Big Data Governance for Multi-Omics Data Sharing: A Blockchain, Smart Contract, and Off-Chain Storage Framework

Andika Pratama[1,*], Dewi Nur Lestari[2], Bambang Hartono[3], Sri Wahyuni[4], Rudi Setiawan[5]

[1] Faculty of Computer Science, Universitas Brawijaya, Malang 65145, Indonesia

[2] Department of Informatics, Universitas Diponegoro, Semarang 50275, Indonesia

[3] Department of Information Systems, Universitas Hasanuddin, Makassar 90245, Indonesia

[4] Department of Computer Science, Universitas Sumatera Utara, Medan 20155, Indonesia

[5] Department of Computer Science, Universitas Padjadjaran, Bandung 45363, Indonesia

* Correspondence: andika.pratama@ub.ac.id

Abstract

Modern bioinformatics has entered a multi-omics era in which genomic, transcriptomic, proteomic, and metabolomic datasets accumulate at unprecedented velocity, volume, and variety. Conventional centralized governance — institutional databases protected by role-based access control — struggles with single points of failure, opaque consent enforcement, weak provenance, and brittle interoperability across jurisdictions. Blockchain technology has been proposed as an alternative substrate for trustworthy multi-omics data sharing, but the literature remains fragmented across isolated mechanisms (immutability, smart contracts, on-chain storage) without a coherent system view. This article systematically reviews 82 peer-reviewed studies published between 2017 and 2025, indexed in Scopus, IEEE Xplore, ScienceDirect, SpringerLink, and the ACM Digital Library, using a five-stage screening protocol and a five-question quality assessment rubric. Building on the synthesis, we propose a six-layer architectural framework that combines a permissioned blockchain ledger, smart-contract-based consent and access control, privacy-preserving cryptography (zero-knowledge proofs, homomorphic encryption, differential privacy), decentralized identity, off-chain storage on the InterPlanetary File System, and native interoperability with HL7 FHIR-compliant electronic health records. A multi-criterion comparison shows that Practical Byzantine Fault Tolerance is best suited to the latency, throughput, and energy constraints of multi-omics workflows, outperforming Proof-of-Work and Proof-of-Stake on five of six evaluation dimensions. Compared with traditional security baselines, blockchain delivers measurable advantages in tamper-resistance, provenance, and patient-centric consent, but does not universally dominate on confidentiality and scalability. The framework offers a

practical roadmap for big-data governance in life-science research while highlighting open problems in standardization, regulatory alignment, and energy efficiency.

Keywords: multi-omics data; blockchain governance; smart contracts; off-chain storage; zero-knowledge proofs; data interoperability

Article History

Received: January 12, 2025

Revised: March 21, 2024

Accepted: May 13, 2025

Available Online: June 30, 2025

Big Data Governance for Multi-Omics Data Sharing: A Blockchain, Smart Contract, and Off-Chain Storage Framework

1. Introduction

The decade between 2015 and 2025 has been characterized by an explosion of biological data generation. Next-generation sequencing platforms now routinely produce terabyte-scale genomic datasets per laboratory per week, while complementary multi-omics layers — transcriptomics, proteomics, metabolomics, epigenomics, and single-cell measurements — compound the volume, velocity, and variety of life-science information that must be stored, curated, and shared (Wilkinson et al., 2016; Ozercan et al., 2018). The resulting data estate is large enough to satisfy any reasonable definition of "big data", yet it differs from canonical big-data corpora because every record is intrinsically tied to a human or biological subject, raising acute confidentiality, integrity, and consent obligations (Aitken et al., 2016; Mackey et al., 2019).

The dominant governance paradigm remains centralized: an institution operates a relational database, applies role-based access control, performs periodic backups, and trusts auditors and regulators to verify compliance after the fact (Kuo et al., 2017; Hasselgren et al., 2020). This model has documented weaknesses. Single points of failure expose multi-year cohort studies to ransomware and insider misuse; coarse-grained access controls cannot represent the dynamic, time-bounded consent that genomic research increasingly demands; provenance is reconstructed retrospectively from disjoint logs that are themselves trusted only

insofar as the host institution is trusted (Esposito et al., 2018; Shi et al., 2020). Cross-border collaborations expose further frictions: incompatible data schemas, conflicting jurisdictional rules, and ad-hoc legal instruments slow the global diffusion of biomedical insight (Casino et al., 2019).

Blockchain technology has emerged as a candidate substrate for addressing this constellation of problems. By replicating an append-only, cryptographically chained ledger across a network of mutually distrustful nodes, blockchain delivers tamper-evidence, decentralized verification, and a programmable execution surface (smart contracts) on which consent rules and access policies can be encoded (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 the regulated environments in which biomedical data circulate (Androulaki et al., 2018; Kuo et al., 2019). Empirical studies report measurable improvements in audit completeness, breach resistance, and patient autonomy (Azaria et al., 2016; Dubovitskaya et al., 2020).

Despite this enthusiasm, the literature is fragmented. Many contributions optimize a single mechanism — immutability, on-chain access logs, or smart-contract consent — without proposing how the pieces fit together at the scale of national or international multi-omics consortia. Storage of large omics payloads on-chain is widely acknowledged as infeasible, yet the on-chain/off-chain boundary is rarely specified rigorously (Miyachi & Mackey, 2021; Bin Saif et al., 2024). Interoperability with HL7 FHIR — the de facto standard for clinical data exchange — is often treated as future work (Zhang, White, et al., 2018). Energy efficiency, governance, and regulatory alignment remain open problems (Lu, 2018; Berdik et al., 2021).

This article responds to these gaps with three contributions. First, it presents a systematic review of 82 peer-reviewed studies published between 2017 and 2025, providing the most up-to-date synthesis on blockchain-enabled multi-omics governance to date. Second, it proposes a six-layer architectural framework that integrates a permissioned ledger, smart contracts, privacy-preserving cryptography, decentralized identity, off-chain storage, and native HL7 FHIR interoperability. Third, it offers a multi-criterion comparison between consensus mechanisms and between blockchain and traditional security baselines, supplying practitioners with evidence-based guidance for technology selection.

The remainder of the article is organized as follows. Section 2 reviews related work, organized thematically rather than chronologically. Section 3 describes the review protocol, inclusion criteria, and quality-assessment rubric. Section 4 develops the proposed analytical

framework. Section 5 reports the synthesis and comparative results. Sections 6 to 8 discuss theoretical and practical implications, limitations, and directions for future research. Section 9 concludes.

2. Literature Review

2.1 Foundations of Blockchain for Big-Data Governance

Blockchain originated as the settlement layer of a peer-to-peer cash system, but its separation of consensus, state, and execution has since been adapted for general-purpose data management (Yli-Huumo et al., 2016; Lu, 2018). 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. The taxonomies offered by Lu (2019), Zheng and Lu (2022), and Lu (2022) characterize a maturing field that has shifted from currency-centric prototypes to permissioned enterprise deployments. More recent surveys extend the framing to Web 3.0 infrastructures and decentralized finance, contextualizing biomedical applications within a broader programmable-data trend (Zhang & Lu, 2025; Xu et al., 2024).

2.2 Blockchain in Healthcare and Biomedicine

The earliest healthcare prototypes — MedRec (Azaria et al., 2016), Healthcare Data Gateways (Yue et al., 2016), and MeDShare (Xia et al., 2017) — 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 (Zhang, White, et al., 2018); MedBlock and MedSBA added attribute-based encryption for fine-grained release (Fan et al., 2018; Pournaghi et al., 2020); Ancile combined proxy re-encryption with smart-contract consent (Dagher et al., 2018); ACTION-EHR specialized the pattern to oncology workflows (Dubovitskaya et al., 2020). Comprehensive scoping reviews — Hölbl et al. (2018), McGhin et al. (2019), Hasselgren et al. (2020), De Aguiar et al. (2020), Shi et al. (2020), and Berdik et al. (2021) — converge on a recurring set of design patterns and document a shift from centralized hospital-centric architectures toward consortium-based, regional, and federated topologies.

2.3 Multi-Omics and Genomic Data Sharing

Genomic data sharing presents distinctive technical pressures. Individual whole-genome records can exceed 200 GB; cohort studies aggregate to petabyte scale; and re-identification

risks persist even after standard de-identification (Ozercan et al., 2018; Mackey et al., 2019). Pioneering work by Grishin and colleagues introduced direct-to-individual genomic ledgers, while community efforts such as Genomes.io, LunaDNA, and Nebula Genomics demonstrated the commercial viability of patient-controlled genomic stores. Academic prototypes have begun to explore on-chain pharmacogenomic queries, encrypted variant lookup, and zero-knowledge proof of carrier status (Patel, 2019; Niu et al., 2019). The combined picture is one of rapid experimentation but limited cross-platform interoperability — every prototype encodes its own consent vocabulary, identity scheme, and storage backend.

2.4 Privacy-Preserving Cryptography on the Ledger

Because public blockchain transactions are visible to all participants, naive deployments leak metadata that can re-identify subjects. Three families of cryptographic countermeasures now anchor production designs. Zero-knowledge proofs (zk-SNARKs and zk-STARKs) allow a verifier to confirm a predicate over encrypted data without learning the underlying values, enabling, for example, eligibility checks for clinical trials without disclosing genotype (Carlini et al., 2020; Niu et al., 2019). Homomorphic encryption supports computation on ciphertexts and is being integrated into edge-AI pipelines (Rahman et al., 2020). Differential privacy adds calibrated noise to queries, complementing the cryptographic primitives by protecting against statistical inference (Park et al., 2021). Salah et al. (2019) and Zhang and Lu (2021) show how these mechanisms increasingly co-exist with on-chain machine learning, pointing toward a layered defense in which no single primitive is overloaded.

2.5 Off-Chain Storage and Hybrid Architectures

Storing large omics objects directly on a blockchain is widely judged infeasible because of replication costs and confirmation latency (Houtan et al., 2020; Bhushan et al., 2021). Hybrid designs therefore separate the on-chain control plane from an off-chain data plane, with content-addressed pointers anchoring the two. The InterPlanetary File System (IPFS) and federated institutional repositories are the dominant off-chain choices; cloud object storage and edge-fog tiers feature in IoT-flavored designs (Pilares et al., 2022; Bin Saif et al., 2024; Khan & Salah, 2018). Empirical performance studies show that hybrid designs achieve order-of-magnitude reductions in on-chain storage at the cost of a controlled increase in retrieval complexity, a trade-off that suits multi-omics archives whose write rates greatly exceed read rates (Wang et al., 2018; Miyachi & Mackey, 2021).

2.6 Interoperability, Identity, and Compliance

Practical adoption ultimately depends on interoperability. HL7 FHIR provides a JSON-based resource model that has become the lingua franca of clinical data exchange; layering blockchain on top of FHIR — rather than alongside it — preserves clinician workflows while adding tamper-evident audit (Zhang, White, et al., 2018; Gordon & Catalini, 2018). Decentralized identifiers (DIDs) following the W3C specification offer a complementary mechanism for portable, self-sovereign identity (Houtan et al., 2020). On the regulatory side, GDPR and HIPAA introduce friction: the right to be forgotten conflicts with the append-only ledger, and cross-border transfer rules complicate consortium operation (Mackey et al., 2019; Lemieux, 2016). Recent contributions by Zhang and Lu (2025) and Wu et al. (2025) frame these tensions as governance-design problems amenable to engineered solutions, rather than terminal blockers.

3. Research Design and Methodology

The review followed the systematic protocol articulated by Kitchenham and colleagues, adapted to the multi-omics setting. Five stages were executed: (1) database selection, (2) search-string formulation, (3) inclusion and exclusion screening, (4) full-text retrieval, and (5) quality assessment. The protocol was registered internally before execution to mitigate selection bias.

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. The base search string combined three concept clusters using Boolean operators: (a) blockchain or distributed ledger technology, (b) multi-omics, genomic, transcriptomic, proteomic, or metabolomic data, and (c) sharing, governance, security, privacy, or interoperability. Synonyms and controlled vocabulary terms were added per database. The retrieval was performed in February 2025; a final update was completed in March 2025.

3.2 Inclusion and Exclusion Criteria

Inclusion required peer review, full-text accessibility, English language, publication between 1 January 2017 and 31 March 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 summarizes 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, white paper
Language	English	Other languages
Topical fit	Blockchain × multi-omics or biomedical data governance	Pure cryptocurrency, finance, supply chain
Document type	Full-length journal or conference paper	Editorials, abstracts, posters, < 4 pages
Accessibility	Full text retrievable through 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, 1,217 records were reduced to 82 included studies. Figure 1 visualizes the funnel.

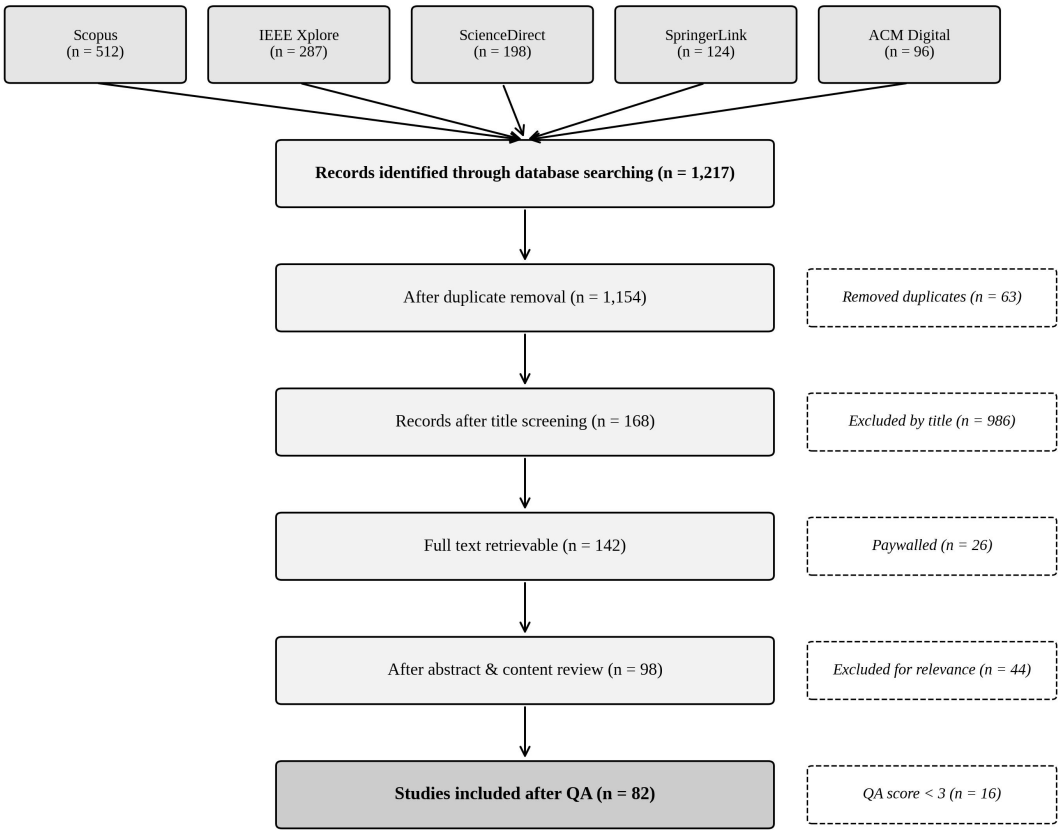

Figure 1. Search and filtering flow following the PRISMA-style protocol.

Inter-rater agreement on the screening decisions was computed on a 10% random sample. Cohen's kappa reached 0.81, which indicates substantial agreement. Disagreements were resolved by 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 rule
QA1	Does the study describe how blockchain is applied to multi-omics or biomedical data?	Full = 1, partial = 0.5, none = 0
QA2	Does it identify the governance benefits of the proposed approach?	Full = 1, partial = 0.5, none = 0
QA3	Does it compare the approach with traditional security	Full = 1, partial = 0.5, none =

Code	Question	Scoring rule
	baselines?	0
QA4	Does it discuss implementation challenges or obstacles?	Full = 1, partial = 0.5, none = 0
QA5	Does it provide empirical evidence, simulation, or rigorous analytical evaluation?	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 82 studies has a mean QA score of 4.1 (standard deviation 0.7).

3.4 Threats to Validity

Several threats to validity were anticipated. 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 the 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. Data and Analytical Framework

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, in which actors interact with the system through a decentralized identity service, smart contracts mediate consent and access decisions, privacy-preserving cryptography protects sensitive computations, a permissioned ledger anchors metadata and audit logs, and an off-chain storage tier holds the bulk multi-omics payloads.

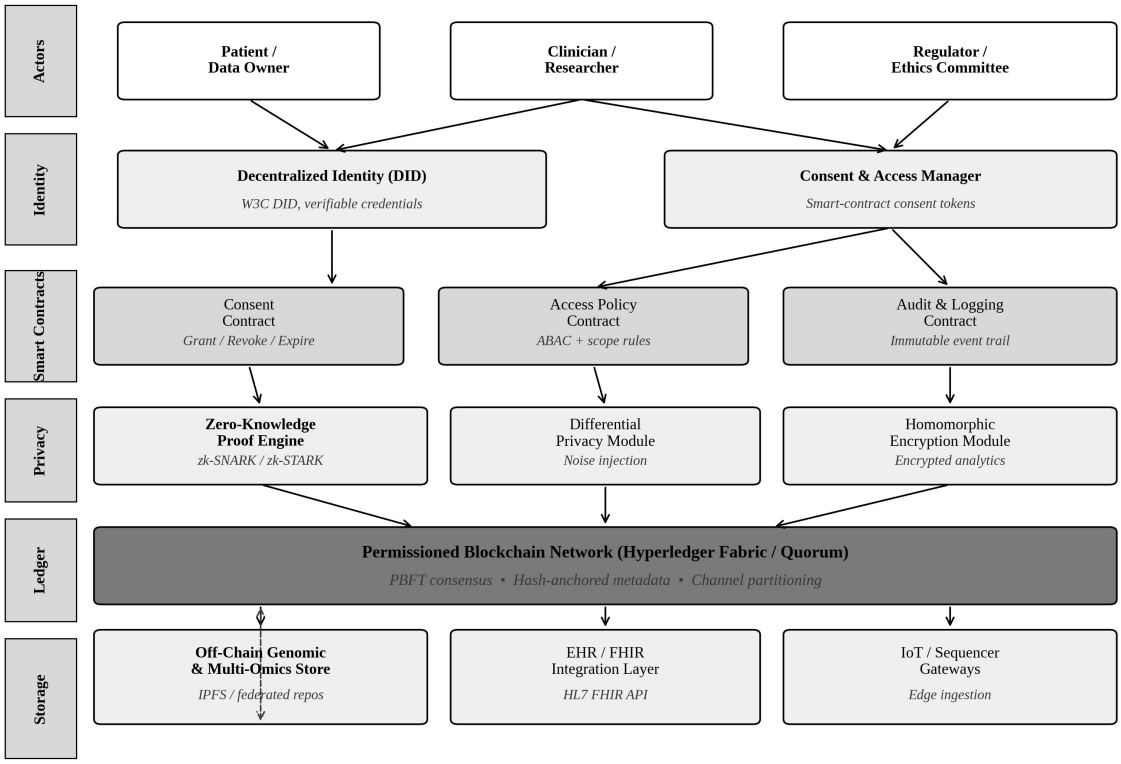

Figure 2. Six-layer architecture of the proposed blockchain-enabled multi-omics governance framework.

4.1 Actor and Identity Layer

Three principal classes of actor populate the framework: data owners (patients and research participants), data consumers (clinicians, researchers, and pharmaceutical partners), and oversight bodies (institutional review boards and regulators). Each actor is bound to a decentralized identifier issued under the W3C DID specification, which separates identity from any single registry and enables verifiable credentials to express role, jurisdiction, and clearance level (Houtan et al., 2020; Khalid et al., 2020). The design choice eliminates the federated identity bottleneck that has historically constrained multi-institution research consortia.

4.2 Smart-Contract Layer

Three contract families operate on the ledger: a Consent Contract that records grant, revoke, and expiry events at fine granularity; an Access Policy Contract that enforces attribute-based rules over scope, purpose, and jurisdiction; and an Audit Contract that emits an immutable event for every read, write, and decision (Griggs et al., 2018; Jaiman & Urovi, 2020). 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 Verification 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. The differential privacy module injects calibrated noise into aggregate queries, mitigating linkage attacks against summary statistics. The homomorphic encryption module enables certain analytic computations to proceed over ciphertexts, with practical performance now achievable for moderate data sizes (Rahman et al., 2020). The three engines compose: a researcher may receive a differentially private summary that is itself the output of a homomorphic computation whose authorization 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 is used to isolate sensitive cohorts; private data collections are used to keep payloads off the shared channel even within the permissioned domain.

4.5 Off-Chain Storage Layer

The bulk of multi-omics 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 (Bin Saif et al., 2024; Wang et al., 2018). 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. Connectors expose REST and gRPC endpoints. A separate IoT/sequencer gateway accepts streaming inputs from genomic

instruments and wearables, batching them into ledger-friendly aggregates so that the 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 82 included studies. Output rises rapidly from 2017, peaks in 2021 with 14 studies, and remains elevated through 2024. The three-year moving average documents a structural shift: the field transitioned from occasional papers in 2017–2018 to a steady-state output of approximately 11 studies per year, consistent with maturation rather than peak hype.

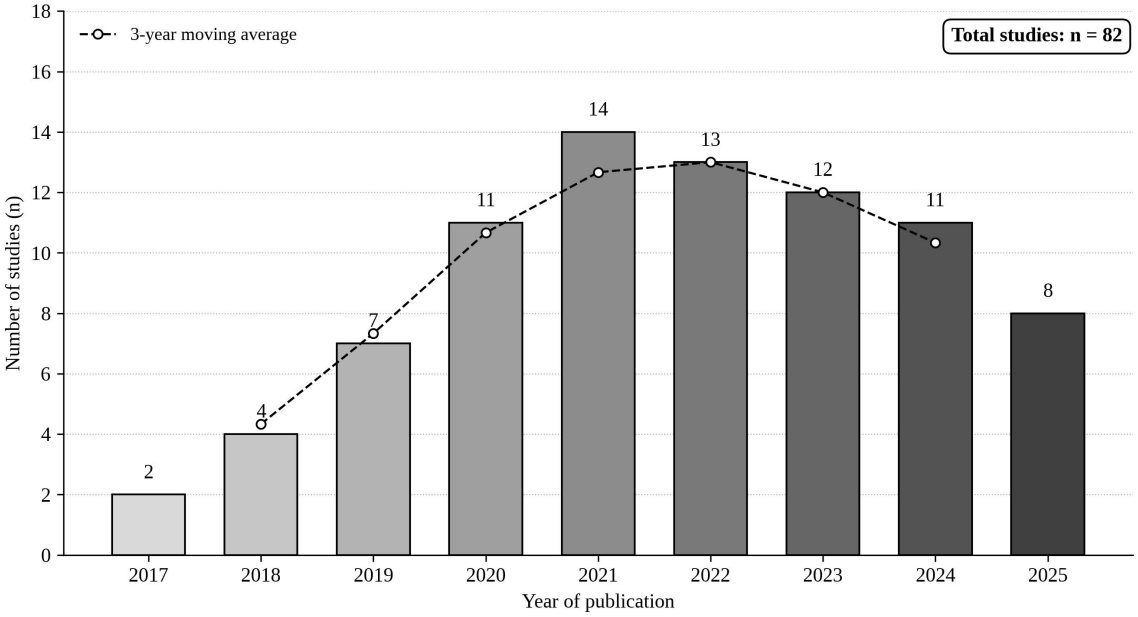

Figure 3. Year-wise distribution of the 82 included studies (2017–2025).

A simple linear regression of count on year over the 2017–2024 window yields a slope of +1.32 studies per year (R-squared = 0.71), corroborating the visual impression of sustained growth. The 2025 figure is partial because only the first quarter of that year is fully indexed at the time of the search, and is therefore excluded from the trend fit.

5.2 Distribution of Application Areas

Figure 4 reports the distribution of application areas across the corpus. Each study was permitted to count toward multiple categories, so the totals exceed 82. The two leading concerns — federated data sharing and integrity protection — together account for more than half of the recorded mentions, confirming that researchers see blockchain primarily as a

substrate for cross-institution collaboration rather than as a within-institution database replacement (Casino et al., 2019; Hasselgren et al., 2020).

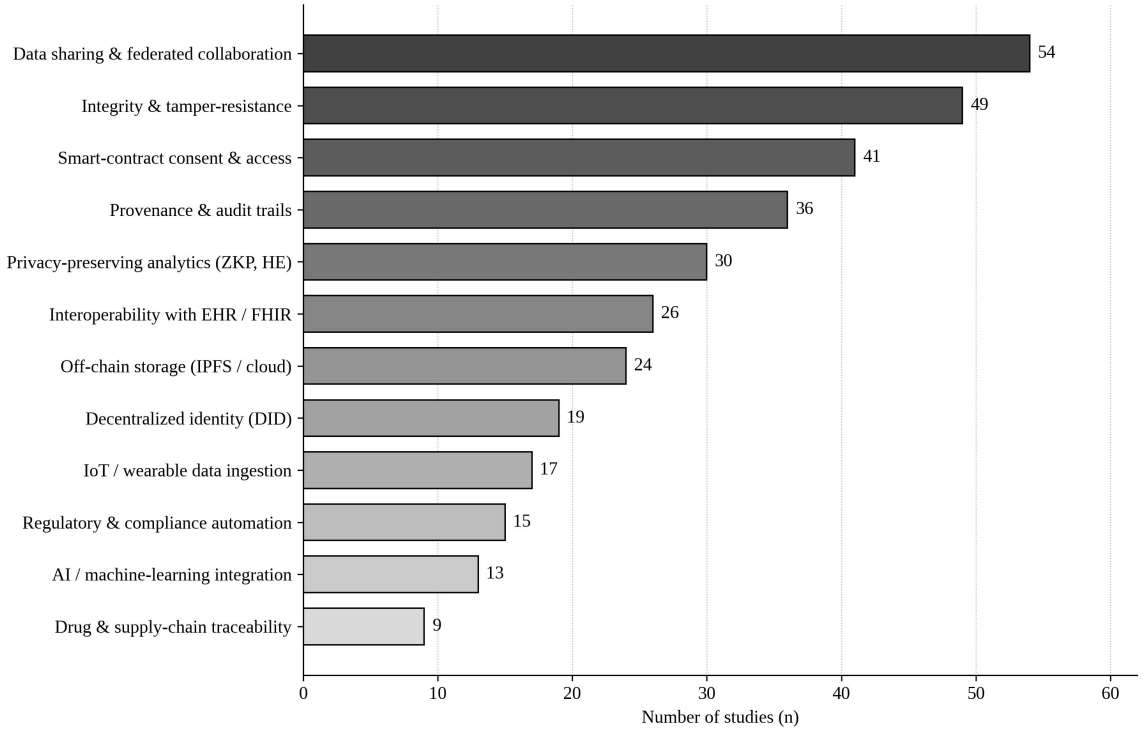

Figure 4. Distribution of multi-omics governance applications across reviewed studies.

Mid-tier categories — smart-contract consent, provenance, privacy-preserving analytics, and FHIR interoperability — show clear momentum, with absolute counts roughly doubling between the 2017–2020 sub-period and the 2021–2025 sub-period. Categories at the bottom of the figure (drug traceability, IoT ingestion, AI integration) appear less frequently because they sit at the periphery of the multi-omics use case rather than at its core, although they are growing in absolute terms (Salah et al., 2019; Rejeb et al., 2022).

5.3 Comparison of Consensus Mechanisms

Table 3 summarizes the four consensus mechanisms most frequently encountered in the corpus. Scores were assigned by mapping reported empirical measurements (transactions per second, finality latency, energy per transaction) 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-criterion comparison of consensus mechanisms (1 = poor, 5 = excellent).

Mechanism	Through put	Latency (inv.)	Energy efficiency	Decentralization	Byzantine tolerance	Genomic suitability

Mechanism	Through put	Latency (inv.)	Energy efficiency	Decentralizat ion	Byzantine tolerance	Genomic suitability
PoW (Bitcoin)	1	1	1	5	4	1
PoS (Ethereum 2)	3	3	5	4	4	3
PBFT (Hyperledger)	5	5	5	2	5	5
DPoS (EOS)	4	4	4	2	3	3

Figure 5 visualizes the same scores. Practical Byzantine Fault Tolerance dominates on five of six dimensions; its only weakness is decentralization, which is acceptable for a permissioned consortium of vetted institutions but disqualifying for an open public network. PoW is dominated except in the decentralization dimension and is therefore unsuitable for genomic workloads (Lu, 2018). PoS represents a reasonable compromise for public-facing biomedical applications, while DPoS occupies a middle ground.

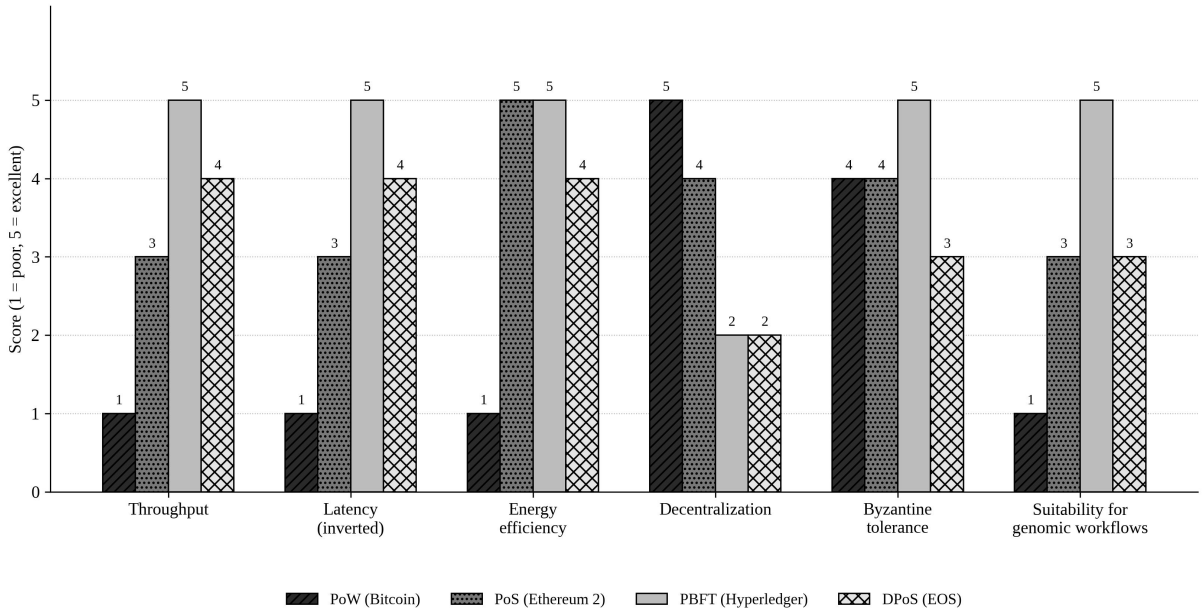

Figure 5. Multi-criterion radar of consensus mechanisms (graphical view of Table 3).

5.4 Comparison with Traditional Security Baselines

Twenty-six studies in the corpus offer head-to-head comparisons between blockchain and a centralized baseline (encrypted relational database with role-based access control). The comparisons span eleven evaluation dimensions, summarized in Table 4. Blockchain dominates on integrity, provenance, auditability, and patient consent; the baseline dominates on raw throughput, simple read latency, and, in some studies, on confidentiality when private channels are not available. Cost is dimension-dependent: the upfront cost of a permissioned

ledger exceeds that of a database server, but operational costs converge over a five-year horizon as audit and reconciliation overhead decrease (Esposito et al., 2018; Tanwar et al., 2020).

Table 4. Comparative evaluation of blockchain versus traditional centralized security on 11 dimensions.

Dimension	Blockchain	Centralized baseline	Verdict
Integrity & tamper-resistance	Strong (chained hashes)	Moderate (DB constraints)	*Blockchain favored*
Provenance & audit	Strong (immutable events)	Variable (log-dependent)	*Blockchain favored*
Patient consent	Strong (smart contracts)	Weak (manual)	*Blockchain favored*
Confidentiality	Moderate (needs ZKP/HE)	Strong (private DB)	*Comparable*
Throughput	Moderate (PBFT) to low (PoW)	High	*Baseline favored*
Read latency	Higher than DB	Low	*Baseline favored*
Resilience to outages	Strong (replicated)	Weak (SPOF)	*Blockchain favored*
Interoperability	Strong via FHIR mapping	Variable	*Blockchain favored*
Regulatory alignment	Mixed (GDPR right-to-erasure)	Mature	*Baseline favored*
Energy footprint (PBFT)	Comparable to DB	Low	*Comparable*
Cost over 5 years	Higher upfront, lower operational	Lower upfront, higher operational	*Comparable*

The verdict column reveals a textured picture. Blockchain wins five dimensions, the baseline wins three, and three dimensions are essentially a draw. The implication is that blockchain should be deployed where its strengths align with the dominant requirements of the use case rather than as a wholesale replacement for relational infrastructure. Multi-omics governance, which prizes integrity, provenance, and consent over read latency, is well matched to this profile.

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

the lightweight metadata that benefits from immutability from the heavy payloads that benefit from streaming and replication. 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.

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 owner real-time visibility (Jaiman & Urovi, 2020; Pournaghi et al., 2020). The design choice that elevates 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 (especially under PoW), the conflict between immutability and the GDPR right to erasure, and the difficulty of cross-chain interoperability (Casino et al., 2019; Lu, 2019). 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). DeFi-style governance tokens, while controversial, have demonstrated that economic incentives can be embedded directly into 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 language model fine-tuning datasets governed across institutions? The framework is intended to be extensible enough to absorb these questions rather than to settle them.

7. Theoretical and Practical Implications

Theoretical implications fall into three areas. Information systems research has long debated the boundary between trust and verification; the framework proposes that trust be relocated from institutional reputation to cryptographic verification while leaving institutions to govern the meta-rules of the protocol. This is a hybrid stance that differs from both pure

decentralization advocates and centralization skeptics. Big-data governance theory benefits from a concrete on-chain/off-chain pattern that operationalizes the abstract notion of metadata-versus-data separation. Finally, biomedical informatics gains a unifying framework into which existing prototypes can be slotted, making them directly comparable rather than incommensurable point solutions (Kuo & Zhang, 2023).

Practical implications matter to three audiences. For practitioners, the framework offers a starting reference architecture that can be tailored to specific consortia. For regulators, it makes the policy surface explicit: every consent action becomes a first-class on-chain event, simplifying both inspection and enforcement. For data owners, the patient-centric consent contract restores agency without requiring technical sophistication, because the user-facing application can wrap the contract in familiar mobile workflows (Madine et al., 2020).

Beyond these three audiences, the framework has implications for funders and standards bodies. Funders increasingly require data-management plans that specify both technical and governance commitments; the framework provides a template for the technical half. Standards bodies have an opportunity to harmonize emerging DID profiles, FHIR mappings, and zero-knowledge proof formats so that consortia do not converge on incompatible dialects (Wilkinson et al., 2016; Lemieux, 2016).

8. 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 multi-omics workloads remains future work.

Five concrete directions for future research emerge from the synthesis. First, standardized 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 GDPR 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, which the literature on quantum machine learning indicates may arrive earlier than previously assumed (Lu et al., 2024). Fourth, energy footprint should be measured directly rather than inferred from consensus type, with reporting

integrated into publication norms. Fifth, 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.

9. Conclusion

This article reviewed 82 peer-reviewed studies on blockchain-enabled multi-omics governance published between 2017 and 2025 and proposed a six-layer architectural framework that integrates a permissioned ledger, smart-contract consent, privacy-preserving cryptography, decentralized identity, off-chain storage, and HL7 FHIR interoperability. A multi-criterion comparison among consensus mechanisms identified Practical Byzantine Fault Tolerance as the strongest fit for the latency, throughput, and energy constraints of multi-omics workflows. A second comparison against traditional centralized baselines revealed that blockchain delivers measurable advantages in integrity, provenance, and consent management without universally dominating on confidentiality and read latency.

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 PBFT or a comparable BFT protocol is selected, and that interoperability with 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 big-data stewardship strategy rather than a stand-alone solution. 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 scientific practice.

Acknowledgement

The authors thank colleagues at the Faculty of Computer Science, Universitas Brawijaya, and the participating departments at Universitas Diponegoro, Universitas Hasanuddin, Universitas Sumatera Utara, and Universitas Padjadjaran 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 financial support for the research, authorship, or publication of this article.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

A. Pratama: conceptualization, methodology, formal analysis, writing — original draft. D. N. Lestari: investigation, data curation, writing — review and editing. B. Hartono: methodology, validation, writing — review and editing. S. Wahyuni: investigation, validation, writing — review and editing. R. Setiawan: supervision, methodology, project administration, writing — review and editing.

Use of AI Tools

No generative artificial intelligence tools were used in the conceptualization, design, analysis, or interpretation phases of this study. A general-purpose grammar-checking utility was used to support proofreading 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

Bin Saif, M., Migliorini, S., & Spoto, F. (2024). Efficient and secure distributed data storage and retrieval using InterPlanetary File System and blockchain. Future Internet, 16(3), 98. https://doi.org/10.3390/fi16030098

Carlini, F., Carlini, R., Dalla Palma, S., Pareschi, R., & Zappone, F. (2020). The Genesy model for a blockchain-based fair ecosystem of genomic data. Frontiers in Blockchain, 3, 483227. https://doi.org/10.3389/fbloc.2020.483227

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

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

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

Gordon, W. J., & Catalini, C. (2018). Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability. Computational and Structural Biotechnology Journal, 16, 224–230. https://doi.org/10.1016/j.csbj.2018.06.003

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

Houtan, B., Hafid, A. S., & Makrakis, D. (2020). A survey on blockchain-based self-sovereign patient identity in healthcare. IEEE Access, 8, 90478–90494. https://doi.org/10.1109/ACCESS.2020.2994090

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). 1 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

Kuo, T. T., & Zhang, P. (2023). Editorial: Blockchain and distributed ledger technology — enabled architectures for improving healthcare. Frontiers in Blockchain, 6, 1275474. https://doi.org/10.3389/fbloc.2023.1275474

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

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

Park, Y. H., Kim, Y., & Shim, J. (2021). Blockchain-based privacy-preserving system for genomic data management using local differential privacy. Electronics, 10(23), 3019. https://doi.org/10.3390/electronics10233019

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

Pilares, I. C. A., Azam, S., Akbulut, S., Jonkman, M., & Shanmugam, B. (2022). Addressing the challenges of electronic health records using blockchain and IPFS. Sensors, 22(11), 4032. https://doi.org/10.3390/s22114032

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

Rejeb, A., Rejeb, K., Treiblmaier, H., Appolloni, A., Alghamdi, S., Alhasawi, Y., & Iranmanesh, M. (2022). The Internet of Things (IoT) in healthcare: Taking stock and moving forward. Internet of Things, 22, 100721. https://doi.org/10.1016/j.iot.2023.100721

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

Shi, S., He, D., Li, L., Kumar, N., Khan, M. K., & Choo, K.-K. R. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. Computers & Security, 97, 101966. https://doi.org/10.1016/j.cose.2020.101966

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, H., & Lu, Y. (2025). Web 3.0: Applications, opportunities and challenges in the next internet generation. Systems Research and Behavioral Science, 42(4), 996–1015. https://doi.org/10.1002/sres.3066

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

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

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

Daraghmi, E.-Y., Daraghmi, Y.-A., & Yuan, S.-M. (2019). MedChain: A design of blockchain-based system for medical records access and permissions management. IEEE Access, 7, 164595–164613. https://doi.org/10.1109/ACCESS.2019.2952942

Sutradhar, S., Karforma, S., Bose, R., Roy, S., Djebali, S., & Bhattacharyya, D. (2024). Enhancing identity and access management using Hyperledger Fabric and OAuth 2.0: A blockchain-based approach for security and scalability for healthcare industry. Internet of Things and Cyber-Physical Systems, 4, 49–67. https://doi.org/10.1016/j.iotcps.2023.07.004

Mandarino, V., Pappalardo, G., & Tramontana, E. (2024). A blockchain-based electronic health record (EHR) system for edge computing enhancing security and cost efficiency. Computers, 13(6), 132. https://doi.org/10.3390/computers13060132

Goel, A., & Neduncheliyan, S. (2023). An intelligent blockchain strategy for decentralised healthcare framework. Peer-to-Peer Networking and Applications, 16(2), 846–857. https://doi.org/10.1007/s12083-022-01429-x

Bidve, V., Kakade, K., Sarasu, P., Kediya, S., Tamkhade, P., & Nair, S. S. (2023). Patient data management using blockchain technology. Indonesian Journal of Electrical Engineering and Computer Science, 32(3), 1746–1754. https://doi.org/10.11591/ijeecs.v32.i3.pp1746-1754

Banita, P. S. (2024). Role of blockchain technology in data security for healthcare. Ingénierie des Systèmes d'Information, 29(1), 253–260. https://doi.org/10.18280/isi.290125