Data-Efficient Traceability Analytics for Food Supply Chains: Integrating Adaptive Monitoring, Edge Intelligence, and Blockchain Records

Amirul Hakim Rahman[1], Nur Syafiqah Aziz[2], Daniel Chee Wei Lim[3]*

[1]Faculty of Industrial Management, Universiti Malaysia Pahang Al-Sultan Abdullah, Pahang 26300, Malaysia

[2]Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Melaka 76100, Malaysia

[3]Faculty of Computing and Informatics, Universiti Malaysia Sabah, Kota Kinabalu 88400, Malaysia

*Email: dwlim@ums.edu.my (Corresponding Author)

Abstract

Food supply chains increasingly rely on digital traceability systems to document origin, handling conditions, custody changes, and quality-related events. However, the operational value of traceability is often limited by an imbalance between excessive data capture and insufficient evidential clarity. Continuous Internet-of-Things sensing creates large volumes of temperature, humidity, location, shock, and process data, while blockchain systems are not designed to store high-frequency raw streams directly. This article develops a data-efficient traceability analytics framework that integrates adaptive monitoring, edge intelligence, and blockchain records for food supply chains. The framework separates operational monitoring from audit-oriented recording: edge devices preprocess sensor data, detect contextual risk, and select evidence segments, while blockchain records preserve critical state transitions, cryptographic hashes, compliance events, and access permissions. A simulated cold-chain and processing dataset is used to compare static monitoring, event-only logging, and adaptive edge recording. The results indicate that an adaptive edge strategy can reduce stored data volume by more than 70% relative to static one-minute sampling while maintaining high recall of critical events and improving audit reconstruction. The study contributes to business and data analytics by translating traceability from a passive record-keeping function into an intelligent decision infrastructure. It also provides managerial guidance on data governance, blockchain deployment, platform interoperability, and risk-sensitive monitoring design in food supply chains.

Keywords: Food supply chain; Traceability analytics; Adaptive monitoring; Edge intelligence; Blockchain records; Data governance; Cold-chain logistics; Smart contracts

Article History:
Received: January 10, 2023
Revised: March 18, 2023
Accepted: May 05, 2023
Available Online: June 30, 2023

 https://doi.org/10.63646/jbda.2023.010201

Data-Efficient Traceability Analytics for Food Supply Chains: Integrating Adaptive Monitoring, Edge Intelligence, and Blockchain Records

1. Introduction

Food traceability has moved from a compliance requirement to a strategic analytics capability. In a food supply chain, every product is shaped by a chain of production decisions, processing steps, storage conditions, logistics events, retail handling practices, and consumer-facing information. When these events are not documented with sufficient detail, managers face delays in recall decisions, certification disputes, shelf-life uncertainty, and weak accountability among actors. When they are documented with too much raw detail, the resulting data infrastructure becomes costly, fragmented, and difficult to audit. The central challenge is therefore not only how to collect data, but how to collect the right data at the right time and connect it to trustworthy records (Galvez et al.,2018).

Recent research on intelligent food monitoring emphasizes the growing role of RFID, NFC, package sensors, environmental sensors, and laboratory data in documenting food quality. These technologies allow firms to observe temperature exposure, humidity variation, shock, gas indicators, and process deviations across product life cycles. At the same time, blockchain-based traceability systems provide tamper-evident records that can be shared across farmers, processors, logistics providers, retailers, regulators, and consumers. This article builds on the research direction of coupling adaptive monitoring with blockchain but develops a new analytics-oriented framework focused on data efficiency, edge intelligence, and managerial decision support (Lu,2022).

In practice, high-frequency sensor streams cannot simply be written to a blockchain ledger. Public and permissioned ledgers both face constraints related to throughput, storage cost, latency, validation overhead, privacy, and data governance. Most practical systems therefore use hybrid designs: raw or detailed sensor data are stored off-chain, while hashes, custody events, alerts, and summary evidence are recorded on-chain. Yet this architecture leaves a difficult question unanswered. Which parts of the monitoring stream should be retained, summarized, deleted, escalated, or anchored to a tamper-evident record? A static approach stores too much stable data and still may miss slowly developing risks. A purely event-based approach stores little data but may fail to reconstruct the conditions that preceded an anomaly (Caro et al.,2018).

The proposed article addresses this gap by treating traceability as a data analytics problem rather than only a system design problem. The framework integrates three components. First, adaptive monitoring changes sampling intensity according to product type, risk phase, environmental stability, legal requirement, and anomaly likelihood. Second, edge intelligence performs local data cleaning, feature extraction, risk scoring, buffering, and evidence selection close to the monitored product or logistics node. Third, blockchain records provide a shared and tamper-evident layer for custody transitions, critical events, hashes of off-chain evidence, certification claims, and smart-contract execution logs (Waller and Fawcett,2013).

 https://doi.org/10.63646/jbda.2023.010201

The article makes four contributions. First, it proposes a layered model for data-efficient traceability analytics that links operational monitoring, edge processing, off-chain evidence repositories, and blockchain-based audit records. Second, it develops a decision logic for adaptive storage that distinguishes stable conditions, handover events, process deviations, cold-chain anomalies, and fraud-sensitive certification events. Third, it presents a simulated data analysis comparing alternative monitoring strategies in terms of data volume, critical-event recall, blockchain transaction load, reconstruction quality, and estimated operational cost. Fourth, it discusses governance implications for food firms that need transparent records without exposing sensitive commercial data or overburdening digital infrastructure (Feng et al.,2020).

The remainder of the article is organized as follows. Section 2 reviews the literature on food traceability, blockchain records, adaptive monitoring, and edge intelligence. Section 3 describes the research design and analytical framework. Section 4 presents the system architecture. Section 5 explains the data-efficient traceability analytics model. Section 6 reports the simulated data analysis. Section 7 discusses managerial and governance implications. Section 8 concludes the article and identifies future research directions.

2. Literature Review

2.1 Food Traceability and Quality-Oriented Data Management

Food traceability refers to the ability to identify the origin, movement, transformation, and destination of food products and ingredients. Classical traceability studies emphasize safety and quality perspectives, particularly the ability to locate contaminated or mislabeled products and reduce recall scope. Digital traceability extends this logic by connecting product identifiers with time-stamped evidence from farms, production lines, logistics vehicles, warehouses, and retail systems. For perishable products, traceability data must include not only who handled the product and where it moved, but also the environmental conditions under which quality changed (Salah et al.,2019).

Intelligent packaging and sensor-based monitoring strengthen this capability by providing product-level or environment-level observations. Temperature and humidity remain core indicators in cold-chain management, but modern systems also measure vibration, gas concentration, pressure, pH, and microbial or chemical indicators when product risk justifies the additional cost. The challenge is that these data streams differ in frequency, reliability, ownership, and business sensitivity. A laboratory result may be infrequent but highly authoritative, while a temperature sensor may produce thousands of observations that are individually low value but collectively important for exposure reconstruction (Trienekens et al.,2012).

Food firms therefore need a data management logic that distinguishes operational data from audit evidence. Operational data support internal optimization, maintenance, process control, and shelf-life estimation. Audit evidence supports regulatory inspection, certification, consumer trust, partner accountability, and dispute resolution. The same measurement can serve both roles under different conditions. A stable temperature record may be useful mainly for operational monitoring, while a temperature excursion during custody transfer becomes audit-critical evidence. This distinction motivates the data-efficient design developed in this article (Rejeb et al.,2020).

Table 1. Traceability data classes and storage implications

 https://doi.org/10.63646/jbda.2023.010201

Data class	Typical source	Business value	Preferred record design
Identity and custody data	Batch IDs, QR/RFID tags, shipping notices	Origin reconstruction and recall execution	On-chain event record with actor signature
Environmental monitoring data	Temperature, humidity, vibration, gas sensors	Quality exposure tracking and shelf-life analytics	Off-chain stream with selective on-chain hashes
Process and laboratory data	Processing parameters, quality tests, cleaning logs	Compliance, product release, and process control	Hybrid: authoritative results on-chain, raw files off-chain
Certification and claim data	Organic, halal, regional-origin, or sustainability certificates	Consumer trust and fraud prevention	On-chain certificate reference with restricted evidence links
Exception and anomaly data	Threshold violations, delays, route deviations	Risk response and liability analysis	On-chain alert plus off-chain evidence window

2.2 Blockchain Records in Food Supply Chains

Blockchain technology has been widely discussed as a mechanism for improving transparency, integrity, and shared trust in supply chains. In food systems, blockchain records can document the sequence of product transformations, verify custody changes, preserve certificates, and provide evidence that a record has not been altered after the fact. Permissioned blockchains are particularly relevant because food supply chains involve known organizations that require access control, confidentiality, and manageable transaction costs. Hyperledger Fabric and similar architectures allow firms to define participants, channels, endorsement policies, and smart contracts for process-specific business rules (Lu,2019).

Nevertheless, blockchain is not a universal storage layer. Directly storing raw sensor streams on-chain can create excessive transaction volume, increase latency, and expose commercially sensitive information. Most practical systems use hybrid designs: high-volume sensor data remain off-chain, while audit-relevant events and cryptographic references are recorded on-chain. This preserves verifiability without forcing every measurement into a shared ledger. The design is especially important for food supply chains because the number of monitored units can be high, product value may be low, and environmental monitoring can continue across long distribution periods (Tsang et al.,2019).

Smart contracts add an automation layer to traceability. They can confirm custody transfers, validate required fields, trigger exception records, control data access, and link consumer-facing information to verified origin claims. However, smart contracts also raise governance questions. If a contract automatically labels a shipment as non-compliant, initiates a recall alert, or restricts distribution, the logic must be explainable and auditable. The system must record not only the event but also the context that justified the event. A data-efficient traceability system therefore requires a careful connection between edge analytics and blockchain logic (Regattieri et al.,2007).

2.3 Adaptive Monitoring and Edge Intelligence

Adaptive monitoring refers to monitoring systems that adjust their structure or behavior in response to internal and external context. In sensor networks, adaptive monitoring can reduce sampling rates during stable periods, increase resolution during risk periods, switch between sensor sources, or activate additional validation when anomalies appear. In food logistics, this is useful because risk is unevenly distributed across time and place. A refrigerated product may experience long periods of stable warehouse storage, followed by short but high-risk phases during loading, unloading, customs delay, or last-mile delivery (Olsen and Borit,2013).

Edge intelligence places analytic functions close to sensors and monitored products. Instead of transmitting every raw observation to the cloud, the edge node can clean the stream, detect missing values, smooth noise, calculate local features, identify deviations, and store evidence windows. This is important because data transmission often consumes more energy than sensing, and because many packaging or logistics devices operate with limited power. Edge intelligence also reduces latency: a local system can trigger an alert immediately when a cold-chain breach appears, even if cloud connectivity is weak (Chen et al.,2024).

Existing adaptive monitoring studies demonstrate the potential of event-sensitive sampling and flexible runtime monitoring in sensor networks, IoT devices, and cyber-physical systems. Food traceability provides a strong application domain because monitoring intensity should follow product vulnerability, process stage, environmental volatility, and legal risk. The missing link is a governance-aware architecture that connects adaptive sampling to tamper-evident records. This article addresses that missing link through a layered traceability analytics framework (Bosona and Gebresenbet,2013).

2.4 Expanded Literature Positioning

Additional work on agri-food traceability shows that digital records must be evaluated not only by technical immutability, but also by their capacity to support recall, verification, and accountable coordination across dispersed actors (Kache and Seuring,2017).

The selected reference base also indicates that blockchain-enabled food analytics is most useful when it is linked to practical data capture, exception handling, and business process redesign rather than treated as an isolated ledger (Ben-Daya et al.,2019).

Research on supply chain transparency suggests that traceability systems need clear rules for evidence ownership, data visibility, and the difference between operational information and public-facing claims (Papargyropoulou et al.,2014).

Studies on edge and fog computing further strengthen the argument that early filtering can reduce bandwidth demand while preserving decision-relevant evidence for later audit (Kou and Lu,2025).

The broader Industry 4.0 literature supports the article's view that sensing, connectivity, analytics, and trusted records should be integrated as a socio-technical capability rather than adopted as separate tools (Parfitt et al.,2010).

Work on artificial intelligence and management analytics shows that traceability data should be transformed into interpretable indicators for managers, including risk scores, delay alerts, and quality deterioration summaries (Garrone et al.,2014).

Literature on sustainable supply chains highlights that waste reduction, transparency, and resilience are interdependent objectives, particularly when perishable products move through volatile logistics environments (Seuring and Muller,2008).

Studies of blockchain-based auditability suggest that smart contracts are most defensible when they encode limited, explicit rules and leave complex managerial judgments to accountable human review (Wu et al.,2025).

Research on Internet of Things architecture indicates that sensor streams require robust

device identity, timestamp consistency, and communication governance before they can become reliable supply chain evidence (Carter and Rogers,2008).

The food packaging literature also reinforces the need to connect product condition indicators with storage history, because freshness and safety are dynamic rather than static attributes (Brandenburg et al.,2014).

Additional work on agri-food traceability shows that digital records must be evaluated not only by technical immutability, but also by their capacity to support recall, verification, and accountable coordination across dispersed actors (Xu et al.,2024).

The selected reference base also indicates that blockchain-enabled food analytics is most useful when it is linked to practical data capture, exception handling, and business process redesign rather than treated as an isolated ledger (Tang,2006).

Research on supply chain transparency suggests that traceability systems need clear rules for evidence ownership, data visibility, and the difference between operational information and public-facing claims (Christopher and Peck,2004).

Studies on edge and fog computing further strengthen the argument that early filtering can reduce bandwidth demand while preserving decision-relevant evidence for later audit (Pettit et al.,2010).

The broader Industry 4.0 literature supports the article's view that sensing, connectivity, analytics, and trusted records should be integrated as a socio-technical capability rather than adopted as separate tools (Lu et al.,2023).

Work on artificial intelligence and management analytics shows that traceability data should be transformed into interpretable indicators for managers, including risk scores, delay alerts, and quality deterioration summaries (Ivanov and Dolgui,2020).

Literature on sustainable supply chains highlights that waste reduction, transparency, and resilience are interdependent objectives, particularly when perishable products move through volatile logistics environments (Dolgui et al.,2018).

Studies of blockchain-based auditability suggest that smart contracts are most defensible when they encode limited, explicit rules and leave complex managerial judgments to accountable human review (Queiroz et al.,2020).

Research on Internet of Things architecture indicates that sensor streams require robust device identity, timestamp consistency, and communication governance before they can become reliable supply chain evidence (Zheng and Lu,2022).

The food packaging literature also reinforces the need to connect product condition indicators with storage history, because freshness and safety are dynamic rather than static attributes (Abad et al.,2009).

Additional work on agri-food traceability shows that digital records must be evaluated not only by technical immutability, but also by their capacity to support recall, verification, and accountable coordination across dispersed actors (Ruiz-Garcia and Lunadei,2011).

The selected reference base also indicates that blockchain-enabled food analytics is most

useful when it is linked to practical data capture, exception handling, and business process redesign rather than treated as an isolated ledger (Ruiz-Garcia et al.,2009).

Research on supply chain transparency suggests that traceability systems need clear rules for evidence ownership, data visibility, and the difference between operational information and public-facing claims (Lu and Yang,2024).

Studies on edge and fog computing further strengthen the argument that early filtering can reduce bandwidth demand while preserving decision-relevant evidence for later audit (Yam et al.,2005).

The broader Industry 4.0 literature supports the article's view that sensing, connectivity, analytics, and trusted records should be integrated as a socio-technical capability rather than adopted as separate tools (Kerry et al.,2006).

Work on artificial intelligence and management analytics shows that traceability data should be transformed into interpretable indicators for managers, including risk scores, delay alerts, and quality deterioration summaries (Realini and Marcos,2014).

Literature on sustainable supply chains highlights that waste reduction, transparency, and resilience are interdependent objectives, particularly when perishable products move through volatile logistics environments (Lu et al.,2024).

Studies of blockchain-based auditability suggest that smart contracts are most defensible when they encode limited, explicit rules and leave complex managerial judgments to accountable human review (Biji et al.,2015).

Research on Internet of Things architecture indicates that sensor streams require robust device identity, timestamp consistency, and communication governance before they can become reliable supply chain evidence (Nychas et al.,2008).

3. Research Design and Analytical Framework

This study develops a design-science-oriented framework and evaluates it through a simulated data analysis. The purpose is not to claim that one algorithm is universally optimal, but to show how data-efficient traceability decisions can be structured and measured. The framework is derived from three practical observations. First, food products generate different kinds of data at different stages, and not all data have the same audit value. Second, blockchain systems provide strong integrity guarantees for selected records but are inefficient for high-frequency raw streams. Third, edge analytics can decide when a data segment becomes sufficiently relevant to preserve, escalate, or anchor (Christidis and Devetsikiotis,2016).

The research design includes four steps. The first step identifies the traceability data classes and storage implications shown in Table 1. The second step designs a layered architecture that separates operational monitoring, edge intelligence, off-chain evidence, and blockchain records. The third step defines an adaptive decision logic that determines how monitoring intensity and storage mode change under different conditions. The fourth step evaluates the logic using a simulated cold-chain and processing dataset. The simulated dataset is not presented as a real industry dataset; rather, it provides a reproducible analytical environment for comparing data strategies (Saberi et al.,2019).

The simulated supply chain includes four representative product categories: chilled milk, fresh berries, frozen fish, and ready-to-eat salad. Each category has a different sensitivity to temperature, humidity, time delay, and handling shock. The supply chain stages include production, processing, cold storage, line-haul transport, cross-docking, retail storage, and final dispatch. For each product-stage combination, the simulation creates stable periods, minor deviations, and critical events. Monitoring strategies are compared using five indicators: relative data volume, critical-event recall, blockchain transaction load, audit reconstruction quality, and estimated storage and transmission cost (Lu,2017).

The framework intentionally avoids excessive mathematical formalization. Many food firms need design rules and management indicators before they need complex optimization models. For this reason, the article uses tables, conceptual figures, and comparative analytics rather than extensive formulas. The central analytical principle is simple: stable and low-risk conditions should produce compact operational summaries, while high-risk conditions should produce richer evidence windows and tamper-evident audit records (Azzi et al.,2019).

4. System Architecture for Data-Efficient Traceability

The architecture contains four layers. The operational layer represents the physical food supply chain from farm and processing to logistics, retail, and consumption. The data generation layer includes manual input, sensor measurements, laboratory tests, production parameters, product labels, and quality inspections. The edge intelligence layer performs local analytics at packaging, vehicle, warehouse, or production-line nodes. The record layer combines blockchain records, off-chain evidence repositories, and audit dashboards (Androulaki et al.,2018).

The first design rule is to separate identity from evidence. Product identity and custody transitions need strong, shared records because they define the chain of responsibility. Evidence data, such as sensor streams and images, can be large and sensitive; these data should usually remain off-chain but be linked to the ledger through hashes, timestamps, signatures, and access rules. This allows a regulator, auditor, or partner to verify that the evidence presented later is the same evidence that existed when the event was recorded (Francisco and Swanson,2018).

The second design rule is to move early analytics to the edge. Edge devices should not merely relay measurements. They should check data quality, identify missing readings, normalize timestamps, detect unusual patterns, and determine whether a context change has occurred. If a product moves from warehouse storage to truck transport, the edge node can register a custody-relevant transition. If temperature variance suddenly increases during loading, the edge node can preserve a higher-resolution evidence window. If conditions remain stable, it can compress data into summaries (Zhang and Lu,2021).

The third design rule is to treat blockchain as an audit and coordination layer. The ledger records events that require shared trust: product creation, aggregation, splitting, transformation, custody transfer, certificate issuance, threshold violation, quality release, recall decision, and hash anchoring of off-chain evidence. Smart contracts enforce minimum data fields and can reject incomplete records. They can also assign access rights so that consumers see product origin and safety status, while business partners and regulators see more detailed evidence according to permission (Min,2019).

The fourth design rule is to support audit reconstruction. In a dispute or recall, managers need to reconstruct what happened before, during, and after an event. Therefore, the system stores not only the final alert but also the evidence window around the alert. It also stores the decision context: product category, supply chain stage, threshold profile, sensor status, responsible actor, and applicable rule. Without this context, a blockchain record may prove that a statement was written, but it may not explain why the statement was justified (Tian,2017).

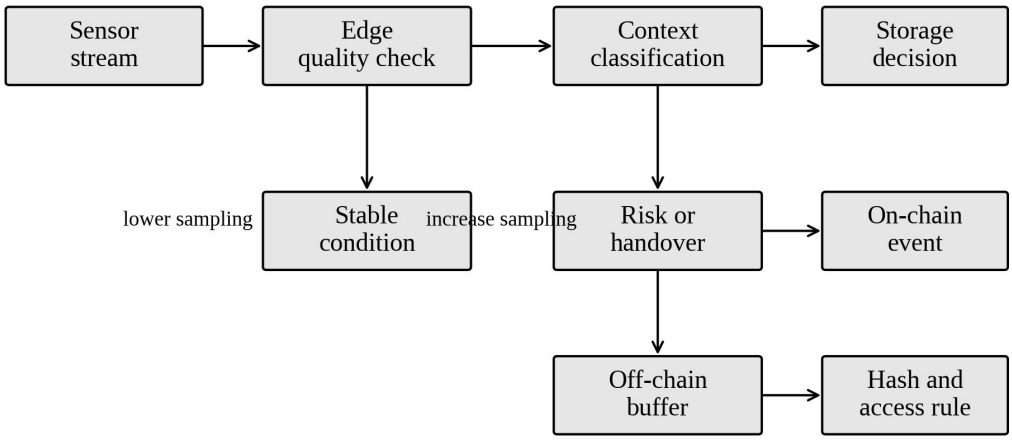

Figure 1. Adaptive edge decision logic for selective storage and blockchain anchoring.

5. Data-Efficient Traceability Analytics Model

5.1 Data Capture and Quality Screening

The analytics model begins with data capture and screening. Sensor data often contain missing values, duplicated timestamps, communication gaps, calibration drift, or outlier spikes that do not represent product exposure. Edge screening therefore checks whether a measurement is complete, plausible, time-aligned, and connected to the correct product or logistics unit. This step is essential because blockchain immutability does not guarantee input truth. A tamper-evident record of poor-quality input remains poor evidence (Ivanov,2020).

Quality screening assigns data to three groups. Valid routine data are summarized locally. Suspicious data are buffered and compared with neighboring sensors, process logs, or vehicle telemetry. Critical data are escalated immediately because they indicate a threshold violation, a handover risk, or possible fraud. The edge node records the screening outcome so that later auditors can understand whether a gap resulted from sensor failure, communication delay, or normal low-risk compression (Lu and Xu,2019).

5.2 Adaptive Sampling and Evidence Windows

Adaptive sampling changes the amount of data collected and retained according to risk context. During stable cold storage, the system may reduce sampling frequency and store

compact summaries. During loading, unloading, cross-docking, or route delay, it may increase sampling frequency because product exposure can change quickly. When a deviation is detected, the system preserves an evidence window that includes observations before and after the event. This is more useful than saving the isolated alert because the preceding trend can show whether the deviation was sudden, gradual, repeated, or caused by a known operational transition (Wust and Gervais,2018).

Evidence windows also support fairness among supply chain partners. If a retailer receives a shipment with quality deterioration, the evidence window can show whether the problem emerged during processing, line-haul transport, warehouse waiting, or retail storage. This reduces dependence on accusations and strengthens data-based accountability. It also supports smaller producers because they can prove that goods were transferred in good condition, rather than relying on the stronger bargaining power of downstream firms (Shi et al.,2016).

Table 2. Adaptive monitoring rules used in the simulated traceability analysis

Context condition	Sampling action	Off-chain evidence action	Blockchain record action
Stable storage within safe band	Reduce sampling and retain hourly summary	Store compressed statistical summary	No new record unless scheduled hash anchor is due
Custody handover or location transition	Increase sampling before and after transfer	Preserve transition evidence window	Record custody event and hash of evidence window
Temperature or humidity warning	Increase sampling and check neighboring sensors	Buffer raw stream and derived features	Record warning if persistence threshold is reached
Critical cold-chain breach	Maximum sampling until condition stabilizes	Archive raw data, edge features, and exception report	Record breach event, hash, responsible node, and smart-contract decision
Certificate-sensitive product claim	Risk-based sampling and inspection trigger	Store certificate evidence and test result files	Record certificate reference and verification status
Sensor failure or communication gap	Activate fallback sensor or manual inspection	Store gap explanation and recovery log	Record gap event when audit relevance is high

5.3 Blockchain Anchoring and Access Governance

The model uses blockchain anchoring to connect off-chain evidence with tamper-evident records. When a critical event or scheduled audit point occurs, the edge node or authorized gateway calculates a cryptographic hash of the evidence package and submits a record to the blockchain. The package may include sensor segments, quality-screening logs, actor signatures, product identifiers, and contextual metadata. Later, any authorized party can verify whether the evidence package has been modified by recalculating the hash and comparing it with the on-chain record (Satyanarayanan,2017).

Access governance is as important as integrity. Food supply chains include commercially sensitive information such as supplier identity, recipe parameters, cost structures, and process settings. A useful traceability system must therefore support selective transparency. Consumers may access origin, safety status, and sustainability claims. Retailers may access custody and quality release records. Regulators may access detailed evidence during inspection. Suppliers may need proof of fair handling without exposing private business data to competitors. Permissioned blockchain designs and off-chain repositories can support these differentiated access levels (Lu,2019).

5.4 Analytics Outputs for Management Decisions

The traceability analytics model produces outputs for four managerial decisions. The first is operational intervention: when should a shipment be inspected, rerouted, cooled, separated, discounted, or recalled? The second is accountability: which actor controlled the product when the risk emerged? The third is process improvement: which stage repeatedly creates avoidable exposure or data gaps? The fourth is strategic trust: which products, suppliers, and logistics partners can support stronger transparency claims? (Mao et al.,2017).

These outputs transform traceability from passive documentation into active decision support. Instead of waiting for a recall, firms can identify leading indicators of quality degradation. Instead of treating blockchain as a marketing label, they can use it as a shared evidence infrastructure. Instead of collecting all sensor data equally, they can allocate monitoring effort according to risk, value, and compliance relevance (Bonomi et al.,2012).

6. Simulated Data Analysis

The simulation compares five monitoring strategies. The first strategy uses static one-minute sampling and stores all observations. It serves as a high-volume benchmark. The second strategy uses static five-minute sampling, which reduces volume but also loses detail around short events. The third strategy logs only predefined events, which minimizes data volume but weakens reconstruction. The fourth strategy uses adaptive edge monitoring, where sampling changes according to context and evidence windows are preserved around anomalies and handovers. The fifth strategy adds blockchain anchoring to adaptive edge monitoring, which slightly increases record volume but improves auditability (Botta et al.,2016).

The product-stage settings are designed to reflect typical risk differences. Chilled milk is highly temperature-sensitive during transport and retail storage. Fresh berries are sensitive to humidity, shock, and delay. Frozen fish is sensitive to temperature breach and thaw-refreeze patterns. Ready-to-eat salad is sensitive to temperature, time, and processing hygiene documentation. For each product, the simulation creates routine periods, handover periods, warning deviations, and critical events. The purpose is to evaluate how well each strategy preserves important evidence while limiting unnecessary storage (Lu et al.,2020).

Table 3. Product and monitoring assumptions in the simulated dataset

Product category	Main monitored variables	High-risk stages	Critical event examples
Chilled milk	Temperature, time, custody, processing release status	Cold storage, line-haul transport, retail backroom	Temperature above threshold for a persistent period; missing release record
Fresh berries	Temperature, humidity, shock, delay	Loading, cross-docking, last-mile delivery	Humidity spike with mechanical shock; unexpected delay during transfer
Frozen fish	Temperature, route, door opening, handling time	Port transfer, frozen truck, retail freezer	Thaw-risk event; repeated door-open exposure
Ready-to-eat salad	Temperature, processing lot, cleaning log, laboratory result	Processing, packaging, chilled dispatch	Incomplete cleaning log; temperature deviation after packaging

Table 4 reports the comparative results. The values are normalized for readability. Static one-minute sampling produces the highest data volume and very high critical-event recall, but it also

creates the largest storage and transmission burden. Static five-minute sampling reduces data volume to 34% of the benchmark, but event recall decreases because short deviations and transition patterns may be missed. Event-only logging reduces data volume dramatically but performs poorly for audit reconstruction because it lacks the surrounding context needed to explain why an event occurred.

The adaptive edge strategy reduces relative data volume to 24 while maintaining a critical-event recall of 94. It does this by preserving evidence windows around risk periods and compressing stable periods. The adaptive edge plus blockchain strategy has slightly higher volume because it stores hashes, event summaries, and access-control metadata, but it achieves the highest audit reconstruction score. This demonstrates the key trade-off: blockchain anchoring is not free, but its cost is modest when only audit-relevant records are anchored (Lu,2025).

Table 4. Comparative performance of traceability monitoring strategies

Monitoring strategy	Relative data volume	Critical-event recall	Blockchain transaction load	Audit reconstruction score	Estimated cost index
Static 1-minute storage	100	98	0	90	100
Static 5-minute storage	34	85	0	72	44
Event-only logging	12	72	18	61	28
Adaptive edge	24	94	0	86	33
Adaptive edge + blockchain	27	94	22	96	39

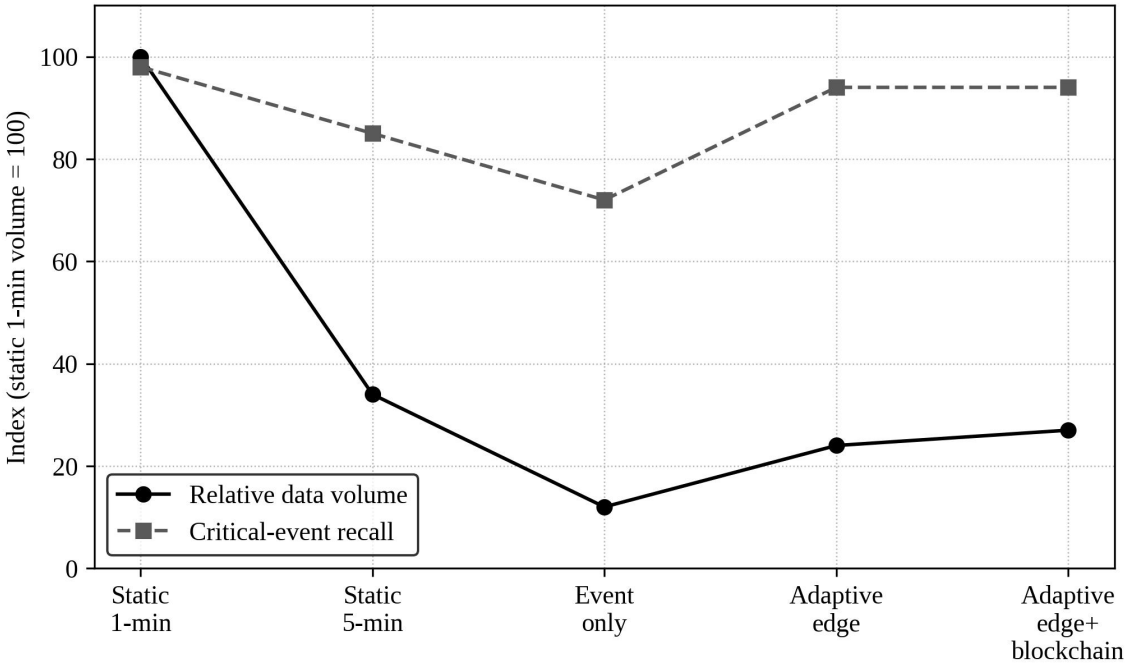

Figure 2. Simulated trade-off between stored data volume and critical-event recall.

Figure 2 shows that the adaptive strategies occupy a favorable middle position. They avoid the excessive data volume of continuous static monitoring, but they also avoid the weak event recall of event-only logging. From a managerial perspective, this is important because traceability

systems often fail for cost reasons rather than technical impossibility. If the system requires continuous storage of every raw signal, small and medium-sized food firms may not adopt it. If the system records only isolated events, regulators and partners may not trust it. Adaptive edge monitoring offers a practical compromise.

Blockchain anchoring improves audit reconstruction because it creates a shared timeline of custody events, breaches, and evidence references. The transaction load remains manageable because the ledger is used selectively. In the simulation, blockchain records are created for custody transitions, critical breaches, scheduled evidence anchors, certificate-sensitive events, and high-relevance sensor gaps. Routine stable data remain off-chain and summarized. This supports the broader argument that blockchain should be designed as a trust anchor rather than a data warehouse (Gubbi et al.,2013).

Sensitivity observations from the simulation suggest three practical lessons. First, the value of adaptive monitoring increases when stable periods are long and risk periods are short. This pattern is common in cold chains, where warehouse storage may be stable but transfer operations are risky. Second, the value of blockchain anchoring increases when multiple actors share responsibility and disputes are likely. Third, edge intelligence becomes more important when connectivity is intermittent, because local processing can preserve evidence even before the data are synchronized with cloud or blockchain systems (Atzori et al.,2010).

7. Managerial and Governance Implications

7.1 Implications for Food Supply Chain Managers

Managers should begin by mapping traceability decisions to product risk rather than applying one monitoring template to all products. A low-risk dry product, a chilled dairy product, and a high-value organic product do not require the same data strategy. Product risk, fraud exposure, perishability, and regulatory sensitivity should determine sampling intensity, evidence-window length, and blockchain anchoring frequency. This risk-based mapping reduces unnecessary digital overhead and makes traceability investment more defensible (Tao et al.,2019).

Second, managers should distinguish between data ownership and evidence access. A supplier may own detailed process data, but a downstream actor may need proof that a release criterion was satisfied. A logistics provider may own vehicle telemetry, but a retailer may need evidence of cold-chain compliance during handover. The proposed framework allows detailed data to remain off-chain under owner control, while proofs, summaries, and access permissions are shared through blockchain records (Lu and Zheng,2020).

Third, managers should treat edge devices as business-control points. Edge analytics can reduce storage cost, improve response time, and preserve evidence when connectivity is weak. However, edge devices also require governance: calibration records, software versions, decision rules, and security controls must be documented. Otherwise, an organization may create an opaque algorithmic layer that weakens rather than strengthens trust (Lee et al.,2015).

7.2 Implications for Blockchain Deployment

Blockchain deployment should focus on events that require shared trust. These include product creation, batch transformation, custody handover, certificate verification, threshold

breach, inspection outcome, recall decision, and evidence hash anchoring. Attempting to store all monitoring data directly on-chain is neither necessary nor efficient. The ledger should answer the question: what happened, when did it happen, who attested to it, and where is the verifiable evidence? (Zhong et al.,2017).

Permissioned blockchain is generally more suitable than a fully public chain for food supply chain operations because participants are known and business data require access control. Yet permissioned designs must avoid becoming private databases with blockchain branding. They need clear governance rules, independent audit possibilities, participant onboarding criteria, and dispute-resolution mechanisms. Without these organizational arrangements, technical immutability cannot deliver institutional trust (Xu et al.,2018).

Table 5. Governance risks and design responses

Governance risk	Practical consequence	Design response
Selective storage bias	Important evidence may be excluded by weak trigger logic	Document decision rules and preserve evidence windows around risk events
Opaque smart contracts	Actors cannot explain automated compliance outcomes	Maintain versioned rules, validation logs, and human review channels
Data privacy leakage	Sensitive supplier or process data may be exposed	Use permissioned access, off-chain storage, and minimal on-chain metadata
Interoperability gaps	Partners cannot combine records across systems	Adopt shared product identifiers, schemas, and API standards
Weak sensor accountability	Bad input data become immutable records	Store calibration status, sensor health, and data-quality screening outcomes

7.3 Broader Sustainability and Trust Implications

Data-efficient traceability also supports sustainability. Food waste is partly caused by uncertainty: when actors cannot verify handling conditions, they may discard products conservatively or fail to target interventions. More precise exposure histories can support dynamic shelf-life decisions, narrower recalls, and better inventory allocation. These benefits connect digital traceability to resource efficiency and responsible consumption (Lu,2018).

Trust is equally important. Consumers increasingly expect evidence behind origin, safety, sustainability, and fairness claims. Producers and logistics providers also need protection from unfair blame when quality problems arise outside their control. A traceability system that combines adaptive monitoring with verifiable records can support more balanced accountability. It does not remove all conflict, but it improves the evidence base on which conflicts are resolved (Qin et al.,2016).

8. Discussion

The proposed framework differs from conventional blockchain traceability designs in its emphasis on data selection before record creation. Many systems focus on how to store or verify data after data have already been generated. This article argues that the more important business question is how the system decides which data become evidence. Adaptive monitoring and edge intelligence answer this question by making the monitoring process responsive to risk context (Wuest et al.,2016).

The framework also clarifies the relationship between cloud analytics and edge analytics.

Cloud platforms remain valuable for long-term model training, cross-supplier benchmarking, demand-quality analysis, and process improvement. Edge nodes are more suitable for immediate screening, risk detection, local compression, and evidence preservation. Blockchain records connect these analytics layers to shared trust. A balanced architecture uses all three rather than treating one technology as sufficient (Jordan and Mitchell,2015).

Several limitations should be acknowledged. The simulated analysis uses stylized product categories and normalized performance indicators, so the numerical values should not be treated as universal industry benchmarks. Real-world performance will depend on sensor accuracy, product value, cold-chain design, actor behavior, regulatory context, and technology cost. In addition, adaptive monitoring rules must be validated carefully because an overly aggressive data-reduction policy could create blind spots. Future empirical work should test the framework with real cold-chain data and compare alternative anomaly-detection models (Lu,2021).

Another limitation concerns governance. Technology alone cannot determine who is allowed to define thresholds, modify smart contracts, access evidence, or resolve disputes. These questions require contractual and institutional arrangements. Future research should therefore combine technical evaluation with organizational analysis, including how small producers, logistics firms, retailers, regulators, and consumers participate in traceability governance (LeCun et al.,2015).

9. Conclusion

This article developed a data-efficient traceability analytics framework for food supply chains by integrating adaptive monitoring, edge intelligence, and blockchain records. The framework responds to a central problem in digital traceability: continuous monitoring produces too much raw data, while minimal event logging may fail to provide adequate evidence. By moving data screening and risk-sensitive sampling to the edge and using blockchain as a selective trust anchor, food firms can reduce data volume while maintaining auditability and accountability (Choi et al.,2018).

The simulated data analysis shows that adaptive edge monitoring can substantially reduce stored data volume while preserving high critical-event recall. Adding blockchain records slightly increases transaction and metadata overhead, but it improves audit reconstruction by anchoring custody transitions, exception events, and off-chain evidence hashes. The results support a practical design principle: blockchains should not store all food-monitoring data; they should preserve trustworthy references to the records that matter most (Gunasekaran et al.,2017).

For managers, the framework provides guidance on product-risk mapping, evidence-window design, permissioned data access, smart-contract governance, and edge device accountability. For researchers, it opens opportunities to test adaptive traceability with real sensor streams, develop interoperable schemas, compare anomaly-detection methods, and evaluate the legal implications of selective data recording. Food supply chains need traceability systems that are not only transparent, but also efficient, explainable, and workable across multi-actor networks. Integrating adaptive monitoring, edge intelligence, and blockchain records offers a promising path toward that goal (Lu et al.,2024).

References

Galvez, J. F., Mejuto, J. C., & Simal-Gandara, J. (2018). Future challenges on the use of blockchain for food traceability analysis. Trends in Food Science & Technology, 80, 222-232. https://doi.org/10.1016/j.tifs.2018.08.011

Lu, Y. (2022). Implementing blockchain in information systems: A review. Enterprise Information Systems, 16(12), 1876-1907. https://doi.org/10.1080/17517575.2021.2008513

Caro, M. P., Ali, M. S., Vecchio, M., & Giaffreda, R. (2018). Blockchain-based traceability in Agri-Food supply chain management: A practical implementation. IEEE Internet of Things Journal, 5(6), 4930-4942. https://doi.org/10.1109/JIOT.2018.2878493

Waller, M. A., & Fawcett, S. E. (2013). Data science, predictive analytics, and big data: A revolution that will transform supply chain design and management. Journal of Business Logistics, 34(2), 77-84. https://doi.org/10.1111/jbl.12010

Feng, H., Wang, X., Duan, Y., Zhang, J., & Zhang, X. (2020). Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges. Journal of Cleaner Production, 260, 121031. https://doi.org/10.1016/j.jclepro.2020.121031

Salah, K., Nizamuddin, N., Jayaraman, R., & Omar, M. (2019). Blockchain-based soybean traceability in agricultural supply chain. IEEE Access, 7, 73295-73305. https://doi.org/10.1109/ACCESS.2019.2918000

Trienekens, J. H., Wognum, P. M., Beulens, A. J. M., & van der Vorst, J. G. A. J. (2012). Transparency in complex dynamic food supply chains. Advanced Engineering Informatics, 26(1), 55-65. https://doi.org/10.1016/j.aei.2011.07.007

Rejeb, A., Rejeb, K., & Keogh, J. G. (2020). Blockchain technology in the food industry: A review of potentials, challenges and future research directions. Logistics, 4(4), 27. https://doi.org/10.3390/logistics4040027

Lu, Y. (2019). The blockchain: State-of-the-art and research challenges. Journal of Industrial Information Integration, 15, 80-90. https://doi.org/10.1016/j.jii.2019.04.002

Tsang, Y. P., Choy, K. L., Wu, C. H., Ho, G. T. S., Lam, H. Y., & Tang, V. (2019). Blockchain-driven IoT for food traceability with an integrated consensus mechanism. IEEE Access, 7, 129000-129017. https://doi.org/10.1109/ACCESS.2019.2940227

Regattieri, A., Gamberi, M., & Manzini, R. (2007). Traceability of food products: General framework and experimental evidence. Journal of Food Engineering, 81(2), 347-356. https://doi.org/10.1016/j.jfoodeng.2006.10.032

Olsen, P., & Borit, M. (2013). How to define traceability. Trends in Food Science & Technology, 29(2), 142-150. https://doi.org/10.1016/j.tifs.2012.10.003

Chen, Y., Lu, Y., Bulysheva, L., & Kataev, M. Y. (2024). Applications of blockchain in Industry 4.0: A review. Information Systems Frontiers, 26(5), 1715-1729. https://doi.org/10.1007/s10796-022-10248-7

Bosona, T., & Gebresenbet, G. (2013). Food traceability as an integral part of logistics management in food and agricultural supply chain. Food Control, 33(1), 32-48. https://doi.org/10.1016/j.foodcont.2013.02.004

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4, 2292-2303. https://doi.org/10.1109/ACCESS.2016.2566339

Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research, 57(7), 2117-2135. https://doi.org/10.1080/00207543.2018.1533261

Lu, Y. (2017). Industry 4.0: A survey on technologies, applications and open research issues. Journal of

Industrial Information Integration, 6, 1-10. https://doi.org/10.1016/j.jii.2017.04.005

Azzi, R., Chamoun, R. K., & Sokhn, M. (2019). The power of a blockchain-based supply chain. Computers & Industrial Engineering, 135, 582-592. https://doi.org/10.1016/j.cie.2019.06.042

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., et al. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. Proceedings of the Thirteenth EuroSys Conference, 30, 1-15. https://doi.org/10.1145/3190508.3190538

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

Zhang, C., & Lu, Y. (2021). Study on artificial intelligence: The state of the art and future prospects. Journal of Industrial Information Integration, 23, 100224. https://doi.org/10.1016/j.jii.2021.100224

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

Tian, F. (2017). A supply chain traceability system for food safety based on HACCP, blockchain and Internet of Things. 2017 International Conference on Service Systems and Service Management, 1-6. https://doi.org/10.1109/ICSSSM.2017.7996119

Ivanov, D. (2020). Predicting the impacts of epidemic outbreaks on global supply chains: A simulation-based analysis on the coronavirus outbreak. International Journal of Production Research, 58(10), 2904-2915. https://doi.org/10.1080/00207543.2020.1750727

Lu, Y., & Xu, L. D. (2019). Internet of Things (IoT) cybersecurity research: A review of current research topics. IEEE Internet of Things Journal, 6(2), 2103-2115. https://doi.org/10.1109/JIOT.2018.2869847

Wust, K., & Gervais, A. (2018). Do you need a blockchain? 2018 Crypto Valley Conference on Blockchain Technology, 45-54. https://doi.org/10.1109/CVCBT.2018.00011

Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. IEEE Internet of Things Journal, 3(5), 637-646. https://doi.org/10.1109/JIOT.2016.2579198

Satyanarayanan, M. (2017). The emergence of edge computing. Computer, 50(1), 30-39. https://doi.org/10.1109/MC.2017.9

Lu, Y. (2019). Artificial intelligence: A survey on evolution, models, applications and future trends. Journal of Management Analytics, 6(1), 1-29. https://doi.org/10.1080/23270012.2019.1570365

Mao, Y., You, C., Zhang, J., Huang, K., & Letaief, K. B. (2017). A survey on mobile edge computing: The communication perspective. IEEE Communications Surveys & Tutorials, 19(4), 2322-2358. https://doi.org/10.1109/COMST.2017.2745201

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the Internet of Things. Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, 13-16. https://doi.org/10.1145/2342509.2342513

Botta, A., de Donato, W., Persico, V., & Pescape, A. (2016). Integration of cloud computing and Internet of Things: A survey. Future Generation Computer Systems, 56, 684-700. https://doi.org/10.1016/j.future.2015.09.021

Lu, Y., Zheng, X., Li, L., & Xu, L. D. (2020). Pricing the cloud: A QoS-based auction approach. Enterprise Information Systems, 14(3), 334-351. https://doi.org/10.1080/17517575.2019.1669827

Lu, Y. (2025). The current status and developing trends of Industry 4.0: A review. Information Systems Frontiers, 27(1), 215-234. https://doi.org/10.1007/s10796-021-10221-w

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645-1660.

https://doi.org/10.1016/j.future.2013.01.010

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

Tao, F., Zhang, H., Liu, A., & Nee, A. Y. C. (2019). Digital twin in industry: State-of-the-art. IEEE Transactions on Industrial Informatics, 15(4), 2405-2415. https://doi.org/10.1109/TII.2018.2873186

Lu, Y., & Zheng, X. (2020). 6G: A survey on technologies, scenarios, challenges, and the related issues. Journal of Industrial Information Integration, 19, 100158. https://doi.org/10.1016/j.jii.2020.100158

Lee, J., Bagheri, B., & Kao, H. A. (2015). A cyber-physical systems architecture for Industry 4.0-based manufacturing systems. Manufacturing Letters, 3, 18-23. https://doi.org/10.1016/j.mfglet.2014.12.001

Zhong, R. Y., Xu, X., Klotz, E., & Newman, S. T. (2017). Intelligent manufacturing in the context of Industry 4.0: A review. Engineering, 3(5), 616-630. https://doi.org/10.1016/J.ENG.2017.05.015

Xu, L. D., Xu, E. L., & Li, L. (2018). Industry 4.0: State of the art and future trends. International Journal of Production Research, 56(8), 2941-2962. https://doi.org/10.1080/00207543.2018.1444806

Lu, Y. (2018). Blockchain and the related issues: A review of current research topics. Journal of Management Analytics, 5(4), 231-255. https://doi.org/10.1080/23270012.2018.1516523

Qin, J., Liu, Y., & Grosvenor, R. (2016). A categorical framework of manufacturing for Industry 4.0 and beyond. Procedia CIRP, 52, 173-178. https://doi.org/10.1016/j.procir.2016.08.005

Wuest, T., Weimer, D., Irgens, C., & Thoben, K. D. (2016). Machine learning in manufacturing: Advantages, challenges, and applications. Production & Manufacturing Research, 4(1), 23-45. https://doi.org/10.1080/21693277.2016.1192517

Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. Science, 349(6245), 255-260. https://doi.org/10.1126/science.aaa8415

Lu, Y. (2021). Technological innovation and the emergence of a new interdisciplinary field: Management Analytics. Nanotechnologies in Construction, 13(3), 181-192. https://doi.org/10.15828/2075-8545-2021-13-3-181-192

LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521, 436-444. https://doi.org/10.1038/nature14539

Choi, T. M., Wallace, S. W., & Wang, Y. (2018). Big data analytics in operations management. Production and Operations Management, 27(10), 1868-1883. https://doi.org/10.1111/poms.12838

Gunasekaran, A., Papadopoulos, T., Dubey, R., Wamba, S. F., Childe, S. J., Hazen, B., & Akter, S. (2017). Big data and predictive analytics for supply chain and organizational performance. Journal of Business Research, 70, 308-317. https://doi.org/10.1016/j.jbusres.2016.08.004

Lu, Y., Ivanov, L. A., Wang, F., Pisarenko, Z. V., & Ye, C. (2024). Management analytics: A bibliometric analysis. Nanotechnologies in Construction, 16(3), 257-266. https://doi.org/10.15828/2075-8545-2024-16-3-257-266

Kache, F., & Seuring, S. (2017). Challenges and opportunities of digital information at the intersection of big data analytics and supply chain management. International Journal of Operations & Production Management, 37(1), 10-36. https://doi.org/10.1108/IJOPM-02-2015-0078

Ben-Daya, M., Hassini, E., & Bahroun, Z. (2019). Internet of Things and supply chain management: A literature review. International Journal of Production Research, 57(15-16), 4719-4742. https://doi.org/10.1080/00207543.2017.1402140

Papargyropoulou, E., Lozano, R., Steinberger, J. K., Wright, N., & Ujang, Z. (2014). The food waste hierarchy as a framework for the management of food surplus and food waste. Journal of Cleaner

Production, 76, 106-115. https://doi.org/10.1016/j.jclepro.2014.04.020

Kou, G., & Lu, Y. (2025). FinTech: A literature review of emerging financial technologies and applications. Financial Innovation, 11(1), 1-34. https://doi.org/10.1186/s40854-024-00668-6

Parfitt, J., Barthel, M., & Macnaughton, S. (2010). Food waste within food supply chains: Quantification and potential for change to 2050. Philosophical Transactions of the Royal Society B, 365(1554), 3065-3081. https://doi.org/10.1098/rstb.2010.0126

Garrone, P., Melacini, M., & Perego, A. (2014). Opening the black box of food waste reduction. Food Policy, 46, 129-139. https://doi.org/10.1016/j.foodpol.2014.03.014

Seuring, S., & Muller, M. (2008). From a literature review to a conceptual framework for sustainable supply chain management. Journal of Cleaner Production, 16(15), 1699-1710. https://doi.org/10.1016/j.jclepro.2008.04.020

Wu, H. P., Liu, Z., Dong, H. Y., Lu, Y., & Xu, L. D. (2025). Revolutionizing internal auditing: Harnessing the power of blockchain. Enterprise Information Systems, 19(1-2), 2448003. https://doi.org/10.1080/17517575.2024.2448003

Carter, C. R., & Rogers, D. S. (2008). A framework of sustainable supply chain management: Moving toward new theory. International Journal of Physical Distribution & Logistics Management, 38(5), 360-387. https://doi.org/10.1108/09600030810882816

Brandenburg, M., Govindan, K., Sarkis, J., & Seuring, S. (2014). Quantitative models for sustainable supply chain management: Developments and directions. European Journal of Operational Research, 233(2), 299-312. https://doi.org/10.1016/j.ejor.2013.09.032

Xu, R., Zhu, J., Yang, L., Lu, Y., & Xu, L. D. (2024). Decentralized finance (DeFi): A paradigm shift in the FinTech. Enterprise Information Systems, 18(9), 2397630. https://doi.org/10.1080/17517575.2024.2397630

Tang, C. S. (2006). Perspectives in supply chain risk management. International Journal of Production Economics, 103(2), 451-488. https://doi.org/10.1016/j.ijpe.2005.12.006

Christopher, M., & Peck, H. (2004). Building the resilient supply chain. The International Journal of Logistics Management, 15(2), 1-14. https://doi.org/10.1108/09574090410700275

Pettit, T. J., Fiksel, J., & Croxton, K. L. (2010). Ensuring supply chain resilience: Development of a conceptual framework. Journal of Business Logistics, 31(1), 1-21. https://doi.org/10.1002/j.2158-1592.2010.tb00125.x

Lu, Y., Sigov, A. S., Ratkin, L., Ivanov, L. A., & Zuo, M. (2023). Quantum computing and industrial information integration: A review. Journal of Industrial Information Integration, 35, 100511. https://doi.org/10.1016/j.jii.2023.100511

Ivanov, D., & Dolgui, A. (2020). Viability of intertwined supply networks: Extending the supply chain resilience angles toward survivability. International Journal of Production Research, 58(10), 2904-2915. https://doi.org/10.1080/00207543.2020.1750727

Dolgui, A., Ivanov, D., & Sokolov, B. (2018). Ripple effect in the supply chain: An analysis and recent literature. International Journal of Production Research, 56(1-2), 414-430. https://doi.org/10.1080/00207543.2017.1387680

Queiroz, M. M., Ivanov, D., Dolgui, A., & Wamba, S. F. (2020). Impacts of epidemic outbreaks on supply chains: Mapping a research agenda amid the COVID-19 pandemic. Annals of Operations Research, 319, 1159-1196. https://doi.org/10.1007/s10479-020-03685-7

Zheng, X. R., & Lu, Y. (2022). Blockchain technology: Recent research and future trend. Enterprise Information Systems, 16(12), 1939895. https://doi.org/10.1080/17517575.2021.1939895

Abad, E., Palacio, F., Nuin, M., Gonzalez de Zarate, A., Juarros, A., Gomez, J. M., & Marco, S. (2009). RFID smart tag for traceability and cold chain monitoring of foods: Demonstration in an intercontinental fresh fish logistic chain. Journal of Food Engineering, 93(4), 394-399. https://doi.org/10.1016/j.jfoodeng.2009.02.004

Ruiz-Garcia, L., & Lunadei, L. (2011). The role of RFID in agriculture: Applications, limitations and challenges. Computers and Electronics in Agriculture, 79(1), 42-50. https://doi.org/10.1016/j.compag.2011.08.010

Ruiz-Garcia, L., Barreiro, P., Robla, J. I., & Lunadei, L. (2009). Testing ZigBee motes for monitoring refrigerated vegetable transportation under real conditions. Sensors, 9(7), 4968-4982. https://doi.org/10.3390/s90704968

Lu, Y., & Yang, J. (2024). Quantum financing system: A survey on quantum algorithms, potential scenarios and open research issues. Journal of Industrial Information Integration, 41, 100663. https://doi.org/10.1016/j.jii.2024.100663

Yam, K. L., Takhistov, P. T., & Miltz, J. (2005). Intelligent packaging: Concepts and applications. Journal of Food Science, 70(1), R1-R10. https://doi.org/10.1111/j.1365-2621.2005.tb09052.x

Kerry, J. P., O'Grady, M. N., & Hogan, S. A. (2006). Past, current and potential utilisation of active and intelligent packaging systems for meat and muscle-based products: A review. Meat Science, 74(1), 113-130. https://doi.org/10.1016/j.meatsci.2006.04.024

Realini, C. E., & Marcos, B. (2014). Active and intelligent packaging systems for a modern society. Meat Science, 98(3), 404-419. https://doi.org/10.1016/j.meatsci.2014.06.031

Lu, W., Lu, Y., Li, J., Sigov, A., Ratkin, L., & Ivanov, L. A. (2024). Quantum machine learning: Classifications, challenges, and solutions. Journal of Industrial Information Integration, 42, 100736. https://doi.org/10.1016/j.jii.2024.100736

Biji, K. B., Ravishankar, C. N., Mohan, C. O., & Srinivasa Gopal, T. K. (2015). Smart packaging systems for food applications: A review. Journal of Food Science and Technology, 52, 6125-6135. https://doi.org/10.1007/s13197-015-1766-7

Nychas, G. J. E., Skandamis, P. N., Tassou, C. C., & Koutsoumanis, K. P. (2008). Meat spoilage during distribution. Meat Science, 78(1-2), 77-89. https://doi.org/10.1016/j.meatsci.2007.06.020