 m read distances through coffee sacks. In addition, they incorporated anti-collision protocols, achieving 98% identification accuracy at conveyor speeds of 2.5 m/s [20]. Khan and Turowski (2016) addressed durability concerns with IP67-rated tags capable of withstanding 85–95% humidity levels while maintaining 99.3% read reliability over a 12-month period [21].

Energy efficiency advances were demonstrated by Durmus and Karaca (2022), who implemented a heterogeneous system combining passive ISO/IEC 18000-6C tags with IEEE 802.11ah active readers, resulting in a reduction of power consumption by 73% compared to conventional implementations [22].

2.3. Communication Protocols and Network Architectures

Network optimization remains critical for reliable deployment in agricultural settings. Morales and Castillo (2019) developed a hybrid architecture combining ZigBee mesh networks with LoRaWAN gateways, achieving 99.7% transmission reliability while reducing power requirements by 43% compared to cellular alternatives [19]. For remote monitoring applications, Dalenogare et al. (2022) implemented Sigfox-based networks achieving 40 km ranges with minimal power consumption (50 mA during transmission, 2 μA in sleep mode), enabling 5-year battery lifespans in infrastructure-limited regions [23].

Data transmission efficiency was significantly enhanced by Durmus and Karaca (2022), who implemented specialized compression algorithms to achieve 76% payload reduction, enabling transmission of 24-h environmental data within Sigfox's 12-byte limitations [22].

2.4. Edge Computing and Blockchain Integration

Edge computing deployments enable substantial efficiency improvements. Tippayawong et al. (2021) utilized ARM Cortex-M4 microcontrollers to implement Fast Fourier Transform algorithms that can detect anomalous vibration patterns during transportation, reducing data requirements by 87% while maintaining real-time alerting

capabilities [18]. Signal processing was further refined by MOKOSMART (2024), which implements Kalman filtering on ESP32 microcontrollers, achieving 94% noise reduction with sub-200ms response times [24,25].

Blockchain integration with these sensor networks presents promising traceability solutions. Trollman et al. (2022) developed Ethereum-based ERC-721 contracts that integrated sensor data as transaction validators. By requiring temperature readings within 19–21 °C ranges before allowing ownership transfers, they were able to achieve 3.4-s validation times with minimal gas consumption [26]. Kamble et al. (2020) addressed scalability challenges with a permissioned Hyperledger Fabric network utilizing Practical Byzantine Fault Tolerance consensus, achieving 3500 TPS while processing data from 5000 concurrent sensors [27]. Data provenance was enhanced by Vernall (2023) through elliptic curve cryptography authentication, generating digital signatures with 15 ms verification times while adding only 64 bytes of overhead per measurement [28].

While these studies demonstrate significant technical advances, our work uniquely addresses several critical gaps identified in the literature. As shown in Table 1, where a ✓means presence of topic and × means its absence, existing implementations typically focus on either IoT integration or blockchain utilization but rarely combine these technologies within a comprehensive dual-layer architecture. Furthermore, none of the reviewed works offer process verification capabilities or transaction cost analysis, which are essential for practical deployment in agricultural settings. Unlike existing works, which have focused on either blockchain or IoT in isolation, our framework introduces a dual-layer integration with smart contract-triggered decision enforcement based on simulated IoT sensor inputs such as RFID, GPS, and environmental data. Furthermore, we uniquely model process verification, batch-wise traceability, and mobile validation across multiple stakeholder roles, which are either absent or loosely defined in prior implementations. Our approach integrates blockchain-based ownership transfers with IoT-driven quality assurance in a unified framework, providing both technological innovation and ethical supply chain transparency that previous approaches have not fully achieved.

Table 1. Comparison of our work's contribution with other recent works in similar fields.

Feature	Our Work	Paper 1 [29]	Paper 2 [30]	Paper 3 [20]	Paper 4 [26]	Paper 5 [31]	Paper 6 [4]
Year	**2025**	**2018**	**2019**	**2021**	**2022**	**2022**	**2023**
Blockchain	✓	✓	✓	✓	✓	✓	✓
Dual-Layer Architecture	✓	×	×	×	×	×	×
IoT Integration	✓	✓	✓	✓	✓	×	×
Environmental Sensors	✓	×	✓	×	✓	×	×
Origin Authentication	✓	×	✓	×	×	×	×
Process Verification	✓	×	×	×	×	×	×
Advanced Smart Contracts	✓	✓	✓	✓	✓	✓	✓
Mobile Quality Assessment	✓	✓	×	×	×	×	×
Transaction Cost Analysis	✓	×	×	×	×	×	×

3. Methodology

The following subsections provide a detailed discussion of our system model and methodologies.

3.1. System Architecture and Dataset Design for IoT-Supported Blockchain Integration

In our proposed framework, illustrated in Figure 2, Internet of Things (IoT) technologies are integrated into the coffee supply chain architecture to enable real-world data acquisition and blockchain-based smart contract execution. To maintain our experimental focus on blockchain system performance and functionality, the IoT device data streams were simulated through the creation of structured datasets. We manually generated syn-

thetic datasets [32] to emulate realistic sensor outputs corresponding to RFID tagging [33], GPS tracking, weight measurements, environmental monitoring, and mobile-based validations, thereby effectively simulating an IoT environment without requiring physical device deployment. Each data entry was formatted to match the expected input conditions of the blockchain smart contracts and injected through Remix IDE [34] integrated with Metamask [35,36] during system testing. This approach ensured that the blockchain transactions were validated under realistic operational scenarios while laying a detailed foundation for future experimental implementations. In subsequent work, IoT simulation platforms such as Node-RED [37] can be coupled with custom data generation scripts and used to further automate and enrich the sensor-to-blockchain data pipeline.

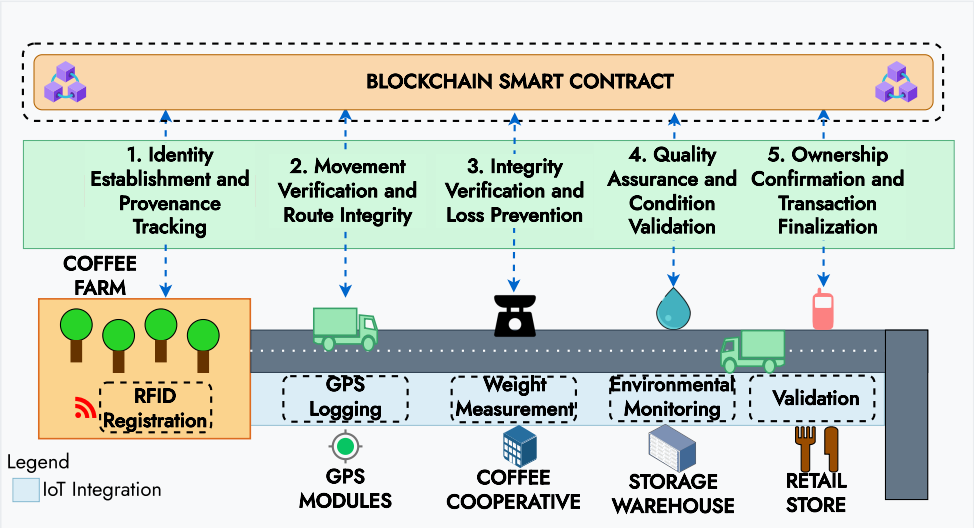

Figure 2. The above architecture illustrates the use of blockchain as a decentralized ledger and smart contracts for automating data validation and storage. Sensor inputs (RFID, GPS, weight, environment, mobile) are captured at key points and submitted via smart contracts, enabling real-time and verifiable traceability throughout the coffee supply chain.

3.1.1. RFID Registration

At the farm level, RFID technology can be used to assign a unique identity to each coffee bean batch immediately after harvest. Impinj Speedway RFID Readers [38] and UHF RFID tags [39] can be used to log critical information such as the farm ID, harvest date, and batch number. This batch ID establishes the foundation of traceability, serving as a consistent reference point for all future blockchain transactions for identity establishment and provenance tracking. Smart contracts can utilize this identity to securely link every ownership transfer, quality verification, and sale event back to the original farm source.

3.1.2. GPS Logging

After the coffee is harvested and tagged, GPS tracking modules can be used to monitor the movement of coffee shipments for movement verification and route integrity. Devices such as the Ublox Neo-6M GPS Module [40] or Queclink GV300 [41] industrial trackers can be used to provide continuous location updates. GPS data are associated with the batch's RFID ID and stored on the blockchain, enabling smart contracts to verify that the shipment followed approved routes. Any unauthorized abnormality can trigger blockchain-based alerts or conditional transaction halts, maintaining the security and authenticity of the transportation phase.

3.1.3. Weight Measurement

At checkpoints such as cooperative centers or export hubs, IoT-enabled weighing systems can be used to verify the weight of coffee bags for integrity verification and loss prevention. Arlyn Scales Ultra Precision IoT-connected weighing systems can be deployed to capture real-time weight measurements [42]. These values can be automatically compared to the original harvest weight recorded during RFID registration. If weight loss exceeds acceptable tolerance thresholds, smart contracts can prevent further transactions or require manual interventions, ensuring that product integrity is upheld throughout the supply chain.

3.1.4. Environmental Monitoring

During storage and transportation, it is essential to maintain optimal environmental conditions to preserve bean quality. DHT22 temperature [43] and humidity sensors linked to Raspberry Pi 4 IoT gateways [44] with LoRaWAN modules [45] can be used to collect environmental data. Smart contracts can monitor this data stream and automatically downgrade or flag batches that experience harmful conditions such as excessive humidity or temperature swings, thereby protecting the end product quality and consumer trust.

3.1.5. Mobile Validation

At final checkpoints such as roasters and retail outlets, mobile validation can be used to confirm the physical handover of coffee batches for ownership confirmation and transaction finalization [46]. Android or iOS NFC-enabled smartphones [47] running blockchain-connected scanning applications can be used to scan RFID tags, validate delivery, and trigger smart contract events. These scans complete the traceability cycle by updating batch statuses in the blockchain ledger, finalizing ownership transfers, and providing verified proof of product authenticity to consumers and businesses alike.

3.2. Smart Contract

The smart contract in the proposed system was developed in Solidity [48] and deployed on the Sepolia Ethereum testnet [49]. It models key interactions across the coffee supply chain, including user registration, bean batch registration, and sales transactions. To maintain experimental alignment with the blockchain's verification and record-keeping capabilities, data streams from hypothetical IoT sensors were manually encoded into structured datasets and used to simulate real-world inputs. These datasets were injected through the Remix IDE and processed via MetaMask, mimicking real-time device interactions without the need for physical hardware integration.

3.2.1. Inputs to Smart Contract

The smart contract accepts input parameters that reflect structured supply chain events. These include alphanumeric data for user and company identification, numerical values for user IDs, bean batch numbers, and batch weights, and blockchain addresses that designate transaction participants. All data values were manually generated to simulate expected outputs from RFID readers, weighing systems, and mobile interfaces.

Although IoT hardware was not physically deployed [50], the structure of each dataset entry corresponds to real-world data collection points. For example, the batch numbers and weights replicate values that would be captured by RFID systems and IoT-connected weighing scales at harvest and aggregation checkpoints. Inputs such as Ethereum addresses simulate identity confirmation typically validated by NFC-enabled mobile scans during retail handoff.

The simulated inputs were formatted to match the parameter types expected by the

smart contract functions. Each entry was manually submitted via Remix IDE and digitally signed in MetaMask, allowing for testing of transaction flow, ledger updates, and function correctness under realistic constraints.

3.2.2. Key Functions of Smart Contract

The smart contract includes a series of core functions that reflect distinct roles and actions within the coffee supply chain. The ***registerUsers()*** function allows stakeholders such as farmers, cooperatives, and retailers to register themselves on the blockchain. This function stores each user's name, a numerical ID, and company affiliation, which are linked to their Ethereum address. This provides a tamper-proof registry of verified participants.

The ***registerBeans()*** function is responsible for registering a coffee batch, and is restricted to the contract owner. It accepts a unique batch number and the associated bean weight. This simulates origin-level events in which harvested coffee is tagged and weighed before entering the supply chain.

The ***sale()*** function facilitates transactions between two registered users. It records the sale of a coffee batch, including the seller and buyer addresses, batch number, weight of the transferred beans, and timestamp. The function updates the ledger to reflect the remaining available weight for that batch, thereby ensuring traceability and preventing over-allocation. This function was used throughout the simulation to emulate ownership transfers, aggregation, and retail delivery.

The contract also includes two view functions, ***getUserDetails()*** and ***getBeanDetails()***, which allow for data retrieval without altering the ledger. These functions make the system transparent and queryable, supporting traceability across the entire supply chain.

3.3. Ledger Structure

The smart contract stores all data on-chain using Solidity mappings and structured arrays [51]. These serve as the blockchain-based ledger, ensuring data persistence and immutability. User information is stored in a mapping that associates each Ethereum address with a ***UserDetails*** structure. As shown in Figure 3, this structure records the user's name, ID, and company name, forming the basis for participant identification and role verification.

Coffee batch information is stored in a mapping from batch numbers to ***BeanDetails***. This structure captures the batch's initial weight, its unique batch number, and the timestamp of the most recent transaction. These fields enable the system to monitor the flow of coffee from registration to final sale, preserving batch-level traceability.

Sales transactions are stored in an array of ***SaleDetails*** structures. Each entry in this array represents a confirmed transaction, including the seller's and buyer's addresses, the batch number involved, the quantity of beans transferred, and the time of sale. This array forms the transaction history, recording each step of the batch's movement through the supply chain.

While the ledger structure is sufficient for functional testing and validation of traceability logic, it currently does not include data fields for environmental conditions or product origin. These can be incorporated in future versions of the contract by extending the data structures used in the mappings.

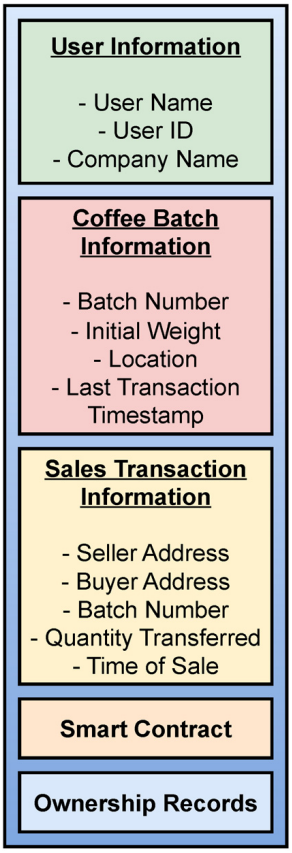

Figure 3. Blockchain ledger structure illustrating the on-chain storage of user identities, coffee batch metadata, and sales transactions. These components are managed through smart contract mappings and arrays to ensure traceability, ownership transparency, and immutable record-keeping.

3.4. Roles and Interaction

As illustrated in Figures 4 and 5, our proposed system models the coffee supply chain through a role-based smart contract structure in which every participant is responsible for specific stages of the product life cycle. These roles include coffee farmers, cooperatives, transporters, warehouses, retailers, and end consumers. Our system also incorporates IoT devices, mobile interfaces, and blockchain-backed ledger functionality to ensure data integrity and traceability across all interactions. Each participant is uniquely identified through their Ethereum address and registered using the ***registerUsers()*** function within the smart contract. Their interactions are structured to reflect real-world workflows and are validated on-chain to ensure accuracy, ownership consistency, and accountability.

The process begins at the coffee farm, where beans are harvested and physically tagged with RFID identifiers. While no hardware was used in the simulation, this phase was modeled in the dataset by assigning each batch a unique ID. The farmer, acting as the batch owner, registers both the user and the beans via the ***registerUsers()*** and ***registerBeans()*** functions. These records establish the origin of the beans and create a persistent reference for traceability.

After being tagged, the beans are transported to the next stage of the supply chain. Simulated IoT devices are modeled to send weight data, such as when a cooperative or weighing center receives a batch. The ***sale()*** function is used to record this handoff, log the new batch weight, and update ownership. In future deployments, IoT-enabled scales could trigger this update automatically through middleware such as mobile applications or APIs [52].

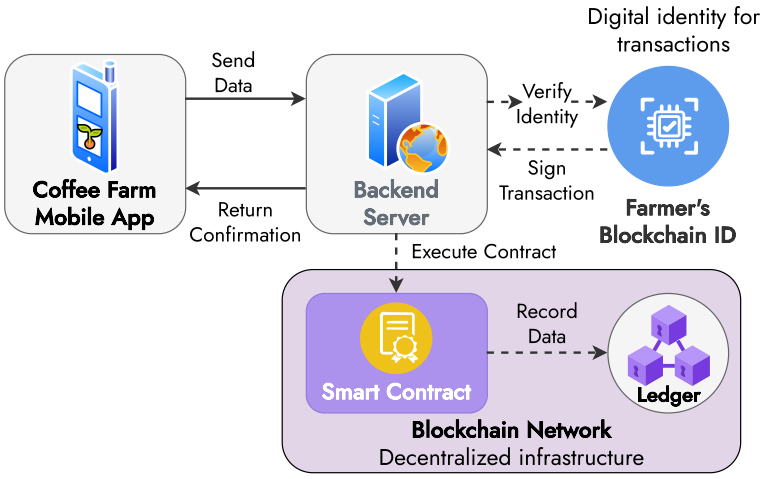

Figure 4. This diagram shows how farmers interact with the blockchain via a mobile app linked to a backend server. The server verifies identity, signs transactions with the farmer's blockchain ID, and triggers a smart contract to record data on the decentralized ledger. A confirmation is then returned to the app, ensuring secure, authenticated, and verifiable transactions.

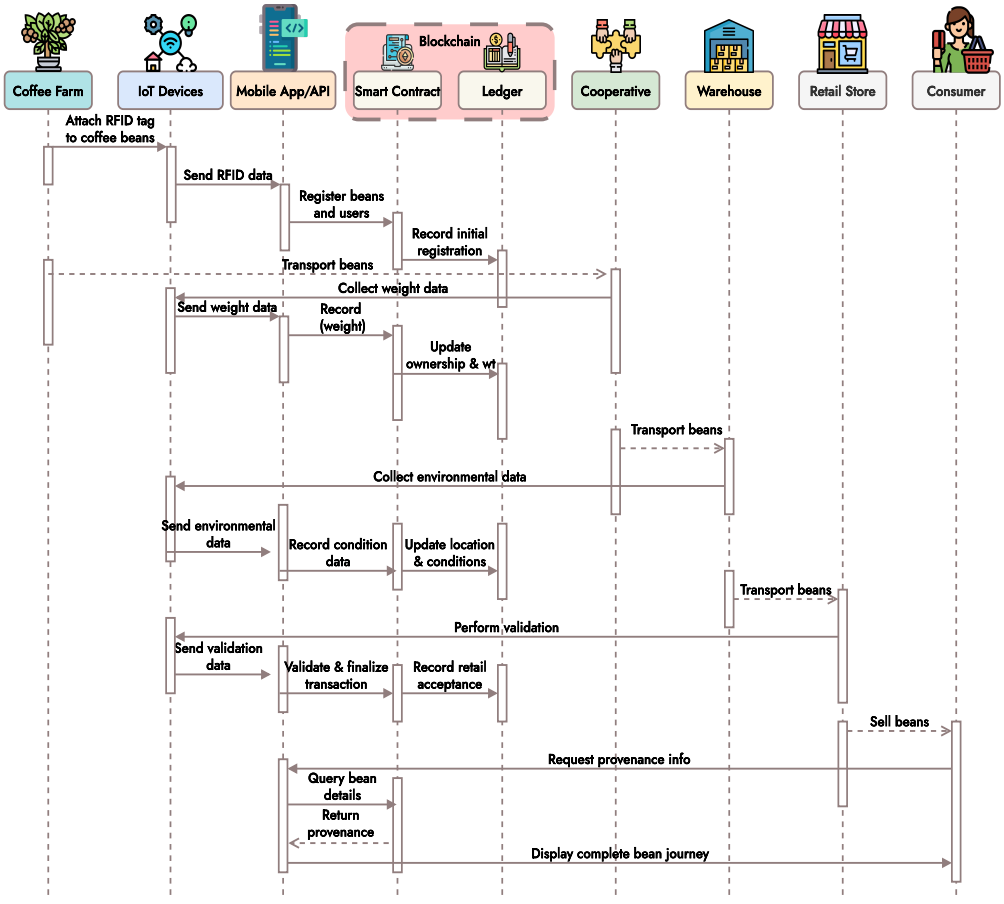

Figure 5. RFID data initiate bean registration through a mobile app at the farm level. As the batch progresses, simulated IoT devices capture weight and environmental data submitted on-chain through smart contracts. Ownership, location, and retail validations are logged, enabling consumers to query batch provenance, with all steps aligned to supply chain roles and automated through blockchain.

Environmental data collection is also part of the system's design, as shown in the diagram above. During transportation and storage, simulated temperature and humidity

readings are recorded in the dataset and associated with the batch. Although the smart contract does not currently include environmental parameters, these values could be submitted through extensions to the ***sale()*** function or through additional condition-checking modules in future iterations. This step is critical for quality assurance, as it enables traceability not just of ownership but also of product handling conditions.

Mobile validation is included near the retail endpoint. Retailers use simulated mobile devices to finalize the transaction, acting as the final receivers before product delivery. This is again represented by a ***sale()*** transaction, capturing the transfer from the transporter or warehouse to the retail outlet. The final update to the ledger marks the retail acceptance of the product and completes the traceability cycle.

Finally, consumers do not contribute data to the blockchain, but benefit from its transparency. They can query product information by batch number using the ***getBeanDetails()*** function, which returns a verified summary of the product's origin, ownership history, and supply chain journey. This supports consumer-facing applications such as QR code scans at the point of sale, allowing customers to access authenticated provenance data and reinforce trust in ethical sourcing and quality control.

As illustrated in Figure 4, the roles and interactions represented in the smart contract align with the sequence diagram in Figure 5, where each real-world action is either directly executed through a contract function or simulated through structured input. This design ensures traceability, enforces secure data flow, and provides the foundation for future integration with automated IoT systems.

4. Results and Discussion

This section presents the performance evaluation of the proposed blockchain-based coffee supply chain system using a simulated dataset of 1000 transactions. These transactions represent events such as user registration, ownership transfers, and coffee sales modeled across four key stakeholder roles: farmer, roaster, exporter, and retailer. The testing was performed on the Sepolia testnet, which closely mimics the behavior of the real Ethereum blockchain (mainnet) [53], using Remix IDE with Metamask integration. Key metrics discussed in further detail below are transaction fees, execution time, and transaction reliability. We visualize the results using histogram-style distribution figures, with transaction data grouped into bins to identify broader trends in fee cost and time performance.

4.1. Transaction Fee Distribution

A total of 1000 transactions were executed to analyze the gas fee distribution in our blockchain-enabled coffee supply chain system. Figure 6 presents the relative frequency distribution of transaction fees along with a Cumulative Distribution Function (CDF) curve [54]. The X-axis segments transaction fees into 13 bins of approximately 0.00025 ETH each, while the left Y-axis displays the percentage of transactions within each bin. The right Y-axis reflects the accumulated percentage of transactions across the bins, enabling a clear view of how transaction fees build up cumulatively.

As can be seen, the distribution is heavily right-skewed, indicating that most transactions incur very low fees. Specifically, 63.0% of transactions fall within the ETH 0–0.00025 range, and an additional 18.0% are within ETH 0.00025–0.0005, meaning that over 81% of all interactions cost less than ETH 0.0005. The third bin (ETH 0.0005–0.00075) accounts for 7.5%, while only 1.5% of transactions exceed ETH 0.0015. The final bin, covering all transactions above ETH 0.003, contains just 0.1%. This extremely small fraction corresponds to the initial smart contract deployment, which is typically the most gas-intensive operation. After deployment, the remaining contract interactions such

as ownership transfers, status updates, and coffee sale logging incur significantly lower gas costs.

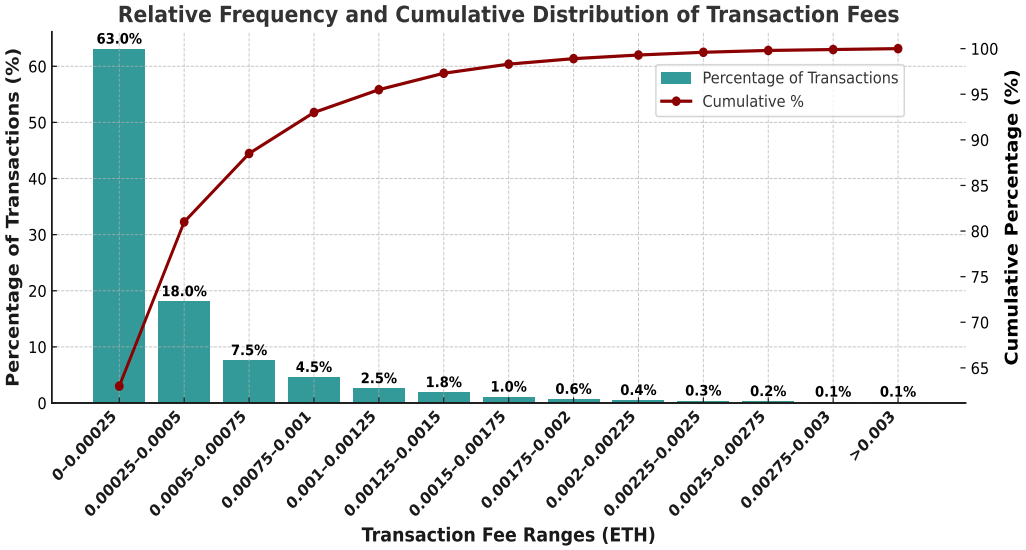

Figure 6. This figure shows the relative frequency and cumulative distribution of transaction fees from 1000 blockchain interactions. Most transactions (over 95%) incur fees below ETH 0.001, as shown by the bars and CDF curve, indicating cost efficiency. Higher fees are limited to rare events such as contract deployment.

The CDF curve confirms that over 95% of all transactions incur gas fees below ETH 0.001, illustrating that the system is computationally efficient for the vast majority of use cases. The shape of the curve rises sharply in the first few bins and flattens thereafter, reinforcing the interpretation that only a negligible portion of interactions fall into high-cost categories.

These findings validate the cost-effectiveness and operational scalability of the proposed framework. The system is not only capable of supporting frequent low-cost blockchain interactions, which is an essential characteristic for real-time supply chain logging, but also minimizes the financial burden of adopting blockchain technology in practical deployments. By isolating the high one-time cost of contract deployment and ensuring that all recurring operations remain lightweight, the architecture promotes both sustainability and extensibility for broader adoption.

4.2. Transaction Time Distribution

We analyzed transaction completion times to assess the responsiveness of the system under real-world blockchain conditions. A total of 1000 transactions were executed on the Sepolia testnet, with the resulting distribution visualized in Figure 7. The X-axis represents 10-s transaction time intervals, while the Y-axis reflects the relative frequency (percentage) of transactions that fall into each range.

As shown in Figure 7, this distribution illustrates a prominent peak in the 90–100 s range, which accounts for 29.0% of all recorded transactions, making it the most dominant interval by a significant margin. Several other bins, such as 0–10, 20–30, 40–50, and 80–90 s, each hold 9.7% of the transactions, suggesting moderate activity, with none approaching the peak observed for the 90–100 s bin. Only a small fraction of transactions occur in the extremities, with a minimum confirmation time of 12 s and a maximum of 108 s.

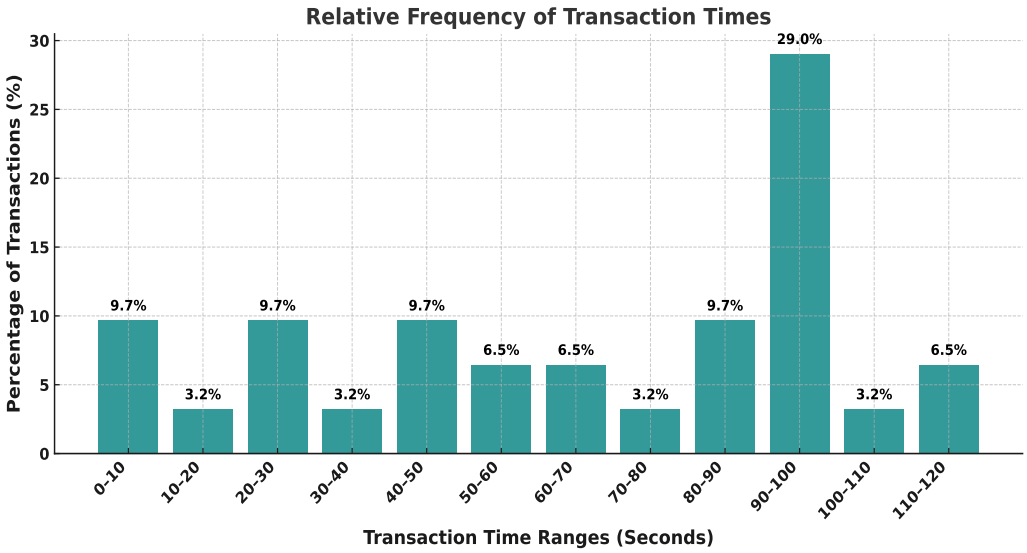

Figure 7. This figure presents the distribution of transaction completion times for 1000 interactions on the Sepolia testnet. Most confirmations occurred between 90–100 s (29%), with variability across other intervals. The results highlight potential latency challenges for time-sensitive IoT-integrated supply chains.

These results indicate that while the system is capable of handling confirmations under 60 s in many cases, network conditions and transaction queueing likely contribute to longer confirmation delays. The variability in transaction completion times points to external factors such as blockchain network congestion or wallet latency rather than to inconsistencies in the contract itself [11]. Although this variability may not critically impact batch-based supply chain operations, it could still present a limitation for IoT-integrated use cases requiring real-time responsiveness, which we plan to resolve in our future work.

4.3. Administrative Gas Overhead in the Smart Contract

Smart contracts often include administrative functions to support secure role transitions, especially when there are multiple parties involved in a process such as a supply chain. In the context of our smart contract for coffee supply chains, the two functions ***transferOwnership()*** and ***renounceOwnership()*** were observed during testing, allowing for further insights into the gas efficiency of control-layer operations such as supply chains.

The ***renounceOwnership()*** function, which removes the current owner by assigning the zero address, recorded the lowest average gas fee at approximately ETH 0.000058. This is consistent with its simple design involving a single state update and emission of an ownership change event.

On the other hand, the ***transferOwnership()*** function, which is used to delegate control to another address, has a slightly higher average gas fee of ETH 0.000227. This marginal increase also reflects the additional logic required to validate the new owner's address and update the relevant storage variable.

While not part of the primary supply chain flow, these administrative functions are still essential for managing access control and contract governance. Their relatively low gas consumption demonstrates that critical updates to contract roles can be performed efficiently without notably introducing computational overhead or affecting the scalability of the system.

4.4. Discussion and Observations

The average transaction fee across 1000 operations is ETH 0.00034, with a standard deviation of ETH 0.00040. Similarly, the mean transaction time is 65.74 s, with a standard deviation of 34.24 s. These values reflect a system in which the majority of interactions occur at very low gas costs, demonstrating cost-efficiency in smart contract execution. The low mean fee and right-skewed distribution suggest that only a small number of operations (e.g., initial deployment) incur higher costs, while routine transactions remain lightweight. On the other hand, the transaction time shows greater variability, with a standard deviation exceeding 50% of the mean. This indicates that while many transactions are processed quickly, others experience delays, likely caused by external testnet factors such as congestion or wallet response latency. Overall, these behavioral patterns align with expected outcomes in a simulated Ethereum environment and reinforce the practicality of using blockchain for decentralized supply chain interactions.

The above performance evaluations confirm that the smart contract system performs reliably and cost-effectively in the Sepolia testnet, which closely mimics the behavior of the actual Ethereum mainnet. Most transactions incur low and consistent gas fees, indicating that routine operations can be executed without significance resource demands. Even administrative functions such as ***transferOwnership()*** demonstrate minimal overhead, supporting the efficiency of control-level processes within the smart contract.

While transaction times vary, the majority fall within acceptable bounds for supply chain scenarios that are event-driven but do not critically require real-time execution. The observed inconsistency points to limitations in the testing infrastructure rather than to flaws in the smart contract logic, suggesting that performance can be improved under optimized deployment conditions.

These outcomes align with the concerns raised in the literature review in Section 2.1. Existing studies emphasize the importance of ensuring transparency and data immutability in agricultural supply chains. The current system supports this by providing time-stamped and tamper-resistant records. Section 2.2 discusses the technical challenges of integrating IoT and blockchain systems; the dual-layer architecture used in this work demonstrates a structured way of modeling sensor input in a blockchain-friendly format. Section 2.3 highlights the lack of traceability and trust in conventional supply chains. By making all transactional data visible and verifiable on-chain, the proposed system improves traceability and builds stakeholder confidence. Finally, Section 2.4 notes the absence of practical full-stack models. Our work fills that gap by offering a complete design, from data simulation to blockchain integration. These connections reinforce the value of the proposed framework and its relevance to the existing body of research.

4.5. Security and Threat Considerations

While blockchain inherently provides immutable and transparent data recording, securing the overall supply chain system required identifying and mitigating potential threats across the broader architecture. To this end, we adopt the STRIDE threat modeling framework, which is commonly used in cybersecurity design, to classify security concerns and evaluate the robustness of our proposed architecture.

STRIDE stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege [55]. As presented in Table 2, these categories collectively capture the main classes of security threats typically encountered in software and hardware-integrated systems such as blockchain and IoT-enabled supply chains.

In our system, STRIDE helps to outline how both the IoT (sensor and data layer) and blockchain (smart contract layer) components might be vulnerable to various attacks as well as what mitigation strategies are in place or planned. Table 2 summarizes the potential

threats and how our framework addresses them, either through current mechanisms or proposed enhancements in future deployments.

In this threat model, data tampering itself is treated as a core attack vector that our blockchain implementation inherently resists through immutability. However, threats outside the chain remain a concern, including spoofed sensor inputs and physical tampering with IoT devices. Although our current prototype is simulation-based, this threat analysis offers a roadmap for securing future physical deployments.

STRIDE evaluation highlights the foundational security properties of the system and points to enhancements for future field readiness. As we move toward hardware integration and pilot studies, this model will inform both architectural adjustments and threat mitigation priorities.

Table 2. STRIDE threat modeling for the proposed blockchain–IoT framework.

STRIDE Category	Potential Threat in the System	Mitigation Strategy (Current and Planned)
Spoofing Identity	Malicious actors may impersonate legitimate users or sensors to submit falsified data.	Smart contracts enforce strict user registration via ***registerUsers*** and access control using ***onlyOwner***. Sensor authentication protocols are part of future enhancements.
Tampering with Data	Attackers could alter sensor data during transmission or before it is stored on-chain.	Blockchain immutability ensures post-submission integrity. Future work includes encrypted sensor transmission and data signing.
Repudiation	Users might deny initiating or participating in transactions.	Ethereum stores all transactions on-chain with cryptographic signatures and timestamps, enabling full audit trails.
Information Disclosure	Leakage of sensitive data like GPS location or user identity.	Minimal Personally Identifiable Information is recorded. Future work includes off-chain encrypted storage and proxy re-encryption mechanisms.
Denial of Service (DoS)	Excessive requests may overload sensors or smart contracts.	Ethereum's gas mechanism limits resource abuse. Rate limiting and transaction prioritization are proposed for future deployment.
Elevation of Privilege	Unauthorized users might access restricted contract functions.	Solidity-based role enforcement using ***onlyOwner*** ensures role-based restrictions.

5. Challenges and Future Work

While the proposed framework and results demonstrate the potential and novelty of this research, a number of challenges were encountered that define its current limitations and can provide a guide for future development. One primary challenge was the use of simulated IoT sensor data rather than physical device integration. Although structured datasets were used to emulate realistic sensor outputs, these do not completely reflect real-world device behavior, potential sensor failures, or recurrent connectivity issues. We acknowledge that the absence of live sensor deployment limits the current system's reproducibility and hardware-specific insights. As part of future work, our framework will be extended to incorporate IoT hardware using platforms such as Raspberry Pi and Node-RED to allow for live data collection and on-chain validation [56].

Another challenge was the variability in transaction execution time, which ranged from 12 to 108 s during testing on the Sepolia testnet via Remix IDE and Metamask. These delays were influenced by external infrastructure factors which were beyond the smart contract's control. Our future work will include deploying the smart contract in a more stable or performance-optimized blockchain environment such as a private Ethereum network in order to achieve more consistent responsiveness, especially in preparation for IoT-triggered events in the supply chain process. Our future work will also include a

comprehensive security assessment, including threat modeling of common supply chain attacks such as data spoofing, unauthorized access, and sensor tampering, in order to evaluate the robustness of the proposed blockchain–IoT integration.

While this study emphasizes functional and architectural validation, we recognize the need for formal modeling of system parameters such as latency, reliability, and throughput. Future work will include mathematical modeling and simulation-driven optimization after real-world IoT data are integrated into the framework, in addition to comparison with other platforms such as Hyperledger [57].

Future work will also explore interoperability with existing supply chain certification platforms such as Rainforest Alliance and Fairtrade [58] by aligning our transaction schema with standardized data formats such as GS1 EPCIS 2.0 [59]. This will enhance compatibility with external auditing systems and support broader Environmental, Social, and Governance (ESG) compliance.

Lastly, our testing involved a limited number of users and transaction flows, which does not fully capture the scalability and concurrency challenges of a real-world coffee supply chain. As our next step, we plan to scale up by supporting multiple concurrent product batches, simulate interactions across larger stakeholder networks, and evaluate smart contract performance under higher load conditions [60].

In addition to addressing these above challenges, future extensions will also include implementing decentralized storage such as InterPlanetary File System (IPFS) [61] for off-chain sensor metadata, introducing role-based permission control through access modifiers, and exploring the use of blockchain oracle [6] to securely bridge off-chain and on-chain data sources. These enhancements aim to make the system more robust, adaptable, and deployable in diverse agricultural supply chain contexts.

6. Conclusions

This paper has presented a blockchain and IoT-enabled framework for enhancing traceability, accountability, and transparency across the coffee supply chain. By integrating simulated IoT data with Ethereum-based smart contracts, the proposed system captures and automates key supply chain events such as batch registration, weight verification, environmental monitoring, and ownership transfer. A structured dataset was designed to reflect realistic sensor outputs, allowing the system to be tested under conditions that closely resemble actual field deployments. Our system architecture accommodates RFID registration, GPS tracking, and mobile validation workflows, thereby laying the groundwork for seamless integration with real-world hardware platforms.

The proposed smart contract was deployed and evaluated on the Sepolia Ethereum testnet and transaction data were analyzed across multiple performance dimensions, including gas cost, execution time, and administrative overhead. The results demonstrate that the proposed system operates within low transaction cost bounds while maintaining functional correctness and reliability, which is our main priority for this work. Similarly, our interaction model enforces role-specific permissions and immutably records all transactions in the decentralized ledger, ensuring verifiability across all stakeholder actions in the coffee supply chain.

While the current implementation relies on simulated inputs, our framework is modular and extensible, offering a feasible path toward physical deployment using platforms such as Node-RED and Raspberry Pi. The novelty of this work lies in its detailed mapping of real-world coffee logistics into smart contract logic as well as in its simulation-based validation strategy, which provides a replicable approach for similar supply chain scenarios. Our future extensions will focus on real sensor integration, blockchain oracle support for off-chain data, and broader scalability testing under multi-batch parallel conditions.

Author Contributions: The authors declare that they have equally contributed to the paper. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to privacy and commercial restrictions.

Acknowledgments: We want to thank the authors of the literature cited in this paper for contributing useful ideas to this study.

Conflicts of Interest: The authors declare no conflicts of interest; the funders had no role in the design of the study, in the collection, analysis, or interpretation of data, in the writing of the manuscript, or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

API	Application Programming Interface
CDF	Cumulative Distribution Function
ETH	Ethereum
ESG	Environmental, Social, and Governance
GPS	Global Positioning System
ID	Identification
IoT	Internet of Things
IPFS	InterPlanetary File System
NFC	Near-Field Communication
QR Code	Quick-Response Code
RFID	Radio-Frequency Identification

References

1. Daviron, B.; Ponte, S. *The Coffee Paradox: Global Markets, Commodity Trade and the Elusive Promise of Development*; Zed Books: London, UK, 2005.
2. Macdonald, K. Globalising justice within coffee supply chains? Fair Trade, Starbucks and the transformation of supply chain governance. *Third World Q.* **2007**, *28*, 793–812. [CrossRef]
3. Azis, A.M.; Irjayanti, M.; Rusyandi, D. Visibility and information accuracy of coffee supply chain in West Java Indonesia. In *Modeling Economic Growth in Contemporary Indonesia*; Emerald Publishing Limited: Leeds, UK, 2022; pp. 225–236.
4. Alamsyah, A.; Widiyanesti, S.; Wulansari, P.; Nurhazizah, E.; Dewi, A.S.; Rahadian, D.; Ramadhani, D.P.; Hakim, M.N.; Tyasamesi, P. Blockchain traceability model in the coffee industry. *J. Open Innov. Technol. Mark. Complex.* **2023**, *9*, 100008. [CrossRef]
5. Lukas, K.D. The Supply Chain of Fair Trade Coffee: Challenges, Opportunities & the Future Inside a Troubled Industry. Master's Thesis, University of Vermont, Burlington, VT, USA, 2015.
6. Upadhyay, K.; Dantu, R.; He, Y.; Badruddoja, S.; Salau, A. Auditing metaverse requires multimodal deep learning. In Proceedings of the 2022 IEEE 4th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA), Atlanta, GA, USA, 14–17 December 2022; pp. 39–46.
7. Tharatipyakul, A.; Pongnumkul, S.; Riansumrit, N.; Kingchan, S.; Pongnumkul, S. Blockchain-based traceability system from the users' perspective: A case study of Thai coffee supply chain. *IEEE Access* **2022**, *10*, 98783–98802. [CrossRef]
8. Garcia, A.; Dávila, J.; Wong, L. Framework to improve the traceability of the coffee production chain in peru by applying a blockchain architecture. In Proceedings of the 2022 32nd Conference of Open Innovations Association (FRUCT), Tampere, Finland, 9–11 November 2022; pp. 93–101.
9. Sabio, R.P.; Spers, E.E. Does coffee origin matter? An analysis of consumer behavior based on regional and national origin. In *Coffee Consumption and Industry Strategies in Brazil*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 297–320.
10. da Costa, T.P.; Gillespie, J.; Cama-Moncunill, X.; Ward, S.; Condell, J.; Ramanathan, R.; Murphy, F. A systematic review of real-time monitoring technologies and its potential application to reduce food loss and waste: Key elements of food supply chains and IoT technologies. *Sustainability* **2022**, *15*, 614. [CrossRef]

11. Upadhyay, K.; Dantu, R.; Zaccagni, Z.; Badruddoja, S. Is your legal contract ambiguous? Convert to a smart legal contract. In Proceedings of the 2020 IEEE International Conference on Blockchain (Blockchain), Rhodes, Greece, 2–6 November 2020; pp. 273–280.
12. Badruddoja, S.; Dantu, R.; Widick, L.; Zaccagni, Z.; Upadhyay, K. Integrating DOTS with blockchain can secure massive IoT sensors. In Proceedings of the 2020 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW), New Orleans, LA, USA, 18–22 May 2020; pp. 937–946.
13. Upadhyay, K.; Dantu, R.; He, Y.; Salau, A.; Badruddoja, S. Make consumers happy by defuzzifying the service level agreements. In Proceedings of the 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), Atlanta, GA, USA, 13–15 December 2021; pp. 98–105.
14. Upadhyay, K.; Dantu, R.; He, Y.; Salau, A.; Badruddoja, S. Paradigm shift from paper contracts to smart contracts. In Proceedings of the 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), Atlanta, GA, USA, 13–15 December 2021; pp. 261–268.
15. Upadhyay, K.; Dantu, R.; He, Y.; Badruddoja, S.; Salau, A. Can't Understand SLAs? Use the Smart Contract. In Proceedings of the 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), Atlanta, GA, USA, 13–15 December 2021; pp. 129–136.
16. Swindall, M.I.; Upadhyay, K.; Brusuelas, J.H.; West, G.; Wallin, J.F. Smart Digital Edition Management: A Blockchain Framework for Papyrology. In Proceedings of the 2024 Computers and People Research Conference, Murfreesboro, TN, USA, 29 May–1 June 2024; pp. 1–10.
17. Rutayisire, J.; Markon, S.; Raymond, N. IoT based Coffee quality monitoring and processing system in Rwanda. In Proceedings of the 2017 International Conference on Applied System Innovation (ICASI), Sapporo, Japan, 13–17 May 2017.
18. Kittichotsatsawat, Y.; Jangkrajarng, V.; Tippayawong, K.Y. Enhancing Coffee Supply Chain towards Sustainable Growth with Big Data and Modern Agricultural Technologies. *Sustainability* **2021**, *13*, 4593. [CrossRef]
19. Morales, A.; Castillo, J. Application of the Internet of Things through a Network of Wireless Sensors in a Coffee Crop for Monitoring and Control its Environmental Variables. *Rev. Fac. Ing.* **2019**, *46*, 101–116.
20. Varriale, V.; Cammarano, A.; Michelino, F.; Caputo, M. Sustainable Supply Chains with Blockchain, IoT and RFID: A Simulation on Order Management. *Sustainability* **2021**, *13*, 6372. [CrossRef]
21. Khan, R.; Turowski, K. A Survey of Current Challenges in IoT Security and Possible Countermeasures. 2016. Available online: https://www.semanticscholar.org/paper/A-Survey-of-Current-Challenges-in-Manufacturing-IoT-Khan-Turowski/f2a2e39cdfa0c3e3b89415d8a33fbb9baa1a8b5a (accessed on 1 May 2025).
22. Durmus, K.; Karaca, Y. Internet of Things enabled real time cold chain monitoring in a container port. *J. Shipp. Trade* **2022**, *7*, 9. [CrossRef]
23. Dalenogare, L.; Benitez, G.; Ayala, N.; Frank, A. The expected contribution of Industry 4.0 technologies for industrial performance. *J. Manuf. Syst.* **2022**, *204*, 383–394. [CrossRef]
24. MOKOSMART. Top 7 Examples of IoT in the Coffee Supply Chain. 2024. Available online: https://www.mokosmart.com/iot-in-the-coffee-supply-chain/ (accessed on 1 May 2025).
25. Albraheem, L.; Alajlan, H.; Alkhair, L.A.; Gwead, S.B. An IoT-based smart plug energy monitoring system. *Int. J. Adv. Comput. Sci. Appl.* **2023**, *14*. [CrossRef]
26. Trollman, H.; Garcia-Garcia, G.; Jagtap, S.; Trollman, F. Blockchain for Ecologically Embedded Coffee Supply Chains. *Logistics* **2022**, *6*, 43. [CrossRef]
27. Kamble, S.; Gunasekaran, A.; Sharma, R. Blockchain Technology in Supply Chain Operations: Applications, Challenges and Research Opportunities. *Transp. Res. Part E Logist. Transp. Rev.* **2020**, *142*, 102067.
28. Vernall, D. Increasing Supply Chain Visibility Through the Use of IoT Sensors and Blockchain. 2023. Available online: https://www.linkedin.com/pulse/increasing-supply-chain-visibility-through-use-iot-sensors-vernall-hljrc/ (accessed on 1 May 2025).
29. Thiruchelvam, V.; Mughisha, A.; Shahpasand, M.; Bamiah, M. Blockchain-based Technology in the Coffee Supply Chain Trade: Case of Burundi Coffee. *J. Telecommun. Electron. Comput. Eng.* **2018**, *10*, 121–125.
30. Mondal, S.; Wijewardena, K.; Karuppuswami, S.; Kriti, N.; Kumar, D.; Chahal, P. Blockchain Inspired RFID-Based Information Architecture for Food Supply Chain. *IEEE Internet Things J.* **2019**, *6*, 5803–5813. [CrossRef]
31. Bager, S.; Düdder, B.; Henglein, F.; Hébert, J.; Wu, H. Event-Based Supply Chain Network Modeling: Blockchain for Good Coffee. *Front. Blockchain* **2022**, *5*, 846783. [CrossRef]
32. Goyal, M.; Mahmoud, Q.H. A systematic review of synthetic data generation techniques using generative AI. *Electronics* **2024**, *13*, 3509. [CrossRef]
33. Su, J.; Sheng, Z.; Huang, C.; Li, G.; Liu, A.X.; Fu, Z. Identifying RFID tags in collisions. *IEEE/ACM Trans. Netw.* **2022**, *31*, 1507–1520. [CrossRef]

34. Jain, S.M. Introduction to remix IDE. In *A Brief Introduction to Web3: Decentralized Web Fundamentals for App Development*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 89–126.
35. Lee, W.M.; Lee, W.M. Using the metamask chrome extension. *Beginning Ethereum Smart Contracts Programming: With Examples in Python, Solidity, and JavaScript*; Apress: Berkeley, CA, USA, 2019; pp. 93–126.
36. Nhan, T.; Upadhyay, K.; Poudel, K. Towards Patient-Centric Healthcare: Leveraging Blockchain for Electronic Health Records. In Proceedings of the 2024 Computers and People Research Conference,Murfreesboro, TN, USA, 29 May–1 June 2024; pp. 1–8.
37. Lekić, M.; Gardašević, G. IoT sensor integration to Node-RED platform. In Proceedings of the 2018 17th International Symposium Infoteh-Jahorina (Infoteh), East Sarajevo, Bosnia and Herzegovina, 21–23 March 2018; pp. 1–5.
38. Wang, Z.; Chen, Y.; Wan, W.; Xie, Y.; Ou, Y. Reading Method of Physical Characteristic Data of RFID Radio Frequency for Wireless Perception. In Proceedings of the 2021 2nd International Conference on Electronics, Communications and Information Technology (CECIT), Sanya, China, 27–29 December 2021; pp. 879–883.
39. Nikitin, P.V.; Rao, K.; Lazar, S. An overview of near field UHF RFID. In Proceedings of the 2007 IEEE International Conference on RFID, Grapevine, TX, USA, 26–28 March 2007; pp. 167–174.
40. Mehta, D.; Verma, P.; Rawat, A. Data Analysis of U-blox GPS on Static and Dynamic Drone Platform. In Proceedings of the 2023 IEEE Wireless Antenna and Microwave Symposium (WAMS), Ahmedabad, India, 7–10 June 2023; pp. 1–4.
41. Cardoso, E.S.; Lieira, D.D.; Teixeira, M.A.; Nakamura, L.H.V.; Meneguette, R.I. IS-DASPA: An IoT system for data analysis from soil preparation in agribusiness. In Proceedings of the 2023 18th Iberian Conference on Information Systems and Technologies (CISTI), Aveiro, Portugal, 20–23 June 2023; pp. 1–6.
42. Bue, G.; Makinen, J.; Cox, M.; Watts, C.; Campbell, C.; Vogel, M.; Colunga, A.; Conger, B. Long-duration testing of a spacesuit water membrane evaporator prototype. In Proceedings of the 42nd International Conference on Environmental Systems, San Diego, CA, USA, 15–19 July 2012; p. 3459.
43. Ahmad, Y.A.; Gunawan, T.S.; Mansor, H.; Hamida, B.A.; Hishamudin, A.F.; Arifin, F. On the evaluation of DHT22 temperature sensor for IoT application. In Proceedings of the 2021 8th International Conference on Computer and Communication Engineering (ICCCE), Kuala Lumpur, Malaysia, 22–23 June 2021; pp. 131–134.
44. Upton, E.; Halfacree, G. *Raspberry Pi User Guide*; John Wiley & Sons: Hoboken, NJ, USA, 2016.
45. Haxhibeqiri, J.; De Poorter, E.; Moerman, I.; Hoebeke, J. A survey of LoRaWAN for IoT: From technology to application. *Sensors* **2018**, *18*, 3995. [CrossRef]
46. Rehman, M.; Petrillo, A.; Baffo, I.; Iovine, G.; De Felice, F. Optimizing Coffee Supply Chain Transparency and Traceability through Mobile Application. *Procedia Comput. Sci.* **2025**, *253*, 2116–2126. [CrossRef]
47. Madlmayr, G.; Langer, J.; Kantner, C.; Scharinger, J. NFC devices: Security and privacy. In Proceedings of the 2008 Third International Conference on Availability, Reliability and Security, Barcelona, Spain, 4–7 March 2008; pp. 642–647.
48. Kumar, H.; Upadhyay, K. Decentralized Engagement: Blockchain's Lens on Social Media. In *Proceedings of the International Congress on Blockchain and Applications*; Springer: Berlin/Heidelberg, Germany, 2024; pp. 278–287.
49. Ali, S.; Robinson, B.; Solomon, S.; Poudel, S.; Sharma, A.; Upadhyay, K. Chain Your Loot: Implementing Blockchain into Gaming Loot Box Markets. In Proceedings of the 2025 IEEE 15th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 6–8 January 2025; pp. 861–867.
50. Singh, D.; Sandhu, A.; Thakur, A.; Priyank, N. An overview of IoT hardware development platforms. *Int. J. Emerg. Technol.* **2020**, *11*, 155–163.
51. Sande Ríos, J. Optimizing Compilation of Array Accesses in Solidity Smart Contracts. Bachelor's Thesis, The Complutense University of Madrid, Madrid, Spain, 2023.
52. Agarwal, P.; Alam, M. Investigating IoT middleware platforms for smart application development. In *Proceedings of the Smart Cities—Opportunities and Challenges: Select Proceedings of ICSC 2019*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 231–244.
53. Robinson, P. The merits of using ethereum mainnet as a coordination blockchain for ethereum private sidechains. *Knowl. Eng. Rev.* **2020**, *35*, e30. [CrossRef]
54. Pianosi, F.; Wagener, T. A simple and efficient method for global sensitivity analysis based on cumulative distribution functions. *Environ. Model. Softw.* **2015**, *67*, 1–11. [CrossRef]
55. Salau, A.; Dantu, R.; Morozov, K.; Upadhyay, K.; Badruddoja, S. Towards a Threat Model and Security Analysis for Data Cooperatives. In Proceedings of the SECRYPT, Lisbon, Portugal, 11–13 July 2022; pp. 707–713.
56. Balamurugan, C.; Satheesh, R. Development of raspberry pi and IoT based monitoring and controlling devices for agriculture. *J. Soc. Technol. Environ. Sci.* **2017**, *6*, 207–215.
57. Mohammed, A.H.; Abdulateef, A.A.; Abdulateef, I.A. Hyperledger, Ethereum and blockchain technology: A short overview. In Proceedings of the 2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 11–13 June 2021; pp. 1–6.
58. Bredberg, S. Fairtrade versus Rainforest Alliance. Bachelor's Thesis, Department of Economics, Lund University, Lund, Sweden, 2010.

59. Sohn, B.; Woo, S.; Han, J.; Cho, H.; Byun, J.; Kim, D. Gs1 connected car using epcis-ons system. In Proceedings of the 2016 IEEE International Congress on Big Data (BigData Congress), San Francisco, CA, USA, 27 June–2 July 2016; pp. 426–429.
60. Vangala, A.; Das, A.K.; Kumar, N.; Alazab, M. Smart secure sensing for IoT-based agriculture: Blockchain perspective. *IEEE Sens. J.* **2020**, *21*, 17591–17607. [CrossRef]
61. Salau, A.; Dantu, R.; Upadhyay, K. Data cooperatives for neighborhood watch. In Proceedings of the 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Sydney, Australia, 3–6 May 2021; pp. 1–9.