Acta Informatica Pragensia
2026, Volume 15, Issue 2, 566–592
https://doi.org/10.18267/j.aip.312

PRAGUE UNIVERSITY OF ECONOMICS AND BUSINESS

Review Open Access

Blockchain in Bioinformatics Data Security: Systematic Evidence, Research Gaps and Pathways Forward

Dennis Opoku Boadu [1], **Fredrick Boafo** [2], **Kwabena Owusu-Mensah** [1], **Michael Kwakye** [3], **Isaac Osei** [4]

[1] Department of Computer Science, University of Ghana, Accra, Ghana
[2] Department of Computer Science, Lancaster University Ghana, Accra, Ghana
[3] Ghana Christian University College, Amranhia, Ghana
[4] Department of Computer Science and Engineering, SRM University–AP, Andhra Pradesh, India

Corresponding author: Dennis Opoku Boadu (doboadu@st.ug.edu.gh)

Editorial Record

First submission received:
November 11, 2025

Revisions received:
December 16, 2025
February 21, 2026
March 11, 2026

Accepted for publication:
March 11, 2026

Academic Editor:
Zdenek Smutny
Prague University of Economics and Business, Czech Republic

This article was accepted for publication by the Academic Editor upon evaluation of the reviewers' comments.

How to cite this article:
Boadu, D. O., Boafo, F., Owusu-Mensah, K., Kwakye, M., & Osei, I. (2026). Blockchain in Bioinformatics Data Security: Systematic Evidence, Research Gaps and Pathways Forward. *Acta Informatica Pragensia*, 15(2), 566–592. https://doi.org/10.18267/j.aip.312

Abstract

Background: The growth of high-throughput sequencing and multi-omics research has intensified the need for secure, interoperable and transparent data management infrastructures. Blockchain technology has been widely proposed as a potential solution; however, its feasibility, empirical maturity and comparative performance in bioinformatics remain unclear.

Objective: This systematic review analyses blockchain applications in bioinformatics, highlighting claimed security and governance benefits, comparing them with traditional data security approaches, discussing implementation challenges and assessing the empirical rigor of existing studies using a structured quality assessment framework.

Methods: This overview was conducted using Scopus, ScienceDirect, IEEE Xplore, ACM Digital Library and SpringerLink for publications from 2014 to 2024. Search strings combined blockchain, bioinformatics and security-related terms. Sixty-five studies met the inclusion criteria. Each study was evaluated using five equally weighted quality dimensions: application specificity, clarity of benefits, empirical evaluation, challenge articulation and reproducibility.

Results: Most studies focused on blockchain use cases in genomic data sharing, provenance tracking and access control, with a strong emphasis on conceptual benefits such as immutability and auditability. Fewer studies provided empirical evaluations or direct comparisons with traditional security mechanisms. Quality assessment results revealed a predominance of conceptual and prototype-level contributions; over half of the studies lacked empirical benchmarking and reproducibility was frequently limited. Heterogeneity in blockchain architectures and the absence of standardized genomic benchmarking environments hindered cross-study comparison. No study demonstrated deployment within a production-scale genomic pipeline.

Conclusion: Blockchain demonstrates conceptual potential for enhancing provenance, decentralized governance and tamper-resistant auditing in bioinformatics data management. However, empirical validation remains limited and significant technical, regulatory and organizational challenges persist. The current evidence base is insufficient to support large-scale adoption. Future research should prioritize benchmarking using realistic genomic workloads, hybrid architectures that integrate off-chain storage, consent-aware governance models and alignment with regulatory frameworks such as GDPR and HIPAA.

Index Terms

Blockchain; Bioinformatics; Genomic data security; Privacy; Interoperability; Benchmarking; GDPR compliance.

1 INTRODUCTION

The exponential growth of bioinformatics data, driven by high-throughput sequencing and large-scale genomic studies, has created urgent demand for robust, reliable data security architectures. Conventional centralized storage systems provide basic access control and encryption but struggle to guarantee integrity, provenance, verifiability and transparent auditability across distributed and collaborative scientific ecosystems. These systems are prone to breaches, lack end-to-end auditability and often fail to ensure tamper resistance in distributed environments (Amin et al., 2021; Lu et al., 2021). Given the critical role of bioinformatics in medicine, drug discovery and personalized healthcare, weaknesses in data security directly translate into substantial risks, including privacy violations, identity theft and loss of intellectual property (Arvind et al., 2023; Sohail et al., 2024).

Blockchain technology, characterized by its decentralized, immutable and transparent ledger, represents a potentially transformative alternative in various domains. Prior research has illuminated its capacity to enhance traceability, ensure data integrity and foster trust in biomedical data transactions (Bin Saif et al., 2024; Litoussi et al., 2023; Shi et al., 2020). Despite these promising attributes, existing methodologies remain disjointed and predominantly exploratory. Current applications of blockchain technology often focus on narrow contexts, such as electronic health records or isolated genomic datasets, and fail to adequately address the distinctive computational and infrastructural demands of large-scale bioinformatics workflows (Kuo & Zhang, 2023). Furthermore, many implementations neglect critical use cases, including secure provenance tracking for variant calling, collaborative efforts on multi-omics data and safeguarding intermediate states within genomic workflows that inherently require specific attention to mutability and scalability. Ongoing challenges related to scalability, energy consumption and the integration of blockchain solutions with legacy systems further impede their practical adoption in real-world settings (Saputra & Setiawan, 2023).

While the literature on blockchain for health and biomedical data is expanding, a clear, domain-specific synthesis in bioinformatics remains lacking. Most studies emphasize conceptual benefits but fall short of systematically comparing blockchain-based solutions with traditional security methods in areas such as data integrity, traceability, access control and regulatory compliance (Dursi et al., 2021; Park et al., 2021). There is also insufficient analysis of limitations of blockchain, including computational overhead, interoperability constraints and its suitability for genomic-scale data (Jia et al., 2024; Zass et al., 2023). The absence of rigorous comparative evaluations hinders stakeholders' ability to assess the feasibility, costs and operational performance of blockchain-based solutions, thereby slowing their adoption in practice.

Although blockchain has been widely discussed in healthcare, bioinformatics poses unique challenges that are not present in traditional clinical workflows. Genomic pipelines require mutable preprocessing, high-performance computing scale, dynamic consent handling and multi-omics integration properties that are fundamentally misaligned with the append-only structure and replication overhead of blockchain. This distinction is often overlooked in literature, resulting in conceptual claims that do not translate into practical genomic contexts. Moreover, comparative analyses with traditional security models remain limited because most blockchain proposals exist only as prototypes and lack standardized benchmarking environments, reproducible genomic datasets or performance metrics tailored to high-volume sequencing workflows.

Therefore, this paper addresses these gaps by critically examining how blockchain technology is being applied to enhance the security and management of bioinformatics data. Specifically, it:

1. synthesizes current blockchain applications in bioinformatics, including genomic data sharing, health data repositories and clinical trial management (S. Chen et al., 2021; Nguyen et al., 2019);
2. provides a comparative analysis of blockchain versus traditional security approaches, highlighting benefits and drawbacks (Al-Aamri et al., 2023; Verma et al., 2023);
3. identifies unresolved challenges such as scalability, energy requirements and integration barriers that must be addressed for sustainable adoption (Hosseini et al., 2019; Park et al., 2021); and
4. outlines future research directions and design considerations for effective blockchain deployment in bioinformatics (Agbo & Mahmoud, 2019; Gomes et al., 2024).

The remainder of this paper is structured as follows: Section 2 reviews related literature, Section 3 describes the review methodology, Section 4 presents the results, Section 5 discusses implications and limitations, and Section 6 concludes the paper.

2 RELATED WORKS

Blockchain technology has garnered significant attention as a potential solution for improving the security, integrity and accessibility of biomedical and bioinformatics data. Existing literature can be categorized into three primary themes: genomic data sharing, secure data management and privacy/access control. Collectively, these areas demonstrate the growing applicability of blockchain in these fields and highlight a fragmented research landscape that calls for a comparative synthesis to assess its implications for genomic-scale workflows. This synthesis is crucial for identifying best practices and guiding future research towards more cohesive and effective applications of blockchain technology in biomedicine.

2.1 Blockchain for genomic data sharing

Amin et al. (2021) highlighted the potential of blockchain technology to mitigate risks associated with data manipulation and leakage in centralized repositories. While these studies illustrate how blockchain can facilitate democratized access to genomic data, they often fail to address significant challenges, including scalability, interoperability and integration with existing bioinformatics infrastructure. Furthermore, prevailing data sharing models tend to focus on mechanisms for exchanging data rather than on downstream computational processes, including sequence alignment, variant calling and multi-omics integration, which can be particularly bottleneck-prone.

2.2 Blockchain-based secure data management

The exploration of blockchain technology for managing and protecting large-scale biological datasets highlights its potential for secure data exchange. Key studies, including Hosseini et al. (2019), have examined various cryptographic techniques within blockchain frameworks, such as authenticated encryption, to uphold confidentiality and integrity. For instance, recent research by Verma et al. (2023) emphasized how the intrinsic properties of transparency and immutability of blockchain can significantly enhance trustworthiness in healthcare and bioinformatics. Similarly, Agbo & Mahmoud (2019) underscored the transformative role of smart contracts in automating access control to sensitive data. Despite these promising insights, the practical deployment of blockchain in handling the vast, heterogeneous and high-volume datasets characteristic of bioinformatics remains inadequately assessed (Jia et al., 2024). Comparative analyses across the existing literature frequently reveal discrepancies in the evaluation of scalability and interoperability. Many studies overlook the computational realities inherent in genomic workflows, which often handle terabytes to petabytes of data.

The integration of blockchain methodologies with federated genomic analysis platforms and distributed computing systems remains a significant challenge in bioinformatics (Ni et al., 2025). Current frameworks often overlook the incorporation of vital privacy-preserving cryptographic techniques, such as homomorphic encryption and secure multi-party computation (Damar et al., 2025). These techniques are essential for ensuring data confidentiality and security, which are paramount in handling sensitive genomic information. Furthermore, the consensus mechanisms inherent in blockchain can introduce latency and replication overhead, presenting additional obstacles. This latency often conflicts with the requirements of workflow phases that require mutable intermediate states or rapid, iterative computations. As such, the potential applications of blockchain technology in bioinformatics become increasingly complex and necessitate further exploration to address these limitations effectively (Mudannayake et al., 2025). Overall, for blockchain to achieve successful real-world implementation in bioinformatics, it must evolve to incorporate essential privacy-preserving techniques and minimize the adverse effects of consensus processes on computational workflows.

2.3 Privacy and access control

A complementary strand of research has focused on privacy preservation and access governance in bioinformatics. Nguyen et al. (2019) demonstrated how blockchain technology enables secure sharing of electronic health records (EHRs) while preserving patient privacy. Similarly, S. Chen et al. (2021) emphasized the capacity of blockchain to enforce accountability through the traceability of all data access and modifications. These frameworks enhance trust and regulatory compliance; however, they rarely integrate with bioinformatics-specific pipelines, including genome annotation, proteomics and clinical genomics (Johnston et al., 2022; Zhu et al., 2024). Furthermore, privacy-centric models tend to prioritize transactional access control over high-performance computational environments, such as

high-performance computing (HPC) clusters and distributed multi-omics platforms, which process genomic data. This oversight contributes to a widening gap between conceptual design and operational requirements.

Current research highlights the potential of blockchain technology to improve transparency, traceability and security within biomedical data ecosystems. However, many studies are isolated, often focusing on specific use cases rather than providing a comprehensive, comparative framework for bioinformatics. There are ongoing challenges, including scalability, energy consumption, interoperability and insufficient integration with high-performance genomic workflows, that impede practical adoption. Additionally, some studies focus on EHRs, general medical data sharing or overarching security concepts, whereas there is little emphasis on specialized tasks such as genomic sequencing pipelines, multi-omics integration, federated analysis and long-term data stewardship. Many reviews in this area rely on narrative synthesis rather than structured evidence mapping or systematic quality assessments.

In contrast, the present study explicitly focuses on bioinformatics and genomic data security, using a transparent PRISMA-guided selection process[1]. It employs a quality assessment framework aligned with five research questions to quantify the scarcity of empirically grounded studies and comparative evaluations. This review offers an evidence-driven perspective that aligns with the computational and interoperability demands outlined in the Introduction, thereby laying the foundation for more domain-specific blockchain solutions.

2.4 Uniqueness and contribution of this review

Blockchain technology has increasingly attracted attention in academic research related to healthcare and biomedical data management. This growing interest has resulted in the publication of several systematic literature reviews and surveys. However, upon close examination of this body of literature, it becomes apparent that most reviews have focused primarily on healthcare information systems and data sharing, rather than treating bioinformatics as a distinct computational and analytical discipline. Consequently, there is currently no systematic review that would offer an evidence-weighted, quality-assessed synthesis of blockchain applications specifically aligned with bioinformatics workflows, including genomic sequencing, variant calling and multi-omics analysis.

Several systematic reviews have focused on blockchain adoption and security within healthcare settings. For example, Tandon et al. (2020) conducted a systematic literature review examining blockchain applications across healthcare information systems, including EHRs, clinical data exchange and hospital operations. Their analysis synthesized reported benefits, challenges and future research directions, but did not distinguish between clinical record management and bioinformatics pipelines that involve large-scale computation and iterative data processing. Similarly, Saeed et al. (2022) reviewed blockchain technology in healthcare with an emphasis on privacy, integrity and interoperability, yet their scope remained centred on healthcare data management rather than computational bioinformatics workflows.

A smaller number of reviews have acknowledged genomic or biomedical data contexts, although their focus has remained limited. Dedeturk et al. (2021) reviewed blockchain applications in genomics and healthcare, primarily classifying data sharing platforms and identifying open issues related to privacy and governance. While their review recognized the sensitivity and scale of genomic data, it did not systematically evaluate blockchain performance, scalability or empirical maturity within end-to-end bioinformatics pipelines.

Across these reviews, several methodological and conceptual limitations are evident. Existing surveys have not isolated bioinformatics workflows as a distinct class of systems with unique computational, storage and regulatory constraints. Moreover, none of the identified reviews have applied a structured quality assessment framework to evaluate empirical rigour, benchmarking practices or reproducibility across studies. Comparative analysis between blockchain-based approaches and traditional bioinformatics security mechanisms has also been largely absent, limiting the ability of prior reviews to assess practical feasibility and performance trade-offs.

The present study addresses these limitations by presenting a systematic literature review focused explicitly on bioinformatics data security. Unlike existing reviews, it evaluates blockchain studies using a structured, multi-dimensional quality assessment framework, systematically examines empirical and comparative evidence and synthesizes findings across applications, benefits, challenges and methodological maturity. By grounding its

[1] See, https://www.prisma-statement.org/

analysis in transparent evidence assessment rather than narrative aggregation, this review provides a domain-specific, methodologically rigorous reference for researchers and practitioners evaluating the suitability of blockchain for modern bioinformatics infrastructure.

3 METHODOLOGY

This study adopts a systematic literature review approach, following the guidelines proposed by Kitchenham et al. (2009) for evidence-based software engineering reviews. The objective is to ensure transparency, reproducibility and methodological rigour in identifying, screening and synthesizing research into blockchain applications in bioinformatics data security. The review process comprises eight stages: (1) research objectives and questions, (2) quality assessment framework, (3) database selection, (4) search strategy, (5) inclusion and exclusion criteria, (6) search and filtering outcomes, (7) data extraction and (8) threats to validity.

3.1 Research objectives and questions

This systematic literature review aims to critically evaluate the state of research into blockchain in bioinformatics and genomic data security. The review is designed to move beyond conceptual claims by systematically examining how blockchain has been applied, the benefits asserted, the limitations reported and the extent to which existing studies have provided empirical, reproducible evidence. To achieve this, the review adopts clearly defined research objectives and a structured quality assessment framework that guides study selection, data extraction and synthesis.

3.1.1 Research objectives

The review pursues five interrelated objectives:

1. To identify and classify existing blockchain applications in bioinformatics, with a particular emphasis on genomic and multi-omics data management.
2. To analyse the security, governance and interoperability benefits claimed for blockchain-based bioinformatics systems.
3. To evaluate the extent to which blockchain-based approaches compare with traditional data security and data management methods.
4. To synthesize the technical, regulatory and organizational challenges associated with blockchain adoption in bioinformatics.
5. To assess the empirical rigour, effectiveness and reproducibility of existing blockchain-based bioinformatics studies.

These objectives collectively frame the scope of the review and ensure that evidence is evaluated not only for conceptual relevance but also for methodological robustness and practical feasibility.

3.1.2 Research questions

To operationalize the above objectives within a systematic review framework, five research questions (RQ1–RQ5) were formulated. The research questions guide the screening process, data extraction and subsequent analysis, ensuring transparency and reproducibility in the review methodology.

RQ1: What types of blockchain applications have been proposed or implemented for bioinformatics and genomic data management?

RQ2: What benefits are claimed for using blockchain in bioinformatics data security and governance?

RQ3: How do blockchain-based approaches compare with traditional security and data management methods in bioinformatics?

RQ4: What challenges and limitations are reported in the implementation of blockchain for bioinformatics data?

RQ5: To what extent do existing studies empirically demonstrate the effectiveness and reproducibility of blockchain-based bioinformatics solutions?

The research questions are introduced at this stage to ensure they inform the methodological design of the review rather than being imposed retroactively during interpretation.

3.2 Quality assessment framework

To systematically evaluate the quality and maturity of the included studies, a structured quality assessment (QA) framework was applied. The QA framework is explicitly aligned with the research objectives and research questions and serves as a core component of the methodology rather than a post-hoc evaluative tool.

Each included study was assessed across five quality dimensions:

- **QA1** – Domain specificity: whether the study clearly defines a bioinformatics or genomics-related use case and explains how blockchain is applied in that context (aligned with RQ1).
- **QA2** – Articulation of benefits: whether the study explicitly states and motivates the intended benefits of using blockchain for bioinformatics data security and management (aligned with RQ2).
- **QA3** – Empirical evaluation and comparison: whether the study provides empirical evaluation, benchmarking or comparison with traditional security or data management approaches (aligned with RQ3).
- **QA4** – Challenges and limitations: whether the study discusses technical, regulatory or organizational challenges associated with blockchain adoption in bioinformatics (aligned with RQ4).
- **QA5** – Reproducibility and technical transparency: whether sufficient technical detail is provided to support understanding, validation or reuse of the proposed approach (aligned with RQ5).

All five QA criteria were weighted equally to avoid bias towards either conceptual or experimental studies and to provide a balanced assessment of evidence quality. Scoring decisions are based on explicit criteria defined prior to analysis, ensuring consistency across the review.

3.2.1 Quality assessment checklist

To assess the robustness and relevance of included studies, we applied five QA criteria, each scored as 1 ("criterion met") or 0 ("criterion not met"). These criteria are deliberately aligned with the research questions. Each paper received a QA score ranging from 0 to 5. Only studies with a total QA score ≥ 1 and a clear focus on blockchain-based mechanisms for bioinformatics or closely related biomedical data security were retained in the final synthesis.

To ensure methodological rigour, a structured quality assessment checklist was applied to all candidate studies, adapted from Kitchenham et al. (2009). The five quality assessment questions (QA1–QA5) align with the research questions and were assessed based on the following:

- clarity of application domain,
- articulation of benefits,
- empirical evaluation,
- discussion of challenges,
- reproducibility.

All five QA criteria were weighted equally because each captures a distinct, non-overlapping dimension of study quality: domain relevance, benefit clarity, empirical evaluation, challenge articulation and reproducibility. Differential weighting would bias the assessment towards specific study types. Equal weighting provides a neutral, standardized scoring framework.

3.2.2 Disagreement resolution procedure

Although the primary screening and scoring were conducted by a single reviewer, all borderline or ambiguous scoring decisions were subjected to a secondary verification process. For each such case, the reviewer performed a second independent pass using the predefined QA criteria and cross-checked it against evidence extracted from the full text of the study. When uncertainty persisted, a conservative scoring strategy was adopted to avoid overestimating study quality. This procedure ensured internal consistency and mitigated the risk of subjective bias highlighted in the review.

3.2.3 Distribution of scores

Studies that scored 0 across all five QA criteria were excluded from the final synthesis, as they did not provide sufficient technical, methodological or conceptual substance for evidence-based analysis. Consequently, the QA Table A1 (in Appendix A) contains only the 65 included studies with a total QA score of 1 or higher. Duplicate entries and overlapping publications from the same project were merged and counted once to avoid inflating evidence.

External validity is limited because most included studies represent controlled prototypes rather than operational systems. As a result, findings may not generalize to production-scale genomics environments. Furthermore, excluding paywalled or industry-implemented blockchain solutions may underrepresent state-of-the-art systems not published in academic venues.

Furthermore, excluding paywalled studies introduces an unavoidable selection bias. Industry-led blockchain deployments in genomics and biomedical data management are disproportionately unpublished or available only through proprietary documentation. These systems may include advanced architectural features, performance optimizations or compliance models that are not represented in academic literature. Their omission may lead the present review to underestimate the maturity of operational blockchain systems and overrepresent early-stage academic prototypes.

3.3 Database selection

To minimize disciplinary blind spots and reduce selection bias, five major digital libraries were selected: Scopus, ScienceDirect, IEEE Xplore, ACM Digital Library and SpringerLink. These databases collectively index high-quality journals and conference proceedings across computer science, biomedical sciences and interdisciplinary technological fields. By drawing on both engineering and biomedical repositories, the review ensured a balanced, representative sample of relevant literature.

Non-English studies were excluded because inconsistent translation of domain-specific terminology (e.g., genomic workflows, cryptographic primitives, consensus mechanisms, privacy models) introduces interpretation bias and undermines the replicability of quality assessment. Restricting the corpus to English-language publications, therefore, standardizes conceptual meaning and reduces the risk of methodological distortion. Paywalled studies without institutional access were also excluded, as full-text review was essential for methodological evaluation; relying solely on abstracts would have introduced systematic bias into the analysis.

Databases such as PubMed and Web of Science were not used as primary sources because preliminary scoping searches showed substantial overlap with Scopus-indexed biomedical literature and limited coverage of computer science conference proceedings, which are central to blockchain research. Google Scholar was excluded due to its lack of transparent indexing criteria and limited support for reproducible systematic review filtering.

3.4 Search strategy

Search strings were constructed using combinations of key terms related to blockchain, bioinformatics, genomics and biomedical data security. Boolean operators were applied to maximize the retrieval of relevant literature. Representative search phrases included:

Scopus (advanced search)

> TITLE-ABS-KEY (“blockchain” AND (“bioinformatics” OR “genomic data” OR “genomics” OR “biomedical data”) AND (“security” OR “privacy” OR “integrity” OR “provenance”)) AND PUBYEAR > 2013 AND PUBYEAR < 2025

IEEE Xplore

> (“blockchain” AND (“genomic” OR “bioinformatics” OR “biomedical”)) AND (“security” OR “privacy” OR “integrity” OR “access control”) AND (Publication Year: 2014–2024)

ACM Digital Library (advanced query)

> +(blockchain) AND + (bioinformatics OR genomics OR “genomic data” OR “biomedical data”) AND + (security OR privacy OR integrity OR provenance) AND publicationDate: [2014 to 2024]

ScienceDirect

(blockchain AND ("bioinformatics" OR "genomic data" OR "biomedical data") AND ("security" OR "privacy" OR "integrity" OR "access control") AND (2014–2024))

SpringerLink

"blockchain" AND ("bioinformatics" OR "genomic data" OR "biomedical data") AND ("security" OR "privacy" OR "integrity" OR "provenance")

The search was restricted to the period 2014–2024 to capture developments in blockchain technology beyond its origins in cryptocurrency. Subject areas were limited to computer science, medicine, immunology and microbiology. Search queries were adapted to the syntax of each database to ensure optimal recall and precision.

3.5 Inclusion and exclusion criteria

Studies were screened using explicit inclusion and exclusion criteria (Table 1). These criteria ensured that only studies directly relevant to the research questions were included.

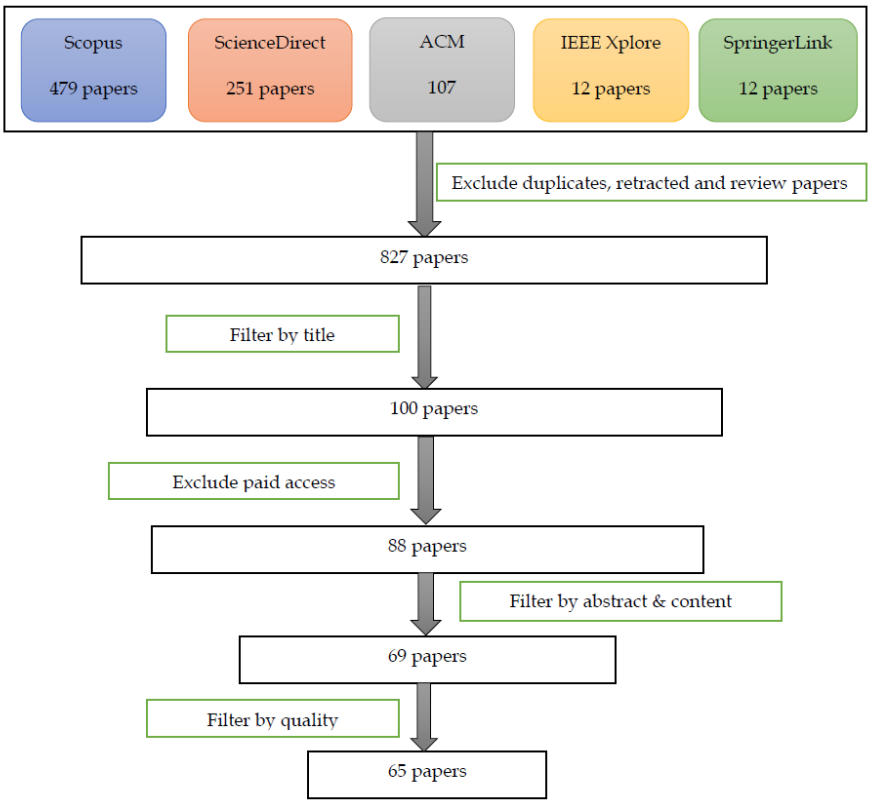

Figure 1. *Search and filtering processes – flow diagram.*

In addition to these criteria, papers that did not address the research questions were excluded during full-text screening. The filtering process illustrated in Figure 1 ensured that only studies aligned with the review objectives were retained. The inclusion/exclusion criteria were tied directly to the research questions (RQ1–RQ5), ensuring methodological consistency.

Table 1. *Inclusion and exclusion criteria.*

Search engine	Link	Inclusion	Exclusion
Scopus	https://www.scopus.com/search/form.uri?display=advanced	Articles published between 2014–2024	Non-English articles
ScienceDirect	https://www.sciencedirect.com/search/entry	Computer science and biomedical subject areas	Non–peer-reviewed articles

Search engine	Link	Inclusion	Exclusion
ACM	https://dl.acm.org/search/advanced	Papers addressing the research questions and discussing blockchain applications to biological data	Paywalled articles
IEEE Xplore	https://ieeexplore.ieee.org/search/advanced	Only final published papers	Documents that are not full papers
SpringerLink	https://link.springer.com	Peer-reviewed publications	Names, affiliations, editors and reviewers not considered

3.6 Search and filtering outcomes

Search and filtering outcomes:

- 861 records retrieved;
- 34 duplicates removed (827 unique records);
- 758 excluded by title/abstract;
- 69 full texts reviewed;
- 65 included in final synthesis.

3.6.1 Database selection and justification

Five electronic databases were selected to ensure comprehensive coverage across computer science, bioinformatics and biomedical research:

- Scopus was chosen for its broad multidisciplinary coverage and citation indexing, enabling identification of high-impact and cross-domain studies.
- IEEE Xplore and the ACM Digital Library were included to capture blockchain research originating from computer science and engineering communities, where most blockchain architectures and protocols are published.
- ScienceDirect and SpringerLink were selected to ensure coverage of biomedical, bioinformatics and interdisciplinary journals not comprehensively indexed in engineering-focused databases.

The combination of these databases minimizes disciplinary bias and balances technical blockchain literature with domain-specific bioinformatics research. Other databases were not included where they offered substantial overlap or limited relevance to blockchain or bioinformatics security. This selection strategy aligns with best practices for systematic reviews in interdisciplinary fields.

3.7 Data extraction and synthesis

For each included study, data were systematically extracted using a standardized template, covering:

- bibliographic details (author(s), year, source);
- application domain (e.g., genomic data, EHR, clinical trials);
- blockchain features (immutability, decentralization, cryptography, smart contracts);
- reported benefits (traceability, privacy, integrity, access control);
- reported challenges (scalability, computational cost, interoperability); and
- gaps identified (e.g., lack of real-world validation, limited comparative analysis).

The extracted data were synthesized thematically into four categories:

1. genomic data sharing and control;
2. secure data management and storage;
3. privacy, access control and compliance; and
4. comparisons with traditional security methods.

A comparative analysis was conducted to contrast blockchain-based approaches with traditional security techniques, highlighting their strengths, weaknesses and unresolved challenges. All findings were mapped back to the research questions (RQ1–RQ5).

We used JabRef to organize and refine the dataset. JabRef automatically detected duplicates using DOI, title similarity and metadata matching, while borderline cases such as preprint and extended conference versions were manually verified. Filtering functions enabled tagging of each record as "included", "excluded", "full-text required" or "pending QA review", thereby maintaining a transparent audit trail. Table 2 shows the years of publication of the research projects considered.

Table 2. *Years of publication.*

Total	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
65	0	0	0	0	2	5	11	15	12	11	9

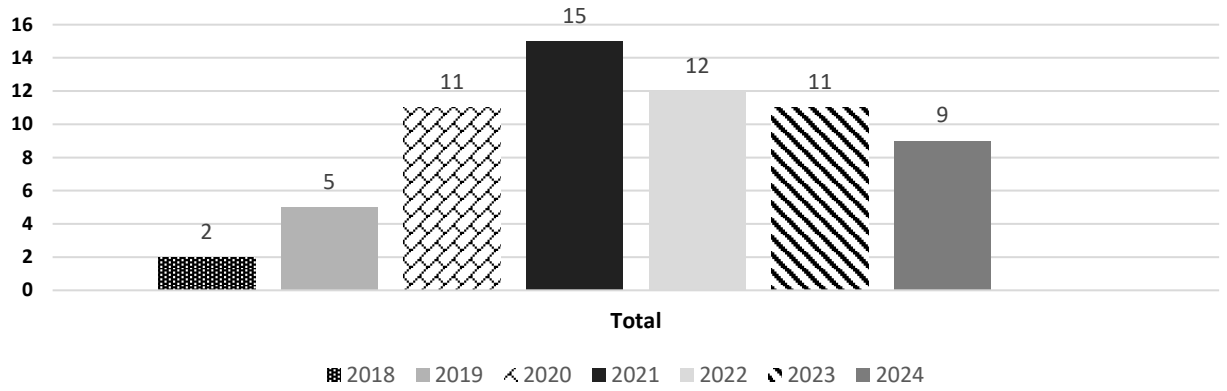

Figure 1. *Bar chart representing years of publication.*

A detailed breakdown of the quality assessment scores for all included studies is provided in Appendix A (Table A1).

3.8 Threats to validity

Despite methodological safeguards, several threats to validity remain:

- **Construct validity:** The scope of included studies depends on the search terms and databases. Although five major databases and multiple synonyms were used, some relevant studies may have been missed.
- **Internal validity:** Subjectivity may arise in applying inclusion/exclusion criteria and quality assessments. This was mitigated by structured criteria and independent review checks.
- **External validity:** Exclusion of non-English and paywalled studies may limit the comprehensiveness of results. Nonetheless, inclusion of multidisciplinary sources across a decade enhances generalizability. A major external validity threat arises from the fact that nearly all included studies present conceptual designs or small-scale prototypes rather than production-level implementations. Bioinformatics workflows routinely operate at terabyte to petabyte scale, involve multi-stage preprocessing and depend on HPC infrastructure conditions not simulated in existing blockchain studies. As such, conclusions regarding feasibility, scalability and regulatory alignment should be interpreted with caution, since prototype-based results may not generalize to large-scale genomic environments.
- **Reliability:** Most steps were performed by one researcher, with secondary verification. While this reduces risk of error, inter-rater reliability could not be fully established. Transparency is maintained through explicit documentation and the flow diagram.
    - *High-scoring studies* (≥ 4.5) tended to provide comprehensive accounts of applications, benefits, challenges of blockchain and, in some cases, limited comparative analysis with traditional methods.
    - *Low-scoring studies* (< 3) generally lacked methodological detail, empirical validation or comparative analysis, limiting their contribution to the synthesis.

4 RESULTS

This chapter presents a visual interpretation of the quality assessment results, revealing how the included studies performed across the five QA criteria. Radar charts and evidence maturity model illustrate structural patterns, methodological strengths and weaknesses and thematic gaps in literature. Where individual scoring decisions were ambiguous, the predefined QA criteria were reapplied for consistency. Because a single primary reviewer conducted the screening, borderline cases were re-evaluated to reduce subjectivity and maintain scoring reliability. Also, the authors developed a QA failure summary table (Table 3) showing the distribution of studies that failed each QA criterion.

Table 3. *Distribution of studies failing each QA criterion.*

QA criterion	Number of studies scoring 0	Percentage	Typical cause of failure
QA1 – Domain specificity	5	8%	Not bioinformatics-focused
QA2 –Clarity of benefits	3	5%	Benefits implied but not articulated
QA3 – Empirical evaluation	33	51%	No benchmarking or comparison
QA4 – Discussion of challenges	8	12%	Missing limitations section
QA5 – Reproducibility	12	18%	Insufficient technical detail

This distribution demonstrates that empirical evaluation (QA3) and reproducibility (QA5) were the most common points of failure, highlighting structural limitations in the current evidence base. These patterns further justify the interpretation of blockchain research in bioinformatics as concept-heavy but empirically immature.

4.1 Radar of QA scores

To better understand how studies performed across the five criteria, results were visualized using a radar chart. Figure 3 illustrates the distribution of scores across QA1–QA5. Most studies fully addressed QA1 (applications) and QA2 (benefits), demonstrating strong conceptual grounding. In contrast, QA3 (comparisons with traditional methods) exhibited the weakest coverage, with many studies scoring 0 or 0.5. QA4 (challenges) and QA5 (effectiveness and reproducibility) were addressed to a moderate extent, though several studies lacked sufficient empirical detail.

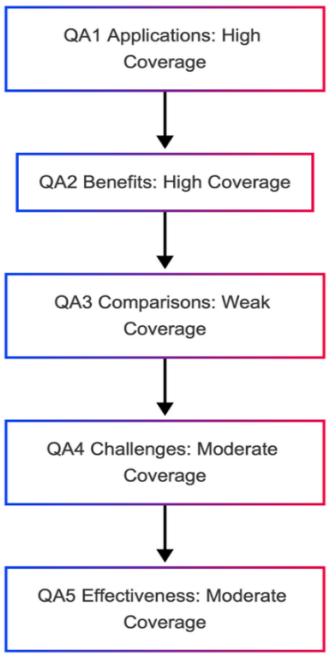

Figure 2. *Distribution of scores across QA1–QA5.*

4.1.1 *Radar of quality assessment results (QA1–QA5)*

The radar shows the number of studies scoring 1 (fully addressed), 0.5 (partially addressed) or 0 (not addressed) across each QA criterion. A partial score of 0.5 represents incomplete fulfilment, for instance, when a study asserted performance benefits without reporting metrics or when it mentioned challenges without linking them to empirical evidence. This widespread occurrence of partial scores reflects inconsistencies in methodological transparency and reporting standards across the field.

A closer examination of the QA outcomes reveals clear quantitative patterns. Thirty-three studies scored 0 on QA3, indicating a systemic absence of comparative evaluation against traditional security or data management methods. Similarly, twelve studies scored 0 on QA5, demonstrating inadequate reporting of technical details such as architectural descriptions, datasets, protocols or implementation specifics, thus limiting reproducibility. These deficiencies are not incidental but reflect underlying methodological gaps that hinder the development of rigorous, evidence-based blockchain research in bioinformatics.

The strong performance in QA1 and QA2 confirms that the conceptual applications and benefits of blockchain are well articulated in the literature. However, the weak performance in QA3 reflects deeper structural issues. A key factor contributing to this gap is heterogeneity in blockchain architecture. The included studies used public, private, consortium and hybrid blockchains, each with different consensus mechanisms, throughput characteristics, governance models and security properties. Such diversity makes direct comparison challenging and often discourages researchers from conducting structured benchmarking. Moreover, the absence of standardized genomic datasets, common evaluation pipelines and reproducible performance metrics further inhibits cross-study comparison.

4.2 Research question coverage

Figure 4 presents a radar chart illustrating the extent to which the studies addressed the five research questions. The chart reinforces the trends observed in the radar and highlights which areas of inquiry remain underdeveloped. The analysis measured how well the included studies collectively addressed the five research questions:

- RQ1 (blockchain applications): 53 studies (82%);
- RQ2 (benefits of blockchain): 52 studies (80%);
- RQ3 (comparisons with traditional methods): 32 studies (49%);
- RQ4 (implementation challenges): 50 studies (77%);
- RQ5 (effectiveness in sensitive data protection): 49 studies (75%).

Overall, the studies strongly engaged with applications of blockchain (RQ1) and articulated its potential benefits (RQ2). Comparatively fewer studies addressed RQ3, indicating that evaluations of blockchain alongside established security methods remain limited.

The radar chart illustrates the proportion of studies addressing each research question. While applications and benefits are well established, comparative and evaluative research (RQ3) remains the least developed. This gap stems from several structural challenges. Firstly, most studies rely on synthetic datasets or limited prototypes that cannot be meaningfully compared to production-grade systems. Secondly, blockchain frameworks vary significantly in consensus algorithm, scalability and architectural design, complicating attempts to establish common baselines for comparison. Thirdly, comparative evaluation requires access to genomic-scale computational infrastructure, which many research teams do not have. As a result, studies often assert advantages of blockchain without providing empirical validation.

Future research should address these shortcomings by adopting shared benchmarking datasets, standardized genomic workflows, reproducible evaluation frameworks and performance metrics that enable consistent cross-study comparison. Establishing these baselines is crucial for evaluating whether blockchain offers tangible benefits over alternatives, such as secure cloud storage, federated architecture, multi-party computation frameworks or advanced encryption-based systems.

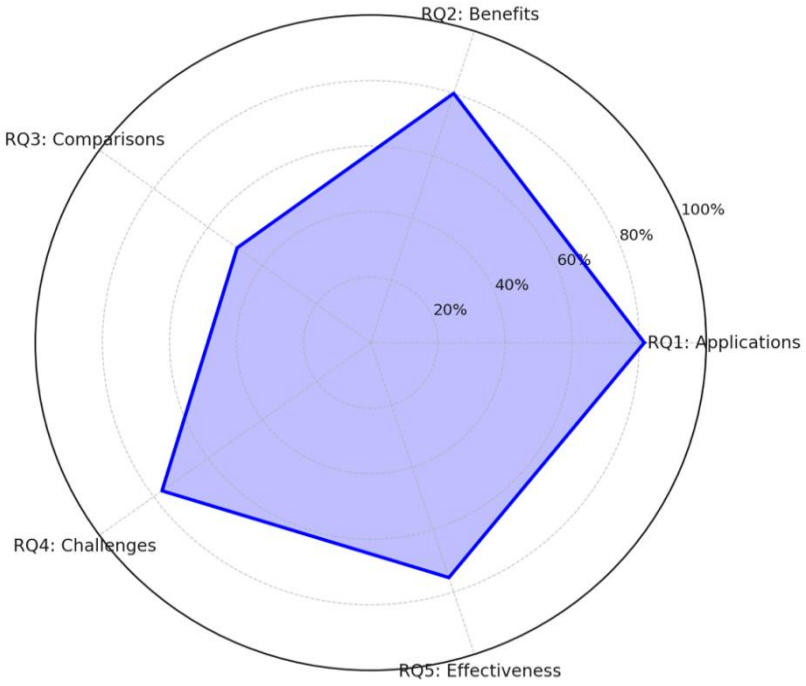

Figure 3. *Coverage of research questions (RQ1–RQ5).*

These findings indicate that although the conceptual promise of blockchain is well recognized, the field requires more empirical, comparative and real-world studies to advance from theoretical proposals to validated bioinformatics solutions.

4.3 Evidence maturity model

The evidence maturity model on Figure 5 illustrates the developmental trajectory of blockchain applications in bioinformatics across four stages: conceptual proposals, prototypes, implementations and benchmarking studies, culminating in real-world deployments. The distribution of studies across these stages further contextualizes the QA results and highlights structural barriers to maturity.

The majority of studies fall within the conceptual proposal stage, presenting frameworks, architectures or high-level designs without empirical testing. These works emphasize theoretical advantages of blockchain – immutability, decentralization, provenance, traceability – but rarely address regulatory constraints, performance bottlenecks or scalability requirements inherent to genomic workflows.

A moderate number of studies advanced to the prototype implementation stage. These prototypes demonstrate functional feasibility using small-scale or synthetic datasets, focusing on identity management, access control or metadata traceability. However, they rarely incorporate genomic-scale data, multi-institutional coordination or computational intensity reflective of real bioinformatics environments.

Only a small fraction of studies reach the benchmarking stage. These works perform quantitative evaluation - typically measuring transaction latency, consensus overhead, block-size constraints or storage performance - and occasionally compare blockchain to non-blockchain alternatives. Nevertheless, their scarcity reveals that empirical scrutiny remains limited, and the small-scale evaluation environments in which they are conducted reduce the generalizability of the findings.

Figure 4. *Evidence maturity model.*

Finally, the real-world deployment stage is nearly absent. None of the included studies demonstrate deployment of blockchain in production bioinformatics environments that handle sensitive genomic or multi-omics data. This aligns with systemic challenges identified elsewhere: data erasure requirements under the General Data Protection Regulation (GDPR), the high-throughput genomic processing demands that are incompatible with blockchain consensus overhead, and complex governance requirements across multiple institutions.

Taken together, the maturity analysis and QA score distribution reveal a consistent pattern: low QA3 and QA5 scores correspond directly to systemic weaknesses in empirical design and reproducibility. With 33 studies (51%) lacking comparative evaluation and 12 studies (18%) lacking implementation detail, the field remains concept-rich but evidence-poor. Addressing these shortcomings will require hybrid systems, regulation-aligned architecture, shared benchmarking infrastructure and multi-institutional pilot deployments capable of testing blockchain on the scale required for bioinformatics.

4.4 Comparative analysis of representative blockchain-based bioinformatics and biomedical data security studies

Table 4 provides an illustrative overview of representative studies frequently cited in the literature to contextualize the diversity of blockchain approaches discussed in prior work. A detailed evidence synthesis is presented in Section 5.

Table 4. *Comparative analysis of representative blockchain-based bioinformatics and biomedical data security studies.*

Study	Application domain	Blockchain architecture	Dataset type	Evaluation approach	Key contributions	Major limitations
Gürsoy et al. (2020a)	Genomic metadata provenance	Permissioned blockchain	Real metadata	Prototype; functional validation	FAIR-compliant provenance tracking	No throughput/ latency benchmarking; genomic-scale feasibility untested
Grishin et al. (2019)	Genomic data sharing	Hybrid blockchain + off-chain	Synthetic genomic datasets	Prototype only	User-centric genomic data marketplace	No cost/scalability evaluation; security assumptions unverified
Hosseini et al. (2019)	Secure genomic encryption (Cryfa)	Cryptographic tool integrated with BC workflows	Real genomic data	Benchmark (encryption speed & overhead)	Strong privacy and compression efficiency	Not a blockchain system; lacks pipeline interoperability
Ismail et al. (2019)	Medical data sharing	Private blockchain	Synthetic EHR metadata	Small-scale prototype	Secure access and logging functions	No adversarial testing; no comparison with traditional security models
Malamas et al. (2020)	Fine-grained medical data access	Hierarchical multi-chain	None (conceptual)	Architectural analysis	Scalability through multi-tier blockchain design	No empirical evaluation; genomic applicability unclear
Amin et al. (2021)	Biomedical supply chain	Hyperledger Fabric	Synthetic supply-chain data	Prototype	Traceability and auditability	No genomic context; small-scale evaluation
Pilares et al. (2022)	Electronic health record (EHR) + interplanetary file system (IPFS) storage	Permissioned ledger + IPFS	Synthetic EHR	Prototype	Efficient off-chain storage and metadata referencing	Not tested under high-volume (omics) workloads
Nguyen et al. (2019)	Mobile-cloud EHR sharing	Public/consortium	Synthetic health records	Prototype	Privacy-preserving distributed access	No assessment of genomic data mutability needs

Study	Application domain	Blockchain architecture	Dataset type	Evaluation approach	Key contributions	Major limitations
Bamakan et al. (2021)	Biomedical patent analytics	Generic blockchain	Real text	Text-mining evaluation	Analytical framework for innovation mapping	Not bioinformatics security; no performance data
Agbo & Mahmoud (2019)	Healthcare systems	Multiple blockchain frameworks	None	Comparative framework	Systematic comparison of platforms	No bioinformatics-specific analysis; no empirical tests

5 DISCUSSION

This section interprets the results presented in Section 4 in relation to the five research questions (RQ1–RQ5) defined in Section 3.1. The findings reveal strong coverage of applications of blockchain (RQ1) and benefits (RQ2), moderate attention to challenges (RQ4) and effectiveness (RQ5), but limited comparative evaluations against traditional security methods (RQ3). This chapter interprets these results within the broader literature, identifies structural and methodological gaps and outlines implications for research and practice.

5.1 Critical synthesis across studies

Across the 65 reviewed studies, blockchain proposals were predominantly conceptual or implemented on a prototype scale, with a near absence of real-world, genomic-scale deployments. Empirical validation was rare: fewer than ten studies conducted benchmarking experiments or compared blockchain with traditional systems. This imbalance reflects several structural constraints:

- Genomic data scales (Terabyte-Perabyte) exceed blockchain storage and throughput limits.
- Immutability conflicts with dynamic consent and erasure requirements.
- Consensus algorithms introduce latency incompatible with high-throughput bioinformatics workflows.
- Regulatory uncertainty discourages institutional adoption.

For example, Gursoy et al. (2020) and Grishin et al. (2019) proposed frameworks for genomic data sharing but did not evaluate throughput, latency or costs on the population scale. Ismail et al. (2019) implemented a permissioned ledger for medical data; however, performance was tested only using synthetic metadata, rather than real genomic files. These patterns reflect an overarching challenge: blockchain systems in bioinformatics have not been validated under realistic workloads.

A key source of inconsistency is the heterogeneity of blockchain architectures used across studies. Public chains (e.g., Ethereum-like systems) suffer from scalability, privacy and finality constraints; private or consortium chains improve performance but weaken decentralization; hybrid models introduce complex interoperability and governance challenges. However, few studies examined how these architectural trade-offs influence the feasibility of core bioinformatics pipelines such as variant calling, multi-omics integration or federated genomic collaboration.

5.2 Structural barriers explaining prototype dominance

The predominance of conceptual and prototype-level contributions aligns directly with structural constraints identified across the literature:

1. Technical barriers

- Blockchain cannot store or process large genomic files; off-chain systems (IPFS, cloud storage) introduce additional complexity.
- Consensus mechanisms introduce latency inconsistent with workflows requiring rapid, iterative analysis.
- On-chain metadata persistence poses risks of privacy leakage, especially in multi-omic or longitudinal studies.

2. Regulatory barriers

- Immutability conflicts with the GDPR “right to erasure”.
- Clinical and genomic data often cross borders, yet legal harmonization is limited.

- Consent models require dynamic updates, which immutable-only ledgers cannot easily support.

3. Organizational barriers

- Bioinformatics infrastructures rely on HPC clusters that are not designed for blockchain integration.
- Institutions resist technologies requiring decentralized governance or shared trust models.
- Limited incentives exist for multi-institutional blockchain-based collaboration.

These barriers collectively explain why blockchain in bioinformatics remains in an exploratory phase, with very limited operational adoption.

5.3 Research question analysis

Blockchain applications in bioinformatics (RQ1)

Eighty-two percent (82%) of the studies demonstrated the potential of blockchain in genomic data sharing, provenance tracking, patient data management, federated collaboration and clinical trials. These results align with prior work (Grishin et al., 2019; Hussein et al., 2019), which has emphasized the utility of blockchain in enabling transparent sharing and immutable audit trails.

However, these applications remain conceptual or limited to small testbeds. None have incorporated petabyte-scale genomic pipelines, dynamic preprocessing steps or high-performance computational workloads typical of real-world bioinformatics. This disconnect illustrates a core limitation: blockchain architectures diverge significantly from the mutable, iterative, high-throughput demands of bioinformatics workflows.

Benefits of blockchain in bioinformatics (RQ2)

Eighty percent (80%) of the reviewed articles reported benefits such as immutability, transparency, decentralization, cost efficiency and patient empowerment. These benefits can be regarded as theoretical, whilst limitations to improved auditability and access control in small tests can be seen as empirical benefits. These reflect the core attributes of blockchain and reinforce its promise as a transformative technology in data-intensive domains. Studies have consistently argued that blockchain enhances trust and accountability, particularly in multi-institutional collaborations where data security is critical (Bamakan et al., 2021; Ali et al., 2022).

However, these benefits have been predominantly theoretical or demonstrated through limited prototypes. Few studies have empirically validated claims of cost efficiency, interoperability or attack resilience. This absence of empirical benchmarks limits confidence in the ability of blockchain to outperform traditional security mechanisms in production environments.

Comparative evaluation with traditional security methods (RQ3)

Comparative evaluation was the weakest area, with less than half of the studies (49%) addressing how blockchain performs relative to conventional security systems. Traditional systems (centralized databases, encryption frameworks, federated architectures) have been acknowledged as effective but vulnerable to breaches, insider threats and interoperability challenges. Blockchain has often been described as a superior alternative due to its decentralization, immutability and accountability.

However, these claims have rarely been substantiated through controlled experiments. RQ3 coverage was low for three structural reasons:

1. Prototype systems cannot support rigorous benchmarking on a genomic scale.
2. Lack of standardized datasets and workflows prevents meaningful cross-study comparison.
3. Blockchain heterogeneity (public vs private vs consortium) makes it difficult to establish fair baselines.

Only 32 studies have compared blockchain with traditional systems. Future work must use throughput, latency, storage overhead, attack resilience, re-identification risk and costs as standardized metrics. RQ3 exhibits low coverage because very few studies implement baseline comparisons. Benchmarking requires high-volume data, stable implementations and standardized metrics-conditions rarely met by prototype-level blockchain systems.

Challenges and limitations of blockchain adoption (RQ4)

Seventy-seven percent (77%) of the studies identified challenges, including scalability constraints, storage limitations, privacy and regulatory conflicts, interoperability issues, consensus overhead and energy consumption. These findings align with recent reviews (Dursi et al., 2021; Saputra & Setiawan, 2023), highlighting the immaturity of blockchain for genomic-scale applications.

Notably, most discussions have been conceptual. Very few studies have quantified performance bottlenecks or evaluated cost implications of consensus mechanisms, off-chain storage or privacy-preserving cryptographic integrations. Without empirical data, stakeholders cannot reliably assess the feasibility of blockchain.

Effectiveness in securing sensitive data (RQ5)

Seventy-five percent (75%) of the studies discussed the effectiveness of blockchain in protecting sensitive data. Reported strengths included:

- secure sharing and collaboration (43 studies);
- privacy and access control (38 studies);
- auditability and transparency (33 studies); and
- resilience to attacks (20 studies).

The decentralized model of blockchain reduces reliance on single points of failure and enhances tamper-resistance. However, validation was typically limited to pilots or synthetic datasets. Only a minority evaluated real-world adversarial scenarios, key-management failures or re-identification risks from on-chain metadata. As a result, the security advantages of blockchain remain promising but under-validated.

5.4 Synthesis of QA results

The quality assessment strengthened these findings. The QA scores were highest for applications (QA1) and benefits (QA2), confirming the conceptual maturity of the literature. QA3 – the criterion aligned with comparative evaluation – was the weakest, reflecting the scarcity of empirical benchmarking. QA4 and QA5 were moderately addressed but lacked rigorous quantitative evidence.

Figures 3 and 4 confirm this uneven coverage and show that RQ3 remains the largest research gap. The low QA3 and QA5 scores correlate with the dominance of conceptual papers lacking reproducible implementations or computational experiments. These patterns reinforce the structural immaturity illustrated in the evidence maturity model: the field is concept-rich but evidence-poor.

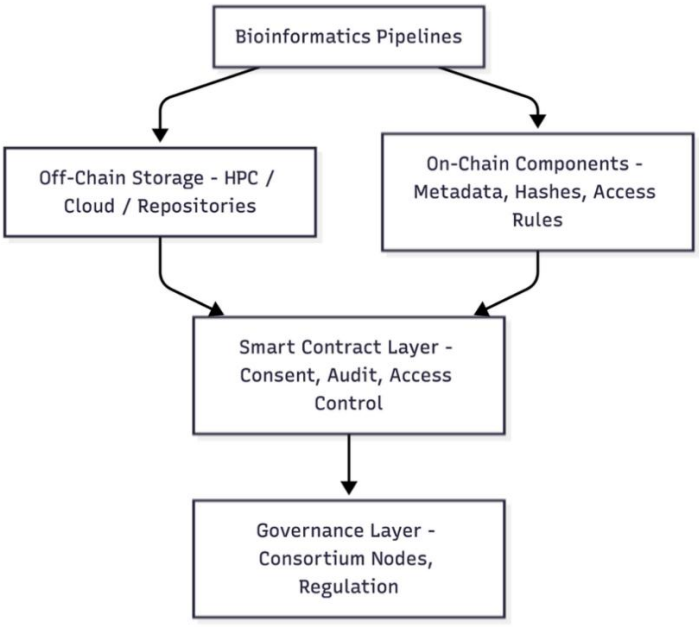

Figure 5. *Conceptual framework for blockchain in bioinformatics.*

5.5 Implications for research and practice

5.5.1 Implications for research

The findings indicate that blockchain research in bioinformatics remains exploratory. Future research should prioritize:

1. controlled comparative evaluations against traditional systems using standard benchmarks;
2. empirical validation through multi-institutional pilot studies involving genomic-scale datasets;
3. hybrid architecture integrating blockchain with cloud/HPC systems, federated learning and AI pipelines;
4. standardization frameworks for interoperability, auditability, consent updating and privacy-by-design compliance; and
5. development of realistic benchmarking datasets that model genomic, multi-omic and longitudinal data flows.

A minimal viable blockchain prototype for genomics should support scalable off-chain storage, key rotation and revocation, dynamic consent management and sub-second metadata access latency. Achieving GDPR-compliant erasure will require cryptographic unlinkability rather than strict immutability.

5.5.2 Implications for practice

Practitioners should adopt a cautious but informed approach. Blockchain offers significant potential for enhancing provenance, integrity and collaborative governance, but deployment should begin with narrowly scoped pilots. Governance models must account for privacy, compliance, energy use and multi-institutional coordination. Healthcare and research organizations should prioritize hybrid architecture rather than full-chain solutions.

Blockchain deployment in bioinformatics must be reconciled with stringent regulatory frameworks such as GDPR and Health Insurance Portability and Accountability Act (HIPAA). The GDPR "right to erasure" is particularly challenging in immutable ledger environments; practical compliance requires cryptographic unlinkability, off-chain storage of identifiable data and revocation-based key management rather than literal deletion of on-chain records. HIPAA introduces additional constraints regarding auditability, minimum necessary access and data minimization requirements, necessitating fine-grained smart contract governance and role-based authorization. These regulatory tensions underscore the need for hybrid architectures that combine decentralization with privacy-preserving computation.

5.6 Limitations of the review

This review was limited to English-language, peer-reviewed articles indexed in selected databases, potentially excluding grey literature or industry implementations. The screening and QA assessment were conducted by a single reviewer, which may introduce interpretative bias despite structured procedures. Additionally, industrial blockchain applications in bioinformatics are often proprietary and not publicly documented, meaning that cutting-edge deployments may be underrepresented.

5.7 Future research directions

Future work should:

- conduct controlled studies comparing blockchain and non-blockchain security models;
- develop scalable prototypes that can support genomic-scale datasets;
- investigate energy-efficient consensus mechanisms tailored to bioinformatics;
- explore ethical frameworks for patient consent, ownership and equitable genomic data use;
- enhance interoperability with EHRs, cloud providers and federated computing systems;
- integrate advanced privacy-preserving technologies, such as zero-knowledge proofs, homomorphic encryption and secure enclaves, to mitigate privacy risks; and
- establish reproducible benchmarking frameworks for variant calling, multi-omics integration and longitudinal genomic workflows.

Scalability, hybrid architecture and rigorous evaluation using realistic pipelines remain the highest research priorities. Future benchmarking studies should evaluate blockchain frameworks against traditional secure storage and federated computation systems using realistic genomic workloads. For example, a variant-calling pipeline using a 1 TB whole-genome sequencing dataset could be processed under two conditions: (i) metadata managed through Hyperledger Fabric with off-chain IPFS storage and (ii) traditional secure cloud storage with audit logging. Metrics such as transaction throughput, metadata access latency, storage overhead, fault tolerance and costs per computation cycle would allow meaningful comparison and address the evidence gaps highlighted by RQ3 and QA3.

6 CONCLUSION

This systematic review synthesized 65 studies on blockchain-based approaches for bioinformatics and genomic data security published between 2014 and 2024. The findings show a rapidly growing but uneven field: blockchain is widely recognized as a promising enabler of integrity, provenance, decentralized access control and auditability across bioinformatics workflows, yet robust empirical validation remains scarce. Most contributions focus on conceptual architectures or limited prototypes, with few comparative analyses or real-world deployments.

By integrating a PRISMA-guided search strategy, focused research questions and a structured quality assessment, this review mapped dominant application domains, identified where claimed benefits lack evidence, highlighted methodological and governance challenges and proposed design principles for future blockchain-based bioinformatics infrastructures.

Overall, while blockchain offers credible architectural benefits, its current evidence base is insufficient for real-world adoption. Urgently needed are controlled benchmarking studies, genomic-scale pilot deployments and regulation-aligned hybrid architectures that can validate whether blockchain meaningfully improves data integrity, auditability and collaborative governance in bioinformatics.

ADDITIONAL INFORMATION AND DECLARATIONS

Acknowledgments: The authors thank the anonymous reviewers and the editor for their constructive comments, which helped improve the clarity and quality of the manuscript.

Conflict of Interests: The authors declare no conflict of interest.

Author Contributions: D.O.B.: Conceptualization, Methodology, Formal analysis, Investigation, Data curation, Writing – Original draft preparation, Writing – Review and Editing. F.B.: Methodology, Supervision, Validation, Writing – Review and Editing. K.O.-M.: Conceptualization, Validation, Writing – Review and Editing. M.K.: Investigation, Data curation, Visualization, Writing – Review and Editing. I.O.: Methodology, Validation, Supervision, Writing – Review and Editing.

Statement on the Use of Artificial Intelligence Tools: During manuscript revision, the authors used ChatGPT, developed by OpenAI, for language refinement, editorial support, and improvement of clarity in selected sections of the manuscript. The tool was not used to generate research data, conduct analysis, make methodological decisions, or replace authorial interpretation. All AI-assisted outputs were critically reviewed, edited, and approved by the authors, who take full responsibility for the accuracy, integrity, and final content of the manuscript.

Data Availability: No new primary dataset was generated or analysed in this study. The review was based on published literature retrieved from Scopus, ScienceDirect, IEEE Xplore, ACM Digital Library, and SpringerLink, see a list of included studies in Appendix A (Table A2).

APPENDIX A

Table A1. *Quality assessment (QA) scores of included studies.*

No.	Study (Author, Year)	Domain	Blockchain Type	Consensus	Dataset	Evidence Level	Benefits	Limitations	QA
1	Li et al., 2021	IoMT / Biomedical	Private	Not Spec.	None	Conceptual	Integrity, traceability	No empirical evaluation	4
2	Brogan et al., 2018	Health activity	Public	Not Spec.	Synthetic	Prototype	Authentication	No comparison baseline	1
3	Bamakan et al., 2021	Patent analytics	Generic	Not Spec.	Real text	Prototype	Trend forecasting	Not bioinformatics	5
4	Sutradhar et al., 2024	Healthcare IAM	Health IT	PBFT	None	Prototype	Scalability, identity Mgmt.	No genomic focus	5
5	Akash & Ferdous, 2022	Digital Twins	EHR	Consortium	Not Spec.	Prototype	Secure linkage	No large-scale tests	4
6	Mandarino et al., 2024	EHR	Edge	Not Spec.	None	Conceptual	Cost-efficiency	No empirical validation	0
7	Houtan et al., 2020	Patient identity	EHR	Not Spec.	None	Conceptual	Self-sovereign identity	No data tests	4
8	Hosseini et al., 2019	Genomic encryption	Genomics	N/A (Encryption tool)	N/A	Real genomic	Benchmark	Strong encryption	0
9	Malamas et al., 2020	Medical data	Hierarchical BC	Not Spec.	None	Prototype	Fine-grained access	No scalability metrics	4.5
10	Al-Kaabi & Abdullah, 2023	Health record	IPFS+BC	Not Spec.	None	Conceptual	Distributed storage	Not evaluated	0
11	Pilares et al., 2022	EHR	IPFS	Not Spec.	Synthetic	Prototype	Storage optimization	Limited dataset	5
12	Rajput et al., 2021	PHR sharing	PHR	Not Spec.	None	Prototype	Emergency access	No adversarial testing	1
13	Yao et al., 2022	Blockchain econ	Generic	Not Spec.	None	Conceptual	Mapping	Not relevant to bioinformatics	0
14	Hussein et al., 2019	Biomedical data	Private	Not Spec.	None	Prototype	Adaptive storage	Evaluation missing	5
15	Ali et al., 2022	Searchable encryption	IoT Health	Hybrid	NN-based	Synthetic	Prototype	Searchable encryption	0
16	Xu et al., 2023	BFT algorithm	Medical data	BFT	Synthetic	Benchmark	Fast consensus	Not bioinformatics	4.5
17	W. Chen et al., 2021	EMR sharing	EMR	Not Spec.	None	Prototype	Proxy re-encryption	Small-scale validation	4
18	Sharma et al., 2020	IoMT	E-health	Not Spec.	None	Conceptual	Smart contracts	No data evaluation	0
19	Jennath et al., 2020	Healthcare AI	EHR	Not Spec.	None	Prototype	Trust, security	No genomic angle	5
20	Srinivasu et al., 2021	E-health	ML+BC	Not Spec.	Synthetic	Prototype	Pattern detection	No scalability tests	4.5
21	Usman et al., 2021	Blockchain health	Biomedical	Not Spec.	None	Prototype	Secure records	No benchmarks	5
22	Rana et al., 2022	E-health	Blockchain	Not Spec.	None	Prototype	Secure sharing	Lacks comparative testing	5
23	Baysal et al., 2023	Medical data	Generic	Not Spec.	None	Conceptual	Integrity	No empirical work	4
24	Zhang et al., 2023	Health data	Not Spec.	Not Spec.	None	Conceptual	Data management	No evaluation	4
25	T et al., 2024	Healthcare	Blockchain	Not Spec.	Synthetic	Prototype	Identity mgmt	No genomic datasets	5
26	Bidve et al., 2023	Biomedical	Hybrid	Not Spec.	Synthetic	Prototype	Privacy preservation	No scalability data	5

No.	Study (Author, Year)	Domain	Blockchain Type	Consensus	Dataset	Evidence Level	Benefits	Limitations	QA
27	Saidi et al., 2022	EHR	Not Spec.	Not Spec.	None	Conceptual	Distributed control	Not validated	0
28	Mao et al., 2024	Genomic	Blockchain	Not Spec.	Synthetic	Prototype	Traceability	No large dataset	4.5
29	Ali et al., 2023	Healthcare	IoT+BC	Not Spec.	None	Prototype	Secure IoT	No benchmarking	5
30	Liu et al., 2020	Generic	BC security	Not Spec.	None	Conceptual	Security model	Not bioinformatics	0
31	Mallikarjuna et al., 2022	EHR	Blockchain	Not Spec.	None	Prototype	Security	No evaluation	5
32	Mayer et al., 2021	Biomedical	Blockchain	Not Spec.	None	Conceptual	Integrity	Missing reproducible detail	3
33	Lemieux et al., 2020	Record integrity	Generic	Not Spec.	None	Conceptual	Provenance	Not empirical	4
34	Huang et al., 2022	Healthcare	Consortium	Not Spec.	Synthetic	Prototype	Fast access	No genomics	5
35	Farahat et al., 2022	Health data	Blockchain	Not Spec.	None	Prototype	Decentralization	Limited testing	5
36	Abutaleb et al., 2023	Medical	Consortium	Not Spec.	None	Prototype	Trust	No datasets	5
37	Ezil Sam Leni et al., 2023	Healthcare	Blockchain	Not Spec.	None	Prototype	Accountability	No external validation	5
38	Ismail et al., 2019	Medical	Blockchain	Not Spec.	Synthetic	Prototype	Security	No baseline comparison	5
39	Chhabra et al., 2024	Healthcare	Blockchain	Not Spec.	Synthetic	Prototype	Robustness	No real data	5
40	Liu et al., 2023	Healthcare	Blockchain	Not Spec.	None	Prototype	Optimization	Missing empirical evaluation	4.5
41	Jang et al., 2021	Medical	Blockchain	Not Spec.	Synthetic	Prototype	Privacy	No genomic relevance	5
42	Tao & Ling, 2021	Generic	Blockchain	Not Spec.	None	Conceptual	Security	Not relevant	0
43	Zala et al., 2022	Biomedical	Blockchain	Not Spec.	None	Prototype	Sharing	No experiments	5
44	Yang et al., 2019	Genomics	Blockchain	Not Spec.	Synthetic	Prototype	Sharing	Missing scalability tests	4
45	Banita, 2024	Healthcare	Blockchain	Not Spec.	Synthetic	Prototype	Tracking	No baselines	4.5
46	Yaqoob et al., 2022	IoT Health	Blockchain	Not Spec.	None	Conceptual	Integrity	Not evaluated	3
47	Alqaralleh et al., 2024	Healthcare	BC+AI	Not Spec.	None	Prototype	Prediction + Security	No benchmark	5
48	Xu et al., 2018	Generic	Blockchain	Not Spec.	None	Conceptual	Overview	Not relevant	0
49	Tagde et al., 2021	Healthcare	Blockchain	Not Spec.	None	Prototype	Data security	Limited evaluation	4
50	Jia et al., 2021	Health	Blockchain	Not Spec.	Synthetic	Prototype	Safe queries	Missing comparisons	5
51	Goel & Neduncheliyan, 2023	Biomedical	BC	Not Spec.	None	Prototype	Framework	No performance data	4
52	Murphy et al., 2021	Generic	Blockchain	Not Spec.	None	Conceptual	Analysis	Not evaluative	0
53	Gross & Miller, 2021	Biosecurity	Blockchain	Not Spec.	None	Conceptual	Trust	No datasets	4
54	Gürsoy et al., 2020a	Genomic	Blockchain	Not Spec.	Real (metadata)	Prototype	Provenance	No throughput data	5
55	Gürsoy et al., 2020b	Genomic	Blockchain	Not Spec.	Synthetic	Prototype	Traceability	Not compared	5
56	Gürsoy et al., 2022	Genomic	Blockchain	Not Spec.	Real metadata	Prototype	FAIR compliance	Prototype-only	5
57	Wong et al., 2019	Biomedical	Blockchain	Not Spec.	Real	Prototype	Access logging	Limited scalability	5

No.	Study (Author, Year)	Domain	Blockchain Type	Consensus	Dataset	Evidence Level	Benefits	Limitations	QA
58	Grishin et al., 2019	Genomics	Blockchain	Not Spec.	Synthetic	Prototype	Democratized sharing	No empirical tests	2
59	Costa et al., 2023	Generic	Blockchain	Not Spec.	None	Conceptual	Overview	Not relevant	0
60	Zghaibeh et al., 2020	Cybersecurity	Blockchain	Not Spec.	None	Conceptual	Defense	No bioinformatics link	2
61	Rohini et al., 2024	Biomedical	Blockchain	Not Spec.	Synthetic	Prototype	Privacy	Missing rigorous testing	5
62	Carlini et al., 2020	Biosecurity	Blockchain	Not Spec.	None	Prototype	Auditability	Not evaluated	5
63	Sultana et al., 2020	Health data	BC	Not Spec.	Synthetic	Prototype	Anonymity	No benchmarks	4
64	Jeong et al., 2021	Health	Blockchain	Not Spec.	Synthetic	Prototype	Data access tracking	Small datasets	4
65	Tan et al., 2022	Biomedical	Blockchain	Not Spec.	None	Prototype	Secure sharing	No large-scale tests	5

Table A2. *List of included studies.*

No.	Study (Author, Year)	Title of the study
1	Li et al., 2021	Is blockchain for Internet of Medical Things a panacea for COVID-19pandemic?
2	Brogan et al., 2018	Authenticating Health Activity Data Using Distributed Ledger Technologies
3	Bamakan et al., 2021	Blockchain technology forecasting by patent analytics and text mining
4	Sutradhar et al., 2024	Enhancing identity and access management using Hyperledger Fabric and OAuth 2.0: A block-chain-based approach for security and scalability for healthcare industry
5	Akash & Ferdous, 2022	A Blockchain Based System for Healthcare Digital Twin
6	Mandarino et al., 2024	A Blockchain-Based Electronic Health Record (EHR) System for Edge Computing Enhancing Security and Cost Efficiency
7	Houtan et al., 2020	A Survey on Blockchain-Based Self-Sovereign Patient Identity in Healthcare
8	Hosseini et al., 2019	Cryfa: A secure encryption tool for genomic data
9	Malamas et al., 2020	A Hierarchical Multi Blockchain for Fine Grained Access to Medical Data
10	Al-Kaabi & Abdullah, 2023	A survey: medical health record data security based on interplanetary file system and blockchain technologies
11	Pilares et al., 2022	Addressing the Challenges of Electronic Health Records Using Blockchain and IPFS
12	Rajput et al., 2021	A Blockchain-Based Secret-Data Sharing Framework for Personal Health Records in Emergency Condition
13	Yao et al., 2022	A multi-dimension traceable privacy-preserving prevention and control scheme of the COVID-19 epidemic based on blockchain
14	Hussein et al., 2019	An Adaptive Biomedical Data Managing Scheme Based on the Blockchain Technique
15	Ali et al., 2022	An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach for Healthcare Systems Using Neural Network
16	Xu et al., 2023	An Optimized Byzantine Fault Tolerance Algorithm for Medical Data Security
17	W. Chen et al., 2021	Authorized Shared Electronic Medical Record System with Proxy Re-Encryption and Blockchain Technology
18	Sharma et al., 2020	Blockchain Based Smart Contracts for Internet of Medical Things in e-Healthcare
19	Jennath et al., 2020	Blockchain for Healthcare: Securing Patient Data and Enabling Trusted Artificial Intelligence
20	Srinivasu et al., 2021	Blockchain Technology for Secured Healthcare Data Communication among the Non-Terminal Nodes in IoT Architecture in 5G Network
21	Usman et al., 2021	The case for establishing a blockchain research and development program at an academic medical center
22	Rana et al., 2022	Blockchain Technology and Artificial Intelligence Based Decentralized Access Control Model to Enable Secure Interoperability for Healthcare
23	Baysal et al., 2023	Blockchain technology applications in the health domain: a multivocal literature review
24	Zhang et al., 2023	Design pattern recommendations for building decentralized healthcare applications
25	T et al., 2024	Developing a Patient-Centric Healthcare IoT Platform with Blockchain and Smart Contract Data Management
26	Bidve et al., 2023	Patient data management using blockchain technology
27	Saidi et al., 2022	DSMAC: Privacy-Aware Decentralized Self-Management of Data Access Control Based on Blockchain for Health Data
28	Mao et al., 2024	Efficient and Secure Management of Medical Data Sharing Based on Blockchain Technology

No.	Study (Author, Year)	Title of the study
29	Ali et al., 2023	Empowering Precision Medicine: Unlocking Revolutionary Insights through Blockchain-Enabled Federated Learning and Electronic Medical Records
30	Liu et al., 2020	Enhancing Privacy and Data Security across Healthcare Applications Using Blockchain and Distributed Ledger Concepts
31	Mallikarjuna et al., 2022	Blockchain technology: A DNN token-based approach in healthcare and COVID-19 to generate extracted data
32	Mayer et al., 2021	FogChain: A Fog Computing Architecture Integrating Blockchain and Internet of Things for Personal Health Records
33	Lemieux et al., 2020	Having Our "Omic" Cake and Eating It Too?: Evaluating User Response to Using Blockchain Technology for Private and Secure Health Data Management and Sharing
34	Huang et al., 2022	Sharing medical data using a blockchain-based secure HER system for New Zealand
35	Farahat et al., 2022	Improving Healthcare Applications Security Using Blockchain
36	Abutaleb et al., 2023	Integrity and Privacy-Aware, Patient-Centric Health Record Access Control Framework Using a Blockchain
37	Ezil Sam Leni et al., 2023	Block-chain based Secure Data Access over Internet of Health Application Things (IHoT)
38	Ismail et al., 2019	Lightweight Blockchain for Healthcare
39	Chhabra et al., 2024	Navigating the Maze: Exploring Blockchain Privacy and Its Information Retrieval
40	Liu et al., 2023	Overview of Internet of Medical Things Security Based on Blockchain Access Control
41	Jang et al., 2021	PDPM: A Patient-Defined Data Privacy Management with Nudge Theory in Decentralized E-Health Environments
42	Tao & Ling, 2021	Practical Medical Files Sharing Scheme Based on Blockchain and Decentralized Attribute-Based Encryption
43	Zala et al., 2022	PRMS: Design and Development of Patients' E-Healthcare Records Management System for Privacy Preservation in Third Party Cloud Platforms
44	Yang et al., 2019	Proof-of-Familiarity: A Privacy-Preserved Blockchain Scheme for Collaborative Medical Decision-Making
45	Banita, 2024	Role of Blockchain Technology in Data Security for Healthcare
46	Yaqoob et al., 2022	Blockchain for healthcare data management: opportunities, challenges, and future recommendations
47	Alqaralleh et al., 2024	Blockchain-assisted secure image transmission and diagnosis model on Internet of Medical Things Environment
48	Xu et al., 2018	Blockchain-based decentralized content trust for docker images
49	Tagde et al., 2021	Blockchain and artificial intelligence technology in e-Health
50	Jia et al., 2021	SE-Chain: A Scalable Storage and Efficient Retrieval Model for Blockchain
51	Goel & Nedunchelivan, 2023	An intelligent blockchain strategy for decentralised healthcare framework
52	Murphy et al., 2021	Assessing the potential use of blockchain technology to improve the sharing of public health data in a western Canadian province
53	Gross & Miller, 2021	Protecting privacy and promoting learning: blockchain and privacy preserving technology should inform new ethical guidelines for health data
54	Gürsoy et al., 2020a	Using blockchain to log genome dataset access: efficient storage and query
55	Gürsoy et al., 2020b	Using Ethereum blockchain to store and query pharmacogenomics data via smart contracts
56	Gürsoy et al., 2022	Storing and analyzing a genome on a blockchain
57	Wong et al., 2019	Prototype of running clinical trials in an untrustworthy environment using blockchain
58	Grishin et al., 2019	Data privacy in the age of personal genomics
59	Costa et al., 2023	Sec-Health: A Blockchain-Based Protocol for Securing Health Records
60	Zghaibeh et al., 2020	SHealth: A Blockchain-Based Health System With Smart Contracts Capabilities
61	Rohini et al., 2024	Smart Patient Consent Management Model for Health Information Exchange Based on Blockchain Technology
62	Carlini et al., 2020	The Genesy Model for a Blockchain-Based Fair Ecosystem of Genomic Data
63	Sultana et al., 2020	Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology
64	Jeong et al., 2021	A Study on Smart Healthcare Monitoring Using IoT Based on Blockchain
65	Tan et al., 2022	MB-BC: Drug Traceability System Based on Multibranched Blockchain Structure

REFERENCES

Abutaleb, R. A., Alqahtany, S. S., & Syed, T. A. (2023). Integrity and Privacy-Aware, Patient-Centric Health Record Access Control Framework Using a Blockchain. *Applied Sciences*, 13(2), 1028. https://doi.org/10.3390/app13021028

Agbo, C. C., & Mahmoud, Q. H. (2019). Comparison of blockchain frameworks for healthcare applications. *Internet Technology Letters*, 2(5), e122. https://doi.org/10.1002/itl2.122

Akash, S. S., & Ferdous, M. S. (2022). A Blockchain Based System for Healthcare Digital Twin. *IEEE Access*, 10, 50523–50547. https://doi.org/10.1109/ACCESS.2022.3173617

Al-Aamri, A., Kamarul Azman, S., Daw Elbait, G., Alsafar, H., & Henschel, A. (2023). Critical assessment of on-premise approaches to scalable genome analysis. *BMC Bioinformatics*, 24(1), Article number 354. https://doi.org/10.1186/s12859-023-05470-2

Ali, A., Almaiah, M. A., Hajjej, F., Pasha, M. F., Fang, O. H., Khan, R., Teo, J., & Zakarya, M. (2022). An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach for Healthcare Systems Using Neural Network. *Sensors*, 22(2), 572. https://doi.org/10.3390/s22020572

Ali, A., Al-rimy, B. A. S., Tin, T. T., Altamimi, S. N., Qasem, S. N., & Saeed, F. (2023). Empowering Precision Medicine: Unlocking Revolutionary Insights through Blockchain-Enabled Federated Learning and Electronic Medical Records. *Sensors*, 23(17), 7476. https://doi.org/10.3390/s23177476

Al-Kaabi, R. A., & Abdullah, A. A. (2023). A survey: medical health record data security based on interplanetary file system and blockchain technologies. *Indonesian Journal of Electrical Engineering and Computer Science*, 30(1), 586–597. https://doi.org/10.11591/ijeecs.v30.i1.pp586-597

Alqaralleh, B. A. Y., Vaiyapuri, T., Parvathy, V. S., Gupta, D., Khanna, A., & Shankar, K. (2024). Blockchain-assisted secure image transmission and diagnosis model on Internet of Medical Things Environment. *Personal and Ubiquitous Computing*, 28(1), 17–27. https://doi.org/10.1007/s00779-021-01543-2

Amin, M. R., Zuhairi, M. F., & Saadat, M. N. (2021). Transparent Data Dealing: Hyperledger Fabric Based Biomedical Engineering Supply Chain. In *Proceedings of the 2021 15th International Conference on Ubiquitous Information Management and Communication, IMCOM 2021*. IEEE. https://doi.org/10.1109/IMCOM51814.2021.9377418

Arvind, S., Shankar, S., Hemanand, D., Kumar, C. A., & Rao, G. N. (2023). A study on data protection in cloud environment. *International Journal on Recent and Innovation Trends in Computing and Communication*, 11(10), 1748–1753. https://doi.org/10.17762/ijritcc.v11i10.8750

Bamakan, S. M. H., Babaei Bondarti, A., Babaei Bondarti, P., & Qu, Q. (2021). Blockchain technology forecasting by patent analytics and text mining. *Blockchain: Research and Applications*, 2(2), 100019. https://doi.org/10.1016/j.bcra.2021.100019

Banita, P. S. (2024). Role of Blockchain Technology in Data Security for Healthcare. *Ingenierie Des Systemes d'Information*, 29(1), 253–260. https://doi.org/10.18280/isi.290125

Baysal, M. V., Özcan-Top, Ö., & Betin-Can, A. (2023). Blockchain technology applications in the health domain: a multivocal literature review. *Journal of Supercomputing*, 79(3), 3112–3156. https://doi.org/10.1007/s11227-022-04772-1

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

Brogan, J., Baskaran, I., & Ramachandran, N. (2018). Authenticating Health Activity Data Using Distributed Ledger Technologies. *Computational and Structural Biotechnology Journal*, 16, 257–266. https://doi.org/10.1016/j.csbj.2018.06.004

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

Chen, S., Li, Q., Wang, W., Yang, Y., & Jiang, J. (2021). Application of blockchain in the cluster of unmanned aerial vehicles. *IET Blockchain*, 1(1), 33–40. https://doi.org/10.1049/blc2.12004

Chen, W., Zhu, S., Li, J., Wu, J., Chen, C. L., & Deng, Y. Y. (2021). Authorized shared electronic medical record system with proxy re-encryption and blockchain technology. *Sensors*, 21(22), 7765. https://doi.org/10.3390/s21227765

Chhabra, A., Saha, R., Kumar, G., & Kim, T. H. (2024). Navigating the Maze: Exploring Blockchain Privacy and Its Information Retrieval. *IEEE Access*, 12, 32089–32110. https://doi.org/10.1109/ACCESS.2024.3370857

Costa, L. Da, Pinheiro, B., Cordeiro, W., Araujo, R., & Abelem, A. (2023). Sec-Health: A Blockchain-Based Protocol for Securing Health Records. *IEEE Access*, 11, 16605–16620. https://doi.org/10.1109/ACCESS.2023.3245046

Damar, M., Aydın, Ö., & Erenay, F. S. (2025). Blockchain Technology in Digital Health and Medical Technologies. *Blockchain in Healthcare Today*, 8(3), 409. https://doi.org/10.30953/bhty.v8.409

Dedeturk, B. A., Soran, A., & Bakir-Gungor, B. (2021). Blockchain for genomics and healthcare: A literature review, current status, classification and open issues. *PeerJ*, 9, e12130. https://doi.org/10.7717/peerj.12130

Dursi, L. J., Bozoky, Z., De Borja, R., Li, J., Bujold, D., Lipski, A., Rashid, S. F., Sethi, A., Memon, N., Naidoo, D., Coral-Sasso, F., Wong, M., Quirion, P., Lu, Z., Agarwal, S., Pavlov, K., Ponomarev, A., Husic, M., Pace, K., . . . Brudno, M. (2021). CANDIG: Secure federated genomic queries and analyses across jurisdictions. *bioRxiv (Cold Spring Harbor Laboratory)*. https://doi.org/10.1101/2021.03.30.434101

Ezil Sam Leni, A., Shankar, R., Thiagarajan, R., & Patil, V. R. (2023). Block-chain based Secure Data Access over Internet of Health Application Things (IHoT). *KSII Transactions on Internet and Information Systems*, 17(5), 1484–1502. https://doi.org/10.3837/tiis.2023.05.010

Farahat, I. S., Aladrousy, W., Elhoseny, M., Elmougy, S., & Tolba, A. E. (2022). Improving Healthcare Applications Security Using Blockchain. *Electronics*, 11(22), 3786. https://doi.org/10.3390/electronics11223786

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

Gomes, C. M., Marchini, G., Júnior, J. de B., Carvalhal, G., Caldeira, M. P. R., Saldiva, P. H., Krieger, J. E., Agena, F., Reis, S., Paschoal, C., Froes, M., Srougi, M., Nahas, W. C., & Favorito, L. A. (2024). The landscape of biomedical research funding in Brazil: A current overview. *International Brazilian Journal of Urology*, 50(2), 209–222. https://doi.org/10.1590/S1677-5538.IBJU.2024.9905

Grishin, D., Obbad, K., & Church, G. M. (2019). Data privacy in the age of personal genomics. *Nature Biotechnology*, 37(10), 1115–1117. https://doi.org/10.1038/s41587-019-0271-3

Gross, M., & Miller, R. C. (2021). Protecting privacy and promoting learning: blockchain and privacy preserving technology should inform new ethical guidelines for health data. *Health and Technology*, 11(5), 1165–1169. https://doi.org/10.1007/s12553-021-00589-9

Gürsoy, G., Bjornson, R., Green, M. E., & Gerstein, M. (2020a). Using blockchain to log genome dataset access: efficient storage and query. *BMC Medical Genomics*, 13, 78. https://doi.org/10.1186/s12920-020-0716-z

Gürsoy, G., Brannon, C. M., & Gerstein, M. (2020b). Using Ethereum blockchain to store and query pharmacogenomics data via smart contracts. *BMC Medical Genomics*, 13(1), 74. https://doi.org/10.1186/s12920-020-00732-x

Gürsoy, G., Brannon, C. M., Ni, E., Wagner, S., Khanna, A., & Gerstein, M. (2022). Storing and analyzing a genome on a blockchain. *Genome Biology*, 23(1), 134. https://doi.org/10.1186/s13059-022-02699-7

Hosseini, M., Pratas, D., & Pinho, A. J. (2019). Cryfa: A secure encryption tool for genomic data. *Bioinformatics*, 35(1), 146–148. https://doi.org/10.1093/bioinformatics/bty645

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

Huang, J., Qi, Y. W., Asghar, M. R., Meads, A., & Tu, Y. C. (2022). Sharing medical data using a blockchain-based secure EHR system for New Zealand. *IET Blockchain*, 2(1), 13–28. https://doi.org/10.1049/blc2.12012

Hussein, A. F., ALZubaidi, A. K., Habash, Q. A., & Jaber, M. M. (2019). An adaptive biomedical data managing scheme based on the blockchain technique. *Applied Sciences*, 9(12), 2494. https://doi.org/10.3390/app9122494

Ismail, L., Materwala, H., & Zeadally, S. (2019). Lightweight Blockchain for Healthcare. *IEEE Access*, 7, 149935–149951. https://doi.org/10.1109/ACCESS.2019.2947613

Jang, S., Rahmadika, S., Shin, S. U., & Rhee, K. H. (2021). PDPM: A patient-defined data privacy management with nudge theory in decentralized e-health environments. *IEICE Transactions on Information and Systems*, E104D(11), 1839–1849. https://doi.org/10.1587/TRANSINF.2021NGP0015

Jennath, H. S., Anoop, V. S., & Asharaf, S. (2020). Blockchain for healthcare: Securing patient data and enabling trusted artificial intelligence. *International Journal of Interactive Multimedia and Artificial Intelligence*, 6(3), 15–23. https://doi.org/10.9781/ijimai.2020.07.002

Jeong, S., Shen, J. H., & Ahn, B. (2021). A Study on Smart Healthcare Monitoring Using IoT Based on Blockchain. *Wireless Communications and Mobile Computing*, 2021, 9932091. https://doi.org/10.1155/2021/9932091

Jia, D. Y., Xin, J. C., Wang, Z. Q., Lei, H., & Wang, G. R. (2021). SE-Chain: A Scalable Storage and Efficient Retrieval Model for Blockchain. *Journal of Computer Science and Technology*, 36(3), 693–706. https://doi.org/10.1007/s11390-020-0158-2

Jia, W., Wu, Q., Li, R., Hou, S., & Kang, C. (2024). Role of CENPF and NDC80 in the rehabilitation nursing of hepatocellular carcinoma and cirrhosis: An observational study. *Medicine*, 103(18), E37984. https://doi.org/10.1097/MD.0000000000037984

Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering – A systematic literature review. *Information and Software Technology*, 51(1), 7–15. https://doi.org/10.1016/j.infsof.2008.09.009

Lemieux, V. L., Hofman, D., Hamouda, H., Batista, D., Kaur, R., Pan, W., Costanzo, I., Regier, D., Pollard, S., Weymann, D., & Fraser, R. (2020). Having Our "Omic" Cake and Eating It Too?: Evaluating User Response to Using Blockchain Technology for Private and Secure Health Data Management and Sharing. *Frontiers in Blockchain*, 3, 558705. https://doi.org/10.3389/fbloc.2020.558705

Li, X., Tao, B., Dai, H. N., Imran, M., Wan, D., & Li, D. (2021). Is blockchain for Internet of Medical Things a panacea for COVID-19 pandemic? *Pervasive and Mobile Computing*, 75. https://doi.org/10.1016/j.pmcj.2021.101434

Liu, H., Crespo, R. G., & Martínez, O. S. (2020). Enhancing privacy and data security across healthcare applications using Blockchain and distributed ledger concepts. *Healthcare*, 8(3), 243. https://doi.org/10.3390/healthcare8030243

Lu, X., Fu, S., Jiang, C., & Lio, P. (2021). A Fine-Grained IoT Data Access Control Scheme Combining Attribute-Based Encryption and Blockchain. *Security and Communication Networks*, 2021, 5308206. https://doi.org/10.1155/2021/5308206

Malamas, V., Kotzanikolaou, P., Dasaklis, T. K., & Burmester, M. (2020). A Hierarchical Multi Blockchain for Fine Grained Access to Medical Data. *IEEE Access*, 8, 134393–134412. https://doi.org/10.1109/ACCESS.2020.3011201

Mallikarjuna, B., Shrivastava, G., & Sharma, M. (2022). Blockchain technology: A DNN token-based approach in healthcare and COVID-19 to generate extracted data. *Expert Systems*, 39(3), e12778. https://doi.org/10.1111/exsy.12778

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

Mao, X., Li, C., Zhang, Y., Zhang, G., & Xing, C. (2024). Efficient and Secure Management of Medical Data Sharing Based on Blockchain Technology. *Applied Sciences*, 14(15), 6816. https://doi.org/10.3390/app14156816

Mayer, A. H., Rodrigues, V. F., Da Costa, C. A., Da Rosa Righi, R., Roehrs, A., & Antunes, R. S. (2021). FogChain: A Fog Computing Architecture Integrating Blockchain and Internet of Things for Personal Health Records. *IEEE Access*, 9, 122723–122737. https://doi.org/10.1109/ACCESS.2021.3109822

Mudannayake, O., Indika, A., Jayasinghe, U., Lee, G. M., & Alawatugoda, J. (2025). On Privacy-Preserved Machine Learning Using Secure Multi-Party Computing: Techniques and Trends. *Computers, Materials & Continua*, 85(2), 2527–2578. https://doi.org/10.32604/cmc.2025.068875

Murphy, S., Reilly, P., & Murphy, T. (2021). Assessing the potential use of blockchain technology to improve the sharing of public health data in a western Canadian province. *Health and Technology*, 11(3), 547–556. https://doi.org/10.1007/s12553-021-00539-5

Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2019). Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems. *IEEE Access*, 7, 66792–66806. https://doi.org/10.1109/ACCESS.2019.2917555

Ni, E., Tang, X., Zhou, X., Lee, D., Elhussein, A., Knight, E., Gürsoy, G., & Gerstein, M. (2025). Recent advances and future prospects for blockchain in biomedicine. *Cell Reports Methods*, 5(8), 101114. https://doi.org/10.1016/j.crmeth.2025.101114

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

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

Rana, Sumit Kumar, Rana, Sanjeev Kumar, Nisar, K., Ag Ibrahim, A. A., Rana, A. K., Goyal, N., & Chawla, P. (2022). Blockchain Technology and Artificial Intelligence Based Decentralized Access Control Model to Enable Secure Interoperability for Healthcare. *Sustainability*, 14(15), 9471. https://doi.org/10.3390/su14159471

Rohini, K. R., Rajakumar, P. S., & Geetha, S. (2024). Smart Patient Consent Management Model for Health Information Exchange Based on Blockchain Technology. *Journal of Computer Science*, 20(7), 730–741. https://doi.org/10.3844/jcssp.2024.730.741

Saeed, H., Malik, H., Bashir, U., Ahmad, A., Riaz, S., Ilyas, M., Bukhari, W. A., & Khan, M. I. A. (2022). Blockchain technology in healthcare: A systematic review. *PLoS ONE*, 17(4), 0266462. https://doi.org/10.1371/journal.pone.0266462

Saidi, H., Labraoui, N., Ari, A. A. A., Maglaras, L. A., & Emati, J. H. M. (2022). DSMAC: Privacy-Aware Decentralized Self-Management of Data Access Control Based on Blockchain for Health Data. *IEEE Access*, 10, 101011–101028. https://doi.org/10.1109/ACCESS.2022.3207803

Sharma, A., Sarishma, Tomar, R., Chilamkurti, N., & Kim, B. G. (2020). Blockchain based smart contracts for internet of medical things in e-healthcare. *Electronics*, 9(10), 1609. https://doi.org/10.3390/electronics9101609

Sohail, M. N., Anjum, A., Saeed, I. A., Syed, M. H., Jantsch, A., & Rehman, S. (2024). Optimizing Industrial IoT Data Security Through Blockchain-Enabled Incentive-Driven Game Theoretic Approach for Data Sharing. *IEEE Access*, 12, 51176–51192. https://doi.org/10.1109/ACCESS.2024.3382571

Srinivasu, P. N., Bhoi, A. K., Nayak, S. R., Bhutta, M. R., & Woźniak, M. (2021). Blockchain technology for secured healthcare data communication among the non-terminal nodes in iot architecture in 5g network. *Electronics*, 10(12), 1437. https://doi.org/10.3390/electronics10121437

Sultana, M., Hossain, A., Laila, F., Taher, K. A., & Islam, M. N. (2020). Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology. *BMC Medical Informatics and Decision Making*, 20(1), 256. https://doi.org/10.1186/s12911-020-01275-y

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 block-chain-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

T, D. B., T, T. P. H., P, T. N. D., T, P. N., D, K. T., G, K. H., T, N. B., & K, B. L. (2024). Developing a Patient-Centric Healthcare IoT Platform with Blockchain and Smart Contract Data Management. *International Journal of Advanced Computer Science and Applications*, 15(4), 1039–1046. https://doi.org/10.14569/ijacsa.2024.01504115

Tagde, P., Tagde, S., Bhattacharya, T., Tagde, P., Chopra, H., Akter, R., Kaushik, D., & Rahman, M. H. (2021). Blockchain and artificial intelligence technology in e-Health. *Environmental Science and Pollution Research*, 28(38), 52810–52831. https://doi.org/10.1007/s11356-021-16223-0

Tan, X., Kang, Z., Wei, F., Gao, C., Wei, Z., & Huang, H. (2022). MB-BC: Drug Traceability System Based on Multibranched Blockchain Structure. *Wireless Communications and Mobile Computing*, 2022, 5163003. https://doi.org/10.1155/2022/5163003

Tandon, A., Dhir, A., Islam, N., & Mäntymäki, M. (2020). Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. *Computers in Industry*, 122, 103290. https://doi.org/10.1016/j.compind.2020.103290

Tao, J., & Ling, L. (2021). Practical Medical Files Sharing Scheme Based on Blockchain and Decentralized Attribute-Based Encryption. *IEEE Access*, 9, 118771–118781. https://doi.org/10.1109/ACCESS.2021.3107591

Usman, M., Kallhoff, V., & Khurshid, A. (2021). The case for establishing a blockchain research and development program at an academic medical center. *Blockchain in Healthcare Today*, 4, 161. https://doi.org/10.30953/bhty.v4.161

Verma, S., Srivastava, M., Fatima, S., & Mishra, S. K. (2023). Enhancing security in Blockchain Technology: A Comprehensive study. *Journal for ReAttach Therapy and Developmental Diversities*, 6(8s), 941-949. https://doi.org/10.53555/jrtdd.v6i8s.2910

Xu, G., Yao, T., Zhang, K., Meng, X., Liu, X., Xiao, K., & Chen, X. (2023). An Optimized Byzantine Fault Tolerance Algorithm for Medical Data Security. *Electronics*, 12(24), 5045. https://doi.org/10.3390/electronics12245045

Xu, Q., Jin, C., Rasid, M. F. B. M., Veeravalli, B., & Aung, K. M. M. (2018). Blockchain-based decentralized content trust for docker images. *Multimedia Tools and Applications*, 77(14), 18223–18248. https://doi.org/10.1007/s11042-017-5224-6

Yang, J., Onik, M. M. H., Lee, N. Y., Ahmed, M., & Kim, C. S. (2019). Proof-of-familiarity: A privacy-preserved blockchain scheme for collaborative medical decision-making. *Applied Sciences*, 9(7), 1370. https://doi.org/10.3390/app9071370

Yao, S., Jing, P., Li, P., & Chen, J. (2022). A multi-dimension traceable privacy-preserving prevention and control scheme of the COVID-19 epidemic based on blockchain. *Connection Science*, 34(1), 1654–1677. https://doi.org/10.1080/09540091.2022.2077912

Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2022). Blockchain for healthcare data management: opportunities, challenges, and future recommendations. *Neural Computing and Applications*, 34(14), 11475–11490. https://doi.org/10.1007/s00521-020-05519-w

Zala, K., Thakkar, H. K., Jadeja, R., Singh, P., Kotecha, K., & Shukla, M. (2022). PRMS: Design and Development of Patients' E-Healthcare Records Management System for Privacy Preservation in Third Party Cloud Platforms. *IEEE Access*, 10, 85777–85791. https://doi.org/10.1109/ACCESS.2022.3198094

Zass, L., Johnston, K., Benkahla, A., Chaouch, M., Kumuthini, J., Radouani, F., Mwita, L. A., Alsayed, N., Allie, T., Sathan, D., Masamu, U., Seuneu Tchamga, M. S., Tamuhla, T., Samtal, C., Nembaware, V., Gill, Z., Ahmed, S., Hamdi, Y., Fadlelmola, F., ... Mulder, N. (2023). Developing Clinical Phenotype Data Collection Standards for Research in Africa. *Global Health, Epidemiology and Genomics*, 2023, 6693323. https://doi.org/10.1155/2023/6693323

Zghaibeh, M., Farooq, U., Hasan, N. U., & Baig, I. (2020). SHealth: A Blockchain-Based Health System with Smart Contracts Capabilities. *IEEE Access*, 8, 70030–70043. https://doi.org/10.1109/ACCESS.2020.2986789

Zhang, P., Kelley, A., Schmidt, D. C., & White, J. (2023). Design pattern recommendations for building decentralized healthcare applications. *Frontiers in Blockchain*, 6, 1006058. https://doi.org/10.3389/fbloc.2023.1006058

Acta Informatica Pragensia is published by the Prague University of Economics and Business, Czech Republic | eISSN: 1805-4951