



Blockchain-enabled traceability and certification for frozen food supply chains: A conceptual design

Havva Uyar^{a,b}, Athanasios Papanikolaou^{a,*}, Evgenia Kapassa^{a,c}, Marios Touloupou^{a,d}, Stamatia Rizou^a

^a R&D and Innovation Department, SingularLogic, Athens, Greece

^b Department of Natural Resources Development and Agricultural Engineering, Agricultural University of Athens, Athens, Greece

^c Management, Entrepreneurship and Digital Business, Cyprus University of Technology, Paphos, Cyprus

^d Department of Electrical Engineering, Computer Engineering And Informatics, Cyprus University of Technology, Limassol, Cyprus

ARTICLE INFO

Keywords:

Blockchain
Smart contract
Ethereum
Solidity
Cold chain compliance

ABSTRACT

Ensuring traceability, compliance certification and cold chain integrity in frozen food supply chains remains a persistent challenge, exacerbated by fragmented monitoring systems, manual audits and vulnerability to data manipulation. This study presents a conceptual design for a blockchain-enabled compliance architecture that addresses these challenges by integrating real-time Internet of Things (IoT) data acquisition, permissioned blockchain-based data storage and smart contract-driven compliance automation. Following a Design Science Research (DSR) methodology, the research focuses on the initial phases (problem identification, objective specification and artefact conceptualization) providing a structured foundation for future demonstration and evaluation. The proposed design is structured across three interdependent layers: (1) a Data Acquisition Layer that ensures continuous and secure sensor-based monitoring; (2) a Data Storage Layer that leverages blockchain for immutable recording and transparent auditability; and (3) an Application Layer that integrates smart contracts for automated compliance enforcement and user interfaces for stakeholder interaction. By translating regulatory compliance requirements into a modular, blockchain-based design, this work contributes to the theoretical grounding of decentralized regulatory infrastructures in agri-food systems. The proposed architecture embodies design principles that may inform similar traceability systems across other regulated supply chains. Although empirical validation is forthcoming, the conceptualization serves as a scaffold for future DSR iterations and contributes to design knowledge in the domain of digital compliance architectures.

1. Introduction

The frozen food industry operates within a highly regulated environment, where maintaining product safety, quality and regulatory compliance across multi-tiered supply chains is critical. The cold chain must remain uninterrupted to prevent contamination, spoilage and the proliferation of foodborne pathogens, as even minor deviations from prescribed storage temperatures can compromise food safety [1,2]. Despite technological advancements, the sector continues to face significant challenges related to cold chain breaches, fraudulent food labeling and inefficient recall mechanisms, undermining both consumer trust and compliance with stringent food safety regulations [3–5].

Fraudulent practices, such as the mislabeling of lower-quality frozen goods as premium products, exacerbate existing vulnerabilities and

highlight the urgent need for robust, tamper-proof traceability and certification mechanisms. Conventional traceability systems, largely reliant on centralized databases and periodic audits, are susceptible to data manipulation, human error and inefficiencies, making it difficult to guarantee real-time visibility and compliance across distributed stakeholders [6,7].

The adoption of Internet of Things (IoT) technologies has improved real-time monitoring of key parameters, such as temperature and humidity, during storage and transportation [8,9]. However, the reliance on fragmented data infrastructures often weakens the overall integrity and auditability of compliance records. The need for an integrated solution that ensures the authenticity, security and real-time availability of traceability and certification data has therefore become increasingly apparent.

* Corresponding author.

E-mail address: apapanikolaou@singularlogic.eu (A. Papanikolaou).

<https://doi.org/10.1016/j.atech.2025.101085>

Received 2 May 2025; Received in revised form 5 June 2025; Accepted 5 June 2025

Available online 6 June 2025

2772-3755/© 2025 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

Governments and regulatory bodies enforce strict compliance requirements to safeguard the frozen food sector. In the European Union, Regulation (EC) No 178/2002 mandates comprehensive traceability "from farm to fork" [10], while Regulation (EC) No 37/2005 outlines requirements for the monitoring of temperatures during the transport, storage and warehousing of frozen foodstuffs [11]. In the United States, the Food Safety Modernization Act (FSMA) imposes similar mandates, including continuous temperature monitoring and prompt non-compliance reporting. Nonetheless, existing compliance verification mechanisms remain largely manual, slow and prone to data integrity issues.

Blockchain technology offers a promising avenue for addressing these limitations. As a decentralized, tamper-evident ledger, blockchain can securely record immutable compliance events across stakeholders, ensuring transparency, traceability and accountability. Smart contracts (programmable self-executing agreements) further enhance this potential by enabling automated enforcement of compliance protocols based on real-time IoT sensor data, without the need for intermediaries [7,8].

While blockchain solutions for agri-food supply chains have been explored in recent years, many implementations suffer from lack of granularity, poor IoT integration, limited real-time monitoring capabilities and minimal focus on regulatory compliance automation [3,5]. Moreover, empirical studies and structured conceptual designs addressing compliance certification in frozen food logistics specifically remain scarce, highlighting a clear gap in literature.

This study addresses this gap by conceptualising a blockchain-enabled architecture that integrates IoT-driven cold chain monitoring with Ethereum-based smart contracts to automate traceability, certification and compliance verification processes in frozen food supply chains. Adopting the Design Science Research (DSR) methodology, this paper focuses on the early phases of artefact design, namely, problem identification, objective specification and initial system conceptualisation. In doing so, the study contributes to the theoretical landscape of blockchain-based regulatory systems in agri-food contexts. Specifically, it develops a conceptual artefact grounded in compliance-oriented design principles, offering a blueprint for how decentralized technologies can embed regulatory logic directly into operational infrastructures. This contribution extends existing literature by focusing not only on traceability but also on the automation of certification processes in compliance-heavy environments.

The remainder of this paper is structured as follows. Section 2 reviews relevant literature on blockchain-enabled traceability in agri-food supply chains. Section 3 outlines the Design Science Research methodology guiding this study. Section 4 presents the proposed conceptual system architecture, detailing its layered components and stakeholder roles. Section 5 discusses future work. Finally, Section 6 concludes by summarizing key contributions and limitations.

2. Background

Blockchain technology has emerged as a transformative innovation in agri-food supply chains, offering secure, transparent and tamper-proof traceability systems that address long-standing challenges such as fraud, contamination, inefficiencies and regulatory compliance [12,4,5]. Traditional supply chain management systems, reliant on centralized databases and paper-based documentation, remain vulnerable to data manipulation, interoperability issues and inefficiencies in recall management, particularly during food safety incidents [6,3]. By leveraging distributed ledger technology, blockchain enhances supply chain visibility, ensuring that all stakeholders, including farmers, processors, distributors, retailers and consumers, have real-time access to an immutable history of transactions related to food products [13]. Moreover, integrating smart contracts with IoT-enabled sensors facilitates automated compliance monitoring, enabling real-time tracking of temperature, humidity and other critical parameters for perishable goods, thereby reducing food spoilage and waste ([7]; Kamble et al. [8]).

Studies have also highlighted blockchain's potential to streamline recall management by allowing contaminated or non-compliant batches to be quickly identified and removed from circulation, reducing health risks and economic losses. Despite these advantages, high computational costs, scalability issues and resistance to adoption remain significant barriers, particularly in developing economies where blockchain infrastructure is less established [14,15]. However, emerging permissioned blockchain solutions and hybrid models that optimize consensus mechanisms and energy efficiency are progressively making blockchain more viable for large-scale agricultural supply chains [2,9].

Building upon blockchain's ability to enhance traceability and transparency in agri-food supply chains, smart contracts further strengthen these systems by enabling automated compliance, real-time monitoring and tamper-proof enforcement of supply chain agreements [1,7,8]. Smart contracts, which are self-executing digital agreements stored on a blockchain, allow supply chain participants to define and enforce predefined conditions without the need for intermediaries, thereby improving efficiency and trustworthiness [16,17]. In the context of cold chain logistics, smart contracts can automatically validate whether perishable goods, such as frozen food products, have been stored and transported under optimal conditions by integrating data from IoT sensors and RFID tags [13,5]. If temperature deviations or regulatory violations are detected, smart contracts can trigger automated alerts, financial penalties or batch recalls, ensuring that non-compliant products are flagged before reaching consumers [2,9]. Additionally, these contracts facilitate seamless regulatory auditing, as compliance records are permanently logged on the blockchain and can be accessed by government authorities, certification bodies and quality control agencies. Despite these advantages, challenges such as legal recognition of smart contracts, cross-platform interoperability and computational overhead must be addressed to enable widespread adoption in agri-food supply chains [14,15]. Nevertheless, as blockchain ecosystems continue to evolve, the combination of traceability systems with smart contract automation holds significant potential to enhance food safety, streamline compliance and reinforce accountability across global agri-food networks [6,3,4].

While this background review synthesises key literature on blockchain, compliance, and traceability in agri-food supply chains, we acknowledge that it may not fully capture the breadth of recent developments in this fast-evolving field. In future work, it is planned to apply a more structured review approach, drawing on Multivocal methodologies [18] that incorporate both academic and grey literature. This will support a more comprehensive understanding of blockchain's practical applications and regulatory implications across diverse food system contexts.

3. Methodology

This study adopts the Design Science Research (DSR) methodology as the guiding framework for conceptualising a blockchain-based traceability and certification architecture for frozen food supply chains. DSR is a widely recognised methodological approach for research that aims to design, develop and ground technological artefacts in real-world problem settings, while also contributing to the knowledge base of the field [19–21]. It is particularly suited for socio-technical domains such as agri-food supply chains, where systemic inefficiencies, fragmented data environments and evolving compliance demands call for rigorously designed and well-justified digital solutions. In the context of this study, DSR provides a structured lens for addressing critical traceability and compliance issues in frozen food supply chains by conceptualising a blockchain-based system architecture. The methodology enables for defining the problem space, specifying design objectives and developing an initial solution in the form of a conceptual artefact.

The standard DSR framework consists of six interrelated activities, as identified by Peffers et al. [21]. These activities include problem identification and motivation, defining the objectives for a solution, design

and development, demonstration, evaluation and communication (Fig. 1). Although these steps are often presented as sequential, DSR does not prescribe a strictly linear process. Instead, it allows for iterative and staged progress depending on the maturity of the artefact and the aims of the research [22,19]. As such, DSR is increasingly used in multi-phase contributions where individual papers may focus on selected steps of the full cycle, particularly when the primary aim is to establish foundational design knowledge or conceptual clarity.

This study focuses on the early phases of the DSR cycle, specifically on problem identification and motivation, definition of objectives for a solution and the initial design of the proposed system architecture. These three activities constitute the scope of the present research. The remaining stages, demonstration, evaluation and broader communication, are deferred to subsequent studies and future publications, in line with the practices in staged DSR contributions [22,23]. The first two steps are addressed in the Introduction and Background sections of this paper, which describe the traceability and compliance challenges in frozen food logistics and outline the key objectives for the proposed blockchain-based solution and smart contracts application. This structuring is consistent with established DSR practice, where formal activities may be embedded in traditional academic sections if their alignment is clearly articulated [19,21].

In line with DSR practices, this study applied the methodology by first identifying the problem through documented challenges in cold chain compliance and traceability, as described in the Introduction and Background sections. Design objectives—such as improving data integrity, enabling real-time monitoring, and embedding regulatory logic—were specified based on literature and regulatory requirements. These objectives informed the conceptual development of the system architecture, which serves as the artefact produced at this stage. While later DSR phases such as demonstration and evaluation are outside the scope of this paper, the structured progression from problem identification to artefact conceptualization aligns with the early phases of the DSR process.

3.1. Artefact description and design scope

The artefact developed in this study is a conceptual system architecture for a blockchain-based traceability and certification solution, tailored to the operational and regulatory requirements of frozen food

supply chains. Its design is situated within the DSR methodology, following the iterative and structured process of designing artefacts that solve identified problems while contributing to theory [19,21].

The design process was guided by the need to address traceability gaps, fragmented compliance data and limited automation in existing cold chain monitoring systems [3,5]. The artefact conceptualises a permissioned blockchain network that integrates smart contracts and IoT data to support real-time compliance tracking, data provenance and event-driven automation in alignment with regulatory standards. Drawing from principles of architectural design in socio-technical systems [22], the study reflects key functional requirements derived from both literature and documented cold chain challenges.

The artefact was designed to fulfil three core methodological objectives. First, it ensures traceability across all stages of the supply chain by enabling tamper-evident recording of critical events (from production to delivery) on a decentralised ledger. Second, it facilitates the integration of real-time data from distributed IoT sensors (e.g., temperature and humidity monitors), which is critical for cold chain integrity and regulatory compliance. Third, it embeds compliance logic within Ethereum-based smart contracts, allowing automated verification of environmental thresholds, the triggering of alerts and the enforcement of predetermined agreements.

The design of the system architecture followed modularisation principles commonly applied in blockchain system design. Specifically, functional areas such as user management order processing, inventory tracking and delivery status were conceptualised as separable smart contract modules. This separation of concerns was intended to enhance maintainability, support role-based access control and align with real-world task divisions among supply chain stakeholders.

In line with the goal of controlled accessibility and privacy-preserving compliance, the architecture leverages the Hyperledger Besu client to support a private Ethereum-compatible blockchain. It also incorporates BlockScout as a blockchain explorer to allow authorised entities to monitor transactions and verify compliance actions transparently. These design choices reflect both technical suitability and alignment with common practices in enterprise-grade blockchain deployments.

Although no functional prototype is implemented at this stage, the conceptual artefact represents a methodologically structured response to a clearly defined compliance problem in the frozen food sector. It will

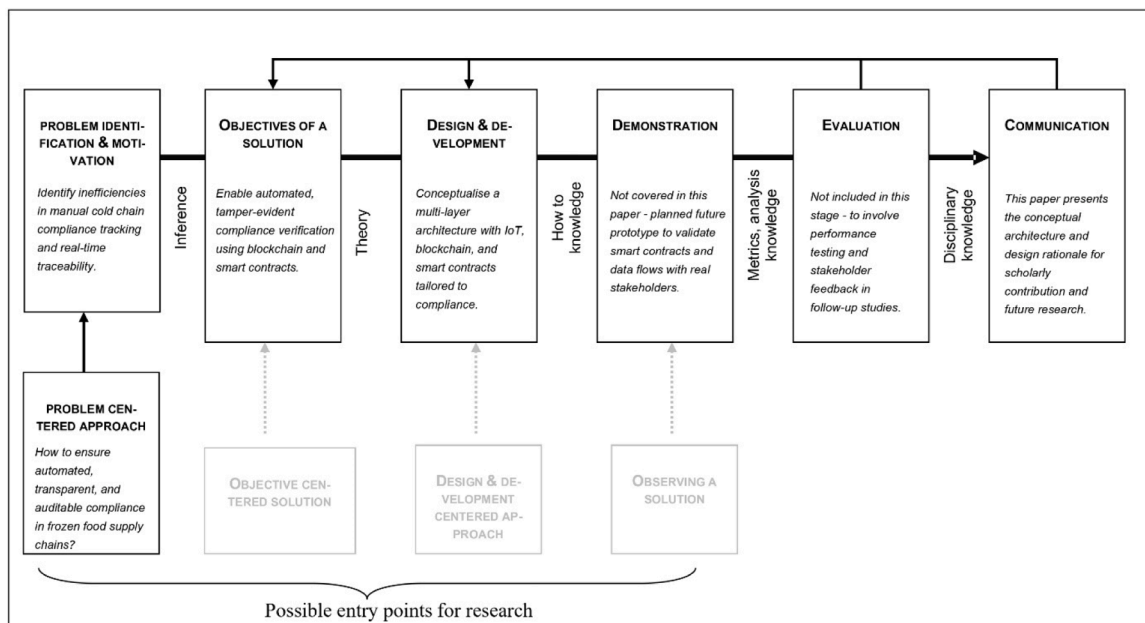


Fig. 1. DC research process for the study (Adopted from Peffers et al. [21]).

serve as the foundation for subsequent phases of demonstration and evaluation, consistent with staged contributions in DSR [23]. In this way, the study advances both the practical understanding of blockchain's role in regulatory enforcement and the theoretical foundations of design-oriented research in agri-food traceability systems.

4. Conceptual system architecture

This section presents the conceptual system architecture for a blockchain-based traceability and certification system, designed to meet the practical and regulatory needs of frozen food supply chains. The development of this architecture is guided by the following main research question:

RQ: How can a blockchain-based architecture be conceptualized to enable secure, real-time traceability and automated compliance certification for frozen food supply chains?

To explore this, the study also examines three related sub-questions:

SRQ1: What are the key traceability and compliance challenges in frozen food logistics, and how can blockchain technology help address them?

SRQ2: What design principles should guide the development of a blockchain-based traceability and certification system for frozen food supply chains?

SRQ3: What are the main components and functions needed to support IoT data integration, smart contract automation, and compliance processes?

The main contribution of this study is the design of a conceptual system architecture that combines real-time IoT monitoring with blockchain and smart contracts to support traceability and compliance. This section describes the system's structure and key parts, responding directly to the research questions and setting the stage for future

development and testing. Specifically, SRQ1 is addressed by identifying key traceability and compliance gaps tackled by the system design; SRQ2 is reflected in the design principles adopted across the layers; and SRQ3 is answered through the technical breakdown of how IoT data, smart contracts, and stakeholder functions are implemented.

The architecture aims to solve common problems in cold chain management (e.g. lack of traceability, scattered data, and slow manual checks) by using blockchain, connected sensors, and automated rules. It supports full tracking of products, real-time monitoring, and automatic checks based on defined rules and regulations. The system is designed to meet specific regulatory requirements, including:

- Continuous temperature monitoring in line with Regulation (EC) No 37/2005, which mandates that quick-frozen foodstuffs must be maintained at -18°C or below during transport, storage and warehousing, with limited permissible fluctuations during transport (up to $+3^{\circ}\text{C}$).
- Full traceability from origin to point-of-sale, as required by Regulation (EC) No 178/2002 ("from farm to fork").
- Tamper-evident, audit-ready compliance records to support inspections, audits and certifications (e.g., HACCP, FSMA).
- Automation of compliance enforcement, reducing dependence on paper logs and manual audits.

The architecture is structured across three interdependent layers: (1) *Data Acquisition Layer*, (2) *Data Storage Layer* and (3) *Application Layer*. A conceptual diagram of this architecture is recommended for inclusion (see Fig. 2). The data Acquisition layer represents clusters of sensors that operate in a decentralized mode and collect all required data in every stage of the frozen food supply process. The Data Storage and Validation Layer represents the blockchain network, the entirety of its nodes (blocks). The layer includes consensus mechanisms and algorithms (Proof of Stake, Proof of Authority, etc.) that validate each transaction within the blockchain network. It is important to clarify that within the context of blockchain by transaction we mean any exchange of data

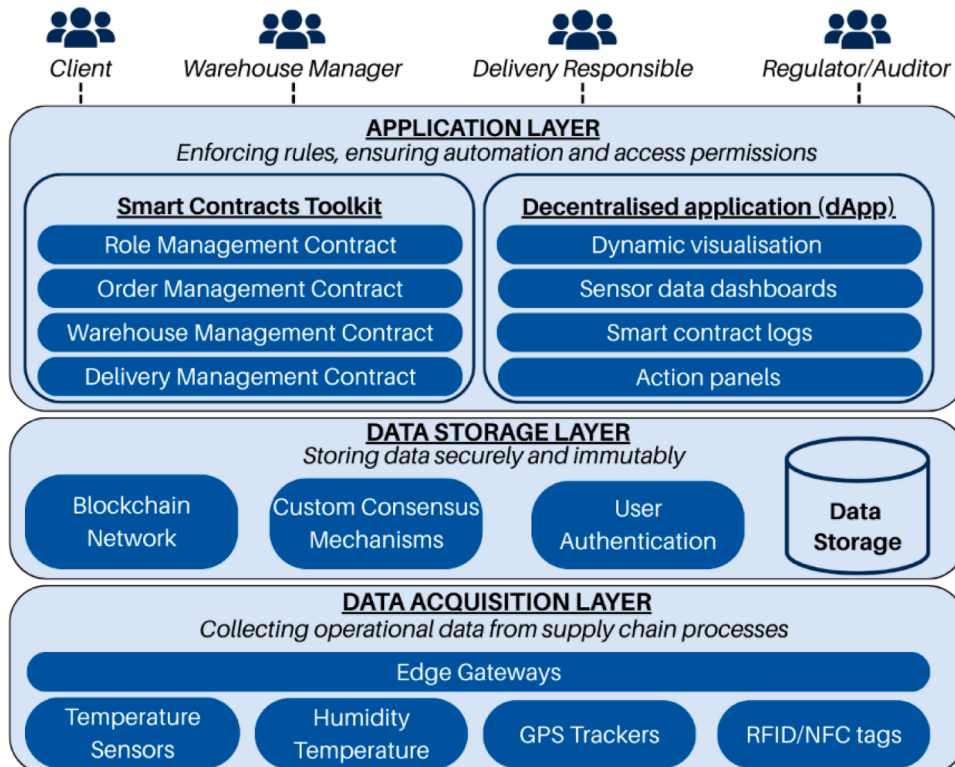


Fig. 2. Proposed three layer system architecture for blockchain-enabled cold chain compliance.

between two separate actors within the network. Finally, the Application Layer encompasses the proposed smart contracts along with the user interface, serving as the primary point of interaction between the blockchain, IoT devices and end users. This layer facilitates the execution of core functions and manages system alerts, ensuring seamless communication and coordination across all components of the architecture. It acts as the interface through which users engage with the system and where automated responses (e.g. compliance checks, notifications) are triggered based on real-time data inputs. An important clarification is that while smart contract functions are triggered and interacted with, through the Application Layer, they reside on the Data Storage Layer. This means that their code and state are directly deployed and stored in the blockchain.

4.1. Data acquisition layer

The Data Acquisition Layer serves as the foundation of the proposed architecture, enabling continuous, real-time monitoring of environmental parameters critical to the integrity and compliance of frozen food logistics. This layer comprises a network of strategically deployed IoT-enabled sensors and devices that collect, aggregate and transmit data related to temperature, humidity, location and other compliance-relevant variables across different stages of the supply chain. This layer responds directly to SRQ3 by enabling IoT data collection and real-time environmental monitoring, forming the technical basis for traceability and compliance verification.

To support granular environmental monitoring, the system integrates multiple sensor types, including:

- *Wireless temperature sensors* (e.g. Bluetooth Low Energy (BLE), Zigbee-enabled devices) for monitoring ambient and product-level conditions inside containers or cold rooms;
- *Humidity sensors* to capture moisture levels during storage and transport, which can affect product quality and safety;
- *GPS trackers and RFID/NFC tags*, embedded in pallets or shipment containers, to ensure real-time geolocation and identification of goods;
- *Edge gateways*, responsible for local aggregation and transmission of sensor data via secure communication protocols (e.g., MQTT or HTTPS).

These devices are deployed at key control points across the supply chain (e.g. production facilities, warehouses, refrigerated trucks, retail cold storage units). Each sensor is cryptographically registered on the blockchain, ensuring tamper-resistance and auditability of the data source.

Sensor nodes are configured to capture and transmit data at pre-defined intervals (e.g., every 10 min), with immediate broadcasting of anomalies that breach compliance thresholds (e.g., temperature spikes exceeding -15°C). Data is first aggregated at local gateways, where initial validation checks (e.g., signal integrity, timestamping, anomaly detection) are performed before securely transmitting to the blockchain network. This approach reduces bandwidth consumption, ensures temporal consistency and enables early detection of cold chain breaches or device failures. Gateways are further responsible for filtering redundant signals, compressing data payloads and enforcing digital signing mechanisms to preserve data authenticity.

The design of the Data Acquisition Layer explicitly aligns with legal standards such as EU Regulation (EC) No 37/2005, which mandates continuous monitoring of frozen food temperatures in -18°C with permissible deviations of no $>3^{\circ}\text{C}$ during transport. To this end:

- Sensors are configured with hardcoded regulatory thresholds for automatic detection of non-compliant conditions;
- Devices initiate event-driven data capture upon detecting abrupt environmental changes;

- All readings are timestamped and digitally signed, ensuring traceability to source and time of recording.

Such measures not only facilitate real-time response to anomalies but also support retrospective validation during inspections or audits, offering regulators and certification bodies verifiable proof of compliance. While the current conceptualisation focuses on temperature, humidity and location parameters, future extensions may incorporate shock sensors, CO₂ sensors or light exposure monitors, enabling a more holistic view of product handling and transport conditions. Additionally, integration with on-chain oracles may enable dynamic reconfiguration of thresholds based on updated legal or climatic requirements, enhancing adaptability.

4.2. Data storage layer

The Data Storage Layer constitutes the secure, decentralised backbone of the proposed system, providing immutable, tamper-evident storage for all compliance-relevant data generated by the Data Acquisition Layer. Its core function is to ensure integrity, availability and auditability of traceability records across the entire frozen food supply chain. By leveraging a permissioned blockchain infrastructure, this layer eliminates the need for centralised intermediaries, thus enhancing trust, reducing administrative overhead and improving regulatory responsiveness. This component contributes to both SRQ1 and SRQ3 by addressing data integrity and trust challenges in traceability systems, while also enabling immutable recording of events for automated compliance tracking.

This architecture employs *Hyperledger Besu* as the underlying blockchain client due to its compatibility with Ethereum-based smart contracts and its robust support for private, permissioned networks. A permissioned setup is essential in the context of compliance-sensitive food supply chains, where data confidentiality, granular access control and operational isolation are paramount. Hyperledger Besu offers the following advantages:

- *Fine-grained permissioning* for role-based access to blockchain data and operations;
- *Enterprise-ready privacy mechanisms*, such as private transaction groups;
- *Ethereum Virtual Machine (EVM) support*, enabling the deployment of custom smart contracts for regulatory logic;
- *Rich logging and diagnostic capabilities*, essential for debugging, audit trails and governance reviews.

This configuration ensures that supply chain actors can interact with the blockchain according to pre-defined access rules, while preserving the transparency of critical events.

Each transaction or event recorded on the blockchain corresponds to a traceability event (e.g. order placement, inventory dispatch, delivery confirmation) or an environmental data point (e.g., temperature breach, sensor malfunction). The data structure for each transaction includes:

- Unique shipment and batch identifiers,
- Sensor device IDs and environmental readings (e.g., temperature, humidity),
- Smart contract execution logs (e.g., compliance status changes, automated actions),
- Role-based user interactions (e.g., inventory updates order confirmations).

This design ensures that every critical event in the supply chain lifecycle is chronologically and immutably recorded, providing stakeholders with a reliable source of truth that supports both operational decision-making and regulatory audits.

To enhance system observability, *BlockScout* is chosen as the

blockchain explorer interface. It allows authorised actors to visualise and verify blockchain transactions, contract events and sensor logs in real time. This improves audit readiness and reinforces confidence in the authenticity of compliance workflows. The blockchain serves as an immutable data repository and audit log for compliance-related events enforced by smart contracts. It does not, by itself, evaluate regulatory thresholds or trigger actions; instead, it ensures that the outputs of such enforcement (e.g. alerts, decisions, certificates) are securely and permanently documented.

Given the volume and frequency of sensor-generated data in cold chain environments, the architecture also allows for *off-chain data storage integration*, where large datasets (e.g., raw temperature logs) may be stored in secure repositories (e.g., IPFS, cloud storage), with corresponding hashes recorded on-chain for verification. This hybrid approach balances scalability with verifiability. In summary, the blockchain layer serves as a secure, distributed compliance infrastructure, anchoring the trust layer of the system while supporting automated enforcement and traceability. Its integration with smart contracts, audit tooling and permissioned governance mechanisms makes it a foundational component of the proposed architecture for cold chain certification.

4.3. Application layer

The Application Layer represents the functional apex of the proposed architecture, where technological artefacts converge with regulatory processes and human actors. It operationalizes compliance logic, governs stakeholder roles and facilitates interaction through an user interface. This layer integrates smart contracts with stakeholder access control, automates audit mechanisms and enables users to interact with the system in a secure, role-based manner. Its core function is to ensure that regulatory requirements are not merely recorded but actively enforced through executable code. This layer aligns with SRQ2 and SRQ3 by implementing modular smart contracts and role-based stakeholder access, directly embedding compliance rules into system operations.

4.3.1. Smart contracts for embedded compliance

Solidity-based smart contracts are deployed on a permissioned Ethereum-compatible blockchain (Hyperledger Besu). These contracts formalise regulatory rules and operational procedures into modular code blocks, enabling machine-enforced traceability and certification.

Smart contracts encode compliance workflows that would otherwise require manual audits, third-party verifications or paper-based reporting. For instance, contracts validate whether temperature thresholds defined under EU Regulation (EC) No 37/2005 are upheld across the supply chain, based on IoT sensor data fed into the blockchain at pre-set intervals. A single deviation (e.g., a product remaining above -15°C for >15 min) triggers automated workflows such as:

- Logging a violation and creating an immutable compliance event,
- Halting the order dispatch or flagging the shipment as compromised,
- Notifying designated authorities or quality managers via integrated alert protocols.

In addition to incident-based actions, smart contracts also issue compliance certificates for batches that meet all traceability and environmental integrity requirements. These certificates are recorded on-chain, cryptographically linked to the product's journey and verifiable by auditors or consumers.

Smart contracts are organised into four core modules:

1. **Role Management Contract:** Establishes role-based access control (RBAC), governing who can perform what operations. It ensures governance hierarchy, data protection and operational clarity. Role

delegation and revocation functions support scalability and compliance with internal policy shifts.

2. **Order Management Contract:** Manages the full lifecycle of product orders, linking each order with IoT data and associated events. It supports creation, validation, modification (by authorised users) and timestamped completion.
3. **Warehouse Management Contract:** Controls stock visibility, dispatch readiness and storage compliance. Integrates directly with environmental data from storage units to block the release of goods not meeting certification criteria.
4. **Delivery Management Contract:** Tracks the flow of goods post-dispatch. It records status transitions (e.g., 'In Transit', 'Delivered') and anomalies, issuing digital proof of delivery and final compliance status.

Each contract interacts autonomously and logs its actions on the blockchain, establishing a verifiable and distributed enforcement layer. These mechanisms reduce administrative workload, increase consistency and align digital infrastructure with food safety legislation.

4.3.2. Stakeholder role definition and operational mapping

The roles defined in this system were derived from prior work on role-based models in blockchain applications. Role assignment aligns with well-established patterns in RBAC (Role-Based Access Control), where permissions are attached to roles rather than individual users, allowing for easier policy enforcement and security. This approach reflects best practices in Ethereum smart contract development, where poorly implemented access control has led to critical security vulnerabilities [24]. To ensure a secure and maintainable architecture, roles were mapped to smart contract functions using modular contract design, following principles described in formal RBAC models such as SC-RBAC [25,26]'s foundational RBAC framework. These models support the principle of least privilege and allow traceable, role-specific interactions within the blockchain system. Table 1 outlines the core roles defined within the proposed system design, their respective operational responsibilities and the associated smart contract functions.

Wallet-based identification ensures that only authorized users assigned specific roles can perform actions, supporting cryptographic accountability and complying with data governance standards. All role assignments, access changes, and operational events are immutably recorded on the blockchain, providing an auditable and transparent log accessible to authorized stakeholders. This shared ledger fosters trust and accountability among participants without compromising data privacy. Importantly, the Administrator role is designed to be flexible and context-dependent. It does not represent a centralized technical authority overseeing the entire blockchain network. Instead, it is assigned to a person or entity responsible for managing access permissions within the smart contract system, depending on the governance structure of the specific implementation. This flexibility allows the architecture to fit different business scenarios while maintaining transparency and auditability through on-chain records of role assignments

Table 1
Role-based actor responsibilities and smart contract functions.

Role	Responsibilities	Smart Contract Functions
Client	Places product orders, receives goods	Create orders, view compliance status
Warehouse Manager	Monitors inventory, authorises dispatch	Update stock, validate storage conditions
Delivery Responsible	Logs shipping milestones, confirms delivery	Change delivery status, confirm handover
Regulator/Auditor	Views compliance logs, certifies audits	Read-only access to smart contract events, generate audit reports
Administrator	Manages roles, system configuration	Assign roles, revoke permissions

and actions. This zero-trust security model aligns with GDPR, FSMA and general data governance principles, ensuring only authorised, traceable access.

4.3.3. Interfaces and usability considerations

To foster adoption and simplify interaction, the Application Layer includes a *decentralised application (dApp)* with user-specific dashboards. Interfaces are built for accessibility via both web and mobile environments and structured around real-time contract events. Each interface module includes:

- *Dynamic visualisation* of order and shipment status,
- *Sensor data dashboards* with alerts and historical trends,
- *Smart contract logs*, translated into legible audit events (e.g., "Batch 37 certified compliant at 13:42 UTC"),
- *Action panels* (e.g., dispatch approval, delivery confirmation, audit initiation) based on the user's role.

The front-end is designed to be event-driven, responding to changes emitted from smart contracts (e.g. *orderApproved*, *Non-ComplianceDetected*, *DeliveryConfirmed*). All transactions are logged and time-stamped immutably on-chain and made human-readable via BlockScout or custom monitoring panels. APIs are available to support external integrations with legacy systems (e.g., ERP, national food safety registries).

5. Future research

This study presents a conceptual design for a blockchain-enabled traceability and certification system tailored to the specific regulatory and operational challenges of frozen food supply chains. While the proposed architecture addresses several critical gaps in current traceability mechanisms, particularly in terms of real-time compliance verification, auditability, and automation, there are several areas that will be explored further in future research.

First, the work remains at the conceptual and architectural design phase, without a fully implemented prototype. Although the system is designed based on established blockchain, IoT and smart contract technologies, empirical testing and demonstration are essential to validate its practical feasibility. Future work will therefore focus on developing a working prototype that instantiates the conceptual model, integrating real-time IoT data acquisition, smart contract-based compliance verification and decentralised stakeholder interfaces.

Testing and evaluation of the prototype will involve the definition of structured performance metrics. Furthermore, stakeholder feedback will play a central role in validating the system's usability, trustworthiness, and alignment with the needs of producers, warehouse managers, transporters, retailers, and regulators. A particularly important avenue for future research is stakeholder impact analysis, including factors affecting user adoption and the socio-technical challenges of integrating decentralised systems into highly regulated, traditionally conservative sectors. Usability tests will be conducted to collect insights on the system's adoption potential, perceived barriers, and requirements for further improvement. While this study offers a foundational step toward blockchain-enabled compliance and traceability in frozen food logistics, much work remains to translate conceptual designs into operational, scalable and widely adopted solutions. The challenges of technical implementation, user engagement, regulatory acceptance and economic viability must all be systematically addressed in future stages of research and development.

6. Conclusion

This study presented a conceptual architecture for a blockchain-enabled traceability and certification system designed specifically for the frozen food supply chain, addressing critical challenges related to

regulatory compliance, cold chain integrity, and trust among distributed stakeholders. By integrating IoT-based real-time data acquisition, decentralised blockchain data storage, and smart contract-driven compliance automation, the proposed system aims to enhance the transparency, reliability, and auditability of cold chain operations.

The design aligns closely with key regulatory mandates, such as EU Regulation (EC) No 178/2002 and Regulation (EC) No 37/2005, embedding compliance verification directly into the technological fabric of the supply chain. Smart contracts serve as autonomous regulatory agents, enforcing temperature control thresholds, issuing automated alerts for non-compliance, and ensuring immutable certification records. Through permissioned blockchain deployment and modular smart contract architecture, the system seeks to balance transparency, data privacy, and operational scalability. These are essential factors for real-world adoption in highly regulated sectors.

This study contributes to the growing body of research on blockchain-enabled traceability by offering a structured, compliance-focused system architecture tailored to the regulatory and operational needs of frozen food logistics. Unlike many existing approaches that prioritize traceability in general agri-food contexts, this work focuses on automating certification and compliance processes through the integration of IoT-based monitoring and smart contract logic. By translating complex regulatory requirements into modular system components, the proposed conceptual artefact provides a design blueprint for embedding regulatory logic directly into digital infrastructures. In doing so, it extends the literature not only in terms of technical integration but also by emphasizing regulatory automation in compliance-intensive environments.

Beyond its applied relevance, the architecture contributes to design knowledge by mapping compliance functions to blockchain and IoT capabilities in a structured manner. This may serve as a reference model for future system design efforts in similarly regulated supply chains. As a result, the artefact supports theory-building related to digital compliance infrastructures, particularly in contexts where automation, auditability, and distributed accountability are essential.

However, as with any conceptual design study, this work has limitations. The architecture has not yet been implemented or validated in real-world settings, and its technical performance, integration feasibility, and user acceptance remain untested. The current design also does not fully address the legal enforceability of smart contracts, the variation in stakeholder digital readiness, or the challenges of data interoperability with existing legacy systems.

In line with the iterative nature of the Design Science Research methodology, future work will focus on operationalising the architecture through prototype development, empirical testing, and stakeholder engagement. These next steps will help refine the artefact, address its current limitations, and evaluate its practical utility and scalability. As supply chains become increasingly complex, the demand for digitally enforced, auditable, and trustworthy traceability frameworks is expected to grow. This need applies not only to frozen foods but also across other sectors handling perishable goods.

Ethics statement

Not applicable: This manuscript does not include human or animal research.

CRediT authorship contribution statement

Havva Uyar: Writing – review & editing, Writing – original draft, Methodology, Investigation, Formal analysis. **Athanasios Papanikolaou:** Writing – review & editing, Writing – original draft, Validation, Investigation. **Evgenia Kapassa:** Writing – review & editing, Validation, Supervision. **Marios Touloupas:** Writing – review & editing, Validation, Supervision. **Stamatia Rizou:** Writing – review & editing, Validation, Supervision, Project administration, Funding acquisition.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

- [1] Q. Lin, H. Wang, X. Pei, J. Wang, Food safety traceability system based on blockchain and EPCIS, *IEEE Access* 7 (2019) 20698–20707.
- [2] Y.P. Tsang, K.L. Choy, C.H. Wu, G.T.S. Ho, H.Y. Lam, Blockchain-driven IoT for food traceability with an integrated consensus mechanism, *IEEE Access* 7 (2019) 129000–129017.
- [3] J.F. Galvez, J.C. Mejuto, J. Simal-Gandara, Future challenges on the use of blockchain for food traceability analysis, *TrAC Trends Anal. Chem.* 107 (2018) 222–232.
- [4] A. Kamilaris, A. Fonts, F.X. Prenafeta-Boldú, The rise of blockchain technology in agriculture and food supply chains, *Trends Food Sci. Technol.* 91 (2019) 640–652.
- [5] F. Tian, An agri-food supply chain traceability system for China based on RFID & blockchain technology, in: *Proceedings of the 2016 13th International Conference on Service Systems and Service Management (ICSSSM)*, IEEE, 2016, pp. 1–6.
- [6] M.P. Caro, M.S. Ali, M. Vecchio, R. Giaffreda, Blockchain-based traceability in Agri-Food supply chain management: a practical implementation, in: *Proceedings of the 2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany)*, IEEE, 2018, pp. 1–4.
- [7] F. Casino, T.K. Dasaklis, C. Patsakis, A systematic literature review of blockchain-based applications: current status, classification and open issues, *Telemat. Inform.* 36 (2019) 55–81.
- [8] S. Kamble, A. Gunasekaran, H. Arha, Understanding the blockchain technology adoption in supply chains-Indian context, *Int. J. Prod. Res.* 57 (7) (2019) 2009–2033.
- [9] M.A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, H. Janicke, Blockchain technologies for the internet of things: research issues and challenges, *IEEE Internet. Things. J.* 6 (2) (2018) 2188–2204.
- [10] European Commission, Regulation (EC) No 178/2002 of the European parliament and of the council, Off. J. Eur. Communities L31 (2002) 1–24. <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32002R0178>.
- [11] European Commission, Regulation (EC) No 37/2005 of the European parliament and of the council, Off. J. Eur. Union L10 (2005) 18–19. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32005R0037>.
- [12] K. Behnke, M.F.W.H.A. Janssen, Boundary conditions for traceability in food supply chains using blockchain technology, *Int. J. Inf. Manag.* 52 (2020) 101969.
- [13] H. Feng, X. Wang, Y. Duan, J. Zhang, X. Zhang, Applying blockchain technology to improve agri-food traceability: a review of development methods, benefits and challenges, *J. Clean. Prod.* 260 (2020) 121031.
- [14] M. Kouhizadeh, J. Sarkis, Blockchain practices, potentials and perspectives in greening supply chains, *Sustainability* 10 (10) (2018) 3652.
- [15] M. van Hilten, G. Ongena, P. Ravesteijn, Blockchain for organic food traceability: case studies on drivers and challenges, *Frontiers in Blockchain* 3 (2020) 567175.
- [16] R. Azzi, R.K. Chamoun, M. Sokhn, The power of a blockchain-based supply chain, *Comput. Ind. Eng.* 135 (2019) 582–592.
- [17] K. Christidis, M. Devetsikiotis, Blockchains and smart contracts for the internet of things, *IEEE Access* 4 (2016) 2292–2303.
- [18] M. Themistocleous, P. Cunha, E. Tabakis, M. Papadaki, Towards cross-border CBDC interoperability: insights from a multivocal literature review, *J. Enterp. Inf. Manag.* 36 (5) (2023) 1296–1318, <https://doi.org/10.1108/JEIM-11-2022-0411>.
- [19] S. Gregor, A.R. Hevner, Positioning and presenting design science research for maximum impact, *MIS Q.* (2013) 337–355.
- [20] A.R. Hevner, S.T. March, J. Park, S. Ram, Design science in information systems research, *MIS Q.* (2004) 75–105.
- [21] K. Peffers, T. Tuunanen, M.A. Rothenberger, S. Chatterjee, A design science research methodology for information systems research, *Journal of management information systems* 24 (3) (2007) 45–77.
- [22] R. Baskerville, A. Baiyere, S. Gregor, A. Hevner, M. Rossi, Design science research contributions: finding a balance between artifact and theory, *J. Assoc. Inf. Syst.* 19 (5) (2018) 3.
- [23] M.K. Sein, O. Henfridsson, S. Purao, M. Rossi, R. Lindgren, Action design research, *MIS Q.* (2011) 37–56.
- [24] J.P. Töberg, J. Schiffel, F. Reiche, B. Beckert, R. Heinrich, R. Reussner, Modeling and enforcing access control policies for smart contracts, in: *Proceedings of the 2022 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*, Newark, CA, USA, 2022, pp. 38–47, <https://doi.org/10.1109/DAPPS55202.2022.00013>.
- [25] Y. Ding, J. Jin, J. Zhang, Z. Wu, K. Hu, SC-RBAC: a smart contract based RBAC model for DApps, in: D. Milošević, Y. Tang, Q. Zu (Eds.), *Human Centered Computing. HCC 2019. Lecture Notes in Computer Science*, Vol 11956, Springer, Cham, 2019, https://doi.org/10.1007/978-3-030-37429-7_8.
- [26] R.S. Sandhu, E.J. Coyne, H.L. Feinstein, C.E. Youman, Role-based access control models, *Computer* 29 (2) (1996) 38–47, <https://doi.org/10.1109/2.485845>. (Long. Beach. Calif)Feb.