International Journal of Engineering Trends and Technology
ISSN: 2231-5381/ https://doi.org/10.14445/22315381/IJETT-V74I8P134

Volume 74 Issue 8, 508-517, August 2026

Review Article

Blockchain for Industrial IoT Security: A PRISMA-Based Systematic Literature Review

Enrique Lee Huamaní[1], Erasmo Montufar-Barrientos[2], Carlos Ponce-Sanchez[3]

[1]*Image Processing Research Laboratory, Universidad de Ciencias y Humanidades, Lima-Perú.*
[2]*Facultad de Ciencias e Ingeniería, Universidad de Ciencias y Humanidades, Lima-Perú.*
[3]*Universidad Nacional de Ingeniería, Lima-Perú.*

[1]*Corresponding Author : ehuamaniu@uch.edu.pe*

Received: 31 July 2025 Revised: 28 July 2026 Accepted: 05 August 2026 Published: 29 August 2026

Abstract *- The Industrial Internet of Things (IIoT) has expanded the attack surface of modern industrial systems, creating a greater need for tamper-evident, auditable, and low-latency security mechanisms. We reviewed 44 peer-reviewed journal articles published between 2019 and 2024. Under the PRISMA 2020 framework, these studies were selected from 26,994 records retrieved from Scopus, ScienceDirect, IEEE Xplore, and the ACM Digital Library. For each included paper, we recorded the industrial context, security objective, role of blockchain, complementary technologies, validation approach, and reported limitations. The studies were subsequently organized into seven primary themes for descriptive synthesis: foundations and reviews; integrity and privacy; architecture and edge integration; 5G/6G convergence; authentication and access control; AI-enabled intelligent security; and trust, traceability, and industrial applications. Across the corpus, blockchain is used most often for device authentication, data integrity, access control, traceability, secure data exchange, and distributed trust management. Permissioned and edge-assisted architectures are generally regarded as more suitable for industrial constraints than resource-intensive public-chain designs. Even so, scalability, interoperability, latency, energy consumption, smart-contract robustness, and limited long-term industrial validation remain unresolved. Publications appearing after 2024 are discussed separately as a contextual update on Edge AI, TinyML, mobile edge computing, and zero-trust integration; they are not included in the 44-study review corpus.*

Keywords *- Industrial IoT security, Blockchain, Systematic Literature Review, PRISMA, Edge computing, Access control, Distributed trust.*

1. Introduction

The Industrial Internet of Things (IIoT) continues to reshape manufacturing, energy, logistics, healthcare, and industrial automation through pervasive sensing, machine-to-machine communication, and increasingly autonomous decision-making.

Clear operational benefits are enabled by this connectivity, but the cyber-attack surface is also enlarged. Compromised sensors, forged telemetry, weak device identities, and unauthorized access can disrupt operations, degrade safety, and undermine trust in industrial control environments [4, 7, 9, 17, 20, 24, 35].

For this reason, blockchain has been investigated as a decentralized trust layer for IIoT. Distributed ledgers can provide tamper-evident records, shared verification, programmable policy enforcement through smart contracts, and auditable provenance. In the reviewed literature, these capabilities are associated with device authentication, integrity protection, access control, secure data exchange, traceability, and inter-organizational trust [1, 3, 5, 6, 14, 21, 32, 37, 44, 54].

The architecture largely determines the security gains that can be achieved. In industrial environments, strict limits are imposed by latency, throughput, energy consumption, interoperability, deterministic behavior, and resilience requirements. To operate within these constraints, researchers examine private or permissioned chains, lightweight consensus, edge-assisted validation, software-defined networking, and next-generation connectivity [2, 11, 13, 15, 25-27, 48, 49, 52, 55].

Two recurring gaps are addressed in this review. First, the available evidence is dispersed across general IoT surveys, Industry 4.0 reviews, security frameworks, and application-specific studies, making it difficult to compare blockchain's contribution to distinct IIoT security objectives [12, 18, 28, 31, 34, 40, 42]. Second, hybrid architectures that combine blockchain with federated learning, deep learning, digital twins, and edge intelligence are becoming increasingly relevant, yet they are not always examined through a transparent evidence-selection process [8, 29, 33, 41].

We therefore use a PRISMA-based systematic review to document the search and screening process, map all 44 included studies, synthesize the evidence around four research questions, and discuss post-2024 hybrid directions separately as contextual material.

2. Method

2.1. Research Questions

The review was structured around research questions covering four aspects of blockchain use in industrial IoT networks: recent advances, data-protection mechanisms, applied techniques, and implementation constraints. These questions guided the selection of studies and were also used to organize the synthesis and interpretation presented in the following sections.

Table 1. Research questions

Title	Description
Id	Questions
RQ1	What are the most significant advances in the application of blockchain to improve the security of industrial IoT networks?
RQ2	How does blockchain contribute to improving data integrity and confidentiality in industrial IoT networks?
RQ3	What blockchain techniques have existing research proposed to secure industrial IoT networks?
RQ4	What are the main challenges and limitations associated with the use of blockchain in the security of industrial IoT networks?

2.2. Selection of the Data Sources

We searched four established academic databases: IEEE Xplore (n=4,454), Scopus (n=12,532), ACM Digital Library (n=1,773), and ScienceDirect (n=8,235). In total, the four database counts yielded 26,994 initial records. Engineering, computer science, cybersecurity, and industrial digitalization are covered collectively by these sources, reducing reliance on a single indexing service and broadening the evidence base used in the review.

2.3. Search Approach

The search protocol combined predefined Boolean queries with database filters, eligibility criteria, duplicate removal, and progressive screening. We focused on peer-reviewed journal articles indexed in IEEE Xplore, Scopus, the ACM Digital Library, and ScienceDirect. The search results were then restricted to English-language journal articles published between 2019 and 2024 and available in full text.

2.3.1. Search String

The core Boolean query used in the review is presented in Figure 1.

("blockchain" OR "distributed ledger technology" OR "smart contracts")
AND
("Industrial Internet of Things" OR "Industrial IoT" OR "IIoT")

Fig. 1 Generic Boolean search structure used across databases

Figure 1 presents the generic Boolean structure used in the search. Although the wording was adapted to each database interface, the two main concept blocks-blockchain-related technologies and Industrial IoT-were kept unchanged. In Scopus, we searched the title, abstract, and keywords, while the title and abstract fields were searched in ScienceDirect and the ACM Digital Library. IEEE Xplore, in contrast, was queried using the title field. Manual relevance checks were subsequently performed to ensure that the retrieved studies focused on industrial security rather than consumer IoT or unrelated blockchain applications.

2.3.2. Inclusion Criteria for Studies to be Included in this Review

A study was included only when all of the predefined conditions were met. Specifically, the article had to be (i) a peer-reviewed journal publication written in English and (ii) published between 2019 and 2024. In addition, (iii) blockchain or distributed-ledger technology had to be addressed explicitly, and (iv) a direct contribution had to be made to security, trust, privacy, access control, integrity, resilience, or secure data exchange within an Industrial IoT, Industry 4.0, or closely related industrial cyber-physical context.

Duplicate records, conference proceedings, editorials, preprints, book chapters, inaccessible full texts, non-English publications, and records outside the 2019–2024 search window were excluded. We also removed studies that focused exclusively on consumer IoT or other non-industrial domains. In addition, papers were excluded when blockchain or IoT was mentioned without a clear contribution to security-related issues.

During the screening process, each candidate paper was evaluated against at least one of the predefined review dimensions. These dimensions included authentication or access control, data integrity or confidentiality, trust or traceability, attack resilience, blockchain architecture or consensus, secure industrial data sharing, and implementation constraints relevant to IIoT.

2.3.3. Conducting Review Process

Study selection followed the PRISMA 2020 framework. We first applied database filters based on publication year, language, source type, and full-text availability. Duplicate records were then removed, after which the remaining records were screened by title and abstract. Full texts were subsequently evaluated against the predefined industrial-security criteria.

Through this sequence, a clear connection was maintained between the initial search, the final 44-study evidence corpus, and the thematic synthesis presented in the Results section.

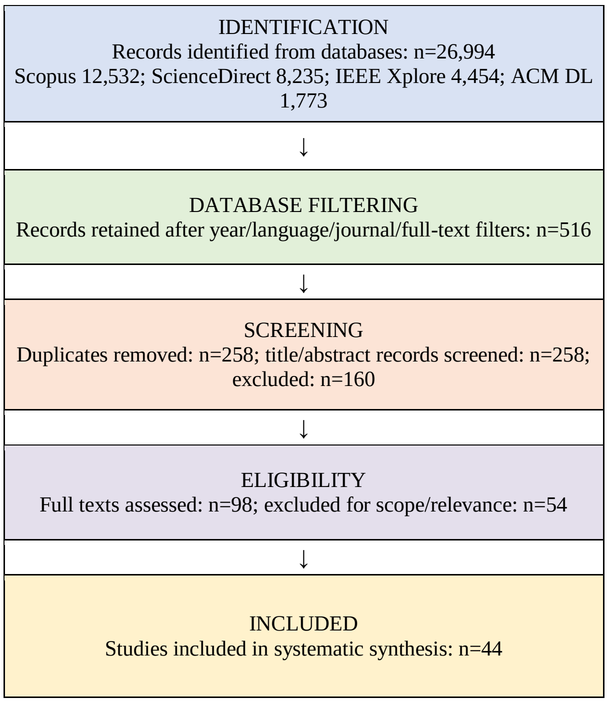

Fig. 2 PRISMA 2020 flow of study identification, screening, eligibility, and inclusion

Figure 2 summarizes the selection process. The search initially returned 26,994 records, and 516 remained after automatic database filtering. We removed 258 duplicates and screened the remaining 258 records by title and abstract; 160 were excluded at that stage. Full-text eligibility was then assessed for 98 articles, of which 54 were excluded because they lacked direct industrial-security alignment. The final systematic synthesis, therefore included 44 studies.

2.3.4. Data Extraction and Synthesis Strategy

For every included study, we extracted the publication year, industrial context, security objective, role of blockchain, complementary technologies, validation approach, and reported limitations. Descriptive quantitative summaries were combined with qualitative thematic coding aligned with RQ1-RQ4. Because substantial differences were found across architectures, datasets, evaluation metrics, and validation conditions, a formal meta-analysis was not considered appropriate. Each study was assigned one primary thematic category for descriptive counting, while secondary contributions were retained in the RQ mapping.

2.3.5. Corpus Boundary and Treatment of Supporting References

The primary corpus contains 44 studies: references [1-15, 17-21, 23-29, 31-35, 37, 40-42, 44, 48-50, 52-55]. These publications met the predefined journal article, date, relevance, and industrial-security criteria. Eleven sources from 2019-2024 were retained only for contextual or methodological discussion and were not counted in the primary synthesis: conference papers [16, 22, 38, 46, 51]; a preprint [30]; editorials [36, 45]; a book chapter [39]; and broader domain references whose principal scope was outside direct IIoT security [43, 47].

Five references published in 2025 [56-60] were added only after the systematic search had been completed. We use them to contextualize rapidly emerging hybrid directions rather than as part of the primary corpus. Accordingly, they were excluded from the PRISMA counts, the 44-study matrix, and the quantitative thematic frequencies. By keeping this separation, the 2019-2024 review remains reproducible while recent developments can still be acknowledged in the Discussion.

3. Results

The final evidence corpus contained 44 studies. We report the results at three levels: the PRISMA screening workflow, study-level coding for every included article, and thematic synthesis around the four research questions. With the evidence presented in this manner, the conclusions can be traced to the complete corpus rather than to only a small set of representative papers.

3.1. Quantitative Synthesis of the Screened Evidence

Table 2. Quantitative synthesis of the screening workflow

Stage	Count	Interpretation
Initial records identified	26,994	IEEE Xplore: 4,454; Scopus: 12,532; ACM Digital Library: 1,773; ScienceDirect: 8,235
Records after automatic database filters	516	English, journal, accessibility, and 2019-2024 restriction
Duplicates removed	258	50.0% of the filtered set, indicating high overlap across databases
Title/abstract exclusions	160	Records that did not answer the research questions

Scope exclusions	54	Records outside the industrial-security focus of the review
Final included studies	44	8.53% of filtered records and approximately 0.16% of the initial search yield

3.2. Coverage and Thematic Coding of the 44 Included Studies

To make study coverage transparent, we coded every article in the primary corpus by publication year, principal focus, primary synthesis theme, and research-question coverage. The complete set of 44 studies is listed in Table 3. Primary themes were used only for descriptive counting; an individual study could still contribute to more than one research question.

Table 3. Included studies and thematic coding of the systematic review corpus (n=44)

Ref.	Year	Primary focus coded in this review	Primary theme	RQ coverage
[1]	2020	Blockchain-edge framework	Architecture/edge	RQ1,RQ3
[2]	2020	5G-enabled industrial automation review	5G/6G convergence	RQ1,RQ4
[3]	2020	Secure sensor communication	Integrity/privacy	RQ2,RQ3
[4]	2022	IoT security state-of-the-art review	Foundations/review	RQ1-RQ4
[5]	2020	Cross-domain device authentication	Authentication/access	RQ1,RQ3
[6]	2020	Tokenized trustless IIoT applications	Trust/traceability	RQ1,RQ3
[7]	2021	IIoT blockchain security survey	Foundations/review	RQ1,RQ4
[8]	2023	Blockchain + federated-learning IDS	AI/intelligent security	RQ1,RQ3,RQ4
[9]	2021	Blockchain for IIoT survey	Foundations/review	RQ1-RQ4
[10]	2024	Blockchain integration for IIoT security	Trust/traceability	RQ1-RQ4
[11]	2020	Private blockchain for IIoT	Architecture/edge	RQ1,RQ3,RQ4
[12]	2021	Industry 4.0 blockchain applications review	Foundations/review	RQ1,RQ4
[13]	2022	Blockchain + 5G adoption	5G/6G convergence	RQ1,RQ3,RQ4
[14]	2020	Decentralized blockchain security	Authentication/access	RQ1,RQ3
[15]	2022	Blockchain-integrated SDN	Architecture/edge	RQ3,RQ4
[17]	2021	Industrial blockchain security mechanisms	Integrity/privacy	RQ2-RQ4
[18]	2020	Blockchain IoT applications survey	Foundations/review	RQ1,RQ4
[19]	2020	Industrial healthcare blockchain platform	Integrity/privacy	RQ1-RQ3
[20]	2021	Blockchain attacks/challenges in IoT	Integrity/privacy	RQ2,RQ4
[21]	2022	IIoT supply-chain requirements	Trust/traceability	RQ1,RQ3,RQ4
[23]	2023	Multi-chain petroleum data sharing	Integrity/privacy	RQ2-RQ4
[24]	2024	Blockchain in IoT cybersecurity review	Foundations/review	RQ1-RQ4
[25]	2023	Blockchain-IoT-6G convergence	5G/6G convergence	RQ1,RQ3,RQ4
[26]	2020	Blockchain framework for IoT	Architecture/edge	RQ1,RQ3,RQ4
[27]	2024	Opportunistic block validation	Architecture/edge	RQ3,RQ4
[28]	2024	Blockchain in IoT security	Foundations/review	RQ1-RQ4
[29]	2024	Deep-learning-integrated blockchain	AI/intelligent security	RQ1,RQ3
[31]	2021	Industry 4.0 + blockchain review	Foundations/review	RQ1,RQ4
[32]	2022	Secure data sharing in smart industries	Integrity/privacy	RQ2,RQ3
[33]	2023	Blockchain trust for digital twins	AI/intelligent security	RQ1,RQ3
[34]	2023	IoT-blockchain integration review	Foundations/review	RQ1,RQ4
[35]	2021	IoT/IIoT blockchain survey	Foundations/review	RQ1-RQ4
[37]	2022	Schloss secure IIoT architecture	Architecture/edge	RQ1,RQ3,RQ4
[40]	2023	Blockchain-IoT in Industry 4.0/5.0	Foundations/review	RQ1,RQ4
[41]	2023	Blockchain + deep learning for digital twins	AI/intelligent security	RQ2,RQ3
[42]	2022	Blockchain-based IoT security solutions	Integrity/privacy	RQ1-RQ4
[44]	2021	Blockchain access control/privacy review	Authentication/access	RQ2-RQ4
[48]	2022	Blockchain-based 6G and IIoT systems	5G/6G convergence	RQ1,RQ3,RQ4
[49]	2023	Blockchain + 6G industrial automation	5G/6G convergence	RQ1,RQ3,RQ4
[50]	2023	Blockchain cybersecurity for connected networks	Integrity/privacy	RQ2,RQ3
[52]	2022	BIoT for futuristic industrial networking	Architecture/edge	RQ1,RQ3,RQ4
[53]	2021	Security audit of an industrial blockchain platform	Integrity/privacy	RQ2,RQ4
[54]	2021	Blockchain-based IIoT access-control review	Authentication/access	RQ2-RQ4
[55]	2023	Blockchain + 802.11ax IoT WLANs	Architecture/edge	RQ3,RQ4

The coding produced 11 foundations/review studies (25.0%), 9 integrity/privacy studies (20.5%), 8 architecture/edge studies (18.2%), 5 studies on 5G/6G convergence (11.4%), 4 authentication/access-control studies (9.1%), 4 AI/intelligent-security studies (9.1%), and 3 trust/traceability studies (6.8%).

The corpus included 10 studies from 2020, 10 from 2021, 9 from 2022, 10 from 2023, and 5 from 2024. These figures are used to describe the composition of the evidence base; they are not citation-based bibliometric indicators.

3.3. RQ1: What are the most Significant Advances in the Application of Blockchain to Improve the Security of Industrial IoT Networks?

Five functional advances recur across the corpus. Device authentication and access control are addressed in [5, 14, 44, 54]; integrity, privacy, and secure data exchange in [3, 17, 19, 23, 32, 42, 50, 53]; and decentralized trust and traceability in [6, 10, 21]. Another group of studies examines architectural decentralization and edge-aware operation [1, 11, 15, 26, 27, 37, 52, 55], while convergence with intelligent or next-generation networking technologies is explored in [2, 8, 13, 25, 29, 33, 41, 48, 49]. These patterns and the trade-offs associated with them are further reinforced by general reviews and surveys [4, 7, 9, 12, 18, 20, 24, 28, 31, 34, 35, 40].

The evidence does not point to a single universally superior blockchain algorithm; instead, a set of architectural choices stands out. Researchers use permissioned ledgers, consortium governance, off-chain storage, edge-assisted verification, lightweight consensus, multi-chain designs, and programmable smart contracts to adapt blockchain to industrial constraints. The application domains identified in the coded corpus are summarized in Figure 3, while representative technical patterns are presented in Table 4. Taken together, the studies support the use of blockchain mainly as a trust and coordination layer that complements existing industrial systems rather than replacing industrial middleware altogether.

Fig. 3 Thematic map of blockchain security applications identified in the 44-study corpus

3.4. RQ2: How does Blockchain Aid in Enhancing Data Integrity and Confidentiality in Industrial IoT Networks?

The strongest contribution to integrity and confidentiality is observed when blockchain is used as a trust anchor for logging, provenance, verification, and access enforcement rather than as the sole repository for industrial data [3, 17, 23, 32, 42, 44, 50, 53, 54].

3.4.1. Data Integrity and Provenance

Hash-linked records, timestamped transactions, digitally signed events, and consensus-backed audit trails make unauthorized modification easier to detect and provenance easier to establish across multiple stakeholders. In industrial settings, researchers apply these mechanisms to sensor readings, device events, operational records, digital-twin interactions, and cross-organizational data sharing [3, 19, 23, 32, 33, 41, 53]. Their value is especially evident when integrity evidence must be shared among parties that do not depend on a single administrative authority. Privacy and confidentiality are generally handled through hybrid designs instead of placing sensitive industrial data directly on-chain.The reviewed studies combine blockchain with encryption, permissioned membership, access-control policies, secure data-sharing models, off-chain repositories, and trusted edge processing [11, 17, 20, 32, 42, 44, 50, 54]. In some architectures, local anomaly detection or feature extraction is performed before trusted events are committed to the ledger, thereby reducing unnecessary data transmission [8, 29, 41].

3.4.2. Resilience and DoS-Related Considerations

Decentralized verification and replicated records can reduce dependence on a single trusted server and thus lessen some consequences of single points of failure. Volumetric denial-of-service attacks, however, are not eliminated by blockchain.

Its resilience is shaped by consensus design, validator placement, communication overhead, and network conditions [20, 24, 27, 35, 37, 55]. For this reason, the literature treats blockchain as one component of layered resilience rather than as a standalone DoS-prevention mechanism.

3.5. RQ3: What Blockchain Techniques have Existing Research Proposed to Secure Industrial IoT Networks?

The corpus does not identify one dominant technique. Instead, a multi-layered security landscape is revealed. Researchers propose blockchain-edge integration [1, 15, 26, 37, 52], secure authentication and access control [5, 14, 44, 54], cryptographic integrity and privacy mechanisms [3, 17, 32, 42, 50], smart-contract and token-based policy enforcement [6, 10], supply-chain or multi-party traceability [21, 23], intelligent anomaly detection [8, 29, 41], and 5G/6G-aware designs intended to improve latency, throughput, and industrial connectivity [2, 13, 25, 48, 49]. Representative technical examples are presented in Table 4, and the full 44-study coverage is documented in Table 3.

Table 4. Representative blockchain techniques for Industrial IoT network security

Reference	Proposed approach	Technique	Primary security contribution
[1]	Blockchain-edge framework for IIoT	Edge computing + blockchain	Decentralized authentication
[3]	Secure industrial sensor communication	Blockchain encryption + consensus	Confidentiality and integrity
[5]	Cross-domain IIoT authentication	Blockchain-assisted authentication	Secure device identity
[6]	Tokenized trustless IIoT applications	Tokenization + smart contracts	Distributed trust enforcement
[10]	Integrated IIoT security	Distributed ledger + policy logic	Multi-function security
[13]	Blockchain with 5G for IIoT	5G integration + consensus optimization	Low-latency secure communication
[14]	Decentralized IIoT security	Distributed ledger architecture	Resilient decentralized security
[15]	Blockchain-integrated SDN	SDN + lightweight consensus	Energy-aware secure networking
[17]	Industrial blockchain security	Cryptography + consensus	Integrity protection
[21]	Blockchain in IIoT supply chains	Traceability + distributed ledger	Supply-chain provenance
[23]	Petroleum-sector secure data sharing	Multi-chain blockchain	Inter-organizational data security
[29]	Deep-learning-integrated blockchain	AI anomaly detection + blockchain	Intelligent threat detection
[32]	Secure data sharing in smart industries	Privacy-preserving blockchain	Secure data exchange
[33]	Trust for IIoT digital twins	Blockchain + digital twin	Trusted digital-twin interactions
[37]	Schloss secure IIoT architecture	Blockchain system architecture	Secure industrial platform

Two implementation tendencies are repeatedly observed in the evidence. First, researchers favor private, permissioned, or consortium architectures in industrial settings because these designs support controlled governance and can reduce latency relative to open public-chain designs [11, 13, 17, 35]. Second, blockchain is increasingly integrated with edge computing, SDN, digital twins, deep/federated learning, and next-generation mobile networks. These complementary technologies are used to address the performance and intelligence limitations of ledger-only designs [1, 8, 15, 25, 29, 33, 37, 41, 48, 49, 52].

3.6. RQ4: What are the Main Challenges and Limitations Associated with the use of Blockchain in the Security of Industrial IoT Networks?

Scalability, interoperability, latency, implementation complexity, and energy or computational cost are the main barriers reported across the literature. These issues become particularly important in factories and critical infrastructures, where deterministic response times, predictable networking behavior, constrained devices, and integration with legacy systems are often required [2, 7, 13, 15, 20, 24-27, 31, 34, 35, 48, 49, 52, 55].

Other concerns are equally practical: smart-contract defects, key and identity management, privacy leakage, cross-organizational governance, and the limited amount of long-duration field validation. Security-audit work shows that conventional secure engineering and testing are still required for blockchain-based industrial platforms [53].

Likewise, access-control and privacy reviews note that correct authorization or confidentiality is not guaranteed by ledger immutability alone [44, 54]. The literature therefore provides substantial proof-of-concept evidence, but far less evidence is available on long-term maintainability, migration cost, standardized interoperability, and operational governance.

3.7. Edge AI, TinyML, and Hybrid Security Architectures

The systematic search ended in 2024. To place rapidly emerging directions in context without changing the predefined corpus, we reviewed five 2025 publications separately as a post-search update [56-60]. These sources were not included in the PRISMA counts, the 44-study coding table, or the quantitative theme frequencies. Continued interest is shown in zero-trust combinations of AI, blockchain, and edge computing [56], blockchain-assisted edge architectures [57, 58], mobile-edge resource optimization [59], and TinyML or on-device inference for constrained environments [60]. Although these directions are promising, stronger comparative claims will require reproducible industrial benchmarks for latency, throughput, energy consumption, security effectiveness, and fault tolerance.

Table 5. Post-search hybrid directions highlighted by 2025 contextual literature

Direction	Security value	Main gap	Refs.
AI + blockchain + edge + zero-trust	Adaptive verification	Integration/resource cost	[56]
Blockchain-assisted edge	Low-latency secure sharing	Deployment maturity	[57]
Smart-factory blockchain	Integrity and traceability	Benchmark comparability	[58]
Blockchain + mobile edge	Energy-aware offloading	Workload management	[59]
TinyML / on-device inference	Local anomaly detection	Model drift, memory, benchmarks	[60]

3.8. Real-World Deployments and Case-Study Implications

Evidence from real deployments remains less mature than the conceptual and prototype literature. Even so, several sector-specific settings are represented in the included corpus: industrial healthcare [19], supply-chain traceability [21], petroleum-sector data sharing [23], SDN-enabled industrial networking [15], digital-twin trust and secure communication [33, 41], secure industrial platforms [37, 53], and advanced industrial networking [48, 49, 52, 55].

These examples also show why implementation choices cannot be separated from context. A technique that improves traceability or decentralized trust may still be unsuitable when deterministic latency, constrained memory, or legacy interoperability dominate the deployment requirements.

4. Discussion

Taken as a whole, the 44-study corpus indicates that blockchain is most valuable for IIoT security when it functions as an enabling trust layer rather than as a standalone replacement for industrial middleware. The available evidence is distributed across several thematic areas. Foundational reviews define the design space [4, 7, 9, 12, 18, 24, 28, 31, 34, 35, 40]. Secure communication, data sharing, audits, and confidentiality are addressed by integrity and privacy studies [3, 17, 19, 20, 23, 32, 42, 50, 53], while architecture-focused work examines edge integration, private chains, SDN, validation, and industrial platforms [1, 11, 15, 26, 27, 37, 52, 55]. Across these groups, authentication, provenance, policy automation, and shared trust repeatedly emerge as the main benefits.

The review also highlights an important limitation of the evidence base. It is difficult to compare directly with many papers that report conceptual architectures, simulations, limited testbeds or domain-specific prototypes. A meaningful meta-analysis was not feasible due to differences in consensus mechanisms, hardware, datasets, network conditions, threat models, and evaluation metrics.

The 2025 literature post-search [56-60] provides further support for hybrid edge intelligence, zero-trust integration, mobile-edge optimization, and TinyML, but these papers were intentionally excluded from the 44-study corpus to maintain the temporal boundary and reproducibility of the systematic search.

Methodologically, the work is designed as a systematic literature review and not a bibliometric review. The quantitative part describes the search and screening process and summarizes the thematic distribution of the included evidence. Citation-network, co-authorship, bibliographic-coupling and keyword co-occurrence analysis were not conducted.

The classification was instead derived directly from the research questions, PRISMA workflow, eligibility criteria, study-level coding and qualitative synthesis of the manuscript. The review was limited to four databases, journal articles in English and the period 2019–2024. Further updates may include database coverage and standardized quality-assessment instruments, and benchmarking criteria in common.

5. Conclusion

The systematic literature review reveals that blockchain can enhance IIoT security by providing verifiable device identity, tamper-evident records, secured data exchange, access governance, traceability, and distributed trust. In the 44 studies included, blockchain is not primarily presented as a standalone solution but as one layer of a larger security architecture. Industry-relevant designs are increasingly integrating permissioned ledgers with edge computing, lightweight consensus, smart contracting, software-defined networking, digital twins, AI-driven analytics and next-gen connectivity. These architectures aim to preserve the auditability and distributed-trust properties of blockchain, while reducing latency, communication overhead and resource consumption.

Nevertheless, several challenges remain to be addressed before wide industrial adoption, such as interoperability, scalability, energy and computation cost, smart-contract and identity risks, and lack of long-term real-world validation. Priorities for future research are reproducible large-scale industrial testbeds, standardized latency/throughput/energy/security benchmarks, secure smart-contract engineering, interoperability models, and rigorous evaluation of on-device intelligence integrated with verifiable trust frameworks.

Overall, the findings support a cautious approach to adoption. Blockchain can serve as a credible security-enabling technology for IIoT when its architecture is aligned with the operational constraints of the target environment and when security claims are validated beyond proof-of-concept settings.

References

[1] Tanesh Kumar et al., “BlockEdge: Blockchain-Edge Framework for Industrial IoT Networks,” *IEEE Access*, vol. 8, pp. 154166-154185, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[2] Ishan Mistry et al., “Blockchain for 5G-Enabled IoT for Industrial Automation: A Systematic Review, Solutions, and Challenges,” *Mechanical Systems and Signal Processing*, vol. 135, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[3] Geetanjali Rathee et al., “A Secure IoT Sensors Communication in Industry 4.0 using Blockchain Technology,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 1, pp. 533-545, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[4] Abdullah Ayub Khan et al., “Internet of Things (IoT) Security with Blockchain Technology: A State-of-the-Art Review,” *IEEE Access*, vol. 10, pp. 122679-122695, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] Meng Shen et al., “Blockchain-Assisted Secure Device Authentication for Cross-Domain Industrial IoT,” *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 942-954, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[6] Daniele Mazzei et al., “A Blockchain Tokenizer for Industrial IoT Trustless Applications,” *Future Generation Computer Systems*, vol. 105, pp. 432-445, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[7] Shahid Latif et al., “Blockchain Technology for the Industrial Internet of Things: A Comprehensive Survey on Security Challenges, Architectures, Applications, and Future Research Directions,” *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 11, pp. 1-37,2021. [CrossRef] [Google Scholar] [Publisher Link]

[8] Saqib Ali, Qianmu Li, and Abdullah Yousafzai, “Blockchain and Federated Learning-based Intrusion Detection Approaches for Edge-Enabled Industrial IoT Networks: A Survey,” *Ad Hoc Network*, vol. 152, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] R. Lakshmana Kumar et al., “A Survey on Blockchain for Industrial Internet of Things,” *Alexandria Engineering Journal*, vol. 61, no. 8, pp. 6001-6022, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] Yash Bobde et al., “Enhancing Industrial IoT Network Security Through Blockchain Integration,” *Electronics*, vol. 13, no. 4, pp. 1-23, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] Minho Jo et al., “Private Blockchain in Industrial IoT,” *IEEE Network*, vol. 34, no. 5, pp. 76-77, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[12] Mohd Javaid et al., “Blockchain Technology Applications for Industry 4.0: A Literature-based Review,” *Blockchain: Research and Applications*, vol. 2, no. 4, pp. 1-11, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[13] Manpreet Kaur et al., “Adoption of Blockchain with 5G Networks for Industrial IoT: Recent Advances, Challenges, and Potential Solutions,” *IEEE Access*, vol. 10, pp. 981-997, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[14] Ali Hassan Sodhro et al., “Towards Blockchain-Enabled Security Technique for Industrial Internet of Things based Decentralized Applications,” *Journal of Grid Computing*, vol. 18, no. 4, pp. 615-628, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[15] Sasikumar Asaithambi et al., “An Energy-Efficient and Blockchain-Integrated Software Defined Network for the Industrial Internet of Things,” *Sensors*, vol. 22, no. 20, pp. 1-25, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Varsha Prafull Patil, and Sharada Ohatkar “Blockchain for IoT/Industrial IoT Applications,” *2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, Pune, India, pp. 1-7, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[17] Sheikh Mohammad Idrees et al., “Security Aspects of Blockchain Technology Intended for Industrial Applications,” *Electronics*, vol. 10, no. 8, pp. 1-24, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[18] Laphou Lao et al., “A Survey of IoT Applications in Blockchain Systems: Architecture, Consensus, and Traffic Modeling,” *ACM Computing Surveys*, vol. 53, no. 1, pp. 1-32, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[19] Ahmed Farouk et al., “Blockchain Platform for Industrial Healthcare: Vision and Future Opportunities,” *Computer Communications*, vol. 154, pp. 223-235, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[20] Saurabh Singh, A.S.M. Sanwar Hosen, and Byungun Yoon, “Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network,” *IEEE Access*, vol. 9, pp. 13938-13959, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[21] Zhao-Hui Sun et al., “Potential Requirements and Opportunities of Blockchain-based Industrial IoT in Supply Chain: A Survey,” *IEEE Transactions on Computational Social Systems*, vol. 9, no. 5, pp. 1469-1483, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[22] S. Prasanna Venkatesh al., “Secure IoT with Blockchain for Industrial Application,” *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, Kamand, India, pp. 1-6, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[23] Samir M. Umran al., “Multi-Chain Blockchain based Secure Data-Sharing Framework for Industrial IoTs Smart Devices in Petroleum Industry,” *Internet of Things*, vol. 24, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[24] Love Allen Chijioke Ahakonye, Cosmas Ifeanyi Nwakanma, and Dong-Seong Kim, “Tides of Blockchain in IoT Cybersecurity,” *Sensors*, vol. 24, no. 10, pp. 1-27, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[25] Abu Jahid, Mohammed H. Alsharif, Trevor J. Hall, “The Convergence of Blockchain, IoT and 6G: Potential, Opportunities, Challenges and Research Roadmap,” *Journal of Network and Computer Applications*, vol. 217, pp. 1-26, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[26] Deepa Pavithran al., “Towards Building a Blockchain Framework for IoT,” *Cluster Computing*, vol. 23, no. 3, pp. 2089-2103, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[27] Seungchul Lee, and Jae-Hoon Kim, “Opportunistic Block Validation for IoT Blockchain Networks,” *IEEE Internet of Things Journal*, vol. 11, no. 1, pp. 666-676, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[28] Shreya B. Jadhav, “Blockchain in IoT Security,” *IJRASET Journal for Research in Applied Science and Engineering Technology*, vol. 12, no. 4, pp. 1073-1078, 2024. [CrossRef] [Publisher Link]

[29] Ahamed Aljuhani et al., “A Deep-Learning-Integrated Blockchain Framework for Securing Industrial IoT,” *IEEE Internet of Things Journal*, vol. 11, no. 5, pp. 7817-7827, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[30] Gang Wang, “SoK: Applying Blockchain Technology in Industrial Internet of Things,” *Cryptology ePrint Archive*, pp .1-30, 2021. [Google Scholar] [Publisher Link]

[31] Alain Aoun et al., “A Review of Industry 4.0 Characteristics and Challenges, with Potential Improvements using Blockchain Technology,” *Computers and Industrial Engineering*, vol. 162, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[32] Gunasekaran Manogaran et al., “Blockchain Assisted Secure Data Sharing Model for Internet of Things based Smart Industries,” *IEEE Transactions on Reliability*, vol. 71, no. 1, pp. 348-358, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[33] Sasikumar Asaithambi et al., “Blockchain-based Trust Mechanism for Digital Twin Empowered Industrial Internet of Things,” *Future Generation Computer Systems*, vol. 141, pp. 16-27, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[34] Naresh Adhikari, and Mahalingam Ramkumar, “IoT and Blockchain Integration: Applications, Opportunities, and Challenges,” *Network*, vol. 3, no. 1, pp. 115-141, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[35] Sanjeev Kumar Dwivedi et al., “Blockchain-based Internet of Things and Industrial IoT: A Comprehensive Survey,” *Security and Communication Networks*, vol. 2021, no. 1, pp. 1-21, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[36] Kim-Kwang Raymond Choo, Zheng Yan, and Weizhi Meng, “Editorial: Blockchain in Industrial IoT Applications: Security and Privacy Advances, Challenges, and Opportunities,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4119-4121, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[37] Fatemeh Ghovanlooy Ghajar, Axel Sikora, and Dominik Welte, “Schloss: Blockchain-based System Architecture for Secure Industrial IoT,” *Electronics*, vol. 11, no. 10 pp. 1-18, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[38] Rakshit Kothari, Kalpana Jain, and Naveen Choudhary, “Integration of Cross-Chain Technology-based High-Performance Blockchain Network for Industrial Internet of Things,” *2024 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)*, Windhoek, Namibia, pp. 1-7, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[39] Geetanjali Rathee, Sharmi Dev Gupta, and Naveen Jaglan, *A Review on Blockchain and its Necessitate in Industrial IoT*, Innovations in Computer Science and Engineering, Springer, Singapore, vol. 103, pp. 207-217, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[40] Amit Kumar Tyagi et al., "Blockchain-Internet of Things Applications: Opportunities and Challenges for Industry 4.0 and Society 5.0," *Sensors*, vol. 23, no. 2, pp. 1-30, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[41] Prabhat Kumar et al., "Blockchain and Deep Learning for Secure Communication in Digital Twin Empowered Industrial IoT Network," *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 5, pp. 2802-2813, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[42] Israa Al-Barazanchi et al., "Blockchain Technology - based Solutions for IoT Security," *Iraqi Journal for Computer Science and Mathematics*, vol. 3, no. 1, pp. 1-12, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[43] Javid Mousavi et al., "Blockchain in Supply Chain Management: A Review, Bibliometric, and Network Analysis," *Environmental Science and Pollution Research International*, vol. 33, no. 12, pp. 1-26, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[44] Pradnya Patil, M. Sangeetha, and Vidhyacharan Bhaskar, "Blockchain for IoT Access Control, Security and Privacy: A Review," *Wireless Personal Communications*, vol. 117, no. 3, pp. 1815-1834, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[45] Hong-Ning Dai et al., "Guest Editorial: Special Section on Next Generation Blockchain Technology with Industrial IoT in Industry 4.0," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 12, pp. 9151-9152, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[46] Nandita Goyal et al., "IoT based Blockchain System for Security from Identity Theft in Industrial Automation," *2024 International Conference on Trends in Quantum Computing and Emerging Business Technologies*, Pune, India, pp. 1-4, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[47] Oskar Juszczyk, and Khuram Shahzad, "Blockchain Technology for Renewable Energy: Principles, Applications and Prospects," *Energies*, vol. 15, no. 13, pp. 1-24, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[48] Gaurav Dhiman, and Atulya K. Nagar, "Blockchain-based 6G and Industrial Internet of Things Systems for Industry 4.0/5.0," *Expert Systems*, vol. 39, no. 10, pp. 1-2, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[49] Mano Yadav et al., "Exploring Synergy of Blockchain and 6G Network for Industrial Automation," *IEEE Access*, vol. 11, pp. 137163-137187, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[50] Deepak Choudhary, and Roop Pahuja, "A Blockchain-based Cyber-Security for Connected Networks," *Peer-to-Peer Networking and Applications*, vol. 16, no. 4, pp. 1852-1867, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[51] Piyush Pant et al., "Blockchain for AI-Enabled Industrial IoT with 5G Network," *2022 14th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, Ploiesti, Romania, pp. 1-4, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[52] N. Nasurudeen Ahamed, and R. Vignesh, "A Blockchain IoT (BIoT) Integrated into Futuristic Networking for Industry," *International Journal of Mathematical, Engineering and Management Sciences*, vol. 7, no. 4, pp. 525-546, 2022, [CrossRef] [Google Scholar] [Publisher Link]

[53] Jan Stodt et al., "Security Audit of a Blockchain-based Industrial Application Platform," *Algorithms*, vol. 14, no. 4, pp. 1-21, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[54] Peng Zhai, Liping Zhang, and Jingsha He, "A Review of Blockchain-based Access Control for the Industrial IoT," *Converter*, vol. 2021, no. 3, pp. 308-316, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[55] Arezou Zamanyzadeh Abyaneh, Nizar Zorba, and Bechir Hamdaoui, "Empowering Next-Generation IoT WLANs Through Blockchain and 802.11ax Technologies," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 7, pp. 7412-7421, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[56] Inam Ullah Khan et al., "Integrating AI, Blockchain, and Edge Computing for Zero-Trust IoT Security: A Comprehensive Review of Advanced Cybersecurity Framework," *Computers, Materials and Continua*, vol. 85, no. 3, pp. 4307-4344, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[57] Sasikumar Asaithambi et al., "A Secure and Trustworthy Blockchain-Assisted Edge Computing Architecture for Industrial Internet of Things," *Scientific Reports*, vol. 15, no. 1, pp. 1-17, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[58] Meryam Essaid, and Hongtaek Ju, "Blockchain Solutions for Enhancing Security and Privacy in Industrial IoT," *Applied Sciences*, vol. 15, no. 12, pp. 1-26, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[59] Yiyi Zhang et al., "Energy-Efficient Blockchain-IIoT with Mobile Edge Computing: Optimizing Resource Allocation and Multi-Hop Offloading," *Results in Engineering*, vol. 26, pp. 1-16, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[60] Soroush Heydari, and Qusay H. Mahmoud, "Tiny Machine Learning and On-Device Inference: A Survey of Applications, Challenges, and Future Directions," *Sensors*, vol. 25, no. 10, pp. 1-23, 2025. [CrossRef] [Google Scholar] [Publisher Link]