КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1127
UDC 004.056

Illia Kuznietsov
PhD student, Department of Cybersecurity
State University «Kyiv Aviation Institute», Kyiv, Ukraine
ORCID: 0009-0008-0430-5318
5776391@stud.kai.edu.ua

Andrii Mishchenko
Doctor of Technical Sciences, Professor of the Department of Technical Information Security
State University «Kyiv Aviation Institute», Kyiv, Ukraine
ORCID: 0000-0001-8376-1777
andrii.mishchenko@npp.kai.edu.ua

SECURING AVIATION NETWORKS THROUGH BLOCKCHAIN: ARCHITECTURE, CHALLENGES, AND SOLUTIONS

Abstract. The aviation industry depends on data integrity across supply chains spanning OEMs, MRO organizations, airlines, lessors, and national regulators. Centralized data management systems – still dominant in the sector – expose the ecosystem to single points of failure and provide limited traceability of millions of aircraft parts circulating annually. This paper presents a structured review of blockchain-based security architectures for aviation networks, synthesized from 14 peer-reviewed sources published between 2018 and 2025, retrieved from IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, and Wiley/Hindawi. On this basis, a thirteen-step design method is proposed for integrating permissioned blockchain with distributed cloud infrastructure in aviation environments. The method is grounded in quantitative acceptance criteria – throughput ≥ 500 TPS, smart contract execution latency < 200 ms (p95), system availability 99.9% – and maps each design phase to specific security controls (integrity, access control, auditability, privacy, resilience, governance). Core mechanisms are formalized via hash-chain integrity verification, attribute-based access control functions, zero-knowledge proof verification, and a composite pre-ledger trust-scoring model. The principal finding: permissioned blockchain architectures – Hyperledger Fabric in particular – can support aviation requirements for immutable audit trails, decentralized identity management, and regulatory compliance with EASA and FAA; adoption remains constrained by organizational readiness and the unresolved GIGO problem at the ledger boundary.

Keywords: blockchain; distributed ledger technology; permissioned blockchain; aviation; supply chain; traceability; governance; auditability; access control; privacy; resilience; smart contracts.

INTRODUCTION

Aircraft safety depends fundamentally on the trustworthiness of data. Every component installed on a commercial aircraft carries a documentary provenance – from the manufacturer's certificate through successive maintenance events, ownership transfers, and regulatory inspections. When this provenance is accurate, the system functions. When it is not, consequences range from costly removal from service to catastrophic failures. The problem is that today this documentary provenance is held in fragmented, centralized systems: proprietary enterprise resource planning (ERP) platforms, paper logbooks, and siloed databases independently maintained by each participant in the aviation value chain [2, 5].

This fragmentation gives rise to three interrelated problems. First, centralized architectures create single points of failure: a compromised or unavailable database at one MRO organization can halt maintenance processes for an entire fleet. Second, verifying the provenance of frequently traded spare parts is difficult when records are dispersed across incompatible systems. The risk of unapproved or counterfeit components underscores the importance of aircraft-parts traceability, as discussed in the MRO literature [2, 5]. Third, the regulatory environment defined by EASA and FAA requirements mandates full traceability and non-repudiation of maintenance records – requirements that paper logbooks and conventional databases satisfy only at significant manual cost and residual fraud risk [2, 11].

Distributed ledger technology (DLT) – and permissioned blockchain in particular – offers a structurally different approach. Rather than concentrating trust in a single database operator, a permissioned blockchain distributes the ledger among authorized nodes operated by different organizations, while restricting network participation to verified entities. Each transaction is cryptographically linked to its predecessor, producing append-only records that no single participant can unilaterally alter. Smart contracts encode business logic – access policies, compliance checks, automated workflows – directly in the ledger [3, 5, 6].

The potential is evident. The practical reality is more complex. Efthymiou et al. [2] characterise blockchain adoption readiness among MRO organizations as largely exploratory: through semi-structured interviews with industry practitioners, they find that willingness to adopt is restrained by safety-culture inertia and uncertainty about long-term return on investment. Efthymiou et al. [2] and Ye et al. [13] identify organizational, regulatory, and technological adoption barriers: high implementation costs, the absence of standardized regulatory frameworks, and the GIGO problem – blockchain guarantees immutability once a record is entered, but does not itself verify the authenticity of data submitted to the ledger.

This paper makes the following contributions. First, a structured taxonomy of blockchain-based security mechanisms for aviation is provided, organised across seven security dimensions (Section 3). Second, critical gaps in existing research are identified and characterized (Section 4). Third, a thirteen-step design method – with quantitative acceptance criteria, formalized security mechanisms, and measurable outcomes – is proposed for integrating permissioned blockchain into aviation network architectures (Section 6).

Problem Statement.

The multi-party nature of the aviation ecosystem – OEMs, MRO organizations, airlines, lessors, parts brokers, and regulatory authorities – requires a level of mutual trust that current information systems do not adequately provide. Centralized ERP platforms operated by individual organizations cannot deliver cross-organizational transparency. Physical logbooks are susceptible to damage, loss, and deliberate falsification; a single forged traceability document can introduce an unapproved part into a safety-critical structure. Advanced sensor- and RFID-based tracking solutions improve visibility within a single organization but do not extend trust across organizational boundaries [5, 11].

Permissioned blockchain architectures address several of these deficiencies – immutable records, cryptographic non-repudiation, decentralized trust – but their integration into existing aviation IT environments raises questions that the current literature largely leaves unanswered. These are condensed into three research questions.

Research Questions.

RQ1. How can permissioned blockchain architecture satisfy the requirements for data integrity, spare-parts traceability, and secure cross-organizational communication in aviation, and what are the measurable performance thresholds (throughput, latency, availability) such an architecture must meet?

RQ2. Which cryptographic and protocol-level mechanisms – specifically hash-chain verification, attribute-based access control, and zero-knowledge proofs – are required to ensure data authenticity, immutability, and controlled access in a distributed cloud environment compliant with EASA and FAA requirements?

RQ3. What structured design method with quantitative acceptance criteria can guide the integration of permissioned blockchain into existing aviation enterprise systems, accounting for organizational readiness, cost constraints, and interoperability requirements?

RESEARCH METHODOLOGY

Search Strategy.

A structured search of peer-reviewed literature was conducted across five academic databases: IEEE Xplore, ScienceDirect (Elsevier), SpringerLink, ACM Digital Library, and Wiley/Hindawi. The search query combined four conceptual groups using Boolean operators:

("blockchain" OR "distributed ledger technology" OR "DLT") AND ("aviation" OR "aerospace" OR "aircraft" OR "MRO") AND ("security" OR "privacy" OR "trust" OR "integrity") AND ("cloud computing" OR "distributed cloud" OR "federated cloud")

The search was restricted to English-language peer-reviewed publications from January 2018 to December 2025. Journal articles and conference proceedings were included; preprints, editorial pieces, and industry reports were excluded.

Source Selection.

Retrieved publications were assessed against inclusion and exclusion criteria. The final corpus comprised 14 studies that satisfied all criteria.

Inclusion criteria. A work was included if it (a) proposed, evaluated, or reviewed a blockchain-based architecture or mechanism applicable to aviation or aerospace networks; (b) addressed at least one of the seven security dimensions; (c) was published in a peer-reviewed venue; and (d) contained sufficient technical detail to evaluate the proposed mechanisms.

Exclusion criteria. A work was excluded if it (a) addressed blockchain in non-aviation sectors without transferable architectural insights; (b) was purely conceptual with no technical content; (c) duplicated the findings of another included publication by the same authors; or (d) was not available in English.

The corpus of 14 studies encompasses both aviation-specific works and broader blockchain and cybersecurity research with transferable architectural insights (notably identity management and access-control mechanisms for permissioned networks). The inclusion of the latter is justified by the limited volume of aviation-specific literature with the requisite level of technical detail. The transferability of each mechanism to the aviation context was assessed within the analytical framework (Section 2.3).

Analytical Framework.

Each included study was analyzed along three axes: (1) which of the seven security dimensions it addresses; (2) the specificity of the proposed mechanisms (conceptual, architectural, or implemented/evaluated); (3) the maturity of empirical validation (theoretical argument, simulation, prototype, or production deployment). This three-axis classification provided the foundation for both the taxonomy in Section 3 and the gap analysis in Section 4.

TAXONOMY OF BLOCKCHAIN SECURITY MECHANISMS

The fourteen reviewed studies collectively address seven security dimensions relevant to aviation networks. This section synthesises the mechanisms identified in the literature, organised by dimension.

Identity Management.

Decentralized identity (DID) frameworks replace centralized identity providers with self-sovereign credentials anchored to the blockchain. In the aviation context, each participant – whether an OEM, an MRO facility, or an individual maintenance engineer – receives a DID verified in the distributed ledger without requiring a single certificate authority. Ho et al. [5] demonstrate a blockchain system for enhancing aircraft-parts traceability and trackability in inventory management. Extending this approach to MRO technician credential management scenarios – for example, EASA Part-66 licences as verifiable credentials with on-chain revocation – is a logical development consistent with the W3C DID Core architecture [15], although aviation deployment of such an approach requires separate validation. Efthymiou et al. [2] characterise the complexity of manual cross-organizational certificate verification as one of the principal operational obstacles to adoption.

A trusted registry of authorized participants is the foundation of a DID framework. In permissioned blockchains such as Hyperledger Fabric, the Membership Service Provider (MSP) maintains this registry, binding each participant's cryptographic identity to their organizational role and access privileges [6]. This binding is non-trivial in aviation, where a single organization (e.g., an MRO facility) may simultaneously occupy multiple roles – parts supplier, maintenance provider, and regulatory reporting entity – requiring role-composition of credentials that current DID standards (W3C DID Core 1.0) support but few aviation implementations have validated in practice [15].

Access Control.

Access control in a multi-party aviation blockchain must satisfy two competing requirements: regulators and OEMs require broad audit access to maintenance records, while airlines and MRO organizations require that commercially sensitive operational data remain confidential. This tension was identified as the primary adoption barrier in three of the fourteen reviewed studies [2, 5, 12].

Formula 1 formalises the attribute-based access control (ABAC) decision function enforced through smart contracts:

$$AC_{ij} = f(ID_i, R_j, P_{ij}, t, \sigma_{ij}) \quad (1)$$

where $AC_{ij} \in \{0, 1\}$ is the binary access decision for subject i requesting resource j; ID_i is the verified decentralized identity of the subject; R_j is the resource classification level; P_{ij} is the policy set encoded in the smart contract; t is the request timestamp; σ_{ij} is the digital signature of the request.

Attribute-based encryption (ABE) extends this model to the data layer: off-chain data are encrypted under an ABE policy such that only subjects whose attributes satisfy the policy can decrypt them, even if in possession of the ciphertext [4, 8]. Decentralized key management introduces particular complexity: threshold cryptography with $k = \lceil 2n/3 \rceil + 1$ for safety-critical data classes ensures that no single compromised organization can

unilaterally access restricted records – provided the fraction of compromised participants does not exceed the scheme's permissible threshold [6].

Data Integrity.

Data integrity is the foundational property that makes blockchain relevant to aviation. The hash-chain structure guarantees that any modification to a historical record is computationally detectable.

Formula 2 describes hash-chain integrity verification:

$$H(B_n) = SHA-256(H(B_{n-1}) \parallel T_n \parallel D_n \parallel N_n) \quad (2)$$

where $H(B_n)$ is the cryptographic hash of block n; $H(B_{n-1})$ is the hash of the preceding block; T_n is the block timestamp; D_n is the Merkle root of the transactions; N_n is the nonce; ‖ denotes concatenation.

The collision resistance of SHA-256 provides approximately 2^{128} security against collision-finding attacks, making construction of an alternative block with the same hash computationally infeasible for a bounded adversary under current cryptographic assumptions. For aviation data, this means: once a maintenance record, parts certificate, or inspection report is committed to the ledger, any subsequent falsification attempt breaks chain validity from the point of modification, creating a detectable inconsistency [3, 6]. Merkle trees require only $O(\log_2 m)$ hash comparisons to verify the inclusion of any single transaction, enabling efficient integrity audits even as the ledger grows.

Audit Logging and Non-Repudiation.

Every transaction committed to the blockchain constitutes a tamper-resistant, timestamped audit record attributable to a specific identity through digital signatures. This property directly supports the non-repudiation requirement embedded in EASA Part-145 and FAA 14 CFR Part 43: every maintenance action must be traceable to the certifying individual, who cannot subsequently deny having made the certification [2, 5].

The reviewed studies converge on a two-tier logging architecture. On-chain logs capture cryptographic commitments (hashes) and metadata – who, what, when – while detailed data are stored off-chain in distributed cloud storage referenced by on-chain pointers. Architecturally, smart contracts can trigger alerts when transaction patterns deviate from established baselines – for example, an unusually high volume of parts certifications from a single MRO facility within a short time window; analogous anomaly-monitoring approaches are discussed in IoT/blockchain contexts in [8, 14].

Network Governance.

Governance in a multi-party blockchain defines who may join the network, how consensus rules change, how smart contracts are updated, and how disputes between participants are resolved. Sedlmeir et al. [12] highlight the complexity of transparency and governance in organizational blockchain environments; in the reviewed aviation corpus, this dimension remains the least specified — most studies assume a governance structure without detailing its mechanisms. The design method (Section 6, Step 10) addresses this gap by requiring a formal governance document specifying participation rules, smart-contract update procedures with a mandatory k-of-n endorsement threshold (k > n/2), dispute resolution procedures, and alignment with EASA/FAA requirements.

Privacy.

The privacy dimension encompasses two distinct requirements: data confidentiality (preventing unauthorized access to sensitive records) and transaction privacy (preventing network observers from inferring commercially sensitive information from transaction metadata patterns).

Formula 3 describes the zero-knowledge proof (ZKP) verification condition:

$$\exists w: V(x, \pi) = 1 \Leftrightarrow Prove(x, w) \rightarrow \pi \quad (3)$$

where x is the public statement (e.g., "this part has a valid traceability record"); w is the private witness (the full traceability record); π is the proof generated by the prover; $V(x, \pi)$ is the verification function, returning 1 (accepted) or 0 (rejected).

In the aviation context, ZKPs allow a parts broker to prove to an airline that a component has been properly maintained throughout its service life, without revealing the identities of previous operators or the specific maintenance costs – information whose disclosure would confer competitive advantage [5, 9]. For bulk data encryption, a hybrid scheme is applied: data are encrypted with AES-256-GCM (authenticated encryption), and the AES key is encrypted with the recipient's RSA-2048 (conventional key exchange; long-term post-quantum protection requires migration to NIST PQC algorithms, identified as a future research direction), with the encrypted key stored on-chain alongside the data hash [3].

Resilience.

The decentralized architecture of a permissioned blockchain provides inherent resilience against individual node failures. For Hyperledger Fabric v2.5 with the Raft/CFT ordering service, resilience is provided

by replication and majority quorum: the system can survive crash-fault node failures but does not protect against malicious (Byzantine) behaviour by consensus nodes. If the threat model includes malicious insiders at the consensus layer, additional application-level controls or a supported BFT extension are required. Decentralisation represents a material improvement over centralized architectures, where failure of a single database server can halt operations [6].

Disaster recovery in a blockchain-based aviation system exploits inherent data replication: every full node maintains a complete copy of the ledger. Recovery from a local disaster requires only that the participant rejoin the network and synchronise with surviving nodes. Sarkar et al. [11] demonstrate an analogous principle in the context of drone-network security, where decentralized key management enhances resilience in environments with unreliable infrastructure.

UNRESOLVED PROBLEMS AND RESEARCH GAPS

The structured review identifies seven gaps that the existing literature does not adequately address. The gaps are ranked by severity, defined as the product of their impact on adoption feasibility and the degree of consensus in the literature regarding their significance.

High implementation cost. Deploying a permissioned blockchain across even a subset of the aviation supply chain requires infrastructure investment, integration with legacy systems (many MRO organizations still rely on IBM AS/400 / IBM i platforms), staff training, and ongoing network operations. No study in the reviewed corpus provides a validated cost model. Efthymiou et al. [2] characterise cost as the primary adoption barrier – particularly for smaller MRO organizations – but do not quantify it.

Absence of standardized regulatory frameworks. No dedicated EASA or FAA guidance on the admissibility of blockchain-based maintenance records as primary documentation was identified in the reviewed corpus. Ye et al. [13] note that this regulatory vacuum is self-reinforcing: regulators hesitate to issue guidance without production-scale evidence, and operators hesitate to invest without regulatory clarity.

The GIGO problem. Blockchain guarantees that records, once entered, cannot be altered. It does not guarantee that records were accurate at the time of entry. A maintenance engineer certifying an inspection that was never performed, or an IoT sensor reporting false readings, will produce immutable but erroneous records. A quantitative framework for pre-ledger data validation is proposed in Section 5.

Insufficient specificity of architectural proposals. Most reviewed studies present conceptual architectures without specifying consensus parameters, throughput requirements, latency budgets, or integration interfaces with existing aviation IT systems (e.g., ATA iSpec 2200, ATA SPEC 2000, and ATA SPEC 42) [16].

Auditability-privacy tension. Privacy-preserving mechanisms (ZKP, ABE) introduce computational overhead. No reviewed study quantifies this overhead in an aviation-realistic scenario.

The scalability trilemma. Blockchain platforms face the well-known trilemma: decentralisation, security, and throughput cannot be simultaneously maximized. For aviation workloads, the critical question is whether platforms can sustain throughput during peak operations while maintaining sub-second finality.

Key management complexity. Key rotation, revocation, and recovery procedures must operate across organizational boundaries without introducing single points of trust – a requirement that threshold cryptography satisfies theoretically but that has not been validated in aviation-scale deployments [3, 6].

PRE-LEDGER DATA VALIDATION: A RISK-BASED FRAMEWORK

To address the GIGO problem identified in Section 4, a composite risk metric is proposed for assessing data authenticity prior to ledger commitment. The framework assigns a trust score to each data submission on the basis of four factors.

Formula 4 defines the composite pre-ledger data trust score:

$$TS(d) = w_1 \cdot S_{\text{src}}(d) + w_2 \cdot S_{\text{dev}}(d) + w_3 \cdot S_{\text{cross}}(d) + w_4 \cdot S_{\text{hist}}(d) \quad (4)$$

where $TS(d) \in [0, 1]$ is the composite trust score for submission d; $S_{src}(d)$ is the source credibility score, based on the submitting entity's historical accuracy rate and credential validity; $S^{dev}(d)$ is the deviation score, measuring departure from expected values (e.g., an implausibly short part-inspection interval triggers a low score); $S^{c}{}_{r}{}^{o}{}_{ss}(d)$ is the cross-validation score, based on corroboration from independent data sources (IoT sensor readings, third-party reports); $S^{h}{}_{is}{}^{t}(d)$ is the historical consistency score; w_1, w_2, w_3, w_4 are weights satisfying $\Sigma w_k = 1$.

A submission is committed to the ledger if $TS(d) \geq \theta$, where θ is a configurable threshold. For safety-critical data (e.g., airworthiness directives, life-limited parts certificates), $\theta \geq 0.85$ is recommended. Submissions scoring below θ are flagged for manual review by authorized validators.

Weights w_1 through w_4 require empirical calibration. As initial values, $w_1 = 0.30$; $w_2 = 0.25$; $w_3 = 0.25$; $w_4 = 0.20$ are recommended for MRO maintenance-record submissions, reflecting the industry's prioritisation of source credibility in a domain where certified engineers bear personal accountability for their certifications. These values are to be refined using operational data following system deployment.

PROPOSED THIRTEEN-STEP DESIGN METHOD

This section presents the design method for integrating permissioned blockchain into aviation network architectures. Each step specifies inputs, actions, outputs, relevant security controls, and a measurable success criterion. Table 3 consolidates these criteria.

Step 1: Requirements elicitation and stakeholder analysis. The method begins with a structured analysis of the aviation ecosystem's security requirements, regulatory obligations, and stakeholder relationships. Inputs include applicable EASA and FAA regulations (EASA Part-145 for maintenance organization approval, EASA Part-M for continuing airworthiness management, and FAA 14 CFR Part 43), documented operational pain points, and existing data-flow maps. Outputs are a formal requirements specification document and a prioritized security-requirements list mapped to the seven dimensions. Measurable criterion: every security requirement is traced to at least one regulatory provision; the document is signed by representatives of all participating organizations.

Step 2: Top-level system architecture design. This step produces a conceptual architecture integrating distributed cloud storage with a permissioned blockchain layer. The architecture follows a three-tier model (Fig. 2): data tier (distributed cloud storage with AES-256 encryption at rest), consensus tier (permissioned blockchain), and application tier (interfaces for OEMs, MRO organizations, airlines, and regulators). Measurable criterion: a traceability matrix covers all seven security dimensions.

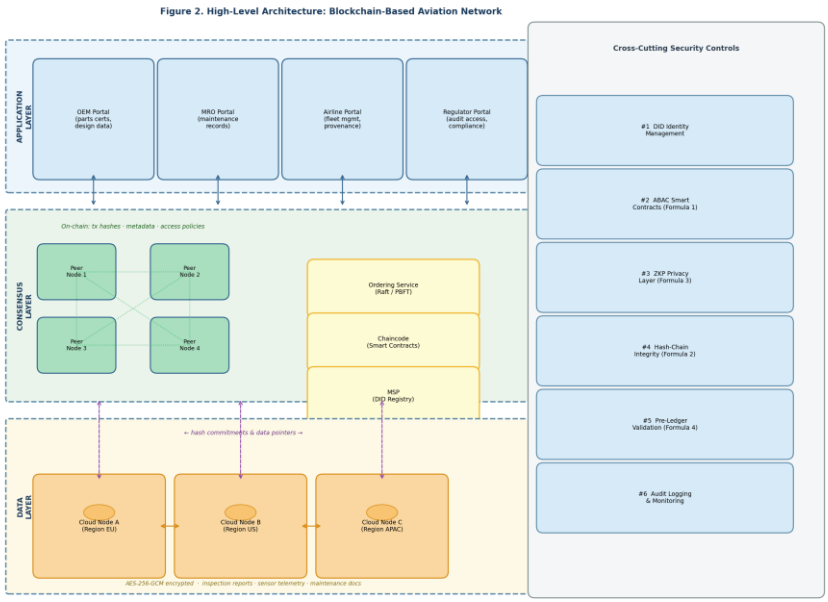

Fig. 2. Three-tier architecture: data tier (AES-256-GCM), consensus tier (Hyperledger Fabric, Raft/CFT), application tier with portals for OEMs, MRO organizations, airlines, and regulators; cross-cutting security controls span all tiers

Step 3: Permissioned blockchain network configuration. Hyperledger Fabric v2.5+ is recommended for aviation MRO applications on the basis of its permissioned architecture, configurable consensus, and channel-based data isolation. Fabric v2.5 uses a Raft/CFT ordering service by default; actual latency is determined by topology, block configuration, and workload. In networks with heightened adversarial requirements, additional application-layer controls or a supported BFT extension should be considered. Measurable criterion: sustained throughput ≥ 500 TPS under a representative workload over a 1-hour test run.

Step 4: Decentralized identity management system. Each participating organization and individual user is assigned a W3C-compliant DID anchored to the blockchain. Verifiable credentials encode role-specific qualifications (EASA Part-66). The credential lifecycle is managed by smart contracts. Measurable criterion: end-to-end credential verification completes within 500 ms.

Step 5: Smart-contract-based access control. Each data resource is classified into one of four levels: public, internal, confidential, and restricted. Smart contracts evaluate access requests against the policy set P_{ij} (Eq. 1), taking into account the requester's DID, role attributes, and temporal constraints. Criterion: 100% of access decisions match the expected outcome on ≥ 500 test cases.

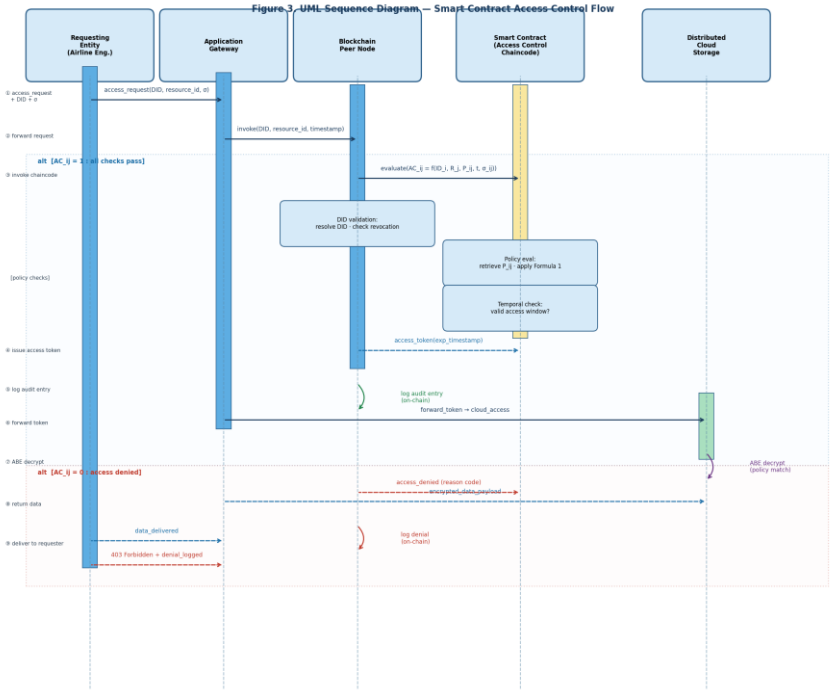

Fig. 3. UML sequence diagram: a DID-authenticated request undergoes three parallel checks (DID validation, ABAC, temporal constraints); upon $AC_{ij}=1$, a token is issued and the event logged; upon $AC_{ij}=0$, a denial is returned with logging, ensuring non-repudiation

Step 6: Data integrity and provenance implementation. Each data asset (certification records, inspection reports, installation events) is processed through a pipeline: serialisation to canonical form, SHA-256 hashing, on-chain hash commitment, AES-256-GCM off-chain storage. A Merkle tree is constructed for the transactions of each block. Measurable criterion: integrity verification of a single record completes in under 100 ms.

Step 7: Pre-ledger data validation. The trust-scoring framework (Eq. 4) is implemented. Submissions with $TS(d) \geq \theta$ are committed automatically; those below the threshold are routed to a manual-review queue. $\theta = 0.85$ for safety-critical data; $\theta = 0.70$ for operational data. Measurable criterion: false-acceptance rate < 1% on an adversarial test set.

Step 8: Data privacy implementation. ZKP modules (zk-SNARK, Groth16: constant proof size of approximately 192 bytes) are deployed for prove-without-reveal scenarios. RSA-2048 or RSA-4096 handles asymmetric key exchange; AES-256-GCM handles authenticated encryption of off-chain data. Measurable criterion: zk-SNARK proof generation for a parts-traceability statement in under 10 seconds.

Step 9: Audit logging and continuous monitoring. Three log streams: on-chain transaction logs (natively tamper-resistant), off-chain access logs (committed to the blockchain as hash digests), and infrastructure logs (node health, network performance). Smart-contract alert rules detect anomalous patterns. Measurable criterion: alert latency ≤ 30 seconds from anomaly occurrence.

Step 10: Network governance framework establishment. The governance document specifies: participation rules (application, verification, admission, suspension, exclusion), smart-contract governance (endorsement threshold $k > n/2$ organizations for updates), dispute-resolution procedures (mediation, arbitration, appeal), and regulatory alignment with EASA/FAA. Measurable criterion: the document addresses applicable ISO/IEC 27001 controls in accordance with a documented Statement of Applicability (SoA).

Step 11: Resilience planning and disaster recovery. The disaster-recovery plan specifies: RTO (Recovery Time Objective) ≤ 4 hours and RPO = 0 (zero data loss – achievable through ledger replication). Failover mechanisms and off-chain data backup procedures are also defined. Measurable criterion: successful disaster-recovery exercise under simulated single-site failure within the target RTO.

Step 12: Testing, validation, and performance optimisation. Four testing categories: functional (smart-contract correctness), security (penetration testing, static analysis of chaincode in the implementation language – e.g., gosec for Go chaincode or native Fabric linters, adversarial data injection), load (sustained throughput ≥ 500 TPS), and scalability. Measurable criteria: smart-contract latency < 200 ms (p95); throughput ≥ 500 TPS (1 h); availability ≥ 99.9%; no known unpatched critical vulnerabilities prior to production deployment.

Step 13: Deployment and continuous improvement. Phased deployment: pilot with 3-5 organizations, followed by expansion over 6-12 months. Continuous improvement driven by operational metrics with quarterly review cycles and annual governance audits. Measurable criterion: 90-day pilot deployment with all performance targets met.

PLATFORM COMPARISON

Table 1 provides a structured comparison of four blockchain platforms evaluated for suitability in aviation network deployment. The comparison criteria are derived from the security dimensions and performance requirements established in Sections 3 and 6.

Table 1

Comparison of blockchain platforms for aviation network deployment

Criterion	Hyperledger Fabric v2.5	Ethereum (PoS)	ConsenSys Quorum	R3 Corda v5
Consensus mechanism	Raft/CFT (Fabric v2.5+)	Gasper (Casper FFG + LMD GHOST)	IBFT 2.0, QBFT	Notary-based (pluggable)
Throughput (TPS)	2,000-20,000 (configuration- and benchmark-dependent) [17, 18]	~15-30 (L1); higher with L2	100-800	500-2,000
Finality latency	Raft: ~50 ms (CFT)	Casper FFG: ~12.8 min (2-epoch checkpoint × 6.4 min)	IBFT: ~2-5 s	~1-3 s
Permission model	Natively permissioned (MSP)	Permissionless by default	Natively permissioned	Natively permissioned
Data privacy	Channels + private data collections	Public / private L2 transactions	Tessera	Point-to-point (need-to-know)
Aviation suitability	High: permissioned by design, channel isolation, high throughput	Low: permissionless, public finality latency incompatible with aviation	Medium: permissioned with privacy, lower maturity	Medium-high: need-to-know model aligns with aviation

SECURITY REQUIREMENTS MAPPING

Table 2 maps six core aviation security requirements to specific blockchain mechanisms, relevant regulatory standards, and the implementation approach prescribed by the design method.

Table 2

Mapping of aviation security requirements to blockchain mechanisms

Security requirement	Aviation problem	Blockchain mechanism	Regulatory standard	Method step
Data integrity	Falsification of certificates and maintenance records; loss of paper logbooks	Hash chain (Eq. 2); Merkle tree; SHA-256	EASA Part-M, M.A.614; FAA 14 CFR 43.12	Step 6
Traceability	Risk of unapproved and counterfeit components in the aviation supply chain; importance of parts traceability discussed in MRO literature [2, 5]	Immutable transaction chain; asset tracking; Merkle proofs	EASA Part-21; FAA Part 21 Subpart K	Steps 6-7
Access control	Regulatory audit vs. commercial confidentiality	ABAC (Eq. 1); ABE; DID verification	EASA Part-145.A.55; FAA Order 8900.1	Steps 4-5

Continuation of the table 2

Auditability	Non-repudiation of maintenance certification; regulatory inspection	Tamper-resistant on-chain logs; digital signatures; DID attribution	EASA Part-145.A.50; FAA AC 43-9C	Steps 8-9
Privacy	Protection of operational data (fleet ratios, costs)	ZKP (Eq. 3); ABE; AES-256-GCM	GDPR Art. 25; EASA data protection provisions	Step 8
Resilience	Single points of failure; operational continuity under disruptions	Raft/CFT replication; node redundancy; RTO ≤ 4 h	EASA Part-145.A.65; FAA SMS Order 8000.369B	Steps 3, 11

DESIGN METHOD EVALUATION FRAMEWORK

Table 3 consolidates the measurable success criteria for each step of the design method, transforming the method from a procedural description into a verifiable engineering specification.

Table 3

Design method steps with measurable success criteria

Step	Name	Security control	Key output	Success criterion
1	Requirements elicitation	All (scope definition)	Requirements specification	100% traceability; stakeholder sign-off
2	Architecture design	Resilience, Governance	Conceptual architecture	Coverage of all 7 security dimensions
3	Network configuration	Access control, Resilience	Operational network	≥ 500 TPS; latency ≤ 50 ms (Raft/CFT)
4	Identity management	Identity, Privacy	DID system	Credential verification ≤ 500 ms
5	Access control	ABAC, Integrity	Smart contracts + ABE	100% correctness on ≥ 500 tests
6	Data integrity	Integrity, Logging	Hash chain + Merkle tree	Record verification ≤ 100 ms
7	Pre-ledger validation	Integrity, Governance	TS(d) pipeline	False-acceptance rate < 1%
8	Privacy	Privacy	ZKP + AES-256-GCM/RSA	Proof generation ≤ 10 s
9	Audit and monitoring	Audit logging	Monitoring system	Alert latency ≤ 30 s
10	Network governance	Governance, Access	Policy document	Applicable ISO/IEC 27001 controls mapped in SoA
11	Resilience and DR	Resilience, Integrity	DR plan	RTO ≤ 4 h; RPO = 0
12	Testing	All (verification)	Test reports	< 200 ms (p95); ≥ 500 TPS; ≥ 99.9%; no known unpatched critical vulnerabilities
13	Deployment	All, Response	Production system	90-day pilot with all performance targets met

RESULTS AND DISCUSSION

Literature Convergence.

The structured review reveals clear consensus on six properties that permissioned blockchain provides for aviation networks. Record immutability is the most consistently cited benefit, appearing in 12 of the 14 reviewed studies: the hash-chain structure (Formula 2) guarantees that records once committed cannot be altered without detection. Auditability and non-repudiation follow closely (11/14 studies), supported by inherent tamper-resistant logging and digital signature attribution. Decentralized identity management and access control are addressed in 9 of 14 studies. Parts traceability – the specific aviation use case – is the focus of 7 studies, with Ho et al. [5] and Efthymiou et al. [2] providing the most detailed treatment. Resilience against node failures (8/14) and network governance (6/14) complete the picture, though the latter remains underspecified.

Resolution of Identified Gaps.

The design method addresses each of the seven gaps identified in Section 4 through specific, measurable mechanisms.

The implementation cost barrier is addressed through the phased deployment strategy (Step 13), which limits initial investment to a pilot consortium of 3-5 organizations. The 90-day pilot produces operational cost data that subsequent participants can use to construct business cases.

The regulatory framework gap is mitigated through the governance framework (Step 10), which explicitly includes provisions for regulatory authority participation and audit access. The method positions blockchain as a supplementary assurance layer that complements rather than replaces existing record-keeping obligations.

The GIGO problem receives the most original treatment through the pre-ledger data trust-scoring framework (Formula 4, Step 7). A formalized quantitative approach to pre-ledger data validation in an aviation blockchain context was not encountered in the reviewed corpus. The framework materially raises the bar compared with systems that unconditionally commit all submitted data.

The architectural specificity gap is directly addressed by the platform comparison (Table 1), the security requirements mapping (Table 2), and the quantitative success criteria (Table 3). The auditability–privacy tension is resolved through the combination of ZKP, ABE, and the Hyperledger Fabric channel mechanism. The scalability trilemma is addressed through Fabric's channel architecture (horizontal scaling). Key management complexity is handled through the threshold cryptography approach (Step 5) and organizational procedures in the governance framework (Step 10).

Limitations.

Three limitations of this work must be acknowledged. First, the design method has not been validated through a production deployment. The quantitative criteria in Table 3 are derived from published platform benchmarks and engineering judgement, not from empirical measurements in an operational aviation environment. A pilot implementation is required to validate these targets.

Second, the structured review is constrained by the search strategy. Studies published in languages other than English, in non-included venues, or as industry documents were excluded. Given that significant blockchain development occurs in industry, this exclusion may have missed relevant practical experience.

Third, the pre-ledger data trust-scoring framework (Formula 4) requires empirical calibration of the weights (w_1 through w_4) and threshold (θ). The values proposed in Section 5 are initial recommendations based on domain analysis; they have not been validated against real MRO operational data.

CONCLUSIONS

This paper presents three contributions to the field of blockchain-based aviation network security.

Contribution 1: A structured taxonomy of blockchain security mechanisms for aviation (Section 3, Table 2). The taxonomy organises mechanisms from 14 peer-reviewed sources across seven security dimensions and maps each to specific aviation regulatory requirements (EASA Part-M, Part-145, Part-21; FAA 14 CFR Parts 21 and 43). Unlike prior reviews, the taxonomy identifies the mathematical foundations – hash-chain verification (Formula 2), attribute-based access control (Formula 1), and zero-knowledge proof verification (Formula 3).

Contribution 2: A trust-scoring framework TS(d) for mitigating the GIGO problem (Section 5, Formula 4). The composite trust score provides a quantitative, configurable mechanism for assessing data authenticity prior to blockchain commitment. For safety-critical aviation data, a threshold $\theta \geq 0.85$ is specified with initial weights $w_1 = 0.30$; $w_2 = 0.25$; $w_3 = 0.25$; $w_4 = 0.20$. The target acceptance criterion is a false-acceptance rate < 1% on adversarial test data (Table 3, Step 7).

Contribution 3: A thirteen-step design method with quantitative acceptance criteria (Section 6, Table 3). The method transforms blockchain integration from an abstract recommendation into a verifiable engineering specification. Each step specifies measurable criteria: ≥ 500 TPS (Step 3), smart-contract latency < 200 ms p95 (Step 12), availability ≥ 99.9% (Step 12), credential verification ≤ 500 ms (Step 4), integrity verification ≤ 100 ms (Step 6). Hyperledger Fabric v2.5+ is selected as the reference platform on the basis of the criteria in Table 1 – principally its permissioned membership model, channel isolation, and documented throughput.

The conclusions presented are subject to the limitations noted in Section 10.3. The quantitative targets of the method are derived from published benchmarks, not from empirical aviation deployment data. Validation through a pilot implementation with a consortium of 3–5 aviation organizations is the necessary next step.

Future Research Directions.

Five research directions are identified: (1) pilot implementation of the method with an MRO consortium of 3-5 organizations for empirical validation of Table 3 and calibration of the Formula 4 weights; (2) adaptive governance models through upgradeable smart contracts for dynamic network rule adjustment; (3) zk-STARK and recursive proof composition to reduce computational overhead; (4) post-quantum cryptography

(CRYSTALS-Kyber for key encapsulation, CRYSTALS-Dilithium for digital signatures, standardized by NIST in 2024) for long-term architectural resilience; (5) integration with digital-twin platforms and AI-based predictive maintenance analytics.

REFERENCES

1. Alkhateeb, A., Catal, C., Kar, G., & Mishra, A. (2022). Hybrid blockchain platforms for the Internet of Things (IoT): A systematic literature review. *Sensors, 22*(4), 1304. https://doi.org/10.3390/s22041304
2. Efthymiou, M., McCarthy, K., Markou, C., & O'Connell, J. F. (2022). An exploratory research on blockchain in aviation: The case of maintenance, repair and overhaul (MRO) organizations. *Sustainability, 14*(5), 2643. https://doi.org/10.3390/su14052643
3. Gousteris, S., Stamatiou, Y. C., Halkiopoulos, C., Antonopoulou, H., & Kostopoulos, N. (2023). Secure distributed cloud storage based on blockchain technology and smart contracts. *Emerging Science Journal, 7*(2), 469-485. https://doi.org/10.28991/ESJ-2023-07-02-012
4. Honar Pajooh, H., Rashid, M., Alam, F., & Demidenko, S. (2021). Multi-layer blockchain-based security architecture for the Internet of Things. *Sensors, 21*(3), 772. https://doi.org/10.3390/s21030772
5. Ho, G. T. S., Tang, Y. M., Tsang, K. Y., Tang, V., & Chau, K. Y. (2021). A blockchain-based system to enhance aircraft parts traceability and trackability for inventory management. *Expert Systems with Applications, 179*, 115101. https://doi.org/10.1016/j.eswa.2021.115101
6. Latif, S., Idrees, Z., Huma, Z., & Ahmad, J. (2021). Blockchain architecture for industrial IoT. *Journal of Industrial Information Integration, 21*, 100190.
7. Javed, A. R., Hassan, M. A., Shahzad, F., Ahmed, W., Singh, S., Baker, T., & Gadekallu, T. R. (2022). Integration of blockchain technology and federated learning in vehicular IoT networks: A comprehensive survey. *Sensors, 22*(12), 4394. https://doi.org/10.3390/s22124394
8. Popoola, O., Rodrigues, M., Marchang, J., Shenfield, A., Ikpehai, A., & Popoola, J. (2024). A critical literature review of security and privacy in smart home healthcare schemes adopting IoT and blockchain: Problems, challenges and solutions. *Blockchain: Research and Applications, 5*(2), 100178. https://doi.org/10.1016/j.bcra.2023.100178
9. Qammar, A., Karim, A., Ning, H., & Ding, J. (2023). Securing federated learning with blockchain: A systematic review. *Artificial Intelligence Review, 56*, 3951-3985.
10. Raja Santhi, A., & Muthuswamy, P. (2022). Influence of blockchain technology in manufacturing supply chain and logistics. *Logistics, 6*(1), 15. https://doi.org/10.3390/logistics6010015
11. Sarkar, S., Shafaei, S., Jones, T. S., & Totaro, M. W. (2025). Secure communication in drone networks: A comprehensive survey of lightweight encryption and key management techniques. *Drones, 9*(8), 583. https://doi.org/10.3390/drones9080583
12. Sedlmeir, J., Buhl, H. U., Fridgen, G., & Keller, R. (2022). The transparency challenge of blockchain in organizations. *Electronic Markets, 32*, 1779-1794.
13. Ye, Y., Min, X., Liu, X., Chen, X., Cao, K., Howlader, S. M. R. K., & Chen, X. (2025). Secure and intelligent low-altitude infrastructures: Synergistic integration of IoT networks, AI decision-making and blockchain trust mechanisms. *Sensors, 25*(21), 6751. https://doi.org/10.3390/s25216751
14. Zubaydi, H. D., Varga, P., & Molnár, S. (2023). Leveraging blockchain technology for ensuring security and privacy aspects in the Internet of Things: A systematic literature review. *Sensors, 23*(2), 788. https://doi.org/10.3390/s23020788
15. Sporny, M., Guy, A., Sabadello, M., & Reed, D. (Eds.). (2022). *Decentralized identifiers (DIDs) v1.0: Core architecture, data model, and representations*. W3C. https://www.w3.org/TR/did-core/
16. Air Transport Association of America. (2023). *iSpec 2200: Information standards for aviation maintenance; SPEC 2000: e-business specification for materiel management; SPEC 42: Administration of aviation parts and products*. ATA.
17. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., et al. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. In *Proceedings of the Thirteenth EuroSys Conference* (Article 30). ACM. https://doi.org/10.1145/3190508.3190538
18. Nasir, Q., Qasse, I. A., Abu Talib, M., & Bou Nassif, A. (2018). Performance analysis of Hyperledger Fabric platforms. *Security and Communication Networks, 2018*, Article 3976093. https://doi.org/10.1155/2018/3976093

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

Кузнецов Ілля Сергійович
аспірант кафедри кібербезпеки
Державний університет «Київський авіаційний інститут», Київ, Україна
ORCID: 0009-0008-0430-5318
5776391@stud.kai.edu.ua

Міщенко Андрій Віталійович
доктор технічних наук, професор кафедри технічного захисту інформації
Державний університет «Київський авіаційний інститут», Київ, Україна
ORCID: 0000-0001-8376-1777
andrii.mishchenko@npp.kai.edu.ua

ЗАХИСТ АВІАЦІЙНИХ МЕРЕЖ ЗА ДОПОМОГОЮ БЛОКЧЕЙНУ: АРХІТЕКТУРА, ПРОБЛЕМИ ТА РІШЕННЯ

Анотація. Авіаційна галузь залежить від цілісності даних у всіх ланцюгах поставок, що охоплюють виробників оригінального обладнання (OEM), організації технічного обслуговування та ремонту (MRO), авіакомпанії, лізингодавців та національні регуляторні органи. Централізовані системи управління даними, які досі домінують у цьому секторі, наражають екосистему на єдині точки відмови та забезпечують обмежену відстежуваність мільйонів деталей літаків, що обертаються щорічно. У цій статті представлено структурований огляд архітектур безпеки на основі блокчейну для авіаційних мереж, синтезований з 14 рецензованих джерел, опублікованих між 2018 і 2025 роками, отриманих з IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library та Wiley/Hindawi. На цій основі пропонується тринадцятиетапний метод проектування для інтеграції блокчейну з дозволом з розподіленою хмарною інфраструктурою в авіаційних середовищах. Метод ґрунтується на кількісних критеріях прийнятності – пропускна здатність ≥ 500 TPS, затримка виконання смарт-контрактів < 200 мс (p95), доступність системи 99,9% – і зіставляє кожен етап проектування з певними засобами контролю безпеки (цілісність, контроль доступу, аудит, конфіденційність, стійкість, управління). Основні механізми формалізовані за допомогою перевірки цілісності хеш-ланцюга, функцій контролю доступу на основі атрибутів, перевірки доказів з нульовим розголошенням та складеної моделі оцінки довіри перед реєстром. Основний висновок: архітектури блокчейну з дозволом, зокрема Hyperledger Fabric, можуть підтримувати вимоги авіації щодо незмінних журналів аудиту, децентралізованого управління ідентифікацією та відповідності нормативним вимогам EASA та FAA; впровадження залишається обмеженим організаційною готовністю та невирішеною проблемою GIGO на межі реєстру.

Ключові слова: блокчейн; технологія розподіленого реєстру; блокчейн з дозволом; авіація; ланцюг поставок; відстежуваність; управління; можливість аудиту; контроль доступу; конфіденційність; стійкість; смарт-контракти.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Alkhateeb, A., Catal, C., Kar, G., & Mishra, A. (2022). Hybrid blockchain platforms for the Internet of Things (IoT): A systematic literature review. *Sensors, 22*(4), 1304. https://doi.org/10.3390/s22041304
2. Efthymiou, M., McCarthy, K., Markou, C., & O'Connell, J. F. (2022). An exploratory research on blockchain in aviation: The case of maintenance, repair and overhaul (MRO) organizations. *Sustainability, 14*(5), 2643. https://doi.org/10.3390/su14052643
3. Gousteris, S., Stamatiou, Y. C., Halkiopoulos, C., Antonopoulou, H., & Kostopoulos, N. (2023). Secure distributed cloud storage based on blockchain technology and smart contracts. *Emerging Science Journal, 7*(2), 469-485. https://doi.org/10.28991/ESJ-2023-07-02-012
4. Honar Pajooh, H., Rashid, M., Alam, F., & Demidenko, S. (2021). Multi-layer blockchain-based security architecture for the Internet of Things. *Sensors, 21*(3), 772. https://doi.org/10.3390/s21030772
5. Ho, G. T. S., Tang, Y. M., Tsang, K. Y., Tang, V., & Chau, K. Y. (2021). A blockchain-based system to enhance aircraft parts traceability and trackability for inventory management. *Expert Systems with Applications, 179*, 115101. https://doi.org/10.1016/j.eswa.2021.115101

6. Latif, S., Idrees, Z., Huma, Z., & Ahmad, J. (2021). Blockchain architecture for industrial IoT. *Journal of Industrial Information Integration, 21*, 100190.
7. Javed, A. R., Hassan, M. A., Shahzad, F., Ahmed, W., Singh, S., Baker, T., & Gadekallu, T. R. (2022). Integration of blockchain technology and federated learning in vehicular IoT networks: A comprehensive survey. *Sensors, 22*(12), 4394. https://doi.org/10.3390/s22124394
8. Popoola, O., Rodrigues, M., Marchang, J., Shenfield, A., Ikpehai, A., & Popoola, J. (2024). A critical literature review of security and privacy in smart home healthcare schemes adopting IoT and blockchain: Problems, challenges and solutions. *Blockchain: Research and Applications, 5*(2), 100178. https://doi.org/10.1016/j.bcra.2023.100178
9. Qammar, A., Karim, A., Ning, H., & Ding, J. (2023). Securing federated learning with blockchain: A systematic review. *Artificial Intelligence Review, 56*, 3951-3985.
10. Raja Santhi, A., & Muthuswamy, P. (2022). Influence of blockchain technology in manufacturing supply chain and logistics. *Logistics, 6*(1), 15. https://doi.org/10.3390/logistics6010015
11. Sarkar, S., Shafaei, S., Jones, T. S., & Totaro, M. W. (2025). Secure communication in drone networks: A comprehensive survey of lightweight encryption and key management techniques. *Drones, 9*(8), 583. https://doi.org/10.3390/drones9080583
12. Sedlmeir, J., Buhl, H. U., Fridgen, G., & Keller, R. (2022). The transparency challenge of blockchain in organizations. *Electronic Markets, 32*, 1779-1794.
13. Ye, Y., Min, X., Liu, X., Chen, X., Cao, K., Howlader, S. M. R. K., & Chen, X. (2025). Secure and intelligent low-altitude infrastructures: Synergistic integration of IoT networks, AI decision-making and blockchain trust mechanisms. *Sensors, 25*(21), 6751. https://doi.org/10.3390/s25216751
14. Zubaydi, H. D., Varga, P., & Molnár, S. (2023). Leveraging blockchain technology for ensuring security and privacy aspects in the Internet of Things: A systematic literature review. *Sensors, 23*(2), 788. https://doi.org/10.3390/s23020788
15. Sporny, M., Guy, A., Sabadello, M., & Reed, D. (Eds.). (2022). *Decentralized identifiers (DIDs) v1.0: Core architecture, data model, and representations*. W3C. https://www.w3.org/TR/did-core/
16. Air Transport Association of America. (2023). *iSpec 2200: Information standards for aviation maintenance; SPEC 2000: e-business specification for materiel management; SPEC 42: Administration of aviation parts and products*. ATA.
17. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., et al. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. In *Proceedings of the Thirteenth EuroSys Conference* (Article 30). ACM. https://doi.org/10.1145/3190508.3190538
18. Nasir, Q., Qasse, I. A., Abu Talib, M., & Bou Nassif, A. (2018). Performance analysis of Hyperledger Fabric platforms. *Security and Communication Networks, 2018*, Article 3976093. https://doi.org/10.1155/2018/3976093

Отримано редакцією журналу / Received: 24.02.26
Прорецензовано / Revised: 02.03.26
Схвалено до друку / Accepted: 25.06.26