



Blockchain-Enabled Security, Trust and Intelligent Safety in Transportation Systems: A Review

Tamnar Pratiksha Bhaskar¹, Bangar Abhishek Popat², Bhosale Sachin Bajirao³

¹ Department of Computer Engineering / Jaihind College of Engineering / SPPU, Pune, India

² Department of Computer Engineering / Jaihind College of Engineering / SPPU, Pune, India

³ Department of Computer Engineering / Jaihind College of Engineering / SPPU, Pune, India

Abstract. Modern transport systems such as ports, roads, railways and the networks that connect them are becoming more digital, but this also exposes them to fraud, spoofing, data leakage and untrusted partners. Blockchain is widely proposed as a way to remove single points of failure and to keep tamper-proof records. This paper presents a structured narrative review of four primary studies published between 2025 and 2026, supported by related works cited inside them. The studies are organised into four themes: blockchain and zero-knowledge proofs (ZKPs) for the maritime supply chain; blockchain-based authentication and authorization for the Internet of Vehicles (IoV); blockchain-based trust management for multi-provider transport networks; and intelligent sensing for railway level-crossing safety. The reviewed work reports that ZKPs can verify documents without revealing sensitive data, that a permissioned blockchain can authenticate vehicles in about 150 ms in simulation, and that a ledger-based Level of Trust can replace untrustworthy providers within seconds. However, most results come from simulations, test beds or single-site studies, and live field validation, standard metrics and quantum-safe design are still missing. The paper contributes a thematic synthesis, a comparison of fourteen studies, a list of research gaps, a detailed conceptual five-layer architecture and a prioritised research agenda.

Keywords: Blockchain; Zero-Knowledge Proof; Trust Management; Hyperledger Fabric; Maritime Supply Chain; Internet of Vehicles; Authentication; Smart Contracts; Edge Computing; Intelligent Transportation

I. Introduction

Transport and logistics systems carry people and goods across borders, and they depend on many organisations that do not fully trust each other. Maritime transport handles nearly 90 % of global goods, yet it still relies on paper-heavy documents, many stakeholders and manual verification [10]. Research quoted in [1] estimates that about 40 % of delays at major ports are caused by administrative burdens such as manual document checking and incompatible systems. Earlier studies on blockchain in shipping report benefits such as less paperwork and fewer manual verification delays [12], [13], but also barriers to adoption [18].

The same problem appears on the road. The Internet of Vehicles (IoV) connects vehicles, roadside units (RSUs), pedestrians, sensors and the cloud, but connected vehicles can be attacked through Denial of Service (DoS), spoofing, replay and data breaches [2], [25]. In next-generation telecommunication networks, an operator may buy security and connectivity services from many providers across edge, optical, packet and cloud domains, so it must continuously decide which provider can be trusted [3]. Even in railways, level crossings remain a high-risk point, because safety depends on unpredictable road users and conventional protection cannot confirm that the crossing is clear [4].



Blockchain is attractive for all these cases because it is decentralised, keeps an immutable record and can be programmed with smart contracts. However, a blockchain alone does not solve everything. Public ledgers expose sensitive trade data, consensus can add delay, and ledgers grow over time [1], [2]. For this reason, the reviewed studies combine blockchain with other tools: zero-knowledge proofs for privacy [1], certificates and a permissioned Hyperledger Fabric network for fast authentication [2], and trust values with closed-loop monitoring for provider selection [3].

The aims of this review are to (i) summarise how blockchain-based security and trust methods are used in different transport domains, (ii) compare their techniques, results and limitations, (iii) identify the research gaps that must be closed before real deployment, and (iv) propose research directions and a conceptual architecture based only on the reviewed literature.

II Review Methodology and Literature Selection Criteria

1. Scope and Sources

This is a structured narrative review. The core of the review is a set of four primary studies [1]–[4] that were collected and read in full, covering maritime logistics, vehicular networks, multi-provider transport networks and railway safety. Related works that these studies discuss in detail (for example, other blockchain authentication schemes for IoV) were also included, and they are cited as secondary studies [5]–[37]. All numerical values in this paper are quoted as reported by the original authors; no experiment was repeated by the present authors.

2. Inclusion and Exclusion Criteria

- Included: studies that apply blockchain, zero-knowledge proofs, trust management or intelligent sensing to transport, logistics or transport-network security and safety.
- Included: studies that report a design, a simulation, a prototype or a literature-based comparison with clear methods and results.
- Included: studies published recently (2025–2026 for the primary studies), so that the review reflects current work.
- Excluded: material that was not available in full, or claims that could not be traced to a specific study.

3. Data Extraction

For every study, the following items were extracted: the problem addressed, the technology and platform used, the validation method, the main reported results and the stated limitations. These items were then grouped into themes and compared in Section IV. Table 1 lists the four primary studies.

Table 1. Primary studies selected for this review.

Ref.	Domain	Main technology	Validation type
[1]	Maritime supply chain	Blockchain with zk-SNARKs, zk-STARKs and Bulletproofs; PRISMA and DSRM methodology	Literature review of 56 studies plus a simulated prototype
[2]	Internet of Vehicles	Hyperledger Fabric, EtcdRaft consensus, smart contracts, SUMO simulator	Traffic simulation with 35 normal and 1 emergency vehicle; extended to 150 vehicles
[3]	Multi-provider transport networks (6G)	Blockchain / DLT, smart-contract offers, Level of Trust (LoT), closed loops	Laboratory demonstration with edge, optical and cloud providers
[4]	Railway level crossings	CNN / YOLO, LiDAR, radar, sensor fusion, machine learning	Narrative review of 22 sources



4. Limitations of the Review

Because the review is based on a small, selected set of papers and does not use a logged database search, it is narrative and not a full systematic review. The conclusions therefore describe the reviewed evidence and should not be read as a complete survey of the whole field.

III. Literature Review

1. Blockchain and Zero-Knowledge Proofs in the Maritime Supply Chain

Curado et al. [1] study how blockchain and ZKPs can improve efficiency, privacy and regulatory compliance in the maritime supply chain. They follow the PRISMA method for the literature review: of 141 records from Scopus and Web of Science, 46 duplicates were removed, 95 were screened, 79 were sought for retrieval, 75 were assessed and 56 studies were finally included. The solution design follows the Design Science Research Methodology (DSRM) in five stages, from problem identification to communication of results.

The main idea is that a ZKP lets one party prove that a statement is true without revealing the data behind it; ZKP-based identity sharing on blockchains has been surveyed in [14], and zk-SNARKs and zk-STARKs have been compared for blockchain identity management in [15], and a systematic comparison of zk-SNARKs, zk-STARKs and Bulletproofs for privacy-preserving authentication is given in [9]. Three use cases are described. First, a customs declaration is checked with a zk-SNARK, which proves that the declared value is above a threshold and that the HS code is in a non-restricted category without showing the product description or exact value. Second, a VAT exemption claim is proved with a zk-STARK (a transparent proof system that needs no trusted setup [16]), without uploading the full invoice. Third, a customs officer proves membership of an authorised role without revealing name or ID. Port-level blockchain architectures and readiness models are discussed in [19], [20]. The proposed port-level architecture links shippers, IoT sensors, a smart-contract ZKP verifier, the port authority and a read-only audit view for regulators through eight workflow steps.

The three ZKP protocols are compared in Table 3 of this paper. The authors recommend a hybrid approach: zk-SNARKs for frequent, latency-sensitive tasks such as customs pre-clearance, and zk-STARKs for infrequent, high-security cases such as VAT exemption. The use of ZKPs is also linked to the EU eFTI regulation, whose implementation challenges are discussed in [17]. The authors also give a threat model covering Sybil attacks, collusion among validators, quantum attacks, smart-contract exploits, metadata leakage and IoT data forgery.

A prototype was built using the Ethereum Rinkeby testnet, the ZoKrates toolkit, Node.js scripts, Ganache and MetaMask. Proof generation took about 4.2 s, on-chain verification about 170 ms, the cost was about 290,000 gas units per transaction, and all valid test cases were verified successfully. The authors clearly state that these values come from a simulation with mock freight data and not from a live port. Pilot figures from earlier projects, such as up to 70 % reduction in document processing time at Rotterdam, are taken from the literature (and Maersk's estimate that blockchain could reduce costs by 20 % is reported in [11]), while the 30–40 % cost saving and over 50 % trust improvement for the proposed system are estimates.

2. Blockchain Authentication and Authorization for the Internet of Vehicles

Alsaeed et al. [2] propose BAAIoV, a framework that uses a permissioned Hyperledger Fabric blockchain to register vehicles, authenticate them and control access to network resources. The framework is built on Hyperledger Fabric [22]. The architecture has vehicles with on-board units (OBUs), a Trusted Authority (TA), a Certificate Authority (CA), a Membership Service Provider (MSP), peer nodes and smart contracts, all connected over a 5G network. Vehicle identity is tied to an X.509 certificate, and certificate revocation lists are used to block misused identities. The network uses the EtcdRaft consensus protocol,



which is crash fault tolerant and has lower delay than Practical Byzantine Fault Tolerance (PBFT). The configuration has 3 organisations, 6 peer nodes, 3 orderer nodes, 10 transactions per block and a 2 s batch timeout.

A special feature is emergency handling. When an ambulance enters an authentication zone, a smart contract checks its certificate and emergency flag, broadcasts a signed alert to nearby vehicles and RSUs, and logs the event; vehicles that falsely claim emergency status are denied. A Python middleware connects the SUMO traffic simulator with the blockchain, so that blockchain responses change vehicle behaviour in the simulation.

The reported results are as follows. Legitimate emergency vehicles were authenticated in about 150 ms, while malicious vehicles took about 300 ms and were rejected. Ambulance arrival time fell from 93 to 81 time units (more than 12 % improvement), and the Emergency Message Delivery Success Rate (EMDSR) was 84 % compared with 68 % for the non-blockchain baseline. Replay and spoofing attacks were detected using time-bound authentication logic and certificate checks. When the number of vehicles rose from 50 to 150, the authentication delay increased from 152 ms to 187 ms and EMDSR decreased from 85.1 % to 81.9 %. Blockchain operation latencies were 6 s for registration, 3.08 s for vehicle approval, 3 s for raising an emergency flag and 0.613 s for a ledger query. In a comparison with Ethereum (supported by the platform studies [22], [23]), the authors report an authentication delay of more than 4 s and a throughput of about 20–30 TPS for Ethereum against about 150 ms and more than 1000 TPS for BAAIoV.

The authors also compare signature schemes for resource-limited OBUs: ECDSA (P-256) needs 2–4 ms to sign and 5–6 ms to verify, Rabin signatures are faster (1–2 ms and 1–3 ms) but not widely standardised, and BLS signatures have smaller size (48 bytes) but higher verification cost (12–14 ms). They note that ECC-based schemes are vulnerable to quantum attacks and mention a lightweight proof of concept with CRYSTALS-Dilithium as future work.

3. Blockchain-Based Trust Management for Multi-Provider Transport Networks

Aleman et al. [3] address a different but related problem. In a 6G environment, an operator builds an end-to-end (E2E) service from many providers in RAN, edge, optical, packet-based transport and cloud domains. Traditional security models cannot adapt to such distributed and changing environments, so the authors build on the Zero Trust idea of continuous verification. Their solution has a Security pillar and a Trust pillar. The operator defines a Security Service Level Agreement (SSLA) and a Trust Service Level Agreement (TSLA), providers register on a distributed ledger, and the operator publishes a smart-contract-based offer. When a network slice is requested, the system selects the most trustworthy providers using a Level of Trust (LoT) value.

Closed loops (CLs) monitor the providers during the service. If a provider violates the SSLA, the loop applies a mitigation action and may replace the provider. The LoT is updated from real-time metrics: small penalties (about 1–2 %) are applied for agreement violations, a larger penalty (10 %) is applied when a provider fails to stop a detected attack, and a provider that replaces another one can earn a reward of up to 10 %. The ledger protects the LoT values from being changed by a single actor, which improves resistance to Sybil and on-off attacks. The process has four phases: preparation, deployment, enforcement and termination.

The experiments used a test bed with edge, edge-IP, optical, cloud-IP and cloud providers, controlled through a graphical interface. When attacks were triggered, the affected providers were replaced by substitute providers that started with LoT = 100. The closed-loop reaction time was about 5.75 s, 6.93 s and 7.16 s for three different providers, with most of the time spent before the metrics were detected. Creating a smart-contract offer took about 68 s, of which provider registration needed 2.74 s and the provider response 8.5 s, which shows that the ledger was not the bottleneck. One ledger-related step showed a delay of about 81.2 s, which the authors explain by transaction batching and block creation. Deployment of an E2E service took



about 50 s, compared with 232.1 s in an earlier ledger-based approach, because only slice data, SLA requirements and LoT values are stored on the ledger.

4. Intelligent Safety Sensing in Rail Transport

The railway review by Gorade et al. [4] is not about blockchain, but it shows how safety systems are built in another transport domain. It covers 22 sources on level crossings, grouped into themes such as camera-based deep learning, LiDAR and radar sensing, sensor fusion, machine learning for crash prediction, and edge deployment. Fayyaz et al. [33] concluded that no single sensor technology is enough, which is why fusion is recommended. Camera systems based on CNN and YOLO give high precision (for example, precision 0.98 and recall 0.88 in a smart-camera study [34]), and a 16-channel 3D LiDAR on a low-power edge platform can detect and track objects in real time [35]. The review also notes that recall is lower than precision, and missed detections are the most dangerous error. Sensor limits in bad weather and at night are discussed in [36], and the OSDaR23 dataset provides synchronised camera, infrared, LiDAR and radar data but is recorded from a train and not from fixed crossings [37]. These observations are useful for this review because transport blockchain systems also depend on trustworthy sensor data.

5. Related Blockchain Authentication Studies

Alsaeed et al. [2] also review earlier IoV authentication schemes; a systematic review of blockchain-based IoV surveys is given in [25], and a survey of blockchain authentication in IoV in [24]. Xu et al. [5] use a multi-TA model to reduce dependence on one authority, but they assume that the TAs do not collude. Qureshi et al. [6] use Hyperledger Fabric with endorsement-based leader selection and give strong privacy, but with high computation cost. BESA-IOV [7] combines lightweight ECC with a blockchain-based public key infrastructure and reports a 35 % reduction in delay and 40 % lower overhead, but it has no mobility simulation or emergency handling. BLAP-IOVs [8] gives high communication success for V2V trust in 5G, but it does not consider emergency prioritisation and has limited scalability.

Other schemes address different needs. Wang et al. [26] combine smart contracts with hybrid PKI to counter malicious attacks, but their consensus uses a lot of energy. Hu et al. [27] use a Byzantine consensus algorithm with a trust game to improve trust and fault tolerance, at the cost of computational overhead. Bagga et al. [28] use AI-based batch authentication with dynamic clustering to reduce delay, but it needs validation at large scale. Eddine et al. [29] propose an ECC and hash-based scheme with low overhead and strong privacy, although its speed under large volumes needs improvement. Gupta et al. [30] use game theory with physically unclonable functions for low-cost, anti-cloning protection, but the protocol is complex and needs real-world testing. Luo et al. [31] note that centralised authentication creates more communication overhead as vehicle density grows, and Zhang et al. [32] use blind signatures and threshold secret sharing for anonymous data registration, but with scalability issues across regions. These works show that low delay, scalability and emergency support are rarely achieved together.

6. Synthesis

Three common patterns can be seen. First, all studies use blockchain mainly for trust: tamper-proof audit trails [1], [2], decentralised identity [2] and protected trust values [3]. Second, heavy work is moved off-chain or to the edge, such as ZKP generation in [1], the Python middleware in [2] and closed-loop monitoring in [3], so that the ledger is not slowed down. Third, almost all validation is done by simulation or in a laboratory, and not on live ports, roads or networks.

IV. Comparative Analysis of Existing Studies

Table 2 compares the primary and related studies. The reported metrics are not directly comparable, because the tasks, platforms and test conditions differ.



Table 2. Comparison of representative studies.

Author, year	Objective	Method / technology	Major reported findings	Limitations
Curado et al., 2025 [1]	Private document verification and compliance in maritime logistics	Blockchain + ZKPs; ZoKrates; Ethereum test-net	Proof ≈ 4.2 s; verification ≈ 170 ms; $\approx 290,000$ gas; 100 % success	Simulation with mock data; cost and trust gains are estimates
Alsaeed et al., 2025 [2]	Vehicle authentication and emergency prioritisation	Hyperledger Fabric; EtcDRaft; SUMO	Delay ≈ 150 ms; EMDSR 84 % vs 68 %; arrival 81 vs 93	Simulation only; assumes trusted TAs
Aleman et al., 2026 [3]	Trusted providers for E2E transport services	DLT; smart-contract offers; LoT; closed loops	Deployment ≈ 50 s; closed loop 5.75–7.16 s	Laboratory test bed; penalties chosen randomly in tests
Gorade et al., 2025 [4]	Safety at railway level crossings	CNN / YOLO, LiDAR, radar, fusion	High precision for specific tasks	Single-site, fair-weather evidence; no public dataset
Xu et al., 2021 [5]	Decentralised IoV authentication	Multi-TA blockchain	Lower computation; better cross-TA authentication	TAs assumed not to collude
Qureshi et al., 2022 [6]	Anonymous IoV authentication	Hyperledger Fabric with leader endorsement	Strong privacy and decentralisation	High computation cost; scalability
Haider et al., 2024 [7]	Lightweight IoV authentication	ECC + blockchain PKI	35 % less delay; 40 % less overhead	No mobility simulation or emergency handling
Singh et al., 2024 [8]	V2V trust in 5G IoV	Blockchain-based lightweight protocol	High communication success; low overhead	No emergency handling; limited scalability
Wang et al., 2019 [26]	Lightweight blockchain authentication	Smart contracts + hybrid PKI	Better authentication; counters malicious attacks	High energy use for consensus
Hu et al., 2019 [27]	Authentication via consensus	Byzantine consensus with trust game	Better trust and fault tolerance	Computational overhead; limited scalability
Bagga et al., 2021 [28]	Batch authentication	Blockchain with AI-based dynamic clustering	Lower delay; faster verification	Needs large-scale validation
Eddine et al., 2021 [29]	Secure grid authentication	ECC, hash functions, blockchain	Low overhead; strong privacy	Speed and scalability at large volume need work
Gupta et al., 2022 [30]	Game-theoretic authentication	PUFs, dual gaming, dPoW, PoS	Low cost; anti-cloning; anti-side-channel	Complex protocol; needs real-world testing
Zhang et al., 2019 [32]	Private data registration	Blind, threshold and multi-signatures	Anonymity; encourages data sharing	Scalability issues across regions

Table 3 compares the ZKP protocols described in [1]. It shows why no single protocol is best: zk-SNARKs give very small proofs but need a trusted setup and are not quantum-safe, while zk-STARKs remove the trusted setup and resist quantum attacks but produce much larger proofs.



Table 3. Comparison of ZKP protocols (as reported in [1]).

Protocol	Trusted setup	Proof size	Proving / verification complexity	Post-quantum secure	Suggested use in maritime logistics
zk-SNARK	Yes	$\approx 200\text{--}300$ bytes	$O(n) / O(1)$	No	Frequent, latency-sensitive checks (customs pre-clearance)
zk-STARK	No	$\approx 20\text{--}100$ KB	$O(n \log n) / O(\log n)$	Yes	Infrequent, high-security cases (VAT exemption)
Bullet-proofs	No	$O(\log n)$, small	$O(n) / O(n \log n)$	No	Small-range proofs where throughput is not critical

Table 4 compares the permissioned platform used in [2] with Ethereum. The comparison shows that a permissioned ledger with a crash-fault-tolerant consensus suits time-critical vehicle communication, whereas a public chain is slower and charges variable fees. It should be remembered that these numbers come from the authors' own benchmark, and the permissioned design gives up some openness.

Table 4. Hyperledger Fabric (BAAIoV) versus Ethereum, as reported in [2].

Metric	BAAIoV (Hyperledger Fabric)	Ethereum
Authentication delay	≈ 150 ms	> 4 s
Transaction finality	2–3 s (EtdRaft)	4–6 s (PoS)
Transaction fee	None (permissioned)	Variable gas fees
Throughput	1000+ TPS	$\approx 20\text{--}30$ TPS
Privacy support	Native MSP-based access control	Public ledger (optional zk-SNARKs)
Consensus overhead	Low	High

Some further observations can be made from the comparison. In [2], authentication delay is about 150 ms at light load but rises to 187 ms with 150 vehicles, so the delay depends on traffic density. The 3 s emergency flag latency and 6 s registration latency are also much larger than the authentication delay, so the end-to-end time of a blockchain action should be reported separately from the authentication step. In [3], the trust-based design is faster than a ledger-heavy design because less data is stored on the chain. In [1], the choice of ZKP protocol is a trade-off between proof size, speed and long-term security. Finally, the railway review [4] shows the same limitation as the blockchain studies: results look strong in a controlled setting, but field evidence is thin.

V. Research Challenges and Identified Gaps

The challenges below are those that the reviewed studies themselves mention or demonstrate. Table 5 summarises the gaps and the studies that support them.

- Validation is mostly simulated. The maritime prototype uses mock freight data on a testnet [1], the IoV framework is tested in SUMO [2], the trust solution in a laboratory [3], and rail studies are often single-site [4].
- Scalability and ledger growth. In [2], vehicles were increased only to 150 and the ledger grew with simulation time; in [1], storage and consensus delay are listed as scalability limits, and scalability and interoperability remain barriers in real port environments [21].

- Cryptographic cost and quantum risk. zk-SNARKs need a trusted setup and are not quantum-safe, zk-STARK proofs are large [1], and ECC signatures used in [2] are vulnerable to quantum attacks.
- Trust assumptions. BAAIoV assumes trusted behaviour of TAs and registered nodes, and Sybil attacks, insider threats and collusion remain open [2]. In [3], the penalty values were chosen randomly in the tests.
- Limited resources at the edge. OBUs, RSUs, port terminals and IoT devices have limited computing power and bandwidth [1], [2].
- Interoperability and legacy systems. Ports, customs and traffic systems use different formats and old IT, and there are no common standards for smart contracts and ZKP-based documents [1], [2].
- Governance, law and user adoption. Who controls smart contracts and proof circuits, how GDPR and local rules apply, and how non-technical users such as customs officers will use cryptographic tools are still open questions [1].
- Sensor and data integrity. A blockchain keeps data unchanged but cannot tell whether the sensor data was correct at the start; IoT data forgery is listed as a threat [1], and rail studies show that fusion has not been validated in bad weather or at night [4].

Table 5. Research gaps supported by the reviewed evidence.

Gap	Supporting studies	Evidence in the reviewed work
Simulation or test-bed validation only	[1], [2], [3], [4]	Mock data, SUMO, laboratory demonstration, single-site studies
Scalability not proven at real scale	[1], [2], [21]	Up to 150 vehicles only; ledger growth and storage overhead
Quantum and setup risks	[1], [2]	zk-SNARK trusted setup; ECC vulnerable; Dilithium only a proof of concept
Trust and collusion assumptions	[2], [3], [5]	TAs assumed honest; Sybil and collusion open; random penalties
Interoperability and standards missing	[1], [2]	Legacy systems; no smart-contract or ZKP standards
Governance and legal clarity	[1], [2]	Custodianship of contracts; GDPR and ITS-G5 rules
Sensor integrity and datasets	[1], [4]	IoT data forgery; no public multi-sensor crossing dataset

VI. Proposed Research Directions

1. Proposed Detailed Conceptual Architecture

To bring the reviewed ideas together, a layered architecture for secure and trusted transport systems is proposed in Fig. 1. It is derived only from the reviewed literature, and it has not been implemented or validated. The design has five horizontal layers and two vertical support blocks. Each layer receives signed events, hashes and proofs from the layer below it and returns decisions, alerts and access rights to the layer below, so that heavy computation stays near the data source and only small, verified results reach the ledger [1], [2], [3].

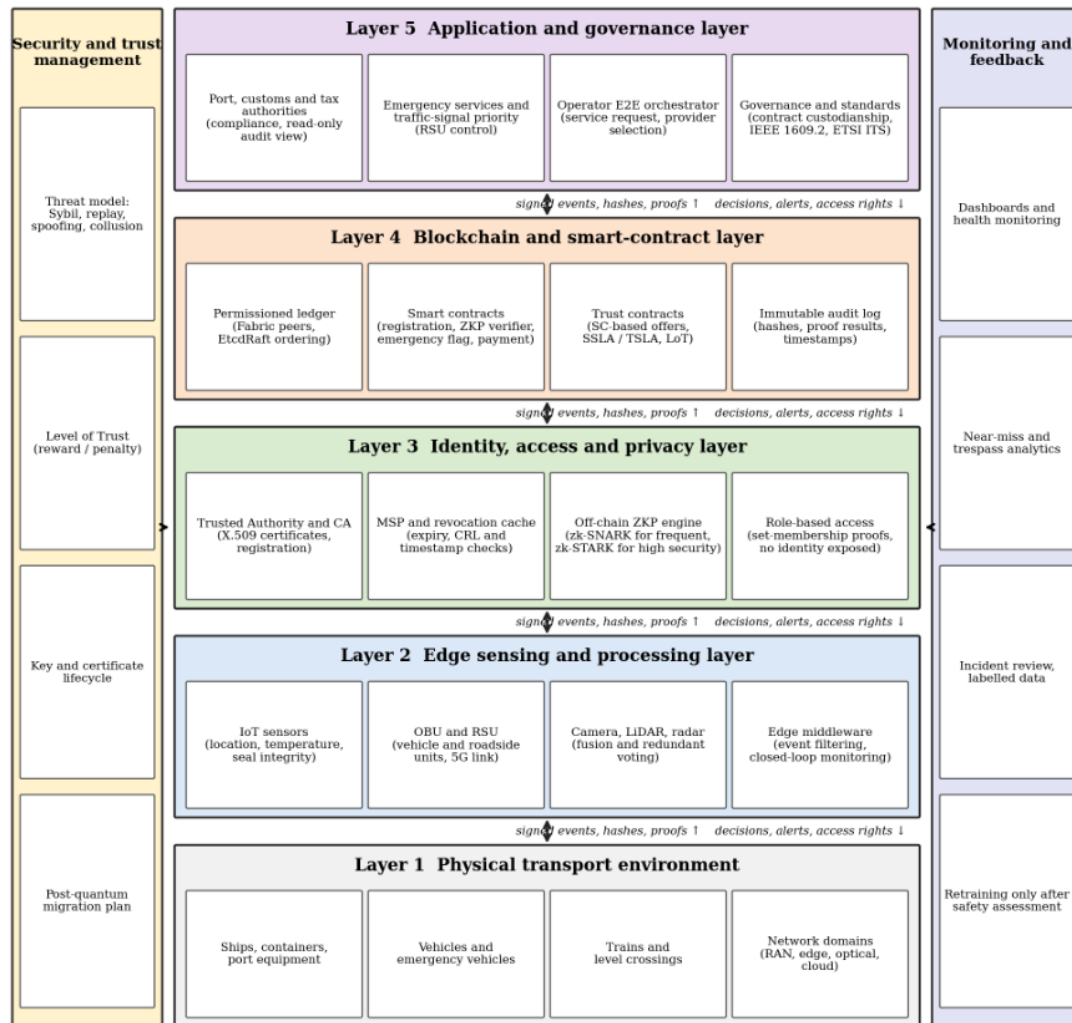


Fig. 1. Proposed detailed conceptual architecture for secure and trusted transport systems (conceptual, not experimentally validated).

2. Layer-wise Description

Table 6 explains what each layer contains, what it does and which reviewed studies it is based on.

Table 6. Layers, components and functions of the proposed architecture.

Layer	Main components	Main functions	Based on
1 Physical transport environment	Ships, containers and port equipment; vehicles and emergency vehicles; trains and level crossings; network domains (RAN, edge, optical, cloud)	Produce the events that must be secured: ship-movements, vehicle movements, crossing occupancy, service requests	[1], [2], [3], [4]



Layer	Main components	Main functions	Based on
2 Edge sensing and processing	IoT sensors (location, temperature, seal integrity); OBUs and RSUs; camera, LiDAR and radar; edge middleware with closed-loop monitoring	Capture data, filter relevant events, run fusion and detection locally, hash and sign readings, keep working without cloud connectivity	[1], [2], [3], [4], [35]
3 Identity, access and privacy	Trusted Authority and CA issuing X.509 certificates; MSP with revocation cache; off-chain ZKP engine; role-based access with set-membership proofs	Register and authenticate entities, check expiry, revocation and timestamps, generate proofs so that sensitive values and identities are never exposed	[1], [2]
4 Blockchain and smart contracts	Permissioned ledger (Fabric peers, EtdcRaft ordering); smart contracts for registration, ZKP verification, emergency handling and payment; trust contracts with SSLA, TSLA and LoT; immutable audit log	Verify proofs on-chain, record only hashes and results, enforce policies automatically, protect trust values from tampering	[1], [2], [3], [22]
5 Application and governance	Port, customs and tax authorities; emergency services and RSU signal control; operator E2E orchestrator; governance bodies and standards	Use verified results for clearance, emergency priority and provider selection; give regulators read-only audit access; define custodianship and standards	[1], [2], [3], [17]
Security and trust management (side block)	Threat model (Sybil, replay, spoofing, collusion); Level of Trust with reward and penalty; key and certificate lifecycle; post-quantum migration plan	Detect attacks, replace untrusted providers, renew keys, prepare quantum-safe algorithms such as CRYSTALS-Dilithium	[1], [2], [3]
Monitoring and feedback (side block)	Dashboards and health monitoring; near-miss and trespass analytics; incident review and labelled data; retraining with safety assessment	Learn from incidents and release updated models or contracts only after independent safety assessment	[3], [4]

3. End-to-End Working of the Proposed Architecture

The following steps show how a request travels through the layers. The same flow can serve a port, a road or a transport-network scenario.

- Step 1, registration: a shipper, vehicle or service provider registers. Vehicles receive an X.509 certificate from the TA and CA [2], and providers register on the ledger with an initial LoT of 100 [3].
- Step 2, sensing: sensors, OBUs or cameras capture data such as location, temperature and seal integrity; the readings are hashed and digitally signed before leaving the edge [1].
- Step 3, edge filtering and proof generation: middleware keeps only relevant events [2], and the off-chain ZKP engine produces a proof, for example that a declared value is above a customs threshold without showing the value [1].
- Step 4, authentication and authorisation: the MSP checks the certificate for expiry and revocation using a cached list, and timestamps block replayed requests [2]; role-based access is proved with a set-membership ZKP so that no identity is revealed [1].
- Step 5, smart-contract execution: the contract verifies the proof and then triggers the action, such as releasing a container, broadcasting a signed emergency alert or accepting a provider offer [1], [2], [3].
- Step 6, ordering and commit: the ordering service (EtdcRaft) groups transactions into blocks, and only hashes and proof results are stored permanently in the ledger [1], [2].
- Step 7, enforcement and trust update: closed loops watch each provider, apply small penalties for SLA violations, a larger penalty after a failed attack mitigation, and replace the provider if needed [3].



- Step 8, audit and feedback: regulators get read-only access to the audit trail [1], and analytics use the logged events to improve detection models, which are released only after independent safety assessment [4].

4. Design Principles

- Privacy by design: prove compliance with ZKPs and keep raw trade data and identities off the ledger [1].
- Light on-chain work: keep proof generation, filtering and monitoring off-chain or at the edge, and store only hashes and results [1], [2], [3].
- Permissioned and lightweight consensus: use a crash-fault-tolerant protocol for time-critical actions, and review Byzantine fault tolerance where malicious insiders are expected [2], [27].
- Hybrid cryptography: choose the proof system according to how often it is used and how long the data must stay secure [1].
- Continuous trust: evaluate every provider and participant during operation and not only at registration [3].
- Standards and safety assurance: follow security and railway safety standards and make updates only after independent assessment [2], [4].

5. Prioritised Research Agenda

The following research directions are suggested in order of priority:

- Field trials and pilots. Test the frameworks at real ports, roads and operator networks, measuring end-to-end results such as clearance time, fraud detection and response time, and not only cryptographic or simulation metrics [1], [2].
- Standard evaluation metrics. Report latency, throughput, failure and false-alarm rates, ledger size and resource use in the same way, so that studies can be compared, as also recommended for safety systems in [4], [34].
- Hybrid and quantum-safe cryptography. Use zk-SNARKs for frequent checks and zk-STARKs for high-security cases as in [1], and study post-quantum signatures such as CRYSTALS-Dilithium as proposed in [2].
- Stronger trust models. Add trust scoring, behaviour-based anomaly detection and decentralised identity to reduce dependence on one authority [2], and test LoT penalty and reward values with realistic data instead of random values [3].
- Lightweight and scalable ledgers. Study Layer-2 solutions, rollups, zero-knowledge rollups, DAG-based ledgers, adaptive batching and lighter consensus methods to reduce on-chain load and delay [1], [2], [3].
- Interoperability and standards. Develop common schemas for trade documents and vehicle messages, and use APIs and middleware to connect legacy systems; alignment with IEEE 1609.2, ETSI ITS and bodies such as UN/CEFACT and WCO is suggested [1], [2].
- Governance, usability and human factors. Define who administers smart contracts, provide simple interfaces so that officers need not understand cryptography [1], and study how people respond to automated warnings [4].
- Trusted data sources. Combine digital signatures from authenticated sensors [1] with weather-resilient sensor fusion and open multi-sensor datasets [4], so that the data written to the ledger is reliable [36], [37].

VII. Conclusion and Future Scope

This review examined four recent studies on blockchain-based security, trust and intelligent safety in transportation, together with related authentication works. The evidence shows that blockchain becomes practical when it is combined with other techniques: ZKPs protect sensitive trade data [1], a permissioned ledger with a lightweight consensus gives fast vehicle authentication [2], and ledger-protected trust values help to choose and replace providers quickly [3]. The railway study [4] adds the lesson that sensor fusion and edge processing are needed for reliable real-time protection.

At the same time, the reported results are mostly from simulations, test beds and single sites. Scalability beyond a few hundred participants, quantum-safe design, collusion and Sybil resistance, legal and governance issues, and the integrity of sensor data are still open. The future scope of this work is to validate the proposed conceptual architecture through a small prototype, to



compare consensus and ZKP choices under the same metrics, and to extend the review with a systematic database search and more studies from other transport domains such as aviation and urban mobility.

References

1. Curado, J., Bhandari, M., Ferreira, J.C., Martins, A.L.: "Blockchain for maritime supply chain: Efficiency and security advancements". *IEEE Access* 13, 201527–201544 (2025). <https://doi.org/10.1109/ACCESS.2025.3636470>
2. Alsaeed, A., Almowuena, S., Alyahya, A.N.: "BAAIoV: A blockchain-based authentication and authorization framework for secure and reliable Internet of Vehicles communication". *IEEE Access* 13, 150821–150837 (2025). <https://doi.org/10.1109/ACCESS.2025.3601003>
3. Alemany, P., et al.: "Securing packet and optical transport connectivity services". *IEEE Open Journal of the Communications Society* 7 (2026).
4. Gorade, P.B., Bangar, A.P., Bhosale, S.B.: "Intelligent railway crossing safety systems using computer vision, sensor fusion, and machine learning: A review". *Int. J. Statistics and Mathematical Research Trends* 1(1) (2025).
5. Xu, Z., Liang, W., Li, K.-C., Xu, J., Jin, H.: "A blockchain-based roadside unit-assisted authentication and key agreement protocol for Internet of Vehicles". *J. Parallel Distrib. Comput.* 149, 29–39 (2021).
6. Qureshi, K.N., Shahzad, L., Abdelmaboud, A., Elfadil Eisa, T.A., Alamri, B., Javed, I.T., Al-Dhaqm, A., Crespi, N.: "A blockchain-based efficient, secure and anonymous conditional privacy-preserving and authentication scheme for the Internet of Vehicles". *Appl. Sci.* 12(1), 476 (2022).
7. Haider, M.H., Fayaz, M., Zhang, Y., Noureen, H., Haider, Z.A., Khan, F.M., Khan, I.U., Rahman, M.M.: "Enhancing authentication security in Internet of Vehicles: A blockchain-driven approach for trust-worthy communication". *ICCK Trans. Adv. Comput. Syst.* 1(1), 48–62 (2024).
8. Singh, A., Rani, P., Ramesh, J.V.N., Athawale, S.V., Alkhayyat, A.H., Aledaily, A.N., Prola, T.A., Sharma, R.: "Blockchain-based lightweight authentication protocol for next-generation trustworthy Internet of Vehicles communication". *IEEE Trans. Consum. Electron.* 70(2), 4898–4907 (2024).
9. Oude Roelink, B., El-Hajj, M., Sarmah, D.: "Systematic review: Comparing zk-SNARK, zk-STARK, and bulletproof protocols for privacy-preserving authentication". *Secur. Privacy* 7(5), 401 (2024).
10. Yang, C.-S.: "Maritime shipping digitalization: Blockchain-based technology applications, future improvements, and intention to use". *Transp. Res. Part E Logist. Transp. Rev.* 131, 108–117 (2019). <https://doi.org/10.1016/j.tre.2019.09.020>
11. Newman, N.: "Can blockchain transform transport?". *Eng. Technol.* 13(6), 58–61 (2018). <https://doi.org/10.1049/et.2018.0605>
12. Liu, J., Zhang, H., Zhen, L.: "Blockchain technology in maritime supply chains: Applications, architecture and challenges". *Int. J. Prod. Res.* 61(11), 3547–3563 (2023). <https://doi.org/10.1080/00207543.2021.1930239>
13. Mukhtar, A., Romli, A., Karimah, N.: "Blockchain network model to improve supply chain visibility based on smart contract". *Int. J. Adv. Comput. Sci. Appl.* 11(10), 1–8 (2020).
14. Zhou, L., Diro, A., Saini, A., Kaisar, S., Hiep, P.C.: "Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities". *J. Inf. Secur. Appl.* 80, 103678 (2024). <https://doi.org/10.1016/j.jisa.2023.103678>
15. Panait, A.-E., Olimid, R.F.: "On using zk-SNARKs and zk-STARKs in blockchain-based identity management". In: *Innovative Security Solutions for Information Technology and Communications*, pp. 130–145. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-69255-1_9
16. Ben-Sasson, E., Bentov, I., Horesh, Y., Riabzev, M.: "Scalable zero knowledge with no trusted setup". In: *Proc. Annu. Int. Cryptol. Conf. (CRYPTO)*, pp. 701–732 (2019). https://doi.org/10.1007/978-3-030-26954-8_23



17. Dasaklis, T.K., Kopanaki, E., Tountalas, P.T., Rachaniotis, N.P., Voutsinas, T.G., Giannakis, K., Chondrokoukis, G.: "Exploring the implementation challenges of the Electronic Freight Transport Information (eFTI) regulation: An empirical perspective from Greece". *Logistics* 8(1), 30 (2024). <https://doi.org/10.3390/logistics8010030>
18. Nguyen, S., Chen, P.S.-L., Du, Y.: "Blockchain adoption in container shipping: An empirical study on barriers, approaches, and recommendations". *Mar. Policy* 155, 105724 (2023). <https://doi.org/10.1016/j.marpol.2023.105724>
19. Ahmad, R.W., Hasan, H., Jayaraman, R., Salah, K., Omar, M.: "Blockchain applications and architectures for port operations and logistics management". *Res. Transp. Bus. Manage.* 41, 100620 (2021). <https://doi.org/10.1016/j.rtbm.2021.100620>
20. Hamidi, S.M.M., Hoseini, S.F., Gholami, H., Kananizadeh-Bahmani, M.: "A three-stage digital maturity model to assess readiness for blockchain implementation in the maritime logistics industry". *J. Ind. Inf. Integr.* 41, 100643 (2024). <https://doi.org/10.1016/j.jii.2024.100643>
21. Aleisa, M.A.: "Blockchain-enabled zero trust architecture for privacy-preserving cybersecurity in IoT environments". *IEEE Access* 13, 18660–18676 (2025). <https://doi.org/10.1109/ACCESS.2025.3529309>
22. Androulaki, E., et al.: "Hyperledger Fabric: A distributed operating system for permissioned blockchains". In: *Proc. 13th EuroSys Conf.*, pp. 1–15 (2018).
23. Zamyatin, A., Al-Bassam, M., Zindros, D., Kokoris-Kogias, E., Moreno-Sanchez, P., Kiayias, A., Knottenbelt, W.J.: "SoK: Communication across distributed ledgers". In: *Financial Cryptography and Data Security, LNCS 12675*, pp. 3–36 (2021).
24. Abbas, S., Talib, M.A., Ahmed, A., Khan, F., Ahmad, S., Kim, D.-H.: "Blockchain-based authentication in Internet of Vehicles: A survey". *Sensors* 21(23), 7927 (2021).
25. Hemmati, A., Zarei, M., Souri, A.: "Blockchain-based Internet of Vehicles (BIOV): A systematic review of surveys and reviews". *Secur. Privacy* 6(6), e317 (2023).
26. Wang, X., Zeng, P., Patterson, N., Jiang, F., Doss, R.: "An improved authentication scheme for Internet of Vehicles based on blockchain technology". *IEEE Access* 7, 45061–45072 (2019).
27. Bagga, P., Sutrala, A.K., Das, A.K., Vijayakumar, P.: "Blockchain-based batch authentication protocol for Internet of Vehicles". *J. Syst. Archit.* 113, 101877 (2021).
28. Eddine, M.S., Ferrag, M.A., Friha, O., Maglaras, L.: "EASBF: An efficient authentication scheme over blockchain for fog computing-enabled Internet of Vehicles". *J. Inf. Secur. Appl.* 59, 102802 (2021).
29. Gupta, M., Kumar, R., Shekhar, S., Sharma, B., Patel, R.B., Jain, S., Dhaou, I.B., Iwendi, C.: "Game theory-based authentication framework to secure Internet of Vehicles with blockchain". *Sensors* 22(14), 5119 (2022).
30. Luo, H., Zhang, J., Li, X., Li, Z., Yu, H., Sun, G., Niyato, D.: "ESIA: An efficient and stable identity authentication for Internet of Vehicles". *IEEE Trans. Veh. Technol.* 73(4), 5602–5615 (2024).
31. Carletti, V., Greco, A., Saggese, A., Vento, B.: "Improving safety through advanced obstacle detection at railway level crossings". *J. Ambient Intell. Humaniz. Comput.* 16(8), 895–904 (2025). <https://doi.org/10.1007/s12652-025-04987-z>