Indonesian Journal of Electrical Engineering and Computer Science
Vol. 44, No. 1, October 2026, pp. 263~271
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v44.i1.pp263-271

Evidence-based evaluation of blockchain frameworks for secure data management

Kapil Dev Das
Department of Computer Science and Engineering, Dumkal Institute of Engineering and Technology, Murshidabad, India

Article Info

Article history:

Received Apr 10, 2026
Revised Aug 20, 2026
Accepted Sep 9, 2026

Keywords:

Blockchain
Consensus
Data sharing
Evaluation framework
Evidence synthesis
Scalability
Secure data management

ABSTRACT

Blockchain-based data management is frequently proposed for environments that require integrity, auditability, controlled sharing, and resistance to unauthorized modification. This review revisits the evidence base for secure data management and responds to a recurring limitation in prior surveys: platform characteristics are often described separately from the decision criteria needed to select an architecture. The revised study retains the original 2019–2025 review scope and expands the cited evidence base to 50 sources. A transparent review protocol, explicit research questions, a five-layer architecture model, and a decision-oriented scoring matrix are combined. The scoring model treats security, scalability, latency, computational/energy efficiency, and real-world applicability as ordinal evidence-synthesis dimensions rather than as measurements from a new experimental testbed. Under baseline weights, Hyperledger Fabric obtains the highest composite score, followed by Ripple, Ethereum, and Bitcoin; sensitivity analysis shows that the ranking is stable under the tested priority scenarios. The main contribution is therefore not a new blockchain taxonomy, but an evidence-to-decision framework that connects architecture, consensus, data placement, and application requirements while explicitly separating literature-derived evidence from experimental validation.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Kapil Dev Das
Department of Computer Science and Engineering
Dumkal Institute of Engineering and Technology
Murshidabad, West Bengal, India
Email: kapil.dev2009@gmail.com

1. INTRODUCTION

Digital services increasingly depend on data that must remain accurate, traceable, available, and selectively shareable across organizational boundaries. Conventional centralized repositories can simplify governance and performance management, but they also create concentrated trust and failure points. Blockchain and related distributed-ledger architectures address part of this problem through replicated state, cryptographic linkage, consensus, and auditable transaction histories [1]–[4]. Their suitability, however, depends strongly on the deployment model, consensus mechanism, workload, privacy requirements, and data-storage strategy. The literature has matured from foundational blockchain descriptions toward application-specific surveys. Studies of blockchain data management distinguish architecture, data structure, and storage-engine concerns [5], while surveys of blockchain applications emphasize the diversity of deployment contexts [6]–[8]. Healthcare and IoT research further shows that blockchain is often used as an integrity, authorization, or audit layer rather than as the repository for all sensitive payloads [9]–[18]. These findings make a simple platform-to-platform comparison insufficient for secure data management.

The original manuscript claimed a "novel multi-dimensional taxonomy," a "structured evaluation framework," and "quantitative comparative analysis." The reviewers correctly noted that the five-layer blockchain architecture and the dimensions of deployment, consensus, application, and data management are established in prior literature. The revised manuscript therefore narrows the novelty claim. Its contribution is an evidence-to-decision matrix that explicitly links five evaluation criteria to architectural layers and application requirements, and then converts literature-derived qualitative evidence into a reproducible ordinal scoring model. This reframing avoids presenting established blockchain concepts as new.

The study addresses four research questions (RQs): RQ1: Which blockchain architectural patterns and frameworks are most relevant to secure data management? RQ2: How do consensus and deployment choices affect security, performance, and efficiency? RQ3: Which recurring trade-offs limit real-world adoption? RQ4: How can evidence from heterogeneous studies be organized into a transparent decision model? The revised manuscript follows the IMRaD structure requested by IJEECS and explicitly connects each result to these questions.

2. PROPOSED EVIDENCE-TO-DECISION FRAMEWORK

The proposed framework should be interpreted as an analytical synthesis rather than a new blockchain protocol. It combines an established five-layer architecture with five decision criteria. The architecture layers are data, network, consensus, smart contract, and application. The decision criteria are security, scalability, latency, computational/energy efficiency, and real-world applicability. Figure 1 presents the architecture used as the structural backbone of the analysis.

Figure 2 shows how the five criteria are mapped to the architecture. Security is examined through integrity, confidentiality, availability, authorization, and attack resistance; scalability through throughput and growth in participants/workload; latency through confirmation or transaction-response delay; efficiency through computational and energy burden; and applicability through deployment fit, interoperability, governance, and domain constraints. This mapping is the main analytical addition of the revision.

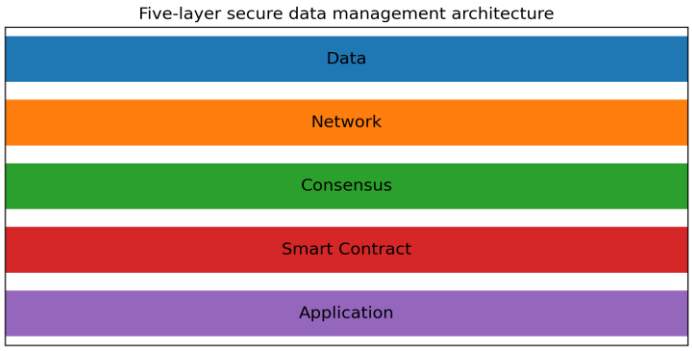

Figure 1. Five-layer architecture used to organize secure blockchain data-management evidence

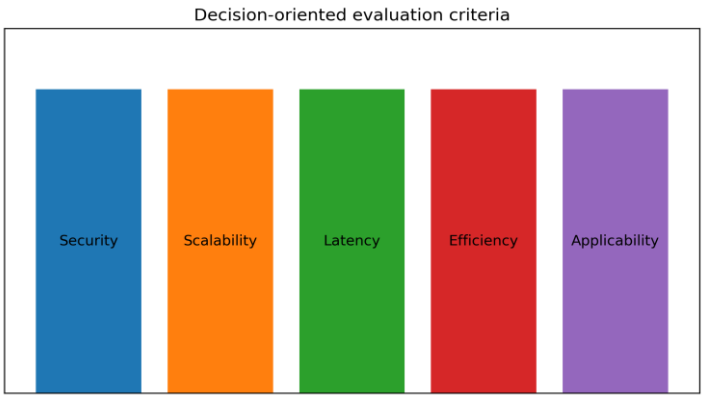

Figure 2. Decision-oriented evaluation criteria mapped to the secure data-management problem

Table 1. Architecture layers and evidence indicators used in the revised framework

Layer	Primary concern	Evidence indicators
Data	Integrity and placement	Hashing, encryption, on/off-chain design, auditability
Network	Communication and propagation	Peer connectivity, propagation overhead, interoperability
Consensus	Agreement and trust	PoW, PoS, PBFT/RPCA, fault tolerance, governance
Smart contract	Programmable control	Access control, automation, contract security
Application	Deployment fit	Healthcare, finance, IoT, supply chain, governance

3. METHOD

3.1. Review design and evidence scope

The study is a structured literature review with comparative evidence synthesis. The original manuscript searched IEEE Xplore, Springer, ScienceDirect, ACM Digital Library, and Google Scholar for literature published during 2019–2025 and reported 19 included peer-reviewed studies. The revision retains that stated scope but does not invent missing screening counts. In particular, the original search log did not record the number of retrieved records, duplicate removals, full-text exclusions, or reasons for each exclusion. Consequently, the revised manuscript reports these limitations explicitly instead of manufacturing a PRISMA flow count. PRISMA 2020 is used as a reporting benchmark [19]. The evidence base was expanded to 50 references for the revised discussion. The 50 references include peer-reviewed surveys, technical studies, application studies, and a small number of foundational or methodological sources. The additional literature strengthens the comparison of healthcare, IoT, supply-chain, privacy, consensus, interoperability, and data-management issues [6], [7], [8], [9]–[11], [13]–[17], [19]–[37].

Table 2. Review protocol and transparency statement

Item	Revised protocol
Databases	IEEE Xplore; Springer; ScienceDirect; ACM Digital Library; Google Scholar
Period	2019–2025 for the substantive review scope
Inclusion	Peer-reviewed work addressing blockchain architecture, secure data management, privacy, consensus, performance, or application evidence
Exclusion	Duplicates; non-peer-reviewed material; purely conceptual material without relevance to secure data management
Core review set	19 studies reported in the original manuscript
Revision evidence base	50 cited sources, including methodological and contextual literature
Synthesis type	Qualitative evidence extraction plus ordinal comparative scoring

3.2. Evidence extraction

For each platform or framework, evidence was organized under deployment type, consensus, data-management pattern, security properties, scalability, latency, efficiency, and application fit. The extraction deliberately distinguishes direct measurements reported by source studies from generalized platform characteristics. This distinction addresses the reviewers' concern that the previous manuscript presented heterogeneous secondary estimates as if they were measurements generated under a common benchmark. The revised comparison therefore does not claim that Bitcoin, Ethereum, Hyperledger Fabric, and Ripple were experimentally tested in the same environment. Instead, each platform receives an ordinal score from 1 (weak evidence/performance for the criterion) to 5 (strong evidence/performance for the criterion), based on the direction and consistency of the literature synthesis. The scoring is a decision-support device, not a statistical estimate.

3.3. Ordinal scoring model

Let p denote a platform and k denote one of five criteria. The platform score is defined as $S(p,k) \in \{1,2,3,4,5\}$. The composite score is calculated as: $C(p) = 0.25S_{security} + 0.25S_{scalability} + 0.20S_{latency} + 0.15S_{efficiency} + 0.15S_{applicability}$

The baseline weights sum to one and place slightly greater emphasis on security and scalability because the research problem concerns secure data management. No confidence interval is reported because the inputs are ordinal synthesis scores rather than repeated experimental observations. This directly addresses the reviewer's concern about presenting variability statistics for data that were not generated through a controlled benchmark.

The scores in Table 3 are deliberately conservative. Bitcoin is strong on security and maturity but is penalized for throughput, latency, and PoW energy burden. Ethereum receives stronger scores after its transition to PoS, while retaining application strength through smart contracts. Hyperledger Fabric scores strongly for enterprise data-management settings because permissioned membership, modular consensus, and

chaincode support align with controlled organizational workflows. Ripple scores strongly on transaction performance and efficiency but receives a lower security/applicability score than Fabric because its governance and application profile differ from a general enterprise data-management platform. These are synthesis judgments, not universal platform benchmarks [6], [24], [25], [38]–[43].

Table 3. Literature-derived ordinal scores and baseline composite scores

Platform	Security	Scalability	Latency	Efficiency	Applicability	Composite
Bitcoin	5	2	2	1	3	2.75
Ethereum	4	4	3	4	5	3.95
Hyperledger Fabric	4	5	5	5	5	4.75
Ripple	3	5	5	5	4	4.35

4. RESULTS AND DISCUSSION

4.1. RQ1: Architectural patterns relevant to secure data management

The literature indicates that secure data management is commonly implemented through combinations of on-chain integrity records, off-chain payload storage, access-control mechanisms, and application-specific smart contracts. Blockchain data-management surveys emphasize that the ledger architecture and storage engine are separate design dimensions [5]. Blockchain–cloud integration studies similarly show that off-chain storage can reduce ledger storage pressure while retaining integrity and auditability through hashes or references [44]. Healthcare surveys repeatedly identify permissioned or hybrid architectures as practical choices where privacy and governance are stronger requirements than open participation [9], [10], [14], [15], [17], [45], [46]. IoT literature adds another constraint: resource-limited devices cannot always execute heavyweight consensus or store complete ledgers. Consequently, lightweight, hierarchical, permissioned, or hybrid designs are repeatedly proposed [11], [13], [20]–[23], [26], [41]. The architectural implication is that "blockchain" should not be treated as one homogeneous technology. Secure data management is better modeled as a stack in which storage, network, consensus, programmable control, and application governance can be varied independently.

4.2. RQ2: Consensus, security, performance, and efficiency

Consensus is a major source of the observed trade-offs. PoW provides strong Sybil resistance in open settings but imposes substantial computational work and can limit throughput. PoS reduces the energy burden associated with mining but introduces stake-based governance and security assumptions. PBFT-family mechanisms can provide low-latency agreement in permissioned networks when the participating validator set is controlled. Consensus surveys consistently classify these mechanisms according to fault model, communication pattern, finality, energy demand, and governance assumptions [24], [25], [42]. The revised analysis also avoids treating consensus as the sole determinant of performance. Network topology, block size, transaction workload, smart-contract execution, storage design, and hardware all influence observed latency and throughput. Studies of IoT and healthcare applications show that application architecture and data-sharing mechanisms can dominate practical performance constraints [11], [13], [16]–[18], [20]–[23], [27], [28].

4.3. RQ3: Comparative evidence and ranking

Table 3 provides the baseline evidence synthesis. Figure 3 visualizes the composite scores and makes the ranking explicit. Hyperledger Fabric leads with 4.75, followed by Ripple at 4.35, Ethereum at 3.95, and Bitcoin at 2.75. The result should not be interpreted as "the best blockchain" in general. It means that, under the stated criteria and equalized ordinal evidence model, Fabric best fits the secure enterprise data-management problem represented by this review. The ranking is consistent with the qualitative evidence: permissioned enterprise architectures benefit when governance, controlled membership, lower latency, and data-management integration are important. Public networks remain valuable where open participation, censorship resistance, and broad ecosystem effects are primary requirements. Ethereum occupies an intermediate position because smart-contract programmability and ecosystem maturity improve applicability, while performance and governance depend on the deployment context [5], [38]–[44].

4.4. RQ4: Sensitivity analysis and decision implications

To test whether the conclusion depends entirely on the baseline weights, two alternative scenarios were evaluated. A security-priority scenario increases the security weight to 0.40, while a performance-priority scenario assigns 0.30 to scalability and 0.25 to latency. Figure 4 shows that the relative ordering

remains unchanged in the tested scenarios: Fabric ranks first, Ripple second, Ethereum third, and Bitcoin fourth. The stability of the ranking is useful because it indicates that the result is not caused by a single arbitrary weight choice, although broader weight elicitation with domain experts would be a valuable future study.

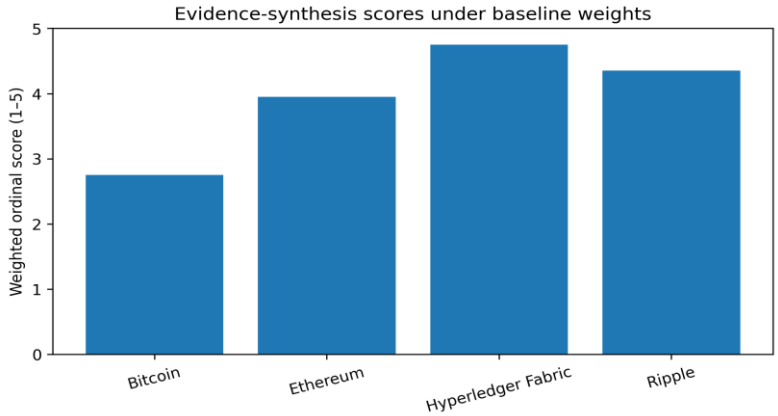

Figure 3. Baseline composite scores derived from the ordinal evidence-synthesis model

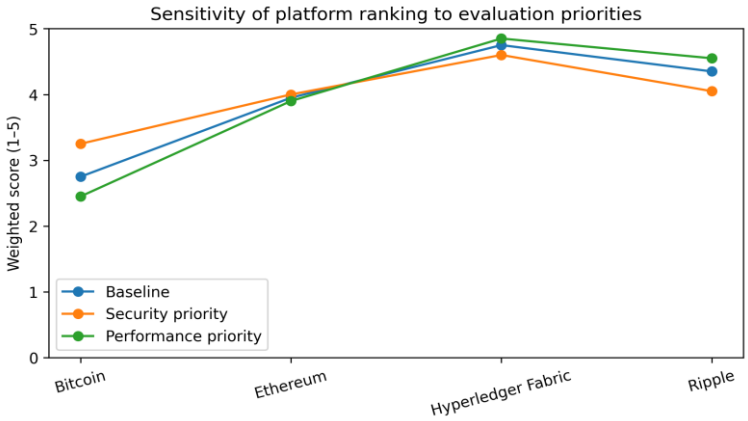

Figure 4. Sensitivity of platform ranking to security- and performance-priority weighting

4.5. Comparison with existing literature

The revised contribution is best understood relative to prior surveys. Casino *et al.* [6] and related surveys classify blockchain applications broadly, while Wei *et al.* [5] focus specifically on blockchain data-management systems. Consensus-focused reviews compare agreement mechanisms [24], [25], while IoT surveys concentrate on security, privacy, resource constraints, and access control [11], [13], [20]–[23]. Healthcare surveys similarly emphasize privacy, authorization, interoperability, and secure sharing [9], [10], [14]–[18], [27], [36]. The distinction of the present review is the explicit bridge between these evidence streams. Instead of proposing another taxonomy of blockchain types, the revised framework maps architecture layers to decision criteria and then produces a reproducible ordinal score. This makes the framework more useful for architecture selection while remaining honest about the fact that the underlying evidence is heterogeneous. In other words, the contribution is synthesis and decision structure, not a new blockchain protocol, consensus algorithm, or taxonomy.

4.6. Applications, challenges, and research gaps

Healthcare is a strong example of why architecture selection matters. Secure sharing studies emphasize access control, privacy preservation, authentication, and interoperability [9], [10], [15]–[18], [27], [28], [36]. For such applications, a hybrid pattern in which sensitive payloads remain in controlled storage while hashes, consent events, or audit references are anchored on a permissioned ledger can reduce privacy and storage risks. IoT introduces additional resource constraints, motivating lightweight consensus,

hierarchical organization, and distributed access-control approaches [11], [13], [20]–[23], [26]. Supply-chain applications emphasize provenance and traceability but also face interoperability and governance challenges [29], [30], [43]. The evidence also exposes recurring limitations. First, performance values reported across studies are difficult to compare because testbeds, node counts, workloads, transaction sizes, and network conditions differ. Second, security is multidimensional and cannot be represented by one universal score. Third, permissioned systems trade openness for governance and efficiency. Fourth, smart contracts introduce their own software-security risks. Fifth, interoperability across chains remains an open technical problem [28], [29]. Finally, privacy-preserving mechanisms must be evaluated alongside regulatory and operational requirements rather than as isolated cryptographic components [14]–[18], [27], [45], [46]. These gaps motivate four research directions: standardized cross-platform benchmarks; reproducible evidence repositories for blockchain performance; hybrid on/off-chain architectures with verifiable privacy controls; and AI-assisted or lightweight consensus optimization. Recent work on quantum threats further suggests that long-lived blockchain data-management systems should consider cryptographic agility and post-quantum migration planning [31].

4.7. Positioning against representative prior studies

Table 4 makes the revised contribution explicit by comparing the principal analytical emphasis of representative prior work with the decision structure used here. Broad application surveys provide taxonomy and status mapping [6]–[8]; blockchain data-management surveys examine storage and ledger architecture [5]; consensus surveys analyze agreement mechanisms [24], [25]; and domain-specific surveys focus on healthcare, IoT, privacy, or secure sharing [9]–[11], [13]–[18], [20]–[23], [27], [28], [36], [37]. These studies are complementary rather than interchangeable. The present framework connects their evidence dimensions to a common architecture-selection problem.

Table 4. Comparing representative early works

Literature emphasis	Representative refs.	Main value	Gap addressed here
Blockchain applications	[6]–[8]	Broad classification of use cases	Does not directly produce a secure-data-management decision score
Blockchain data management	[5], [44]	Architecture, storage, cloud integration	Limited cross-platform decision matrix
Consensus mechanisms	[24], [25]	Security/performance trade-offs	Consensus not connected to application/data-placement criteria
IoT security and privacy	[11], [13], [20]–[23], [26]	Resource constraints, attacks, access control	Domain-specific rather than cross-domain platform selection
Healthcare data security	[9], [10], [37], [14]–[18], [27], [28], [36]	Privacy, access, sharing, interoperability	Strong domain evidence but not a general platform-ranking model
Current secure data-sharing work	[32], [45]–[49]	Recent frameworks and systematic reviews	Evidence is heterogeneous; need explicit evidence-to-decision mapping
Revised framework	This study	Architecture-to-criteria mapping + ordinal synthesis	Separates literature synthesis from experimental benchmarking

4.8. Data placement and privacy implications

A central implication of the reviewed evidence is that "secure data management on blockchain" does not require storing every data object on-chain. Healthcare and IoT studies repeatedly use blockchain to record hashes, consent events, authorization decisions, metadata, or transaction proofs while retaining sensitive or high-volume payloads in controlled off-chain repositories [5], [9], [10], [14]–[18], [27], [28], [36], [44]. This architecture reduces ledger growth and limits direct exposure of sensitive content. However, it also introduces dependency on the availability, integrity, and governance of the off-chain repository. Therefore, the data layer in Figure 1 should be interpreted as a placement decision rather than a requirement for complete on-chain storage.

Privacy is also not equivalent to immutability. A ledger can make unauthorized modification difficult while still revealing transaction metadata, identities, access patterns, or permanently retained references. Privacy-preserving healthcare studies therefore combine blockchain with encryption, attribute-based access control, proxy re-encryption, or other mechanisms [13], [15], [16], [22], [27], [45], [46]. The revised framework consequently treats confidentiality and privacy as evidence dimensions within security, rather than assuming that blockchain itself provides privacy.

4.9. Why a common benchmark is still required

The ordinal scoring model is useful for synthesis but cannot replace controlled benchmarking. A rigorous experimental validation should define the same hardware, software versions, node count, transaction

size, workload distribution, network bandwidth, fault model, and measurement interval for every platform. Throughput should be reported with repeated trials; latency should distinguish submission, confirmation, and finality; energy should be measured using a consistent boundary; and security should be evaluated against an explicit threat model. Without these controls, a numerical TPS value taken from one study cannot be directly compared with a value obtained from another study under different conditions. This limitation explains the deliberate terminology used in the revised paper: "ordinal evidence-synthesis score" rather than "measured performance." The distinction is important for scientific reproducibility and directly responds to the reviewer's concern that the earlier manuscript presented secondary estimates without sufficient experimental normalization.

4.10. Threats to validity

Four threats to validity remain. First, publication and database bias may exclude relevant studies not indexed in the selected sources. Second, the original review did not preserve complete search and screening logs, limiting retrospective reproduction of the 19-study core set. Third, ordinal scoring necessarily introduces researcher judgment, even when the scoring rules are stated in advance. Fourth, platform software and consensus mechanisms evolve; therefore, a platform ranking should not be interpreted as permanent. These limitations are not hidden in the revised manuscript and should guide future validation.

Despite these limitations, the revised framework improves transparency in three ways: it states exactly what the score represents, it separates evidence synthesis from experimental measurement, and it shows how alternative weights affect the ranking. This is a more defensible contribution than the original claim of a novel taxonomy.

5. CONCLUSION

This revised review addresses the central concerns raised by the reviewers by narrowing the novelty claim, strengthening the literature base, clarifying the review protocol, introducing a formal ordinal scoring model, linking results to the research questions, and adding explicit sensitivity analysis. The analysis shows that blockchain platform choice is a context-dependent decision rather than a universal ranking problem. Under the criteria and weights defined here, Hyperledger Fabric provides the strongest overall fit for secure enterprise data management, while Ethereum, Ripple, and Bitcoin offer different trade-offs that can be preferable under alternative requirements.

The most important methodological qualification is that the comparative scores synthesize published evidence; they are not results from a common experimental benchmark. This limitation is retained explicitly to avoid overstating the contribution. Future work should validate the decision matrix through controlled experiments using common hardware, workloads, transaction sizes, network conditions, and repeated trials. A larger systematic review with preserved database export files and complete PRISMA counts would also strengthen reproducibility.

ACKNOWLEDGMENTS

The authors thank the faculty members of the Department of Computer Science and Engineering, Dumkal Institute of Engineering and Technology, for academic support and guidance.

FUNDING INFORMATION

The authors state that no funding was involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Kapil Dev Das	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The author declares no conflict of interest.

INFORMED CONSENT

Informed consent is not applicable because this study does not involve human participants or identifiable personal data.

ETHICAL APPROVAL

Ethical approval is not applicable because this study is based on published literature and does not involve human or animal subjects.

DATA AVAILABILITY

Data availability is not applicable to this review because no new experimental dataset was created. The evidence sources are identified in the reference list. The ordinal scoring matrix reported in Table 3 is derived from the literature synthesis described in the Method section.

REFERENCES

[1] N. Nahar, K. Andersson, O. Schelen, and S. Saguna, "A Survey on Zero Trust Architecture: Applications and Challenges of 6G Networks," *IEEE Access*, vol. 12, pp. 94753–94764, 2024, doi: 10.1109/ACCESS.2024.3425350.

[2] C. D. Morar and D. E. Popescu, "A Survey of Blockchain Applicability, Challenges, and Key Threats," *Computers*, vol. 13, no. 9, p. 223, Sep. 2024, doi: 10.3390/computers13090223.

[3] A. K. Ranjan and P. Kumar, "A survey on blockchain-based privacy preserving techniques for edge internet of things," *Int. J. Comput. Appl.*, vol. 47, no. 6, pp. 497–508, Jun. 2025, doi: 10.1080/1206212X.2025.2498687.

[4] N. Y. Al-Matari, A. T. Zahary, and A. A. Al-Shargabi, "A survey on advancements in blockchain-enabled spectrum access security for 6G cognitive radio IoT networks," *Sci. Rep.*, vol. 14, no. 1, p. 30990, Dec. 2024, doi: 10.1038/s41598-024-82126-y.

[5] Q. Wei, B. Li, W. Chang, Z. Jia, Z. Shen, and Z. Shao, "A Survey of Blockchain Data Management Systems," *ACM Trans. Embed. Comput. Syst.*, vol. 21, no. 3, pp. 1–28, May 2022, doi: 10.1145/3502741.

[6] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telemat. Informatics*, vol. 36, pp. 55–81, Mar. 2019, doi: 10.1016/j.tele.2018.11.006.

[7] C. Choudhary, I. Singh, and M. Shafiq, "Blockchain for IoT Security and Privacy: Challenges, Application Areas and Implementation Issues," in *Cross-Industry Blockchain Technology: Opportunities and Challenges in Industry 4.0*, BENTHAM SCIENCE PUBLISHERS, 2022, pp. 1–17. doi: 10.2174/9789815051452122010003.

[8] D. Sukheja, L. Indira, P. Sharma, and S. Chirgaiya, "Blockchain Technology: A Comprehensive Survey," *J. Adv. Res. Dyn. Control Syst.*, vol. 11, no. 0009-SPECIAL ISSUE, pp. 1187–1203, Sep. 2019, doi: 10.5373/JARDCS/V11/20192690.

[9] A. Saha, R. Amin, S. Kunal, S. Vollala, and S. K. Dwivedi, "Review on 'Blockchain technology based medical healthcare system with privacy issues,'" *Secur. Priv.*, vol. 2, no. 5, Sep. 2019, doi: 10.1002/spy2.83.

[10] E. A. Shammar, A. T. Zahary, and A. A. Al-Shargabi, "A Survey of IoT and Blockchain Integration: Security Perspective," *IEEE Access*, vol. 9, pp. 156114–156150, 2021, doi: 10.1109/ACCESS.2021.3129697.

[11] H. D. Zubaydi, P. Varga, and S. Molnár, "Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review," *Sensors*, vol. 23, no. 2, p. 788, Jan. 2023, doi: 10.3390/s23020788.

[12] S. Singh, S. Rathore, O. Alfarraj, A. Tolba, and B. Yoon, "A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology," *Futur. Gener. Comput. Syst.*, vol. 129, pp. 380–388, Apr. 2022, doi: 10.1016/j.future.2021.11.028.

[13] I. Butun and P. Osterberg, "A Review of Distributed Access Control for Blockchain Systems Towards Securing the Internet of Things," *IEEE Access*, vol. 9, pp. 5428–5441, 2021, doi: 10.1109/ACCESS.2020.3047902.

[14] K. Singh, C. Krishna, and D. Kumar, "Professional Ethics, Challenges and Opportunities for Blockchain Technology in Healthcare Sector: A Systematic Review," *Recent Adv. Comput. Sci. Commun.*, vol. 17, no. 1, Jan. 2024, doi: 10.2174/0126662558263462231020111428.

[15] A. Bisht, A. K. Das, and D. Giri, "Personal health record storage and sharing using searchable encryption and blockchain: A comprehensive survey," *Secur. Priv.*, vol. 7, no. 2, Mar. 2024, doi: 10.1002/spy2.351.

[16] M. Qi, Z. Wang, Q.-L. Han, J. Zhang, S. Chen, and Y. Xiang, "Privacy Protection for Blockchain-Based Healthcare IoT Systems: A Survey," *IEEE/CAA J. Autom. Sin.*, vol. 11, no. 8, pp. 1757–1776, Aug. 2024, doi: 10.1109/JAS.2022.106058.

[17] D. Zhao and T. Li, "Distributed Cross-Blockchain Transactions," Feb. 2020, doi: 10.48550/arXiv.2002.11771.

[18] X. Wang, O. T. Tawose, F. Yan, and D. Zhao, "Distributed Nonblocking Commit Protocols for Many-Party Cross-Blockchain Transactions," Jan. 2020, [Online]. Available: http://arxiv.org/abs/2001.01174

[19] M. J. Page *et al.*, "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *BMJ*, p. n71, Mar. 2021, doi: 10.1136/bmj.n71.

[20] S. Singh, A. S. M. S. Hosen, and B. Yoon, "Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network," *IEEE Access*, vol. 9, pp. 13938–13959, 2021, doi: 10.1109/ACCESS.2021.3051602.

[21] K. Carvalho and J. Granjal, "Security and Privacy for Mobile IoT Applications Using Blockchain," *Sensors*, vol. 21, no. 17, p. 5931, Sep. 2021, doi: 10.3390/s21175931.

[22] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, "A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT," *IEEE Access*, vol. 7, pp. 38431–38441, 2019, doi: 10.1109/ACCESS.2019.2905846.

[23] S. Kaur, S. Chaturvedi, A. Sharma, and J. Kar, "A Research Survey on Applications of Consensus Protocols in Blockchain," *Secur. Commun. Networks*, vol. 2021, pp. 1–22, Jan. 2021, doi: 10.1155/2021/6693731.

[24] M. Xie, J. Liu, S. Chen, and M. Lin, "A survey on blockchain consensus mechanism: research overview, current advances and future directions," *Int. J. Intell. Comput. Cybern.*, vol. 16, no. 2, pp. 314–340, May 2023, doi: 10.1108/IJICC-05-2022-0126.
[25] M. Conoscenti, A. Vetrò, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," *IEEE Internet Things J.*, 2017.
[26] H. Saeed *et al.*, "Blockchain technology in healthcare: A systematic review," *PLoS One*, vol. 17, no. 4, p. e0266462, Apr. 2022, doi: 10.1371/journal.pone.0266462.
[27] D. Chawla, S. Kumari, R. S. Rathore, P. S. Mehra, A. K. Das, and N. Kumar, "Quantum Blockchain for Internet of Things: A systematic review, proposed solutions and challenges," *Comput. Electr. Eng.*, vol. 126, p. 110524, Aug. 2025, doi: 10.1016/j.compeleceng.2025.110524.
[28] Y. Lu, "The blockchain: State-of-the-art and research challenges," *J. Ind. Inf. Integr.*, vol. 15, pp. 80–90, Sep. 2019, doi: 10.1016/j.jii.2019.04.002.
[29] M. M. Queiroz, R. Telles, and S. H. Bonilla, "Blockchain and supply chain management integration: a systematic review of the literature," *Supply Chain Manag. An Int. J.*, vol. 25, no. 2, pp. 241–254, Aug. 2019, doi: 10.1108/SCM-03-2018-0143.
[30] G. Perboli, S. Musso, and M. Rosano, "Blockchain in Logistics and Supply Chain: A Lean Approach for Designing Real-World Use Cases," *IEEE Access*, vol. 6, pp. 62018–62028, 2018, doi: 10.1109/ACCESS.2018.2875782.
[31] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and Open Research Challenges," *IEEE Access*, vol. 7, pp. 10127–10149, 2019, doi: 10.1109/ACCESS.2018.2890507.
[32] H. R. Hasan and K. Salah, "Blockchain-Based Proof of Delivery of Physical Assets With Single and Multiple Transporters," *IEEE Access*, vol. 6, pp. 46781–46793, 2018, doi: 10.1109/ACCESS.2018.2866512.
[33] F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 3, pp. 2084–2123, 2016, doi: 10.1109/COMST.2016.2535718.
[34] U. Ullah Tariq *et al.*, "Blockchain-Based Secured Data Sharing in Healthcare: A Systematic Literature Review," *IEEE Access*, vol. 13, pp. 45415–45435, 2025, doi: 10.1109/ACCESS.2025.3547953.
[35] T. Li, J. Zhang, Y. Lin, S. Zhang, and J. Ma, "Blockchain-Based Fine-Grained Data Sharing for Multiple Groups in Internet of Things," *Secur. Commun. Networks*, vol. 2021, pp. 1–13, Feb. 2021, doi: 10.1155/2021/6689448.
[36] Y. Chen, L. Meng, H. Zhou, and G. Xue, "A Blockchain-Based Medical Data Sharing Mechanism with Attribute-Based Access Control and Privacy Protection," *Wirel. Commun. Mob. Comput.*, vol. 2021, no. 1, pp. 1–13, Jan. 2021, doi: 10.1155/2021/6685762.
[37] S. K. Sharma and F. Parwej, "Design and Implementation of a Blockchain-Based Secure Data Sharing Framework to Enhance the Healthcare System," *Blockchains*, vol. 3, no. 3, p. 10, Aug. 2025, doi: 10.3390/blockchains3030010.
[38] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
[39] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.
[40] W. F, Yuan Y, "Blockchain: The state of the art and future trends," *Acta Autom. Sin.*, vol. 42, no. 4, pp. 481–494, 2017.
[41] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and solutions," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2171–2182, 2019, doi: 10.1109/JIOT.2018.2875185.
[42] W. Viriyasitavat and D. Hoonsopon, "Blockchain characteristics and consensus in modern business processes," *J. Ind. Inf. Integr.*, vol. 13, pp. 32–39, Mar. 2019, doi: 10.1016/j.jii.2018.07.004.
[43] H. Treiblmaier, "The impact of the blockchain on the supply chain: A theory-based research framework," *Supply Chain Manag.*, vol. 23, no. 6, pp. 545–559, 2018, doi: 10.1108/SCM.01.2018.0049.
[44] A. Khanna, A. Sah, V. Bolshev, A. Burgio, V. Panchenko, and M. Jasiński, "Blockchain–Cloud Integration: A Survey," *Sensors*, vol. 22, no. 14, p. 5238, Jul. 2022, doi: 10.3390/s22145238.
[45] A. M. Tawfik, A. Al-Ahwal, A. S. T. Eldien, and H. H. Zayed, "Blockchain-based access control and privacy preservation in healthcare: a comprehensive survey," *Cluster Comput.*, vol. 28, no. 8, p. 529, Sep. 2025, doi: 10.1007/s10586-025-05308-x.
[46] M. P. Benchis, "Comparative analysis of blockchain adoption in the public and private sectors: A technology-organization-environment (TOE) framework approach," *J. Innov. Knowl.*, 2025, doi: 10.1016/j.jik.2025.100009.
[47] O. Zorlu and A. Ozsoy, "A blockchain-based secure framework for data management," *IET Commun.*, vol. 18, no. 10, pp. 628–653, Jun. 2024, doi: 10.1049/cmu2.12781.
[48] K. Sabiri, F. Sousa, and T. Rocha, "A systematic review of privacy-preserving blockchain applications in healthcare," *Multimed. Tools Appl.*, vol. 84, no. 32, pp. 39925–39980, Mar. 2025, doi: 10.1007/s11042-024-20541-z.
[49] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, "Blockchain Technology in Healthcare: A Systematic Review," *Healthcare*, vol. 7, no. 2, p. 56, Apr. 2019, doi: 10.3390/healthcare7020056.

BIOGRAPHIES OF AUTHORS



Kapil Dev Das received the B.Tech. degree in Information Technology from IMPS College of Engineering and Technology, Malda, India, and the M.Tech./M.E. degree in Information Technology from IIEST Shibpur, India. His research interests include blockchain, cybersecurity, secure data management, artificial intelligence, and distributed systems. He has academic experience in computer science and engineering education and has worked on research involving blockchain-based security and data-management applications. He is the author of the present study and can be contacted at kapil.dev2009@gmail.com.