

ORIGINAL RESEARCH

Open access

Conceptualizing a Blockchain-Based Compliance Infrastructure for Frozen Food Cold Chains

Wei Zhang^{1*}, Chen Hui², Michael Tan¹

Abstract

Guaranteeing end-to-end visibility, certified conformity, and uninterrupted temperature control in frozen food logistics remains an enduring obstacle, compounded by siloed oversight tools, hands-on inspection routines, and exposure to information falsification. This paper puts forward a blueprint for a blockchain-anchored conformity framework that resolves these difficulties by fusing continuous Internet of Things (IoT) sensing, authorized blockchain-based recordkeeping, and automated conformance enforcement via smart contracts. Adopting a Design Science Research (DSR) approach, the inquiry zeroes in on the formative stages (challenge scoping, goal setting, and artefact blueprinting) to deliver a methodical grounding for subsequent testing and appraisal. The envisioned construct is arranged across three mutually reliant strata: (1) a data acquisition layer that secures uninterrupted and safeguarded sensor-fed tracking; (2) a data storage layer that harnesses blockchain for indelible logs and open verifiability; and (3) an application layer that weaves in smart contracts for hands-off compliance activation along with dashboards for actor engagement. By reinterpreting statutory conformity mandates into a compartmentalized, blockchain-centric blueprint, this investigation fortifies the conceptual basis of decentralized governance apparatuses within agri-food networks. The formulated framework codifies design maxims capable of shaping parallel provenance systems in other heavily audited supply networks. While practical corroboration is yet to come, the architectural outline supplies a platform for later DSR rounds and enriches design intelligence in the arena of digital conformity infrastructures.

Keywords Blockchain, Smart contract, Ethereum, Solidity, Cold chain compliance

*Correspondence:

Wei Zhang

wei.zhang@unimelb.edu.au

¹ Department of Cold Chain Management and Blockchain, Faculty of Agriculture, University of Melbourne, Melbourne, Australia

² Department of Food Traceability and Compliance Infrastructure, Faculty of Agriculture, National University of Singapore, Singapore, Singapore

Introduction

The frozen provisions sector conducts business under a tightly controlled regime, where upholding item integrity, caliber, and statutory adherence throughout layered distribution webs stands as paramount. The refrigeration sequence must stay intact to forestall taint, decay, and the multiplication of foodborne microorganisms, seeing that even negligible divergences from set holding temperatures can imperil food integrity [1, 2]. Notwithstanding technical headway, the field persistently wrestles with acute hurdles linked to cold chain ruptures, falsified goods labeling, and sluggish product withdrawal operations, weakening both purchaser assurance and alignment with exacting food safety decrees [3-5].

Counterfeit maneuvers, such as the re-tagging of substandard frozen merchandise as top-shelf goods, magnify pre-existing loopholes and emphasize the immediate call for sturdy, manipulation-proof tracing and credentialing apparatuses. Orthodox tracing frameworks, still leaning on consolidated data stores and cyclical manual reviews, stand open to record

tampering, operator slip-ups, and procedural lags, obstructing the capacity to ensure instantaneous insight and alignment across dispersed chain participants [6, 7].

The rollout of Internet of Things (IoT) instrumentation has sharpened the live observation of crucial metrics like thermal state and moisture content while goods sit in depots or move along routes [8, 9]. Even so, the reliance on splintered informational backbones often chips away at the broad trustworthiness and inspectability of conformity archives. The appetite for a seamless answer that locks in the veracity, safeguarding, and on-the-spot retrievability of provenance and attestation records has therefore mounted unmistakably.

State agencies and oversight watchdogs lay down rigid conformity duties to shield the frozen edibles segment. Inside the European Union, Regulation (EC) No 178/2002 commands exhaustive trackability "from farm to fork" [10], while Regulation (EC) No 37/2005 spells out stipulations for thermal surveillance throughout the hauling, holding, and housing of quick-frozen consumables [11]. Across the Atlantic, the Food Safety Modernization Act (FSMA) enacts kindred imperatives, taking in round-the-clock temperature monitoring and swift incident flagging. Even so, current conformance validation routines stay overwhelmingly hand-operated, plodding, and wide open to data soundness flaws.

Distributed ledger technology holds out a hopeful route for tackling these constraints. Functioning as a dispersed, tamper-apparent chronicle, blockchain can steadfastly register unalterable conformance episodes among counterparties, locking in openness, trackability, and accountability. Autonomous programmable pacts (smart contracts) magnify this capability by permitting self-activating conformance checks keyed to live IoT data streams, stripping out the call for go-betweens [7, 8].

Whereas blockchain deployments for agri-food value networks have come under scrutiny in recent times, a great many rollouts are afflicted by coarse resolution, flimsy IoT linkage, constrained live-sensing scope, and scant heed to statutory conformance mechanization [3, 5]. Add to this the shortage of hands-on inquiries and systematic conceptual blueprints that home in on cold chain compliance certification for frozen provisions specifically, and a palpable hole in scholarly discourse stands exposed.

This inquiry steps into that hole by mapping out a blockchain-imbued structure that knits IoT-fed refrigeration oversight with Ethereum-grounded programmable pacts to mechanize provenance recording, credentialing, and conformance auditing workflows in frozen food conduits. Embracing the Design Science Research (DSR) method, this write-up spotlights the opening stretches of artefact construction, specifically, issue framing, aim crystallization, and opening system blueprinting. By proceeding this way, the exploration feeds into the conceptual conversation on blockchain-steered regulatory systems within agri-food arenas. In particular, it shapes a conceptual contraption anchored to compliance-steered design precepts, furnishing a template for how decentered technologies can stitch statutory reasoning straight into operative backbones. This addition stretches the available body of work by foregrounding not just chain-of-custody tracking but equally the robotization of credentialing operations inside conformance-dense settings.

The balance of this write-up unfolds as set out below. The following section surveys germane writings on blockchain-powered traceability throughout agri-food logistics webs. The subsequent section maps out the Design Science Research procedure steering this inquiry. The next section rolls out the posited abstract system construct, unpacking its stacked constituents and involved party parts. This is followed by a discussion of prospective onward inquiry. The final section finishes off by recapping central inputs and caveats.

Background

Distributed ledger systems have surfaced as a pivotal innovation for agri-food value chains, delivering protected, open, and tamper-resistant provenance mechanisms that tackle perennial obstacles such as adulteration, spoilage, procedural sluggishness, and statutory alignment [4, 5, 12]. Conventional supply network orchestration tools, built upon centralized databanks and paperwork-heavy recordkeeping, continue to be exposed to record falsification, cross-system friction, and slow-footed product removal procedures, especially when food safety crises erupt [3, 6]. Through the application of

decentralized ledger infrastructure, blockchain magnifies chain-wide clarity, guaranteeing that every actor—cultivators, processors, logistics providers, merchants, and end purchasers—can tap into a live, unalterable chronicle of commodity-linked movements [13]. Furthermore, weaving self-enforcing digital clauses with IoT-equipped sensory apparatus enables around-the-clock, automated conformance verification, permitting nonstop surveillance of thermal exposure, moisture content, and other decisive metrics for degradable consignments, thereby curbing spoilage and material waste [7, 8]. Research has also drawn attention to the technology's capability to speed up targeted recalls by enabling swift isolation and extraction of tainted or rule-violating lots from circulation, cutting down on health threats and fiscal fallout. Notwithstanding these merits, elevated computation demands, throughput constraints, and organizational inertia persist as formidable hindrances, particularly across lower-income regions where ledger-supporting digital fabric is thinner [14, 15]. That said, the rise of permissioned chain configurations and blended architectures that fine-tune consensus mechanics and power consumption is incrementally boosting blockchain's fit for expansive, cross-border agricultural conduits [2, 9].

Extending blockchain's capacity to heighten visibility and accountability in agri-food webs, self-executing code-based agreements reinforce these frameworks further by introducing mechanized rule enforcement, perpetual condition tracking, and tamper-immune fulfillment of cross-party obligations [1, 7, 8]. Operating as autonomous digital covenants hosted on a distributed ledger, these programmable contracts permit supply chain participants to encode and activate preset stipulations free from intermediary reliance, lifting both operational speed and stakeholder confidence [16, 17]. In refrigerated goods movement, such automated agreements can independently confirm whether temperature-sensitive cargoes, such as flash-frozen provisions, have been housed and moved within safe thresholds by assimilating feeds from environmental sensors and RFID markers [5, 13]. Should thermal excursions or rule transgressions surface, the contracts can autonomously fire off warnings, levy monetary disincentives, or initiate batch extractions, ensuring nonconforming items are stopped well before consumer contact [2, 9]. Additionally, these mechanisms pave the way for hassle-free regulatory scrutiny, since conformance logs sit indelibly etched on the chain for retrieval by oversight agencies, credentialing authorities, and quality verification bodies. Despite these advances, matters such as the juristic enforceability of digital covenants, harmonization across heterogeneous platforms, and processing overhead remain hurdles requiring resolution before widespread rollout across agri-food ecosystems becomes feasible [14, 15]. Even so, as ledger-based environments advance, the fusion of chain-of-custody architectures with mechanized contract logic bears substantial promise for raising food safety benchmarks, simplifying compliance workflows, and cementing accountability throughout worldwide agri-food networks [3, 4, 6].

While this contextual synthesis weaves together seminal works on distributed ledgers, conformance, and source-to-shelf visibility in agri-food webs, we recognize that it may fall short of capturing the full span of recent progress in this rapidly morphing domain. In upcoming phases, the intention is to deploy a more disciplined reviewing framework informed by Multivocal principles [18] that assimilates both peer-reviewed outputs and practitioner-generated material. Doing so will scaffold a more rounded picture of blockchain's operational deployments and statutory reverberations across a spectrum of food system settings.

Materials and Methods

This work applies the design science research (DSR) paradigm as the organizing framework for envisioning a blockchain-grounded trackability and attestation construct targeted at frozen food conduits. DSR represents a well-established methodological orientation for inquiries geared toward conceiving, engineering, and anchoring technological constructs inside actual-world problem landscapes, while simultaneously enriching the discipline's intellectual foundation [19–21]. It is particularly appropriate for socio-technical spheres like agri-food webs, where structural breakdowns, splintered information ecologies, and shifting conformance expectations necessitate meticulously architected and thoroughly rationalized digital interventions. Within the bounds of this study, DSR offers a systematic viewpoint for contending with pivotal traceability and conformance bottlenecks in frozen food logistics by formulating a blockchain-based system

blueprint. The methodology accommodates laying out the problem domain, crystallizing design ambitions, and producing a nascent solution in the shape of a conceptual construct.

The canonical DSR sequence comprises six interlinked undertakings, as detailed by Peffers *et al.* [21]. These undertakings include challenge recognition and rationale, specifying solution aims, blueprinting and construction, illustration, assessment, and dissemination (Figure 1). While these milestones are commonly depicted in linear succession, DSR does not impose a rigid step-by-step trajectory. Rather, it accommodates recurrent loops and phased advances aligned with the construct's stage of development and the investigation's purposes [19, 22]. Correspondingly, DSR sees increasing application in partitioned scholarly deliveries where individual publications may address selected portions of the full arc, especially when the primary goal is establishing bedrock design understanding or construct lucidity.

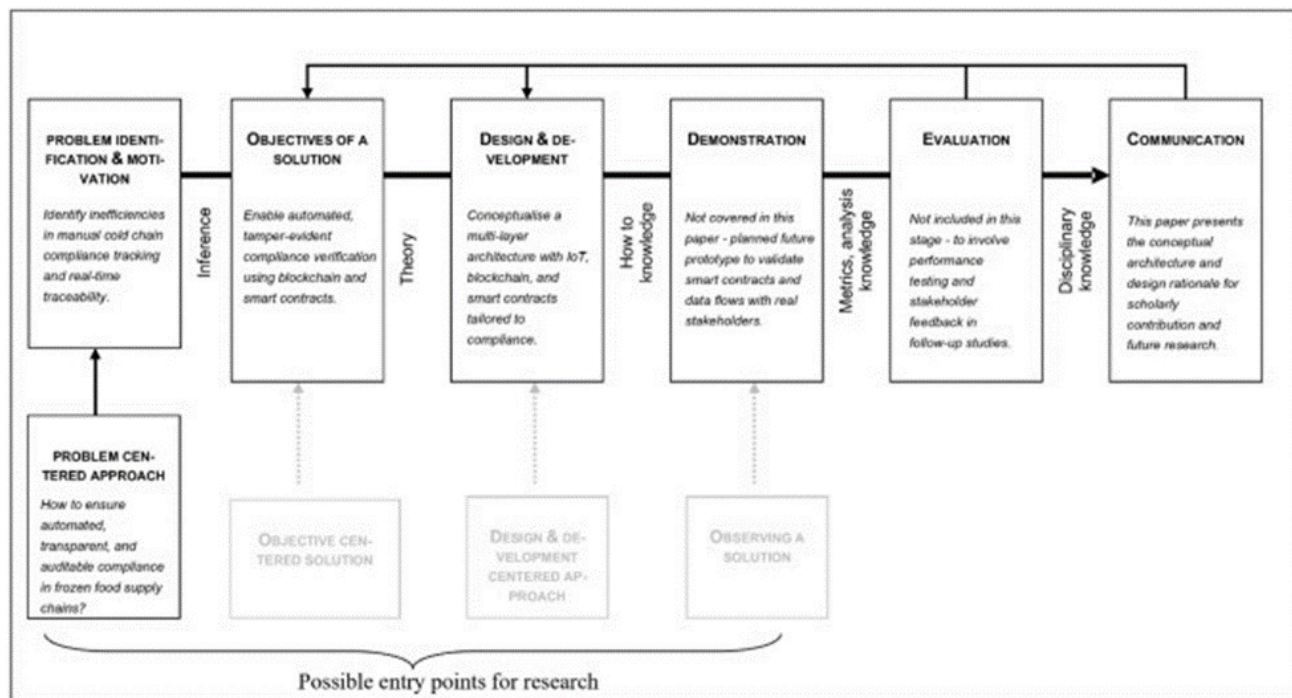


Figure 1. DC research process for the study (Adopted from Peffers *et al.* [21]).

The present investigation concentrates on the anterior stretches of the DSR arc, namely challenge recognition and rationale, enunciation of solution aims, and preliminary drafting of the envisaged system construct. These three undertakings delineate the boundaries of this research effort. The remaining milestones—illustration, assessment, and expansive dissemination—are postponed to later inquiries and forthcoming articles, consistent with conventions observed in staggered DSR outputs [22, 23]. The opening two undertakings are handled within the Introduction and Background segments of this manuscript, which catalogue the provenance and conformance snares in frozen provisions handling and sketch the central aims for the proposed blockchain-steered remedy and the deployment of programmable contracts. This arrangement is consonant with recognized DSR customs, where formal undertakings may be folded into standard academic partitions so long as their correspondence is articulated with clarity [19, 21].

Aligned with DSR tenets, this study operationalized the methodology by first surfacing the problem through substantiated friction points in refrigeration-chain conformance and source-to-shelf oversight, as covered in the Introduction and Background portions. Design targets—encompassing fortifying record veracity, enabling uninterrupted condition monitoring, and baking statutory reasoning into the system—were derived from the scholarly corpus and regulatory texts. These objectives steered the conceptual assembly of the system construct, which constitutes the artefact delivered at this

stage. While subsequent DSR stages such as illustration and assessment reside outside the remit of this paper, the disciplined advance from problem surfacing to construct conceptualization accords with the anterior arc of the DSR sequence.

Artefact description and design scope

The construct produced through this inquiry is a conceptual system blueprint for a blockchain-grounded provenance and credentialing remedy, custom-fitted to the operational and statutory demands of frozen food conduits. Its formulation sits within the DSR tradition, mirroring the cyclical and methodical progression of crafting constructs that remedy pinpointed issues while feeding back into scholarly discourse [19, 21].

The shaping process was steered by the imperative to close traceability fractures, unite splintered conformance records, and overcome the shortfall of mechanization in prevailing cold chain oversight setups [3, 5]. The construct envisions an authorized distributed ledger network that weaves together programmable pacts and IoT feeds to underpin live conformance tracking, record lineage, and occasion-triggered mechanization consonant with statutory benchmarks. Pulling from tenets of architectural formation in socio-technical arenas [22], the inquiry distils core functional imperatives sourced from both scholarly writings and documented refrigeration-chain sticking points.

The construct was shaped to meet three pivotal methodological aims. First, it secures end-to-end provenance across every link of the value web by enabling tamper-apparent inscription of vital occurrences (spanning origination to end distribution) onto a decentralized chronicle. Second, it eases the uptake of live data streams from dispersed IoT detection units (for instance, thermal and humidity loggers), a facet indispensable for upholding refrigeration integrity and statutory alignment. Third, it bakes compliance rule sets into Ethereum-backed programmable pacts, permitting hands-off vetting of environmental ceilings, the firing of warning signals, and the activation of pre-settled accords.

The architecture's formulation adhered to compartmentalization tenets habitually employed in blockchain system crafting. Concretely, functional realms like actor credential management, transaction orchestration, stock surveillance, and consignment standing were envisaged as detachable programmable pact units. This cleaving of concerns was meant to boost serviceability, enable role-anchored access governance, and mirror real-world job splitting among value web participants.

Aligned with the objective of gated entry and privacy-preserving conformance, the construct draws on the Hyperledger Besu client to undergird a closed Ethereum-compatible chain. It also folds in BlockScout as a chain browser, empowering sanctioned parties to observe transactions and validate conformance moves with openness. These design picks mirror both technical fitness and harmony with widespread conventions in enterprise-tier ledger deployments.

Notwithstanding that no working prototype has been built at this juncture, the conceptual construct embodies a methodologically ordered rejoinder to an unmistakably crystallized conformance snag in the frozen provisions segment. It will act as the substratum for ensuing rounds of illustration and appraisal, consonant with staged deliveries in DSR [23]. Through this course, the inquiry propels both the applied grasp of blockchain's part in statutory oversight and the conceptual bedrock of design-steered investigation into agri-food provenance frameworks.

Conceptual System Architecture

This portion lays out the conceptual system blueprint for a blockchain-anchored provenance and credentialing apparatus, architected to satisfy the hands-on and statutory exigencies of frozen food conduits. The moulding of this framework is navigated by the following central investigative query:

- 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 delve into this, the inquiry additionally probes three subsidiary queries:
- 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 central offering of this inquiry is the moulding of a conceptual system construct that unites live IoT sensing with distributed ledger technology and programmable pacts to buttress provenance and conformance. This portion delineates the system's makeup and pivotal constituents, answering squarely to the investigative queries and laying the groundwork for subsequent refinement and trialling. In particular, SRQ1 is tackled by pinpointing core provenance and conformance fissures remedied through the system design; SRQ2 finds expression in the design maxims embraced across the stacked strata; and SRQ3 receives its answer through the technical dissection of how IoT streams, programmable pacts, and stakeholder roles are operationalized.

The architecture sets out to remedy recurrent stumbling blocks in cold chain orchestration (for instance, thin trackability, disjointed records, and plodding manual vetting) by harnessing blockchain, linked sensory apparatus, and mechanized rule sets. It buttresses complete product shadowing, moment-by-moment condition sensing, and self-acting vetting keyed to codified thresholds and statutory stipulations. The system is moulded to align with precise regulatory mandates, among them:

- Uninterrupted temperature tracking consonant with Regulation (EC) No 37/2005, which stipulates that quick-frozen provisions must be held at -18°C or lower during conveyance, holding, and warehousing, with narrow allowable swings in the course of transport (capped at $+3^{\circ}\text{C}$).
- Complete provenance from point of origin to retail endpoint, as dictated by Regulation (EC) No 178/2002 ("from farm to fork").
- Tamper-apparent, inspection-ready conformance logs to facilitate oversight visits, examinations, and credentialing (for instance, HACCP, FSMA).
- Mechanization of conformance activation, lessening reliance on handwritten logs and manual inspection routines.

The architecture is arranged across three mutually dependent strata: (1) data acquisition layer, (2) data storage layer, and (3) application layer. A conceptual illustration of this architecture is suggested for embedding (**Figure 2**). The Data Acquisition stratum embodies groupings of sensing units that function in a dispersed fashion and amass all requisite readings at each juncture of the frozen food handling sequence. The Data Storage and Validation stratum constitutes the distributed ledger network along with the full set of its nodes (blocks). This stratum houses consensus protocols and rulesets (Proof of Stake, Proof of Authority, among others) that ratify every exchange inside the chain network. It warrants underscoring that within the remit of blockchain, an exchange denotes any transfer of information occurring between two distinct parties in the network. Lastly, the application stratum covers the envisioned programmable pacts together with the front-end interface, operating as the chief touchpoint bridging the ledger, IoT devices, and terminal operators. This stratum streamlines the carrying out of principal operations and orchestrates system warnings, guaranteeing fluid interaction and orchestration among all segments of the blueprint. It performs as the portal via which operators interface with the setup and where mechanized reactions (for instance, conformance vetting, alerts) are sparked in response to live data feeds. A key point of clarification is that while programmable pact operations are set in motion and engaged through the Application stratum, their actual dwelling place lies on the Data Storage stratum. This signifies that their program logic and conditions are deployed and held squarely within the chain.

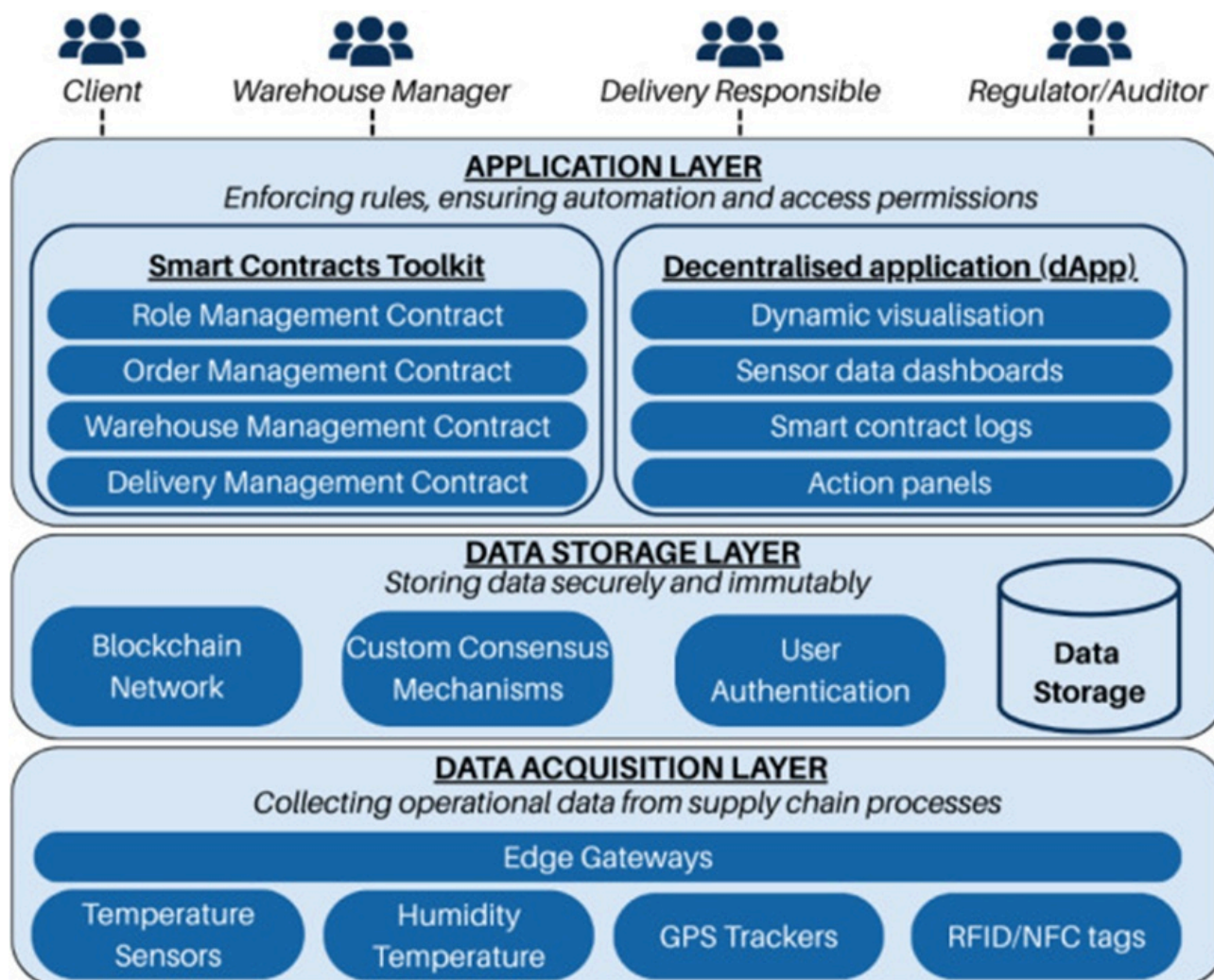


Figure 2. Proposed three-layer system architecture for blockchain-enabled cold chain compliance.

Data acquisition layer

The Data Acquisition stratum acts as the underpinning of the posited construct, allowing persistent, moment-by-moment tracking of ambient variables fundamental to the soundness and conformity of frozen provisions logistics. This stratum is made up of a web of purposefully placed IoT-equipped detectors and apparatuses that capture, pool, and relay measurements tied to thermal state, moisture, geolocation, and other conformity-salient factors throughout different links of the value web. This stratum speaks squarely to SRQ3 by facilitating IoT data intake and live ambient surveillance, constituting the technical substratum for provenance and conformity validation.

To buttress fine-grained ambient observation, the setup melds several detector varieties, among them:

- Cordless thermal detectors (for example, Bluetooth Low Energy (BLE), Zigbee-fitted units) for keeping tabs on surrounding and product-tier states within containers or refrigerated chambers.
- Dampness detectors to register moisture readings during warehousing and movement, capable of influencing product calibre and integrity.
- GPS trackers and RFID/NFC markers, inserted within pallets or consignment crates, to secure live positioning and item recognition.

- Edge aggregation hubs, tasked with local bundling and relay of sensor readings via shielded transmission conventions (for instance, MQTT or HTTPS).

These instruments are stationed at decisive oversight junctures along the supply web (such as processing plants, depots, chiller trucks, and retail cold cabinets). Every detector undergoes cryptographic enrolment on the chain, locking in tamper-proofing and source verifiability.

Detector nodes are set to register and relay readings at fixed cycles (for instance, once every 10 min), with prompt broadcast of aberrations that overshoot conformity ceilings (for example, thermal surges climbing past -15°C). Readings initially converge at local hubs, where opening vetting routines (such as signal soundness, time-marking, and outlier flagging) are carried out ahead of safe onward transmission to the chain network. This tactic trims bandwidth draw, safeguards chronological uniformity, and makes possible the early spotting of refrigeration ruptures or instrument faults. Hubs additionally shoulder the duty of sifting out duplicate signals, condensing data bundles, and applying digital signing procedures to uphold data genuineness.

The configuration of the Data Acquisition stratum explicitly meshes with legal benchmarks like EU Regulation (EC) No 37/2005, which prescribes unbroken logging of frozen edibles temperatures at -18°C with allowed drifts capped at 3°C while in transit. To this effect:

- Detectors come programmed with baked-in statutory thresholds for self-acting flagging of nonconforming states.
- Instruments trigger event-steered data capture upon sensing sharp ambient shifts.
- Every logged value carries a timestamp and digital signature, locking in traceability back to source and instant of capture.

Such provisions not only smooth the path for immediate counteraction to irregularities but also buttress after-the-fact corroboration during examinations or oversight visits, furnishing controllers and credentialing agencies with verifiable attestation of conformity. While the present blueprinting homes in on thermal, dampness, and geolocation indicators, onward iterations could fold in vibration detectors, CO_2 monitors, or light exposure loggers, paving the way for a fuller picture of item treatment and transit circumstances. Beyond that, linkage with on-chain oracles could permit live re-tuning of thresholds in step with refreshed legislative or weather-related mandates, strengthening agility.

Data storage layer

The Data Storage stratum forms the shielded, decentered spine of the posited setup, delivering unchangeable, tamper-evident housing for all conformity-salient information churned out by the Data Acquisition stratum. Its cardinal role lies in safeguarding the wholeness, retrievability, and inspectability of provenance chronicles spanning the entire frozen food value web. By drawing on an authorized distributed ledger fabric, this stratum strips away the call for middleman hubs, thus amplifying trustworthiness, trimming administrative drag, and sharpening regulatory nimbleness. This constituent feeds into both SRQ1 and SRQ3 by confronting data soundness and confidence snags inside traceability frameworks, while equally making possible the indelible logging of incidents for mechanized conformity oversight.

This blueprint marshals Hyperledger Besu as the subjacent chain client, owing to its harmony with Ethereum-grounded programmable pacts and its hardy accommodation of closed, permissioned webs. A permissioned configuration stands as indispensable within the sphere of conformity-critical food conduits, where informational discretion, finely sliced access governance, and operational siloing hold primacy. Hyperledger Besu delivers the following boons:

- Highly detailed permissioning for role-based admittance to chain records and actions.
- Enterprise-calibre stealth provisions, such as secluded transaction clusters.
- Ethereum virtual machine (EVM) backing, permitting the launching of bespoke programmable pacts encoding statutory reasoning.

- Extensive journaling and troubleshooting faculties are vital for error tracing, inspection trails, and stewardship reviews.

This arrangement certifies that value web participants can interface with the chain under preset access parameters, all the while keeping critical incident visibility intact.

Every exchange or incident inscribed on the chain lines up with a provenance milestone (for instance, request submission, stock handoff, receipt validation) or an ambient reading entry (such as a thermal overstep, detector breakdown). The informational scaffold for each exchange encompasses:

- Singular consignment and lot designators
- Detector unit tags and ambient readings (for instance, heat, dampness)
- Programmable pact action trails (such as conformity state shifts, mechanized moves)
- Role-anchored operator engagements (for example, stock amendments, request approvals).

This formulation guarantees that every pivotal juncture throughout the supply web lifespan receives chronological and unalterable documentation, equipping interested parties with a trustworthy bedrock of fact that aids both hands-on decision-making and statutory examinations.

To lift system scrutability, BlockScout is selected as the chain exploration portal. It empowers sanctioned entities to picture and cross-check chain entries, pact-driven occurrences, and sensor chronicles on the fly. This heightens inspection preparedness and shores up belief in the genuineness of conformity operations. The chain functions as an indelible information strongbox and inspection trail for conformity-linked episodes carried out by programmable pacts. It does not, by its own accord, appraise statutory ceilings or set off countermeasures; rather, it certifies that the yields of such activation (for instance, flags, verdicts, credentials) receive protected and perpetual archival.

In light of the heft and tempo of detector-spawned data inside cold chain surroundings, the blueprint likewise makes room for off-chain archival integration, where sprawling recordsets (such as raw thermal logs) may be lodged in shielded repositories (for instance, IPFS, cloud shelves), with matching fingerprints inked on-chain for cross-checking. This blended tack steadies expansibility against corroborability. To encapsulate, the chain stratum performs as a shielded, spread-out conformity backbone, tethering the confidence tier of the setup while buttressing mechanized activation and provenance. Its fusion with programmable pacts, inspection utilities, and permissioned stewardship apparatuses renders it a cornerstone constituent of the posited construct for refrigeration-chain credentialing.

Application layer

The Application stratum embodies the operational pinnacle of the posited construct, where technical components merge with statutory workflows and human participants. It activates conformance reasoning, steers stakeholder entitlements, and eases engagement via a user-facing portal. This stratum knits programmable pacts together with participant access governance, mechanizes inspection routines, and empowers users to interface with the setup in a shielded, role-bound fashion. Its central mission is to ensure that statutory mandates are not simply chronicled but proactively carried out through runnable code. This stratum dovetails with SRQ2 and SRQ3 by materializing compartmentalized programmable pacts and role-grounded stakeholder admittance, stitching conformance stipulations squarely into system workings.

Smart contracts for embedded compliance

Solidity-coded programmable pacts are set in motion on an authorized Ethereum-harmonized chain (Hyperledger Besu). These pacts crystallize statutory stipulations and procedural workflows into compartmentalized code blocks, paving the way for machine-driven provenance and credentialing.

Programmable pacts encode conformance sequences that would otherwise call for hands-on inspections, outside-party confirmations, or document-centered reporting. By way of illustration, pacts check whether thermal ceilings spelled out under EU Regulation (EC) No 37/2005 are maintained along the value web, leaning on IoT detector streams funnelled into the chain at fixed cadences. A solitary drift (for instance, a consignment lingering above -15°C for longer than 15 min) sets off mechanized sequences such as:

- Registering an infraction and forging an indelible conformance entry
- Suspending the consignment release or marking the shipment as tainted
- Pinging assigned overseers or quality supervisors through bundled warning channels

Beyond incident-triggered measures, programmable pacts likewise generate conformance credentials for batches that fulfil every provenance and ambient soundness stipulation. These credentials get etched on-chain, cryptographically tethered to the product's passage, and remain open to scrutiny by examiners or end purchasers.

Programmable pacts are sorted into four central modules:

1. Role management contract: Lays down role-anchored access governance (RBAC), dictating which parties may carry out which operations. It locks in stewardship layering, data safeguarding, and procedural lucidity. Role handover and withdrawal functions underpin expandability and alignment with internal guideline alterations.
2. Order management contract: Oversees the entire span of product order lifecycles, coupling each order with IoT feeds and corresponding events. It backs origination, vetting, amendment (by sanctioned operators), and time-marked finalization.
3. Warehouse management contract: Governs stock insight, dispatch preparedness, and storage conformance. Interlinks straightforwardly with ambient readings from holding facilities to obstruct the release of items falling short of credentialing benchmarks.
4. Delivery management contract: Shadows the movement of items following dispatch. It logs condition shifts (for example, 'In Transit', 'Delivered') and irregularities, furnishing digital attestation of receipt and ultimate conformance standing.

Each pact functions autonomously and inscribes its actions on the chain, putting in place a verifiable and spread-out activation tier. These apparatuses cut down clerical load, lift uniformity, and bring digital fabric into lockstep with food safety legislation.

Stakeholder role definition and operational mapping

The parts codified in this setup were pulled from earlier inquiries into role-based schemas within blockchain deployments. Part allocation meshes with well-settled blueprints in RBAC (Role-Based Access Control), where entitlements are fastened to parts rather than standalone operators, easing both rule rollout and safeguarding. This track mirrors leading conventions in Ethereum programmable pact engineering, where sloppily executed access governance has triggered grave security gaps [24]. To lock in a shielded and serviceable construct, parts were mapped onto programmable pact operations through compartmentalized pact architecture, abiding by tenets captured in structured RBAC formats like SC-RBAC [25, 26] foundational RBAC scaffold. These formats uphold the dictum of minimal privilege and permit traceable, part-specific dealings inside the chain arrangement. **Table 1** lays out the central parts codified within the posited system blueprint, their corresponding operational charges, and the linked programmable pact operations.

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

Role	Key responsibilities	Associated smart contract operations
Client	Submits product purchase requests and receives delivered products	Initiate orders and monitor compliance information
Warehouse manager	Oversees inventory levels and approves product dispatch activities	Modify inventory records and verify storage condition compliance
Delivery responsible	Records shipment progress and validates successful product delivery	Update shipment status and acknowledge product handover
Regulator/Auditor	Examines compliance records and validates audit procedures	Access smart contract event logs in read-only mode and produce audit documentation
Administrator	Oversees user roles and configures system settings	Grant role permissions and remove authorized access

Wallet-rooted identification certifies that only sanctioned operators holding specified parts may carry out actions, buttressing cryptographic accountability and aligning with data stewardship norms. All part designations, admittance alterations, and operational occurrences sit indelibly logged on the chain, yielding an inspectable and lucid chronicle reachable by entitled participants. This communal ledger nurtures reliance and accountability among parties without sacrificing informational discretion. Significantly, the Administrator part is shaped to be supple and setting-reliant. It does not stand for a centralized technical overseer commanding the entire chain web. Rather, it gets conferred upon a person or body charged with curating admittance authorizations inside the programmable pact framework, contingent on the stewardship configuration of the given rollout. This pliability lets the construct accommodate diverse commercial scenarios while upholding lucidity and inspectability via on-chain logs of part designations and deeds. This zero-trust safeguarding paradigm lines up with GDPR, FSMA, and overarching data stewardship maxims, vouchsafing exclusively authorized, trackable admittance.

Interfaces and usability considerations

To spur uptake and streamline engagement, the Application stratum incorporates a dispersed application (dApp) furnished with operator-specific panels. Front-ends are architected for reach via both browser and portable platforms and are built around live pact-driven happenings. Each front-end unit encompasses:

- Lively depiction of order and consignment condition
- Detector feed panels sporting warnings and past patterns
- Programmable pact chronicles rendered into plain inspection episodes (for instance, "Batch 37 certified compliant at 13:42 UTC")
- Action consoles (for example, dispatch clearance, delivery attestation, inspection launch) keyed to the operator's part

The front-end is shaped to be happening-responsive, reacting to shifts broadcast by programmable pacts (for instance, `OrderApproved`, `NonComplianceDetected`, `DeliveryConfirmed`). All dealings are chronicled and time-marked indelibly on-chain and rendered human-decipherable through BlockScout or tailored oversight displays. APIs stand ready to underpin outward linkages with heritage platforms (for instance, ERP, nationwide food safety ledgers).

Future Research

This inquiry lays out a conceptual blueprint for a blockchain-fuelled provenance and credentialing apparatus fitted to the precise statutory and operational hurdles of frozen food conduits. While the posited construct remedies several pivotal fissures in present-day provenance mechanics, above all regarding live conformance vetting, inspectability, and mechanization, several domains will be plumbed further in forthcoming inquiries.

To begin with, the undertaking stays at the conceptual and architectural drafting stage, lacking a fully realized prototype. Albeit the setup is architected atop established chain, IoT, and programmable pact know-how, hands-on trialling and showcasing stand as indispensable to corroborate its on-the-ground workability. Coming efforts will accordingly hone in on crafting a functioning prototype that materializes the conceptual mock-up, fusing live IoT data capture, pact-driven conformance vetting, and dispersed stakeholder front-ends.

Trialling and appraisal of the prototype will call for the spelling out of regimented performance yardsticks. What is more, stakeholder input will occupy a pivotal place in validating the setup's serviceability, dependability, and fit with the exigencies of cultivators, depot overseers, haulers, merchants, and controllers. An especially significant path for upcoming inquiry lies in stakeholder effect analysis, covering elements shaping operator uptake and the socio-technical hurdles of weaving dispersed frameworks into stringently governed, customarily guarded domains. Serviceability probes will be staged to harvest intelligence on the setup's adoption runway, sensed roadblocks, and prerequisites for additional honing. Although this inquiry furnishes a groundwork stride toward blockchain-driven conformance and provenance in frozen provisions logistics, ample labor remains to convert conceptual drafts into functioning, scalable, and broadly embraced remedies. The stumbling blocks of technical instantiation, operator buy-in, statutory endorsement, and commercial feasibility must all be methodically wrestled with in ensuing rounds of inquiry and advancement.

Conclusion

This inquiry put forward a conceptual blueprint for a blockchain-fuelled provenance and credentialing apparatus architected expressly for the frozen provisions value web, tackling pivotal sticking points tied to statutory alignment, refrigeration-chain soundness, and confidence among dispersed participants. By melding IoT-grounded live data capture, decentered chain-based recordkeeping, and programmable pact-steered conformity mechanization, the posited setup strives to lift the lucidity, dependability, and inspectability of cold chain workflows.

The construct dovetails tightly with cardinal statutory directives, such as EU Regulation (EC) No 178/2002 and Regulation (EC) No 37/2005, knitting conformance vetting straight into the technical undergirding of the supply web. Programmable pacts operate as standalone statutory agents, policing thermal boundary adherence, firing mechanized flags for infractions, and locking in indelible credentialing chronicles. Through authorized chain rollout and compartmentalized programmable pact structuring, the setup endeavours to harmonize openness, informational discretion, and operational expandability. These stand as indispensable ingredients for on-the-ground uptake across stringently overseen domains.

This inquiry feeds into the swelling corpus of scholarship on chain-enabled provenance by furnishing a regimented, conformity-anchored system construct fitted to the statutory and hands-on exigencies of frozen provisions logistics. Departing from numerous prevailing approaches that foreground trackability within generic agri-food settings, this undertaking zeroes in on mechanizing credentialing and conformance sequences through the fusion of IoT-based sensing and programmable pact reasoning. By converting intricate statutory stipulations into compartmentalized system constituents, the posited conceptual artefact delivers a design template for stitching regulatory reasoning squarely into digital backbones. In so doing, it stretches the written record not solely in the dimension of technical fusion but equally by foregrounding statutory mechanization inside conformance-dense milieus.

Past its applied import, the construct adds to design intelligence by charting conformance operations onto the chain and IoT faculties in an orderly fashion. This may stand as a referential template for subsequent system crafting undertakings across kindred overseen supply webs. Consequently, the artefact bolsters theory-formation tied to digital conformance backbones, above all within settings where mechanization, inspectability, and spread-out accountability hold primacy.

That said, akin to any conceptual drafting inquiry, this undertaking carries caveats. The construct has yet to be instantiated or corroborated within real-life settings, and its technical throughput, integration workability, and operator embrace stay untested. The present drafting likewise stops short of fully grappling with the juristic binding power of

programmable pacts, the unevenness in stakeholder digital preparedness, or the snarls of data cross-compatibility against entrenched heritage platforms.

In step with the looping character of the design science research approach, onward inquiries will centre on operationalizing the construct through prototype realization, hands-on trialling, and stakeholder immersion. These coming strides will aid in honing the artefact, redressing its present shortcomings, and gauging its practical fitness and expandability. As value webs mount in intricacy, the appetite for digitally policed, inspectable, and trustworthy provenance scaffolds is set to swell. This imperative holds not merely for quick-frozen edibles but also across other segments handling spoilable wares.

Acknowledgements

None

Conflict of interest

None

Financial support

None

Ethics statement

None

Received: 25 Sep 2022

Revised: 22 Oct 2022

Accepted: 13 Nov 2022

Published online: 15 March 2023

Rights and permissions

Open Access The author(s) retain copyright. This article is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. It may be shared and adapted for non-commercial purposes with appropriate attribution, an indication of changes, and distribution of adaptations under the same license. Third-party material may be subject to separate terms identified in its credit line. View the license at <https://creativecommons.org/licenses/by-nc-sa/4.0/>.

References

- Lin Q, Wang H, Pei X, Wang J. Food safety traceability system based on blockchain and EPCIS. *IEEE Access*. 2019;7:20698-707.
- Tsang YP, Choy KL, Wu CH, Ho GTS, Lam HY. Blockchain-driven IoT for food traceability with an integrated consensus mechanism. *IEEE Access*. 2019;7:129000-17.
- Galvez JF, Mejuto JC, Simal-Gandara J. Future challenges on the use of blockchain for food traceability analysis. *TrAC Trends Anal Chem*. 2018;107:222-32.

Kamilaris A, Fonts A, Prenafeta-Boldú FX. The rise of blockchain technology in agriculture and food supply chains. *Trends Food Sci Technol*. 2019;91:640-52.

Tian F. 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. p. 1-6.

Caro MP, Ali MS, Vecchio M, Giaffreda R. 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. p. 1-4.

Casino F, Dasaklis TK, Patsakis C. A systematic literature review of blockchain-based applications: current status, classification and open issues. *Telemat Inform*. 2019;36:55-81.

Kamble S, Gunasekaran A, Arha H. Understanding the blockchain technology adoption in supply chains-Indian context. *Int J Prod Res*. 2019;57(7):2009-33.

Ferrag MA, Derdour M, Mukherjee M, Derhab A, Maglaras L, Janicke H, et al. Blockchain technologies for the Internet of Things: research issues and challenges. *IEEE Internet Things J*. 2018;6(2):2188-204.

European Commission. Regulation (EC) No 178/2002 of the European parliament and of the council. *Off J Eur Communities*. 2002;L31:1-24.

European Commission. Regulation (EC) No 37/2005 of the European parliament and of the council. *Off J Eur Union*. 2005;L10:18-9.

Behnke K, Janssen MFWHA. Boundary conditions for traceability in food supply chains using blockchain technology. *Int J Inf Manag*. 2020;52:101969.

Feng H, Wang X, Duan Y, Zhang J, Zhang X. Applying blockchain technology to improve agri-food traceability: a review of development methods, benefits and challenges. *J Clean Prod*. 2020;260:121031.

Kouhizadeh M, Sarkis J. Blockchain practices, potentials and perspectives in greening supply chains. *Sustainability*. 2018;10(10):3652.

van Hilten M, Ongena G, Ravesteijn P. Blockchain for organic food traceability: case studies on drivers and challenges. *Frontiers in Blockchain*. 2020;3:567175.

Azzi R, Chamoun RK, Sokhn M. The power of a blockchain-based supply chain. *Comput Ind Eng*. 2019;135:582-92.

Christidis K, Devetsikiotis M. Blockchains and smart contracts for the Internet of Things. *IEEE Access*. 2016;4:2292-303.

Themistocleous M, Cunha P, Tabakis E, Papadaki M. Towards cross-border CBDC interoperability: insights from a multivocal literature review. *J Enterp Inf Manag*. 2023;36(5):1296-318.

Gregor S, Hevner AR. Positioning and presenting design science research for maximum impact. *MIS Q*. 2013;37(2):337-55.

Hevner AR, March ST, Park J, Ram S. Design science in information systems research. *MIS Q*. 2004;28(1):75-105.

Peffer K, Tuunanen T, Rothenberger MA, Chatterjee S. A design science research methodology for information systems research. *J Manag Inf Syst*. 2007;24(3):45-77.

Baskerville R, Baiyere A, Gregor S, Hevner A, Rossi M. Design science research contributions: finding a balance between artifact and theory. *J Assoc Inf Syst*. 2018;19(5):3.

Sein MK, Henfridsson O, Purao S, Rossi M, Lindgren R. Action design research. *MIS Q*. 2011;35(1):37-56.

Töberg JP, Schiff J, Reiche F, Beckert B, Heinrich R, Reussner R, et al. 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: IEEE; 2022. p. 38-47.

Ding Y, Jin J, Zhang J, Wu Z, Hu K. SC-RBAC: a smart contract based RBAC model for DApps. In: Milošević D, Tang Y, Zu Q, editors. Human Centered Computing. HCC 2019. Lecture Notes in Computer Science. Vol 11956. Cham: Springer; 2019.

Sandhu RS, Coyne EJ, Feinstein HL, Youman CE. Role-based access control models. *Computer*. 1996;29(2):38-47.