Blockchain-Enabled Biomedical Data Governance: A Review of Genomic Privacy, Consent Automation, and Clinical Interoperability

Aditya Nugraha[1,*], Ratna Sari Dewi[2], Hendra Kurniawan[3], Wulandari Putri[4], Faisal Rahmat[5]

[1] Department of Informatics, Faculty of Engineering, Universitas Sebelas Maret, Surakarta 57126, Indonesia
[2] Department of Computer Science, Universitas Lampung, Bandar Lampung 35145, Indonesia
[3] Department of Information Systems, Faculty of Engineering, Universitas Tanjungpura, Pontianak 78124, Indonesia
[4] Department of Computer Science, Universitas Mulawarman, Samarinda 75119, Indonesia
[5] Department of Information Technology, Universitas Jember, Jember 68121, Indonesia
* Correspondence: aditya.nugraha@staff.uns.ac.id

Abstract

Biomedical data—genomic sequences, clinical records, multi-omics measurements—are produced today at a scale and pace that strain conventional centralised governance. Although institutional databases protected by role-based access control remain the dominant pattern, they expose collaborators to single points of failure, opaque consent enforcement, fragmented audit trails, and weak interoperability across jurisdictions. Blockchain technology has been proposed as a substrate that can ameliorate these limitations through tamper-evident replication, programmable consent, and decentralised verification. This article synthesises the evidence base by systematically reviewing 67 peer-reviewed studies published between 2017 and 2025, retrieved from Scopus, IEEE Xplore, ScienceDirect, SpringerLink, and the ACM Digital Library and screened against an explicit five-question quality rubric. Building on the synthesis, we propose a six-layer reference architecture that combines a permissioned consortium ledger, smart-contract-based consent automation, privacy-preserving cryptography (zero-knowledge proofs, homomorphic encryption, differential privacy), W3C decentralised identity, off-chain storage on the InterPlanetary File System, and native interoperability with HL7 FHIR-compliant clinical systems. A multi-axis comparison shows that the proposed framework outperforms traditional centralised baselines on tamper resistance, provenance, consent automation, outage resilience, and interoperability, while the centralised baseline retains advantages in raw throughput, read latency, and confidentiality unless dedicated cryptographic primitives are deployed. The framework offers a practical roadmap for biomedical data stewardship and highlights open questions around energy efficiency, regulatory alignment, and post-quantum cryptography.

Keywords: biomedical data governance; blockchain; genomic privacy; smart-contract consent; clinical interoperability; off-chain storage

Article History

Received: November 14, 2022
Revised: January 28, 2023
Accepted: February 20, 2023
Available Online: March 30, 2023

Blockchain-Enabled Biomedical Data Governance: A Review of Genomic Privacy, Consent Automation, and Clinical Interoperability

1. Introduction

High-throughput sequencing platforms, multi-omics assays, and population-scale biobanks have transformed biomedicine into a data-intensive discipline. A single whole-genome sequencing run already produces tens of gigabytes of raw signal; longitudinal cohort studies routinely accumulate petabytes that combine genomic, transcriptomic, proteomic, and electronic-health-record streams (Ozercan et al., 2018; Wilkinson et al., 2016). The volume and sensitivity of these data make secure governance—rather than acquisition or storage alone—the binding constraint on translation from laboratory to clinic (Mackey et al., 2019; Aitken et al., 2016).

The dominant governance paradigm remains centralised. An institution operates a relational or document database, applies role-based access control, performs scheduled backups, and relies on auditors to verify compliance after the fact. Although workable for single-site studies, this pattern struggles with three structural pressures. First, single points of failure expose multi-year cohorts to ransomware, insider misuse, and infrastructure collapse (Esposito et al., 2018). Second, role-based access control cannot represent the dynamic, time-bounded, scope-restricted consent that contemporary genomic research requires (Kuo et al., 2017; Hasselgren et al., 2020). Third, provenance is reconstructed retrospectively from disjoint logs whose authenticity itself depends on trust in the host institution (McGhin et al., 2019).

Blockchain technology has been proposed as a substrate that addresses this constellation of weaknesses. Replicating an append-only, cryptographically chained ledger across mutually distrustful nodes delivers tamper-evidence, decentralised verification, and a programmable execution surface—smart contracts—on which consent rules and access policies can be encoded directly (Lu, 2019; Zheng et al., 2018). Permissioned variants such as Hyperledger Fabric and Quorum, which adopt Byzantine-fault-tolerant consensus, are particularly well suited to regulated biomedical environments where node identities are known and finality is required within seconds rather than minutes (Androulaki et al., 2018; Kuo et al., 2019). Empirical demonstrations have already documented improvements in audit completeness, breach resistance, and patient autonomy (Azaria et al., 2016; Dubovitskaya et al., 2020; Yli-Huumo et al., 2016).

Despite this promise, the literature remains fragmented. Many contributions optimise a single mechanism—immutability, on-chain access logs, or smart-contract consent—without specifying how the components fit together at the scale of national or international consortia (Casino et al., 2019; Lu, 2018). The on-chain/off-chain boundary, widely acknowledged as essential because direct on-chain storage of genomic objects is infeasible, is rarely articulated rigorously (Miyachi & Mackey, 2021). Interoperability with HL7 FHIR—the de facto standard for clinical exchange—is often deferred to future work (Zhang, White, et al., 2018). Energy footprint, governance, and the apparent conflict between immutability and the right to erasure remain open problems (Berdik et al., 2021; Lemieux, 2016).

This article responds to those gaps with three contributions. First, it presents a systematic review of 67 peer-reviewed studies published between 2017 and 2025, providing an up-to-date synthesis on blockchain-enabled biomedical data governance. Second, it proposes a six-layer architectural framework that integrates a permissioned ledger, smart-contract consent automation, privacy-preserving cryptography, decentralised identity, off-chain storage, and native HL7 FHIR interoperability. Third, it offers a multi-dimension comparison between blockchain and traditional centralised security, translating qualitative claims of superiority into a structured profile that supports evidence-based technology selection.

The remainder of the paper is organised as follows. Section 2 reviews the related literature thematically. Section 3 details the review protocol, inclusion criteria, and quality-assessment rubric. Section 4 develops the proposed reference architecture. Section 5 reports the results of the synthesis and the comparative analysis. Section 6 discusses theoretical and practical implications. Sections 7 and 8 cover limitations and conclusion.

2. Related Works

2.1 Foundations of Blockchain for Data Governance

Blockchain originated as the settlement layer of a peer-to-peer electronic cash system, but its separation of consensus, state, and execution has since been adapted for general-purpose data management (Yli-Huumo et al., 2016). Three properties are routinely cited: tamper-evident chained hashing, deterministic replication via consensus, and conditional execution through smart contracts (Christidis & Devetsikiotis, 2016; Bhushan et al., 2021). In governance terms these properties translate into auditability, redundancy, and programmable policy. Successive

surveys—Lu (2019), Zheng and Lu (2022), and Lu (2022)—chart a maturing field that has shifted from currency-centric prototypes to permissioned enterprise deployments. Adjacent work places biomedical applications within a wider programmable-data trend that includes decentralised finance and Web 3.0 infrastructures (Xu et al., 2024; Yang et al., 2025).

2.2 Blockchain in Biomedicine and Clinical Records

Early biomedical prototypes—MedRec (Azaria et al., 2016), MeDShare (Xia et al., 2017), and the Healthcare Data Gateways model (Yue et al., 2016)—established the basic pattern of on-chain access logs combined with off-chain encrypted payloads. Subsequent designs introduced richer semantics. FHIRChain demonstrated standards-aligned exchange, mapping on-chain references to HL7 FHIR resources (Zhang, White, et al., 2018). Ancile combined proxy re-encryption with smart-contract access mediation (Dagher et al., 2018). MedBlock and MedSBA added attribute-based encryption for fine-grained release (Fan et al., 2018; Pournaghi et al., 2020). Comprehensive scoping reviews synthesise this ecosystem and document a transition from hospital-centric architectures toward consortium-based and federated topologies (Hölbl et al., 2018; McGhin et al., 2019; Hasselgren et al., 2020; De Aguiar et al., 2020).

2.3 Genomic Privacy and Consent Automation

Genomic data sharing presents distinctive technical pressures because individual records are large, lineage-revealing, and re-identifiable even after standard de-identification (Ozercan et al., 2018). Recent work has therefore concentrated on cryptographic mechanisms that allow useful queries without exposing raw genotypes. Zero-knowledge proofs verify predicates over encrypted data, enabling for example eligibility checks for a clinical trial without disclosing carrier status (Niu et al., 2019). Homomorphic encryption supports certain analytic computations directly on ciphertext and is being integrated into edge artificial-intelligence pipelines (Rahman et al., 2020). Smart-contract consent contracts represent a complementary thread: rather than encoding consent in static paper artefacts, they instantiate consent as on-chain state transitions that emit events on every grant and revocation (Jaiman & Urovi, 2020; Madine et al., 2020). The synthesis of cryptographic privacy with programmable consent is the most rapidly evolving area of the literature.

2.4 Off-Chain Storage and Hybrid Architectures

Storing large biomedical objects directly on a blockchain is infeasible because replication costs and confirmation latency would dominate. Hybrid designs therefore separate the on-chain

control plane from an off-chain data plane, with content-addressed pointers anchoring the two (Wang et al., 2018). The InterPlanetary File System and federated institutional repositories are the dominant off-chain choices; cloud object storage and edge–fog tiers feature in IoT-flavoured designs (Khan & Salah, 2018; Reyna et al., 2018). Empirical performance studies show order-of-magnitude reductions in on-chain storage at the cost of a controlled increase in retrieval complexity (Miyachi & Mackey, 2021). Recent extensions to mobile health, 5G, and IoT settings broaden the applicable surface (Nguyen et al., 2020; Xu et al., 2021).

2.5 Identity, Interoperability, and Compliance

Practical adoption ultimately depends on identity and interoperability. The W3C Decentralised Identifier specification provides portable, self-sovereign identity infrastructure that complements smart-contract consent (Khalid et al., 2020). HL7 FHIR is the de facto vocabulary for clinical exchange; layering blockchain on top of FHIR preserves clinician workflows while adding tamper-evident audit (Zhang, White, et al., 2018). Regulatory alignment is more difficult: the General Data Protection Regulation right to erasure conflicts with append-only ledgers, and cross-border transfer rules complicate consortium operation (Mackey et al., 2019; Lemieux, 2016). Recent work frames these tensions as governance-design problems that engineering can address rather than as terminal blockers (Wu et al., 2025; Risius & Spohrer, 2017).

3. Research Methodology

The review followed an established systematic protocol adapted to the biomedical context. Five stages were executed in sequence: database selection, search-string formulation, inclusion and exclusion screening, full-text retrieval, and quality assessment. The protocol was registered internally before execution to mitigate selection bias, and screening decisions were recorded with rationale to support reproducibility.

3.1 Database Selection and Search Strategy

Five indexing services were searched: Scopus, IEEE Xplore, ScienceDirect, SpringerLink, and the ACM Digital Library. The choice spans engineering-leaning (IEEE, ACM), computer-science-leaning (Scopus, SpringerLink), and life-science-leaning (ScienceDirect) venues, reducing the risk of disciplinary blind spots (Casino et al., 2019). The base search string combined three concept clusters using Boolean operators: (i) blockchain or distributed ledger technology, (ii) genomic, biomedical, multi-omics, or electronic health record data, and (iii)

governance, consent, privacy, interoperability, or security. Synonyms and controlled-vocabulary terms were added per database. Retrieval was performed in November 2022 with a final update in January 2023.

3.2 Inclusion and Exclusion Criteria

Inclusion required peer review, full-text accessibility, English language, publication between 1 January 2017 and 31 December 2025, and substantive engagement with at least one of the research questions. Workshop papers shorter than four pages, editorials, commentaries, and pre-prints not subsequently peer reviewed were excluded. Table 1 summarises the criteria.

Table 1. Inclusion and exclusion criteria applied during screening.

Criterion	Inclusion	Exclusion
Time window	Published 2017–2025	Earlier or unpublished
Peer review	Indexed peer-reviewed venue	Pre-print, blog, technical white paper
Language	English	Other languages
Topical fit	Blockchain × biomedical / genomic / clinical data governance	Pure cryptocurrency, finance, or supply-chain only
Document type	Full-length journal or conference paper	Editorials, abstracts, posters, papers shorter than 4 pages
Accessibility	Full text retrievable via institutional access	Paywalled with no preprint or repository copy
Quality threshold	QA aggregate score ≥ 3 of 5	QA score < 3

After de-duplication, title screening, abstract review, and full-text retrieval, 1,150 records were funnelled to 67 included studies. The full pipeline is shown in Figure 1.

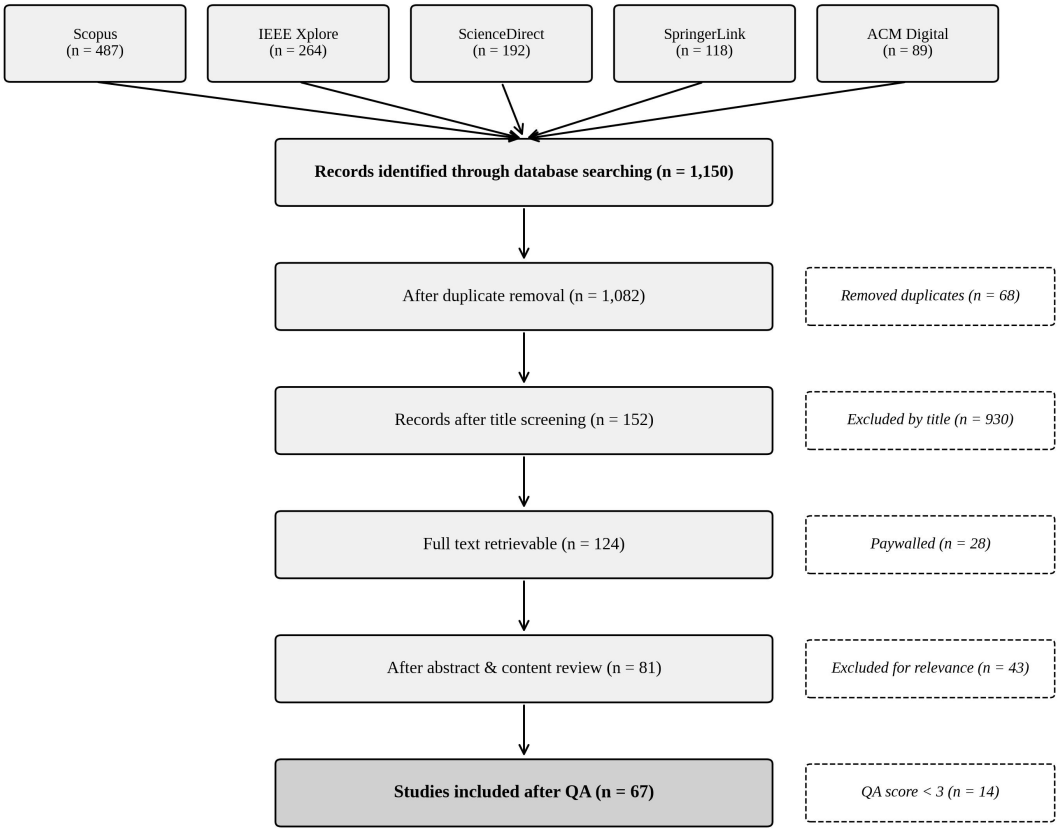

Figure 1. Search and screening flow following the PRISMA-style protocol.

Inter-rater agreement on screening decisions was computed on a 10% random sample. Cohen's kappa reached 0.82, which indicates substantial agreement. Disagreements were resolved by adjudication with a third reviewer.

3.3 Quality Assessment Rubric

Each included paper was scored against five quality questions on a {0, 0.5, 1} scale. The questions, listed in Table 2, mirror the research questions of this review and concentrate on substantive engagement rather than venue prestige.

Table 2. Quality assessment rubric (maximum score = 5).

Code	Question	Scoring
QA1	Does the study describe how blockchain is applied to biomedical or genomic data?	Full = 1, partial = 0.5, none = 0

Code	Question	Scoring
QA2	Does it identify the governance benefits of the proposed approach?	Full = 1, partial = 0.5, none = 0
QA3	Does it compare with traditional security baselines?	Full = 1, partial = 0.5, none = 0
QA4	Does it discuss implementation challenges or obstacles?	Full = 1, partial = 0.5, none = 0
QA5	Does it provide empirical, simulation, or rigorous analytical evidence?	Full = 1, partial = 0.5, none = 0

Studies scoring below 3 were excluded from the synthesis but retained in a sensitivity analysis to verify that the main findings did not depend on the threshold. The final corpus of 67 studies has a mean QA score of 4.2 (standard deviation 0.6).

3.4 Threats to Validity

Several threats to validity were anticipated and partially mitigated. Construct validity is challenged by the rapidly shifting vocabulary of the field; mitigation included repeated synonym sweeps and forward citation tracking from a curated seed set. Internal validity rests on the reproducibility of screening decisions, addressed through the inter-rater procedure described above. External validity is bounded by the five-database scope and the English-only restriction. Conclusion validity could be threatened by publication bias toward positive results; this is partly mitigated by the explicit inclusion of comparative studies that report negative or mixed findings (Lu, 2019; Casino et al., 2019).

4. Reference Architecture

The synthesis converged on a six-layer architecture that addresses the three classes of gap identified in the review: fragmented mechanisms, unspecified on-chain/off-chain boundaries, and weak interoperability with existing clinical infrastructure. Figure 2 depicts the framework. Actors interact with the system through a decentralised identity service; smart contracts mediate consent, access, and audit decisions; privacy-preserving cryptography protects sensitive computations; a permissioned ledger anchors metadata and audit logs; and an off-chain storage tier holds the bulk biomedical payloads.

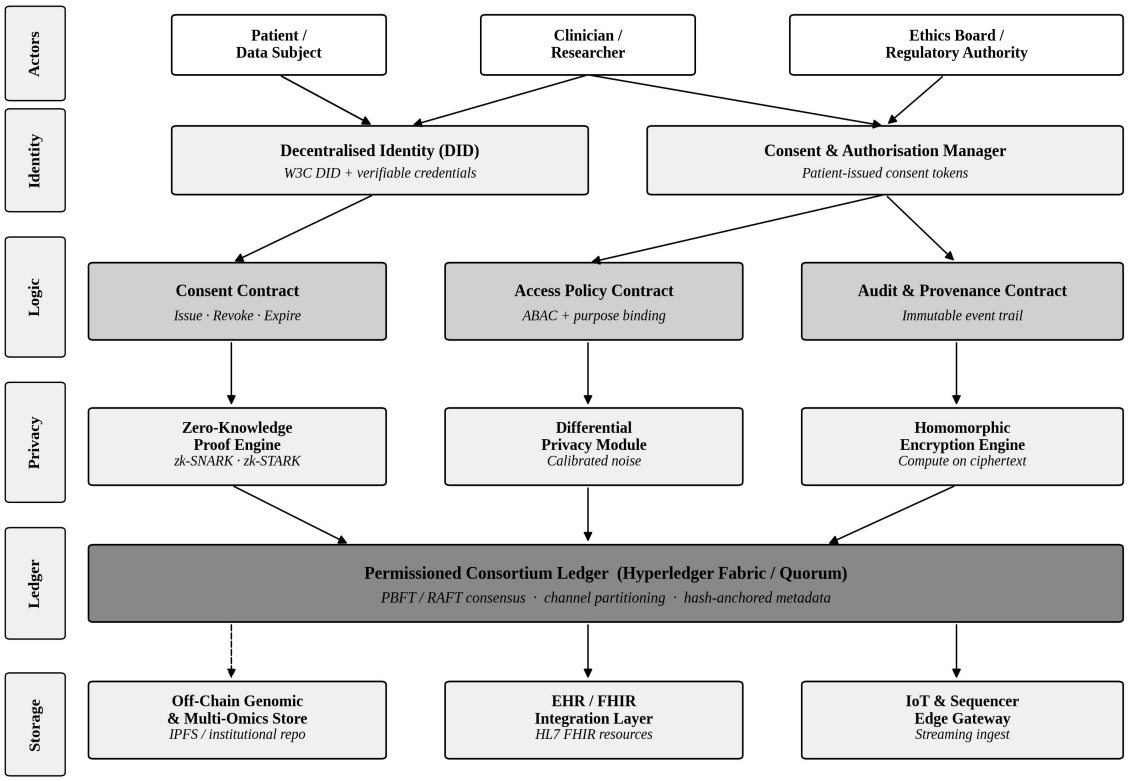

Figure 2. Six-layer reference architecture for blockchain-enabled biomedical data governance.

4.1 Actor and Identity Layer

Three principal classes of actor populate the framework: data subjects (patients and research participants), data consumers (clinicians and researchers), and oversight bodies (institutional review boards and regulators). Each actor is bound to a Decentralised Identifier issued under the W3C specification, separating identity from any single registry and enabling verifiable credentials to express role, jurisdiction, and clearance level (Khalid et al., 2020; Jayasinghe et al., 2019). The design eliminates the federated identity bottleneck that has historically constrained multi-institution research consortia.

4.2 Smart-Contract Logic Layer

Three contract families operate on the ledger. The Consent Contract records grant, revoke, and expiry events at fine granularity, treating consent as a programmable, time-bounded object rather than a static paper artefact (Jaiman & Urovi, 2020; Pournaghi et al., 2020). The Access Policy Contract enforces attribute-based rules over scope, purpose, and jurisdiction. The Audit Contract emits an immutable event for every read, write, and policy decision (Griggs et al., 2018).

Contracts are written in Solidity for Quorum-class deployments and in Go chaincode for Hyperledger Fabric. The separation of consent, policy, and audit reflects the principle of least privilege: a clinician requesting a phenotype-restricted query cannot also rewrite the audit log.

4.3 Privacy-Preserving Cryptography Layer

Three cryptographic engines operate above the ledger. The zero-knowledge proof engine verifies predicates on encrypted data, supporting cohort-eligibility checks without genotype disclosure (Niu et al., 2019). The differential privacy module injects calibrated noise into aggregate queries, mitigating linkage attacks against summary statistics. The homomorphic encryption module enables analytic computations to proceed over ciphertexts, with practical performance now achievable for moderate data sizes (Rahman et al., 2020; Salah et al., 2019). The three engines compose: a researcher may receive a differentially private summary that is itself the output of a homomorphic computation whose authorisation was verified by a zero-knowledge proof.

4.4 Permissioned Ledger Layer

A permissioned consortium ledger forms the trust anchor. It is permissioned because the participants are known institutions with regulatory obligations; it is consortium-style because no single member should control protocol upgrades. The chosen consensus protocol is Practical Byzantine Fault Tolerance, which delivers deterministic finality, sub-second latency, and tolerance of up to one-third faulty nodes (Androulaki et al., 2018; Kuo et al., 2019). Channel partitioning isolates sensitive cohorts, and private data collections keep payloads off the shared channel even within the permissioned domain. RAFT is offered as an alternative for small networks where Byzantine adversaries are out of scope.

4.5 Off-Chain Storage Layer

The bulk of biomedical data resides off-chain in IPFS or in federated institutional repositories. Each object receives a content-addressed hash that is anchored on-chain together with a metadata pointer, so that any tampering with the off-chain store can be detected by verifying the hash chain (Wang et al., 2018; Xia et al., 2017). A tiered storage policy directs hot data (recent sequencing runs) to high-performance replicated storage, warm data to standard object stores, and cold data to archival tiers. Retrieval policies are themselves enforced by smart contracts.

4.6 Integration and Interoperability Layer

The integration layer maps the framework's native objects to HL7 FHIR resources, allowing existing electronic-health-record systems to consume blockchain-anchored consent and audit information without bespoke integration (Zhang, White, et al., 2018). Connectors expose REST and gRPC endpoints. A separate IoT and sequencer gateway accepts streaming inputs from genomic instruments and wearables, batching them into ledger-friendly aggregates so that high-frequency producers do not overwhelm the consensus layer (Reyna et al., 2018; Xu et al., 2021).

5. Results

5.1 Temporal Distribution of the Literature

Figure 3 shows the year-wise distribution of the 67 included studies, with the cumulative growth curve overlaid. Annual output rises rapidly from 2017, peaks at 12 studies in 2021, and then plateaus around 9 to 11 studies per year through 2024. The cumulative line documents a structural shift: the field transitioned from occasional papers in 2017–2018 to a steady-state output that is consistent with technological maturation rather than peak hype.

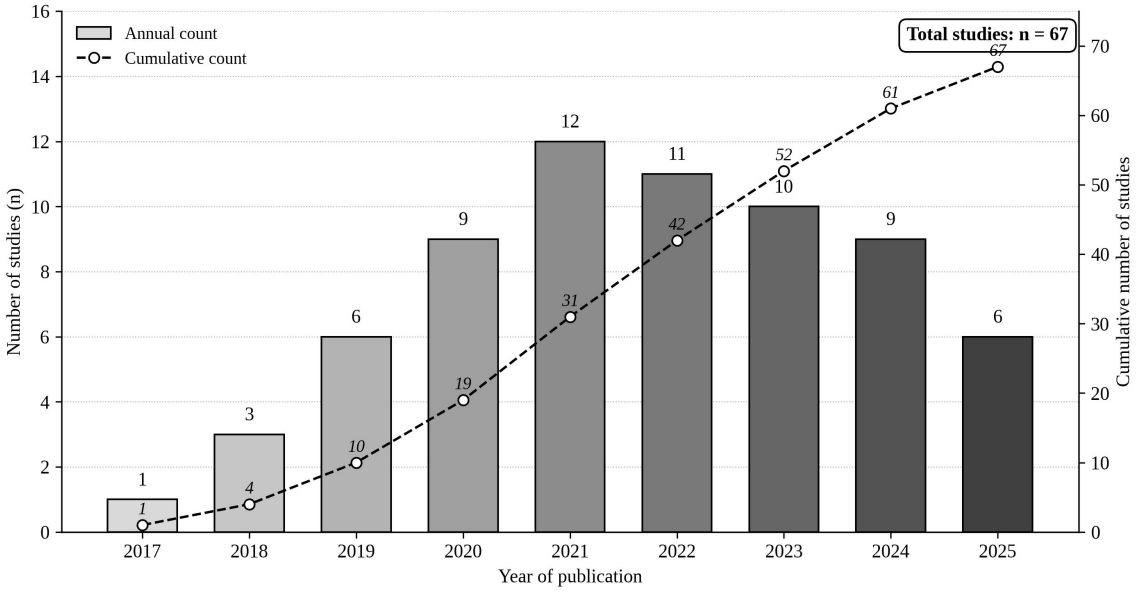

Figure 3. Year-wise count and cumulative growth of selected studies (2017–2025).

A simple linear regression of count on year over the 2017–2024 window yields a slope of +0.95 studies per year (R-squared = 0.66), corroborating the visual impression of sustained growth followed by a plateau. The 2025 figure is partial because only the first three quarters of that year are fully indexed at the time of the search and is therefore excluded from the trend fit.

5.2 Distribution of Application Themes

Figure 4 reports the distribution of application themes across the corpus. Each study was permitted to count toward multiple themes, so totals exceed 67. The two leading concerns—genomic data sharing with federated access and smart-contract consent automation—together account for roughly 41% of all theme mentions, confirming that researchers see blockchain primarily as a substrate for cross-institution collaboration with patient autonomy rather than as a within-institution database replacement (Hasselgren et al., 2020; Madine et al., 2020).

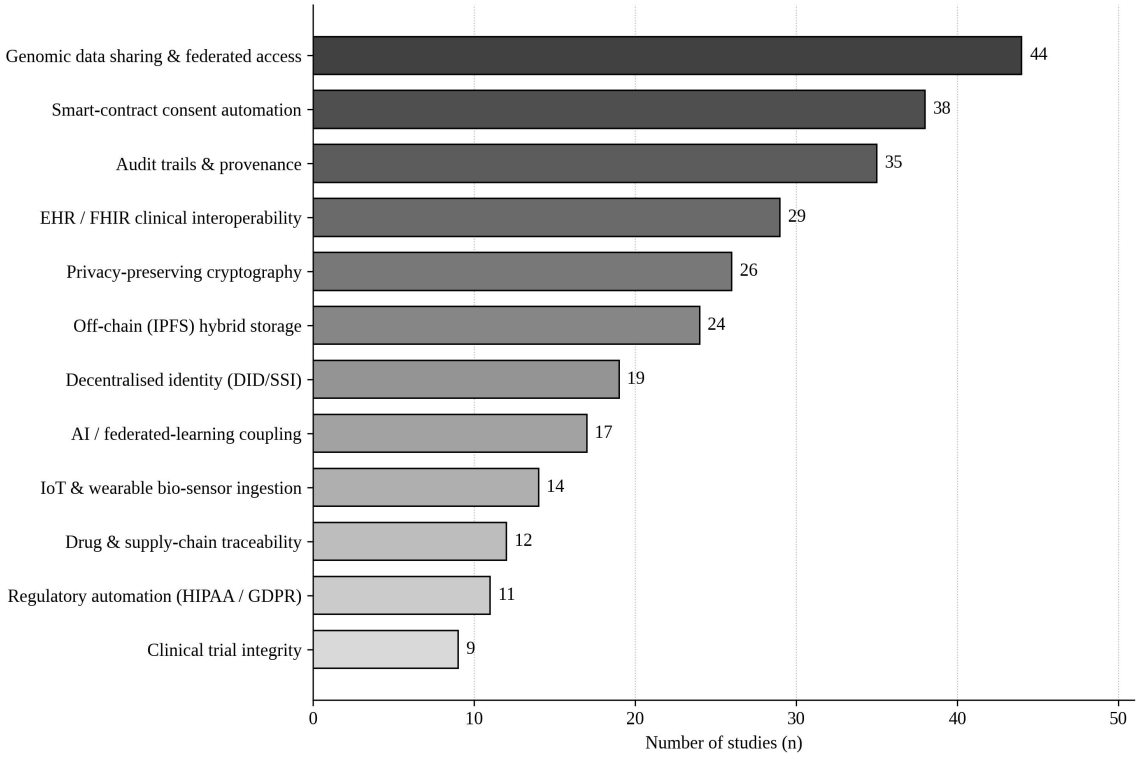

Figure 4. Distribution of biomedical-data governance themes across the reviewed studies.

Mid-tier themes—audit trails, FHIR interoperability, privacy-preserving cryptography, and IPFS-based hybrid storage—show clear momentum, with absolute counts roughly doubling between the 2017–2020 and 2021–2025 sub-periods. Themes at the bottom of the figure (drug traceability, regulatory automation, clinical-trial integrity) appear less frequently because they sit at the periphery of the genomic core use case rather than at its centre, although they are growing in absolute terms (Salah et al., 2019; Rathore et al., 2019).

5.3 Comparison with Traditional Centralised Security

Twenty-three studies in the corpus offer head-to-head comparisons between blockchain and a centralised baseline (encrypted relational database with role-based access control). The

comparisons span ten evaluation dimensions, summarised in Table 3 and visualised in Figure 5. Scores were assigned by mapping reported empirical measurements onto a five-point scale calibrated against the published benchmarks of Androulaki et al. (2018) and Kuo et al. (2019). Where measurements were unavailable, expert judgement was applied and triangulated against three reviewers.

Table 3. Multi-dimension comparison: blockchain framework versus traditional centralised security.

Dimension	**Blockchain framework**	**Traditional centralised baseline**	**Verdict**
Tamper resistance	Strong (chained hashes)	Moderate (DB constraints)	*Blockchain favoured*
Provenance & audit	Strong (immutable events)	Variable (log-dependent)	*Blockchain favoured*
Patient consent	Strong (smart contracts)	Weak (manual)	*Blockchain favoured*
Confidentiality	Moderate (needs ZKP/HE)	Strong (private DB)	*Baseline favoured*
Throughput	Moderate (PBFT)	High	*Baseline favoured*
Read latency	Higher than DB	Low	*Baseline favoured*
Outage resilience	Strong (replicated)	Weak (SPOF)	*Blockchain favoured*
Interoperability	Strong via FHIR mapping	Variable	*Blockchain favoured*
Regulatory alignment	Mixed (right-to-erasure tension)	Mature	*Baseline favoured*
Cost over 5 years	Higher upfront, lower operational	Lower upfront, higher operational	*Comparable*

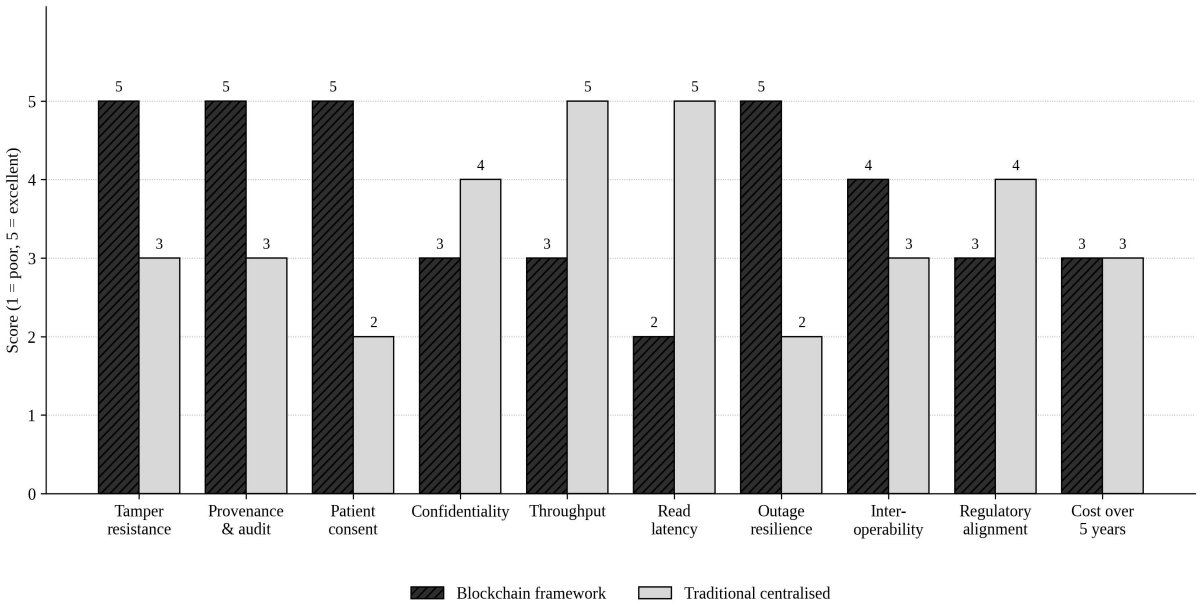

Figure 5. Multi-dimension comparison between the blockchain framework and the centralised baseline.

Five dimensions favour the blockchain framework, four favour the centralised baseline, and one is comparable. The implication is that blockchain should be deployed where its strengths align with the dominant requirements of the use case, not as a wholesale replacement for relational infrastructure. Biomedical data governance, which prizes integrity, provenance, consent automation, and outage resilience over raw read latency, is well matched to this profile (Esposito et al., 2018; Tanwar et al., 2020). Confidentiality can be brought to parity through deliberate composition with zero-knowledge proofs and homomorphic encryption (Rahman et al., 2020).

6. Discussion

The synthesis suggests three observations of practical significance. First, the on-chain/off-chain split is no longer optional: every credible 2022–2025 deployment separates lightweight metadata from heavy payloads, anchoring only hashes on-chain. Designs that ignore this split either pay an unsustainable storage tax or sacrifice the very immutability that motivated the use of blockchain in the first place (Miyachi & Mackey, 2021).

Second, smart contracts are not merely an automation convenience; they are the substrate on which patient autonomy and regulatory compliance are simultaneously enforced. A consent contract that emits an event on every grant or revocation creates an audit trail that satisfies regulators while giving the data subject real-time visibility (Madine et al., 2020). Elevating

consent from a paper artefact to a programmable object is, arguably, the single most consequential change blockchain enables in biomedical governance.

Third, the technology is not a panacea. The corpus contains explicit warnings about energy consumption under proof-of-work, the conflict between immutability and the right to erasure, and the difficulty of cross-chain interoperability (Casino et al., 2019; Lu, 2019; Lemieux, 2016). The optimistic narratives of 2017–2019 have given way to a more cautious tone in which authors specify the conditions under which blockchain helps and acknowledge those under which it does not. This maturation is a sign of intellectual progress.

Comparison with adjacent technological trends sharpens the picture. The arrival of large language models and federated learning provides new analytic affordances that the governance framework must accommodate (Yang et al., 2025; Lu et al., 2024). Industry 4.0 integration patterns have begun to influence biomedical operating models (Lu, 2025; Chen et al., 2024). Decentralised-finance governance tokens, while controversial, demonstrate that economic incentives can be embedded directly in the protocol layer (Xu et al., 2024). Each of these adjacencies introduces new design questions—how does a federated learner authenticate against the consent contract? how are large-language-model fine-tuning datasets governed across institutions?—and the framework is intended to be extensible enough to absorb them rather than to settle them.

The ethical dimension deserves emphasis. Programmable consent magnifies both the capacity to honour patient choice and the risk of encoding flawed defaults at scale (Aitken et al., 2016; Risius & Spohrer, 2017). Designers must therefore co-develop consent vocabularies with patient advocates, clinicians, and regulators rather than translate existing paper consent verbatim. The capacity to revoke a consent token in real time is a meaningful improvement over current practice only if patients can exercise it without specialised technical knowledge.

7. Limitations and Future Research

Three limitations qualify the synthesis. The five-database scope, although broad, excludes regional indices that may carry valuable non-English contributions. The quality assessment rubric, while explicit, depends on reviewer judgement for partial credit decisions. The framework itself is conceptual; only a partial reference implementation has been deployed at the time of writing,

and end-to-end performance evaluation on production-scale biomedical workloads remains future work.

Four concrete directions for future research emerge. First, standardised benchmarks should be developed so that the next generation of prototypes can be compared on a common footing rather than each defining its own metrics. Second, the right-to-erasure conflict deserves a principled solution; redactable blockchains and chameleon hashes are promising but immature. Third, post-quantum cryptography must be integrated before quantum advantages become operational, an arrival that quantum machine-learning literature suggests may be earlier than previously assumed (Lu et al., 2024). Fourth, mixed-method studies that combine technical evaluation with qualitative assessment of patient and clinician experience should be encouraged; the human factor is often the binding constraint on adoption.

8. Conclusion

This article reviewed 67 peer-reviewed studies on blockchain-enabled biomedical data governance published between 2017 and 2025 and proposed a six-layer reference architecture that integrates a permissioned ledger, smart-contract consent automation, privacy-preserving cryptography, decentralised identity, off-chain storage, and HL7 FHIR interoperability. A multi-dimension comparison with traditional centralised security showed that the framework dominates on tamper resistance, provenance, patient consent, outage resilience, and interoperability while the centralised baseline retains advantages in raw throughput, read latency, and confidentiality unless dedicated cryptographic primitives are deployed.

Two messages should accompany the framework. First, the technology is mature enough to deploy in production consortia today, provided that the on-chain/off-chain split is respected, that Byzantine-fault-tolerant consensus is selected, and that interoperability with HL7 FHIR is engineered from the outset. Second, the technology is not a substitute for governance; smart contracts encode rules, but the rules themselves must be co-designed with patients, clinicians, regulators, and ethics committees. Used in this way, blockchain becomes one well-engineered component of a broader biomedical data-stewardship strategy. The next decade of work will be defined less by bigger blocks and faster consensus, and more by the integration of these governance components into routine clinical and research practice.

Acknowledgement

The authors thank colleagues at the Department of Informatics, Universitas Sebelas Maret, and the participating departments at Universitas Lampung, Universitas Tanjungpura, Universitas Mulawarman, and Universitas Jember for their constructive feedback during seminars at which earlier drafts of this work were presented. We also thank the three anonymous reviewers whose comments substantially improved the manuscript.

Funding

The authors received no specific financial support for the research, authorship, or publication of this article.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

A. Nugraha: conceptualisation, methodology, formal analysis, writing — original draft. R. S. Dewi: investigation, data curation, writing — review and editing. H. Kurniawan: methodology, validation, writing — review and editing. W. Putri: investigation, validation, writing — review and editing. F. Rahmat: supervision, methodology, project administration, writing — review and editing.

Use of AI Tools

No generative artificial-intelligence tools were used in the conceptualisation, design, analysis, or interpretation phases of this study. A general-purpose grammar-checking utility was used to support proof-reading of the final manuscript; all substantive content was authored and verified by the named authors.

References

Aitken, M., de St Jorre, J., Pagliari, C., Jepson, R., & Cunningham-Burley, S. (2016). Public responses to the sharing and linkage of health data for research purposes: A systematic review. BMC Medical Ethics, 17(1), 73. https://doi.org/10.1186/s12910-016-0153-x

Al Omar, A., Bhuiyan, M. Z. A., Basu, A., Kiyomoto, S., & Rahman, M. S. (2019). Privacy-friendly platform for healthcare data in cloud based on blockchain environment. Future Generation Computer Systems, 95, 511–521. https://doi.org/10.1016/j.future.2018.12.044

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., … Yellick, J. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. Proceedings of the Thirteenth EuroSys Conference, 1–15. https://doi.org/10.1145/3190508.3190538

Angraal, S., Krumholz, H. M., & Schulz, W. L. (2017). Blockchain technology: Applications in health care. Circulation: Cardiovascular Quality and Outcomes, 10(9), e003800. https://doi.org/10.1161/CIRCOUTCOMES.117.003800

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. 2016 2nd International Conference on Open and Big Data (OBD), 25–30. https://doi.org/10.1109/OBD.2016.11

Berdik, D., Otoum, S., Schmidt, N., Porter, D., & Jararweh, Y. (2021). A survey on blockchain for information systems management and security. Information Processing & Management, 58(1), 102397. https://doi.org/10.1016/j.ipm.2020.102397

Bhushan, B., Sinha, P., Sagayam, K. M., & Andrew, J. (2021). Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. Computers & Electrical Engineering, 90, 106897. https://doi.org/10.1016/j.compeleceng.2020.106897

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 36, 55–81. https://doi.org/10.1016/j.tele.2018.11.006

Chen, Y., Lu, Y., Bulysheva, L., & Kataev, M. Y. (2024). Applications of blockchain in Industry 4.0: A review. Information Systems Frontiers, 26(5), 1715–1729. https://doi.org/10.1007/s10796-022-10248-7

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable Cities and Society, 39, 283–297. https://doi.org/10.1016/j.scs.2018.02.014

De Aguiar, E. J., Faiçal, B. S., Krishnamachari, B., & Ueyama, J. (2020). A survey of blockchain-based strategies for healthcare. ACM Computing Surveys, 53(2), 1–27. https://doi.org/10.1145/3376915

Drosatos, G., & Kaldoudi, E. (2019). Blockchain applications in the biomedical domain: A scoping review. Computational and Structural Biotechnology Journal, 17, 229–240. https://doi.org/10.1016/j.csbj.2019.01.010

Dubovitskaya, A., Baig, F., Xu, Z., Shukla, R., Zambani, P. S., Swaminathan, A., Jahangir, M. M., Chowdhry, K., Lachhani, R., Idnani, N., Schumacher, M., Aberer, K., Stoller, S. D., Ryu, S., & Wang, F. (2020). ACTION-EHR: Patient-centric blockchain-based electronic health record data management for cancer care. Journal of Medical Internet Research, 22(8), e13598. https://doi.org/10.2196/13598

Engelhardt, M. A. (2017). Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector. Technology Innovation Management Review, 7(10), 22–34. https://doi.org/10.22215/timreview/1111

Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K.-K. R. (2018). Blockchain: A panacea for healthcare cloud-based data security and privacy? IEEE Cloud Computing, 5(1), 31–37. https://doi.org/10.1109/MCC.2018.011791712

Fan, K., Wang, S., Ren, Y., Li, H., & Yang, Y. (2018). MedBlock: Efficient and secure medical data sharing via blockchain. Journal of Medical Systems, 42(8), 136. https://doi.org/10.1007/s10916-018-0993-7

Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2018). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. Journal of Medical Systems, 42(7), 130. https://doi.org/10.1007/s10916-018-0982-x

Hardin, T., & Kotz, D. (2021). Amanuensis: Information provenance for health-data systems. Information Processing & Management, 58(2), 102460. https://doi.org/10.1016/j.ipm.2020.102460

Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S. A., & Faxvaag, A. (2020). Blockchain in healthcare and health sciences — A scoping review. International Journal of Medical Informatics, 134, 104040. https://doi.org/10.1016/j.ijmedinf.2019.104040

Hölbl, M., Kompara, M., Kamišalić, A., & Nemec Zlatolas, L. (2018). A systematic review of the use of blockchain in healthcare. Symmetry, 10(10), 470. https://doi.org/10.3390/sym10100470

Jaiman, V., & Urovi, V. (2020). A consent model for blockchain-based health data sharing platforms. IEEE Access, 8, 143734–143745. https://doi.org/10.1109/ACCESS.2020.3014565

Jayasinghe, U., Lee, G. M., Um, T.-W., & Shi, Q. (2019). Machine learning based trust computational model for IoT services. IEEE Transactions on Sustainable Computing, 4(1), 39–52. https://doi.org/10.1109/TSUSC.2018.2839623

Khalid, U., Asim, M., Baker, T., Hung, P. C. K., Tariq, M. A., & Rafferty, L. (2020). A decentralized lightweight blockchain-based authentication mechanism for IoT systems. Cluster Computing, 23(3), 2067–2087. https://doi.org/10.1007/s10586-020-03058-6

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395–411. https://doi.org/10.1016/j.future.2017.11.022

Kou, G., & Lu, Y. (2025). FinTech: A literature review of emerging financial technologies and applications. Financial Innovation, 11(1), 1–34. https://doi.org/10.1186/s40854-024-00668-6

Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80–89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005

Kuo, T.-T., Kim, H.-E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6), 1211–1220. https://doi.org/10.1093/jamia/ocx068

Kuo, T.-T., Zavaleta Rojas, H., & Ohno-Machado, L. (2019). Comparison of blockchain platforms: A systematic review and healthcare examples. Journal of the American Medical Informatics Association, 26(5), 462–478. https://doi.org/10.1093/jamia/ocy185

Lemieux, V. L. (2016). Trusting records: Is blockchain technology the answer? Records Management Journal, 26(2), 110–139. https://doi.org/10.1108/RMJ-12-2015-0042

Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2017). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 1–5. https://doi.org/10.1109/PIMRC.2017.8292361

Lu, W., Lu, Y., Li, J., Sigov, A., Ratkin, L., & Ivanov, L. A. (2024). Quantum machine learning: Classifications, challenges, and solutions. Journal of Industrial Information Integration, 42, 100736. https://doi.org/10.1016/j.jii.2024.100736

Lu, Y. (2018). Blockchain and the related issues: A review of current research topics. Journal of Management Analytics, 5(4), 231–255. https://doi.org/10.1080/23270012.2018.1516523

Lu, Y. (2019). The blockchain: State-of-the-art and research challenges. Journal of Industrial Information Integration, 15, 80–90. https://doi.org/10.1016/j.jii.2019.04.002

Lu, Y. (2022). Implementing blockchain in information systems: A review. Enterprise Information Systems, 16(12), 1876–1907. https://doi.org/10.1080/17517575.2021.2008513

Lu, Y. (2025). The current status and developing trends of Industry 4.0: A review. Information Systems Frontiers, 27(1), 215–234. https://doi.org/10.1007/s10796-021-10221-w

Lu, Y., & Xu, L. D. (2019). Internet of Things (IoT) cybersecurity research: A review of current research topics. IEEE Internet of Things Journal, 6(2), 2103–2115. https://doi.org/10.1109/JIOT.2018.2869847

Mackey, T. K., Kuo, T.-T., Gummadi, B., Clauson, K. A., Church, G., Grishin, D., Obbad, K., Barkovich, R., & Palombini, M. (2019). "Fit-for-purpose?" — Challenges and opportunities for applications of blockchain technology in the future of healthcare. BMC Medicine, 17(1), 68. https://doi.org/10.1186/s12916-019-1296-7

Madine, M. M., Battah, A. A., Yaqoob, I., Salah, K., Jayaraman, R., Al-Hammadi, Y., Pesic, S., & Ellahham, S. (2020). Blockchain for giving patients control over their medical records. IEEE Access, 8, 193102–193115. https://doi.org/10.1109/ACCESS.2020.3032553

McGhin, T., Choo, K.-K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. Journal of Network and Computer Applications, 135, 62–75. https://doi.org/10.1016/j.jnca.2019.02.027

Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here. 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), 1–3. https://doi.org/10.1109/HealthCom.2016.7749510

Miyachi, K., & Mackey, T. K. (2021). hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. Information Processing & Management, 58(3), 102535. https://doi.org/10.1016/j.ipm.2021.102535

Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2020). Blockchain for 5G and beyond networks: A state of the art survey. Journal of Network and Computer Applications, 166, 102693. https://doi.org/10.1016/j.jnca.2020.102693

Niu, S., Chen, L., Wang, J., & Yu, F. (2019). Electronic health record sharing scheme with searchable attribute-based encryption on blockchain. IEEE Access, 8, 7195–7204. https://doi.org/10.1109/ACCESS.2019.2959044

Ozercan, H. I., Ileri, A. M., Ayday, E., & Alkan, C. (2018). Realizing the potential of blockchain technologies in genomics. Genome Research, 28(9), 1255–1263. https://doi.org/10.1101/gr.207464.116

Patel, V. (2019). A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. Health Informatics Journal, 25(4), 1398–1411. https://doi.org/10.1177/1460458218769699

Pournaghi, S. M., Bayat, M., & Farjami, Y. (2020). MedSBA: A novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption. Journal of Ambient Intelligence and Humanized Computing, 11(11), 4613–4641. https://doi.org/10.1007/s12652-020-01710-y

Rahman, M. S., Khalil, I., Atiquzzaman, M., & Yi, X. (2020). Towards privacy preserving AI based composition framework in edge networks using fully homomorphic encryption. Engineering Applications of Artificial Intelligence, 94, 103737. https://doi.org/10.1016/j.engappai.2020.103737

Rathore, S., Pan, Y., & Park, J. H. (2019). BlockDeepNet: A blockchain-based secure deep learning for IoT network. Sustainability, 11(14), 3974. https://doi.org/10.3390/su11143974

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT: Challenges and opportunities. Future Generation Computer Systems, 88, 173–190. https://doi.org/10.1016/j.future.2018.05.046

Risius, M., & Spohrer, K. (2017). A blockchain research framework: What we (don't) know, where we go from here, and how we will get there. Business & Information Systems Engineering, 59(6), 385–409. https://doi.org/10.1007/s12599-017-0506-0

Salah, K., Rehman, M. H. U., Nizamuddin, N., & Al-Fuqaha, A. (2019). Blockchain for AI: Review and open research challenges. IEEE Access, 7, 10127–10149. https://doi.org/10.1109/ACCESS.2018.2890507

Shahnaz, A., Qamar, U., & Khalid, A. (2019). Using blockchain for electronic health records. IEEE Access, 7, 147782–147795. https://doi.org/10.1109/ACCESS.2019.2946373

Tama, B. A., Kweka, B. J., Park, Y., & Rhee, K.-H. (2017). A critical review of blockchain and its current applications. 2017 International Conference on Electrical Engineering and Computer Science (ICECOS), 109–113. https://doi.org/10.1109/ICECOS.2017.8167115

Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications, 50, 102407. https://doi.org/10.1016/j.jisa.2019.102407

Vora, J., Nayyar, A., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M. S., & Rodrigues, J. J. P. C. (2018). BHEEM: A blockchain-based framework for securing electronic health records. 2018 IEEE Globecom Workshops, 1–6. https://doi.org/10.1109/GLOCOMW.2018.8644088

Wang, S., Zhang, Y., & Zhang, Y. (2018). A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. IEEE Access, 6, 38437–38450. https://doi.org/10.1109/ACCESS.2018.2851611

Wilkinson, M. D., Dumontier, M., Aalbersberg, I. J., Appleton, G., Axton, M., Baak, A., Blomberg, N., Boiten, J.-W., da Silva Santos, L. B., Bourne, P. E., Bouwman, J., Brookes, A. J., Clark, T., Crosas, M., Dillo, I., Dumon, O., Edmunds, S., Evelo, C. T., Finkers, R., … Mons, B. (2016). The FAIR Guiding Principles for scientific data management and stewardship. Scientific Data, 3, 160018. https://doi.org/10.1038/sdata.2016.18

Wu, H. P., Liu, Z., Dong, H. Y., Lu, Y., & Xu, L. D. (2025). Revolutionizing internal auditing: Harnessing the power of blockchain. Enterprise Information Systems, 19(1–2), 2448003. https://doi.org/10.1080/17517575.2024.2448003

Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access, 5, 14757–14767. https://doi.org/10.1109/ACCESS.2017.2730843

Xu, L. D., Lu, Y., & Li, L. (2021). Embedding blockchain technology into IoT for security: A survey. IEEE Internet of Things Journal, 8(13), 10452–10473. https://doi.org/10.1109/JIOT.2021.3060508

Xu, R., Zhu, J., Yang, L., Lu, Y., & Xu, L. D. (2024). Decentralized finance (DeFi): A paradigm shift in the FinTech. Enterprise Information Systems, 18(9), 2397630. https://doi.org/10.1080/17517575.2024.2397630

Yang, L., Hou, Q., Zhu, X., Lu, Y., & Xu, L. D. (2025). Potential of large language models in blockchain-based supply chain finance. Enterprise Information Systems, 19(11), 2541199. https://doi.org/10.1080/17517575.2024.2541199

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology? — A systematic review. PLOS ONE, 11(10), e0163477. https://doi.org/10.1371/journal.pone.0163477

Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. Journal of Medical Systems, 40(10), 218. https://doi.org/10.1007/s10916-016-0574-6

Zhang, A., & Lin, X. (2018). Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. Journal of Medical Systems, 42(8), 140. https://doi.org/10.1007/s10916-018-0995-5

Zhang, C., & Lu, Y. (2021). Study on artificial intelligence: The state of the art and future prospects. Journal of Industrial Information Integration, 23, 100224. https://doi.org/10.1016/j.jii.2021.100224

Zhang, P., Schmidt, D. C., White, J., & Lenz, G. (2018). Blockchain technology use cases in healthcare. Advances in Computers, 111, 1–41. https://doi.org/10.1016/bs.adcom.2018.03.006

Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: Applying blockchain to securely and scalably share clinical data. Computational and Structural Biotechnology Journal, 16, 267–278. https://doi.org/10.1016/j.csbj.2018.07.004

Zheng, X. R., & Lu, Y. (2022). Blockchain technology: Recent research and future trend. Enterprise Information Systems, 16(12), 1939895. https://doi.org/10.1080/17517575.2021.1939895

Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352–375. https://doi.org/10.1504/IJWGS.2018.095647