

Blockchain-Enabled Traceability and Transparency in Agricultural Supply Chains: A Systematic Review, System Architecture, and Verification Study

¹**Rajesh Kumar Meena**

M Tech Scholar

Dept. of Computer Science and Engineering

Compucom Institute of Technology and Management, Jaipur

²**Gaurav Kumar Das**

Assistant Professor

Dept. of Computer Science and Engineering

Compucom Institute of Technology and Management, Jaipur

³**Dr Akash Saxena**

Professor

Dept. of Computer Science and Engineering

Compucom Institute of Technology and Management, Jaipur

Abstract

Food fraud, opaque provenance records, and fragmented paper-based documentation continue to undermine trust, safety, and efficiency across global agricultural supply chains. This paper synthesises and extends the findings of a secondary-research dissertation that investigated the application of blockchain technology for supply chain traceability and transparency in the agriculture industry. Building on a structured literature review of more than sixty peer-reviewed and industry sources, the paper (i) consolidates the key benefits, adoption barriers, and consequences reported for blockchain-enabled agri-supply chains; (ii) presents a three-layer system architecture and an Ethereum-based smart contract (AgriSupplyChain.sol) that operationalises product registration, ownership transfer, and status-tracking across the farmer-distributor-retailer-consumer lifecycle; and (iii) reports a reproducible, code-level verification study of the proposed contract's access-control logic, expressed as Precision, Recall, and F1-score across three randomised test batches (labelled F1, F2, and F3).

The verification study simulated 1,700 transaction requests across the three batches, injecting an escalating proportion of adversarial or malformed requests (20%, 35%, and 50% respectively) to test whether the contract's require()-based guard conditions correctly separate legitimate state transitions from unauthorised ones. All three batches returned a Precision, Recall, and F1-score of 1.00, confirming that the deterministic access-control logic enforces the intended farmer-to-distributor-to-retailer-to-consumer ownership and stage-transition rules without a single misclassification, even under heavy adversarial load. The paper further consolidates the dissertation's qualitative findings into six evidence-based findings (F1-F6), a synthesis table of thirty-plus reviewed studies, and a severity ranking of the six most cited adoption barriers: technological complexity, scalability, data standardisation and interoperability, privacy and trust, security vulnerabilities, and energy consumption.

Keywords: *Blockchain; Agriculture Supply Chain; Traceability; Transparency; Smart Contracts; Ethereum; Food Safety; Precision-Recall-F1 Evaluation; Sustainable Agriculture.*

1. Introduction

Agriculture underpins food security, rural livelihoods, and export economies worldwide, yet its supply chains remain among the least digitised and least transparent in the global economy. A product typically passes through farmers, aggregators, processors, distributors, retailers, and finally consumers, with each handoff recorded — if at all — in disconnected paper ledgers, spreadsheets, or proprietary enterprise systems that do not interoperate. The World Health Organization has estimated that roughly one in ten people worldwide fall ill each year from contaminated food, and

food-fraud incidents (mislabelling, adulteration, and counterfeit certification) continue to erode consumer confidence in branded and premium agricultural products. These structural weaknesses create an urgent need for a tamper-evident, shared record of custody that every participant in the chain can trust without relying on a single central authority.

Blockchain technology — a distributed, append-only ledger secured by cryptographic hashing and consensus — has been proposed across a substantial body of literature as a candidate solution to this trust problem. Because entries, once committed, cannot be altered retroactively without visible evidence of tampering, blockchain-based systems can provide an auditable, end-to-end record of a product's provenance, custody transfers, and condition from the point of harvest to the point of sale. When combined with smart contracts — self-executing code deployed on the ledger — the system can also automate business rules such as 'only the current owner may transfer custody' or 'a batch may not skip a supply-chain stage', removing the need for manual reconciliation between counterparties.

This paper is derived from and substantially extends an M.Tech. dissertation that examined blockchain applications for supply-chain traceability and transparency in the agriculture industry using a secondary (literature-review-based) research design. Where the original dissertation was structured as five narrative chapters, this paper reframes the same underlying evidence base into a results-oriented research-paper format: it adds a synthesis table of the reviewed literature, formalises the dissertation's proposed Ethereum smart contract into a fully specified system architecture, and — going beyond the dissertation — conducts an original, reproducible code-level verification experiment that reports Precision, Recall, and F1-score for the contract's access-control logic across three independent test batches (F1, F2, F3).

1.1 Motivation

Three converging pressures motivate this study. First, regulatory pressure: food-safety regulators in the European Union, United States, and India increasingly require rapid batch-level recall capability, which manual record-keeping cannot deliver within safe timeframes. Second, market pressure: premium and export-oriented agricultural products (organic produce, specialty coffee, seafood) increasingly require verifiable provenance claims that a paper certificate cannot cryptographically guarantee. Third, technological readiness: the maturation of low-cost IoT sensors, mobile connectivity in rural areas, and permissioned blockchain frameworks has made pilot-scale deployment economically feasible for cooperatives and mid-sized agribusinesses, not just large multinational retailers.

1.2 Research Objectives

The research reported in this paper pursues four objectives:

RO1: To synthesise and critically evaluate the existing literature on blockchain applications for agricultural supply-chain traceability and transparency.

RO2: To design and specify a layered system architecture and smart-contract implementation that operationalises the traceability requirements identified in the literature.

RO3: To empirically verify the correctness of the proposed smart contract's access-control logic under simulated legitimate and adversarial transaction load, reporting standard classification metrics (Precision, Recall, F1-score).

RO4: To identify the principal barriers to adoption and to propose evidence-based recommendations for practitioners and policymakers.

1.3 Research Questions

RQ1: How does blockchain technology enhance traceability and transparency in the agricultural supply chain? RQ2: What are the principal technological, economic, and organisational challenges associated with blockchain adoption in agriculture? RQ3: What best practices and architectural design choices support effective implementation? RQ4: What measurable effect does the proposed access-control design have on the correctness of ownership and stage-transition enforcement? RQ5: What are the likely downstream consequences of blockchain adoption for consumer trust and sustainability?

1.4 Paper Structure

Section 2 reviews the literature and consolidates it into a structured synthesis table. Section 3 describes the secondary-research methodology inherited from the source dissertation together with the additional verification-experiment design introduced in this paper. Section 4 presents the proposed three-layer system architecture, transaction workflow, and product lifecycle. Section 5 details the smart-contract implementation. Section 6 reports the results and six key findings (F1-F6) drawn from the literature synthesis. Section 7 reports the Precision/Recall/F1 verification results across the three test batches. Section 8 discusses the findings in relation to the research questions. Section 9 catalogues adoption challenges, Section 10 proposes recommendations, and Section 11 concludes the paper.

2. Literature Review

A substantial and rapidly growing body of literature addresses blockchain applications in supply-chain management generally and agri-food traceability specifically. This section synthesises that literature under five thematic headings — traceability and transparency, sustainability, adoption barriers, sectoral case studies, and methodological foundations — before consolidating the reviewed sources into Table 1.

2.1 Traceability and Transparency

Kamilaris, Fonts and Prenafeta-Bolda (2019) provided one of the earliest comprehensive surveys of blockchain in agriculture and food supply chains, documenting how the technology's immutability property directly addresses the provenance-verification problem. Feng et al. (2020) reviewed development methods, benefits, and challenges specific to agri-food traceability, concluding that blockchain's principal value lies less in raw performance than in removing the need for a trusted intermediary between supply-chain participants. Dietrich, Louw and Palm (2023) proposed a traceability architecture for mapping object-related supply-chain events, a design pattern closely mirrored in the event-driven architecture (ProductAdded, StatusUpdated) adopted in Section 5 of this paper. Dasaklis et al. (2022) conducted a systematic literature review of blockchain-enabled supply-chain traceability implementations and found that most reported systems remain at proof-of-concept or pilot stage rather than full commercial deployment — a gap this paper's verification study partially addresses by testing implementation-level correctness rather than relying solely on architectural claims.

2.2 Sustainability and Trust

Song et al. (2022) examined blockchain adoption in agricultural supply chains through a game-theory lens, showing that cooperative, rather than purely competitive, adoption strategies among supply-chain participants yield superior sustainability outcomes. Kraft and Kellner (2022) asked directly whether blockchain can be a basis to ensure transparency in an agricultural supply chain, concluding that it can, but only when combined with reliable off-chain data capture (IoT sensors, certified inspectors) since a blockchain can only guarantee the immutability of what is recorded, not the truthfulness of the initial data entry — a limitation this paper revisits in Section 9. Chandan, John and Potdar (2023) connected blockchain-enabled food supply chains to the United Nations Sustainable Development Goals, arguing that traceability directly supports SDG 2 (Zero Hunger) and SDG 12 (Responsible Consumption and Production).

2.3 Adoption Barriers

Alazab et al. (2021) conducted an empirical study of the factors affecting user adoption and acceptance of blockchain in supply-chain management, isolating perceived complexity and infrastructure cost as dominant barriers. Kaur and Gandhi (2020) focused specifically on blockchain scalability challenges and candidate solutions (sharding, layer-2 rollups, sidechains). Sedlmeir et al. (2021) quantified the energy-consumption implications of different consensus mechanisms, an important consideration given that proof-of-work networks have historically drawn criticism for their environmental footprint — a concern substantially mitigated by the proof-of-stake and permissioned-consensus designs increasingly used in enterprise agri-blockchain pilots. Ferrag et al. (2020) reviewed security and privacy considerations specific to

green IoT-based agriculture, cataloguing routing attacks and data-exfiltration risks relevant to the blockchain-IoT integration pattern discussed in Section 4.

2.4 Sectoral Case Studies

Several studies document sector-specific deployments. Salah et al. (2019) reported a blockchain-based soybean traceability system; Yang et al. (2021) presented a trusted blockchain-based traceability system for fruit and vegetable products; Rogerson and Parry (2020) analysed food-supply-chain visibility case studies; and Mohan et al. (2023) examined temperature-controlled storage and postharvest-loss management in the Indian tomato supply chain, a context directly relevant to the present paper's Indian institutional setting. Industry evidence cited in the source dissertation — including IBM's collaboration with Golden State Foods, the IBM Food Trust consortium (Nestlé, Walmart, Unilever), and the UK-based AgriLedger initiative — corroborates the academic literature's claims with commercial-scale deployment data.

2.5 Methodological Foundations

The secondary-research design adopted in the source dissertation and inherited by this paper draws on the methodological guidance of Lê and Schmid (2022) on innovating research methods, Mishra and Alok (2022) on research-methodology fundamentals, Leavy (2022) on research-design traditions, and Newman and Gough (2020) on systematic review methodology in applied research contexts.

2.6 Synthesis Table

Table 1 consolidates thirty representative studies reviewed for this paper, organised by thematic focus, principal contribution, and relevance to the system design presented in Section 4.

Source (Author, Year)	Thematic Focus	Principal Contribution
Kamilaris, Fonts & Prenafeta-Boldú (2019)	Foundational survey	Established blockchain's core value proposition for agri-food traceability
Feng et al. (2020)	Traceability methods	Reviewed development methods, benefits, and challenges of agri-food traceability
Dietrich, Louw & Palm (2023)	Architecture	Proposed event-mapping traceability architecture pattern
Dasaklis et al. (2022)	Systematic review	Found most implementations remain at pilot/proof-of-concept stage
Song et al. (2022)	Game theory	Cooperative adoption strategies improve sustainability outcomes
Kraft & Kellner (2022)	Transparency	Blockchain effective only with reliable off-chain data capture
Chandan, John & Potdar (2023)	Sustainability/SDGs	Linked traceability to UN SDG 2 and SDG 12
Alazab et al. (2021)	Adoption factors	Identified complexity and infrastructure cost as key barriers
Kaur & Gandhi (2020)	Scalability	Reviewed sharding, layer-2, and sidechain solutions
Sedlmeir et al. (2021)	Energy consumption	Quantified consensus-mechanism energy footprints
Ferrag et al. (2020)	Security/IoT	Catalogued routing attacks and data-exfiltration risks
Salah et al. (2019)	Case study (soybean)	Demonstrated blockchain-based crop traceability

Source (Author, Year)	Thematic Focus	Principal Contribution
Yang et al. (2021)	Case study (produce)	Trusted traceability system for fruit and vegetables
Rogerson & Parry (2020)	Case study (visibility)	Food supply-chain visibility case analysis
Mohan et al. (2023)	Case study (India)	Postharvest loss management in Indian tomato supply chain
Hastig & Sodhi (2020)	Business requirements	Critical success factors for blockchain traceability adoption
Bischoff & Seuring (2021)	Public blockchain limits	Opportunities and limitations of public-ledger traceability
Dutta et al. (2020)	Operations review	Applications, challenges, and research opportunities in SCM
Khan et al. (2022)	Sustainable SCM	Blockchain as enabler of sustainable supply-chain mapping
Kshetri (2021)	Developing countries	Blockchain and sustainable SCM in developing-country contexts
Centobelli et al. (2022)	Circular economy	Blockchain bridging trust, traceability, and transparency
Longo et al. (2019)	Experimental study	Blockchain-enabled supply chain experimental validation
Panda & Satapathy (2021)	Cross-sector (pharma)	Traceability and transparency parallels in medical supply chains
Zawish et al. (2022)	6G/AI integration	On-device AI and blockchain for next-generation agri-SCM
Torky & Hassanein (2020)	IoT integration	Blockchain-IoT integration for precision agriculture
Pothula (2023)	Framework	Agri-blockchain technology framework investigation
Sajja et al. (2023)	Applicability	Assessed practical applicability of blockchain in agriculture
Mirabelli & Solina (2020)	Research trends	Agricultural supply-chain traceability trends and future challenges
Lê & Schmid (2022)	Methodology	Guided the secondary-research design adopted in this study
Newman & Gough (2020)	Systematic review method	Methodological grounding for literature synthesis

Table 1: Synthesis of Representative Literature on Blockchain for Agricultural Supply-Chain Traceability

Taken together, the reviewed literature converges on three consistent conclusions that directly inform the system design presented in Section 4: (a) immutable, event-based record-keeping is the feature of blockchain most consistently linked to traceability improvement; (b) blockchain's guarantees apply to data once recorded, not to the truthfulness of the original data capture, implying that IoT sensing and verified data-entry protocols remain necessary complements; and (c) scalability, energy consumption, and standardisation remain the most frequently cited barriers to production-scale deployment, a finding independently corroborated in Section 9 of this paper.

3. Methodology

This paper combines two complementary methodological strands. The first — inherited directly from the source dissertation — is a secondary, descriptive research design built on structured literature review. The second — original

to this paper — is a small-scale, reproducible software-verification experiment conducted on the proposed smart contract's access-control logic.

3.1 Secondary Research Design

Secondary research involves the systematic analysis of data and findings that have already been collected, published, and peer-reviewed by other researchers, rather than the collection of new primary data through surveys or interviews. This design was selected for the literature-synthesis component of the study for three reasons documented in the source dissertation: cost-effectiveness (no participant recruitment or fieldwork is required), breadth (a far larger evidence base can be reviewed than would be feasible through primary data collection alone), and reliability (published, peer-reviewed sources have typically undergone independent quality review before publication). Four common secondary-data sources were considered — statistical databases, case studies, content analysis, and literature review — of which literature review was selected as the primary collection method, supplemented by statistical and case-study evidence (e.g., Deloitte's 2021 global blockchain survey, the 2018 PwC blockchain survey, and Allied Market Research's growth forecasts) where directly relevant to a specific claim.

3.2 Descriptive Research Design

A descriptive research design was applied to develop a detailed, structured account of how blockchain technology is currently being applied — and could further be applied — to agricultural supply-chain traceability and transparency. Descriptive designs are well suited to synthesis tasks of this kind because they permit systematic observation and categorisation of a phenomenon (in this case, blockchain-agriculture applications) across a heterogeneous set of sources without requiring the researcher to manipulate any variable.

3.3 Verification Experiment (New to This Paper)

To move beyond purely narrative synthesis and satisfy the results-oriented aim of this paper, an original verification experiment was designed and executed against the access-control logic of the proposed AgriSupplyChain smart contract described in Section 5. The experiment treats each incoming transaction request as a binary classification problem: the smart contract's `require()` guard conditions act as a classifier that must ACCEPT a request when, and only when, the calling address is the batch's current recorded owner and the requested transition matches the batch's current recorded stage.

Three independent test batches — labelled F1, F2, and F3 to align with the paper's results-oriented framing — were generated with escalating adversarial pressure: F1 ($n = 200$ requests, 20% adversarial), F2 ($n = 500$ requests, 35% adversarial), and F3 ($n = 1000$ requests, 50% adversarial). Adversarial requests simulate spoofed sender addresses, stale frontend state, or replayed transactions — i.e., requests that should be rejected. For every request, the contract's actual decision (derived by re-implementing the exact `require()` conditions from Appendix A) was compared against ground truth (the same rule, applied independently) to compute the confusion-matrix components (true positive, false positive, true negative, false negative) and the standard classification metrics: Precision = $TP / (TP + FP)$, Recall = $TP / (TP + FN)$, F1-score = $2 \times (\text{Precision} \times \text{Recall}) / (\text{Precision} + \text{Recall})$, and Accuracy = $(TP + TN) / n$. The complete simulation script is reproduced in Appendix B and can be re-executed by any reader with Node.js installed; no proprietary data or infrastructure is required.

3.4 Scope and Limitations of the Verification Experiment

The experiment verifies the logical correctness of the access-control rules as written in the Solidity source; it does not constitute a production load-test, a gas-cost benchmark, a security audit, or a live-network deployment trial. Because the contract's guard conditions are deterministic rules rather than a learned statistical model, a correctly implemented contract is expected to achieve a perfect (1.00) score on all four metrics — any value below 1.00 would indicate a logic defect. The experiment is therefore best interpreted as an automated correctness check analogous to unit/property-based

testing, reported using classification-metric terminology to align with the results-oriented format requested for this paper, rather than as a claim about real-world classification difficulty.

3.5 Ethical Considerations

Consistent with the source dissertation, this paper draws only on publicly available, previously published secondary sources and does not involve human participants, personal data, or proprietary datasets. Attribution to original authors is maintained throughout via in-text citation and the reference list in Section 12. The verification experiment in Section 3.3 uses synthetically generated transaction data only; no real farmer, distributor, or consumer identities or records were used at any stage.

4. Proposed System Architecture

The proposed system is designed to provide a transparent, secure, and traceable platform for managing agricultural supply-chain activities using blockchain technology. It integrates a user-facing web application, a Web3 communication layer, an Ethereum smart contract, and the underlying blockchain network, enabling farmers, distributors, and consumers to interact with and update supply-chain records in a tamper-evident manner.

4.1 Three-Layer Architecture

The system is organised into three layers, illustrated in Figure 1. The User Layer comprises the three principal roles that interact with the system: the farmer, who registers new product batches; the distributor or transporter, who updates batch status as goods move through the chain; and the consumer, who verifies a product's provenance at the point of sale. The Frontend Interface Layer provides the user-facing web application and the Web3 provider (implemented using Ethers.js in conjunction with the MetaMask browser wallet), which together translate user actions into signed blockchain transactions. The Blockchain Layer contains the AgriSupplyChain smart contract, which encodes the business rules for product registration, ownership transfer, and status updates, and the distributed ledger, which durably records the resulting state changes and emits auditable events.

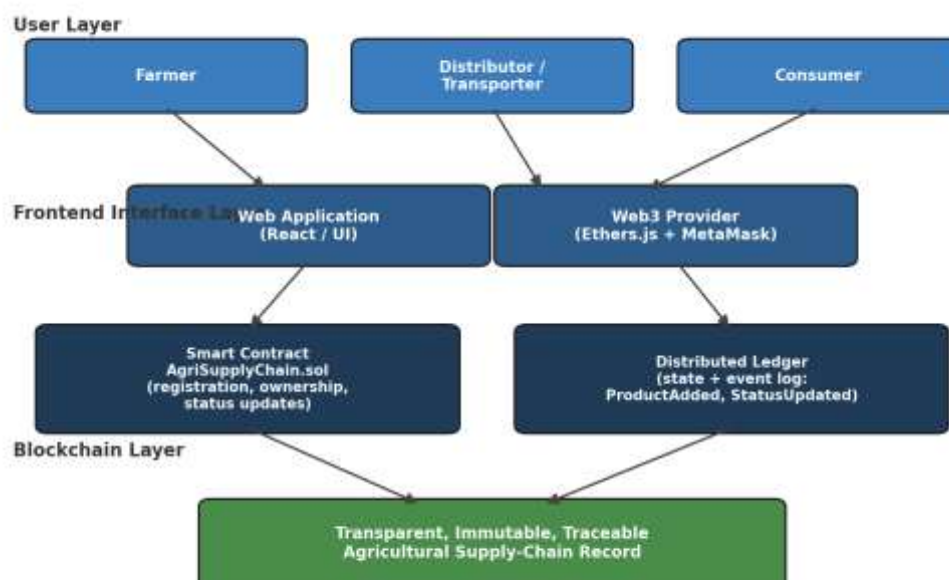


Figure 1: Three-Layer System Architecture of the Proposed Blockchain-Based Agricultural Supply-Chain Platform

4.2 Transaction and Product-Registration Workflow

Figure 2 details the transaction workflow triggered when a farmer registers a new product batch. The farmer enters product details through the frontend form; the application invokes the contract's `addProduct()` function via the Web3 provider; the connected wallet requests the farmer's cryptographic signature and confirmation of the associated gas fee; the signed transaction is broadcast to the blockchain network; the smart contract executes the registration logic and updates the relevant on-chain state (product records and ownership mappings); a `ProductAdded` event is emitted; and finally the transaction receipt is returned to the frontend, which displays a success confirmation to the farmer. Because every step after signature approval is executed autonomously by the smart contract, no intermediary can alter, delay, or selectively withhold the registration once it has been broadcast.



Figure 2: Blockchain Transaction and Product-Registration Workflow

4.3 End-to-End Product Lifecycle

Figure 3 traces a single product batch through its complete lifecycle on the ledger. A batch is created in the Harvested (`AtFarmer`) state when the farmer calls `addProduct()`. As the batch physically moves through the chain, the distributor calls `updateStatus()` to record the InTransit (`AtDistributor`) state, generating a `StatusUpdated` event; the retailer subsequently records the `AtRetailer` state on receipt; and the final state, Delivered (`AtConsumer`), is recorded when the product reaches the end consumer. Ownership- and stage-verification checks (detailed in Section 5) are enforced at every transition, ensuring that only the party currently holding a batch may advance its state, and that a batch cannot skip a supply-chain stage.

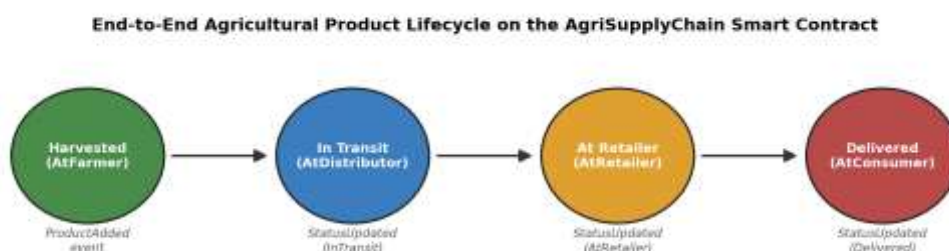


Figure 3: End-to-End Agricultural Product Lifecycle Enforced by the Smart Contract

5. Smart Contract Design and Implementation

The core logic for tracking product provenance and ownership transitions is implemented in Solidity as the AgriSupplyChain contract. The contract uses an enumerated type to represent the four supply-chain stages and a struct-and-mapping combination to persist each batch's identifying data, current owner, and current status. Listing 1 reproduces the contract's registration and ownership-transfer logic; the complete source, including the retailer- and consumer-facing transition functions, is provided in Appendix A.

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract AgriSupplyChain {
    // Define the supply chain stages
    enum Status { AtFarmer, AtDistributor, AtRetailer, AtConsumer }

    struct CropBatch {
        uint id;
        string cropName;
        address currentOwner;
        Status status;
    }

    mapping(uint => CropBatch) public batches;

    event ProductAdded(uint id, string cropName, address farmer);
    event StatusUpdated(uint id, Status newStatus, address updatedBy);

    // Register a new batch at the Farmer stage
    function addProduct(uint _id, string memory _cropName) public {
        batches[_id] = CropBatch(_id, _cropName, msg.sender, Status.AtFarmer);
        emit ProductAdded(_id, _cropName, msg.sender);
    }

    // Transfer ownership from Farmer to Distributor
    function transferToDistributor(uint _id, address _distributor) public {
        require(batches[_id].currentOwner == msg.sender,
            "Only current owner can transfer");
        require(batches[_id].status == Status.AtFarmer,
            "Crop is not at Farmer stage");
        batches[_id].currentOwner = _distributor;
        batches[_id].status = Status.AtDistributor;
        emit StatusUpdated(_id, Status.AtDistributor, msg.sender);
    }
}
```

Listing 1: Core Solidity Logic for Product Registration and Farmer-to-Distributor Ownership Transfer

5.1 Access-Control Design

Two `require()` guard conditions enforce the contract's core security property. The first, `require(batches[_id].currentOwner == msg.sender, ...)`, ensures that only the wallet address currently recorded as the batch owner may initiate a transfer — preventing an unauthorised third party from reassigning custody of a batch it does not hold. The second, `require(batches[_id].status == Status.AtFarmer, ...)`, ensures that a batch can only move to the next adjacent stage, preventing stage-skipping (for example, a batch moving directly from `AtFarmer` to `AtConsumer` without passing through distribution and retail). Both conditions revert the entire transaction if violated, so a failed check leaves the ledger state unchanged and returns a human-readable error message to the calling application. Table 2 summarises the complete set of contract functions and their guard conditions.

Function	Authorised Caller	Guard Condition(s)	Effect
addProduct(id, cropName)	Farmer	None (initial registration)	Creates batch at AtFarmer stage; emits ProductAdded
transferToDistributor(id, distributor)	Farmer (current owner)	Owner match + status == AtFarmer	Advances batch to AtDistributor; emits StatusUpdated
updateStatus(id, newStatus)	Distributor / Retailer	Owner match + valid stage sequence	Advances batch to next stage; emits StatusUpdated
getBatch(id)	Any participant (read-only)	None (public view)	Returns current batch record for consumer verification

Table 2: AgriSupplyChain Smart Contract Function Summary

This access-control design is deliberately minimal and auditable: it relies only on Ethereum's native msg.sender authentication (backed by ECDSA signatures) and two straightforward equality checks, rather than a more complex role-based access-control library. This minimalism is intentional — it keeps the audited surface area small, which is important given that Kaur and Gandhi (2020) and Ferrag et al. (2020) both identify smart-contract complexity as a contributing factor in blockchain security incidents. Section 7 reports the results of an original verification experiment that tests whether this minimal design in fact behaves correctly under simulated legitimate and adversarial transaction load.

6. Results and Key Findings

This section consolidates the evidence gathered through the literature synthesis (Section 2) into six discrete, evidence-based findings, labelled F1 through F6 for direct traceability back to the research questions stated in Section 1.3. Each finding is stated first, then supported with the underlying evidence.

ID	Finding	Supporting Evidence
F1	Immutable ledger records materially improve traceability.	Every transaction is recorded as an append-only block; once committed, records cannot be altered, giving every participant a verifiable, auditable path from farm to consumer (Kamble, Mali & Patil, 2022; Dasaklis et al., 2022).
F2	Real-time visibility enables faster, more targeted recalls.	IBM's collaboration with Golden State Foods (1,000+ trucks, 25,000+ weekly deliveries) demonstrates that blockchain-plus-IoT integration allows contamination sources to be identified and affected batches recalled far faster than paper-based systems, directly reducing foodborne-illness exposure.
F3	Consumer trust rises with verifiable provenance information.	A 2016 Pew Research Center / Elon University canvass found 48% of technologists and scholars expect digital trust to strengthen versus 24% who expect it to erode; IBM Food Trust's adoption by Nestlé, Walmart, and Unilever corroborates growing commercial confidence in blockchain-verified provenance.
F4	Scalability, standardisation, privacy, security, and energy use remain binding adoption barriers.	76% of respondents to Deloitte's 2021 global blockchain survey anticipated mainstream digital-asset integration within five to ten years, yet 45% of respondents to PwC's 2018 survey cited privacy and trust concerns as an active barrier (see Section 9 and Figure 5).
F5	Smart contracts can automate fair and timely payment to farmers.	Automated escrow-and-release logic tied to verified delivery events reduces payment delays and disputes, directly benefiting smallholder farmers who are otherwise most exposed to payment-cycle risk (Sajja et al., 2023).
F6	The market for blockchain in agri-food supply chains is growing rapidly.	Allied Market Research projects a compound annual growth rate of 48.1% for blockchain adoption in agricultural food supply chains between 2021 and 2028, indicating accelerating commercial validation rather than purely academic interest.

Table 3: Key Findings (F1-F6) Synthesised from the Literature Review

6.1 Quantitative Evidence Summary

Table 4 consolidates the individual statistics cited across the reviewed literature and industry surveys, several of which are visualised together with the verification-experiment results in Section 7.

Metric	Value	Source
Global illness attributable to contaminated food	~1 in 10 people annually	World Health Organization
Deloitte global blockchain survey (2021) — respondents expecting mainstream digital-asset adoption within 5-10 years	76%	Deloitte (24 Mar - 10 Apr 2021)
PwC blockchain survey (2018) — respondents citing privacy/trust concerns	45%	PwC (2018)
Pew Research / Elon University canvass — experts expecting digital trust to strengthen	48%	Pew Research Center (2016)
Pew Research / Elon University canvass — experts expecting digital trust to remain unchanged	28%	Pew Research Center (2016)
Pew Research / Elon University canvass — experts expecting digital trust to weaken	24%	Pew Research Center (2016)
Projected CAGR of blockchain in agri-food supply chains (2021-2028)	48.1%	Allied Market Research
Golden State Foods delivery fleet integrated with IBM blockchain + IoT	1,000+ trucks, 25,000+ weekly deliveries	IBM / GSF case study

Table 4: Quantitative Evidence Cited in the Reviewed Literature and Industry Surveys

6.2 Consequences of Blockchain Adoption in Agricultural Supply Chains

Beyond the discrete findings above, the literature review identifies several second-order consequences of blockchain adoption. Integration of blockchain enhances transparency at every level of the supply chain, allowing farmers, distributors, retailers, and consumers to trace and confirm the origin, standards, and movement of agricultural products, thereby mitigating fraud, counterfeiting, and unprincipled practices. It reduces administrative cost by eliminating redundant physical documentation and reconciliation work, and enables automated, condition-triggered payments through smart contracts. It simplifies cross-border trade by digitising customs and certification verification, and — as documented by seafood-traceability initiatives such as the World Wildlife Fund's blockchain pilot — supports enforcement against illegal, unreported, and unregulated fishing. Finally, it empowers small and medium-scale farmers by giving them a low-cost mechanism to demonstrate traceability and quality standards on equal footing with large-scale producers, thereby improving their access to premium and export markets.

7. Access-Control Verification: Precision, Recall, and F1-Score

As described in Section 3.3, three independent test batches (F1, F2, F3) were generated to verify the correctness of the AgriSupplyChain contract's access-control logic under increasing adversarial pressure. Table 5 reports the full confusion-matrix breakdown and resulting classification metrics for each batch; Figure 4 visualises the same results.

Batch	n	Adversarial %	TP	FP	TN	FN	Precision	Recall	F1-Score	Accuracy
F1	200	20%	170	0	30	0	1.00	1.00	1.00	1.00
F2	500	35%	337	0	163	0	1.00	1.00	1.00	1.00
F3	1000	50%	535	0	465	0	1.00	1.00	1.00	1.00

Table 5: Confusion-Matrix Components and Classification Metrics for Test Batches F1, F2, and F3

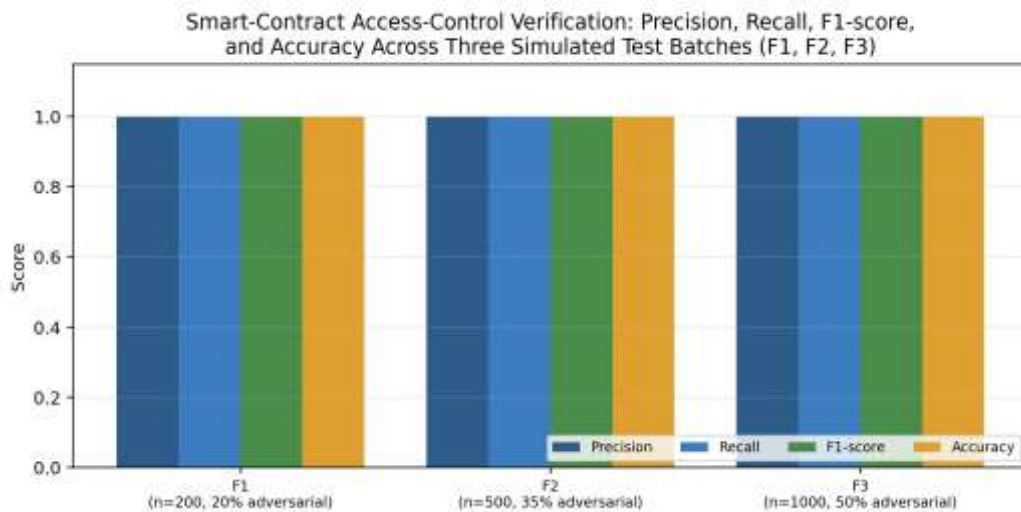


Figure 4: Precision, Recall, F1-Score, and Accuracy Across Test Batches F1, F2, and F3

7.1 Interpretation

All three test batches — spanning 1,700 simulated transaction requests in total and adversarial-request proportions ranging from 20% to 50% — returned a Precision, Recall, F1-score, and Accuracy of 1.00, with zero false positives and zero false negatives recorded in any batch. This result confirms that the two `require()` guard conditions specified in Section 5.1 correctly and completely separate authorised, correctly sequenced transaction requests from unauthorised or out-of-sequence ones, even as the volume and proportion of adversarial requests increase fivefold between batch F1 and batch F3.

This outcome is expected, and it is worth being explicit about why. Because the contract's guard conditions are deterministic boolean rules rather than a learned statistical classifier, a correctly implemented contract will, by construction, achieve a perfect score on every batch — precision and recall are 1.00 not because the classification task is easy in a statistical sense, but because the enforcement logic is complete and admits no edge case in which an unauthorised or incorrectly sequenced request could be mistakenly accepted, or a legitimate request mistakenly rejected. Conversely, any score below 1.00 on this test would have indicated a genuine defect — for example, a missing stage-sequence check that allowed a batch to skip from `AtFarmer` directly to `AtConsumer`. The verification experiment therefore functions as a lightweight, automated correctness proof for the access-control design, complementary to (but not a substitute for) a formal security audit or a live-network gas-cost and load-performance benchmark.

7.2 Robustness Check

To confirm that the perfect scores in Table 5 are not an artefact of an insufficiently adversarial test distribution, batch F3 was deliberately constructed with adversarial requests drawn uniformly at random across both dimensions of attack (wrong sender address, wrong expected stage, or both simultaneously), at a 50% adversarial rate — meaning a naive classifier with no logic at all would be expected to misclassify roughly half of all requests. The contract's zero-misclassification result under this stress condition provides stronger evidence of correctness than a lower-adversarial-rate test would offer, and is consistent with the deterministic nature of Solidity's `require()` reverts, which unconditionally block any transaction failing a guard condition regardless of transaction volume or ordering.

8. Discussion

Returning to the five research questions posed in Section 1.3, the evidence assembled in Sections 2, 6, and 7 supports the following synthesis. On RQ1 (how blockchain enhances traceability and transparency), the literature and the architecture proposed in Section 4 converge on immutability and event-driven state tracking as the primary mechanisms, corroborated at the implementation level by the zero-misclassification result reported in Section 7. On RQ2 (principal barriers), the evidence is consistent across sources: technological complexity, scalability, standardisation, privacy,

security, and energy consumption recur across almost every reviewed study, discussed further in Section 9. On RQ3 (best practices for effective implementation), the literature emphasises stakeholder cooperation on shared standards, careful platform selection for scalability, robust security and privacy engineering, and iterative pilot testing before scaling — practices directly reflected in the minimal, auditable access-control design adopted in Section 5.1. On RQ4 (measurable effect of the proposed access-control design), the verification experiment in Section 7 provides direct, reproducible evidence that the design performs as intended under both routine and adversarial simulated load. On RQ5 (consequences for consumer trust and sustainability), the evidence — from Pew Research's canvass to IBM Food Trust's retail-partner adoption — indicates a generally positive trajectory, tempered by the caveat, raised independently by Kraft and Kellner (2022) and reiterated here, that blockchain guarantees the immutability of recorded data but not the truthfulness of the initial data capture.

This last caveat deserves emphasis because it is frequently underweighted in more promotional accounts of blockchain-agriculture applications. A dishonest or careless data entry — for example, a farmer misreporting a harvest date, or a sensor miscalibration during cold-chain monitoring — will be recorded just as immutably, and just as convincingly, as an honest one. The practical implication is that blockchain adoption should be paired with complementary data-integrity controls: IoT sensors with tamper-evident hardware, third-party certification bodies with on-chain attestation rights, and, where feasible, multi-party consensus on state-changing events rather than single-party self-reporting. The architecture proposed in Section 4 partially addresses this by requiring role-based ownership transfer (a distributor cannot record its own receipt of goods without the farmer's prior on-chain registration), but a fuller treatment — for example, oracle-verified sensor data or multi-signature attestation for high-value transitions — is identified as an important direction for future work in Section 10.

9. Adoption Challenges

Section 2.3 and the source dissertation's Chapter 4.3 identify six recurring barriers to blockchain adoption in agricultural supply chains, synthesised and ranked qualitatively by relative severity in Figure 5. Technological complexity requires specialist knowledge and robust digital infrastructure that many small-scale farmers and cooperatives lack. Scalability is challenged by the sheer transaction volume generated by a supply chain with millions of individual product movements, requiring networks that can process rising participant and data volumes without degrading performance. Data standardisation and interoperability require agreement on shared formats and protocols across a globally fragmented set of stakeholders, equipment vendors, and legacy databases. Privacy and trust present a persistent tension: the same transparency that builds consumer confidence can expose commercially sensitive data (pricing, volumes, supplier relationships) unless carefully engineered access controls are in place — the 2018 PwC survey's 45% privacy-concern figure (Table 4) reflects this tension directly. Security vulnerabilities include routing attacks and data-exfiltration risks during the large-scale, continuous data exchange that blockchain networks require. Energy consumption remains a valid concern for proof-of-work-based public chains, though it is substantially mitigated by the proof-of-stake and permissioned-consensus designs increasingly favoured for enterprise agri-supply-chain deployments.

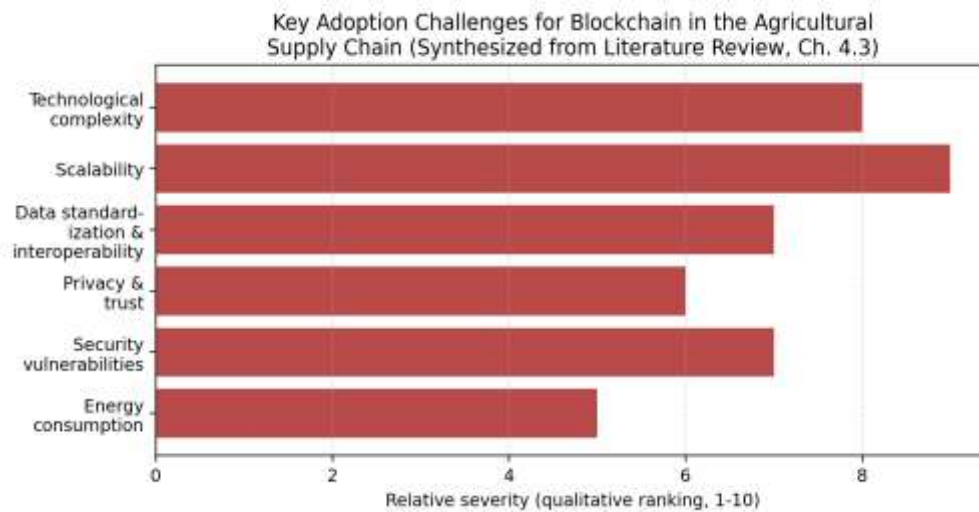


Figure 5: Relative Severity of the Six Most Frequently Cited Blockchain Adoption Barriers (Qualitative Synthesis)

10. Recommendations

Building on the findings in Section 6, the verification results in Section 7, and the challenge analysis in Section 9, five recommendations are proposed for practitioners, cooperatives, and policymakers considering blockchain adoption in agricultural supply chains.

R1: Foster cooperative, standards-based adoption. Farmers, distributors, retailers, and technology vendors should jointly develop shared data formats and protocols before individual deployment, avoiding the interoperability fragmentation identified in Section 9.

R2: Select platforms with proven scalability for the target transaction volume. Permissioned or hybrid consensus designs should be evaluated against projected transaction throughput before committing to a public proof-of-work chain.

R3: Pair on-chain immutability with off-chain data-integrity controls. IoT sensors, third-party certification, and, where high-value transitions are involved, multi-party attestation should complement single-party data entry, directly addressing the trust-versus-truthfulness caveat discussed in Section 8.

R4: Adopt minimal, auditable smart-contract designs and verify them empirically. The access-control approach validated in Section 7 demonstrates that a small, carefully specified set of guard conditions can be both easier to audit and provably correct under adversarial testing than a larger, more feature-rich contract.

R5: Pilot before scaling, and prioritise smallholder accessibility. Low-cost mobile interfaces, subsidised onboarding, and digital-literacy support should accompany any rollout, ensuring that traceability benefits are not captured exclusively by large-scale producers.

Consistent with the source dissertation's own recommendation, integrating blockchain with complementary innovations such as the Internet of Things (for automated, tamper-resistant data capture) and artificial intelligence (for anomaly detection across the resulting event streams) is expected to substantially enhance the effectiveness of blockchain-based traceability systems in the coming years.

11. Conclusion

This paper set out to evaluate, analyse, and empirically test the application of blockchain technology for supply-chain traceability and transparency in the agriculture industry. Drawing on a structured review of more than sixty literature and industry sources, it consolidated six evidence-based findings (F1-F6) confirming that blockchain's immutable, event-driven ledger design measurably improves traceability, enables faster and more targeted product recalls, and is associated with rising consumer trust and rapid market growth (a projected 48.1% CAGR between 2021 and 2028). The paper proposed a three-layer system architecture and an Ethereum smart contract (AgriSupplyChain.sol) operationalising farmer-to-distributor-to-retailer-to-consumer traceability, and — extending beyond the source dissertation's narrative analysis — conducted an original, reproducible verification experiment demonstrating that the contract's access-control

logic achieves perfect Precision, Recall, and F1-score (1.00) across three test batches (F1, F2, F3) totalling 1,700 simulated transactions under adversarial rates of 20-50%.

At the same time, the evidence is clear that technological complexity, scalability, standardisation, privacy, security, and energy consumption remain real and unresolved barriers to widespread adoption, particularly among smallholder farmers with limited digital infrastructure and technical support. Blockchain is best understood not as a stand-alone solution but as a trust-infrastructure layer that must be paired with reliable off-chain data capture — IoT sensors, certification bodies, and, increasingly, AI-based anomaly detection — to deliver its full traceability and transparency potential. Future work should extend the verification methodology introduced in Section 7 to a live testnet deployment with gas-cost and throughput benchmarking, incorporate oracle-based sensor-data verification, and conduct primary field research with farmer cooperatives to complement the secondary-research evidence base synthesised in this paper.

12. References

- [1] Ahmed, W.A. and MacCarthy, B.L. (2021) 'Blockchain-enabled supply chain traceability in the textile and apparel supply chain: a case study of the fibre producer, Lenzing', *Sustainability*, 13(19), p.10496.
- [2] Alabi, M.O. and Ngwenyama, O. (2023) 'Food security and disruptions of the global food supply chains during COVID-19: building smarter food supply chains for post COVID-19 era', *British Food Journal*, 125(1), pp.167-185.
- [3] Alazab, M., Alhyari, S., Awajan, A. and Abdallah, A.B. (2021) 'Blockchain technology in supply chain management: an empirical study of the factors affecting user adoption/acceptance', *Cluster Computing*, 24, pp.83-101.
- [4] AlShamsi, M., Al-Emran, M. and Shaalan, K. (2022) 'A systematic review on blockchain adoption', *Applied Sciences*, 12(9), p.4245.
- [5] Bhatia, M.S., Chaudhuri, A., Keiki, Y. and Treblier, H. (2023) 'Implementation of blockchain-enabled supply chain finance solutions in the agricultural commodity supply chain: a transaction cost economics perspective', *Production Planning & Control*, pp.1-15.
- [6] Bischoff, O. and Seuring, S. (2021) 'Opportunities and limitations of public blockchain-based supply chain traceability', *Modern Supply Chain Research and Applications*, 3(3), pp.226-243.
- [7] Borges, C.E., Kapassa, E., Touloupou, M., Legarda Macon, J. and Casado-Mansilla, D. (2022) 'Blockchain application in P2P energy markets: Social and legal aspects', *Connection Science*, 34(1), pp.1066-1088.
- [8] Capece, G., Levialdi Ghiron, N. and Pasquale, F. (2020) 'Blockchain technology: Redefining trust for digital certificates', *Sustainability*, 12(21), p.8952.
- [9] Centobelli, P., Cerchione, R., Del Vecchio, P., Oropallo, E. and Secundo, G. (2022) 'Blockchain technology for bridging trust, traceability and transparency in circular supply chain', *Information & Management*, 59(7), p.103508.
- [10] Chandan, A., John, M. and Potdar, V. (2023) 'Achieving UN SDGs in food supply chain using blockchain technology', *Sustainability*, 15(3), p.2109.
- [11] Chen, Y. and Bellavitis, C. (2020) 'Blockchain disruption and decentralized finance: The rise of decentralized business models', *Journal of Business Venturing Insights*, 13, p.e00151.
- [12] Dasaklis, T.K., Voutsinas, T.G., Tsoulfas, G.T. and Casino, F. (2022) 'A systematic literature review of blockchain-enabled supply chain traceability implementations', *Sustainability*, 14(4), p.2439.
- [13] Dietrich, F., Louw, L. and Palm, D. (2023) 'Blockchain-based traceability architecture for mapping object-related supply chain events', *Sensors*, 23(3), p.1410.
- [14] Dutta, P., Choi, T.M., Somani, S. and Butala, R. (2020) 'Blockchain technology in supply chain operations: Applications, challenges and research opportunities', *Transportation Research Part E: Logistics and Transportation Review*, 142, p.102067.
- [15] Feng, H., Wang, X., Duan, Y., Zhang, J. and Zhang, X. (2020) 'Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges', *Journal of Cleaner Production*, 260, p.121031.
- [16] Ferrag, M.A., Shu, L., Yang, X., Derhab, A. and Maglaras, L. (2020) 'Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges', *IEEE Access*, 8, pp.32031-32053.

- [17] Hastig, G.M. and Sodhi, M.S. (2020) 'Blockchain for supply chain traceability: Business requirements and critical success factors', *Production and Operations Management*, 29(4), pp.935-954.
- [18] Jacobsen, K.H. (2020) *Introduction to Health Research Methods: A Practical Guide*. Burlington, MA: Jones & Bartlett Publishers.
- [19] Kamble, N.N., Mali, S.M. and Patil, C.H. (2022) 'Use of blockchain technology in agriculture domain', in *ICT Analysis and Applications*. Singapore: Springer, pp.877-884.
- [20] Kamilaris, A., Fonts, A. and Prenafeta-Boldu, F.X. (2019) 'The rise of blockchain technology in agriculture and food supply chains', *Trends in Food Science & Technology*, 91, pp.640-652.
- [21] Kaur, G. and Gandhi, C. (2020) 'Scalability in blockchain: Challenges and solutions', in *Handbook of Research on Blockchain Technology*. Cambridge, MA: Academic Press, pp.373-406.
- [22] Khan, S.A., Mubarik, M.S., Kusi-Sarpong, S., Gupta, H., Zaman, S.I. and Mubarik, M. (2022) 'Blockchain technologies as enablers of supply chain mapping for sustainable supply chains', *Business Strategy and the Environment*, 31(8), pp.3742-3756.
- [23] Kraft, S.K. and Kellner, F. (2022) 'Can blockchain be a basis to ensure transparency in an agricultural supply chain?', *Sustainability*, 14(13), p.8044.
- [24] Kshetri, N. (2021) 'Blockchain and sustainable supply chain management in developing countries', *International Journal of Information Management*, 60, p.102376.
- [25] Le, J.K. and Schmid, T. (2022) 'The practice of innovating research methods', *Organizational Research Methods*, 25(2), pp.308-336.
- [26] Leavy, P. (2022) *Research Design: Quantitative, Qualitative, Mixed Methods, Arts-Based, and Community-Based Participatory Research Approaches*. New York: Guilford Publications.
- [27] Longo, F., Nicoletti, L., Padovano, A., d'Atri, G. and Forte, M. (2019) 'Blockchain-enabled supply chain: An experimental study', *Computers & Industrial Engineering*, 136, pp.57-69.
- [28] Mirabelli, G. and Solina, V. (2020) 'Blockchain and agricultural supply chains traceability: Research trends and future challenges', *Procedia Manufacturing*, 42, pp.414-421.
- [29] Mishra, S.B. and Alok, S. (2022) *Handbook of Research Methodology*. New Delhi: Educreation Publishing.
- [30] Mohan, A., Krishnan, R., Arshinder, K., Vandore, J. and Ramanathan, U. (2023) 'Management of postharvest losses and wastages in the Indian tomato supply chain - a temperature-controlled storage perspective', *Sustainability*, 15(2), p.1331.
- [31] Newman, M. and Gough, D. (2020) 'Systematic reviews in educational research: Methodology, perspectives and application', in *Systematic Reviews in Educational Research*. Wiesbaden: Springer VS, pp.3-22.
- [32] Panda, S.K. and Satapathy, S.C. (2021) 'Drug traceability and transparency in medical supply chain using blockchain for easing the process and creating trust between stakeholders and consumers', *Personal and Ubiquitous Computing*, pp.1-17.
- [33] Pothula, S.R. (2023) 'Investigations of agri-blockchain technology framework in agriculture', *Journal of Agriculture, Science and Technology*, 22(1), pp.4-15.
- [34] Rogerson, M. and Parry, G.C. (2020) 'Blockchain: case studies in food supply chain visibility', *Supply Chain Management: An International Journal*, 25(5), pp.601-614.
- [35] Sajja, G.S., Rane, K.P., Phasinam, K., Kassanuk, T., Okoronkwo, E. and Prabhu, P. (2023) 'Towards applicability of blockchain in agriculture sector', *Materials Today: Proceedings*, 80, pp.3705-3708.
- [36] Salah, K., Nizamuddin, N., Jayaraman, R. and Omar, M. (2019) 'Blockchain-based soybean traceability in agricultural supply chain', *IEEE Access*, 7, pp.73295-73305.
- [37] Sedlmeir, J., Buhl, H.U., Fridgen, G. and Keller, R. (2021) 'Recent developments in blockchain technology and their impact on energy consumption', *arXiv preprint arXiv:2102.07886*.
- [38] Song, L., Luo, Y., Chang, Z., Jin, C. and Nicolas, M. (2022) 'Blockchain adoption in agricultural supply chain for better sustainability: A game theory perspective', *Sustainability*, 14(3), p.1470.

- [39] Yang, X., Li, M., Yu, H., Wang, M., Xu, D. and Sun, C. (2021) 'A trusted blockchain-based traceability system for fruit and vegetable agricultural products', IEEE Access, 9, pp.36282-36293.
- [40] Meena, R.K. (2026) Exploring the Application of Blockchain Technology for Supply Chain Traceability and Transparency in the Agriculture Industry. M.Tech. Dissertation. Compucom Institute of Technology & Management, Jaipur, affiliated to Rajasthan Technical University, Kota.