

Article

A DLT- and ZKP-Enabled Framework for Privacy-Preserving Digital Product Passports in Maritime Container Logistics

Samiullah Khairy¹ and Mariano Falcitelli^{2,*} 

¹ Telecommunications, Computer Engineering, and Photonics Institute (TeCIP), Scuola Superiore Sant'Anna, 56124 Pisa, Italy; samiullah.khairy@santannapisa.it

² Photonic Networks and Technologies National Laboratory (PNTLab), CNIT—National Inter-University Consortium for Telecommunications, 56124 Pisa, Italy

* Correspondence: mariano.falcitelli@cnit.it; Tel.: +39-050882283

Abstract

Background: Maritime container shipping carries over 80% of global trade, yet compliance verification creates a confidentiality–verifiability conflict: carriers treat telemetry as commercially sensitive, while regulators, insurers, and port authorities require verifiable proof that cargo remained within specification. The EU Ecodesign for Sustainable Products Regulation (ESPR) mandates Digital Product Passports (DPPs), but no standardised DPP architecture exists for the multi-stakeholder maritime domain. **Methods:** We present Ocean DPP, a blockchain-anchored platform combining GS1 EPCIS 2.0, oneM2M, IOTA, and Groth16 zero-knowledge proofs (ZKPs), letting stakeholders verify compliance predicates without revealing raw sensor values; Merkle-tree batching reduces anchoring costs. We evaluate it in 16 experiments on a single-host testbed using synthetic workloads and a local IOTA network. **Results:** The platform achieved 95th-percentile latency of 48 ms without ZKP and 500 ms with proof generation, throughput of 7 events/s per host, 304 ms mean proof generation and 9.8 ms verification, 100% EPCIS 2.0 compliance, and zero permanent message loss across four failure-injection scenarios; horizontal scaling reduced the median latency by 37%. **Conclusions:** To the best of our knowledge, Ocean DPP is the first implemented, quantitatively evaluated platform integrating EPCIS 2.0, oneM2M, IOTA, and Groth16 ZKPs for privacy-preserving maritime DPPs; broader multi-host and public-network validation remains for future work.

Keywords: digital product passport; distributed ledger technology; zero-knowledge proof; EPCIS 2.0; oneM2M; IOTA DLT; maritime logistics; container tracking devices; Groth16; supply chain traceability; EU-ESPR



Academic Editor: Amir Alizadeh

Received: 6 June 2026

Revised: 20 July 2026

Accepted: 30 July 2026

Published: 5 August 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

Maritime transport is the backbone of global commerce. According to the United Nations Conference on Trade and Development (UNCTAD), seaborne trade reached 12.7 billion tonnes in 2024, with containerised cargo alone exceeding 800 million twenty-foot equivalent units (TEUs) [1]. As containers traverse multiple jurisdictions, carriers, port authorities, and customs agencies, a fundamental challenge emerges: verifying that containers and their cargo complied with the applicable operational specifications (temperature limits, seal integrity, handling conditions, routing restrictions, and regulatory requirements) throughout the entire logistics chain. Logistics-chain failures encompass a wide spectrum of losses, from spoiled perishables and compromised pharmaceuticals to

regulatory non-compliance and insurance disputes. Cold-chain logistics failures remain a major global challenge, generating substantial economic losses through product spoilage, quality degradation, shelf-life reduction, regulatory non-compliance, recalls, and operational inefficiencies across food and pharmaceutical supply chains. Recent literature further highlights that inadequate monitoring, fragmented information flows, and insufficient end-to-end visibility continue to be key contributors to waste, sustainability impacts, and service disruption [2–4].

Against this backdrop, the European Union introduced Regulation (EU) 2024/1781, the Ecodesign for Sustainable Products Regulation (ESPR) [5], which establishes the legal framework for Digital Product Passports (DPPs), notably machine-readable digital records that accompany a product through its entire lifecycle. The first mandatory DPP implementation, the Battery Passport under Regulation (EU) 2023/1542 [6], becomes compulsory from 18 February 2027. The ESPR Working Plan 2025–2030 [7] identifies eleven further priority product categories and anticipates approximately thirty regulated product families by the end of the decade. The ESPR applies to products rather than to transport operations; its relevance to maritime container logistics is, therefore, indirect but concrete. First, the regulated products themselves move through containerised transport: a battery passport that must remain “accurate, complete and up to date” throughout the product lifecycle cannot ignore the weeks the product spends at sea, where temperature, humidity, and handling events bear directly on regulated attributes such as safety and state of health. Second, the ESPR’s decentralised data architecture expects lifecycle data to be contributed by the distributed actors that hold it; during transit, that actor is the carrier. A container-level passport that records and verifies in-transit conditions is thus the natural mechanism by which the transport leg supplies the product passports of the goods inside, and it is this transport-side gap that Ocean DPP addresses.

Maritime container logistics (the physical layer that moves these regulated products across continents) has no standardised DPP implementation yet. Existing DPP initiatives (Catena-X for automotive [8]; the EU Battery Passport; the textile DPP under preparation) all target manufactured goods with a single dominant data owner. Maritime container shipping is structurally different: it is multi-stakeholder (8–15 independent parties per container shipment [1]) and event-driven, may face severe bandwidth and latency constraints when cellular Non-Terrestrial Network (NTN) communication is used, and requires continuous compliance verification in transit rather than point-in-time declarations.

1.1. The Privacy Paradox

Consider a container in transit carrying regulated cargo (pharmaceuticals, hazardous materials, or high-value goods) subject to specific handling requirements enforced by customs authorities at both the origin and destination ports. Regulators require verifiable proof that the container remained compliant throughout the logistics chain: correct environmental conditions, unbroken seal integrity, authorised routing, and timely event reporting. The carrier, however, regards the precise operational telemetry as commercially sensitive, since it reveals voyage routes, loading patterns, dwell times, and compliance history that competitors and customers could exploit in contract negotiations. Under a conventional data-sharing model, satisfying the compliance requirement forces raw telemetry disclosure; withholding the data makes independent verification impossible. We term this the “maritime privacy paradox” and note that it applies equally to every category of regulated cargo (not only temperature-sensitive goods). Explicitly defined, the maritime privacy paradox is the condition in which no level of raw-data disclosure simultaneously satisfies the carrier’s confidentiality requirement and the external stakeholders’ verification requirement: any disclosure sufficient for independent verification exposes commercially

sensitive operations, and any withholding sufficient to protect them defeats verification. The term is introduced in this paper as a convenient name for the maritime instance of the broader, well-documented tension between verifiability and confidentiality in supply-chain data sharing; the concept itself is not claimed as new, and our contribution lies in resolving it for container logistics through zero-knowledge verification.

Existing systems offer only two options: disclose raw data (verifiable but confidentiality-violating) or issue self-declared compliance flags (private but unverifiable). Zero-knowledge proofs (ZKPs) [9] provide the theoretical resolution: they allow a prover to convince a verifier that a statement is true without revealing any information beyond the truth of the statement. A ZKP-based compliance check lets the carrier prove “a monitored parameter satisfied its declared threshold” without disclosing the underlying sensor readings.

1.2. Contributions

This paper presents “Ocean DPP”, a blockchain-anchored DPP platform that resolves the maritime privacy paradox. The principal contributions are:

- C1. Ocean DPP Architecture. A novel multi-service, standards-compliant event pipeline for maritime DPP, integrating GS1 Electronic Product Code Information Services (EPCIS) 2.0, oneM2M, and GS1 Core Business Vocabulary (CBV) 2.0 canonical event hashing.
- C2. ZKP–EPCIS Integration. Groth16 proof generation embedded directly in the EPCIS enrichment pipeline, with verification key pinning and a browser-side WebAssembly (WASM) verification portal (to the best of our knowledge, the first implemented and quantitatively evaluated integration of ZKPs with EPCIS 2.0 for maritime DPPs).
- C3. IOTA Merkle Batch Anchoring. An event-batching algorithm demonstrating 90–99% reduction in on-chain transaction count while preserving per-event tamper evidence via Merkle inclusion proofs.
- C4. Comprehensive Quantitative Evaluation. Sixteen experiments covering performance, ZKP characterisation, scalability, IOTA anchoring, data quality, and reliability.

The six compounding gaps of Section 2.7 share one unresolved question: the zero-knowledge resolution of the privacy paradox is theoretically sound, but it is not established, to the best of our knowledge, whether it can be realised as a working, standards-compliant maritime DPP pipeline at a latency, throughput, and anchoring cost acceptable for operational container logistics. The central research question of this paper is, therefore: *can a privacy-preserving, standards-compliant DPP framework deliver independently verifiable maritime compliance without disclosing commercially sensitive telemetry, at a performance and cost acceptable for container-logistics operation?* We decompose this question into four research questions, each answered in Section 5 with the inferential statistics reported there:

- RQ1. Pipeline performance. To what extent can the event pipeline ingest, enrich, and persist EPCIS 2.0 events within the latency and throughput bounds required by maritime Internet of Things (IoT) telemetry, and what single-host throughput ceiling is achievable?
- RQ2. ZKP overhead. What is the quantitative cost of embedding Groth16 proof generation and verification in the pipeline, and is it operationally acceptable given maritime event intervals?
- RQ3. IOTA anchoring. To what extent does Merkle batch anchoring reduce on-chain transaction count while preserving per-event tamper evidence, and at what batching trade-off?
- RQ4. Reliability. Under what failure and load conditions does the hybrid messaging architecture preserve every event without loss?

The remainder of the paper is organised as follows. Section 2 reviews foundational technologies and related work. Section 3 presents the system architecture and threat model. Section 4 describes the implementation. Section 5 reports experimental results. Section 6 discusses findings. Section 7 concludes.

This article builds upon and extends the first author's M.Sc. thesis at the University of Pisa [10], condensing and reframing the platform design and experimental evaluation for the journal context.

2. Background and Related Work

2.1. Digital Product Passports and the EU ESPR Mandate

A DPP is a structured, machine-readable digital record that accompanies a product through its entire lifecycle. The ESPR [5] (Article 12) requires DPP data to be “accurate, complete and up to date” and mandates access on a need-to-know basis, explicitly requiring the balancing of transparency with protection of business-sensitive data. The ESPR establishes a decentralised data architecture: product data remains distributed across trusted actors rather than in a single EU-wide database, accessible via a standardised digital identifier linked to a data carrier.

Maritime container logistics presents unique DPP challenges absent from existing frameworks. A single container shipment involves 8–15 independent stakeholders generating continuous high-frequency telemetry across weeks of transit. The DPP must capture dynamic sensor events (temperature, humidity, Global Positioning System (GPS) position, shock, seal status) and support real-time compliance verification in transit, rather than the point-in-time declarations that manufactured-goods DPP architectures provide.

Crucially, a standardised “Digital Cargo Passport” (a DPP specifically designed to record and verify events occurring during containerised transport) does not yet exist. Existing DPP specifications address the product at manufacture or end-of-life, but the in-transit lifecycle of an intermodal container, spanning multiple carriers, ports, and jurisdictions, has not been standardised from a data model perspective. This work proposes an initial container DPP data model, structured as an eight-section EPCIS 2.0 event record compliant with GS1 and oneM2M industry standards, and populated by events generated by Container Tracking Devices (CTDs) that are beginning to be deployed at scale thanks to the convergence of 5G cellular technology and low-cost Narrowband IoT (NB-IoT) NTN satellite connectivity [11–13]. This technological convergence is a key enabler: NB-IoT NTN links make it economically viable for the first time to equip the entire global dry-container fleet with real-time IoT sensing and event reporting, creating the data foundation that container DPPs require. To the best of the authors' knowledge, no existing DPP framework has been designed for or evaluated in this multi-stakeholder, event-driven maritime context.

2.2. GS1 EPCIS 2.0 Standard

The Electronic Product Code Information Services (EPCIS) standard, published as International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 19987 and maintained by GS1, is the flagship data-sharing standard for supply-chain visibility [14]. Each EPCIS event answers five dimensions: *what* (identified objects), *when* (timestamp), *where* (read point and business location), *why* (business step and disposition), and *how* (sensor data).

EPCIS 2.0 (released June 2022) introduces JavaScript Object Notation (JSON) and JSON for Linked Data (JSON-LD) serialisation, a Representational State Transfer (REST) Application Programming Interface (API) replacing legacy Simple Object Access Protocol (SOAP) interfaces, GS1 Digital Link Uniform Resource Identifier (URI) syntax for product identifiers, and sensor data extensions for timestamped measurement series. The com-

panion GS1 Core Business Vocabulary (CBV) 2.0 [15] (ISO/IEC 19988) defines a canonical event hashing algorithm (§8.9.2) that produces a deterministic, interoperable Secure Hash Algorithm 256 (SHA-256) digest from semantically significant event fields only (ensuring that any EPCIS-compliant system can independently verify an anchored event regardless of serialisation format or field ordering). The framework standardises on EPCIS 2.0 JSON/JSON-LD serialisation for cross-vendor interoperability, which is a primary design objective; payload compression is an orthogonal transport-layer concern (e.g., Hypertext Transfer Protocol (HTTP)- or Message Queuing Telemetry Transport (MQTT)-level deflate) that does not alter the document model, and because the canonical CBV digest is computed over semantic fields independently of serialisation, on-chain verification is unaffected by the encoding chosen. The transmission-critical artefact for constrained satellite uplinks is the compliance proof, which Groth16 already keeps compact (≈ 850 bytes, two orders of magnitude smaller than a STARK). A byte-level comparison of JSON against a compressed binary encoding such as Concise Binary Object Representation (CBOR) is left to future work.

2.3. *oneM2M IoT Platform Standard*

oneM2M is a global standardisation initiative for the Internet of Things, aimed at providing a common horizontal middleware layer between devices, networks, and applications [16]. Its functional architecture defines Application Entities (AEs), a Common Services Entity (CSE) responsible for data management and access control, and a hierarchical resource tree rooted at the CSEBase. Furthermore, the standard defines a broad set of Common Service Functions (CSFs) that provide support for core IoT functionalities, such as data handling, security enforcement, device lifecycle management, resource discovery, group management, location services, subscription and notification mechanisms, application provisioning, and charging capabilities [17]. Core resource types include `<container>`, representing logical groupings of data, and `<contentInstance>` (CIN), representing individual data records, while Access Control Policies (ACPs) regulate fine-grained permissions at the resource level.

Beyond the representation of physical devices and software agents, oneM2M supports the abstraction and composition of resources, enabling the creation of virtual AEs that combine the semantics of multiple real AEs. This capability allows the modelling of higher-level digital entities through semantic aggregation mechanisms. In this context, the Digital Product Passport associated with a container can be naturally modelled as an AE within the oneM2M framework, allowing it to be managed, queried, and semantically linked to heterogeneous applications and stakeholders across the logistics value chain.

A key advantage of adopting oneM2M lies in the mitigation of technological lock-in, due to its status as a globally recognised open standard and the availability of open-source implementations. Notably, platforms such as Mobius, developed by KETI and released under a permissive BSD-3-Clause license, provide practical and extensible oneM2M-compliant CSE implementations that can be readily integrated into advanced IoT systems [18]. The standard's CSF-based architecture has also been demonstrated to provide a natural integration surface for distributed ledger technologies: Lee et al. [19] propose a Blockchain Interworking Proxy Entity (BlockIPE) that maps oneM2M CSFs—including data management, security, and device management—to smart contracts on a permissioned ledger, empirically validating that blockchain anchoring can be embedded within a standards-compliant oneM2M platform with modest proxy-level overhead.

2.4. Container Tracking Devices as IoT Event Sources for DPPs

A Container Tracking Device (CTD) is a battery-powered, multi-sensor unit affixed to an ISO 668 [20] intermodal container that continuously acquires environmental and positional telemetry (temperature, humidity, pressure, shock, e-seal status, and Global Navigation Satellite System (GNSS) coordinates) and transmits it to a backend service platform over one or more wireless links [21]. CTDs are the primary physical source of the IoT events that populate a maritime DPP: every EPCIS ObjectEvent recording a sensor observation ultimately originates from data published by a CTD. This layering also clarifies how Ocean DPP relates to the mainstream maritime standards that govern the container and the voyage. The technical committee ISO TC 104 standardises the physical intermodal container (dimensions, identification, and handling, e.g., ISO 668 [20]), and International Maritime Organization (IMO) instruments regulate voyage and cargo safety (e.g., International Convention for the Safety of Life at Sea (SOLAS) verified-gross-mass and dangerous-goods requirements). Ocean DPP is complementary to, rather than competing with, these standards: it operates at the data and compliance-passport layer above them, recording, privacy-protecting, and verifiably anchoring the telemetry generated within containers governed by those standards, and it reuses the standardised physical-container identity rather than redefining it. Formal alignment with ISO TC 104 and IMO digital standardisation is pursued as future work (Section 6.6).

Despite carrying more than 80% of world merchandise trade, the vast majority of intermodal containers remain unequipped with real-time electronic monitoring. Where containers are digitally tagged today, the prevailing technologies are static auto-identification carriers—barcodes and radio-frequency identification (RFID)/near-field communication (NFC) tags—that identify which container or consignment is present but neither sense in-transit conditions nor attest to compliance; they answer “what is this?” rather than “did it stay within specification?”. Ocean DPP differs on both axes: it ingests real-time environmental telemetry from container tracking devices and, through zero-knowledge proofs, lets external parties verify compliance predicates without exposing the underlying readings—capabilities that passive auto-ID tags do not provide. Any universal smart container technology viable for the dry-container fleet must satisfy five stringent constraints: low unit cost, global connectivity, easy installation and maintenance, reliable communication in all stacking situations, and operation from long-lasting batteries [11].

2.4.1. CTD Hardware Architecture

Falcitelli et al. [11] described the design, development, and verification of a prototype CTD developed within the European Space Agency (ESA)-funded 5G SENSOR@SEA project. The device integrates three radio interfaces: NB-IoT for direct uplink to on-board cellular small cells or terrestrial network base stations; Bluetooth Low Energy (BLE) Mesh for forming intra-stack relay networks when NB-IoT coverage reaches only the topmost container in a stack; and GNSS for position acquisition. The stacking topology of containers on ships (typically up to five high) motivated the BLE Mesh design, in which the CTD at the apex of each stack serves as the NB-IoT gateway for the underlying nodes. The prototype was verified in laboratory conditions against relevant ISO and 3rd Generation Partnership Project (3GPP) specifications.

2.4.2. Full-Scale System Assessment

The marine-grade implementation of these devices was subsequently integrated into the complete 5GT System (5G Global Tracking System) and assessed end-to-end in an operational environment by Falcitelli et al. [12]. In addition to the CTDs, the 5GT System encompasses an NB-IoT on-board cellular network with a Ku-band geostationary

Earth orbit (GEO)-satellite-optimised backhauling link, shore-side satellite terminals, and a maritime service platform built on the oneM2M standard. Field trials were conducted on transcontinental liner container ships operated by Ignazio Messina & C. SpA, with involvement from the Port Authorities of the Northern Tyrrhenian and Eastern Adriatic Seas and the satellite operator Eutelsat, confirming correct end-to-end data flow from CTD sensors through the NB-IoT/satellite link to the oneM2M CSE under real open-sea conditions.

2.4.3. IoT Data Format Constraints and Satellite Link Efficiency

Building on the full-scale system assessment described in Section 2.4.2, the next evolutionary step of the CTD is the integration of cellular modems compliant with 3GPP Release 17 and later standards, enabling Non-Terrestrial Network (NTN) connectivity and direct transmission to GEO and low Earth orbit (LEO) satellites [22,23]. This evolution is consistent with ongoing validation efforts such as the LOGICA project [23], which targets integrated real-time monitoring and tracking for multimodal containerised shipments and includes direct satellite communication technologies as well as operational Technology Readiness Level (TRL) 7 prototyping. In this configuration, the CTD is no longer limited to acting as a telemetry source for terrestrial or hybrid systems with satellite backhauling but becomes a natively NTN-capable communication node, significantly extending coverage and service continuity across maritime and intermodal transport routes.

This evolution directly addresses a critical operational constraint for CTD deployments over satellite IoT links: the strict message-size limit imposed by commercial satellite operators, with many LEO and GEO satellite IoT services permitting payloads of only approximately 160 bytes per uplink message. Standard IoT data formats such as JSON, which underpin EPCIS 2.0 event serialisation, are inherently verbose and can easily exceed this threshold. Kumar et al. [13] addressed this bottleneck by studying efficient data encoding strategies for machine-to-machine (M2M) systems tracking and monitoring multimodal dry containers in hybrid terrestrial/non-terrestrial networks (TN/NTN), demonstrating compact binary representations that preserve semantic content while remaining within satellite bandwidth constraints.

Within Ocean DPP, this tension is resolved by decoupling the on-device transmission format, which must remain compact and link-efficient, from the full EPCIS 2.0 representation reconstructed on the terrestrial side by the Translator service. In this way, standards compliance is achieved without requiring CTDs to transmit complete EPCIS payloads over bandwidth-constrained satellite channels. The CTD, therefore, remains the upstream boundary of the event-generation pipeline: each sensor reading published by the device to the oneM2M platform is transformed, once terrestrial connectivity is reached, into a GS1 EPCIS 2.0 ObjectEvent enriched with its associated Groth16 compliance proof.

2.5. DLTs for DPP

Recent research has increasingly explored Distributed Ledger Technologies (DLTs) as a foundational infrastructure for Digital Product Passports, particularly in contexts requiring trusted data sharing across multiple stakeholders. Hulea et al. [24] propose a multi-blockchain architecture integrating decentralised identifiers for product traceability, while Abreu et al. [25] develop a blockchain-based DPP framework for the textile sector, highlighting design principles for lifecycle data management. Similarly, Xia et al. [26] investigate the integration of DPPs with blockchain-enabled reverse supply chains, and Neri et al. [27] analyse DLT selection criteria for battery passport systems. Collectively, these works suggest that DLTs can provide a tamper-evident and auditable layer for managing product-related data across distributed value chains.

DLTs can be broadly categorised into permissioned and permissionless systems, each with distinct implications for DPP deployment. Permissioned frameworks such as Hyperledger Fabric [28] offer controlled access, identity management, and high configurability, making them suitable for consortia-based environments with well-defined governance structures. However, their adoption in large-scale, open logistics ecosystems may be constrained by governance complexity and onboarding requirements. The discontinuation of TradeLens, a blockchain-based trade platform developed by Maersk and IBM, illustrates the challenges associated with achieving sufficient ecosystem-wide participation and long-term sustainability in permissioned settings [29].

In contrast, permissionless DLTs provide open participation models and reduced coordination overhead, which may be advantageous in heterogeneous and loosely coupled supply chains. Among these, IOTA has been specifically positioned for IoT and logistics applications [30]. Its architecture is designed to support scalable and low-cost data anchoring, and recent protocol developments introduce object-based data structures and native smart contract capabilities. According to the IOTA Foundation, the platform targets high throughput (on the order of 10^4 – 10^5 transactions per second) and sub-second finality, while maintaining minimal transaction fees [31].

As reported in Table 1, the main design trade-off concerns the balance between governance control, interoperability, and marginal anchoring cost. The cost comparison should be interpreted qualitatively, since most sources report protocol-level fees and infrastructure characteristics rather than a deployment-specific total cost of ownership.

Table 1. Comparison of DLT paradigms against key Digital Product Passport (DPP) requirements.

Requirement	Permissioned DLT	Permissionless DLT	Implication
Integrity	Controlled consensus [24]	Distributed cryptographic anchoring [32]	Both ensure tamper-evidence; governance model is the key differentiator
Access control	Native identity-based policies [28]	Application-layer (encryption, off-chain)	Permissioned preferred for regulated access; permissionless for cross-domain sharing
Interoperability	Requires consortium onboarding [29]	Open participation model [30]	Permissionless reduces integration friction in heterogeneous ecosystems
Scalability	High in controlled environments	High in open networks (e.g., IOTA targets high throughput) [31]	Relevant for large-scale DPP event streams
Cost	No tx fees; higher infra/governance cost [29]	Low per-tx cost (e.g., IOTA) [32]	Trade-off between fixed (consortium) and marginal (transaction) cost
Logistics fit	Effective in stable consortia	Adopted in open trade initiatives (TLIP, TWIN) [33–35]	Permissionless better suited for cross-border, multi-actor DPP scenarios

A relevant feature for DPP implementation is the support for notarisation mechanisms, enabling the creation of immutable on-chain records that can be used to anchor off-chain data [32]. This approach allows large DPP datasets (e.g., product lifecycle information, certifications, sensor data) to remain off-chain while ensuring their integrity through cryptographic commitments stored on the ledger. Such a hybrid architecture is consistent with emerging best practices in DLT-based data management.

From an application perspective, IOTA has been adopted in logistics-oriented initiatives such as the Trade and Logistics Information Pipeline (TLIP) and TWIN, which aim to facilitate trusted data exchange across international supply chains [33–35]. These implementations highlight the potential of DLTs to support interoperability among diverse actors, including manufacturers, logistics providers, customs authorities, and recycling operators.

Overall, the choice of DLT for DPP systems should be understood as context-dependent. Permissioned platforms may be preferable in regulated or consortium-driven

environments, whereas permissionless solutions such as IOTA may offer advantages in terms of openness, scalability, and reduced integration friction in cross-organisational ecosystems. These considerations are particularly relevant for DPP scenarios, where data must be shared across organisational boundaries while preserving integrity, transparency, and long-term accessibility.

2.6. Groth16 Zero-Knowledge Proofs

In practical terms, a ZKP lets the carrier publish a compact cryptographic receipt demonstrating that a hidden sensor reading satisfied a declared compliance limit; any stakeholder can check the receipt without learning the reading itself. Groth16 is the proof system adopted for this purpose in Ocean DPP. Groth16 [9] is the most compact zero-knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK), producing proofs consisting of three elliptic-curve points (≈ 850 bytes in JSON serialisation). It requires a structured reference string (SRS) produced by a trusted setup ceremony, a one-time public procedure that generates the scheme's common cryptographic parameters. ZKP circuits are expressed as Rank-1 Constraint Systems (R1CS) using the Circom language [36], compiled and executed via the snarkjs library [37]. Three properties (completeness, soundness, and zero-knowledge) guarantee that a valid proof attests to a true statement while revealing nothing beyond that binary truth.

2.7. Related Work and Research Gaps

Table 2 situates Ocean DPP against the most relevant existing systems. Catena-X [8] addresses automotive DPPs using Eclipse Dataspace Connectors but employs proprietary aspect models rather than EPCIS 2.0 and includes no ZKP capability. IBM Food Trust [38], deployed on Hyperledger Fabric, uses proprietary data formats with no privacy-preserving mechanism and no DPP semantics. TradeLens [29], a Hyperledger Fabric deployment for maritime documentation, was shut down in November 2022 due to insufficient adoption; it provided no ZKP capability and no EPCIS integration. VeChain [39] targets luxury goods and pharmaceuticals with a proprietary event format and no ZKP. A systematic review by Silveirinha et al. [40] of 40 articles on ZKP applications in maritime blockchain systems confirmed that no implemented, quantitatively evaluated ZKP system for maritime supply chains existed in the surveyed literature.

Table 2. Comparison of Digital Product Passport and supply-chain traceability systems. ZKP = zero-knowledge proof; EPCIS = EPCIS 2.0 compliance; Eval. = quantitative evaluation published.

System	Domain	DLT	ZKP	EPCIS	Eval.
Catena-X [8]	Automotive	None ^a	No	No	None
EU Battery Passport [6]	Batteries	—	No	No	None
IBM Food Trust [38]	Food	Hyperledger	No	No	Limited
TradeLens [29]	Shipping	Hyperledger	No	No	None
VeChain [39]	Luxury/ Pharma	VeChainThor	No	No	Limited
Ocean DPP (this work)	Maritime	IOTA	Yes	Yes	Yes (16 exp.)

^a Catena-X uses Eclipse Dataspace Connectors for sovereign data exchange; it does not use a blockchain for DPP anchoring.

Six compounding research gaps motivate this work. To the best of our knowledge, in the surveyed literature: (1) no standardised maritime container DPP implementation exists; (2) no ZKP system for maritime supply chains has been implemented and empirically evaluated; (3) no prior work integrates ZKPs with EPCIS 2.0; (4) no DPP addresses the container logistics-chain privacy paradox; (5) IOTA's IoT-targeted architecture has not been evaluated for DPP anchoring with Merkle batching; and (6) few DPP plat-

forms report a rigorous quantitative performance evaluation. Ocean DPP addresses all six gaps simultaneously.

3. System Design and Architecture

3.1. Stakeholder Analysis

Ocean DPP serves five stakeholder categories with distinct and competing data requirements (Table 3). Container operators (carriers) own the sensors and require unrestricted access to raw telemetry for operational decisions; the full sensor stream is commercially sensitive for the reasons set out in Section 1.1. External verifiers (customs, insurers, port authorities) require independently verifiable proof of logistics-chain compliance but have no lawful need for the underlying sensor stream. All three verifier categories are satisfied by the same cryptographic artefact: a Groth16 proof attesting that a monitored parameter satisfied its declared compliance predicate, anchored to an immutable IOTA record. Logistics partners contribute EPCIS events for handling, customs clearance, and port operations via a dedicated External AE write path with container-scoped access control.

A conventional system can satisfy either requirement (full disclosure or binary self-declared flags) but not both simultaneously. Zero-knowledge proofs resolve this deadlock: they produce a statement that is both independently verifiable and perfectly zero-knowledge.

Table 3. Stakeholder data access requirements. ✓ = access granted; × = access withheld.

Stakeholder	Role	Compliance Proof	Raw Sensor Data
Carrier	Data owner and operator	✓	✓
Customs Authority	Regulatory verifier	✓	×
Insurance Underwriter	Claims auditor	✓	×
Port Authority	Entry/exit clearance	✓	×
Logistics Partner	External event contributor	✓	Scoped only

3.2. High-Level Architecture

Figure 1 illustrates the Ocean DPP platform. The complete data path from IoT sensor to blockchain anchor passes through seven loosely coupled components: the IoT data source (CTD), RabbitMQ message broker, Translator, Mobius4 CSE (oneM2M), DPP Core (with inline ZKP and IOTA anchoring modules), API Gateway, and Dashboard with public verification portal.

The key architectural decisions are as follows.

Hybrid messaging (RabbitMQ over oneM2M notifications). The internal event pipeline uses RabbitMQ Advanced Message Queuing Protocol (AMQP) rather than oneM2M HTTP subscriptions. oneM2M notifications are best-effort HTTP POSTs that are lost when a subscriber is unavailable. RabbitMQ provides AMQP acknowledgements, durable queues, per-message persistence, and a Dead Letter Queue (DLQ), satisfying a 30-min. outage-tolerance requirement.

IOTA Locked Notarisation with Merkle batching. Raw event data is never written to any public ledger; only a SHA-256 digest (or a ZKP proof hash) is anchored. Merkle batching reduces the IOTA transaction count proportionally to batch size while per-event integrity remains verifiable via stored sibling proofs.

Groth16 over alternative ZKP systems. Groth16 was selected for its ≈850-byte proof size, two orders of magnitude smaller than an equivalent STARK (≈50 KB), making it suited for maritime satellite uplinks where per-byte transmission costs are significant.

GS1 CBV 2.0 canonical event hashing. The hash is derived exclusively from semantically significant event fields in a deterministic order, making it reproducible by any GS1-compliant implementation without access to Ocean DPP source code.

Verification key pinning. The Groth16 verification key is compiled into the client-side portal at build time, ensuring that even a compromised backend cannot substitute a different verification key to accept forged proofs.

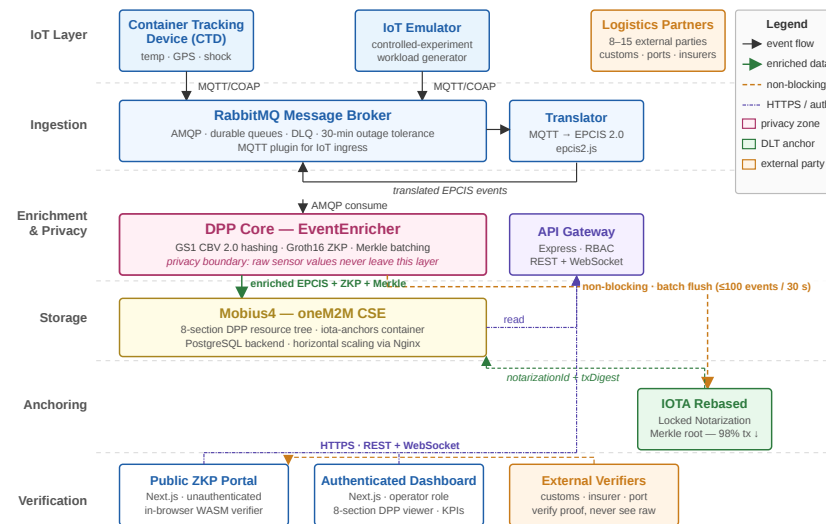


Figure 1. Ocean DPP platform architecture with privacy-preserving verification. IoT sensor payloads enter via MQTT, are translated into EPCIS 2.0 ObjectEvents, enriched with Groth16 ZKP proofs and GS1 CBV 2.0 hashes, persisted to Mobius4 (oneM2M CSE), and asynchronously anchored to IOTA via Merkle batch transactions. External stakeholders verify compliance in-browser via the public portal without accessing raw sensor data.

Table 4 consolidates the selection rationale for the core technologies of Ocean DPP, listing for each the principal alternatives considered and the decision criterion that motivated the choice.

Table 4. Technology-selection rationale: core components, alternatives considered, and decision criteria.

Component	Alternatives Considered	Decision Criterion	Rationale for Selection
IoT service layer—oneM2M	Proprietary IoT platforms; bare MQTT	Standardisation and multi-stakeholder interoperability	Standardised horizontal M2M service layer (resource tree, device management, Common Service Functions) that avoids vendor lock-in and interoperates across independent parties.
Message bus—RabbitMQ (AMQP)	oneM2M HTTP notifications; Apache Kafka	Delivery guarantee under component outage	AMQP acknowledgements, durable queues, per-message persistence, and a Dead Letter Queue satisfy the 30-min outage-tolerance requirement; oneM2M notifications are best-effort HTTP POSTs lost when a subscriber is unavailable.
DLT anchoring—IOTA (permissionless)	Hyperledger Fabric (permissioned); public EVM chains	Cross-border openness and low marginal anchoring cost	Open participation reduces onboarding friction for multi-actor logistics; low per-transaction anchoring cost and IoT-targeted architecture with native notarisation (Table 1).
ZKP system—Groth16	STARKs; PLONK/Bulletproofs	Proof compactness for bandwidth-constrained uplinks	Constant ≈ 850 -byte proof (about two orders of magnitude smaller than an equivalent STARK) and fast succinct verification; the one-time trusted setup is an accepted trade-off.
Event model and hashing—GS1 EPCIS 2.0 + CBV 2.0	Proprietary aspect models; ad-hoc JSON	Open interoperability and verifier independence	Open supply-chain event standard; CBV canonical hashing is reproducible by any GS1-compliant verifier without access to Ocean DPP source code.

3.3. Cryptographic Verification Path

A fundamental challenge of Merkle-based batching is that individual event hashes are leaves inside a batch and not recorded directly on-chain. Ocean DPP addresses this through a five-step cryptographic verification path (Figure 2) that requires no additional on-chain writes.

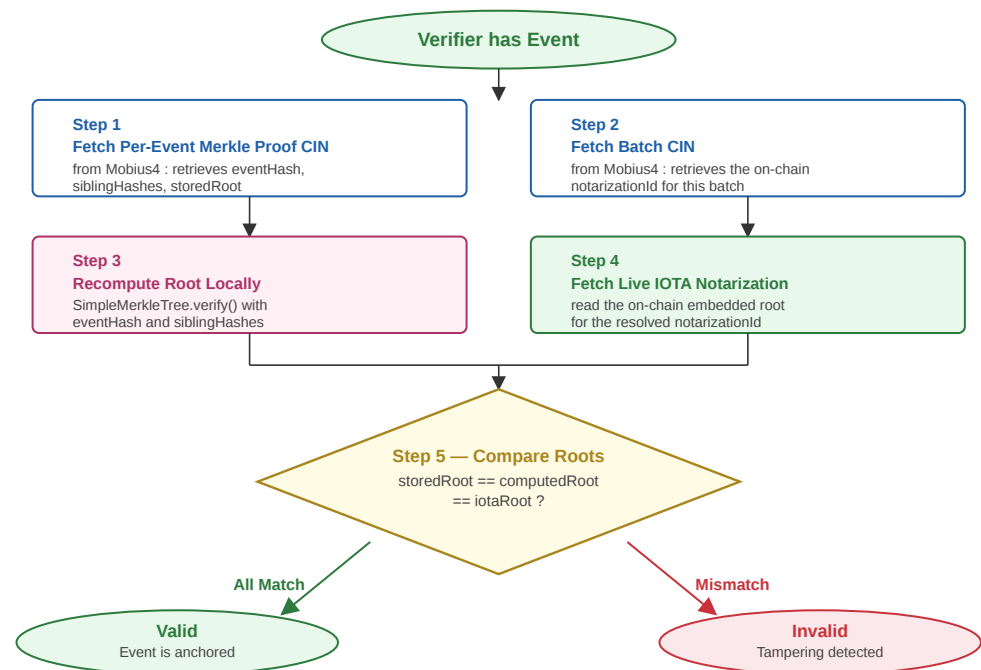


Figure 2. Five-step cryptographic verification path. A verifier fetches per-event and batch CINs from Mobius4, recomputes the Merkle root locally using `SimpleMerkleTree.verify()`, retrieves the live IOTA notarisation, and compares all three roots. The result is a binary valid/invalid judgement that detects both off-chain CIN tampering and on-chain root substitution.

The five steps are: (1) fetch the per-event Merkle proof CIN from Mobius4; (2) fetch the batch CIN and IOTA notarisation identifier; (3) recompute the Merkle root locally; (4) fetch the live IOTA notarisation and read its embedded root; (5) compare stored, computed and on-chain roots (all three must match).

3.4. Threat Model

Four adversary types are in scope. A passive network observer is mitigated by Docker bridge network isolation and Transport Layer Security (TLS) on all external-facing endpoints. A malicious verifier cannot extract the raw sensor value from a Groth16 proof because the actual measured value is a private witness (the prover’s secret input to the proof), never serialised or transmitted. A hash-based message authentication code (HMAC)-based key derivation scheme ($K_c = \text{HMAC-SHA256}(K_{\text{anchor}}, \text{containerId})$), supplied as an additional private circuit input, prevents an observer from brute-forcing the published proof artefacts against the bounded set of plausible readings. A compromised Mobius4 instance exposes raw sensor values to authenticated users with the operator role or above (ZKP privacy is scoped exclusively to the external verification path, which is an acknowledged limitation). Proof forgery is prevented by Groth16 knowledge soundness (under the q -SDH (q -strong Diffie–Hellman) assumption over BN254) and by IOTA Merkle anchoring, which ties each proof hash to a specific blockchain transaction (100% tamper detection rate in experiments, Section 5.3). A dishonest prover is explicitly out of scope: proof generation is performed by the carrier-operated DPP Core, so the threat model assumes

the prover faithfully supplies the CTD-measured value as the private witness. Because the proof attests only that a value satisfying the compliance predicate was supplied as the private witness, the current design cannot cryptographically prevent a dishonest operator from generating a valid proof over a fabricated in-range value; this honest-prover assumption is the principal trust limitation of the framework. Its consequences, the partial mitigation provided by tamper-evident IOTA anchoring, and the authenticated-sensor-binding solution are analysed in Section 6.6.

3.5. Eight-Section DPP Data Model

Each shipping container is represented as eight oneM2M containers in the Mobius4 resource tree: (1) Identification, (2) Dimensions, (3) Manufacturer, (4) EPCIS-Events, (5) Maintenance, (6) Sustainability, (7) Supply-Chain, and (8) Documentation. A technical *iota*-anchors container stores blockchain anchoring artefacts separately from the eight user-facing DPP sections. When ZKP proof generation succeeds, an additional *zkp* object is appended to the enriched EPCIS event; it contains the Groth16 proof, public signals, and a *proofHash* used as the Merkle leaf for anchoring. The actual temperature reading is never persisted in the *zkp* object. Each proof attests to a single sensor reading; proof generation operates at the granularity of the individual EPCIS event, not over time windows or entire shipments. Shipment-level compliance is established by the collection of per-event proofs anchored over the voyage, and aggregate predicates over time windows (for example, bounding the duration of a temperature excursion) would require extended circuit designs.

4. Implementation

Ocean DPP comprises five Node.js microservices (Translator, DPP Core, API Gateway, Ocean-ADM identity provider, and Mobius4 CSE), two PostgreSQL databases, a RabbitMQ AMQP broker, an IOTA Rebased localnet node, and a Next.js frontend, all orchestrated via Docker Compose (Table 5).

Table 5. Technology stack.

Layer	Component	Technology
IoT Platform	Device and data management	Mobius4 (oneM2M CSE)
Translation	IoT → EPCIS	Node.js 20, <i>epcis2.js</i> 2.7
Message Bus	Async communication	RabbitMQ 3 (AMQP 0-9-1)
ZKP	Circuit/proof/verify	Circom 2, <i>snarkjs</i> 0.7, <i>circomlib</i> 2
Blockchain	Immutable anchoring	IOTA Rebased, <i>@iota/notarization</i>
Blockchain	Merkle tree	OpenZeppelin SimpleMerkleTree [41]
Identity	Auth and JSON Web Token (JWT) issuance	Ocean-ADM (Node.js 20)
API	REST + WebSocket gateway	Express.js 4
Dashboard	Authenticated UI/portal	Next.js 14
Deployment	Orchestration	Docker Compose

4.1. Event Enrichment Pipeline

Figure 3 shows the EventEnricher pipeline. Each dequeued AMQP message passes through seven sequential steps: extract and normalise the container identifier; seed the eight-section oneM2M container hierarchy on first encounter; compute the GS1 CBV 2.0 event hash; generate a Groth16 ZKP proof if a temperature observation is present; select the anchor hash; schedule a non-blocking IOTA Merkle anchor; and persist the enriched event to Mobius4, then ACK to RabbitMQ.

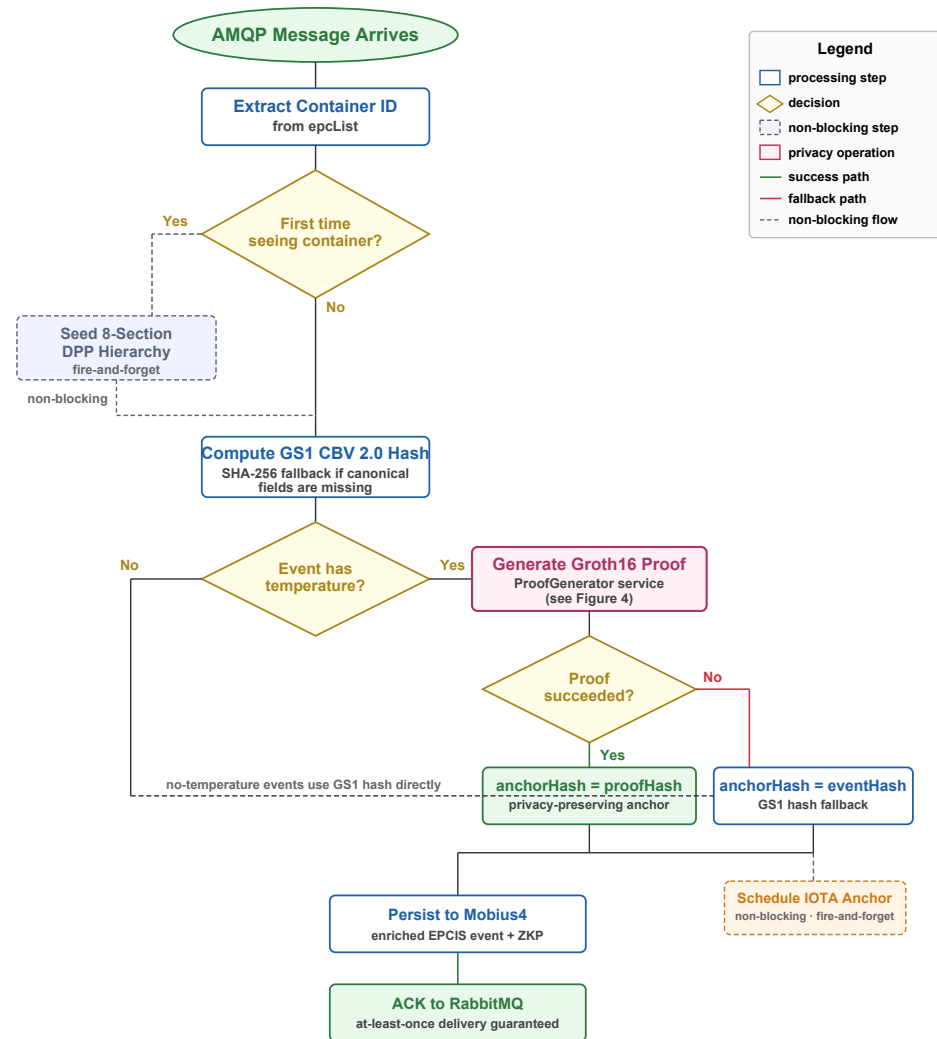


Figure 3. EventEnricher pipeline. The seeding step (dashed) is fire-and-forget; IOTA anchoring is scheduled non-blocking. The pipeline ACKs to RabbitMQ only after successful Mobius4 persistence, implementing at-least-once delivery.

The Translator bridges raw MQTT sensor payloads to GS1 EPCIS 2.0 ObjectEvents using the `epcis2.js` reference library. A 24-h least-recently-used (LRU) idempotency cache suppresses duplicate deliveries. A stable MQTT persistent session (`clean=false`) ensures messages buffered during a Translator restart are redelivered. An adaptive concurrency circuit breaker prevents slow Mobius4 responses from causing unbounded memory growth.

4.2. ZKP Circuit Design and Proof Generation

Conceptually, the circuit is the machine-checkable form of a single compliance question—did the measured temperature stay at or below the contracted limit?—and this subsection describes how that question is encoded for proof generation. The temperature compliance circuit (`tempBound.circom`) uses the Circom 2 language with the `SignedLessThan(16)` component from `circomlib`, scaled by a factor of 10 to convert decimal Celsius to integer arithmetic. This 16-bit signed representation covers $\pm 3276^\circ\text{C}$, accommodating both ambient and sub-zero cargo conditions. Temperature is the first compliance predicate implemented; the circuit architecture is designed for extension to further sensor types (humidity, shock, seal state) following the same signed-integer pattern. Temperature was chosen as the representative predicate because cold-chain compliance is one of the highest-value maritime monitoring requirements; validating one circuit end-to-end es-

establishes the bounded-value construction that the humidity, shock, and seal-state predicates reuse directly, while richer predicates such as GPS-route compliance and multi-condition conjunctions are a larger extension reserved for future work (Section 6.6). Concretely, each of these predicate classes maps onto a known circuit construction. A two-sided range check (lower and upper limits) instantiates two `SignedLessThan` comparators over the same witness and conjoins their outputs, roughly doubling the comparator constraints. Seal status is a Boolean equality check against the expected sealed state, the simplest predicate of the family. Multi-condition compliance (for example, temperature, humidity, and seal simultaneously) is the in-circuit conjunction of the individual predicate outputs, with one proof attesting to the conjunction and constraint counts growing additively with the number of conditions. Temporal predicates (bounding the duration of an excursion) and route compliance are the more substantial extensions: they take multiple readings or positions as witnesses within a single proof (a time window of sensor values, or positions tested against authorised route segments encoded in integer arithmetic) which increases witness size and constraint counts. These variants are design projections rather than evaluated implementations; the temperature circuit validates the comparator building block that the bounded-value predicates share. The circuit includes two private inputs (`actual_temp` and `salt`, the HMAC-derived container key K_c), one public input (`max_temp`), and one output (`compliant`). It compiles to 17 non-linear RICS constraints.

Figure 4 shows the ProofGenerator decision tree. Two skip paths (ZKP disabled; no temperature observation) allow the enrichment pipeline to proceed without a proof. Any prover error returns a typed failure object so that ZKP failures never cause data loss.

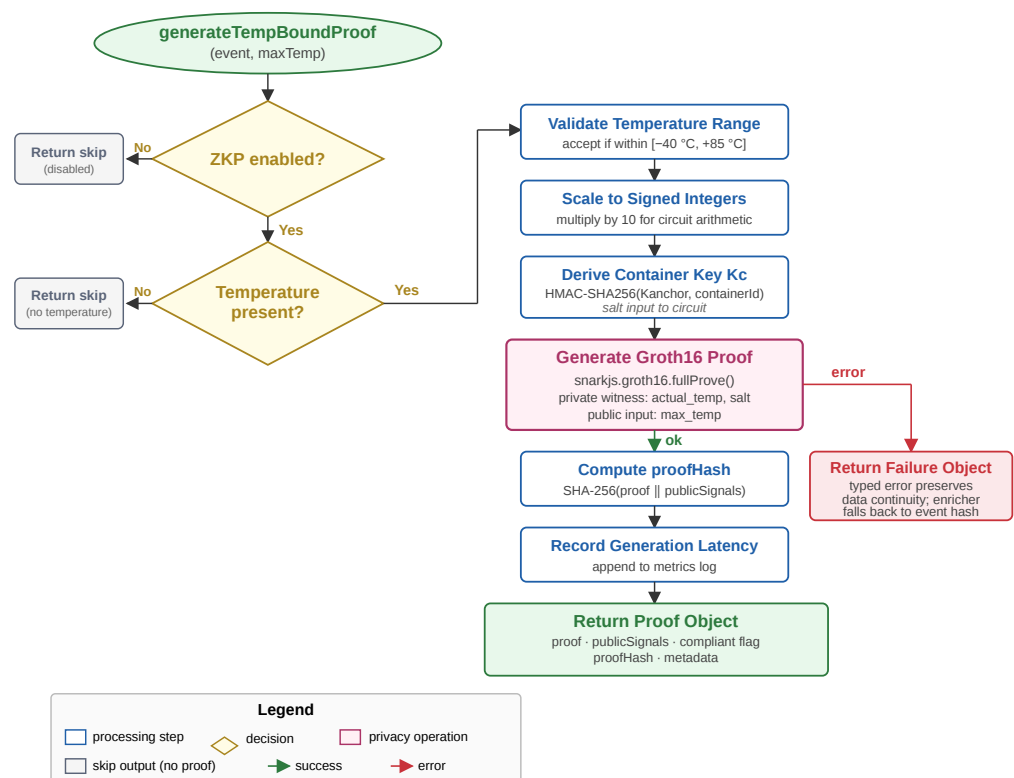


Figure 4. Groth16 proof generation pipeline (ProofGenerator). Two skip paths (ZKP disabled; no temperature observation) allow the enrichment pipeline to proceed without a proof. Any prover error returns a typed failure object; the enricher falls back to the plain GS1 event hash, preserving data continuity.

4.3. IOTA Merkle Batch Anchoring

Figure 5 illustrates the batch anchoring and per-event verifiability pipeline. The `merkleBatch.js` module accumulates event hashes into an in-memory buffer and flushes when the buffer reaches a configurable batch size (default 100 events) or a configurable timeout elapses (default 30 s). At flush, the module: (1) constructs a Merkle tree from accumulated proof hashes; (2) submits one IOTA Locked Notarization transaction embedding the Merkle root; (3) stores per-event sibling proofs and a batch record as CINs in the `iota-anchors` Mobius4 container. The anchoring runs as a fire-and-forget background operation, so IOTA latency never blocks the real-time event pipeline.

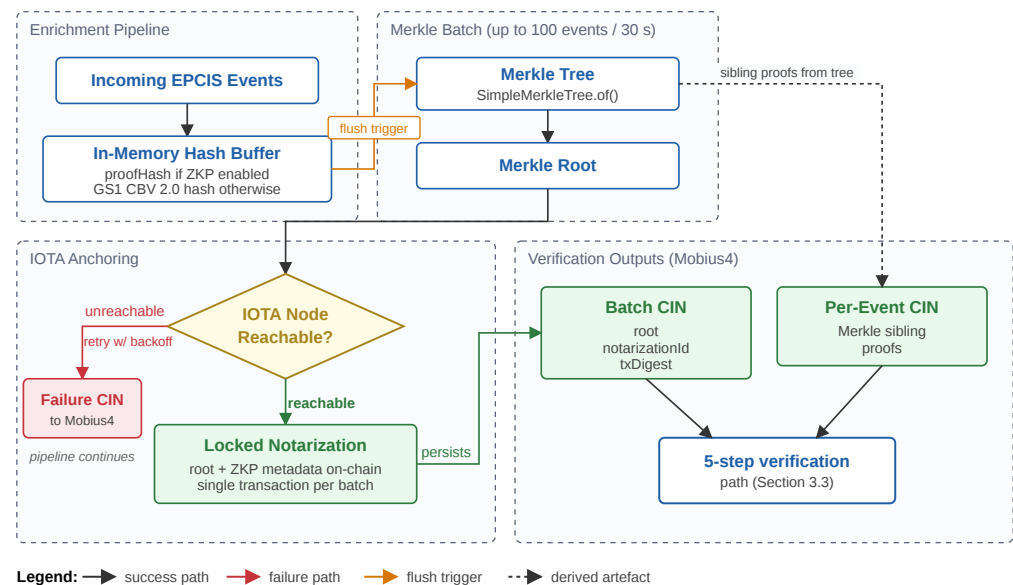


Figure 5. Merkle batch anchoring and per-event verifiability pipeline. Each batch anchors a configurable number of event hashes as a single IOTA Locked Notarization; per-event sibling proofs stored in Mobius4 enable independent verification without additional on-chain writes (five-step path, Figure 2).

The anchoring pipeline was verified end-to-end: a batch of 25 events for container LMCU2231201 was anchored as a single IOTA Locked Notarization (TX latency 3328 ms) with per-event sibling proof links stored in Mobius4, confirming the five-step verification path described in Section 3.3.

4.4. Public Verification Portal and Authenticated Dashboard

The public portal implements a zero-trust verification model. The Groth16 verification key is compiled into the client bundle at build time. When a stakeholder enters a container identifier, the portal verifies the proof entirely in-browser using the WebAssembly snarkjs verifier and the pinned key. Figure 6 shows the portal for a compliant event (left) and a non-compliant event (right): in both cases, the actual temperature reading is withheld, and the portal displays only the binary compliance verdict, the public compliance threshold, and the IOTA immutability check result.

	Compliant Event	Non-Compliant Event
Compliance verdict	PASSED	VIOLATED
Declared threshold	$\leq 19.0\text{ }^{\circ}\text{C}$	$\leq 19.0\text{ }^{\circ}\text{C}$
Raw temperature	Hidden	Hidden
Groth16 proof	Verified	Verified
Proof hash (leaf)	0x4271...ef99	0x0302...b19f
IOTA Merkle root	0xd5f7-46a1	0x855e...aa8

In both cases the raw temperature is never revealed; the Groth16 proof attests only that it satisfies the declared threshold, and the result is anchored to an immutable IOTA notarization.

Figure 6. Public ZKP verification portal output for a compliant event (**left**) and a non-compliant event (**right**). In both cases, the actual temperature reading is withheld; only the binary compliance verdict, the declared threshold, the Groth16 proof hash, and the IOTA anchor details are shown.

The authenticated DPP Passport Viewer renders the eight-section passport structure for an authorised operator, including a key performance indicator (KPI) summary bar (total events, active alarms, ZKP compliance rate, IOTA anchor status) and sensor data charts showing configured compliance thresholds with annotated breach points. A GPS Live Map provides colour-coded container positions: green markers indicate active containers with recent telemetry; red markers indicate containers in alarm state.

After the controlled campaign, the identical Docker Compose stack was deployed on a cloud-hosted virtual machine (VM) and exercised with a commercial CTD on a container during a round-trip between Italy and Germany, providing qualitative confirmation of real-world operability. The CTD hardware and the hybrid terrestrial/satellite connectivity employed in this field test are an evolution of the device class characterised in [11] and validated end-to-end in the 5GT System assessment [12]. No quantitative performance claim is drawn from this field deployment; it provides operability evidence only, and a quantitative field-measurement campaign under operational terrestrial/satellite conditions is reserved for future work (Section 6.6).

5. Experimental Evaluation

5.1. Evaluation Methodology

All 16 controlled experiments were run on a Dell Latitude 5401 (Intel Core i7-9850H, 6 cores/12 threads, 16 GB RAM, SSD) running Windows 11 Pro with Hyper-V. The full Docker Compose stack (up to 9 containers) shared this single host. A Python IoT emulator generated synthetic ocean container telemetry: temperature oscillated sinusoidally in the 14.5–21.5 °C range, bisected by the 19 °C compliance threshold to produce a balanced mix of compliant and non-compliant events (demonstrating the ZKP logistics-chain compliance verification path). Humidity, pressure, GPS coordinates, and shock readings were also emitted, populating the full sensor event model. Latency timestamps were recorded to CSV files. Percentile values use the nearest-rank method with ceiling index $\lceil p \cdot n \rceil$. Throughout, P50, P95, and P99 denote the 50th (median), 95th, and 99th percentiles, respectively. For the steady-state end-to-end summaries, four blank Experiment 1 rows (0.4% of 1000 archival rows) and the three Experiment 7 WASM cold-start rows above 1000 ms (1.5% of 199 rows) were excluded; the Experiment 5 proof-generation outliers were retained and identified explicitly because they are part of the observable proof-generation tail. No negative-latency rows were present in the archival CSVs used for the revised analysis. Uncertainty on reported means and tail percentiles is summarised with 95% percentile bootstrap confidence intervals (CIs). Two-group latency comparisons use two-sided Mann–Whitney U tests

with Cliff's δ effect size, while the three-way Experiment 11 batch-size comparison uses a Kruskal–Wallis test.

Experiment run structure. Each experiment is a single controlled run on the single-host testbed rather than an average over repeated independent runs. The latency experiments (Experiments 1 and 5) each collect approximately 1000 end-to-end events at a one-second per-container emit interval. The throughput and saturation experiments use fixed 60-s measurement windows at increasing calibrated input rates (reported in events per second, derived from a one-time single-emulator calibration so that load is expressed as an event rate rather than as a number of emulator instances). The horizontal-scaling experiments repeat the highest-load case once with one and once with two service replicas, sampling queue depth every five seconds. End-to-end (E2E) latency is measured as the difference between the ingestion and terminal-persistence timestamps recorded to CSV at fixed pipeline points. Reproducibility is supported by the pinned component versions in Table 5, the workload parameters above, and the compliance threshold, percentile rule, and exclusion rule already stated. Because each experiment is a single run, sampling uncertainty is quantified with the bootstrap confidence intervals reported per experiment; repeated independent runs across multiple hosts and days remain future work (Section 6.6).

5.2. Performance Results (RQ1)

Experiment 1–Baseline latency (ZKP disabled). Across 996 clean events (Table 6), the pipeline achieved a mean E2E latency of 32.4 ms, well below the 200 ms target. Figure 7 shows the cumulative distribution function (CDF) and histogram, confirming a tight concentration around the 30 ms median. P95 = 48 ms (95% bootstrap CI [46, 52]) and P99 = 75 ms (95% bootstrap CI [68, 85]) confirm substantial headroom under steady-state conditions.

Table 6. Experiment 1: Baseline end-to-end latency ($n = 996$, ZKP disabled).

Mean (ms)	Std Dev	Median	P95	P99	Max
32.4	9.8	30	48	75	116

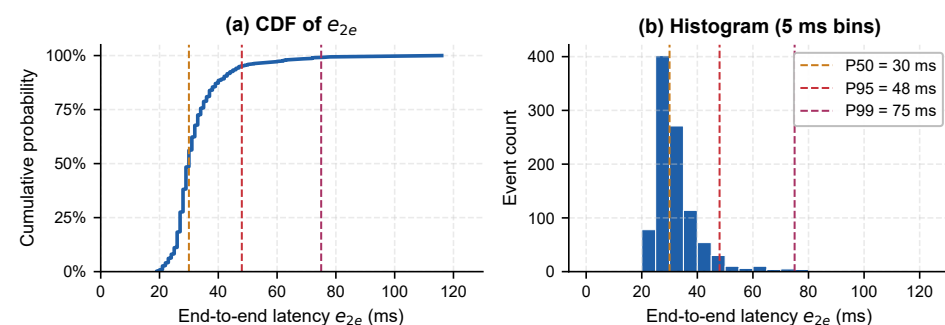


Figure 7. Experiment 1: Baseline latency distribution ($n = 996$, ZKP disabled). (a): CDF with P50, P95, and P99 percentile markers. (b): histogram (5 ms bins) showing the right-skewed distribution with 95% of events completing within 48 ms.

Experiments 2–3–Throughput and saturation. Sustainable throughput on the evaluation hardware is ≈ 7 events/s. Figure 8 shows that at 10 containers (16.7 ev/s), median latency rises to 112 ms and P95 to 191 ms as the RabbitMQ queue grows faster than DPP Core can drain it. Burst tests confirm zero permanent event loss at 50 containers (100% success), while at 100 containers partial Translator-side shedding occurs (61% success), with shed messages buffered in MQTT Quality of Service (QoS)-1 persistent sessions for redelivery.

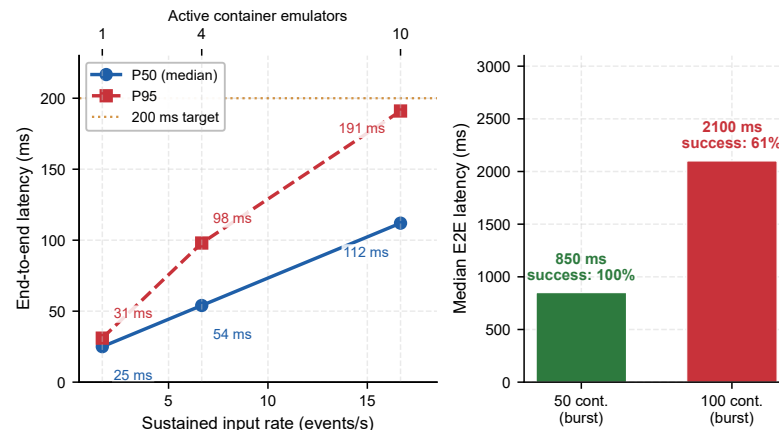


Figure 8. Throughput and burst-capacity results. (left) Experiment 2: end-to-end latency (P50 and P95) vs. input event rate; the dashed line marks the 200 ms latency target. (right) Experiment 3: burst-capacity tests, where bar height shows median E2E latency and labels indicate the success rate. The Mobius4 HTTP write bottleneck is resolved by horizontal scaling (Section 5.4).

Experiment 4—EPCIS 2.0 compliance. All 360 events across three event types (telemetry, alarm, e-seal) passed three-stage validation: mandatory field presence, CBV 2.0 vocabulary compliance, and epcis2.js schema validation (100% pass rate).

5.3. ZKP Results (RQ2)

Experiments 5–6—Proof generation and verification. Figure 9 presents the latency distribution for all ZKP operations on a shared logarithmic scale. Across 198 proofs (Table 7), mean proof generation time was 303.6 ms (median 266 ms). Across the full dataset, 97.5% of proofs completed within 500 ms; the three proofs above 1 s were WASM cold-start events and drove the P99 of 1904 ms. Browser-side WASM verification averaged 9.8 ms (P95 12 ms, P99 17 ms) with 100% success across 195 proofs, yielding a 31:1 generation-to-verification ratio. The one-off generation cost is incurred once per event and then amortised across every independent verifier, each of which adds only 9.8 ms; this is favourable for maritime shipments, for which the typical 8–15 stakeholders per container each need to verify the same compliance claim.

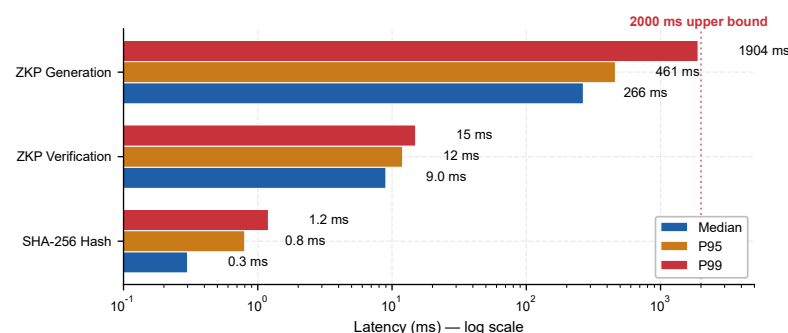


Figure 9. Experiments 5–6: ZKP operation latency distribution. Horizontal bars show median, P95, and P99 for proof generation, browser verification, and SHA-256 hashing. The dashed line marks the 2000 ms upper bound. Log scale.

Experiment 7—ZKP pipeline overhead. Figure 10 compares Experiment 1 (no ZKP) with the steady-state Experiment 7 distribution (three WASM cold-start rows above 1000 ms excluded) across mean, median, P95, and P99 on a logarithmic scale. With ZKP enabled, mean E2E latency rose to 328.4 ms (+296.0 ms), P95 to 500 ms (+452 ms), and

P99 to 591 ms (+516 ms). The overhead originates almost entirely from proof generation (304.7 ms enrichment delta). The median E2E remained 308 ms, which is operationally acceptable for maritime IoT intervals where events arrive every 10–30 s. The Experiment 1 and Experiment 7 steady-state latency distributions are almost completely separated ($U = 17.0$, $p = 5.128 \times 10^{-109}$, Cliff's $\delta = -0.9998$), confirming that the ZKP cost is systematic rather than a tail artefact.

Table 7. ZKP performance summary.

Operation	No. of Proofs	Mean (ms)	Median	P95	P99
Proof generation	198	303.6	266	461	1904
Browser verification	195	9.8	9	12	17
SHA-256 baseline	—	0.4	0.3	0.8	1.2

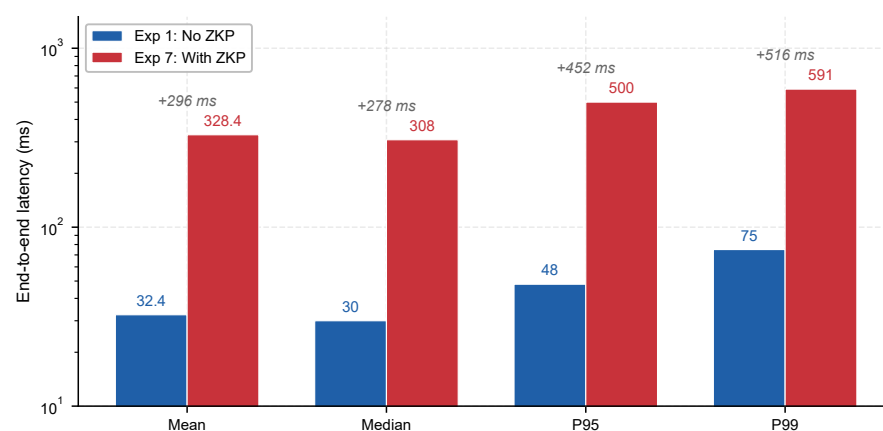


Figure 10. Experiment 7: ZKP overhead on pipeline latency. Grouped bars compare Experiment 1 (no ZKP) with the steady-state Experiment 7 summary (three WASM cold-start rows above 1000 ms excluded) across mean, median, P95, and P99. Log scale; overhead annotations between bar pairs.

Experiment 8—Tamper detection. All 10 tampered events (modified eventTime field) were detected via Merkle inclusion failure with sub-millisecond detection latency, and all 10 unmodified events passed verification (zero false positives; 100% tamper detection rate).

5.4. Scalability Results

Figure 11 shows horizontal scaling results for both pipeline tiers. Adding a second DPP Core instance (Experiment 9) reduced median latency by 37.1% (731 ms → 460 ms; Mann–Whitney $U = 4,035,154$, $p < 10^{-300}$, Cliff's $\delta = 0.899$) and increased throughput by 21.9%. Two Mobius4 instances behind an Nginx round-robin proxy (Experiment 10) eliminated all HTTP connection errors at the 50-container load level (≈ 810 errors → 0), increased successful event throughput from 9.08 to 15.82 events/s (+74.1%), and reduced P95 latency from 17,905 ms to 5446 ms ($\approx 70\%$; Mann–Whitney $U = 1,221,650.5$, $p = 1.606 \times 10^{-16}$, Cliff's $\delta = 0.181$). The small effect size reflects a modest median shift (1148 ms → 801 ms) but strong upper-tail compression together with the elimination of connection errors.

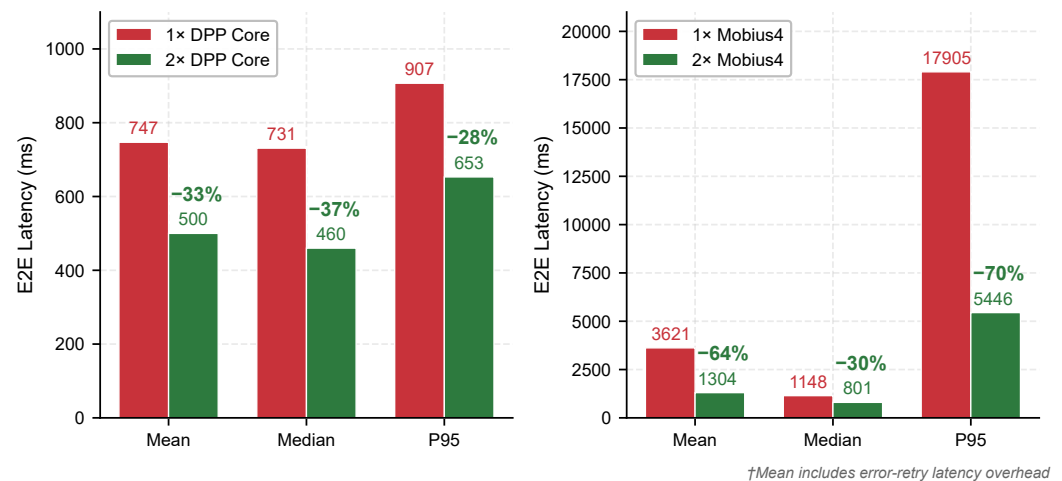


Figure 11. Horizontal scaling results. (left) Experiment 9: DPP-Core 1× vs. 2× instances (median latency −37%, $p < 0.001$). (right) Experiment 10: Mobius4 1× vs. 2× instances (P95 latency −70%, connection errors → 0). Note the different y-axis scales.

5.5. IOTA Anchoring Results (RQ3)

All anchoring measurements in this subsection were obtained on a self-hosted IOTA Re-based localnet; they characterise the batching mechanism and the local confirmation path, and are not a claim about public-mainnet latency or finality under network congestion or real validator conditions (Section 6.6). Experiment 11 is a batch-size sensitivity analysis across batch sizes of 10, 50 and 100 events. Figure 12 shows that blockchain anchor latency is dominated by IOTA network confirmation time, not Merkle tree computation. A Kruskal–Wallis test detects statistically significant differences across batch sizes ($H = 31.57$, $p = 1.395 \times 10^{-7}$), but the three means remain within the same 3.5–4.2 s confirmation window (4036 ms for batch-10, 3529 ms for batch-50, and 4183 ms for batch-100), indicating that batching primarily affects per-event anchoring cost rather than user-visible latency. Batch-50 achieves the tightest mean 95% bootstrap CI ([3481, 3578] ms). Since anchoring runs as a non-blocking background process, this latency does not affect event pipeline throughput.

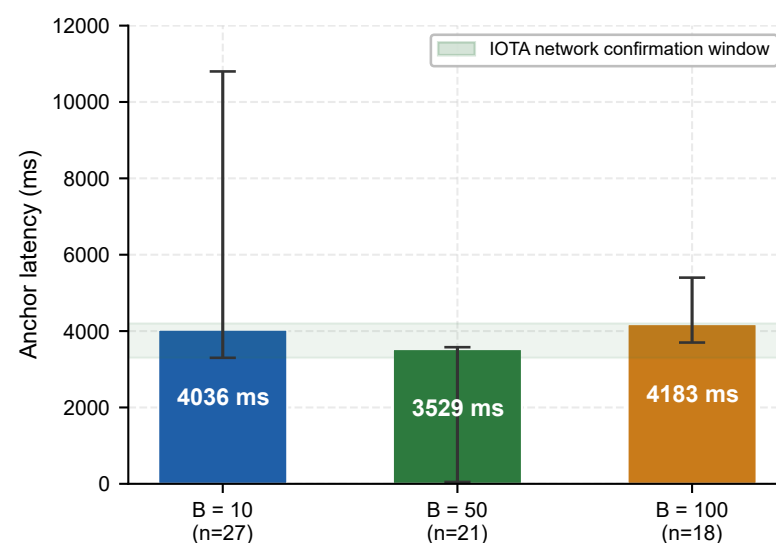


Figure 12. Experiment 11: Blockchain anchor latency by batch size. Bar height shows mean latency; error bars span min–max. The shaded band indicates the IOTA network confirmation window (≈ 3.3 – 4.2 s).

Figure 13 shows that Merkle batching achieves 98% reduction in on-chain transaction count at $B = 50$ and 99% at $B = 100$, while per-event verifiability is preserved. Because anchoring cost on IOTA is incurred per transaction, this 98–99% reduction in on-chain transaction count yields a corresponding reduction in per-event anchoring cost; batch anchoring, therefore, decouples on-chain load, and cost, from the raw event-generation rate, which is the primary architectural lever for scaling to large fleets.

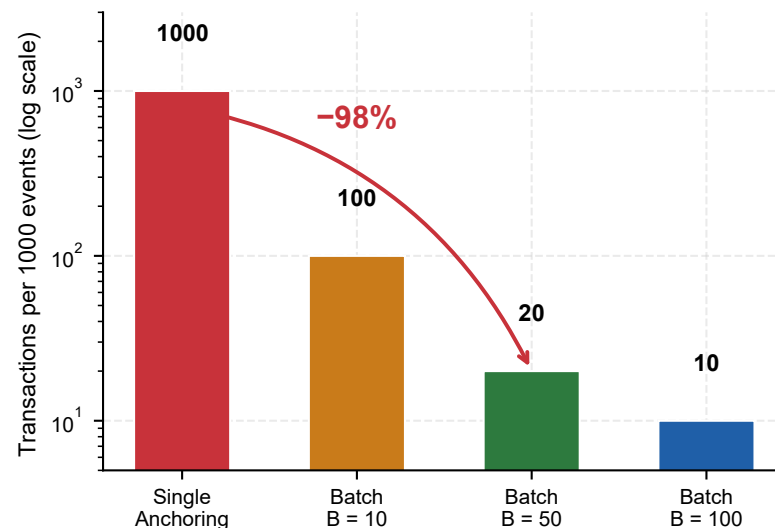


Figure 13. Experiment 12: On-chain transaction reduction via Merkle batching. Each bar shows the number of IOTA transactions required per 1000 events. The arrow highlights the 98% reduction at $B = 50$. Log scale.

5.6. Reliability Results (RQ4)

Figure 14 shows a Gantt-style fault injection timeline for all four reliability experiments. In all scenarios, zero permanent message loss was observed: Experiment 13 (Translator crash)—14 messages buffered via MQTT QoS 1 persistent sessions; Experiment 14 (DPP Core restart)—19 messages buffered in RabbitMQ durable queues, 273 events published post-recovery; Experiment 15 (Mobius4 outage)—18 failures captured in DLQ without blocking the enrichment path; Experiment 16 ($4\times$ burst load)—overflow events negatively acknowledged (nacked) and requeued via backpressure, zero permanent message loss.

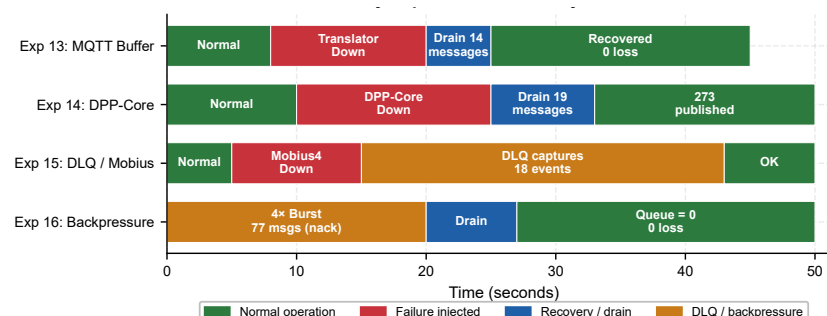


Figure 14. Reliability experiments 13–16: Gantt-style fault injection timeline. Green = normal operation; red = failure injected; blue = recovery / drain; orange = DLQ capture or backpressure active. All tests conclude with zero permanent message loss.

6. Discussion

6.1. Pipeline Performance and Scalability

The P95 end-to-end latency of 48 ms (ZKP disabled, $n = 996$) is well within the requirements for maritime IoT event processing, where sensor readings typically arrive every 10–30 s per container. The tight distribution (median 30 ms, P99 75 ms) indicates that the RabbitMQ-based pipeline introduces minimal queuing jitter under steady-state conditions, validating the choice of AMQP over best-effort oneM2M HTTP notifications.

Throughput saturation at ≈ 7 events/s reflects the Mobius4 HTTP write bottleneck rather than any fundamental limit of the architecture. The horizontal scaling experiments confirm this directly: adding a second Mobius4 instance behind an Nginx round-robin proxy eliminates connection errors entirely at the 50-container load level and reduces P95 latency from 17,905 ms to 5446 ms ($\approx 70\%$; $p = 1.606 \times 10^{-16}$). Cliff's $\delta = 0.181$ shows that the gain is concentrated in the upper tail rather than a wholesale shift of the full distribution, which is consistent with the elimination of HTTP connection errors under load. This result is practically significant for maritime deployments because a vessel carrying 2000–5000 instrumented containers would require only a small number of Mobius4 replicas to sustain the expected telemetry rate; the replicas can be provisioned elastically on a cloud-hosted VM without architectural changes. The expected deployment assumption is a low per-container reporting duty cycle (one reading every 10–30 s), so aggregate load grows linearly with fleet size and is served by horizontally replicating the Mobius4 write tier, which is the only saturating component identified. The IOTA anchoring path is decoupled from the event rate through Merkle batching (Section 5.5) and, therefore, does not become a bottleneck as fleet size grows, and port-level scale (many vessels) is met by the same per-tier horizontal replication rather than by any change to the pipeline design. The principal remaining unknown at vessel and port scale is heterogeneous and intermittent terrestrial/satellite connectivity, which the single-host testbed does not reproduce and which is identified for multi-vessel pilot validation. The 100% EPCIS 2.0 compliance rate across all three event types (telemetry, alarm, e-seal) confirms that the Translator correctly implements the GS1 CBV 2.0 hashing algorithm for all event classes in scope.

Required infrastructure and deployment cost. The runtime footprint is modest: the full system is a Docker Compose stack of up to nine containers—five Node.js (20 LTS) microservices (Translator, DPP Core, API Gateway, identity provider, and the Mobius4 oneM2M CSE), two PostgreSQL databases, a RabbitMQ broker, an IOTA node, and a Next.js portal (Table 5)—which runs on a single commodity host and scales out by replicating only the saturating tier on additional cloud instances, as discussed above. At the edge, it requires a CTD per monitored container plus connectivity; no specialised hardware or permissioned-consortium onboarding is needed. On cost, the build relies on open-source and commodity components, and the marginal on-chain cost is kept low by IOTA's low per-transaction cost together with the 98–99% batching reduction (Section 5.5); the dominant recurring cost is, therefore, cloud compute for the containerised services, which grows with replica count rather than with event volume. A deployment-specific total-cost-of-ownership analysis is addressed as future work, as are the operational risks identified above (the Mobius4 write tier as the scaling bottleneck), in Section 6.6 (the localnet-to-mainnet gap), and in Section 6.4 (the misuse and adoption considerations).

6.2. ZKP Overhead and Privacy Cost–Benefit

The mean Groth16 proof generation time of 304 ms introduces a measurable but operationally acceptable overhead for maritime IoT, where the event interval of 10–30 s per container gives the enrichment pipeline ample headroom. These costs were measured for the compact 17-constraint temperature circuit; richer predicates compile to larger constraint

systems with correspondingly higher proving times, so the reported overhead should be read as the single-predicate baseline rather than a general figure for arbitrary compliance circuits. The 31:1 generation-to-verification ratio is the key cost–benefit figure: a single 304 ms generation investment amortises across every subsequent verification, each costing only 9.8 ms in-browser via WebAssembly. Since a typical container shipment involves 8–15 independent verifying stakeholders (customs, insurer, port authority, logistics partners), the measured amortisation applies per stakeholder: the 304 ms proving cost is incurred once, and each verifier completes an independent 9.8 ms in-browser check. Verification is self-service by design: with the verification key pinned in the public portal, a stakeholder needs no bilateral data-access agreement with the carrier to check compliance.

The privacy guarantee follows from the Groth16 zero-knowledge property: the actual sensor reading is supplied only as a private witness and is never serialised, transmitted, or persisted, so an external verifier learns nothing beyond the binary compliance verdict. Because the compliance threshold (`max_temp`) is the only public input, and the HMAC-derived container key is itself a private circuit input, an observer cannot brute-force the published proof artefacts against the bounded set of plausible readings. This guarantee is scoped to the external verification path: it does not conceal raw telemetry from operator-role users of the originating Mobius4 store, which is governed by conventional access control (Section 3.4). The 100% tamper detection rate across all 10 injected events (Experiment 8) confirms that the Merkle anchoring layer provides a reliable integrity check independent of the ZKP layer.

6.3. Governance of Compliance Thresholds, Keys, and Circuit Versions

The practical governance model separates four concerns. (i) Compliance thresholds: the bound checked by the circuit (e.g., `max_temp`) is the contracted or regulated specification for the shipment and is defined externally by the party that owns that specification (for example, the shipper or the regulator under the cargo contract); it is carried as the circuit’s only public input, so the prover and every verifying stakeholder evaluate the same declared bound rather than a value chosen privately by the operator. (ii) Verification keys: the Groth16 verification key is derived from the circuit by the trusted-setup ceremony and is pinned into the client-side portal at build time, so proof acceptance does not depend on trusting the backend that produced the proof. (iii) Circuit updates: any change to a compliance predicate requires a new trusted-setup ceremony and recompilation, which yields a new, independently versioned verification key rather than an in-place modification. (iv) Version assurance: with the pinned key, a stakeholder verifies against a fixed, auditable circuit build; binding each archived proof to its circuit version through a persisted verification-key hash (`vkeyHash`) is identified as future work (Section 6.6), and would let stakeholders confirm exactly which circuit and policy version produced each historical proof. Legal standing is a further governance consideration. Within the European Union, the eIDAS framework [42] establishes that electronic documents, seals, and timestamps may not be denied legal effect solely on account of their electronic form, and its 2024 revision [43] introduces the European Digital Identity framework, whose recitals explicitly name zero-knowledge proof among the privacy-preserving technologies to be integrated for selective disclosure. Zero-knowledge proofs are not yet a specifically recognised category of legal evidence, however: today, a Groth16 compliance proof would enter a dispute as technical evidence whose probative value is established by expert assessment, strengthened in Ocean DPP’s case by the tamper-evident IOTA anchor that fixes each proof in time. Anchored records could be further reinforced with qualified electronic timestamps under eIDAS. The legal acceptance of cryptographic compliance evidence in cross-border

maritime disputes, therefore, remains jurisdiction-specific and is a matter for regulatory engagement rather than system design alone.

6.4. Misuse Potential and Adoption Considerations

Because the reviewer raises misuse and stakeholder acceptance, we make the residual risks explicit. First, privacy protection is by design scoped to the external verification path: because the raw telemetry is the carrier's own data, it is retained in the carrier-operated EPCIS store and remains readable to authenticated operator-role users (Section 3.4)—the zero-knowledge layer conceals raw values from external verifiers, not from the data owner. A deployment that instead outsources hosting to a neutral third-party operator would additionally require encryption-at-rest under carrier-held keys or on-device proving so that the host cannot read raw values, which we identify as future work. Beyond this, the published artefacts still leak limited information—a non-compliant verdict reveals that a breach occurred, the public threshold discloses the contracted specification (Section 6.6), and event frequency, timing, and container identifiers remain observable to parties with network access. Combined with the current honest-prover assumption, under which an operator could submit a proof over a fabricated in-range value, these are the principal avenues by which the system could be misused or its guarantees over-read. Second, on adoption: the privacy-preserving design directly addresses the structural barrier that discontinued permissioned consortium platforms such as TradeLens [29], namely the reluctance of competing parties to expose commercial data on a shared platform; by revealing only a compliance verdict, Ocean DPP removes the raw-data-sharing precondition. Residual adoption risks remain, however—a published verdict can still expose a compliance failure, and proof issuance is presently operator-controlled—so practical deployment depends on role-based access control over who may trigger and read verdicts, on binding proofs to authenticated CTD readings, and on threshold-hiding commitments and metadata-privacy measures, which we identify as future work.

6.5. Comparison with Related Systems

Ocean DPP is, to the best of our knowledge, the first maritime DPP system with both a quantitative evaluation and a privacy-preserving verification mechanism (Table 2). Existing systems fall into two categories: permissioned blockchain platforms (IBM Food Trust, TradeLens) that provide traceability without privacy preservation, and DPP frameworks (Catena-X, EU Battery Passport) that address manufactured goods rather than in-transit logistics chains. None integrates ZKPs with EPCIS 2.0, and none has been evaluated under realistic maritime operating conditions. As noted in Section 2.7, the systematic review by Silveirinha et al. [40] found no implemented and empirically evaluated ZKP system for maritime supply chains in the surveyed literature; Ocean DPP directly fills that gap.

A direct quantitative benchmark against these systems is not possible from the literature: as Table 2 records, they publish either no quantitative evaluation or only limited evaluations without per-event performance figures. The evaluation is, therefore, designed to isolate the practical cost of each distinguishing layer through an internal configuration comparison, summarised in Table 8. Read as an ablation, the standards-only configuration (A) establishes the conventional-EPCIS baseline: 32.4 ms mean end-to-end latency. Adding tamper-evident anchoring (B) leaves the event path unchanged, because anchoring is asynchronous, and adds 10–20 on-chain transactions per 1000 events. Adding privacy-preserving verification (C) raises mean latency by 296.0 ms, which is the measured price of eliminating raw-data disclosure from external verification. The qualitative trade-offs of alternative DLT platforms are summarised in Table 1.

Table 8. Configuration benchmark: the measured cost of each architectural layer. Configurations A and B share the same event-path measurements because IOTA anchoring is a non-blocking background operation (Section 4.3); anchoring costs are reported separately (Section 5.5). Latency figures are the steady-state end-to-end measurements of Experiments 1 and 7.

Configuration	Mean (ms)	P95 (ms)	P99 (ms)	Tx per 1000 Events	External Verification
A: EPCIS pipeline only (ZKP off, no anchoring)	32.4	48	75	0	requires raw-data disclosure
B: A + IOTA Merkle anchoring	32.4	48	75	10–20 (batch sizes 100/50)	tamper-evident; raw data still required for compliance checks
C: B + Groth16 ZKP (Ocean DPP)	328.4	500	591	10–20	compliance verified without raw-data access

The choice of IOTA as the anchoring layer is also differentiated from prior work. As Section 6.4 notes, the discontinuation of TradeLens in 2022 showed that permissioned consortium blockchains face structural adoption barriers in heterogeneous, open logistics ecosystems [29]. IOTA’s permissionless participation model and low per-transaction-cost architecture are better suited to a scenario where 8–15 independent parties per shipment must each be able to read anchored records without onboarding to a governed consortium.

6.6. Limitations and Future Work

Several limitations bound the current evaluation. First, all 16 controlled experiments used synthetic, emulator-generated workloads. The exploratory Italy–Germany CTD field test confirmed correct end-to-end operation but was not part of the controlled benchmark series and should not be interpreted as a performance measurement. Scale testing reached 100 containers on a single laptop-class host; production deployments at 10,000+ TEU scale would require a dedicated characterisation campaign on cloud infrastructure.

Second, all blockchain anchoring experiments used an IOTA Rebased localnet node. Localnet removes network propagation delay and transaction congestion, so the reported 3.5–4.2 s anchor latency reflects Merkle tree construction and local consensus overhead only, not the behaviour of the public IOTA mainnet. This is appropriate for evaluating the batching algorithm and the pipeline architecture—the contribution being measured is the 98% on-chain transaction reduction and the per-event Merkle proof mechanism, both of which are independent of network conditions. The IOTA Foundation reports sub-second finality targets for the mainnet [31]; mainnet integration and latency characterisation under real network load is reserved for future work.

Third, only a single ZKP circuit (tempBound , 17 R1CS constraints) is implemented and evaluated. Extensibility to humidity bounds, shock magnitude, seal integrity, GPS-route compliance, and multi-condition conjunctions is architecturally supported by the signed-integer circuit pattern but has not been empirically validated. The compliance threshold (max_temp) is a public input visible to any verifier, which discloses the contracted specification even when the raw reading is protected. Groth16 also relies on elliptic-curve pairings over BN254 and is not post-quantum secure; migration to a post-quantum proof system would require a new trusted setup ceremony and circuit recompilation.

Most significantly from a trust perspective, the zero-knowledge proof attests that a value satisfying the compliance predicate was supplied as the private witness; it does not, on its own, bind that witness to the authentic reading produced by the CTD. Because proof generation is performed by the carrier-operated DPP Core, the current design assumes an honest prover that faithfully uses the measured value, and a dishonest operator could, in

principle, generate a valid proof over a fabricated in-range value. Ocean DPP mitigates this only partially: once a proof is committed to IOTA, it is tamper-evident and non-repudiable, so retrospective substitution of an anchored record is detectable, but input authenticity at proof-generation time is not yet cryptographically enforced. Closing this gap—by binding the private witness to an authenticated, CTD-signed commitment to the raw reading, so that the circuit additionally proves the witness equals the value signed by the device—is the most important direction for hardening the trust model.

Future work is organised around seven directions:

1. **Authenticated sensor binding.** Extending the circuit to consume a CTD-signed commitment to the raw reading. As a result, a valid proof attests not only that the private witness satisfies the required predicate but also that it corresponds exactly to the value measured and cryptographically signed by the device through its hardware secure element. This enhancement eliminates the honest-prover assumption identified above and represents the highest-priority hardening measure for the overall trust model.
2. **ZKP circuit library expansion.** Extending the circuit library to cover humidity bounds, shock magnitude thresholds, GPS-route compliance, and composite multi-condition predicates, providing full logistics-chain compliance coverage beyond temperature.
3. **Container DPP data model standardisation.** The eight-section data model proposed here is an initial contribution; further development is needed to align it with the emerging CEN/CENELEC JTC 24 interoperability specifications and forthcoming ESPR delegated acts for transported goods. Engagement with GS1, ISO TC 104 (freight containers), and IMO digital standardisation bodies will be pursued to advance the model toward an industry-recognised container DPP standard.
4. **Artificial intelligence (AI)-based heterogeneous CTD data management.** As CTDs from different vendors begin to be deployed across the global container fleet, data format heterogeneity poses a significant integration challenge. Future work will implement AI models within the Ocean DPP platform to normalise, validate, and semantically enrich telemetry streams from diverse CTD manufacturers. This capability will leverage the new semantic interoperability features of Mobius4, which anticipates the characteristics of version 5 of the oneM2M standard, including enhanced support for AI-assisted data processing and multi-vendor device management at the IoT service layer.
5. **Multi-vessel pilot.** A large-scale operational trial with commercial maritime operators across multiple vessel types and trade routes, including stakeholder usability testing with customs and insurance personnel.
6. **Proof generation throughput.** WASM worker thread parallelism for proof generation to meet the >300 proofs/min. throughput floor at higher event rates.
7. **Verification key auditability.** Persisting vkeyHash alongside each ZKP CIN to enable traceability of circuit upgrades against archived proof batches.

7. Conclusions

This paper has presented Ocean DPP, to the best of our knowledge, the first implemented and quantitatively evaluated framework for privacy-preserving Digital Product Passports in maritime container logistics. Sixteen controlled experiments provided quantitative answers to all four research questions: pipeline P95 latency of 48 ms (ZKP disabled) and 500 ms (ZKP enabled) are within acceptable bounds for maritime IoT event intervals; Groth16 proof generation averages 304 ms, while verification averages 9.8 ms (31:1 ratio); IOTA Merkle batch anchoring achieves 98% on-chain transaction reduction at $B = 50$ while

preserving per-event tamper evidence; and the hybrid messaging architecture achieves zero permanent message loss across four failure-injection scenarios.

In terms of deployment readiness, the following is already validated: the end-to-end pipeline, ZKP generation and verification, horizontal scaling, Merkle batch anchoring, tamper detection, and failure-recovery behaviour were all demonstrated in a controlled single-host testbed under synthetic emulator-generated workloads, while the Italy–Germany CTD field test provided qualitative confirmation of real-world device operability rather than a controlled benchmark. What remains laboratory-based is public-network behaviour (IOTA mainnet latency and finality under congestion), multi-host and fleet-scale throughput, and compliance predicates beyond temperature. Before industrial deployment, these must be validated in a multi-vessel pilot under operational terrestrial and satellite connectivity, with production data volumes and heterogeneous CTD hardware.

These results have direct practical implications. Operationally, Ocean DPP lets the parties that routinely require compliance evidence—customs authorities, insurers, port operators, and logistics partners—independently verify that a shipment met its contracted conditions (for example, cold-chain temperature limits or dangerous-goods handling) without the carrier disclosing raw telemetry, which addresses a recurring adoption barrier in multi-stakeholder logistics. The platform is feasible to deploy with current technology: its services are containerised and run on commodity cloud infrastructure, and the CTD data sources have already been validated in field deployment. Beyond the present evaluation, future research directions are set out as seven directions in Section 6.6—spanning public IOTA-mainnet anchoring, multi-condition compliance circuits, fleet-scale evaluation, and engagement with ISO TC 104 and IMO standardisation—together with a full deployment-cost characterisation.

Ocean DPP resolves the container logistics-chain privacy paradox: external stakeholders can independently verify compliance with declared operational predicates without accessing raw sensor telemetry, demonstrated end-to-end in this work for the temperature-bound predicate and designed for extension to further predicate classes. The carrier’s commercially sensitive data remains private; the regulator’s compliance check remains cryptographically sound. The work also proposes an initial container DPP data model, structured on GS1 EPCIS 2.0 and oneM2M standards, and populated by events from CTDs whose deployment is accelerating with 5G and low-cost NB-IoT NTN satellite technologies. As the coverage of the EU ESPR expands across product categories and the global container fleet progressively becomes instrumented with real-time sensing, Ocean DPP offers a technically grounded, privacy-respecting, and standards-compliant architecture for the digital product passports that global containerised trade will require.

Author Contributions: Conceptualisation, S.K. and M.F.; methodology, S.K. and M.F.; software, S.K.; validation, S.K. and M.F.; formal analysis, S.K. and M.F.; investigation, S.K.; resources, M.F.; data curation, S.K.; writing—original draft preparation, S.K. and M.F.; writing—review and editing, M.F. and S.K.; visualisation, S.K.; supervision, M.F.; project administration, M.F.; funding acquisition, M.F. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Acknowledgments: The authors thank the CNIT research team for providing infrastructure support and for the valuable technical discussions, and acknowledge the Hermez Network for making

publicly available the Powers-of-Tau Phase 1 contribution used in the trusted setup procedure of the zero-knowledge proof scheme adopted in this work.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. United Nations Conference on Trade and Development (UNCTAD). *Review of Maritime Transport 2025*; Technical Report; UNCTAD: Geneva, Switzerland, 2025. Available online: https://unctad.org/system/files/official-document/rmt2025_en.pdf (accessed on 21 July 2026).
2. Han, J.-W.; Zuo, M.; Zhu, W.-Y.; Zuo, J.H.; Lü, E.-L.; Yang, Y.T. A comprehensive review of cold chain logistics for fresh agricultural products: Current status, challenges, and future trends. *Trends Food Sci. Technol.* **2021**, *109*, 536–551. [\[CrossRef\]](#)
3. Chen, Q.; Qian, J.; Yang, H.; Wu, W. Sustainable food cold chain logistics: From microenvironmental monitoring to global impact. *Compr. Rev. Food Sci. Food Saf.* **2022**, *21*, 4189–4209. [\[CrossRef\]](#) [\[PubMed\]](#)
4. Mustafa, M.F.M.S.; Navaranjan, N.; Demirovic, A. Food cold chain logistics and management: A review of current development and emerging trends. *J. Agric. Food Res.* **2024**, *18*, 101343. [\[CrossRef\]](#)
5. European Parliament and Council of the European Union. Regulation (EU) 2024/1781—Ecodesign for Sustainable Products Regulation (ESPR). In *Official Journal of the European Union*; European Parliament and Council of the European Union: Brussels, Belgium, 2024.
6. European Parliament and Council of the European Union. Regulation (EU) 2023/1542 concerning batteries and waste batteries. In *Official Journal of the European Union*; European Parliament and Council of the European Union: Brussels, Belgium, 2023.
7. European Commission, DG Environment. *ESPR Working Plan 2025–2030*; Technical Report; European Commission: Brussels, Belgium, 2025.
8. Catena-X Automotive Network. *Catena-X: The Open Data Ecosystem for the Automotive Value Chain*; Technical Report; Catena-X: Berlin, Germany, 2024.
9. Groth, J. On the size of pairing-based non-interactive arguments. In *Advances in Cryptology—EUROCRYPT 2016*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2016; Volume 9666, pp. 305–326.
10. Khairy, S. Privacy-Preserving Digital Product Passports for Container Logistics: Design, Implementation and Experimental Evaluation of a oneM2M, EPCIS 2.0 and IOTA Platform with Zero-Knowledge Proofs. Master’s Thesis, University of Pisa, Pisa, Italy, 2026. Available online: <https://etd.adm.unipi.it/theses/available/etd-03092026-105158/> (accessed on 3 June 2026).
11. Falcitelli, M.; Misal; Noto, S.; Pagano, P. Development of a Multi-Radio Device for Dry Container Monitoring and Tracking. *IoT* **2024**, *5*, 187–211. [\[CrossRef\]](#)
12. Falcitelli, M.; Noto, S.; Pagano, P.; Gharbaoui, M.; Isca, A.; Fresi, F.; Mancina, A.; Toffetti, M.; Amatruda, A.; Bondoni, N.; et al. Full-Scale Assessment of the “5GT System” for Tracking and Monitoring of Multimodal Dry Containers. *IoT* **2024**, *5*, 922–950. [\[CrossRef\]](#)
13. Kumar, N.; Falcitelli, M.; Kotopoulos De Angelis, F.; Pagano, P.; Noto, S. Evaluating Binary Serialization Protocols for IoT/M2M Applications over Hybrid Terrestrial and Non-Terrestrial Networks. *Telecom* **2026**, *7*, 43. [\[CrossRef\]](#)
14. ISO/IEC 19987; EPCIS Standard, Release 2.0. GS1: Brussels, Belgium, 2022.
15. ISO/IEC 19988; Core Business Vocabulary (CBV) Standard, Release 2.0. GS1: Brussels, Belgium, 2022.
16. oneM2M. *oneM2M Technical Specification: Functional Architecture (TS-0001)*; Technical Report; oneM2M: Sophia Antipolis, France, 2023.
17. Martigne, P. Overview of ETSI machine-to-machine and oneM2M architectures. In *Machine-to-Machine (M2M) Communications*; Elsevier: Amsterdam, The Netherlands, 2015; pp. 27–46.
18. KETI and OCEAN. *Mobius: Open-Source oneM2M IoT Server Platform*; Technical Report; oneM2M: Sophia Antipolis, France, 2024.
19. Lee, J.; Lee, J.; Wang, Z.; Song, J. Enhancing IoT Common Service Functions with Blockchain: From Analysis to Standards-Based Prototype Implementation. *Electronics* **2026**, *15*, 123. [\[CrossRef\]](#)
20. ISO 668:2020; Series 1 Freight Containers: Classification, Dimensions and Ratings. International Organization for Standardization: Geneva, Switzerland, 2020.
21. ISO/TS 18625; 2017 Freight Containers Container Tracking and Monitoring Systems (CTMS): Requirements. ISO: Geneva, Switzerland, 2017. Available online: <https://www.iso.org/standard/63052.html> (accessed on 21 July 2026).
22. 3GPP. Release 17 Overview for Non-Terrestrial Networks (NTN). 3rd Generation Partnership Project. 2022. Available online: <https://www.3gpp.org/technologies/ntn-overview> (accessed on 28 April 2026).
23. CNIT—National Inter-University Consortium for Telecommunications. LOGICA Project. 2026. Available online: <https://www.cnit.it/en/projects/regional-projects/logica-project/> (accessed on 28 April 2026).
24. Hulea, M.; Miron, R.; Muresan, V. Digital Product Passport Implementation Based on Multi-Blockchain Approach with Decentralized Identifier Provider. *Appl. Sci.* **2024**, *14*, 4874. [\[CrossRef\]](#)

25. Abreu, H.; Pereira, V.; Barata, J. Blockchain-based digital product passport: Design principles and demonstration. *Int. J. Prod. Res.* **2025**, *63*, 5863–5882.
26. Xia, H.; Li, J.; Li, Q.; Milisavljevic-Syed, J.; Salonitis, K. Integrating blockchain with digital product passports for managing reverse supply chain. *Procedia CIRP* **2025**, *132*, 215–220. [[CrossRef](#)]
27. Neri, A.; Butturi, M.A.; Sauer, H.L.; Lolli, F.; Gamberini, R.; Sellitto, M.A. Distributed Ledger Technology selection for Digital Battery Passport: A BWM-TOPSIS approach. *IFAC-PapersOnLine* **2024**, *58*, 480–485. [[CrossRef](#)]
28. Hyperledger. *Hyperledger Fabric Documentation*; Technical Report; Hyperledger: San Francisco, CA, USA, 2024.
29. Maersk and IBM. *TradeLens: Digitizing the Global Supply Chain*; Technical Report; Maersk and IBM: Copenhagen, Denmark, 2022.
30. Alsbouy, T.; Al-Aqrabi, H.; Manasrah, A.; Artemi, M. Toward a secure and scalable IoT: A survey of IOTA-based distributed ledger technologies. *Sustain. Comput. Inform. Syst.* **2025**, *48*, 101225. [[CrossRef](#)]
31. Nzakuna, P.S.; Paciello, V.; Lay-Ekuakille, A.; Lusala, A.K.; Iacono, S.D.; Pietrosanto, A. From IOTA Tangle 2.0 to Rebased: A Comparative Analysis of Decentralization, Scalability, and Suitability for IoT Applications. *Sensors* **2025**, *25*, 3408. [[CrossRef](#)] [[PubMed](#)]
32. Carelli, A.; Palmieri, A.; Vilei, A.; Castanier, F.; Vesco, A. Enabling Secure Data Exchange through the IOTA Tangle for IoT Constrained Devices. *Sensors* **2022**, *22*, 1384. [[CrossRef](#)] [[PubMed](#)]
33. Trade and Logistics Information Pipeline (TLIP). Official Website of TLIP. 2025. Available online: <https://www.tlip.io/> (accessed on 4 June 2026).
34. Farina, G.; Kocian, A.; Brunori, G.; Chessa, S.; Lai, M.B.; Nardi, D.; Schifanella, C.; Bonura, S.; Masi, N.; Comella, S.; et al. Interoperable Traceability in Agrifood Supply Chains: Enhancing Transport Systems Through IoT Sensor Data, Blockchain, and DataSpace. *Sensors* **2025**, *25*, 3419. [[CrossRef](#)] [[PubMed](#)]
35. IOTA Foundation. IOTA Manifesto: The World Onchain—Vision for a Trade-Native Digital Infrastructure. Technical Blog/Position Paper. 2026. Available online: <https://blog.iota.org/iota-manifesto/> (accessed on 4 June 2026).
36. Muñoz-Tapia, J.L.; Belles, M.; Isabel, M.; Rubio, A.; Baylina, J. Circom: A robust and scalable language for building complex zero-knowledge circuits. *IEEE Trans. Dependable Secur. Comput.* **2022**, *20*, 4733–4751.
37. Bellés-Muñoz, M.; Baylina, J. *snarkjs: JavaScript and WASM Implementation of zkSNARK Schemes*. Version 0.7.6; GitHub Repository; 2023. Available online: <https://github.com/iden3/snarkjs> (accessed on 21 July 2026).
38. Yiannas, F. *A New Era of Food Transparency Powered by IBM Food Trust*; Walmart Corporate Announcement; Massachusetts Institute of Technology: Cambridge, MA, USA, 2018.
39. VeChain Foundation. *VeChain: Blockchain-Based Supply Chain Platform*; Technical Report; VeChain Foundation: Shanghai, China, 2024.
40. Silveirinha, J.C.; Bhandari, M.; Ferreira, J.C.; Martins, A.L. Enhancing maritime supply chain security and efficiency: A review of Zero-Knowledge Proofs in blockchain applications. *Marit. Policy Manag.* **2025**, *1*–23. [[CrossRef](#)]
41. OpenZeppelin. *@openzeppelin/merkle-tree: JavaScript Library for Merkle Trees*, Version 1.0; GitHub Repository; 2023. Available online: <https://github.com/OpenZeppelin/merkle-tree> (accessed on 21 July 2026).
42. European Parliament and Council of the European Union. Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS). In *Official Journal of the European Union*; European Parliament and Council of the European Union: Brussels, Belgium, 2014.
43. European Parliament and Council of the European Union. Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. In *Official Journal of the European Union*; European Parliament and Council of the European Union: Brussels, Belgium, 2024.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.