HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

DISTRIBUTED LEDGER AND BLOCKCHAIN FRAMEWORKS FOR ENSURING OPERATIONAL-TACTICAL INFORMATION INTEGRITY IN AIR DEFENSE SYSTEMS

Valiyev Oybek Gofurovich
Head of Cycle
Military Institute of Information and Communication Technologies and Communications
Email: valievoybek2@gmail.com
doi:https://doi.org/10.5281/zenodo.23170024

Abstract. This article examines the potential and limitations of distributed ledger and blockchain frameworks for ensuring the integrity, provenance, accountability, and controlled sharing of operational-tactical information in air defense information environments. The study is conducted at the strategic, information-assurance, and systems-engineering level and does not address tactical procedures, targeting logic, vulnerabilities, or methods for defeating air defense systems. A structured qualitative review was performed using official standards and policy documents, peer-reviewed defense and aerospace studies, and relevant publications and legal acts from the Republic of Uzbekistan. The evidence shows that permissioned distributed ledgers can provide tamper-evident audit trails, cryptographic provenance, replicated records, and rule-based authorization across organizational boundaries. The article concludes that the most credible role for distributed ledgers in air defense is as a selective assurance layer for metadata, hashes, provenance, authorization events, configuration records, and audit evidence rather than as a universal repository for high-rate sensor streams.

Keywords: distributed ledger technology; blockchain; air defense; operational-tactical information; information integrity; data provenance; command and control; permissioned ledger; cyber resilience; interoperability; Uzbekistan.

Annotatsiya. Ushbu maqolada havo mudofaasi axborot muhitida operatsion-taktik ma'lumotlarning yaxlitligi, kelib chiqishi, hisobdorligi va nazorat ostida almashinuvini ta'minlash uchun taqsimlangan reyestr va blokcheyn tizimlarining potentsiali va cheklovlari ko'rib chiqiladi. Tadqiqot strategik, axborotni ta'minlash va tizim muhandisligi darajasida olib boriladi va taktik protseduralar, mantiqni nishonga olish, zaifliklar yoki havo mudofaasi tizimlarini mag'lub etish usullarini ko'rib chiqmaydi. Rasmiy standartlar va siyosat hujjatlari, ekspertlar tomonidan ko'rib chiqilgan mudofaa va aerokosmik tadqiqotlar hamda O'zbekiston Respublikasining tegishli nashrlari va huquqiy hujjatlari yordamida tuzilgan sifatli tahlil o'tkazildi. Dalillar shuni ko'rsatadiki, ruxsat etilgan taqsimlangan reyestrlar buzib ko'rsatiladigan audit izlari, kriptografik kelib chiqishi, takrorlangan yozuvlar va tashkilot chegaralari bo'ylab qoidalarga asoslangan avtorizatsiyani taqdim etishi mumkin. Maqolada taqsimlangan reyestrlar uchun havo mudofaasida eng ishonchli rol yuqori

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

tezlikdagi sensor oqimlari uchun universal ombor sifatida emas, balki metama'lumotlar, xeshlar, kelib chiqishi, avtorizatsiya hodisalari, konfiguratsiya yozuvlari va audit dalillari uchun tanlab kafolat qatlami sifatida ekanligi haqida xulosa qilinadi.

Kalit so'zlar: taqsimlangan reyestr texnologiyasi; blokcheyn; havo mudofaasi; operatsion-taktik ma'lumotlar; axborot yaxlitligi; ma'lumotlar kelib chiqishi; qo'mondonlik va boshqarish; ruxsat etilgan reyestr; kiberbardoshlilik; o'zaro moslashuvchanlik; O'zbekiston.

Аннотация. В статье рассматриваются возможности и ограничения технологий распределенного реестра и блокчейна применительно к обеспечению целостности, подтверждению происхождения, подотчетности и контролируемому обмену оперативно-тактической информацией в информационных средах систем противовоздушной обороны (ПВО). Исследование проводится на стратегическом, системно-техническом уровнях и уровне обеспечения информационной безопасности; при этом не затрагиваются вопросы тактических процедур, логики целеуказания, уязвимостей или методов нейтрализации систем ПВО. Был проведен структурированный качественный анализ с использованием официальных стандартов и нормативных документов, рецензируемых исследований в области обороны и аэрокосмической отрасли, а также соответствующих публикаций и правовых актов Республики Узбекистан. Результаты анализа свидетельствуют о том, что распределенные реестры с ограниченным доступом (permissioned ledgers) способны обеспечить формирование защищенных от несанкционированных изменений журналов аудита, криптографическое подтверждение происхождения данных, репликацию записей и авторизацию на основе заданных правил при взаимодействии различных организаций. В статье делается вывод, что наиболее целесообразная роль распределенных реестров в системах ПВО заключается в их использовании в качестве уровня выборочного подтверждения достоверности метаданных, хеш-сумм, сведений о происхождении данных, событий авторизации, записей о конфигурации и доказательств аудита, а не в качестве универсального хранилища для высокоинтенсивных потоков данных от средств обнаружения.

Ключевые слова: технология распределенного реестра; блокчейн; противовоздушная оборона; оперативно-тактическая информация; целостность информации; происхождение данных; командование и управление; реестр с ограниченным доступом; киберустойчивость; интероперабельность; Узбекистан.

INTRODUCTION

Modern air defense increasingly depends on digital information flows linking sensors, command-and-control applications, communications services, logistics, maintenance, and decision-support functions. The operational value of such an environment depends not only on the speed of data exchange but also on whether authorized users and systems can determine that information has not

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

been altered, that its origin can be verified, and that changes are attributable. NATO's 2025 Data Strategy explicitly treats data as a strategic asset and defines trusted data as data whose integrity, associated systems, and processes can be assessed; the strategy also emphasizes secure, interoperable, governed data throughout its life cycle [1]. The 2025 NATO Data Quality Framework adds measurable dimensions such as accuracy, completeness, consistency, timeliness, validity, uniqueness, and granularity, together with lineage and metadata management [2].

These requirements are especially important in safety- and mission-critical information systems. Integrity in this context is broader than preventing unauthorized modification. It includes provenance, version history, authorization, traceability, accountability, and the ability to detect inconsistencies between replicated or federated information services. Distributed ledger technology has therefore attracted attention because it combines cryptographic hashing, digital signatures, replicated records, and consensus mechanisms to produce a shared ledger whose unauthorized alteration is intended to be evident. NIST describes blockchains as distributed, tamper-evident and tamper-resistant digital ledgers and stresses that blockchain is only one component of a wider solution [3].

The defense literature has explored blockchain for logistics, supply chains, identity, unmanned systems, communications, and command-and-control data exchange. However, the suitability of a distributed ledger for air defense cannot be inferred from commercial blockchain applications. Air defense information environments are time-sensitive, heterogeneous, access-controlled, and frequently bandwidth-constrained. They require deterministic governance and must continue operating under degraded communications. Consequently, the key research question is not whether blockchain is 'secure', but where a ledger can add verifiable integrity without imposing unacceptable latency, data-volume, availability, or interoperability costs.

The purpose of this article is to assess distributed ledger and blockchain frameworks as an information-integrity layer for air defense systems. The objectives are to: (i) identify the integrity properties that distributed ledgers can realistically provide; (ii) compare these properties with data-centric defense requirements; (iii) analyze evidence from international and Uzbek research; (iv) examine quantitative and architectural limitations; and (v) propose a cautious framework for research and evaluation. The analysis remains non-operational: it does not describe vulnerabilities, tactical employment, engagement processes, or methods of interfering with air defense systems.

LITERATURE REVIEW

Foundational literature defines blockchain through a combination of cryptographic hashes, asymmetric cryptography, replicated ledgers, validation rules, and consensus. NIST IR 8202 distinguishes permissionless and permissioned approaches and warns that blockchain is not a universal solution; malicious participants, governance, access control, implementation limitations, and operational management remain important [3]. This caution is directly relevant to defense applications. A permissionless public network is generally inconsistent with classified or mission-sensitive

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

information because membership, visibility, governance, and data residency must be tightly controlled. Research therefore tends to favor permissioned architectures for military or government settings.

A systematic review of blockchain applications in the military domain found recurring use cases in secure communications, logistics, identity, unmanned systems, data sharing, and command functions, but also identified interoperability, integration-point security, scalability, privacy, and latency as major barriers [4]. A broader aerospace-and-defense review similarly highlighted battlefield management, border protection, logistics and distributed coordination while identifying latency, large data traffic, smart-contract security, regulation, privacy and interoperability as open research challenges [5]. These findings suggest that the value proposition is strongest where multiple authorized organizations require a common, auditable record but do not wish to rely exclusively on a single database authority.

Recent empirical work provides useful quantitative evidence. Pengkian, Praneetpolgrang and Sirinam designed a blockchain-based digital storage and exchange platform for an Air Force command-and-control environment and tested smart-contract-based transmission of different data sizes. Processing time increased with data volume; the largest tested item, 20 MB, required an average of 1.175 seconds [6]. This is important because integrity assurance is not cost-free. In an operational-tactical environment, a one-second-scale delay may be acceptable for audit records, configuration changes or administrative exchanges but inappropriate for some time-critical data paths. The result supports architectural separation between real-time data transport and ledger-based assurance.

Defense supply-chain research also demonstrates the value of federated trust. A 2021 project for the U.S. Department of Defense and NAVAIR connected separate enterprise blockchain systems while preserving privacy and transaction transparency across military and supplier networks [7]. Although supply-chain requirements differ from air-defense information flows, the study is relevant because it shows that distributed ledgers may be more useful for provenance and cross-organizational accountability than for bulk real-time data carriage.

NATO's digital transformation provides a parallel policy framework even though NATO documents do not prescribe blockchain as the solution. The 2024 Digital Transformation Implementation Strategy calls for secure access to trusted data, a data-centric architecture, harmonized data-sharing standards and resilient data flow [8]. The 2025 Data Strategy requires data to be discoverable, accessible, trusted, regulated, interoperable, curated, shared and secure [1]. The 2026 Alliance Digital Strategy further calls for federated data spaces, persistent access to mission-relevant data and preservation of sovereignty, autonomy and accountability [9]. Distributed ledgers should therefore be evaluated against these requirements rather than adopted for technological novelty.

Uzbekistan has developed a legal and academic basis for distributed-ledger research. Presidential Resolution No. PP-3832 of 3 July 2018, as subsequently amended, recognizes distributed ledger technology as a direction of digital development, calls for an appropriate legal framework and qualified personnel, and provides that specific areas of distributed-ledger implementation may be

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

determined by the competent national agency on proposals from ministries and agencies [10]. Uzbek researchers have also examined blockchain for information and communication technologies, cybersecurity and Internet-of-Things security. Zaripova describes blockchain as a distributed database model supporting trust and transaction-history control [11]. Khudoyqulov and Saidullaev analyze blockchain as a potential mechanism for improving security in Internet-of-Things environments [12]. Recent Uzbek cybersecurity literature emphasizes integrity, authentication, availability and decentralized trust, while also acknowledging privacy and implementation challenges [13].

These Uzbek studies are mostly civilian or general-purpose rather than air-defense-specific. Their significance lies in demonstrating domestic academic competence in cryptography, distributed systems, Internet-of-Things security and blockchain concepts. A responsible defense research agenda should build on these competencies while subjecting any proposed use to stricter requirements for classification, sovereignty, deterministic governance, resilience, certification and interoperability.

METHODOLOGY

The study used a structured qualitative evidence-synthesis method. Sources were included when they met at least one of four criteria: (1) authoritative technical standards or guidance on blockchain and data integrity; (2) official defense or alliance policy on data governance, digital transformation and interoperability; (3) peer-reviewed or professionally reviewed research on blockchain in military, aerospace, command-and-control or security contexts; or (4) Uzbek legal and scientific publications relevant to distributed ledgers, cybersecurity and information integrity. Priority was given to primary institutional sources, identifiable experimental studies and publications with explicit methods.

Evidence was coded into six analytical dimensions: integrity and provenance; identity and authorization; availability and resilience; latency and scalability; interoperability and integration; and governance and sovereignty. Quantitative observations were retained only when they were traceable to a specific study. The 1.175-second processing result for a 20 MB data item, for example, is treated as a finding of one 2026 experimental platform rather than a universal blockchain performance figure [6].

A systems-engineering suitability test was then applied. A blockchain function was considered potentially suitable when multiple authorized entities require a shared and independently verifiable history, later alteration must be detectable, and transaction rates are compatible with the consensus and replication overhead. Conversely, a ledger was considered unsuitable or unnecessary when a single trusted authority is sufficient, data must be processed with extremely low latency, large continuous streams would have to be replicated, or the truthfulness of source data cannot be established independently. This approach follows NIST's warning that blockchain should be selected only when its properties solve an actual problem [3].

The study deliberately excludes implementation parameters that could expose operational weaknesses or facilitate interference with air-defense systems. The proposed framework therefore focuses on assurance architecture, governance and evaluation criteria rather than deployment topology,

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

node placement, tactical communications, engagement data, sensor performance or security-control bypass techniques.

RESULTS AND DISCUSSION

The synthesis indicates that distributed ledgers can strengthen four aspects of operational-tactical information assurance: tamper evidence, provenance, distributed accountability and controlled multi-party synchronization. These benefits are strongest for records that must be trusted after the fact or across organizational boundaries. They are weaker for high-rate data whose value depends primarily on immediate delivery. The distinction leads to a hybrid model in which conventional secure data services remain responsible for real-time transport while the ledger records compact integrity evidence such as hashes, timestamps, provenance metadata, authorization events and configuration-state changes.

Table 1 summarizes the principal suitability findings. It separates plausible assurance functions from limitations that require conventional security and systems-engineering controls.

Table 1. Suitability of distributed-ledger functions for air-defense information assurance

Assurance requirement	**Potential ledger contribution**	**Principal limitation**	**Assessment**
Integrity and tamper evidence	Cryptographic chaining and replicated validation can make later record alteration detectable.	Does not prove that the original input was true or accurate.	High value for audit evidence and provenance [3].
Provenance and accountability	Signed transactions can associate records with authorized identities and preserve chronological history.	Identity infrastructure and private-key protection remain external dependencies.	High value when multiple organizations exchange controlled records [4,7].
Real-time information flow	Ledger can anchor hashes or metadata associated with information exchanges.	Consensus, replication and smart-contract execution add delay; a 2026 Air Force experiment reported 1.175 s for 20 MB [6].	Use selectively; avoid placing all high-rate data on-chain.
Availability and resilience	Replicated records reduce dependence on one database copy.	Network partition, node compromise, resource exhaustion and key loss are not eliminated.	Complement, not replace, resilient communications and backup architectures [3,4].
Interoperability	A shared transaction model can provide common audit	Different blockchain protocols and legacy	Requires standards, APIs and data models

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

	semantics across systems.	interfaces create integration complexity.	aligned with broader data architecture [1,4].
Governance and sovereignty	Permissioned membership supports controlled participation and auditable policy enforcement.	Who operates validators, changes rules and resolves disputes becomes a governance question.	Defense adoption requires sovereign governance and explicit authority [3,9,10].
Data quality	Ledger can preserve lineage and evidence that a record has not changed.	Immutable poor-quality data remains poor-quality data.	Must be combined with data-quality controls for accuracy, completeness and timeliness [2].

The most important result is that integrity and truth are different properties. Blockchain can demonstrate that a particular digital object or hash has not been altered since it was committed to the ledger, but it cannot determine whether a sensor, operator, software process or external data source was correct at the moment of creation. NATO's Data Quality Framework is therefore complementary: accuracy, completeness, consistency, timeliness and validity must be managed before and after ledger anchoring [2]. This observation prevents a common conceptual error in which immutability is treated as synonymous with trustworthy intelligence.

A second result concerns latency and data volume. The 2026 Air Force experiment provides a concrete indication that processing cost rises with data size and that 20 MB required 1.175 seconds on the tested platform [6]. The figure should not be generalized across products, but it illustrates why a ledger should not automatically sit in the critical path of every operational-tactical exchange. A more credible pattern is off-chain storage and transport with on-chain hashes, provenance references, authorization events and audit checkpoints. This reduces ledger volume while preserving evidence of integrity.

Third, permissioned governance is more consistent with defense requirements than open participation. Military information environments require authenticated membership, role-based or attribute-based authorization, classification handling, national control and accountable rule changes. NIST notes that permissioned networks create their own governance questions regarding who operates and controls the network [3]. In a coalition or interagency setting, this is not a minor administrative issue; governance is part of the security architecture.

Fourth, distributed ledgers should be evaluated as part of a broader data-centric architecture. NATO policy emphasizes interoperable, secure and governed data rather than a specific database technology [1,8,9]. Consequently, any blockchain framework should expose standardized interfaces, preserve metadata and classification rules, integrate with identity and access-management services,

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

and avoid creating a new isolated data silo. The ledger should strengthen the data architecture, not compete with it.

For Uzbekistan, Resolution PP-3832 is significant because it explicitly recognizes distributed ledger technology, legal-framework development, personnel training and inter-organizational implementation mechanisms [10]. Uzbek researchers have also examined blockchain in information-security and Internet-of-Things contexts [11-13]. These foundations support experimental research on permissioned ledgers for high-assurance government information systems. Nevertheless, direct transfer to air defense would require a separate defense-specific validation program covering classification, national cryptography requirements, performance under degraded connectivity, interoperability with existing information systems, lifecycle cost, certification, and human oversight.

Based on the evidence, a conceptual four-layer framework can be proposed. The first layer is the existing operational data environment, which continues to carry mission information through approved secure services. The second is an integrity-assurance interface that computes cryptographic fingerprints and attaches standardized provenance metadata. The third is a permissioned ledger containing compact assurance records rather than bulk sensor data. The fourth is governance and audit, defining membership, authorization, key lifecycle, retention, dispute resolution, software change control and independent verification. This layered concept preserves the main advantage of distributed ledgers while limiting performance and data-exposure costs.

Evaluation should therefore use measurable criteria rather than generic claims of 'blockchain security'. Relevant metrics include transaction-confirmation latency, throughput, ledger growth, recovery time, availability during network disruption, percentage of integrity events successfully verified, key-revocation time, interoperability success rate, audit completeness, and administrative overhead. Security testing should also examine implementation correctness and integration boundaries because systematic reviews identify interfaces with sensors, artificial intelligence, networks and other systems as important sources of risk [4].

CONCLUSION AND RECOMMENDATIONS

Distributed ledger and blockchain technologies can contribute to operational-tactical information integrity in air-defense information environments, but their value is specific rather than universal. Their strongest properties are tamper evidence, provenance, replicated accountability and a shared history among authorized participants. These characteristics align with contemporary defense requirements for trusted, secure, interoperable and governed data. However, blockchain cannot validate the truth of source data, cannot replace identity management, encryption, resilient communications or conventional cybersecurity, and may introduce unacceptable overhead if inserted indiscriminately into time-critical data paths.

The reviewed evidence supports a hybrid architecture. High-rate and time-sensitive information should remain within approved real-time data services, while a permissioned ledger may record hashes, provenance metadata, authorization events, configuration changes and selected audit evidence. This

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

approach is consistent with the empirical observation that blockchain processing time increases with data size and with broader research identifying latency, scalability and interoperability as unresolved defense challenges [4-6].

For research institutions and policymakers in Uzbekistan, three priorities are recommended. First, establish controlled laboratory and simulation studies using non-sensitive representative data to compare conventional databases, replicated databases and permissioned ledgers under identical integrity and performance requirements. Second, develop a governance model aligned with national cybersecurity law, data classification, sovereign key management and the distributed-ledger framework established by national policy [10]. Third, connect blockchain research to data-quality and interoperability programs so that integrity assurance does not become a separate technological silo.

Future research should focus on measurable trade-offs: how much additional integrity assurance is achieved per unit of latency, bandwidth, storage and administrative complexity; how ledger evidence can be integrated with data-quality metadata; and how permissioned governance performs across organizational boundaries. Adoption should proceed only when experiments demonstrate a clear assurance advantage over simpler architectures. In this sense, distributed ledger technology is best understood not as a replacement for air-defense information systems, but as a possible supporting trust layer within a carefully governed, data-centric and cyber-resilient architecture.

REFERENCES

1. North Atlantic Treaty Organization. Data Strategy for the Alliance. NATO Official Text, 5 May 2025.
2. North Atlantic Treaty Organization. Data Quality Framework for the Alliance. NATO Official Text, 2025.
3. Yaga, D., Mell, P., Roby, N., & Scarfone, K. Blockchain Technology Overview. NISTIR 8202. National Institute of Standards and Technology, 2018. DOI: 10.6028/NIST.IR.8202.
4. Blockchain Applications in the Military Domain: A Systematic Review. Technologies, 2025, 13(1), 23.
5. Alladi, T., Chamola, V., Parizi, R. M., & Choo, K.-K. R. Blockchain for aerospace and defense: Opportunities and open research challenges. Computers & Industrial Engineering, 151, 106982, 2021.
6. Pengkian, T., Praneetpolgrang, P., & Sirinam, P. The Design and Development of a Smart Digital Data Storage and Exchange Platform for the Air Force Command and Control Systems Using Blockchain Technology. Information Technology Journal KMUTNB, 22(1), 2026.
7. Connecting supplier and DoD blockchains for transparent part tracking. Blockchain: Research and Applications, 2(3), 100017, 2021. DOI: 10.1016/j.bcra.2021.100017.
8. North Atlantic Treaty Organization. NATO's Digital Transformation Implementation Strategy. NATO Official Text, 17 October 2024.

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

9. North Atlantic Treaty Organization. Alliance Digital Strategy. NATO Official Text, 13 January 2026.
10. Republic of Uzbekistan. Presidential Resolution No. PP-3832 of 3 July 2018, On Measures to Develop the Digital Economy and the Sphere of Crypto-Assets Turnover in the Republic of Uzbekistan, as amended. National Database of Legislation (LexUZ).
11. Zaripova, Sh. O. Axborot-kommunikatsiya texnologiyalar sohalarida blokcheyn texnologiyasi tushunchasi va uning imkoniyatlari. FAN va JAMIYAT, 2026/2-1, pp. 49-51.
12. Xudoyqulov, Z. T., & Saidullaev, M. K. Buyumlar Interneti texnologiyasida xavfsizlik muammolari va yechimlar. O'zA, 24 May 2024.
13. Kiberxavfsizlikni ta'minlashda blockchain texnologiyasining ahamiyati. Tadqiqotlar, 62(3), 2025.
14. National Institute of Standards and Technology. Blockchain Technology Overview and related blockchain resources. NIST, updated 2026.
15. North Atlantic Treaty Organization Allied Command Transformation. Digital Transformation: Building the Foundations for a Multi-Domain Operations Enabled Alliance. 2 October 2025.