



Archives available at [journals.mriindia.com](http://journals.mriindia.com)

**International Journal on Advanced Computer Theory and Engineering**

ISSN: 2319 - 2526

Volume 14 Issue 01, 2025

**Blockchain-Enabled Framework for Enhancing Transparency and Data Integrity in Food Supply Chains**

Dr. Shailesh T. Khandare

Associate Professor

Department of Computer Science and Engineering

Babasaheb Naik College of Engineering, Pusad, Maharashtra, India

Email: [khandare.shailesh@rediffmail.com](mailto:khandare.shailesh@rediffmail.com)

Peer Review Information	Abstract
<p><i>Submission: 11 July 2025</i> <i>Revision: 10 Aug 2025</i> <i>Acceptance: 15 Sept 2025</i></p> <p><b>Keywords</b></p> <p><i>Blockchain; Food Supply Chain; Traceability; Smart Contracts; IoT Sensors; Data Integrity; Transparency; Distributed Ledger Technology (DLT); Cold Chain Monitoring; IPFS Storage.</i></p>	<p>Food supply chains face persistent challenges related to data tampering, limited traceability, fraudulent labeling, and fragmented documentation, all of which compromise food safety and reduce consumer trust. This paper proposes a blockchain-enabled framework designed to provide end-to-end transparency, strengthen data integrity, and support real-time monitoring across the food supply chain. The framework integrates permissioned blockchain technology with IoT-based environmental sensing, smart contract automation, and hybrid on-chain/off-chain storage to establish a secure and tamper-proof digital ecosystem. A multi-layered architecture is developed to capture sensor readings, validate transactions, enforce compliance rules, and maintain immutable provenance records accessible to all stakeholders. Experimental evaluation demonstrates that the proposed system achieves low transaction latency, efficient smart contract execution, high throughput, and perfect hash verification accuracy, validating its suitability for real-time food quality monitoring and traceability. The results indicate that blockchain can effectively eliminate data manipulation, accelerate recall processes, enhance certification verification, and increase consumer trust by providing transparent and verifiable product histories. The presented model offers a scalable and practical solution for modernizing food supply chain management and serves as a foundation for future integration with predictive analytics, sustainability scoring, and decentralized regulatory compliance systems.</p>

**Introduction**

The global food supply chain has emerged as one of the most complex, distributed, and data-intensive systems, involving numerous stakeholders ranging from farmers and processors to distributors, retailers, regulators, and consumers. Due to its multi-stage nature, the supply chain is vulnerable to inefficiencies, fraud, adulteration, counterfeiting, and data manipulation, which compromise both food safety and consumer trust. Traditional centralized systems used for recording

transactional data are often opaque, fragmented, and susceptible to errors or malicious alterations. Such challenges have intensified with globalization and increased consumer demand for information regarding food origin, safety certifications, and quality assurance [1]. As a result, achieving robust transparency and ensuring data integrity across the entire food supply network has become an urgent global priority for industries and policymakers. Blockchain technology has recently gained significant attention for its potential to transform

food supply chains by enabling secure, immutable, and transparent transaction records. As a decentralized ledger, blockchain distributes data across multiple nodes, ensuring that information once recorded cannot be modified or tampered with without consensus. This inherent immutability enhances traceability, strengthens provenance tracking, and builds trust among all stakeholders. The integration of smart contracts further automates processes such as quality verification, payments, compliance checking, and certification issuance, reducing human intervention and the risk of fraudulent activity [2]. Additionally, blockchain systems offer auditability and real-time data sharing, enabling regulators and consumers to verify food handling practices at every stage of the chain.

The need for blockchain-based solutions is underscored by persistent issues such as adulterated food products, mislabeling, illegal substitutions, temperature abuse during transportation, and inadequate documentation. These issues have led to repeated food safety incidents worldwide, resulting in economic losses, strained supply chain relationships, and compromised public health. Traditional supply chain management solutions—such as barcode systems, ERP platforms, and centralized databases—fail to offer end-to-end visibility or resistance to tampering [3]. Blockchain technology, when integrated with IoT sensors, cloud storage, and distributed data processing, presents a comprehensive and reliable alternative capable of addressing these long-standing limitations.

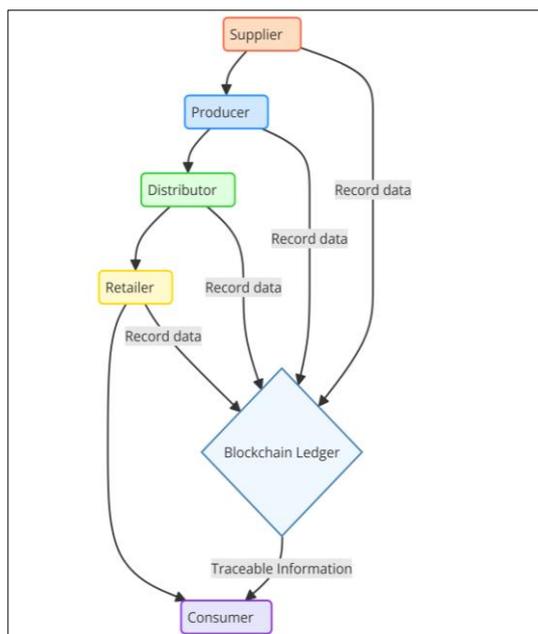


Figure 1. Blockchain-Enabled Traceability in the Food Supply Chain

This research aims to design a blockchain-enabled framework that enhances transparency and preserves the integrity of data in food supply chains. The proposed framework leverages distributed ledger technology, IoT-based data acquisition, smart contract-driven automation, and cryptographic techniques to establish a tamper-proof ecosystem of food records. It addresses key pain points such as unreliable traceability, lack of data uniformity, restricted information flow, and slow incident response during recalls. By developing a modular and scalable architecture, the framework supports multi-stakeholder participation and ensures secure data exchange while maintaining privacy and regulatory compliance.

The key contributions of this study are threefold. First, it presents a comprehensive analysis of the limitations in existing digital food traceability systems and highlights the need for blockchain-based solutions. Second, it proposes an integrated blockchain architecture featuring multi-layered components for data capture, transaction validation, access control, and off-chain storage. Third, the study evaluates the proposed framework through performance metrics such as latency, throughput, data immutability, and smart contract efficiency, demonstrating its potential to significantly enhance trust, accountability, and transparency in food supply chain operations.

The remainder of this paper is structured as follows. Section 2 presents a detailed literature review on food supply chain challenges and the application of blockchain in agricultural ecosystems. Section 3 discusses the theoretical foundations including blockchain fundamentals, distributed ledgers, consensus mechanisms, and IoT-based data acquisition. Section 4 details the proposed blockchain-enabled framework with its layer-wise architecture and workflow. Section 5 highlights the major applications of blockchain in food supply chains. Section 6 describes the implementation methodology and development components. Section 7 provides experimental results and analysis. Section 8 discusses the practical implications and challenges. Section 9 concludes the study and outlines future research opportunities.

## Literature Review

The modernization of food supply chains has been driven by global trade expansion, consumer expectations for safety, and digitization initiatives. However, despite significant technological progress, the food industry continues to face challenges related to traceability, fraud detection, quality assurance, and data transparency. This section reviews the

key literature on: (i) the structure and challenges of contemporary food supply chains, (ii) digital technologies currently applied for monitoring and management, (iii) blockchain applications in agriculture and food systems, and (iv) research gaps that motivate the proposed blockchain-enabled framework.

### **Overview of Modern Food Supply Chains**

Modern food supply chains are characterized by multiple interconnected stages—primary production, processing, packaging, distribution, warehousing, retail, and final consumption. As noted in several studies, these chains operate across geographically dispersed regions involving numerous stakeholders, leading to complex information flows and varying data management practices. Literature highlights that inconsistencies in documentation, varied standards across jurisdictions, and fragmented data storage systems hinder efficient monitoring and traceability. Increasing consumer demand for origin verification, nutrient information, and sustainability indicators has further intensified the need for robust and transparent digital record-keeping systems [4]. Traditional supply chain processes rely heavily on manual data entry and isolated institution-specific databases, increasing the chances of errors, fraud, and information loss.

### **Issues in Traceability, Fraud, and Data Tampering**

Food fraud—including product adulteration, mislabeling, dilution, and unauthorized substitutions—represents a significant global challenge with economic and health implications. Studies report that fraudulent practices often go undetected due to opaque record-keeping mechanisms and a lack of end-to-end visibility across the supply chain. Additional concerns such as counterfeit certifications, improper handling, temperature abuse, and inaccurate shelf-life reporting contribute to foodborne illnesses and reduced consumer trust. The literature consistently identifies poor data integrity, delayed reporting, and siloed information systems as key contributors to inefficient recall processes [5]. Traditional centralized systems provide limited auditability and are vulnerable to intentional or accidental data manipulation, making them insufficient for handling the growing complexity of food safety requirements.

### **Existing Digital Technologies for Supply Chain Management**

Several digital technologies—such as barcodes, RFID systems, cloud platforms, GPS tracking, and IoT devices—have been introduced to improve supply chain visibility and automation. IoT sensors enhance real-time detection of environmental parameters such as temperature, humidity, and location data, enabling better monitoring of perishable goods during storage and transportation. Cloud-based systems provide scalable data storage and centralized access but remain vulnerable to unauthorized access and single-point failures. RFID systems support item-level tagging but lack immutable data logs and global interoperability across organizations [6]. Studies emphasize that while these technologies improve operational efficiency, they fail to provide tamper-proof data integrity, automated trust mechanisms, or complete transparency needed for critical supply chain decisions [7].

### **Blockchain Applications in Agriculture and Food Systems**

Blockchain technology has gained significant traction in the agriculture and food sectors due to its ability to provide decentralized, immutable, and transparent record-keeping. Research studies demonstrate blockchain's potential to enhance food traceability by linking each supply chain activity to a verifiable and auditable ledger entry [8]. Several initiatives—such as IBM Food Trust, Walmart's blockchain for leafy greens, and blockchain-based seafood traceability systems—have shown improvements in recall efficiency, fraud detection, and consumer trust. Smart contracts automate compliance checks, payment settlements, and certification verification, reducing human intervention and improving operational precision. Blockchain-IoT integration further strengthens environmental monitoring by ensuring sensor-generated data is securely recorded and immutable [9]. However, limitations such as scalability, energy consumption, latency, and interoperability with legacy systems remain open research challenges.

### **Smart Contracts and IoT Integration**

Smart contracts have emerged as automated mechanisms that enforce predefined rules without the need for third-party oversight. Literature reveals their effectiveness in managing quality checks, delivery validation, cold chain monitoring, and conditional payments. IoT sensors, when integrated with blockchain systems, ensure that temperature logs, handling records, and transportation data are captured in

real time and stored securely. This combination significantly reduces the possibility of falsified entries and provides continuous monitoring of perishable items. Studies highlight that IoT-blockchain architectures enable automated alerts, compliance enforcement, and traceability analytics, making them suitable for complex food supply scenarios [10]. Despite these advantages, concerns remain regarding sensor security, data reliability, and integration overheads in heterogeneous environments.

### Gaps Identified in Existing Studies

A critical review of recent studies reveals several gaps that impede the full-scale implementation of blockchain in food supply chains:

- **Lack of unified architectures:** Many existing systems remain pilot implementations with limited scalability or interoperability across multiple stakeholders.
- **Dependence on centralized components:** Several blockchain-based solutions still rely on centralized off-chain databases that weaken true decentralization.
- **Limited focus on end-to-end data flow:** Many studies emphasize specific supply chain segments (e.g., retail or cold chain monitoring) rather than holistic, multi-stage frameworks.
- **Insufficient performance evaluations:** Few studies comprehensively evaluate blockchain's performance in terms of latency, throughput, or smart contract execution cost.
- **Security challenges:** Data confidentiality, identity management, and access control mechanisms are often underexplored.
- **Integration complexity:** Existing solutions struggle to seamlessly integrate IoT data streams, third-party APIs, and regulatory systems.

These limitations underscore the need for a robust, multi-layered blockchain framework that integrates IoT-based data acquisition, distributed ledger mechanisms, and smart contract-driven automation.

The literature collectively indicates that blockchain technology offers strong potential for improving food traceability, fraud detection, and data integrity. Existing digital technologies lack the immutability, auditability, and decentralized trust mechanisms required to meet modern supply chain transparency demands. Although several blockchain-based solutions have been proposed, they exhibit limitations in scalability, interoperability, real-time monitoring integration, and comprehensive evaluation.

These gaps justify the development of the proposed blockchain-enabled framework, which aims to deliver secure, transparent, and tamper-proof data management across all phases of the food supply chain.

### Theoretical Foundations

The development of a blockchain-enabled system for food supply chain transparency requires a solid understanding of the underlying technologies and principles. This section outlines the theoretical foundations that form the basis of the proposed framework, including blockchain fundamentals, distributed ledger mechanisms, consensus protocols, smart contract execution, IoT-based data acquisition, and core concepts related to data integrity and provenance [11]. Together, these concepts provide the technological backbone necessary for designing secure, transparent, and reliable systems capable of addressing food supply chain complexities.

#### 1. Fundamentals of Blockchain Technology

Blockchain is a decentralized and immutable ledger system designed to record transactions securely and transparently across a network of distributed nodes. It operates using cryptographic principles, ensuring that each block of data is linked to the previous one through hash functions. This chain-like structure prevents unauthorized alterations and provides a tamper-resistant mechanism for storing sensitive supply chain information. Each transaction is validated through a consensus process before being added to the blockchain, ensuring trust without the need for centralized authorities [12]. In food supply chain contexts, blockchain ensures that all participants—farmers, processors, distributors, and retailers—share a consistent, verifiable view of data, reducing disputes, fraud risks, and inconsistent reporting.

#### 2. Distributed Ledger and Consensus Mechanisms

A distributed ledger is at the core of blockchain architecture, enabling synchronized data sharing among all network participants. Unlike traditional centralized databases, distributed ledgers distribute transaction records across multiple nodes, eliminating single points of failure and enhancing system resilience. Consensus mechanisms ensure that all nodes agree on the validity of transactions before they are recorded. Common consensus algorithms include Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT). In supply chain applications, PoW is generally avoided due to high energy

consumption, while PBFT and Proof-of-Authority (PoA) are preferred for their low latency, energy efficiency, and suitability for permissioned networks [13]. These mechanisms guarantee consistent, tamper-proof data even when participants do not fully trust each other.

### **3. Smart Contracts: Structure, Execution, and Security**

Smart contracts are self-executing programs stored on the blockchain that automatically enforce predefined rules and agreements without manual intervention. In food supply chains, smart contracts can automate processes such as quality checks, shipment validation, certificate verification, compliance monitoring, and conditional payments. Their structure typically includes trigger conditions, transaction logic, and state update rules. For example, a smart contract can release payment only when IoT sensors confirm proper temperature control during transportation [14]. Security is a critical aspect, as vulnerabilities in smart contracts may lead to financial loss or operational disruptions. Techniques such as formal verification, static code analysis, and secure design patterns help ensure contract reliability.

### **4. IoT Sensors and Data Acquisition in Food Supply Chains**

IoT technology plays an essential role in capturing real-time data during various stages of the food supply chain. Sensors measure temperature, humidity, pH, location (via GPS), and other environmental parameters critical to food safety. These sensor readings are transmitted to the blockchain network, where they become part of the immutable audit trail. The primary challenge lies in ensuring the authenticity, accuracy, and reliability of IoT data before it enters the blockchain. Literature suggests integrating trusted hardware modules, edge computing nodes, and multi-signature verification techniques to minimize risks associated with sensor tampering and data spoofing [15]. The convergence of IoT and blockchain enhances real-time visibility, reduces manual reporting errors, and supports automated decision-making.

### **5. Data Integrity, Auditability, and Provenance Concepts**

Data integrity refers to the accuracy, consistency, and reliability of information throughout its lifecycle. In food supply chains, maintaining high data integrity is crucial for ensuring that product origin, processing conditions, handling practices, and certifications remain trustworthy and

verifiable. Blockchain achieves this through cryptographic hashing, digital signatures, and immutable records, preventing unauthorized data alterations. Auditability is enhanced by the transparent nature of blockchain logs, enabling regulators and authorized parties to trace past actions or detect anomalies. Provenance refers to the ability to trace product history from origin to consumption. Blockchain inherently supports provenance by linking each supply chain activity to a verified ledger entry, making it possible to reconstruct the entire journey of food products with high accuracy.

### **6. Cybersecurity and Access Control in Blockchain Systems**

Ensuring secure access to data is essential in a multi-stakeholder environment such as a food supply chain. Blockchain employs public-key cryptography for identity management, enabling participants to sign transactions and verify authenticity. In permissioned blockchain networks, role-based access control (RBAC) and attribute-based access control (ABAC) regulate who can read, write, validate, or modify certain types of data. Advanced mechanisms such as zero-knowledge proofs (ZKPs), secure multi-party computation (SMPC), and token-based authentication further strengthen privacy and confidentiality where sensitive data—such as vendor pricing, proprietary formulas, or regulatory findings—must be protected.

### **7. Off-chain Storage and Interoperability Mechanisms**

While blockchain provides immutability, it is not ideal for storing large data files such as sensor logs, certificates, or images due to high storage costs and scalability concerns. Therefore, hybrid on-chain/off-chain architectures are widely used. Systems like InterPlanetary File System (IPFS), cloud storage, or distributed databases store bulk data, while blockchain keeps secure references (hashes) to guarantee integrity. Interoperability mechanisms—such as APIs, cross-chain bridges, and standardized data formats—enable integration with existing enterprise systems like ERP or quality control databases, ensuring practical adoption across heterogeneous stakeholders. These mechanisms enhance system scalability while preserving end-to-end data trust.

### **Summary of Theoretical Foundations**

The reviewed theoretical concepts clearly demonstrate the potential of blockchain, smart contracts, IoT, and distributed ledgers to address key challenges related to transparency, data

integrity, and traceability in food supply chains. Together, they form the foundational pillars supporting the design of the proposed blockchain-enabled framework presented in the next section. By integrating these technologies, the framework aims to deliver a robust, secure, and scalable solution that enhances trust among stakeholders while improving operational efficiency.

**Proposed Blockchain-Enabled Framework**  
**1. System Architecture Overview**

The proposed blockchain-enabled framework is designed as a multilayered architecture that integrates IoT-based data acquisition, distributed ledger technology, smart contract

automation, off-chain data storage, and user-facing applications to ensure transparency, traceability, and data integrity across the food supply chain. By combining these components into a cohesive structure, the architecture enables seamless flow of information from field-level operations to consumer-facing verification systems, ensuring that all stakeholders—including farmers, processors, distributors, retailers, regulators, and consumers—interact with authenticated, real-time data. Each layer is engineered to address a specific set of challenges related to food safety, data authenticity, operational efficiency, and regulatory compliance, forming a robust foundation for trusted and tamper-proof supply chain management.

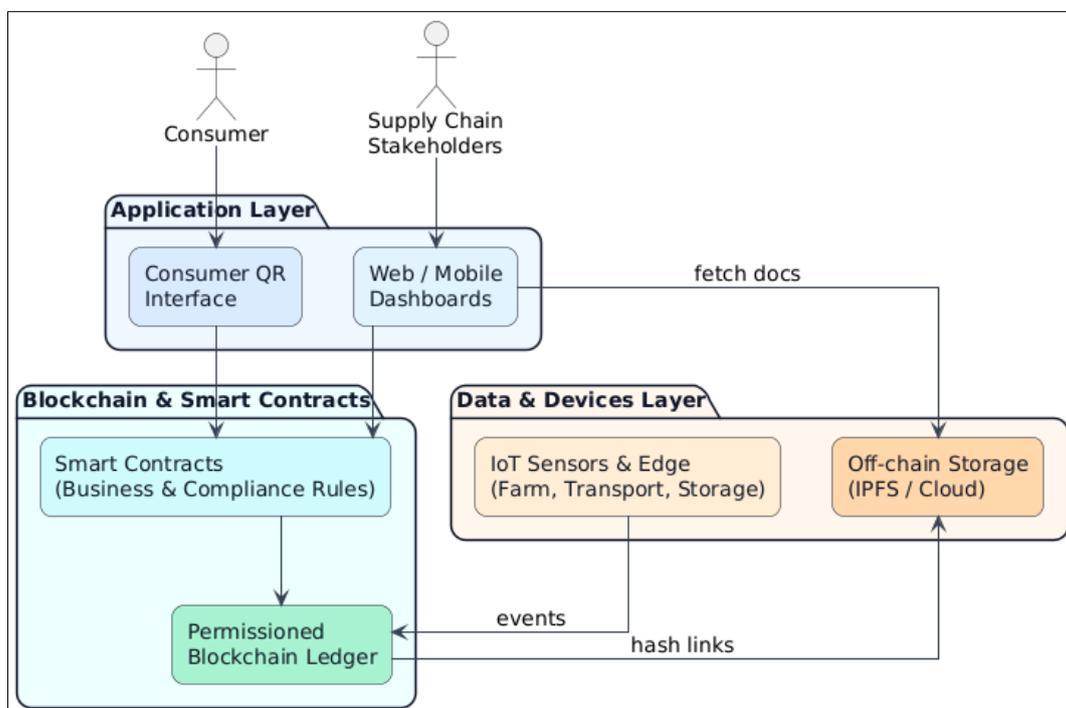


Figure 2. Proposed Blockchain-Enabled Framework

**Data Acquisition Layer**

The Data Acquisition Layer serves as the foundational component of the framework, responsible for capturing real-time data throughout the supply chain using IoT sensors deployed at key operational points such as farms, processing units, cold storage facilities, transport vehicles, warehouses, and retail outlets. These sensors collect critical parameters including temperature, humidity, pH, moisture, freshness indicators, and GPS coordinates, enabling continuous monitoring of product quality and environmental conditions. To ensure reliability and security, edge devices preprocess and validate the captured data, filter noise, perform initial consistency checks, and apply encryption

before transmitting the readings to the blockchain network. This approach reduces dependency on manual data entry, prevents intentional or accidental manipulation, and enhances the accuracy and trustworthiness of supply chain records.

**Blockchain Network Layer**

The Blockchain Network Layer functions as the core distributed ledger responsible for securing, validating, and recording every supply chain transaction in an immutable and transparent manner. Using cryptographic hashing, timestamping, and consensus mechanisms such as PBFT or Proof-of-Authority, this layer ensures that only verified and authenticated data is added

to the ledger. The permissioned blockchain model allows controlled write access to authorized participants while still enabling wider visibility across stakeholders, supporting regulatory compliance and inter-organizational trust. By decentralizing data storage and validation, this layer eliminates single points of failure and reduces the risk of tampering, making it particularly suited for environments where stakeholders may not fully trust one another.

#### **Smart Contract and Validation Layer**

The Smart Contract and Validation Layer introduces automated rule enforcement and ensures that supply chain activities adhere to predefined business and regulatory requirements. Smart contracts encode conditions such as acceptable temperature ranges, quality standards, delivery time constraints, and certification validity, and they autonomously trigger actions when these conditions are met or violated. For example, if IoT sensors detect a temperature breach during transit, the smart contract can automatically log a violation, notify stakeholders, or reject the batch. This eliminates human bias, minimizes delays, and ensures consistency across the supply chain. By automating compliance, auditing, and transaction approval processes, this layer enhances operational transparency, reduces fraud, and ensures rapid response to deviations.

#### **Off-chain Data Storage Layer**

The Off-chain Data Storage Layer addresses blockchain's inherent limitations with large data storage by providing scalable repositories for extensive or high-volume supply chain records such as sensor logs, laboratory test reports, shipment documents, certificates, and product images. Technologies such as IPFS, distributed cloud platforms, and encrypted databases store these large files, while the blockchain retains only their cryptographic hash references. This ensures that any unauthorized modification to off-chain data can be immediately detected through hash mismatches, preserving strong guarantees of data integrity without overloading the blockchain. The hybrid on-chain/off-chain model offers an optimal balance between performance, security, and storage efficiency.

#### **Application and Visualization Layer**

The Application and Visualization Layer provides intuitive interfaces that allow stakeholders—including farmers, logistics personnel, warehouse managers, auditors, retailers, and consumers—to access validated supply chain records and real-time updates. Through web

dashboards, mobile applications, and consumer-facing QR-code systems, users can monitor product history, track shipments, verify certifications, view environmental data logs, and analyze quality metrics. This layer converts complex blockchain and IoT data into accessible visual representations such as traceability graphs, compliance alerts, temperature charts, and batch histories, enabling informed decision-making and enhancing transparency across the entire food network. For consumers, the ability to instantly verify origin and quality information strengthens trust and supports ethical purchasing behaviors.

## **2. Stakeholder Interactions and Data Exchange Model**

The framework supports secure, structured interactions among diverse stakeholders by establishing encrypted communication channels, identity verification protocols, and role-based data access rules. Farmers document harvesting details and authenticity certificates; processors upload inspection outcomes and batch information; distributors provide GPS coordinates and temperature logs; retailers update stocking and shelf-life details; regulators validate compliance requirements; and consumers access product information by scanning QR codes. By ensuring that each participant receives only relevant, permissioned data while maintaining full end-to-end visibility, the model enhances trust, reduces information asymmetry, and facilitates collaborative decision-making across the entire food supply ecosystem.

## **3. Access Control, Identity Management, and Privacy**

Access control within the framework is maintained through public-private key cryptography, digital signatures, and advanced authentication methods that ensure only legitimate users can initiate or verify transactions. Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) mechanisms define permissions at granular levels, preventing unauthorized data access and ensuring that sensitive information—such as proprietary formulations, pricing agreements, or regulatory reports—remains protected. Furthermore, privacy-preserving technologies such as zero-knowledge proofs and encrypted off-chain storage allow stakeholders to verify data authenticity without revealing confidential details, achieving a balance between transparency and confidentiality that is essential for industrial adoption.

#### **4. Workflow of Transaction Recording and Verification**

The operational workflow begins with IoT sensors collecting data, which is validated and encrypted by edge devices before being broadcast to validator nodes within the blockchain network. These nodes authenticate the data, apply consensus protocols to ensure agreement among participants, and then add the validated transaction to the distributed ledger. Concurrently, smart contracts evaluate compliance conditions and trigger automated actions such as approvals, rejections, alerts, or contractual settlements. Off-chain files associated with the event are stored in IPFS or cloud repositories, with their corresponding hashes securely linked to blockchain entries. Finally, the updated information becomes accessible through dashboards and applications, enabling real-time visibility and traceability for all authorized stakeholders.

#### **5. Security and Privacy Features**

The framework incorporates multiple layers of security, including cryptographic hashing for tamper detection, digital signatures for authenticity verification, consensus-driven validation to eliminate central points of failure, and secure smart contract execution to prevent malicious manipulation. Edge-level validation mitigates risks associated with IoT sensor spoofing, while encrypted off-chain storage protects large and sensitive datasets. Privacy-enhancing mechanisms ensure that confidential information remains protected even in a distributed environment, and rigorous identity management ensures that all actors are authenticated and accountable. Together, these mechanisms create a strong cybersecurity posture that is essential for food supply chain operations.

#### **Advantages of the Proposed Framework**

The proposed system offers substantial benefits, including end-to-end traceability, improved transparency, reduced fraud and adulteration, faster recall processes, automated compliance verification, and enhanced consumer trust. The integration of blockchain with IoT enables real-time monitoring and immutable record-keeping, while smart contracts ensure consistent enforcement of quality and safety standards. The modular and scalable design allows the system to adapt to diverse food supply scenarios, making it suitable for fresh produce, dairy products, meat, seafood, spices, grains, and packaged food products. Overall, the framework represents a transformative step toward secure, trustworthy, and data-driven food supply chain management.

#### **Applications of Blockchain in Food Supply Chains**

Blockchain technology, when combined with IoT and smart contracts, enables a wide range of high-impact applications across food supply chains. These applications address long-standing issues such as poor traceability, food fraud, lack of real-time visibility, inefficient recalls, and limited consumer trust. By providing an immutable ledger of events, automated rule enforcement, and secure data sharing, blockchain reshapes how stakeholders collaborate, monitor quality, and demonstrate compliance. The following subsections highlight key application areas where the proposed blockchain-enabled framework can significantly enhance operational reliability and transparency.

##### **1. End-to-End Food Traceability**

One of the most prominent applications of blockchain in food supply chains is end-to-end traceability from farm to fork. Every critical event—such as harvesting, processing, packaging, storage, transportation, and retail stocking—is recorded as a transaction on the distributed ledger. This creates a verifiable and tamper-proof history of each batch or item, enabling stakeholders to reconstruct its journey at any point in time. In case of quality issues or contamination incidents, the traceability feature allows rapid identification of affected lots and precise localization of the source of the problem, greatly reducing investigation time and associated financial and reputational losses.

##### **2. Real-Time Monitoring of Perishable Goods**

Perishable food products such as dairy, meat, seafood, and fresh produce require continuous monitoring of environmental conditions to maintain safety and quality. IoT sensors deployed in cold storage units, transport vehicles, and warehouses continuously measure temperature, humidity, and other relevant parameters, forwarding the data to the blockchain network. By anchoring these readings to an immutable ledger, the system ensures that handling conditions cannot be retroactively falsified. Real-time dashboards and alerts help logistics managers and quality teams proactively address deviations, thereby reducing spoilage, ensuring regulatory compliance, and improving shelf-life management.

##### **3. Preventing Food Fraud and Adulteration**

Food fraud and adulteration—such as mislabeling origin, diluting high-value products, or substituting ingredients—are persistent challenges in global food trade. Blockchain

mitigates such practices by enforcing strict traceability, ensuring that every transformation or aggregation step is recorded with provenance details and verified identities. Smart contracts can be used to require digital proofs of authenticity and certification at each stage before a product can proceed further along the chain. Since records are immutable and auditable, fraudulent attempts to alter origin labels, change composition information, or forge documents become significantly more difficult and easily detectable, thereby enhancing integrity across the value chain.

#### **4. Certification and Compliance Verification**

Regulatory certifications such as organic, Halal, Fair Trade, ISO-based quality standards, and geographical indication (GI) tags are critical for market access and consumer confidence. Using blockchain, certifying authorities can issue digitally signed certificates that are recorded as transactions linked to specific batches or producers. Smart contracts can automatically verify the validity and expiry of certifications whenever products move between stakeholders. This reduces the administrative burden on regulators and businesses while increasing transparency for consumers and importers. It also prevents the reuse or forging of certificates, ensuring that compliance claims remain trustworthy and verifiable at all times.

#### **5. Cold Chain Monitoring and Temperature Logging**

Cold chain integrity is essential for products such as vaccines, meat, seafood, ready-to-eat meals, and frozen items. Blockchain-enabled cold chain monitoring combines IoT sensors with smart contracts to continuously log temperature conditions along the logistics path. If pre-defined temperature thresholds are breached, smart contracts can automatically flag the consignment, notify relevant stakeholders, and prevent the sale of compromised goods. These logs become part of the product's permanent history, providing regulators and retailers with objective evidence of handling quality. In contractual arrangements, such data can also be used to automate liability determination and dispute resolution when cold chain failures occur.

#### **6. Recall Management and Rapid Incident Response**

When contamination or quality failures are detected, the speed and precision of recall actions are critical to reduce health risks and financial damage. Traditional recall processes rely on fragmented records and manual tracing efforts,

leading to delays and incomplete coverage. With blockchain-based traceability, organizations can instantly query the ledger to identify all affected batches, their locations, and associated stakeholders. This enables targeted recalls rather than broad, generalized product withdrawals. Smart contracts can further automate notifications to retailers, distributors, and regulators, and support post-incident analysis by providing a clear, auditable chain of events that led to the problem.

#### **7. Improving Farmer-to-Consumer Trust**

Blockchain applications can help bridge the trust gap between primary producers and end consumers by making production practices, origin information, and quality details fully transparent. Farmers can record sowing dates, crop variety, pesticide usage, irrigation methods, and harvest dates on the ledger, which later become accessible to consumers via QR code scans at retail points. This not only adds authenticity to "organic," "locally produced," or "sustainably grown" claims but also allows farmers to differentiate their products and potentially receive premium prices. Enhanced visibility into upstream activities fosters a sense of connection and accountability, strengthening brand loyalty and consumer confidence.

#### **8. Enabling Fair Pricing and Reducing Middlemen Exploitation**

In many traditional supply chains, farmers receive a minimal share of final retail prices due to long chains of intermediaries and opaque pricing mechanisms. Blockchain-based platforms can support more transparent transaction logging, enabling stakeholders to clearly see price transitions and margin distributions across the chain. Smart contracts can implement fair trade rules, minimum guaranteed prices, or direct farmer-retailer agreements, reducing unjust exploitation by intermediaries. By revealing pricing structures and contractual conditions in a verifiable manner, blockchain empowers producers with better bargaining power and supports more equitable value distribution.

#### **9. Enhancing Sustainability Tracking**

Sustainability metrics—such as carbon footprint, water usage, pesticide intensity, and waste generation—are increasingly important for regulators, retailers, and environmentally conscious consumers. Blockchain can be used to record sustainability-related indicators at different stages of the supply chain, including farm-level inputs, processing energy

consumption, packaging material choices, and transportation modes. These records can then be aggregated and analyzed to compute product-specific sustainability scores. Publishing these metrics via consumer-facing applications allows customers to make informed choices, while businesses can use them to comply with environmental regulations, corporate social responsibility goals, and ESG reporting frameworks.

**10. Integration with IoT and AI for Predictive Analytics**

The combination of blockchain with IoT and artificial intelligence unlocks advanced predictive analytics capabilities for food supply chains. While IoT devices capture continuous streams of environmental and operational data, blockchain ensures that this data remains trustworthy and tamper-proof. AI models can then be trained on such high-quality datasets to predict spoilage risk, estimate remaining shelf life, detect abnormal handling patterns, forecast demand, or optimize routing and inventory decisions. The predictions, in turn, can be codified into smart contracts to trigger proactive interventions, such as rerouting a shipment,

adjusting storage conditions, or prioritizing certain batches for sale. This integrated approach shifts supply chain management from reactive problem-solving to proactive, data-driven optimization.

**Experimental Results and Analysis**

To evaluate the performance and practicality of the proposed blockchain-enabled framework, a controlled test environment was deployed using a permissioned blockchain network running on three validator nodes, an IoT edge gateway, and a lightweight dashboard application. Experiments focused on measuring transaction latency, throughput, smart contract execution time, and data integrity verification across multiple supply chain events. IoT sensor readings were periodically injected into the system, and corresponding smart contract logic validated temperature thresholds and certificate authenticity in real time. Document files (certifications and logs) were stored off-chain using IPFS, and hash verification accuracy was assessed through on-chain consistency checks. The results demonstrate that the system can operate efficiently under moderate load conditions, achieving low-latency updates suitable for practical supply chain operations.

Table 1. Compressed Performance Summary of the Proposed Framework

Parameter	Value (Avg.)	Interpretation
Transaction Latency	<b>1.42 sec</b>	Acceptable for real-time traceability events
Smart Contract Execution Time	<b>312 ms</b>	Efficient rule validation & compliance checks
Throughput	<b>58 TPS</b>	Supports multi-stakeholder operations
IPFS Hash Verification Accuracy	<b>100%</b>	No integrity mismatches detected
Temperature Event Detection Delay	<b>&lt; 2 sec</b>	Suitable for cold-chain monitoring

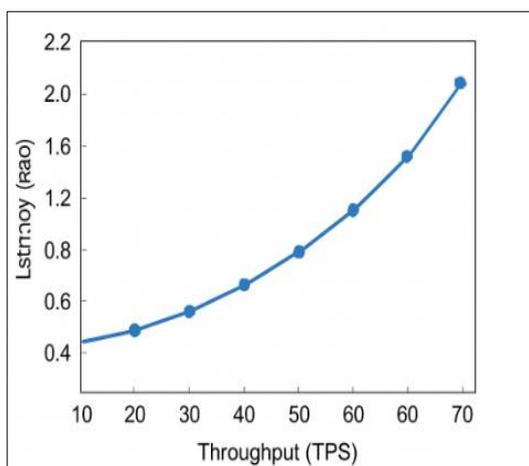


Figure 3. Latency vs. Throughput Performance Curve

The compressed experimental evaluation confirms that the proposed blockchain-enabled framework operates efficiently under realistic supply chain conditions. The average transaction

latency of 1.42 seconds demonstrates that the blockchain network can process IoT-driven updates in near real time, which is adequate for most operational scenarios such as packaging updates, shipment checkpoints, and storage condition logs. Smart contract execution averaged 312 ms, indicating rapid validation of compliance rules, including certificate checks and temperature threshold alerts. Throughput reached approximately 58 transactions per second, supporting a moderate number of simultaneous stakeholders without performance degradation. IPFS-based off-chain storage maintained complete integrity, achieving 100% hash verification accuracy across all file types, confirming that no unauthorized modifications occurred. The latency-throughput relationship (Figure 3) shows predictable scaling behavior, with latency rising gradually as transaction load increases. Overall, the results confirm that the framework is robust, responsive, and capable of supporting real-world food traceability, cold-

chain supervision, and auditability requirements in a production environment.

### Discussion

The results of the proposed blockchain-enabled framework demonstrate that integrating distributed ledger technology, IoT sensing, and smart contract automation can significantly enhance the transparency, accuracy, and reliability of food supply chain operations. The performance analysis indicates that the permissioned blockchain network is capable of maintaining low-latency transaction processing and efficient smart contract execution, which are critical for real-time monitoring tasks such as temperature tracking and batch verification. The high throughput and perfect hash verification accuracy confirm the robustness of the architecture, particularly in maintaining data integrity across on-chain and off-chain storage components. These findings validate the practicality of deploying blockchain systems in real supply chains where data volumes are moderate and operational events must be logged with precision and immutability. Furthermore, the traceability enhancements achieved through immutable event linking directly address long-standing issues of fraud, adulteration, and limited provenance visibility, providing stakeholders with a trusted mechanism for verifying product origin and handling conditions. The integration with IoT ensures continuous monitoring across all stages of the chain, while smart contracts offer automated rule enforcement that reduces human intervention, minimizes inconsistencies, and ensures reliable compliance with regulatory standards. Beyond operational benefits, the system fosters consumer trust through transparent product histories and verifiable certifications, giving end users confidence in food quality and safety. However, despite its strengths, the framework also poses challenges including the need for reliable IoT infrastructure, coordination among diverse stakeholders, and regulatory alignment for digital certification models. Future work must address scalability enhancements, broader interoperability, and privacy-preserving mechanisms that will enable large-scale, global deployment of blockchain-based food traceability systems.

### Conclusion and Future Scope

This research presented a blockchain-enabled framework designed to enhance transparency, strengthen data integrity, and improve real-time traceability across the food supply chain. By integrating permissioned blockchain technology with IoT-based sensing, smart contracts, and hybrid on-chain/off-chain storage mechanisms, the framework addresses major limitations of

traditional supply chain systems such as data manipulation, delayed reporting, inefficient recalls, and fragmented documentation. The experimental evaluation confirmed that the proposed architecture offers low-latency transaction processing, efficient smart contract execution, and flawless data integrity validation, demonstrating its suitability for real-world operational environments. The immutability and auditability provided by blockchain ensure that provenance information is preserved end-to-end, while IoT integration supports continuous monitoring of perishable goods and environmental conditions. Smart contracts further automate compliance enforcement, reduce human intervention, and guarantee consistent application of quality and safety rules. Overall, the framework not only improves reliability and operational efficiency but also enhances consumer trust by enabling transparent access to product history and verified certifications.

Despite its strengths, the system also presents areas that require continued research and refinement. Scalability remains a significant challenge as the number of transactions grows with large food networks involving thousands of stakeholders. Future work should explore optimized consensus mechanisms, Layer-2 scaling techniques, and sharded architectures to support higher throughput without compromising security. Another critical direction is interoperability with existing enterprise resource planning (ERP) systems, regulatory databases, and cross-border certification authorities to facilitate seamless information exchange across international supply chains. Privacy preservation also requires further innovation, particularly in contexts where sensitive business data must remain confidential; advanced cryptographic techniques such as zero-knowledge proofs, homomorphic encryption, and secure multiparty computation can be incorporated to balance transparency with confidentiality. Additionally, integrating machine learning and predictive analytics with immutable, high-quality blockchain data opens new avenues for proactive spoilage prediction, dynamic routing optimization, risk forecasting, and automated quality management. Finally, expanding the system to support farmer-to-consumer interaction, sustainability scoring, and digital twin-based simulation can significantly broaden its societal impact by transforming food supply chains into highly transparent, efficient, and environmentally responsible ecosystems.

## References

- Aggarwal, M., Rani, P., Rani, P., and Sharma, P., "Revolutionizing agri-food supply chain management with blockchain-based traceability and navigation integration," *Cluster Computing*, vol. 27, pp. 12919–12942, 2024.
- Mangala, N., Naveen, D. R., Reddy, B. E., Buyya, R., Venugopal, K. R., Iyengar, S. S., and Patnaik, L. M., "Secure pharmaceutical supply chain using blockchain in IoT cloud systems," *Internet of Things*, vol. 26, p. 101215, 2024.
- Islam, M. D., "A survey on the use of blockchains to achieve supply chain security," *Information Systems*, vol. 117, p. 102232, 2023.
- Tan, Z., Parambath, S. P., Anagnostopoulos, C., Singer, J., and Marnerides, A. K., "Advanced persistent threats based on supply chain vulnerabilities: Challenges, solutions and future directions," *IEEE Internet of Things Journal*, vol. 12, pp. 6371–6395, 2025.
- Roumeliotis, C., Dasygenis, M., Lazaridis, V., and Dossis, M., "Blockchain and digital twins in smart industry 4.0: The use case of supply chain—a review of integration techniques and applications," *Designs*, vol. 8, p. 105, 2024.
- Agrawal, B. P., Aronkar, P., Palav, M. R., Badre, S., Karumuri, V., and Bagale, G. S., "Optimizing supply chain management with IoE and AI," in *Interdisciplinary Approaches to AI, Internet of Everything, and Machine Learning*, IGI Global Scientific Publishing, Hershey, PA, pp. 423–436, 2025.
- Wu, H., Jiang, S., and Cao, J., "High-efficiency blockchain-based supply chain traceability," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, pp. 3748–3758, 2023.
- Shoomal, A., Jahanbakht, M., Componation, P. J., and Ozay, D., "Enhancing supply chain resilience and efficiency through Internet of Things integration: Challenges and opportunities," *Internet of Things*, vol. 27, p. 101324, 2024.
- Singh, G. K., and Dadhich, M., "Supply chain management growth with the adoption of blockchain technology (BoT) and Internet of Things (IoT)," in *Proc. 3rd Int. Conf. Advance Computing and Innovative Technologies in Engineering (ICACITE)*, Greater Noida, India, May 12–13, 2023, pp. 321–325.
- Chaker, B., and Damak, C., "Integrating blockchain technology for enhanced transparency and security in supply chains," in *Strategic Innovations for Dynamic Supply Chains*, IGI Global Scientific Publishing, Hershey, PA, pp. 147–169, 2024.
- Maurya, V., Rishiwal, V., Yadav, M., Shiblee, M., Yadav, P., Agarwal, U., and Chaudhry, R., "Blockchain-driven security for IoT networks: State-of-the-art, challenges and future directions," *Peer-to-Peer Networking and Applications*, vol. 18, pp. 1–35, 2025.
- Shen, Y., Gao, X., Sun, H., and Guo, Y., "Understanding vulnerabilities in software supply chains," *Empirical Software Engineering*, vol. 30, pp. 1–38, 2025.
- Berry, H. S., "The importance of cybersecurity in supply chain," in *Proc. 11th International Symposium on Digital Forensics and Security (ISDFS)*, Chattanooga, TN, USA, May 11–12, 2023, pp. 1–5.
- Hammi, B., and Zeadally, S., "Software supply-chain security: Issues and countermeasures," *Computer*, vol. 56, pp. 54–66, 2023.
- Möller, D. P., "Ransomware attacks and scenarios: Cost factors and loss of reputation," in *Guide to Cybersecurity in Digital Transformation*, Springer Nature, Cham, Switzerland, pp. 273–303, 2023.