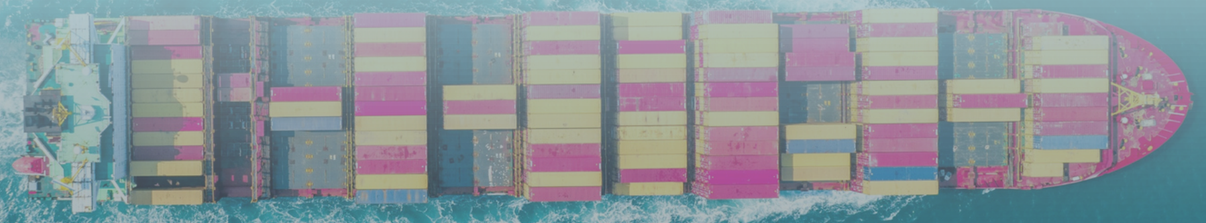
consorzio nazionale
interuniversitario
per le telecomunicazioni

Università di Pisa

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



Candidate: Samiullah Khairy

Supervisor: Dott. Paolo Pagano

Academic year 2025/2026

PROBLEM/MOTIVATION

WHY CONTAINER LOGISTICS NEEDS INTEROPERABLE, AUDITABLE AND PRIVACY-PRESERVING PRODUCT PASSPORTS

Missing maritime DPP standard

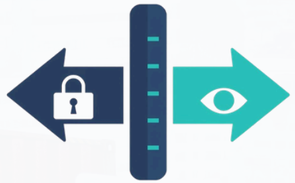
No maritime-specific DPP exists despite 80% of global trade moving by sea

Fragmented, siloed data

8–15 stakeholders, zero shared event format, no tamper-evident record

Privacy vs. compliance

Proving compliance forces exposing sensitive data.The maritime privacy paradox.



The trust deadlock

Share raw data or self-declare. Neither gives both verifiability and privacy.

STATE OF ART

NO PRIOR SYSTEM COMBINES ALL SIX PROPERTIES

System	Domain	EPCIS 2.0	Blockchain	ZKP	Cold-Chain	Evaluation
Catena-X	Automotive	✗	EDC	✗	✗	Limited
IBM Food Trust	Food	✗	Hyperledger	✗	✗	Limited
VeChain	Luxury-Pharma	✗	VeChainThor	✗	✗	Limited
Udokwu 2026	Generic DPP	✗	Ethereum	Proposed	✗	✗
Silveirinha 2025	Maritime	—	—	survey	—	—
Ocean DPP	**Maritime**	✓	**IOTA**	✓	✓	✓(16 exp.)

THESIS STATEMENT & RESEARCH QUESTIONS

This thesis demonstrates that blockchain-anchored Digital Product Passports with privacy-preserving zero-knowledge proof compliance verification are **technically feasible and performance-acceptable** for maritime container logistics.

RQ1 — Performance	Can the EPCIS 2.0 pipeline achieve sub-200 ms latency at sustained throughput?
RQ2 — Privacy Cost	Is Groth16 ZKP overhead acceptable for maritime IoT event intervals?
RQ3 — Immutability	Does Merkle-batched IOTA anchoring provide cost-effective tamper evidence?
RQ4 — Reliability	Does at-least-once delivery hold under realistic failure scenarios?

Four questions. Sixteen experiments. All answered affirmatively.

OUR SOLUTION – OCEAN DPP

A privacy-preserving Digital Product Passport platform for maritime containers, combining standardised events, IoT integration, zero-knowledge proofs and blockchain anchoring.

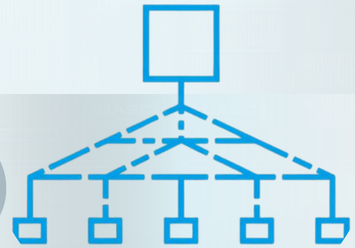
GS1 EPCIS 2.0

Event Standard

Sensor payload to EPCIS event

Groth16 ZKP

Proof of compliance



Merkle Batching

Batch and hash events

IOTA

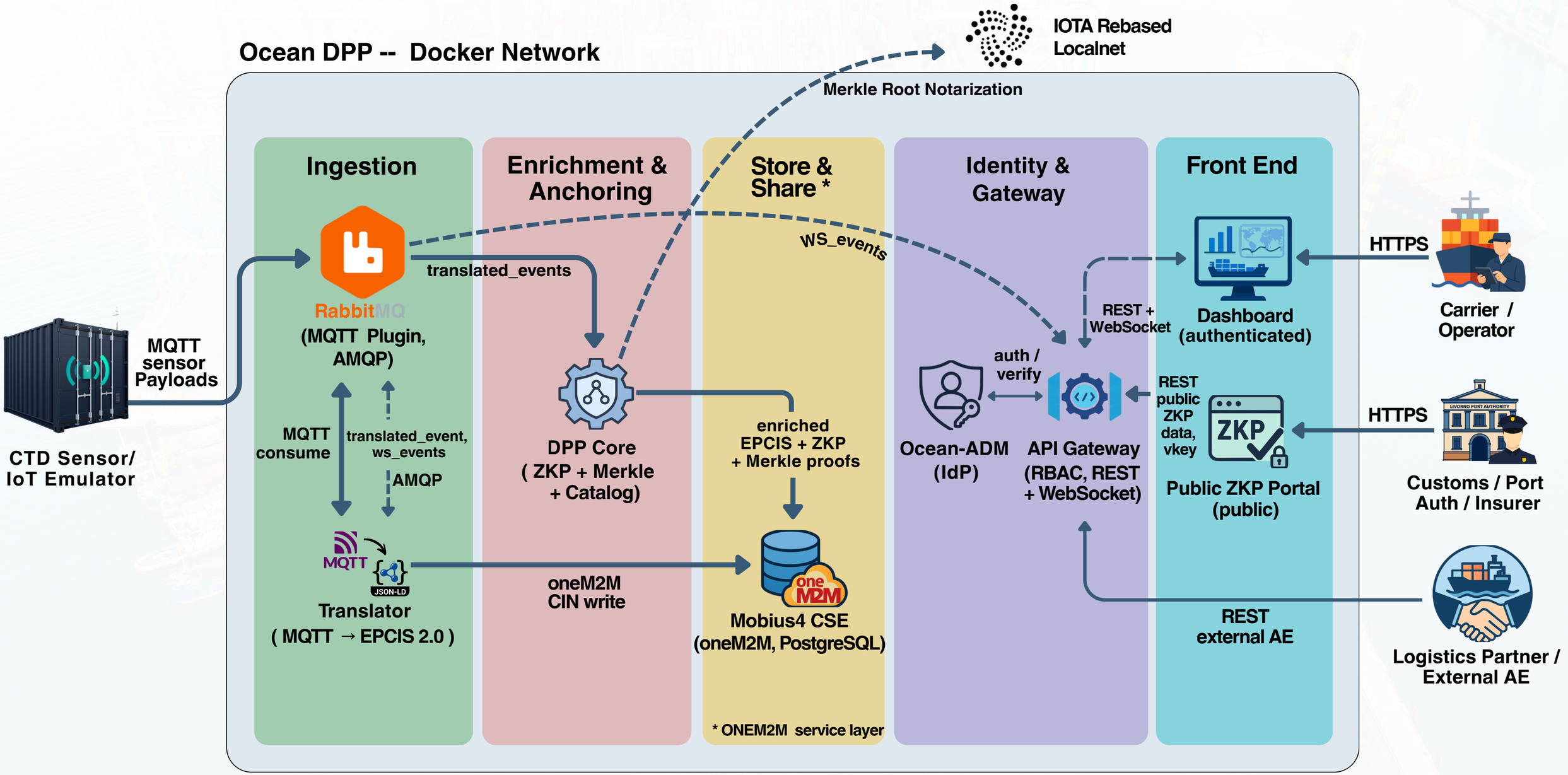
Anchor Merkle root

oneM2M

Mobius OneM2M

Store & share anchored DPP events

SYSTEM ARCHITECTURE



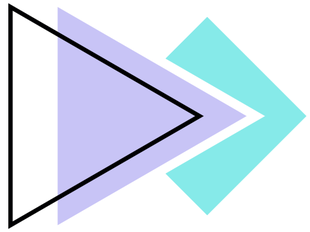
TRANSLATOR

RAW MQTT PAYLOAD

RAW MQTT PAYLOAD

```
{
  "DEVICEID": "LMCU-2847",
  "TEMP": 17.3,
  "HUMIDITY": 65,
  "GPS": "43.72,10.40",
  "TS": "2026-03-01T14:22:08Z"
}
```

No standard, No interoperability



EPCIS 2.0 JSON-LD EVENT

WHAT	Identifier:	urn:epc:id:sscc:LMCU-2847
WHEN	Event Time	2026-03-01T14:22:08Z
WHERE	B. Location:	43.72,10.40 (Port of Livorno)
WHY	B. step: Disposition:	shipping in_transit
HOW	Conditions:	sensorElement: temp 17.3°C

Standardised, interoperable — any GS1 system can read this

HOW ZKP PRIVACY WORKS

The Privacy Paradox

Without ZKP

Raw temperature data

17.3 °C, 18.1 °C, 19.5 °C...

With Ocean DPP

Groth 16 proof

Compliant

non - compliant

304 ms
proof generation

9.8 ms
browser verification

31:1
gen-to-verify ratio

Privacy Boundary

PUBLIC

- ✓ or ✗ Compliance verdict
- Threshold: 19°C
- Proof: 3 elliptic-curve points
- Merkle inclusion proof
- IOTA anchor reference

PRIVATE

- Actual temperature (17.3°C)
- Container key K_c
- Raw sensor stream

PROOF GENERATION & VERIFICATION

THE CLAIM (CIRCUIT)

Rule:
`actual_temp < max_temp`

Private:
`actual_temp, K_c`
`(container secret key)`

Public:
`Public: max_temp (19°C)`

Compiled to:
R1CS (17 constraints)

PROVER'S KNOWLEDGE

Secret witness:
sensor readings + key

Groth16 generates:
short proof π

Proof size:
3 curve points (850 bytes)

Proof reveals nothing about temp or key

VERIFIER'S CHECK

Verifier:
public data + vkey only

Runs Groth16:
verify(π, public signals, vkey)

equations hold → proof valid

No access to hidden temp or key

ZKP IMPLEMENTATION PIPELINE

SETUP PHASE (one-time)

tempBound.circom

actual_temp ≤ max_temp
LessEqThan(16)
17 R1CS constraints

circom compile

→ R1CS constraints
→ WASM witness gen

Trusted Setup

Phase 1: Hermez PoT
(200+ participants, 2^{12})
Phase 2: circuit-specific

Output Keys

proving_key.zkey
(stays on server)
verification_key.json
(pinned in portal)

RUNTIME (per event)

PROOF GENERATION (DPP Core server)

① Sensor event arrives with temp = 17.82°C
② Build witness: {temp×10, threshold×10, key}
③ snarkjs.groth16.fullProve(witness, wasm, zkey)
④ Output: proof {π_a, π_b, π_c} + publicSignals
⑤ proofHash = SHA-256(proof + signals) → Merkle leaf

VERIFICATION (browser, zero-trust)

① Load pinned vkey (build-time, not server)
② Fetch proof + publicSignals from API
③ snarkjs.groth16.verify(vkey, signals, proof)
④ true → compliant | false → violated
⑤ Compare server vkey fingerprint → tamper alert

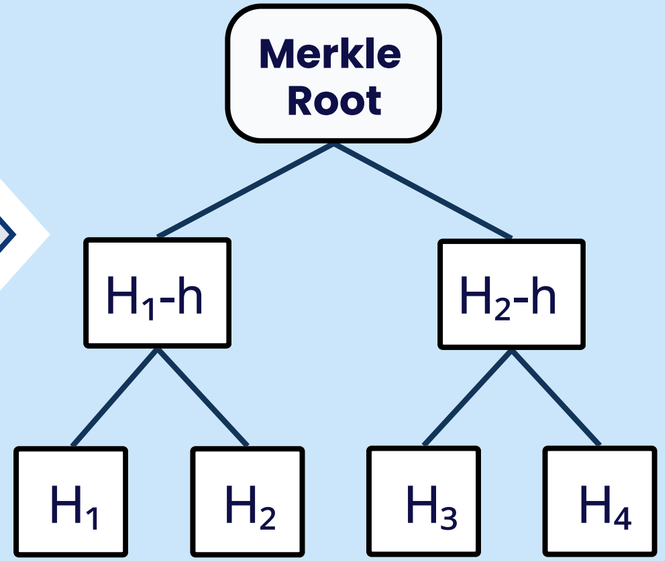
IOTA ANCHORING & MERKLE BATCHING

EVENTS

H_1
H_2
H_3
H_4
H_5
⋮
H_n

Configurable batch size (10, 50, 100)

MERKLE TREE



IOTA ANCHOR

IOTA

Locked Notarization

1 transaction per batch

Immutable · Public · Verifiable

98%
TX reduction at B=50

3.5 s
anchor latency (batch-50)

100%
tamper detection

THE SYSTEM IN ACTION

Circuit: tempBound
3/5/2026, 4:55:51 PM ± 10ms

Verified • Pinned | IOTA Anchored

ZKP PUBLIC SIGNALS (DECODED)

Compliance Result: Violated

Contract Threshold: < 19.0 °C

** The real temperature remains hidden. Math only proves it was below 19.0°C.*

Violated Compliance → Non compliant

MERKLE TREE VERIFICATION

1. Client Proof Hash (Leaf)

`0x0302f525cd1185b7cc0676991810d12bb4418952e8ad4c72a56a6a9b982db19f`

2. IOTA Anchored Merkle Root

`0x055e8c68570ba475926df6f580b1f170499b6d5019ad58b181bdef6181576aa8`

RAW PROOF ARTIFACTS (PI_A, PI_B, PI_C)

Elliptic Curve points generated by groth16, paired against the Verification Key.


```
      "1",
      "0"
    ]
  ],
  "pi_c": [
    "865538930152608572571487322917230700625607173993557500824531792962393504471 2",
    "213825508376427282250274638990802742602231366731705087412054371817045148719 63",
    "1"
  ],
  "protocol": "groth16",
  "curve": "bn128"
}
```


ANCHOR CHAIN ✓ Verified

TX DIGEST	NOTARIZATION ID
A7o5hh4JZr6SGxskuXtd7T1MeZ2177z61325rBucJo8L Explorer	5396ba537336c7e9371f73ed3a4e549674cab6f4ad757a841763ef354b9e7398
BATCH ID	**ANCHORED AT**
batch-1772726151703	3/5/2026, 4:55:55 PM

THE SYSTEM IN ACTION

Circuit: tempBound
3/5/2026, 4:53:56 PM ± 10ms

Verified • Pinned | IOTA Anchored

ZKP PUBLIC SIGNALS (DECODED)

Compliance Result: Passed

Contract Threshold: < 19.0 °C

** The real temperature remains hidden. Math only proves it was below 19.0°C.*

Passed Validation → Compliant

MERKLE TREE VERIFICATION

1. Client Proof Hash (Leaf)

`0x4271000f855b66a5aac60f7682d5ac80e0d221e1edb274c7b73867313b09ef99`

2. IOTA Anchored Merkle Root

`0xd5f57255e7d7b388400bb55ba65929d87d5c7717cc8abc69c5df8be8e3f146a1`

RAW PROOF ARTIFACTS (PI_A, PI_B, PI_C)

Elliptic Curve points generated by groth16, paired against the Verification Key.


```
    "466173257325579472405798662528625858512675186493864478798560782214219035507 4"
  ],
  [
    "1",
    "0"
  ]
],
"pi_c": [
  "109637000206889741034542898943316802363231077546130956852598395319386828255 54",
  "784851109534259499669030290302304925505213860057501304987360050455926966207 1",
  "1"
],
"protocol": "groth16",
```

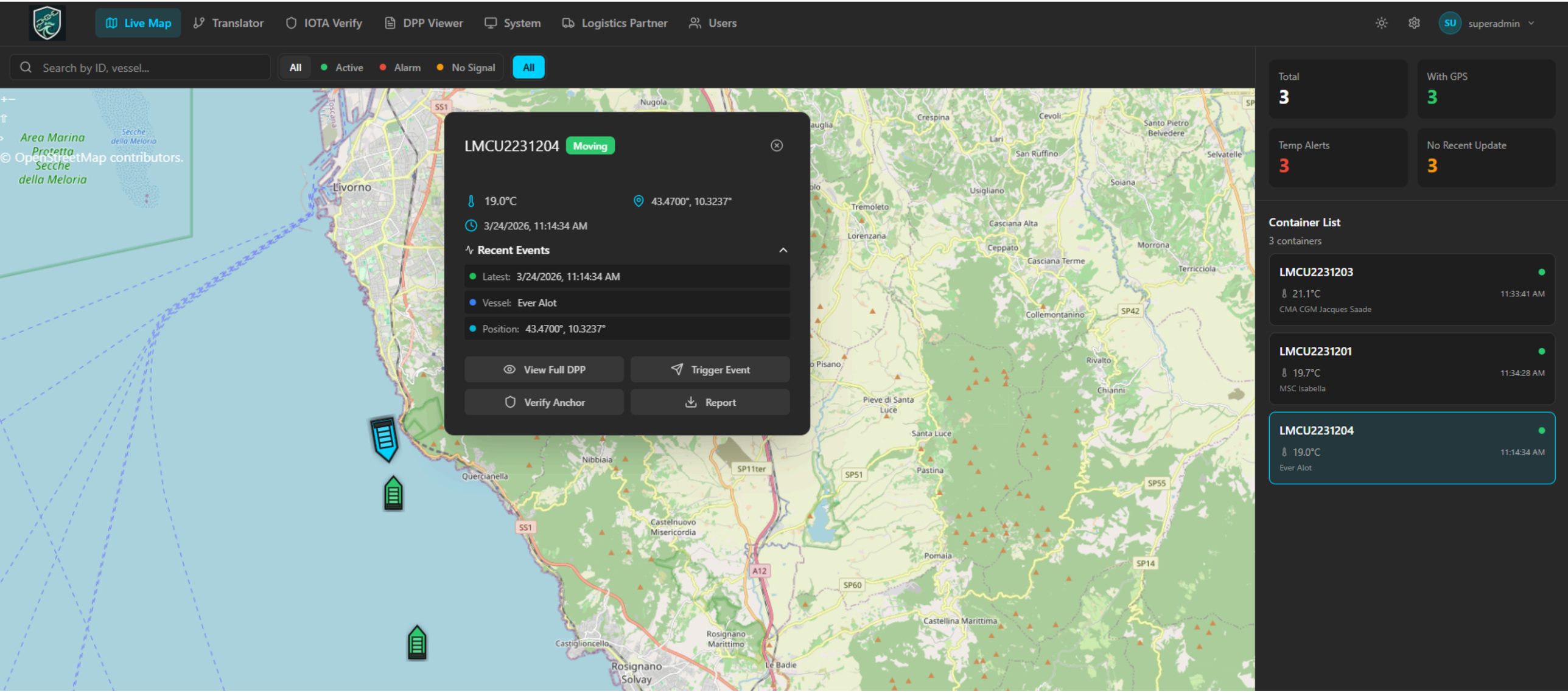

ANCHOR CHAIN

✓ Verified

TX DIGEST	NOTARIZATION ID
eBB9zZiSu8hdNmJqunW1TZsoxq7dK8wL8ZURKDWDa3o	a886fd569dc7f112f7c6e241aebe7704a905d3b7e6fda7aa98a5e0251ab7ee3a
Explorer	

BATCH ID	ANCHORED AT
batch-1772726036429	3/5/2026, 4:54:00 PM

SYSTEM WALKTHROUGH

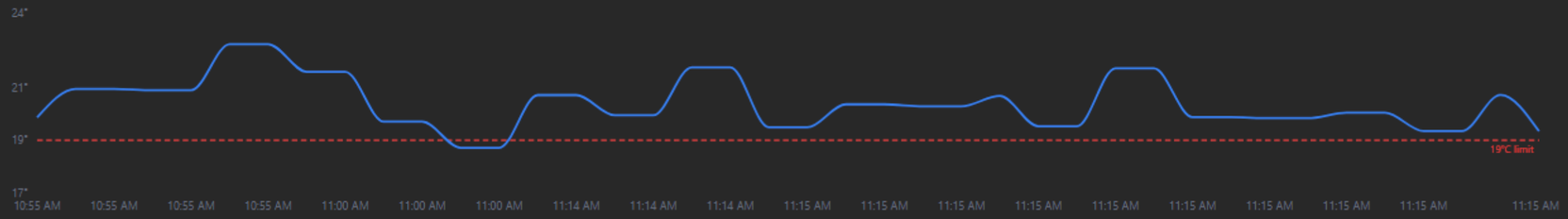


Digital Product Passport LMCU2231201 Live

Sections Timeline JSON | JSON | Share | PDF | Refresh

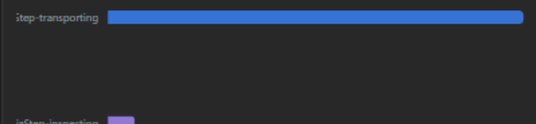
TEMPERATURE	LAST UPDATE	DISPOSITION	ACTIVE ALARMS	ZKP COMPLIANCE	IOTA ANCHORED
19.3°C	13 minutes ago	//ref.gs1.org/cbv/Disp-in transit	46	4%	100%
▲ Above 19 °C threshold	50 events loaded	//ref.gs1.org/cbv/BizStep-transporting	46 alarm events — click to view	2 / 47 proofs pass	50 of 50 events

Temperature Trend last 40 readings — ⚠ 38 exceedances



Event Breakdown 50 total events

BY BUSINESS STEP



ZKP COMPLIANCE

Compliant 2
Non-Compliant 45
Not Evaluated 3

Manufacturing

MANUFACTURER
CIMC Containers

FACTORY LOCATION
Shenzhen, China

PRODUCTION DATE
2025-01-15

BATCH NUMBER
BATCH-2025-001

Materials & Composition

MAIN MATERIAL
Corten Steel

Supply Chain & Distribution

LIVE

CURRENT STAGE
//Ref.Gs1.Org/Cbv/BizStep-Transporting

DISPOSITION
//ref.gs1.org/cbv/Disp-in transit

LAST LOCATION
43.4106, 10.3367

Usage & Operations

LIVE

LAST MAINTENANCE
2025-01-15

NEXT SERVICE
2026-01-15

Sustainability

SUSTAINABILITY SCORE

Documents & Certificates

CONTAINER CERTIFICATE
CSC Certification (CSC-2025-001)

Digital Product Passport

Container details and lifecycle information

Completion 67%

Identification

CONTAINER SERIAL
LMCU2231201

OWNER
CIMC Containers Ltd.

MODEL
DryContainerPassport

E-SEAL STATUS
Detected

Dimensions & Capacity

Metric

LENGTH
6.06 m

WIDTH
2.44 m

HEIGHT
2.59 m

WEIGHT
2200 kg

CAPACITY
33.2 m^3

MAX GROSS
30000 kg

Manufacturing

MANUFACTURER
CIMC Containers

FACTORY LOCATION
Shenzhen, China

PRODUCTION DATE
2025-01-15

BATCH NUMBER
BATCH-2025-001

Materials & Composition

MAIN MATERIAL
Corten Steel

Supply Chain & Distribution

LIVE

CURRENT STAGE
//Ref.Gs1.Org/Cbv/BizStep-Transporting

DISPOSITION
//ref.gs1.org/cbv/Disp-in transit

LAST LOCATION
43.4106, 10.3367

Usage & Operations

LIVE

LAST MAINTENANCE
2025-01-15

NEXT SERVICE
2026-01-15

Sustainability

SUSTAINABILITY SCORE
95%

CARBON FOOTPRINT
1250 kg CO_2

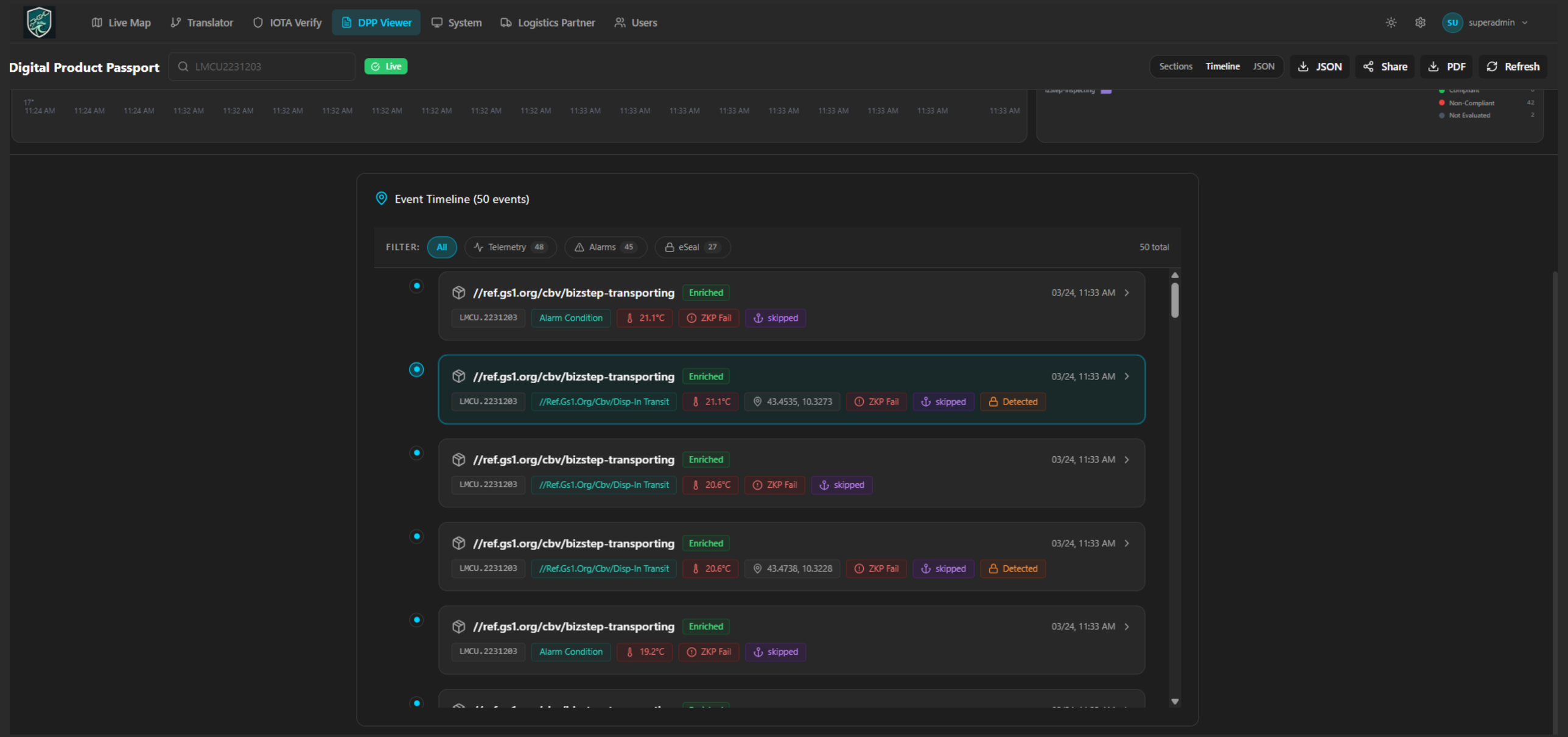
RECYCLABILITY
95% recyclable

Documents & Certificates

CONTAINER CERTIFICATE
CSC Certification (CSC-2025-001)

INSPECTION REPORT
Container Assembly & Safety Manual

CUSTOMS CLEARANCE
See Documentation


Live Map
Translator
IOTA Verify
DPP Viewer
System
Logistics Partner
Users
superadmin
Digital Product Passport
LMCU2231203
Live
Sections
Timeline
JSON
JSON
Share
PDF
Refresh
11:24 AM
11:32 AM
11:33 AM
Non-Compliant
42
Not Evaluated
Event Timeline (50 events)
FILTER:
All
Telemetry 48
Alarms 45
eSeal 27
50 total
//ref.gs1.org/cbv/bizstep-transporting
Enriched
03/24, 11:33 AM
LMCU.2231203
Alarm Condition
21.1°C
ZKP Fail
skipped
//Ref.Gs1.Org/Cbv/Disp-In Transit
43.4535, 10.3273
Detected
20.6°C
43.4738, 10.3228
19.2°C

//ref.gs1.org/cbv/bizstep-transporting Enriched

3/24/2026, 11:33:41 AM

//Ref.Gs1.Org/Cbv/Disp-In Transit | 21.1°C | 43.4535, 10.3273 | ZKP Failed | Detected

SENSOR READINGS

TEMPERATURE	HUMIDITY	SPEED
21.09 CEL	72.48 P1	11.036418052307704 MTS

HEADING	ALTITUDE	BATTERY LEVEL
173.7731154958172 DD	12 MTR	95.40597629215813 P1

SIGNAL STRENGTH
-88 DBM

EPC LIST

urn:epc:id:bic:LMCU.2231203

EVENT DETAILS

EVENT ID
ni:///sha-256;6b743f037e9c08408de7302236410b02eda82898b4e3191cadbe99d4f6e8c380

TYPE
ObjectEvent

ACTION
OBSERVE

BIZ STEP
//ref.gs1.org/cbv/BizStep-transporting

DISPOSITION
//ref.gs1.org/cbv/Disp-in transit

READ POINT
geo:43.453500062029065,10.327323494854804

ESEAL STATUS
Detected

VERIFICATION & CHAIN

ZKP RESULT
✗ Non-compliant

CIRCUIT
tempBound

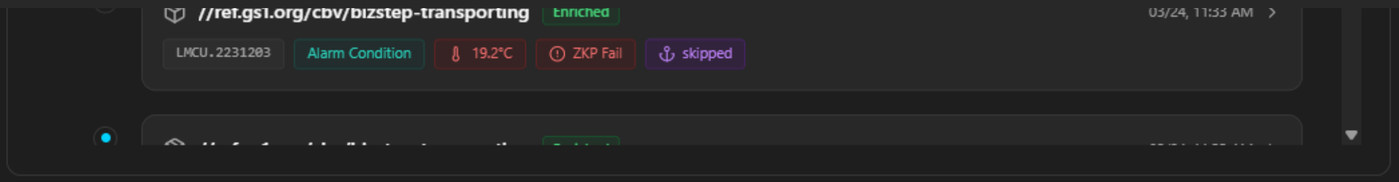
EVENT HASH
36408ece9af2ebf570c78b04ccd810b549722686ef22b506ac9a950dfa091520

HASH METHOD
sha256-canonical

IOTA STATUS
skipped

ENRICHED AT
3/24/2026, 11:33:42 AM

› Show Raw JSON



IOTA Anchor Verification

Cryptographic anchoring of DPP event snapshots on IOTA Tangle

Updated 20s ago

Search by event hash, container ID, TX digest, or Merkle root...

STATISTICS

VERIFIED (24H)
4

MERKLE BATCHES
4

MERKLE PROOFS
52

FAILED
0

FILTER

All Records
Merkle Batches
Merkle Proofs
Failed

IOTA NODE

Private Node
http://172.25.1.93:9000
Total anchors: 56

Anchor Verification Result

Verified | Merkle Batch

MERKLE ROOT

0x482dd4ae0692b98cd2d71b5afb36e251da438ea005e87744843ec96950ef7514

CONTAINER ID
LMCU2231201

ANCHORED AT
3/5/2026, 4:55:39 PM

BATCH ID
batch-1772726136026

LEAF COUNT
1 events

TX LATENCY
3494ms

IOTA TRANSACTION DIGEST

95BUs7RxXA5RZvrLiEW6BBjKUhatHfjCT82EGedpaMGd

Explorer

Notarization object: 2ff38ddd5ba985df...122bbb

Download Proof

← Back to list

Anchor chain — LMCU2231201

Audit Trail

4 records

A7o5hh4JZr...ucJo8L
Merkle Batch
LMCU2231201
3/5/2026, 4:55:55 PM · 25 events

95BUs7RxXA...dpaMGd
Merkle Batch
LMCU2231201
3/5/2026, 4:55:39 PM · 1 events

eBB9zZiSu8...DWDa3o
Merkle Batch
LMCU2231201
3/5/2026, 4:54:00 PM · 25 events

4oAEBp5MYg...drjvJW
Merkle Batch
LMCU2231201
3/5/2026, 4:52:11 PM · 1 events

05/03/2026, 16:52:10	# sha-256;282f67…d5a802c0	//Ref.Gs1.Org/Cbv/BizStep-Transporting	//Ref.Gs1.Org/Cbv/Disp-In Transit	Anchored	Valid	Internal	
05/03/2026, 16:52:09	# sha-256;0ba919…0296a694	//Ref.Gs1.Org/Cbv/BizStep-Transporting	Alarm Condition	Anchored	Failed	Internal	
05/03/2026, 16:52:09	# sha-256;90cb4a…f4e9cade	//Ref.Gs1.Org/Cbv/BizStep-Transporting	//Ref.Gs1.Org/Cbv/Disp-In Transit	Anchored	Failed	Internal	
05/03/2026, 16:52:08	# sha-256;b3ba1e…0e702447	//Ref.Gs1.Org/Cbv/BizStep-Transporting	//Ref.Gs1.Org/Cbv/Disp-In Transit	Anchored	Failed	Internal	
05/03/2026, 16:52:07	# sha-256;db5484…6fa34693	//Ref.Gs1.Org/Cbv/BizStep-Transporting	//Ref.Gs1.Org/Cbv/Disp-In Transit	Anchored	Failed	Internal	
05/03/2026, 16:52:06	# sha-256;29a78a…839ec679	//Ref.Gs1.Org/Cbv/BizStep-Transporting	Alarm Condition	Anchored	Failed	Internal	
05/03/2026, 16:52:06	# sha-256;812ec0…1f1acec1	//Ref.Gs1.Org/Cbv/BizStep-Transporting	//Ref.Gs1.Org/Cbv/Disp-In Transit	Anchored	Failed	Internal	

Submit Observation (POST ObjectEvent as logistics partner)

Container ID: LMCU2231201

Action: OBSERVE

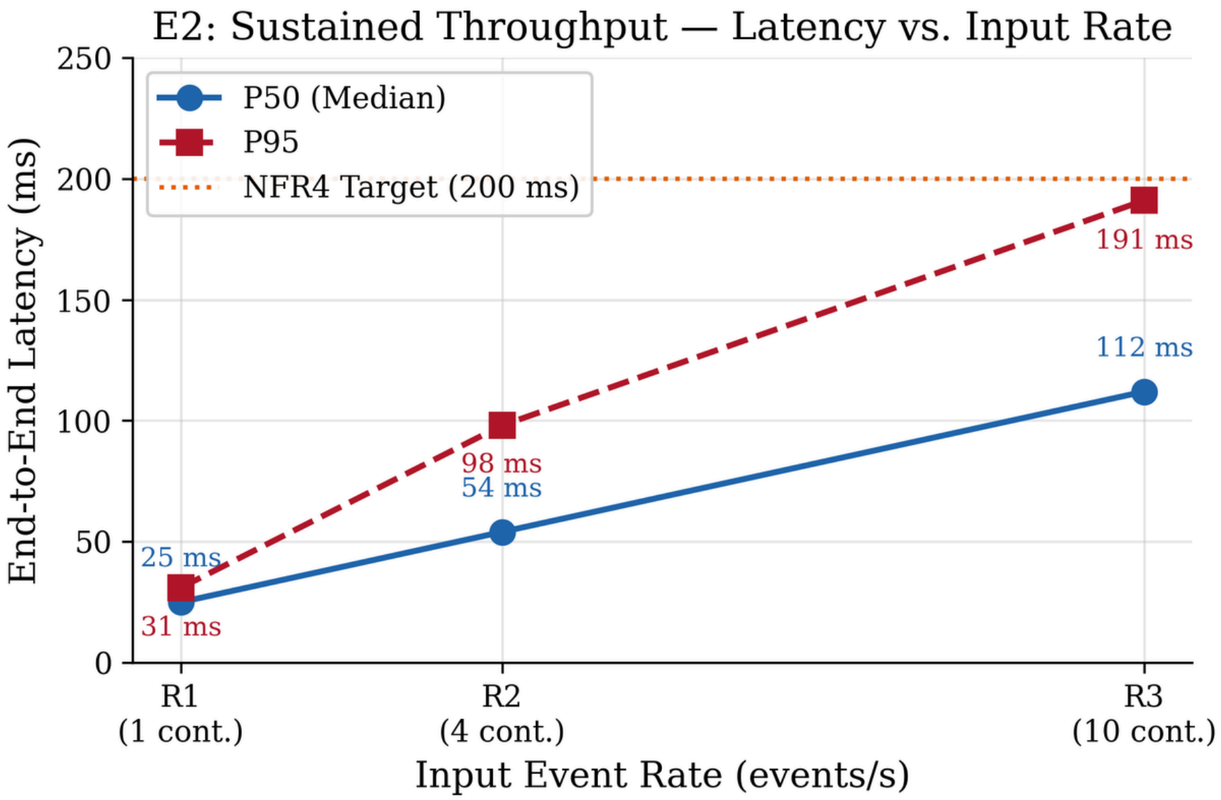
Business Step: Shipping

Submit Event

The backend will assign the GS1 NI-URI eventID, ZKP proof, and IOTA anchor automatically. Raw telemetry is not required here.

RESULTS — PERFORMANCE (RQ1)

Can the EPCIS 2.0 pipeline achieve sub-200 ms latency at sustained throughput?

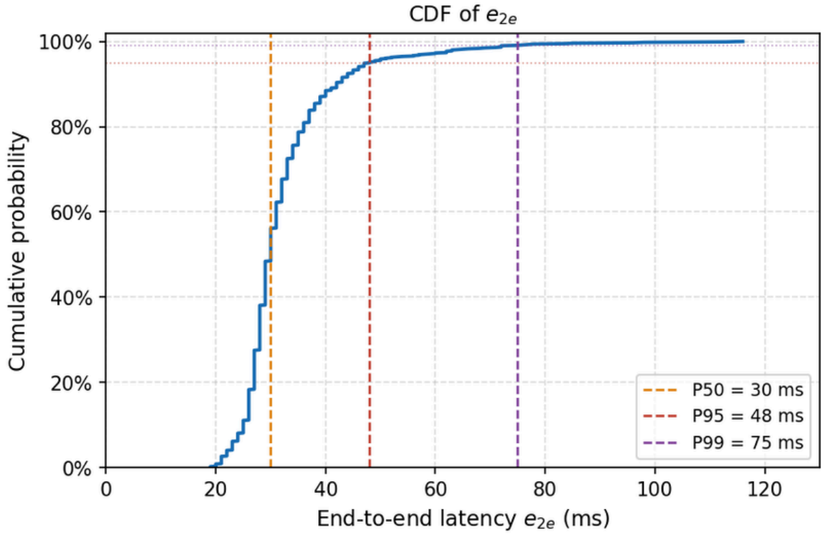


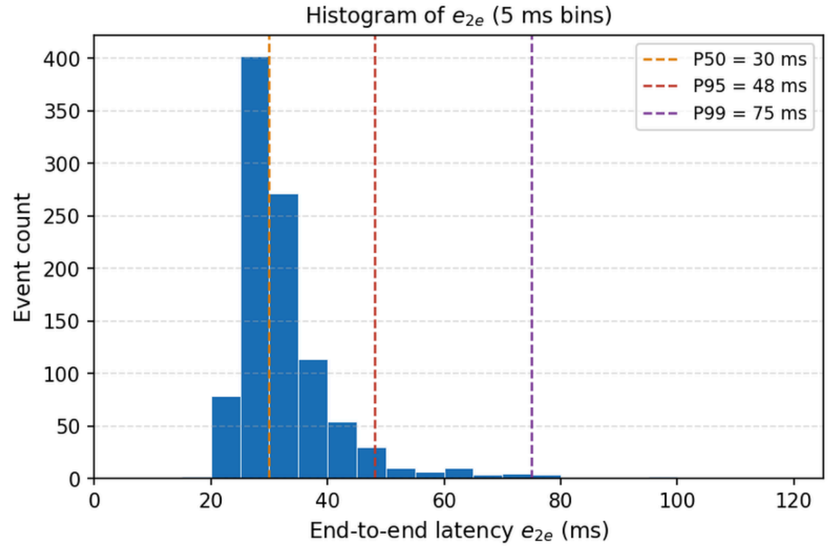
48 ms P95 baseline latency

7 ev/s sustained throughput

NFR4 ✓ below 200 ms target

E1: Baseline latency distribution

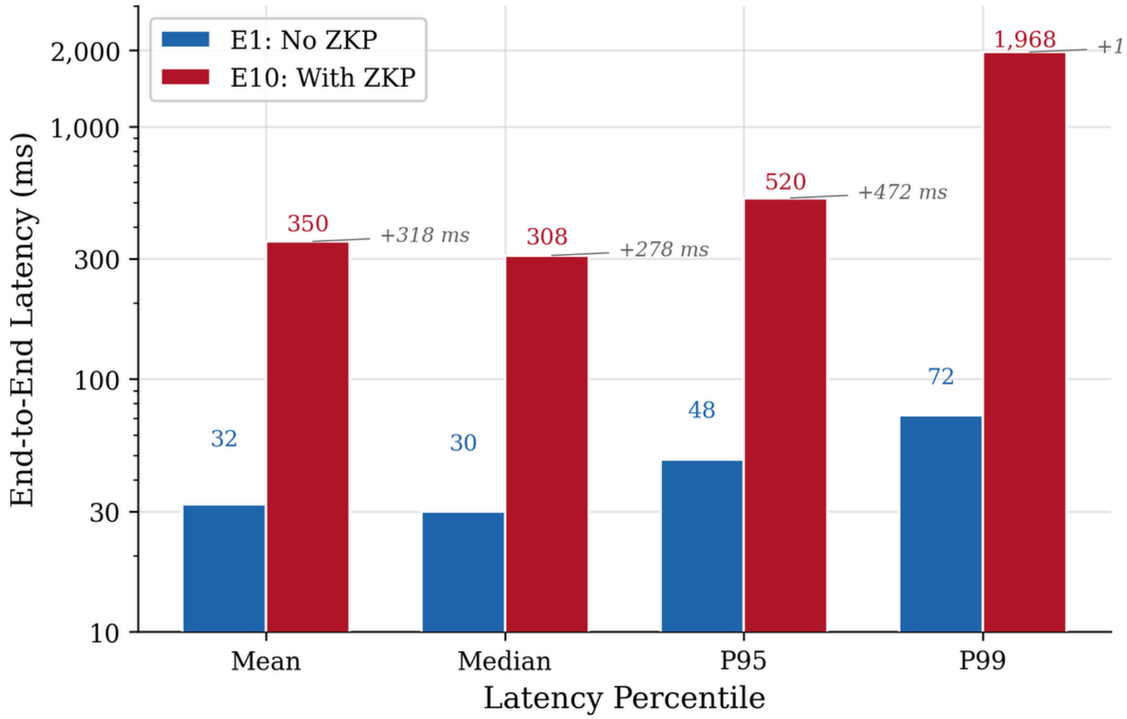




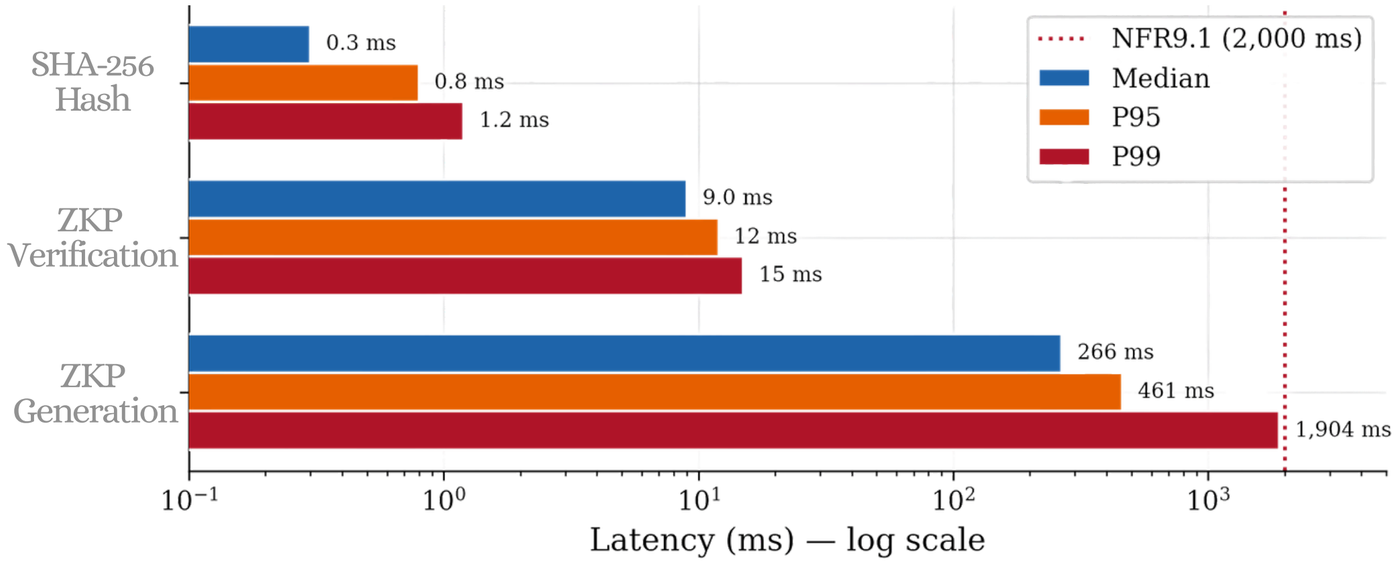
RESULTS — PRIVACY COST (RQ2)

Is Groth16 ZKP overhead acceptable for maritime IoT event intervals?

E5: ZKP Operation Latency



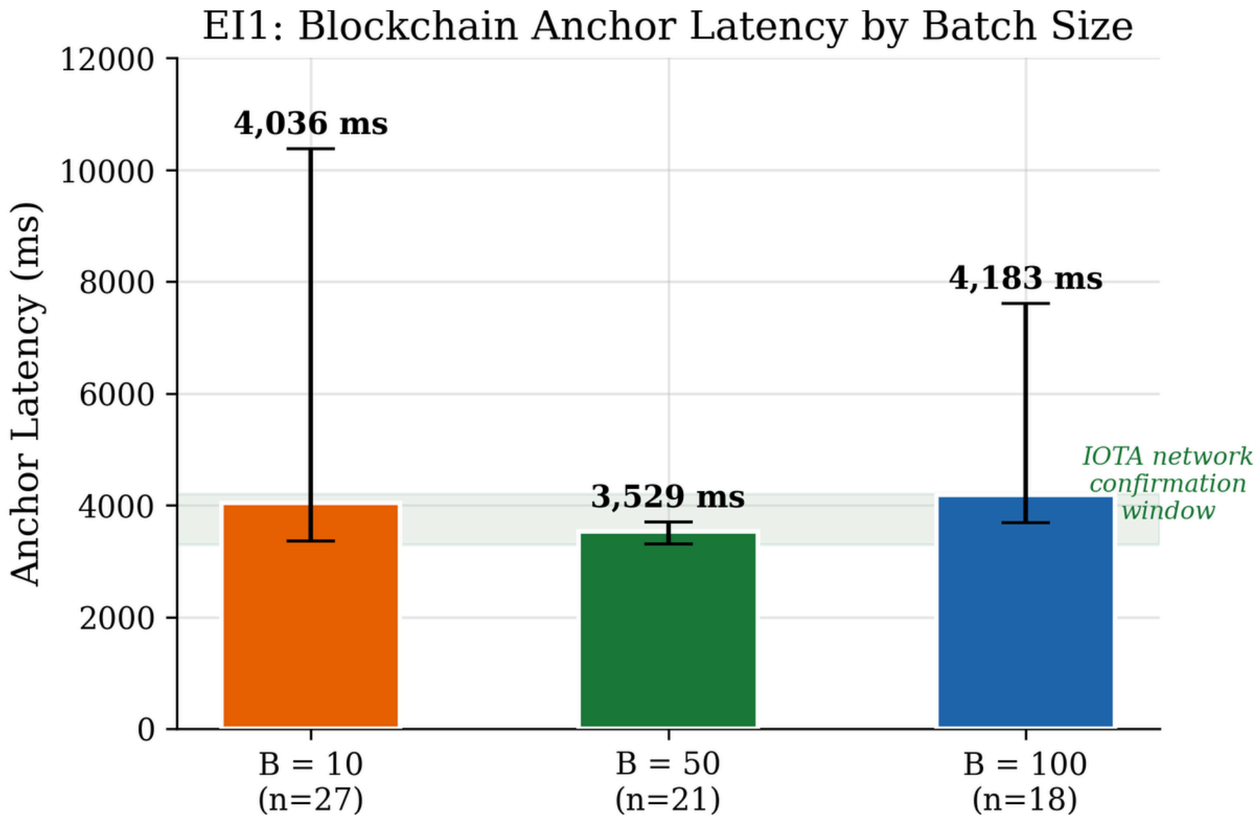
E10: ZKP Overhead on Pipeline

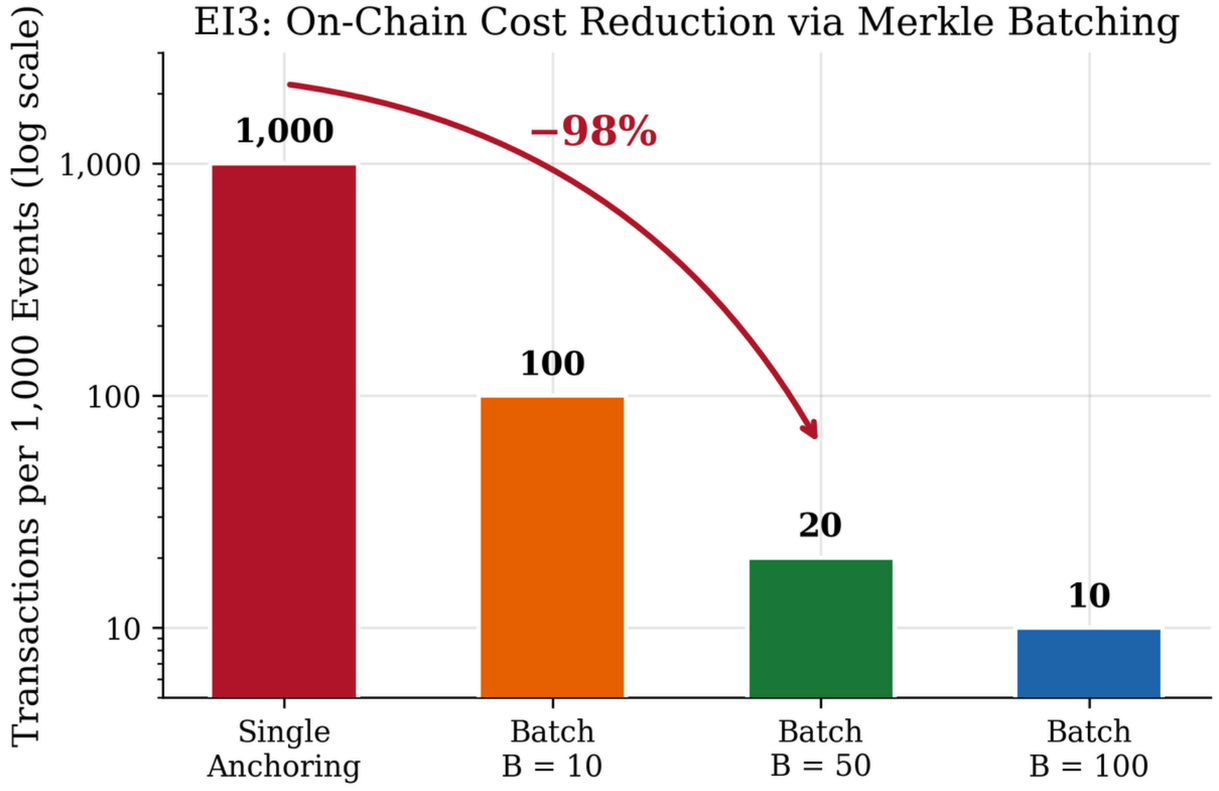


304 ms	9,8 ms	31:1	+318 ms
proof generation mean	brower verification mean	gen-to-verify ratio	extra overhead with ZKP on

RESULTS — IMMUTABILITY & COST (RQ3)

Does Merkle-batched IOTA anchoring provide cost-effective tamper evidence?

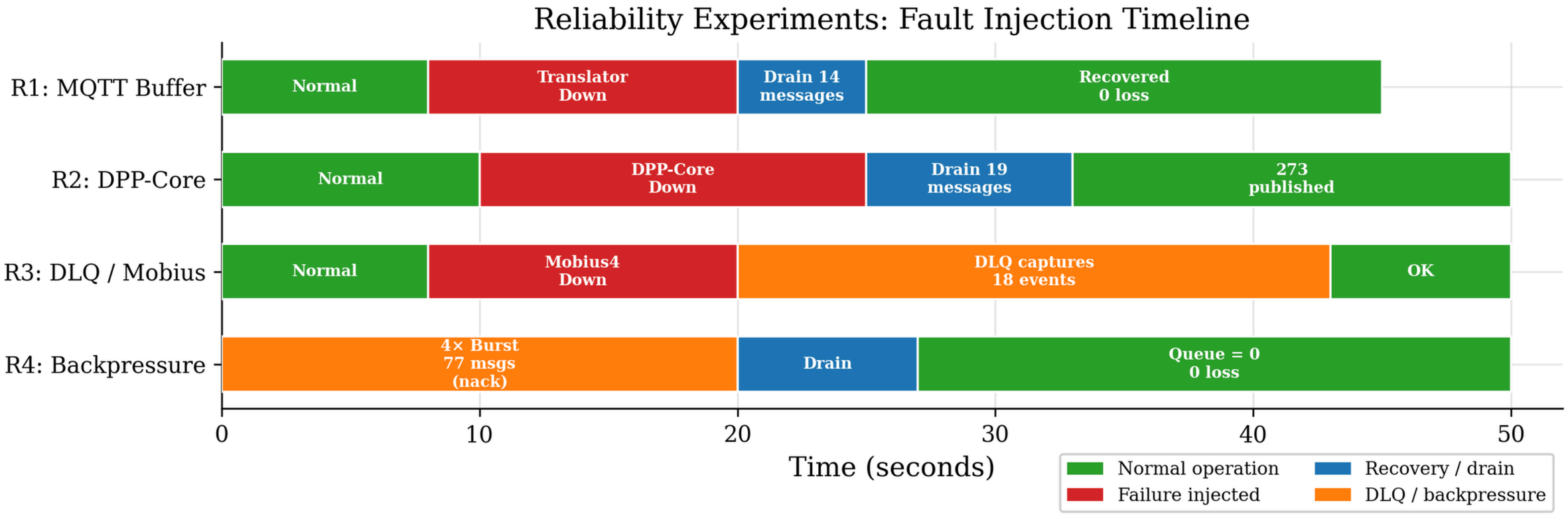




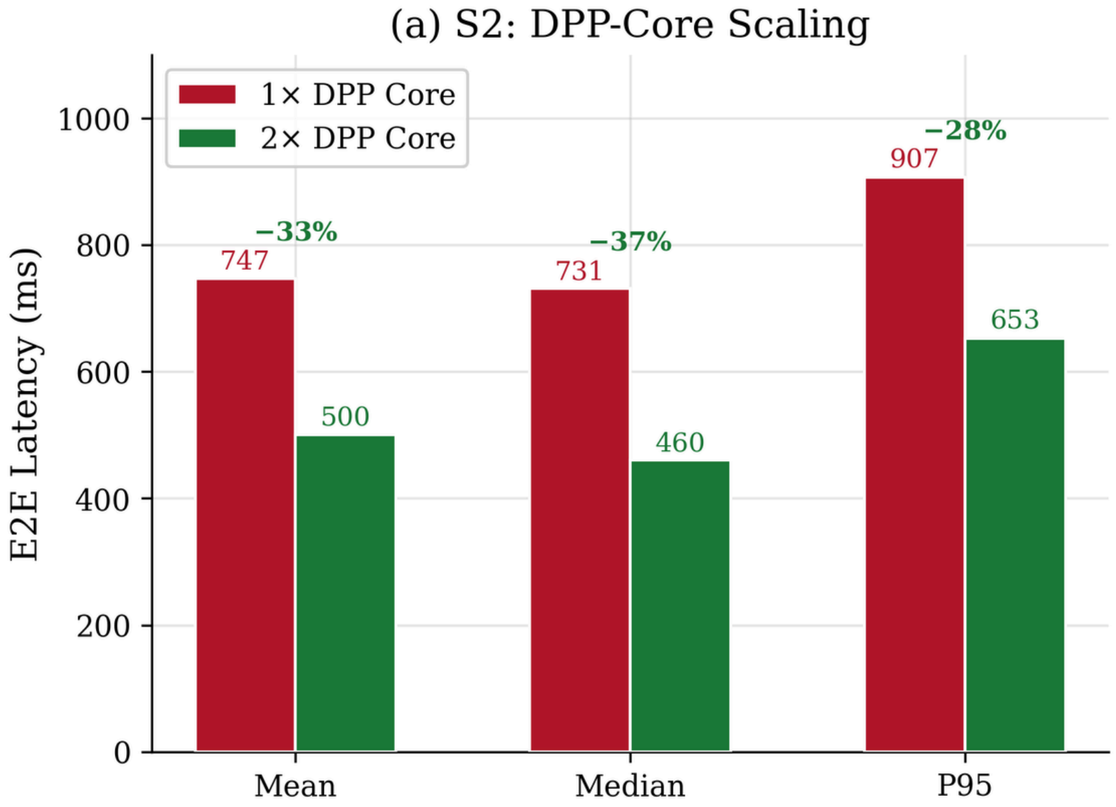
3.5 s	98%	100%
anchor latency (B=50, non-blocking)	TX reduction at B=50	tamper detection

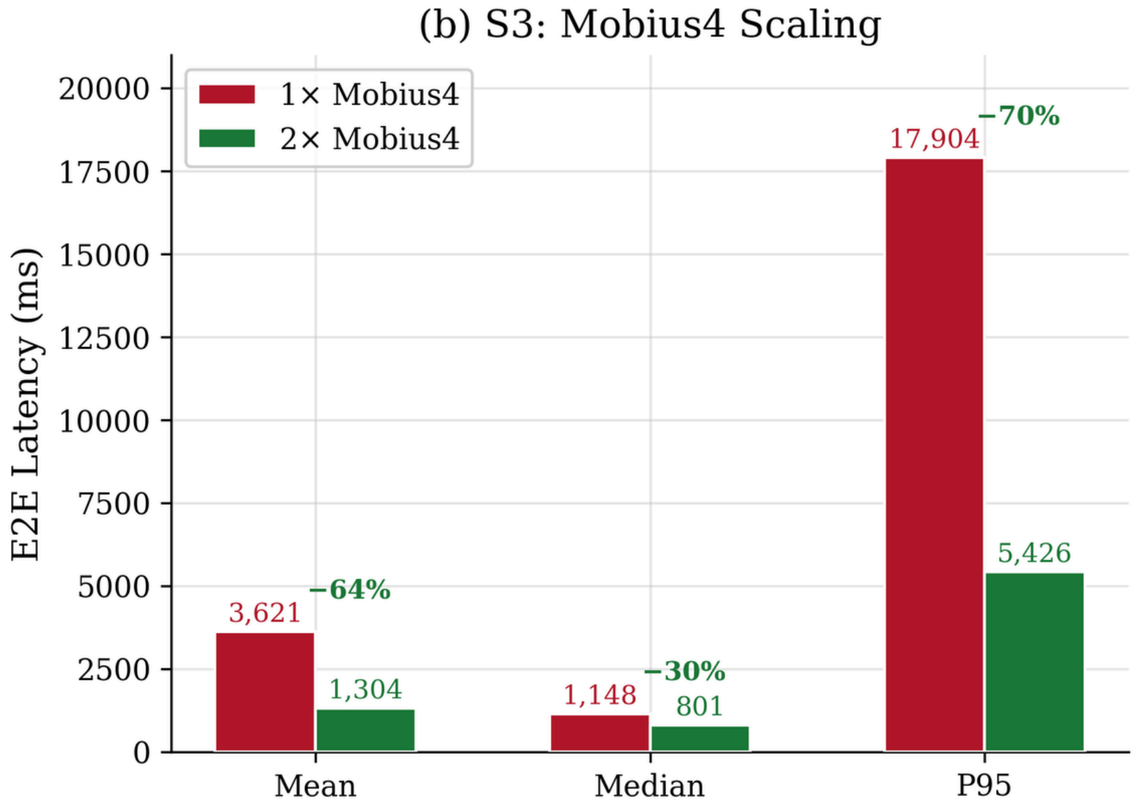
RESULTS — RELIABILITY & SCALING (RQ4)

Does at-least-once delivery hold under realistic failure scenarios



RESULT - SCALABILITY





−37%
median latency
2× DPP Core, $p < 0.001$)

+74%
throughput
(2× Mobius4, errors 810 → 0)

FIELD TEST — REAL CONTAINER, REAL ROUTE

Italy ⟷ Germany

container round-trip

- Commercial Container Tracking Device (CTD)
- Live MQTT telemetry over public internet
- Platform deployed on cloud VM with TLS
- Multi-day voyage with real connectivity

End-to-End Confirmed

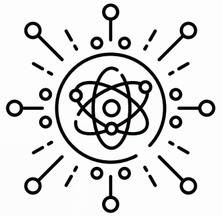
- ✓ MQTT ingestion from real CTD
- ✓ EPCIS 2.0 event generation
- ✓ Groth16 proof creation
- ✓ IOTA blockchain anchoring
- ✓ Dashboard + portal display

Note: This was an exploratory qualitative test, not part of the controlled benchmark series. It confirms operational viability with real hardware under real-world conditions.

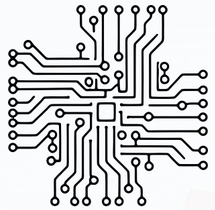
LIMITATIONS

1. Groth16 trusted setup, non–post-quantum; metadata still visible
2. Single ZKP circuit (temperature bound with public threshold)
3. IOTA localnet only; mainnet cost and latency unmeasured
4. Limited scale (≤100 containers); no 10k+ TEU experiments yet
5. Synthetic emulator workloads; only one real CTD field test.

FUTURE WORKS



Post-quantum / universal-setup proofs (PLONK, Halo2, STARKs)



More circuits: humidity, route, multi-condition proofs

IOTA mainnet evaluation and batch-size optimisation.

Large-scale pilot with real carriers, customs, and insurers.

CONTRIBUTIONS

C1

Ocean DPP Architecture

First maritime DPP platform integrating oneM2M, EPCIS 2.0, ZKP, and IOTA in a single microservice architecture with formal threat model and RBAC.

C2

ZKP-EPCIS Integration

First integration of Groth16 zero-knowledge proofs with the GS1 EPCIS 2.0 standard. Resolves the maritime privacy paradox: verifiable compliance without raw data disclosure.

C3

IOTA Merkle Batch Anchoring

Configurable event batching with Merkle trees. 98% on-chain TX reduction at B=50 while preserving per-event tamper evidence via inclusion proofs.

C4

Comprehensive Quantitative Evaluation

16 experiments covering performance, ZKP cost, scalability, IOTA anchoring, EPCIS compliance, and reliability — plus an exploratory field test with a real CTD.

These four contributions fill all six research gaps identified in the literature review.

CONCLUSION

In practice, a GS1 EPCIS 2.0–based Digital Product Passport, anchored on IOTA and combined with zero-knowledge proof checks, can deliver verifiable compliance for maritime container logistics without exposing raw operational data.

Thank you