information

MDPI

Systematic Review

Smart Contracts, Blockchain, and Health Policies: Past, Present, and Future

Kenan Kaan Kurt [1,*], Meral Timurtaş [2], Sevcan Pınar [3], Fatih Ozaydin [4,5,*] and Serkan Türkeli [2,6]

[1] Institute of Health Sciences, Marmara University, 34722 Istanbul, Türkiye
[2] Department of Health Informatics and Technologies, Faculty of Health Sciences, Marmara University, 34722 Istanbul, Türkiye
[3] Department of Business Administration, Faculty of Art and Social Sciences, Istanbul Galata University, 34430 Istanbul, Türkiye; sevcan.pinar@galata.edu.tr
[4] Institute for International Strategy, Tokyo International University, 4-42-31 Higashi-Ikebukuro, Toshima-ku, Tokyo 170-0013, Japan
[5] Nanoelectronics Research Center, Kosuyolu Mah., Lambaci Sok., Kosuyolu Sit., No:9E/3 Kadikoy, 34718 Istanbul, Türkiye
[6] TESODEV Technology Solutions Development Company Ltd., Küçükyalı, 34840 Istanbul, Türkiye
* Correspondence: kenankurt@marun.edu.tr (K.K.K.); fatih@tiu.ac.jp (F.O.)

Abstract

The integration of blockchain technology into healthcare systems has emerged as a technical solution for enhancing data security, protecting privacy, and improving interoperability. Blockchain-based smart contracts offer reliability, transparency, and efficiency in healthcare services, making them a focal point of many studies. However, challenges such as scalability, regulatory compliance, and interoperability continue to limit their widespread adoption. This study conducts a comprehensive literature review to assess blockchain-driven health data management, focusing on the classification of blockchain-based smart contracts in health policy and the health protocols and standards applicable to blockchain-based smart contracts. This review includes 80 core studies published between 2019 and 2025, identified through searches in PubMed, Scopus, and Web of Science using the PRISMA method. Risk of bias and methodological quality were assessed using the Joanna Briggs Institute tool. The findings highlight the potential of blockchain-enabled smart contracts in health policy management, emphasizing their advantages, limitations, and implementation challenges. Additionally, the research underscores their transformative impact on digital health policies in ensuring data integrity, enhancing patient autonomy, and fostering a more resilient healthcare ecosystem. Recent advancements in quantum technologies are also considered as they present both novel opportunities and emerging threats to the future security and design of healthcare blockchain systems.

Keywords: blockchain; data privacy; electronic health records; healthcare security; health policies; smart contracts; systematic review

Academic Editor: Muneer Ahmad

Received: 20 August 2025
Revised: 26 September 2025
Accepted: 27 September 2025
Published: 2 October 2025

Citation: Kurt, K.K.; Timurtaş, M.; Pınar, S.; Ozaydin, F.; Türkeli, S. Smart Contracts, Blockchain, and Health Policies: Past, Present, and Future. *Information* **2025**, *16*, 853. https://doi.org/10.3390/info16100853

1. Introduction

Ensuring the availability, integrity, and confidentiality of electronic health records (EHRs) remains challenging as weak access governance can expose patient data to unauthorized disclosure [1]. Privacy protection is essential as cloud-based repositories and connected medical/IoT devices expand the attack surface in healthcare systems. Addressing these risks in blockchain-enabled settings requires strong authentication and authorization, verifiable auditability and consent management, and compliance with the HIPAA

and GDPR within permissioned networks. Prior studies have leveraged smart contracts for access control, provenance, and fraud detection; however, vulnerabilities and governance—spanning identity, consensus, and operational controls—remain open concerns [2]. In the healthcare literature, smart contracts typically appear as auxiliary components to IoT-driven data sharing rather than as first-class policy mechanisms [3]. The applications span clinical-trial transparency, data-management workflows, and authentication, among others [4,5].

While systematic reviews have examined blockchain in healthcare, few have categorized its smart contracts in health policy [2]. This study presents a theoretically justified classification framework grounded in healthcare informatics theory. The framework is made explicit and operational, thus outlining the step-by-step classification of a given study or system. We develop a theoretically grounded taxonomy following an established classification methodology that addresses compliance constraints, cryptographic mechanisms, and policy implications, clarifying blockchain's regulatory role in digital-health governance. We operationalize the taxonomy (RQ1) by mapping permissioned consensus families (e.g., RAFT and IBFT) to representative healthcare tasks and case studies, yielding a practical set of decision rules. Our synthesis distills recurrent dimensions and gaps, translating them into taxonomy-driven guidance for researchers and practitioners. Overall, we evaluate blockchain-based smart contracts for health-policy use, with an emphasis on consent enforcement, auditability, and verifiable automation in clinical operations.

2. Background

2.1. State of the Art on Blockchain-Based Smart Contracts in Health Management

Permissioned distributed ledgers offer tamper-evident logging and policy-driven access control, which can enhance transparency and operational assurance in healthcare and insurance workflows [5,6]. Smart contracts automate rule-based transactions under these governance constraints, enabling verifiable consent, auditing, and compliant exchanges [7].

Because platforms differ in consensus, finality, identity, and governance, platform selection should be aligned with workflow and regulatory requirements rather than raw throughput figures. Permissioned frameworks (e.g., Hyperledger Fabric) are frequently adopted in consortium settings that require identity, access control, and deterministic finality. Benchmarking with tools such as Hyperledger Caliper has reported lower resource usage in controlled testbeds for permissioned networks compared with PoW-based baselines [8]. The reported lab-scale benchmarks further cite throughputs up to ≈1000 TPS with sub-second latencies under specific network sizes and configurations [9]. To minimize redundancy, we next summarize the consensus families relevant to healthcare and defer expanded platform-specific benchmarks to the Results and the Supplementary File. Taken together, these benchmarks are informative but not dispositive; moving from controlled testbeds to live clinical workflows typically exposes governance, auditing, and standard-alignment hurdles that prototypes seldom encounter.

AI-assisted approaches are being investigated for security analytics and transaction validation. However, AI-driven optimization introduces computational complexity that conflicts with blockchain's distributed consensus requirements, and the centralized nature of AI training contradicts blockchain's decentralized philosophy. A Hyperledger Fabric–based remote patient monitoring prototype validates real-time processing and security [10]. In remote healthcare monitoring, blockchain–smart-contract frameworks enhance protection against fraud and tampering [11], while AI-integrated blockchain for medical IoT strengthens detection and network security [12]. AI-empowered blockchain architectures enhance fraud detection in decentralized healthcare transactions [13] and strengthen secure access in medical IoT environments [12].

Hyperledger Fabric is preferred for its security and controlled access, while Ethereum supports more decentralized smart contracts [7]. Similarly, next-generation blockchain protocols such as Algorand and Bitcoin-NG demonstrate significantly higher transaction throughput for high-demand applications, offering scalable solutions beyond traditional proof-of-work architectures [7]. These advancements underscore the importance of selecting appropriate blockchain platforms tailored to application-specific performance requirements.

While public-chain designs such as Algorand and Bitcoin-NG are frequently cited for higher throughput at the protocol level, healthcare studies predominantly adopt permissioned identity-gated networks where auditability and standard alignment outweigh raw TPS [14,15]; our synthesis reflects this divergence. Platform capabilities vary widely across consensus and identity models. Protocol-level studies often cite Algorand and Bitcoin-NG as higher-throughput designs [14,15]; however, healthcare implementations predominantly adopt permissioned frameworks because governance, auditability, and standard compliance (e.g., the HIPAA/GDPR) typically outweigh raw TPS. The reported testbeds in health contexts therefore show tens of TPS with second-level latencies rather than public-chain peak figures [9] (see Supplementary File).

Protocol-level studies often cite higher peak TPS (e.g., 1.000 TPS) under simplified benchmarks; however, healthcare deployments predominantly report tens of TPS due to compliance and governance overheads, so peak figures should not be taken as decision-useful without healthcare-realistic workloads. Smart contracts support record auditing and controlled data sharing; authentication and authorization typically rely on public-key infrastructures and role-based access [16]. A Hyperledger Caliper performance analysis confirms that permissioned blockchain architectures like Hyperledger Fabric provide low-latency, scalable, and secure transactions [10]. Ucbas et al. [17] compared Fabric with a PoW-based Ethereum baseline and reported lower resource usage under their test configuration.

Mnasri et al. [18] reported Hyperledger Fabric's effectiveness in medical record management. Yang et al. [19] evaluated cross-chain medical-data exchange and observed improved throughput under test conditions. Qiao et al. [20] developed an AI-assisted permissioned system for IoT medical data and demonstrated scalability in a controlled testbed. While the testbed results appear to be promising, real-world deployment faces critical challenges, including model drift in dynamic healthcare environments and the interpretability requirements for clinical decision support.

Complementary ML baselines (e.g., SVM and XGBoost) have been applied to EHR-access anomaly detection and supply-chain fraud analytics [21,22]. However, these AI-augmented approaches face critical vulnerabilities that limit their practical deployment: (1) data imbalance in healthcare datasets can lead to biased fraud detection, potentially flagging legitimate emergency access as anomalous; (2) SVM and XGBoost models lack interpretability, making it difficult for healthcare administrators to understand why specific transactions were flagged during regulatory audits; (3) adversarial attacks can manipulate input features to evade detection, compromising the entire security framework.

2.2. Conceptual Framework: Social Solidarity in Health Data Governance

Social solidarity in healthcare technology contexts refers to collective responsibility for equitable access to health innovations and shared governance of health data resources [23]. Unlike market-based individualism, this framework emphasizes commons-based management of the health information infrastructure, where blockchain technology serves as an institutional mechanism for distributed decision-making and benefit-sharing [24–26]. This conceptualization moves beyond rhetorical invocation to provide an analytical

framework for evaluating how technological design choices affect power distribution in healthcare systems.

In health policy and bioethics, "social solidarity" has been framed as a collective value underpinning equitable access, resource pooling, and mutual support in healthcare systems [23,27]. In our context, blockchain infrastructures may operationalize this solidarity by ensuring transparency, distributed trust, and resistance to opportunistic exclusion.

Terminology. Permissioned blockchain: identity-gated ledger with access controls; public blockchain: open participation with probabilistic or committee-based finality; finality: irreversibility of a committed transaction; consensus families: RAFT (crash-fault-tolerant and leader-based), IBFT/PBFT (Byzantine-fault-tolerant and deterministic), and PoA (identity-anchored). Clinical deployments typically favor permissioned consensus with off-chain clinical payloads.

3. Methods

We conducted a PRISMA-guided systematic review [28] covering January 2019–August 2025 (last update: 19 August 2025) across PubMed, Scopus, and Web of Science to classify blockchain-based smart contracts in health policy.

3.1. Study Design

The review followed a pre-specified protocol covering search, screening, data extraction, and appraisal. Procedures adhered to PRISMA 2020 guidance and established systematic-review stages [29]. The protocol specified search, screening, data extraction, and appraisal steps.

3.2. Information Sources and Search Strategy

In line with the PRISMA 2020 guidelines, a comprehensive literature search was conducted in PubMed, Scopus, and Web of Science (WoS). The search covered the period from January 2019 to August 2025, with the final update performed on 19 August 2025. A combination of controlled vocabulary (e.g., MeSH terms) and free-text keywords was employed to capture variations in terminology related to blockchain, smart contracts, distributed ledger technologies, and consensus mechanisms. Boolean operators ("AND"; "OR"), truncations, and filters were applied to refine the scope of the search. Searches were conducted in PubMed, Scopus, and Web of Science (WoS) for the period January 2019–19 August 2025. Controlled subject terms were combined with free-text keywords; Boolean operators ("AND"; "OR"), truncation, and filters were applied. Document-type filters were set to include peer-reviewed journal articles and peer-reviewed full-paper conference proceedings; editorials, abstract-only short papers/posters, books/book chapters, and non-peer-reviewed sources were excluded. Full search strings and applied filters are provided in the Supplementary File.

Filters were restricted to peer-reviewed journal articles and peer-reviewed full-text conference papers in English; abstract-only or short conference items (e.g., posters, extended abstracts, and workshop briefs), editorials, books/book chapters, and non-peer-reviewed sources were excluded. Full search strings and applied filters are provided in the Supplementary File. Full search strings for each database, together with applied filters, are provided in the Supplementary File, ensuring transparency and reproducibility.

Inclusion criteria required studies to involve blockchain-based applications in a healthcare setting, with smart-contract logic explicitly described, and to be published in English peer-reviewed venues.

We excluded papers without a healthcare context or without a smart-contract application component (e.g., cryptography-only/theoretical works, domain-agnostic security

evaluations, and abstract-only items), consistent with our eligibility criteria. Exclusion criteria therefore comprised cryptography-only approaches, theoretical models without implementation, domain-agnostic performance assessments, and abstracts or posters lacking full-text detail.

3.3. Study Selection

Following the systematic review methodologies [30,31], this study refined 950 identified articles to 80 primary studies. We excluded papers without a healthcare context or without a smart-contract application component (e.g., cryptography-only/theoretical works, domain-agnostic security evaluations, and abstract-only items), consistent with our eligibility criteria.

Exclusion criteria emphasized relevance to blockchain, smart contracts, and healthcare. We excluded studies that lacked an application or smart-contract component or any empirical evaluation; were purely cryptography-only/theoretical; presented domain-agnostic blockchain security evaluations lacking a healthcare context; or were otherwise unrelated.

We included peer-reviewed journal or full-paper conference studies (2019–2025) that (i) addressed healthcare and (ii) implemented or analyzed smart contracts or smart-contract-governed blockchain workflows for health data/policy. Abstract-only or short conference items (e.g., poster/extended abstract) were not eligible (see the Supplementary File, case B8).

We excluded (a) papers with no healthcare context, (b) works on blockchain/cryptography without a smart-contract component or any health application, (c) editorials, tutorials, posters, and non-English items, and (d) duplicates/retractions. Title/abstract screening and full-text review were performed independently by two reviewers; conflicts were resolved by a third reviewer. For transparency, full-text exclusion reasons were coded to one primary category per record: E1 'No healthcare context', E2 'No smart-contract component', E3 'Purely cryptographic/theoretical without application', E4 'Insufficient methodological reporting', E5 'Non-primary/secondary evidence', and E6 'Not in English/No full text'. Category-level counts for full-text exclusions (E1–E6) are reported in the PRISMA flow diagram and Supplementary File -min (counts only); representative borderline exclusions with the primary reason are also listed. Abstract-only or short conference items were not eligible (see Supplementary File).

Selection Breakdown:

- 950 articles identified;
- 89 duplicates removed;
- 239 excluded due to language, etc.;
- 413 excluded due to keywords, title, and abstract;
- 129 excluded due to ambiguous technical material and inadequate research, leaving 80.

Non-scientific sources and blockchain financial ledger studies were excluded.

In total, 950 records were identified. After removing 89 duplicates, 861 records remained. During screening, 239 were excluded (non-journal/non-full-paper, non-English, and bibliographies/retractions), and 413 were excluded for keyword/title/abstract mismatch. At full-text, 129 records were excluded, with primary reasons E1 (no healthcare context), E2 (no smart-contract component), E3 (cryptography-only without application), E4 (insufficient methodological reporting), E5 (non-primary/secondary), and E6 (language/no full text). Therefore, 80 studies were included. Reasons and counts are shown in Figure 1 (PRISMA) and in Supplementary File. A full per-study exclusion list was not compiled due to the scale of screening; however, category-level counts and representative examples are provided (Supplementary File).

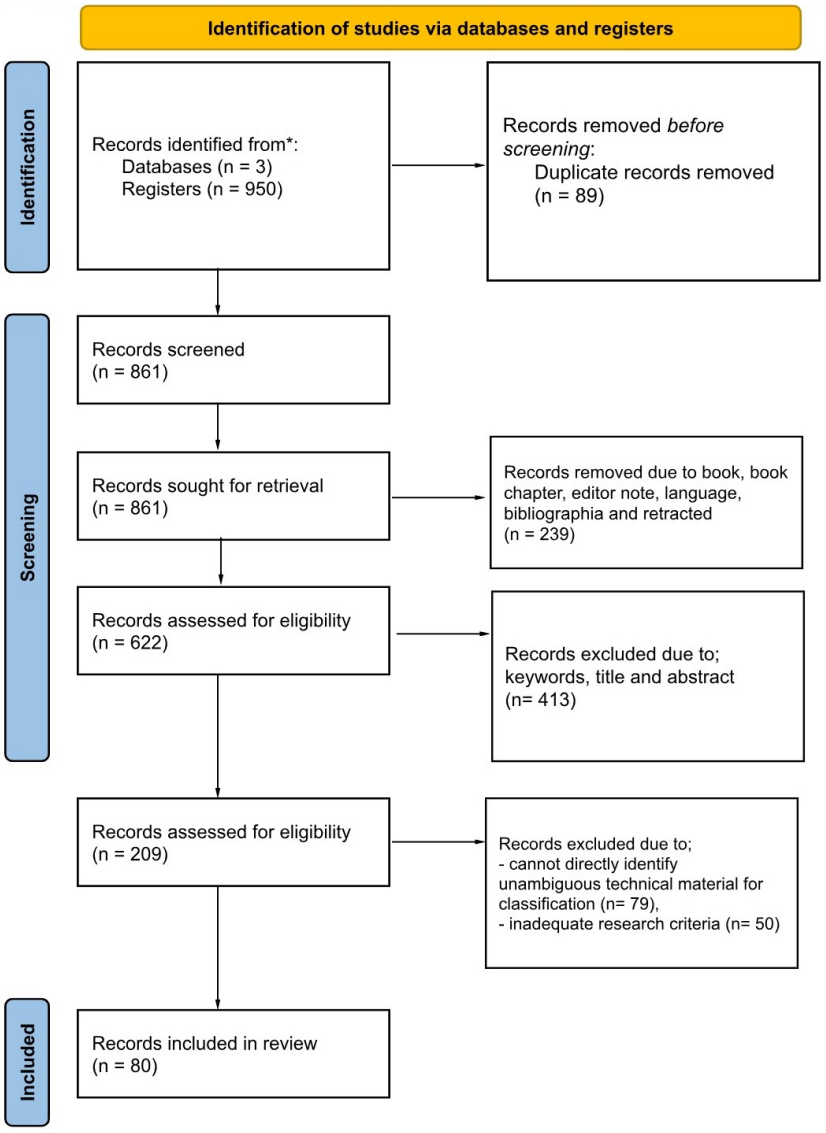

Figure 1. PRISMA flow diagram utilized in this review. * See the text and Supplementary Material for details.

3.4. Research Questions

The development of research questions is a critical component of any systematic review [30,31]. Here, our objective is to define the role of blockchain-based smart contracts in health management policy by addressing key technological aspects, challenges, and future prospects. The research guidance questions (GQs) are categorized into two groups:

GQ1: What taxonomy best classifies blockchain-based smart contracts for health-policy use?

GQ2: Which healthcare protocols and standards (e.g., FHIR; HIPAA/GDPR mapping) should inform smart-contract design?

3.5. Search Strategy

To ensure the reproducibility of this review, a structured search strategy was developed. This included defining search terms, scope, and Boolean operators. Following the methodology recommended by [30], the final search string was (“Blockchain”) AND (“Smart contract”) AND ((“healthcare”) OR (“health”)) OR ((“health record”) OR (“EHR”) OR (“PHR”) OR (“medical record”) OR (“EMR”)).

3.6. Data Collection Process

Two reviewers independently extracted data using a standardized form.

3.7. Quality Assessment

Following Keele et al. [30], we evaluated

- research aims and contextualization;
- literature review and methodology;
- findings and policy relevance.

Only studies with clear objectives, methodology, and conclusions were included.

3.8. Data Items

The extracted data were predefined in line with the study objectives. Items covered bibliographic information, methodological features (research design, analytical framework, and blockchain application domain), and outcome-related details (reported benefits, challenges, and implications). For transparency, we recorded the venue type (journal vs. full-paper conference) for each included study (see the Supplementary File). Where studies used inconsistent terminology (e.g., "decentralized applications" vs. "smart contracts"), terms were harmonized under a unified coding scheme. Broader analytical categories were applied where needed, and all assumptions and simplifications were explicitly documented.

Beyond benefits and design features, we explicitly coded signals of unsuccessful or mixed deployments (e.g., early termination, testnet-only evaluation, failure to scale beyond a proof of concept, or inability to meet governance/standards), and we surfaced these judgments in the risk-of-bias tables in the Supplementary File.

3.9. Risk-of-Bias Assessment

Empirical studies were appraised with the appropriate Joanna Briggs Institute (JBI) Critical Appraisal Checklist [32], scoring each item 0/1 and reporting a total %JBI. Conceptual/engineering studies were appraised with a Technical Relevance Appraisal (TRA) comprising seven 0–2 criteria (0 = not addressed, 1 = partially, or 2 = fully): T1 healthcare-context specificity; T2 smart-contract specificity (on-chain logic and triggers); T3 evaluation method (empirical testbed/simulation/benchmark); T4 reproducibility (data/code availability and parameterization); T5 security/privacy analysis (threat model and compliance); T6 standard alignment (e.g., FHIR or HIPAA/GDPR mapping); and T7 policy linkage (governance, workflows, and stakeholders). Specifically, the JBI Critical Appraisal Checklists for Analytical Cross-Sectional Studies, Quasi-Experimental (non-randomized) Studies, Case Reports, and Case Series were applied according to each study's design.

Two reviewers worked independently and rated all items; disagreements were resolved by discussion, with adjudication by a third reviewer when necessary. Inter-rater reliability was substantial (Cohen's $\kappa = 0.998$, 95% CI [0.99–1]). Per-study judgments are tabulated in the Supplementary File. Two reviewers independently applied the appropriate JBI Critical Appraisal Checklists (Analytical Cross-Sectional, Quasi-Experimental, Case Report, and Case Series). Disagreements were resolved by discussion, with adjudication by a third reviewer when necessary.

Empirical studies were appraised with the appropriate JBI checklists by two independent reviewers (item-level 0/1; %JBI reported). Conceptual/engineering studies used a TRA grid (7 criteria $\times$ 0–2). Pre-specified thresholds were %JBI $\geq$ 50 (empirical) and TRA $\geq$ 6/14 (conceptual/engineering); sub-threshold studies were retained as context but not emphasized in synthesis; limitations flagged in Supplementary File.

The taxonomy development process followed established theoretical frameworks for classification systems in healthcare informatics. We employed Nickerson et al.'s [33]

taxonomy development method, which combines empirical-to-conceptual and conceptual-to-empirical approaches. The initial conceptual foundation was derived from existing healthcare interoperability standards (HL7 FHIR, IHE profiles) and the blockchain consensus mechanism literature. Empirical refinement occurred through iterative analysis of the 80 included studies, with dimensions and characteristics emerging from systematic coding of smart-contract functionalities, deployment contexts, and technical specifications. The final taxonomy underwent validation through expert review by three blockchain-healthcare specialists.

3.10. Taxonomy Construction and Decision Rules

We operationalized the taxonomy using five dimensions (D1–D5) derived from iterative coding: D1—Healthcare Task Context, D2—Smart-Contract Function, D3—Ledger/Network Model, D4—Consensus Family, and D5—Standards and Compliance Linkage. Each dimension has mutually exclusive categories. To ensure reproducibility, we defined decision rules that map study evidence to categories and resolve overlaps. This rule set is provided as Algorithm 1, and we applied it consistently to all 80 studies.

3.11. Effect Measures and Synthesis Methods

Given heterogeneous designs, no meta-analysis was attempted. We performed a narrative synthesis. Engineering metrics (throughput, latency, finality, and cost), when reported, were extracted and tabulated descriptively (Supplementary File). Studies were grouped by healthcare sub-domains and technical focus; non-health use cases were not pooled.

3.12. Heterogeneity and Sensitivity

Heterogeneity was explored qualitatively across platforms, consensus families, and methods. No formal sensitivity analyses were pre-specified.

3.13. Reporting Bias and Certainty of Evidence

Consistent with our protocol, we did not conduct a formal reporting-bias analysis. To mitigate this risk, we performed broad multi-database searches and applied transparent inclusion/exclusion procedures; any residual uncertainty is explicitly acknowledged in the Discussion. Certainty in the body of evidence was assessed qualitatively, taking into account study design, reporting rigor, and cross-study consistency.

3.14. Certainty Assessment

The certainty of the evidence was not quantified using formal grading frameworks such as GRADE [34] as the studies varied widely in type, methodology, and outcomes. Instead, certainty was assessed qualitatively by examining the design of the studies (conceptual vs. empirical), the clarity and completeness of reporting, and the degree of consistency across findings. Greater confidence was assigned to results that were reported consistently across independent studies, while single-study or context-specific findings were interpreted more cautiously. This approach allowed the synthesis to balance methodological diversity with a reasoned evaluation of evidential strength.

3.15. Performance Considerations in Healthcare Contexts

Reported Caliper-style lab benchmarks have cited up to ≈1000 TPS with sub-second latencies under controlled micro-workloads (small payloads, few peers, and simplified chaincode); these are upper-bound indicators, not typical healthcare performance [9]. Across healthcare-like workloads (EHR exchange, consent, IoT/telehealth, and supply chain), studies in our corpus report ≈ 11–20 TPS with ≈2–4 s confirmation, reflecting richer payloads (HL7/FHIR images), audit trails, and multi-party governance.

These performance figures represent theoretical maximums achieved in isolated environments and have not been replicated in healthcare settings where transactions must accommodate complex data schemas, privacy-preserving computations, audit trail requirements, and multi-party consensus protocols typical of clinical workflows. Public-chain ecosystems (e.g., Ethereum/Solidity) enable a wide range of applications; language and tooling vary across platforms [7].

3.16. Critical Vulnerabilities of AI-Augmented Blockchain Security

The integration of AI models into blockchain healthcare systems introduces several critical vulnerabilities:

- Data Imbalance: Healthcare datasets exhibit severe class imbalances, leading to high false positive rates.
- Model Interpretability: Black-box AI models conflict with healthcare's explainability requirements.
- Adversarial Vulnerability: AI models can be compromised through input manipulation attacks.
- Privacy Conflicts: AI training requirements may violate HIPAA/GDPR patient privacy regulations.

Synthesis of vulnerabilities. Across the corpus, class imbalance was frequently underreported at model-development time; where reported, minority classes (e.g., rare fraud or emergency-access events) were not consistently mitigated via reweighting or synthetic oversampling, implying potential inflated precision but poor recall on critical cases. Explainability was often limited to global feature rankings; local error analysis (e.g., per-transaction SHAP) and auditable rationales for flagged events were uncommon, conflicting with healthcare's regulatory audit needs. Adversarial robustness was rarely stress-tested beyond standard noise; few studies evaluated evasion (feature perturbations), poisoning/backdoor risks, or model inversion paths. Finally, privacy/compliance tensions surfaced when training pipelines required centralized data or rich logs, with only a subset articulating data-minimization and consent pathways. These gaps align with our risk-of-bias observations (simulation-heavy validations; limited real-world replication).

3.17. Regulatory Compliance Analysis

Each included study was systematically evaluated for compliance with established healthcare data governance frameworks. We assessed adherence to the HIPAA Privacy and Security Rules, GDPR Articles 25 (data protection by design) and 32 (security of processing), and ISO/IEC 27799 health informatics security guidelines. Studies were categorized based on their explicit consideration of (1) patient consent mechanisms, (2) data minimization principles, (3) breach notification procedures, (4) cross-border data transfer protocols, and (5) audit trail requirements. Two reviewers independently assessed regulatory alignment using a structured checklist derived from legal requirements.

3.18. AI-Model Vulnerability Appraisal

For each AI-augmented security study (e.g., SVM, XGBoost, and BERT), we extracted four vulnerability dimensions: (V1) class imbalance handling (class ratios reported; use of re-weighting/SMOTE/focal loss), (V2) explainability (global or local XAI, such as SHAP/LIME; rule extraction; error analysis), (V3) adversarial robustness (evasion/poisoning/gradient-based tests; defenses), and (V4) privacy/compliance (HIPAA/GDPR alignment; data minimization; auditability). Two reviewers coded V1–V4 independently; disagreements were resolved by consensus/third adjudication. We summarize per-study

judgments in the Supplementary File and reflect gaps/mitigation in the synthesis. No automation tools were used.

4. Findings

The analysis of 80 studies examined author details, methodology, sample size, and study outcomes. Bitcoin-NG and Algorand are gaining attention in healthcare for their high throughput.

Scalability surveys categorize Bitcoin-NG and Algorand as medium-throughput consensus designs [14]; specifically, Algorand's Byzantine Agreement has been empirically analyzed and confirmed for scalability [15]. Nevertheless, EHR transaction management in the healthcare literature predominantly relies on permissioned or healthcare-specific frameworks (e.g., MedRec; multi-hop EHR permission delegation) rather than these public protocols [16].

Gao et al. [35] and Marino and Diaz Paz [36] noted that Ethereum-based smart contracts, despite strong security, suffer from high transaction costs and delays. They suggested that permissioned blockchains like Hyperledger Fabric offer greater computational efficiency. Table 1 compares blockchain frameworks using Hyperledger Caliper benchmarking, highlighting efficiency trade-offs in healthcare.

Table 1. From caliper peaks to clinical reality: performance constraints in healthcare blockchains.

Metric	Lab Conditions	Healthcare Reality	Perf. Impact
Throughput (TPS)	1000+	11–20	−97% to −99%
Latency	Sub-second	2–4 s	+200–400%
Data Complexity	Simple key–value	Complex HL7/DICOM	High
Consensus Participants	3–7 nodes	10–50 institutions	High
Compliance Overhead	None	Significant	High

The critical vulnerabilities of the AI-based fraud detection models presented in Table 2 are listed as follows.

Table 2. AI-based fraud detection models in blockchain healthcare systems.

AI Model	Description	Accuracy	Computational Cost	Scalability	Best Use Case
Random Forest (RF)	Ensemble learning method using decision trees	85–90%	Medium	High	Insurance fraud detection
Neural Network (NN)	Multi-layered deep learning model	92–96%	High	Medium	Transaction anomaly detection
BERT Transformer	NLP-based model for fraud detection via transaction logs	93–98%	Very High	High	Smart-contract security monitoring
Support Vector Machine (SVM)	Classification-based algorithm with kernel functions	80–88%	Medium	Medium	Behavioral fraud analysis

Random Forest (RF): data imbalance bias; limited interpretability for clinical decisions; overfitting with small healthcare datasets.

Neural Network (NN): black-box nature conflicts with medical explainability requirements; high computational overhead, vulnerable to adversarial attacks.

BERT Transformer: massive computational requirements incompatible with blockchain efficiency; privacy concerns with large training datasets; model bias in medical terminology.

Support Vector Machine (SVM): poor performance with non-linear healthcare data; kernel selection complexity; limited scalability in distributed blockchain environments.

The proposed taxonomy is grounded in socio-technical systems theory and healthcare informatics frameworks. Building upon Sittig and Singh's eight-dimensional model of health IT [37] and integrating blockchain-specific technical dimensions, our classification system encompasses four primary domains: (1) Technical Architecture (consensus mechanisms and scalability solutions), (2) Healthcare Context (clinical workflows and data types), (3) Governance Models (permissioned vs. permissionless regulatory compliance), and (4) Interoperability Standards (HL7 integration and API compatibility). The final taxonomy comprises five dimensions—(i) mining, (ii) consensus, (iii) security and encryption, (iv) distributed network, and (v) ledger—derived from systematic coding across the 80 studies.

Each dimension was theoretically justified through established healthcare informatics principles. The Technical Architecture domain draws from distributed systems theory and the Byzantine fault tolerance literature. Healthcare Context dimensions align with clinical workflow theory and health information exchange models. Governance Models reflect institutional theory and regulatory frameworks in healthcare. Interoperability dimensions are grounded in semantic interoperability theory and healthcare standard development. Empirical validation occurred through systematic application to all 80 studies, demonstrating comprehensive coverage (100% classification success rate) and mutual exclusivity of categories. Inter-rater reliability for taxonomy application was substantial,confirming consistent interpretability across independent coders.

Several included studies illustrate important limitations in terms of deployment and scalability. For instance, Jabarulla & Lee evaluated their framework only on an Ethereum testbed, with no sustained field pilot and unresolved scalability issues [38]. Iqbal et al. [39] reported results from a small-scale testbed with modest throughput, raising questions about external validity. Similarly, Mohsan et al. [40] presented a proof of concept limited to the Ethereum testnet, with performance that was sensitive to payload size. Finally, Ali et al. [41] achieved improved TPS under controlled Caliper benchmarks, yet generalization to hospital-scale operations remains unproven. Collectively, these cases show that—alongside reported successes—the evidence base also contains projects that remain at an early stage, encounter scalability constraints, or lack real-world validation. Detailed performance notes supporting these observations are compiled in the Supplementary File.

4.1. Comprehensive Literature Review and Analysis

The following sections summarize the relevant literature, discuss the methodologies employed, and suggest advancements in health policy management and blockchain-based smart contracts by revising the taxonomy and identifying key challenges.

4.2. Proceeding with Article Selection

We illustrate the article selection process and filtering criteria in Figure 1. Initially, 950 articles were identified, and, after filtering, 80 remained. These 80 papers were selected as the primary references for the study. Table 3 provides the detailed classification framework, and Table 4 provides a structured overview of each study, including publication year, reference, publisher, and category.

Table 3. Classification framework for blockchain-based smart contracts in healthcare.

Dimension	Categories	Coding Criteria
D1—Mining	PoW; PoS; Hybrid (PoS-BFT); None/Off-chain emphasis	Identify whether the study relies on on-chain mining incentives or consensus-independent execution; infer from platform defaults if not stated.
D2—Consensus Family	PoW/PoS Nakamoto-style; PBFT/RAFT/PoA (BFT-like); DAG/Other	Use the explicitly declared protocol; if absent, map via platform (e.g., Hyperledger Fabric→PBFT-like). Code unclear if insufficient evidence.
D3—Ledger/Network Model	Public; Private-permissioned; Consortium	Classify by governance/identity: open vs. permissioned vs. consortium-operated; check identity management and node control.
D4—Smart-Contract Primary Function	Access control; Consent management; Incentive/payment; Provenance/audit; Key management; Orchestration/business logic	Inspect stated purpose, ABI/events, and evaluation focus. If multiple, choose the primary function driving outcomes.
D5—Standards and Compliance Linkage	FHIR/HL7; ISO/IEC 27799; HIPAA/GDPR mapping; None	Code explicit standard/regulatory references (article/section). If no concrete mapping, mark 'None'.

Table 4. Overview of every original study, organized by year of publication and containing the study's unique identifier, reference, publisher, and category.

ID	Ref.	Author(s)	Year	Publisher	Type
A20	[42]	Hang et al.	2019	MDPI	Journal
A04	[43]	Jamil et al.	2020	MDPI	Journal
A19	[44]	Dhillon	2020	Frontiers Media	Journal
A21	[45]	Malamas et al.	2020	IEEE	Conference
A26	[46]	Gong and Zhao	2020	Springer Nature	Journal
A11	[47]	Ali et al.	2021	MDPI	Journal
A15	[38]	Jabarulla and Lee	2021	MDPI	Journal
A17	[39]	Iqbal et al.	2021	IEEE	Conference
A02	[40]	Mohsan et al.	2021	MDPI	Journal
A03	[41]	Ali et al.	2022	MDPI	Journal
A06	[48]	Chondrogiannis et al.	2022	Elsevier	Journal
A07	[49]	Su et al.	2022	Elsevier	Journal
A10	[50]	Sutanto et al.	2022	MDPI	Journal
A12	[5]	Zhang et al.	2022	IEEE	Journal
A13	[51]	Careline and Godhavari	2020	SAI	Journal
A16	[52]	Salonikias et al.	2022	MDPI	Journal
A25	[53]	De Olivera et al.	2022	IEEE	Conference
A27	[54]	Bhandawat et al.	2022	Elsevier	Journal
A08	[55]	Haritha and Anitha	2023	IEEE	Conference
A18	[56]	Thantharate and Thantharate	2023	MDPI	Journal

Table 4. *Cont.*

ID	Ref.	Author(s)	Year	Publisher	Type
A22	[57]	Abdelgalil and Mejri	2023	MDPI	Journal
A23	[58]	Chandini and Basarkod	2023	Springer Nature	Journal
A24	[59]	Karmakar et al.	2023	Elsevier	Journal
A43	[60]	Selvarajan et al.	2023	Springer Nature	Journal
A44	[61]	Liu et al.	2023	Elsevier	Journal
A45	[11]	Prajapat et al.	2024	IEEE	Journal
A46	[62]	Balasubramaniam et al.	2024	MDPI	Journal
A47	[63]	Venkatesh et al.	2024	IEEE	Conference
A01	[64]	Pu et al.	2024	Frontiers Media	Journal
A05	[65]	Kaur et al.	2024	Springer Nature	Journal
A09	[66]	Wang et al.	2024	Elsevier	Journal
A14	[67]	Li et al.	2024	Elsevier	Journal
A28	[68]	Bobrova et al.	2024	MDPI	Journal
A29	[69]	Igboanusi et al.	2024	Springer Nature	Journal
A30	[70]	Kaafarani et al.	2024	JMIR	Journal
A31	[71]	Liang et al.	2024	JMIR	Journal
A32	[72]	Mahdi et al.	2024	Springer Nature	Journal
A33	[73]	Takahashi et al.	2024	Springer Nature	Journal
A34	[74]	Wang et al.	2024	JMIR	Journal
A36	[75]	Yang and Li	2024	Springer Nature	Journal
A37	[76]	Duc et al.	2024	SAI	Journal
A38	[77]	Guerra et al.	2024	Taylor & Francis	Journal
A39	[78]	Li et al.	2024	Springer Nature	Journal
A40	[79]	Rekik et al.	2024	IEEE	Conference
A41	[80]	Saha et al.	2024	IEEE	Journal
A42	[81]	Vidhya et al.	2024	Wiley	Journal
A48	[82]	Arabnouri & Shafieinejad	2024	Springer Nature	Journal
A49	[83]	Bunia et al.	2024	IEEE	Conference
A50	[84]	Bieniek et al.	2024	Wiley	Journal
A51	[85]	Alharbi et al.	2024	MDPI	Journal
A52	[86]	Kumar & Ali	2024	Elsevier	Journal
A53	[87]	Rohini et al.	2024	PKP	Journal
A54	[88]	Li et al.	2024	Elsevier	Journal
A56	[89]	Zhu et al.	2024	MDPI	Journal
A58	[90]	Kar et al.	2024	IEEE	Journal
A59	[91]	Zhang et al.	2024	Elsevier	Journal
A62	[92]	Abid et al.	2024	OUP	Journal

Table 4. *Cont.*

ID	Ref.	Author(s)	Year	Publisher	Type
A64	[93]	Ahmed et al.	2024	Univ. of New Mexico	Journal
A65	[94]	Ahmed et al.	2024	MDPI	Journal
A67	[95]	Akhyani et al.	2024	IEEE	Conference
A69	[96]	Ansar et al.	2024	ETP	Journal
A70	[97]	Badidi et al.	2024	IEEE	Conference
A71	[98]	Basudan	2024	Taylor & Francis	Journal
A73	[99]	Chegenizadeh & Tessone	2024	IEEE	Conference
A74	[100]	Devgun et al.	2024	IEEE	Conference
A77	[101]	Kumari et al.	2024	Elsevier	Journal
A78	[102]	Sun et al.	2024	IEEE	Journal
A79	[103]	Rani et al.	2024	Springer Nature	Journal
A80	[104]	Riahi et al.	2024	IEEE	Journal
A55	[105]	Cihan et al.	2025	Wiley	Journal
A57	[106]	Aakanksha & Sundaram,	2025	HICSS	Conference
A60	[107]	Ding et al.	2025	IEEE	Journal
A61	[108]	Abdunabi et al.	2025	SAGE	Journal
A63	[109]	Ahanger et al.	2025	Elsevier	Journal
A66	[110]	Ahmed et al.	2025	Elsevier	Journal
A68	[111]	Ali et al.	2025	ACM	Journal
A35	[112]	Mishra and Mehra	2025	Springer Nature	Journal
A72	[113]	Chaudhry et al.	2025	Elsevier	Journal
A75	[114]	Guo et al.	2025	MDPI	Journal
A76	[115]	Gupta & Lakhwani	2025	Springer Nature	Journal

4.3. Conducting the Quality Evaluation

Each retrieved article was evaluated based on quality assessment criteria. The majority of the studies met at least four out of the six quality criteria, including clear study objectives, a comprehensive literature review, a structured methodology, bibliographic references, and supporting architectural concepts. The quality evaluation assessed the adequacy of structure and organization but did not exclude any articles from the final corpus.

5. Discussion

This section will analyze the guiding questions (GQs) that have been discussed in this context and will put forward potential solutions.

In accordance with PRISMA 2020 Item 23a, the findings of this review were interpreted in the context of the broader body of literature. The synthesized results were compared with existing systematic reviews and primary studies, enabling identification of convergences, divergences, and knowledge gaps. This contextualization enhances the external validity of the conclusions and strengthens their applicability in both academic and practical settings GQ1. What taxonomy best classifies blockchain-based smart contracts for health-policy use?

Research has highlighted blockchain's potential in overcoming healthcare challenges, with smart contracts providing automated and secure solutions tailored to system require-

ments [35]. The taxonomy of blockchain-based smart contracts in health policy involves classifying and structuring different types of smart contracts based on their functionality, execution process, and security mechanisms. As illustrated in Figure 2, the analysis of 80 relevant studies provides insights into blockchain components and their role in enhancing healthcare data management, patient autonomy, and regulatory compliance.

Figure 2. An assessment of the 80 reviewed papers related to blockchain components.

We explicitly present the classification framework in Figure 2 and Table 3, followed by its practical implications. The framework defines five dimensions (D1–D5), their categories, and decision rules for classifying blockchain-based smart contracts in healthcare.

The framework defines five dimensions (D1–D5) used to classify studies and reproduce coding decisions. Categories are mutually exclusive within a dimension; decision rules prioritize explicit statements in the article; otherwise, they are inferred from platform defaults. When evidence is insufficient, code the value as unclear and resolve via second-reviewer check.

Aligning 'consensus' and 'ledger' dimensions with healthcare tasks suggests that BFT-style protocols are more defensible for claim adjudication and auditability than PoW-style incentives given the health-policy accountability requirements. The null/mixed pilots indicate that performance claims obtained under controlled settings may not survive governance and auditing overheads in multi-institution deployments; thus, standard alignment should be treated as a first-order design constraint rather than a late-stage add-on. Future evaluations should report auditable on-chain logic, consent artifacts, and cross-border controls alongside throughput/latency. Otherwise, the reported numbers are not decision-useful for hospitals and payers. A minimum reproducibility card covering consensus parameters, node topology, and FHIR profiles would substantively improve comparability across studies.

To clarify our original contribution and make the proposed taxonomy operational, we formalize five dimensions—mining, consensus, security & encryption, distributed network, and ledger—grounded in the synthesis of 80 studies (see Figure 2) [35]. We then link consensus families to healthcare tasks: PoW is primarily used as an incentive model for provider participation [55,77]; IBFT (BFT) has been applied to health-insurance fraud detection [66,70,112]; and RAFT supports secure health-data storage and verification [80]. For concrete applicability beyond description, we point to case studies across functions: smart-contract EHR and access-control (FHIR-Chain/SmartAccess) [53], health-insurance workflows [50], and patient-monitoring on Hyperledger Fabric with real-time processing and security validation [10]; additional EHR sharing systems (e.g., Ethereum + IPFS) demonstrate feasibility in clinical record management [1]. Cryptographic mechanisms (ABE/CP-ABE, HE, and ZKP) are integrated to enforce fine-grained access, privacy-preserving computation, and verifiable identity—transforming prior building blocks into a policy-aware contract taxonomy for healthcare [41,69,72]. Finally, performance comparisons between Hyperledger Fabric and Ethereum are retained as evidence for throughput/latency trade-offs, but we synthesize them concisely to reduce overlap and emphasize decision criteria rather than reproduction of prior text [9].

For clarity, we briefly note that consensus protocols differ not only in technical operation but also in their policy relevance. For example, RAFT provides fast low-latency consensus suitable for secure intra-hospital data sharing, whereas IBFT ensures fault-tolerant agreement in networks where multiple insurers or providers must validate claims. Such consensus choices matter for clinical workflows, where reliability and auditability are critical. Similarly, permissioned blockchains (restricted membership) are often preferred in healthcare because they enable HIPAA/GDPR compliance through controlled access, while public blockchains (open participation) pose governance and privacy challenges.

5.1. Mining

Mining adds blocks to the blockchain, with miners verifying transactions based on consensus mechanisms [64,73,75]. Proof of Work (PoW) has been explored as an incentive model for healthcare providers, rewarding them with coins such as Ether [55,77]. To streamline data sharing, transactions are grouped into processing pools before mining [48]. A lightweight cryptographic technique enhances security and patient-controlled data access, reducing mining dependency in blockchain-based IoT networks. FHIR-Chain uses smart contracts for secure health data modifications, storing clinical data off-chain with encrypted references [53]. To lower costs, consortium blockchains are preferred over public blockchains [78]. Leader election algorithms improve efficiency in decentralized hospital networks [80]. For scalability, smart contracts and decentralized storage minimize computational overhead. Gas fees and energy-efficient permissioned blockchains offer alternatives to mining-heavy processes, ensuring security and efficiency [77,78].

It should be noted that, while blockchain systems promise transparency, security, and resilience, these remain largely theoretical advantages unless accompanied by solutions to unresolved challenges such as scalability, energy intensity, and interoperability. For instance, Ethereum-based healthcare prototypes demonstrate technical feasibility but remain economically impractical due to high transaction (gas) costs.

5.2. Consensus Mechanisms

Blockchain consensus mechanisms validate data before updates, with data controllers setting policies and processors ensuring compliance [38–40,43,44,49,55,56,58,59,64,76,79,81]. The choice of blockchain depends on the network type: public blockchains allow open

participation, while private ones require approval [74]. Consensus mechanisms replace central authority reliance, ensuring secure and verified transactions across nodes [48]. Chen et al. [116] analyzed lightweight blockchain models for scalable health data storage, comparing PoW and BFT. Their findings show that permissioned blockchains reduce computational overhead while maintaining decentralization. PoW uses cryptographic puzzles, while alternative protocols optimize efficiency and scalability [54]. Byzantine fault tolerance (BFT) enhances data integrity and security, with Istanbul BFT (IBFT) aids health insurance fraud detection [66,70,112]. The Reliable, Replicated, Redundant, and Fault-Tolerant (RAFT) consensus algorithm ensures secure health data storage and verification [80].

5.3. Security and Encryption

Encryption ensures confidentiality, integrity, and access control in healthcare blockchain systems, maintaining data integrity, traceability, and secure sharing [38–40,43,49,58,59,75–77,79–81]. Cryptographic authentication models for EMRs were proposed, enhancing identity verification and mitigating security threats [57,65–68,112,117]. Public-key cryptography and attribute-based encryption (ABE) enable user-controlled access, while Igboanusi et al. [69] introduced a framework integrating ABE, homomorphic encryption (HE) for privacy-preserving computations, and zero-knowledge proof (ZKP) for secure identity verification. Consent management ensures privacy and compliance, while encrypted keyword indexing prevents unauthorized access [72]. CP-ABE restricts EHR access and maintains audit trails, while homomorphic encryption enables secure searches and data exchange [41]. Blockchain's immutability ensures long-term data accuracy, with consensus mechanisms validating and securely storing information [70].

5.4. Distributed Network

Distributed networks store health data across multiple nodes, eliminating central authority dependence while enhancing security and resilience [68,71,72]. This decentralized structure enables secure data sharing, reducing risks of data loss and failure points. Blockchain transactions use PoW and PoS consensus mechanisms, balancing speed, efficiency, and scalability [45]. Smart contracts automate data management, while PoS resolves billing disputes. Decentralized networks improve organ donation transparency, fraud detection, and healthcare verification [69,70]. P2P architectures support hospital data decentralization, while IPFS-based solutions enhance security [39,40,43,49,56,58,59,79–81].

5.5. Ledger

Blockchain is a decentralized immutable ledger ensuring data integrity, security, and transparency [38,46,56,70]. Consensus mechanisms validate transactions without a central authority. It is crucial for audits and secure data access, allowing patients, suppliers, and insurers to retrieve authorized information [42,72,78]. Public blockchains allow open access, while private blockchains restrict entry [54,118]. Blockchain also enhances data sharing and computational efficiency [35].

Future research should validate the proposed taxonomy by implementing a prototype in EHR systems. Gao et al. [35] demonstrated a blockchain-based multi-hop permission delegation model, providing a foundation for healthcare-specific smart-contract testing.

GQ2. Which healthcare protocols and standards (e.g., FHIR; HIPAA/GDPR mapping) should inform smart-contract design?

The healthcare protocols and standards related to smart contracts are presented in Figure 3. The research on blockchain and multi-certificate authority explores secure smart-contract execution for health data access. Ali et al. [47] proposed adaptable policies for record modifications and policy initiation, ensuring patient autonomy. Their multi-certificate authorization (CA) model enhances EHR security by addressing single-certifying

authority vulnerabilities, allowing user re-enrollment if records are lost. Big data analytics optimize health data management through data mining and knowledge discovery [65].

5.6. Solidarity

Blockchain-based healthcare systems promote social solidarity by enabling user-controlled health data and privacy protection, fostering trust between patients and insurers [68,70]. Enterprise blockchain ensures secure data exchange, as seen in Hyperledger Fabric, which supports inventory management without cryptocurrency reliance [54]. Smart contracts enable transparent transactions, strengthening collaboration and trust among stakeholders [44,56,66,71,72,77,79].

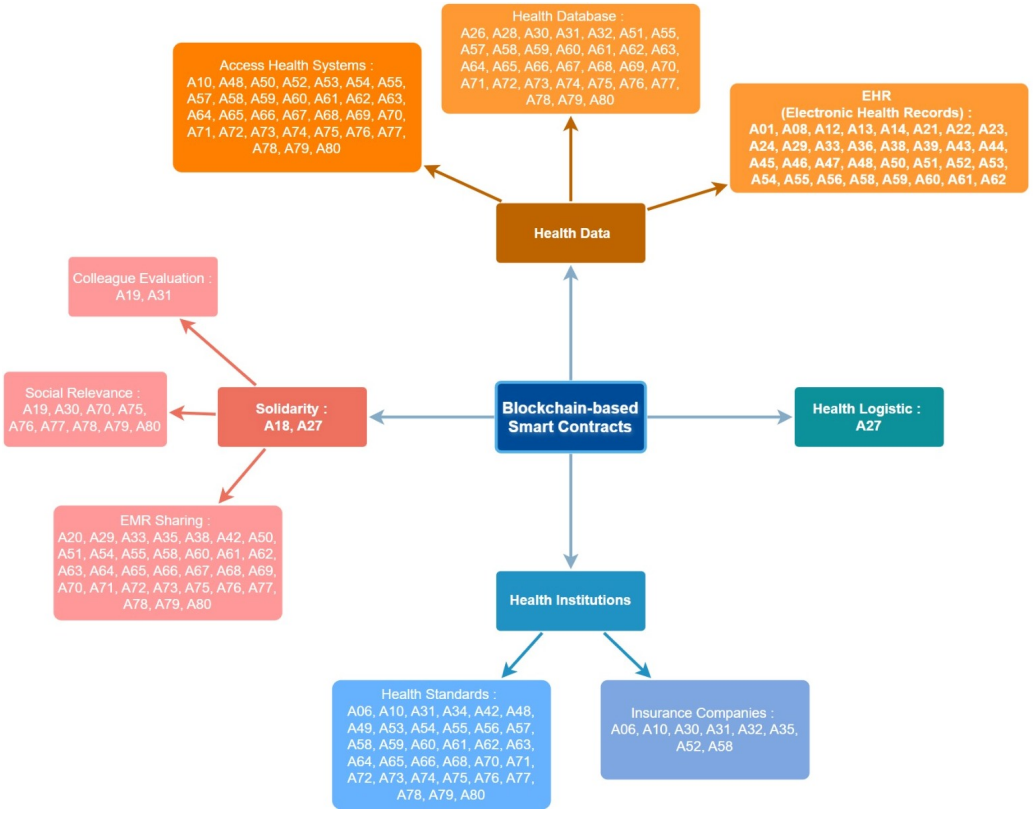

Figure 3. An assessment of the 80 reviewed papers related to blockchain-based smart contracts.

5.7. Health Institutions

Blockchain enables secure decentralized medical data sharing among hospitals, insurers, and researchers without a centralized EHR system. It improves data integrity, patient follow-up, and transaction tracking despite regulatory challenges [42,119]. MedRec ensures secure data management with a transparent audit trail, while homomorphic encryption enhances privacy [41,58,120]. Blockchain streamlines insurance claims, reduces fraud, and enhances efficiency [70,71]. Hyperledger solutions improve security, and real-time access supports emergency response [72,73]. DiabeticChain aids chronic disease management [112]. Smart contracts ensure data verification, access control, and accountability, while an inter-nodal mechanism secures healthcare collaboration [48,52,75].

5.8. Participants

Blockchain's networking capabilities make participants capable of connecting with each other in a verifiable and safe way, even without a trustworthy medium [18,52,70]. Access control mechanisms regulate data retrieval for health institutions, laboratories, providers, and insurers [72,112]. RBAC and ABAC models ensure secure data shar-

ing, privacy, and compliance among healthcare systems, pharmaceutical firms, and researchers [78,80].

5.9. Doctors

Doctors can securely access and manage patient records through encrypted communication and smart contracts [72,80]. Medical records are encrypted, stored in IPFS, and verified via blockchain hashes [44]. Physicians assist in organ donation verification and insurance claim validation, while emergency doctors use biometric authentication for rapid patient interventions [69,70,73].

5.10. Insurance Companies

Traditional insurance systems increase costs and data manipulation risks. Blockchain ensures secure automated transactions with cryptographic protection [59]. It enables transparent access management, allowing secure transaction processing while protecting policyholder data [68,71]. Hyperledger Fabric enhances security and scalability [72]. Blockchain expedites insurance approvals and medical interventions, while decentralized management streamlines claims, prevents fraud, and strengthens trust through immutable records [50,73]. Kaushal et al. [10] developed a Hyperledger Fabric-based smart-contract prototype for remote patient monitoring, validating its real-time processing, security, and efficiency. Future implementations can integrate this model with FHIR-compliant blockchain frameworks for healthcare interoperability.

5.11. Quantum Domain

Emerging quantum computing technologies pose a significant threat to existing cryptographic systems, including those used in both centralized and decentralized infrastructures such as blockchains [121–123]. In response, researchers have begun exploring quantum-resilient blockchain architectures and cryptographic protocols. We expanded our systematic review, including the "Quantum" keyword in the search string, and selected the following studies.

Banerjee et al. [124] proposed a blockchain framework based on quantum resources that maintains decentralization while defending against quantum adversaries, demonstrating a proof-of-concept implementation on IBM's 5-qubit quantum computer with very high fidelity. Kiktenko et al. [125] presented a quantum-secure blockchain platform utilizing quantum key distribution over an urban fiber network to achieve information-theoretic authentication.

In the healthcare domain, quantum-enhanced blockchain solutions have been proposed to ensure the privacy and integrity of sensitive medical data. Selvarajan et al. [60] introduced the Quantum Consultative Transaction Key Generation and Management scheme and a Quantum Trust Reconciliation Agreement Model for secure data exchange in healthcare, enhanced with Tuna Swarm Optimization for nonce verification and trust-based communication.

Prajapat et al. [11] presented a blockchain-integrated quantum authentication scheme for sensor-assisted Internet of Medical Things networks, enabling secure multi-party communication and preventing clinician-side misuse without third-party dependencies. Liu et al. [61] proposed a quantum-enhanced blockchain system employing quantum hash functions, quantum digital signatures, and a proof-of-authority consensus mechanism, offering robust protection against both classical and quantum threats while maintaining scalability and efficiency.

Balasubramaniam et al. [62] introduced a quantum-inspired blockchain (Qchain) alongside an entangled quantum medical record protocol, utilizing entangled states and quantum authentication to ensure privacy and auditability in medical IoT systems. Finally, Venkatesh

et al. [63] proposed a quantum blockchain framework for electronic medical records, integrating quantum key distribution and post-quantum cryptographic techniques, achieving notable reductions in computational and communication overhead while strengthening security against quantum attacks.

Linking Quantum Proposals to Healthcare Regulatory Imperatives

While the above-reviewed studies highlight diverse technical approaches (e.g., quantum key distribution, quantum hash functions, entangled medical records, and post-quantum digital signatures), we emphasize that their significance for healthcare lies not in their technical novelty alone but in their capacity to address established regulatory imperatives. Specifically, healthcare governance frameworks such as the HIPAA and GDPR mandate secure processing, data protection by design, and auditable accountability. In this context,

- Quantum key distribution (QKD) frameworks directly strengthen cross-border data transfer security and tamper-proof communication, addressing the security of processing.
- Quantum digital signatures and quantum-resistant hash functions provide forward-secure audit trails, aligning with the HIPAA requirements for verifiable access and breach notification.
- Quantum consultative trust models and reconciliation mechanisms operationalize patient consent and autonomy, which are critical pillars of healthcare policy and bioethics.
- Entangled medical record protocols and quantum authentication schemes enhance privacy protection in Internet of Medical Things (IoMT) networks, ensuring compliance with both HIPAA and GDPR consent and minimization principles.

Thus, the reviewed works in the quantum domain are not intended as a catalog but as a policy-relevant synthesis: each proposal contributes to healthcare governance by preparing digital infrastructures for the quantum era. By explicitly mapping these quantum-enhanced blockchain approaches to regulatory imperatives, we clarify that their relevance lies in ensuring that healthcare data governance remains resilient, auditable, and patient-centered even under quantum-adversarial conditions.

5.12. Cross-Domain and Emerging Applications

In addition to the domain-specific applications discussed above, several recent studies have introduced blockchain frameworks addressing cross-cutting challenges and emerging use cases in healthcare, education, data sharing, and cooperative machine learning. These works exemplify the broadening landscape of blockchain's applicability beyond traditional verticals.

The BACASE-SH framework introduces a blockchain-based certificate-less authenticated asymmetric searchable encryption scheme to address key privacy and trust issues in smart healthcare systems, particularly tackling challenges like keyword guessing attacks, data integrity, and identity verification between patients and physicians [82].

The SCeFSTA system proposes a smart contract-enabled blockchain framework to implement a fair, secure, and transparent auction mechanism for healthcare transportation, ensuring secure payments, reduced record redundancy, and efficient resource use while promoting competition among service providers [83].

SecureCare introduces a blockchain-assisted wearable body area network (WBAN) architecture for IoT healthcare systems, offering enhanced data privacy, tamper-proof security, and improved scalability for real-time patient monitoring through a decentralized and efficient framework [84].

Alharbi et al. [85] proposed a blockchain- and smart contract-based framework for ensuring data integrity and privacy in remote healthcare monitoring (RHM) using IoT devices, automating secure data transactions while enhancing transparency, reliability, and protection against fraud and tampering.

A smart contract-based authentication scheme was developed for securing 6G-enabled Internet of Nano-Medical Things (IoNMT) networks, offering a decentralized low-latency solution that enhances privacy, energy efficiency, and resistance to various security threats, as validated through both formal models and simulation analyses [86].

To enhance data security and overcome blockchain scalability limitations in remote patient monitoring, the SHORTBLOCKS protocol extends blockchain into a directed acyclic graph structure, combining private and public chains via smart contracts to enable efficient, secure, and scalable healthcare data management [87].

The DAMFSD model introduces a decentralized authorization framework that enables patients to securely and flexibly delegate access rights to trusted entities across healthcare institutions, thereby mitigating the risks associated with centralized authorization systems. Leveraging cryptographic techniques for fine-grained access control and smart contracts for decentralized delegation management, the model enhances interoperability while preserving patient autonomy and auditability [88].

A private permissioned blockchain framework based on Hyperledger Fabric was developed to manage clinical research processes in alignment with FAIR principles, enabling secure decentralized handling of epidemiological data—such as COVID-19 statistics—while ensuring data is findable, accessible, interoperable, and reusable through smart-contract automation and performance-evaluated chaincode execution [105].

A privacy-preserving Byzantine-resilient swarm learning (PBSL) framework integrates deep learning with blockchain-based smart contracts to support secure decentralized medical diagnostics across institutions, using threshold fully homomorphic encryption for data privacy and cosine similarity to detect poisoning attacks in gradient updates, thus addressing major vulnerabilities in traditional swarm learning approaches [89].

A decentralized autonomous organization (DAO)-driven framework was proposed to optimize hospital location planning by enabling stakeholder participation, smart-contract governance, and data-driven decision-making, with a case study in New Zealand illustrating improved healthcare infrastructure planning, equity, and operational efficiency through collaborative blockchain-based models [106].

LA-IMDCN introduces a lightweight remote user authentication scheme for implantable medical device (IMD) communication networks, utilizing a consortium blockchain and smart contracts to secure wireless data transmissions against tampering and eavesdropping while addressing the privacy and reliability challenges unique to IMD environments [90].

A consortium blockchain-based tunnel data bank was designed to eliminate data silos in structural health monitoring (SHM) by enabling traceable tamper-resistant sharing of heterogeneous monitoring data among multiple organizations, with smart contracts managing storage, alert mechanisms, and incremental updates, as demonstrated through real-world tunnel data in Hangzhou [91].

The BADS-ABE scheme enables secure and anonymous medical data sharing in 6G-enabled smart healthcare by integrating blockchain with attribute-based encryption, Groth signatures for identity privacy, distributed key generation via smart contracts and Newton interpolation, and policy hiding to protect attribute privacy while reducing decryption overhead [107].

An advanced authorization framework for body area networks (BANs) integrates a spatiotemporal attribute-based access control (STABAC) model with blockchain-based

smart contracts to enforce fine-grained context-aware access policies while ensuring integrity through formal verification using timed colored Petri nets, thereby enabling secure uninterrupted healthcare service delivery [108].

A smart contract-based access control framework is proposed for IoT-enabled smart healthcare systems, combining decentralized blockchain architecture with the GTRBAC model to support fine-grained temporal policy enforcement without relying on third-party entities, achieving high security, low gas costs, and linear scalability in access control performance [92].

A decade-long analysis of intrusion detection systems (IDSs) for IoT environments highlights the growing integration of AI strategies—such as machine learning, deep learning, and federated learning—to counter security threats like Sybil attacks and DDoS, with emphasis on blockchain-enhanced security, evolving IDS architectures, and deployment models tailored to the resource constraints and heterogeneity of IoT systems [109].

A hybrid multi-criteria decision-making approach combining Type-2 Neutrosophic Numbers (T2NN), CRITIC, and MAIRCA was proposed to evaluate and rank blockchain platforms integrated with Large Language Models (LLMs), identifying Stellar, Klaytn, Openchain, and Hyperledger Fabric as the top-performing platforms across the technological, organizational, and environmental dimensions, thereby supporting more secure, automated, and user-friendly smart-contract and data infrastructures [93].

A decentralized philanthropic framework leverages blockchain, eKYC authentication, and smart contract-based privacy filters to improve transparency, data integrity, and donor trust in charitable giving, aiming for full donation traceability, minimal operational costs, and alignment with the UN Sustainable Development Goals through innovations like coin-toss-based data selection and service-based charity models [94].

A novel framework leverages IOTA distributed ledger technology and its DAG-based Tangle structure to ensure secure, scalable, and miner-less data integrity in next-generation fog-driven e-health and emotion care systems, demonstrating enhanced protection against tampering and unauthorized access while addressing the limitations inherent in DLT consensus and participation [110].

The GRACE scheme integrates blockchain and coalition game theory to optimize resource allocation among SDN controllers in IoT networks, enhancing collaboration, decision-making, and network performance through smart contracts that securely manage device registration and interactions, with demonstrated improvements in time convergence, switch operations, and gas cost efficiency [95].

A comprehensive survey of privacy-preserved and responsible recommender systems (RSs) synthesizes advancements in conventional defenses, differential privacy, federated learning, and blockchain, presenting an interdisciplinary taxonomy and open-source resources that contextualize technical challenges, industrial expectations, and emerging solutions for secure, fair, and transparent recommendation services [111].

A novel encryption scheme, EKT-EDES, combines tri-iterative elliptic-integrated data encryption with a blockchain-backed access control mechanism to secure cloud-stored healthcare records, utilizing IPFS for decentralized storage and smart contract-driven enhanced role-based access control (RBAC) for fine-grained permissions, achieving notable efficiency in encryption, decryption, latency, and throughput metrics [96].

An integrated system architecture combining edge analytics, blockchain, and federated learning is proposed to enhance cybersecurity in healthcare, enabling real-time threat detection and secure data management for electronic health records (EHRs) while offering a set of implementation tools to support robust, decentralized, and privacy-preserving security solutions [97].

A blockchain-empowered delegation framework for Internet of Medical Robotics Things (IoMRT) telesurgery systems integrates multi-hop permission delegation, proxy re-encryption, and attribute-based encryption to ensure fine-grained, traceable, and secure EMR sharing; with data stored on IPFS and delegation depth controlled via smart contracts, the system is validated on the Ethereum test chain and outperforms existing protocols [98].

The zk-DASTARK scheme combines zero-knowledge proof with quantum-resistant digital signatures (CRYSTALS-Dilithium) to ensure both authenticity and privacy of off-chain data fed to smart contracts, enabling secure efficient DApp execution—particularly in sensitive applications like healthcare insurance—through the zk-STARKFeed mechanism deployed on the IOTA blockchain, with proof generation and verification performed in under 60 ms and 10 ms, respectively [113].

PAVA introduces a privacy-preserving attribute-based authentication scheme for healthcare data sharing that leverages smart contracts to enforce dual access policies—one for data providers and one for data users—while maintaining confidentiality of policy attributes through linear secret sharing and blind access mechanisms, enabling verifiable authentication and secure decentralized interactions without revealing sensitive access conditions [99].

FASALKA proposes a privacy classification framework for blockchain smart contracts that combines federated and reinforcement learning to dynamically manage privacy parameters, enabling smart contracts to address over- or under-utilization of privacy levels; deployed on Ethereum via Azure, the system achieves 100% privacy classification accuracy while maintaining comparable throughput to standard Ethereum [100].

CrowdBA introduces a cost-effective quality-driven crowdsourcing architecture for bounding-box annotation by integrating Ethereum blockchain with IPFS to offload storage and computation and employing a Dynamic IoU-weighted bounding-box fusion (DWBF) algorithm within smart contracts to assess annotation quality and fairly distribute incentives, significantly improving accuracy and operational efficiency [114].

A novel smart-contract framework deployed on the CoreDAO blockchain enhances Quality-of-Service (QoS) for the 9NFTMania token by extending ERC20 standards with governance features, dividend distribution, and dynamic fee mechanisms; comparative analysis shows superior accuracy, efficiency, and scalability—particularly for healthcare applications—while leveraging Proof-of-Stake to outperform conventional PoW-based systems [115].

HealthRec-Chain presents a patient-centric framework that combines Ethereum blockchain with IPFS and Java-enabled GPG encryption to securely store and share sensitive medical records and images, addressing challenges of data ownership, interoperability, and scalability; performance evaluations via a personalized dashboard and manual benchmarking confirm its feasibility in enhancing healthcare data security, privacy, and system efficiency [101].

A provenance-aware blockchain-based EHR system is proposed to support efficient traceable sharing of correlated medical records through a DAG-like data structure, dynamic authorization propagation, and an honesty-driven audit mechanism based on Nash equilibrium principles, enabling patients and doctors to manage and access complete lineage-informed medical histories via Ethereum smart contracts [102].

EduCert-Chain presents a secure notarized educational certificate authentication framework built on Hyperledger Fabric, leveraging ECDSA signatures, SHA-256 hashing, and Raft consensus to ensure integrity and traceability; experimental evaluations with two higher education institutions demonstrate reliable performance in terms of throughput and latency, addressing certificate forgery through decentralized verifiable credential issuance [103].

The RL-ICDL-BC framework integrates reinforcement learning-based incentive mechanisms with blockchain and cooperative data learning to encourage privacy-preserving collaboration among distributed healthcare data owners, demonstrating improved participation, fairness, and model performance—achieving approximately 99% COVID-19 detection accuracy even under non-iid data conditions [104].

These emerging frameworks demonstrate blockchain's growing versatility and its critical role in addressing systemic issues across sectors. Their contributions provide a strong foundation for future interdisciplinary research and development.

From a regulatory perspective, one of the most debated tensions is between the immutability of blockchain and patients' rights under the GDPR (e.g., the right to be forgotten). A practical compliance strategy is to store sensitive health data off-chain, with only encrypted references or hashes recorded on-chain. In such a design, deletion requests can be honored by erasing the off-chain record, while the on-chain pointer remains non-identifiable. Similarly, the HIPAA's "minimum necessary use" principle can be operationalized by restricting node participation in permissioned blockchains and using tokenized consent contracts, which allow patients to revoke or modify access rights without altering the blockchain ledger itself. These approaches illustrate how blockchain can be aligned with regulatory imperatives, but they also highlight that compliance must be an explicit design objective rather than an assumed property.

Although this study is primarily a systematic review rather than an engineering implementation, we note that the evidence base increasingly reports prototype-level validations and exposed evaluation data that can guide future applied work. For example, several included systems (e.g., FHIR-Chain, SmartAccess, Hyperledger-Fabric EHR sharing, and DiabeticChain) have released performance metrics such as transaction latency, throughput, and energy costs together with open or semi-open evaluation datasets (see Supplementary File). These prototypes provide early empirical grounding for our taxonomy and highlight practical design patterns (off-chain data references, tokenized consent, and regulatory audit logging) that future developers can adapt and extend. By summarizing these prototyping efforts and the data they expose, we aim to bridge the gap between conceptual classification and actionable design guidance for health informatics engineers and policy-oriented decision-makers.

6. Conclusions

Synthesizing our review, the frequently reported benefits of blockchain-based smart contracts in healthcare—privacy, efficiency, and fraud reduction—are conditional on governance and compliance design; improvements demonstrated under controlled settings often face friction in HIPAA/GDPR-aligned operations [75]. The evidence to date also suggests that permissioned auditable architectures with role-based access control are more defensible for clinical audit trails and claim adjudication than open incentive-driven models [35,73,79].

Cryptographic and data-layer enablers such as ABE, IPFS, and FHIR/ISO/IEC 27799 integration can support secure exchange and provenance, yet declarative compliance claims are insufficient without verifiable mechanisms [126,127].

Policy recommendations for action. Regulators should require reproducibility cards accompanying deployments (consensus parameters, node topology, and failure modes) so that performance and security claims are auditable across contexts, as well as mandate on-chain queryable events for consent capture/revocation and breach notification to operationalize GDPR articles. Providers and payers should prefer BFT-class permissioned consensus for auditability, formalize RBAC/ABAC mappings to clinical roles and FHIR scopes, and include contractual SLAs for key management, incident response, and independent compliance audits. Vendors should publish binding profiles that link FHIR OAuth

scopes to standard smart-contract events (access, provenance, and consent) and define testable conformance criteria for cross-border transfer and data minimization.

Future work. We recommend policy-embedded evaluations that report compliance artifacts and audit costs alongside throughput/latency, enabling decision-useful evidence for adoption. Technology choices (e.g., Hyperledger frameworks, smart contracts, DApps, and cloud backends) should be benchmarked under standardized regulator-witnessable test plans rather than ad hoc lab conditions. Given the growing synergy between AI and blockchain in healthcare governance [12,13], evaluations should include transparency of model–chain interactions and verifiable access trails. Finally, to future-proof deployments, policy roadmaps should incorporate post-quantum cryptography timelines and require periodic re-certification of deployed contracts, aligning cryptographic agility with evolving regulatory frameworks [82].

Supplementary Materials: The following supporting information can be downloaded at: https://www.mdpi.com/article/10.3390/info16100853/s1, Supplementary Material S1. Full Search Strategies; Supplementary Material S2: Review of Studies Included in the Systematic Review; Supplementary Material S3. Risk of Bias Table; Supplementary Material S4. Results of Individual Studies; Supplementary Material S5. Category-level Counts for Full-Text Exclusions (PRISMA Item 16b); Supplementary Material S6. Representative Borderline Exclusions (Study-level Examples).

Author Contributions: Conceptualization, K.K.K., M.T., S.P., F.O. and S.T.; methodology, K.K.K. and S.T.; investigation, K.K.K., M.T., S.P., F.O. and S.T.; resources, K.K.K., M.T., S.P., F.O. and S.T.; data curation, K.K.K., M.T., S.P., F.O. and S.T.; writing—original draft preparation, K.K.K., M.T., S.P., F.O. and S.T.; visualization, K.K.K., M.T., S.P. and S.T.; supervision, S.T.; project administration, S.T.; funding acquisition, F.O. All authors have read and agreed to the published version of the manuscript.

Funding: This research was partially funded by Tokyo International University Personal Research Fund.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data and codes will be shared upon reasonable request.

Conflicts of Interest: Author Serkan Türkeli is employed by TESODEV Technology Solutions Development Company Ltd. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest

Abbreviations

The following abbreviations are used in this manuscript:

ABE	Attribute-Based Encryption
EHR	Electronic Health Record
EMR	Electronic Medical Record
BERT	Bidirectional Encoder Representations from Transformers
BFT	Byzantine Fault Tolerance
CA	Certificate Authorization
CPT-ABE	Ciphertext-Policy Attribute-Based Encryption
FHIR	Fast Healthcare Interoperability Resources
GQ	Research Guidance Question
HE	Homomorphic Encryption
HIPAA	Health Insurance Portability and Accountability Act
GQ	Research Guidance Question
HE	Homomorphic Encryption
HIPAA	Health Insurance Portability and Accountability Act

IoT	Internet of Things
NIH	National Institute of Health
NN	Neural Network
PHR	Personal Health Record
PoW	Proof of Work
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
RAFT	Reliable, Replicated, Redundant, and Fault-Tolerant
RF	Random Forest
SAI	The Science and Information Organization
SVM	Support Vector Machine
WoS	Web of Science
ZKP	Zero-Knowledge Proof

References

1. Sun, J.; Ren, L.; Wang, S.; Yao, X. A blockchain-based framework for electronic medical records sharing with fine-grained access control. *PLoS ONE* **2020**, *15*, e0239946. [CrossRef]
2. McGhin, T.; Choo, K.K.R.; Liu, C.Z.; He, D. Blockchain in healthcare applications: Research challenges and opportunities. *J. Netw. Comput. Appl.* **2019**, *135*, 62–75. [CrossRef]
3. Ante, L. Smart contracts on the blockchain—A bibliometric analysis and review. *Telemat. Inform.* **2021**, *57*, 101519. [CrossRef]
4. Christidis, K.; Devetsikiotis, M. Blockchains and smart contracts for the internet of things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
5. Zhang, L.; Zhang, T.; Wu, Q.; Mu, Y.; Rezaeibagha, F. Secure decentralized attribute-based sharing of personal health records with blockchain. *IEEE Internet Things J.* **2021**, *9*, 12482–12496. [CrossRef]
6. Elhence, A.; Goyal, A.; Chamola, V.; Sikdar, B. A blockchain and ML-based framework for fast and cost-effective health insurance industry operations. *IEEE Trans. Comput. Soc. Syst.* **2022**, *10*, 1642–1653. [CrossRef]
7. Wang, W.; Hoang, D.T.; Hu, P.; Xiong, Z.; Niyato, D.; Wang, P.; Wen, Y.; Kim, D.I. A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Access* **2019**, *7*, 22328–22370. [CrossRef]
8. Alammary, A.S. Building a sustainable digital infrastructure for higher education: A blockchain-based solution for cross-institutional enrollment. *Sustainability* **2024**, *17*, 194. [CrossRef]
9. Kumar, C.S.; Padhy, A.B.; Singh, A.P.; Reddy, K.H.K. A Dynamic Trading Approach Based on Walrasian Equilibrium in a Blockchain-Based NFT Framework for Sustainable Waste Management. *Mathematics* **2025**, *13*, 521. [CrossRef]
10. Kaushal, R.K.; Kumar, N.; Kukreja, V.; Boonchieng, E. Hyperledger fabric based remote patient monitoring solution and performance evaluation. *Peer-to-Peer Netw. Appl.* **2025**, *18*, 105. [CrossRef]
11. Prajapat, S.; Kumar, P.; Kumar, D.; Das, A.K.; Hossain, M.S.; Rodrigues, J.J. Quantum secure authentication scheme for internet of medical things using blockchain. *IEEE Internet Things J.* **2024**, *11*, 38496–38507. [CrossRef]
12. Khan, S.; Khan, M.; Khan, M.A.; Khan, M.A.; Wang, L.; Wu, K. A blockchain-enabled AI-driven secure searchable encryption framework for medical IoT systems. *IEEE J. Biomed. Health Inform.* **2025**, *early access*. [CrossRef]
13. Kapadiya, K.; Patel, U.; Gupta, R.; Alshehri, M.D.; Tanwar, S.; Sharma, G.; Bokoro, P.N. Blockchain and AI-empowered healthcare insurance fraud detection: An analysis, architecture, and future prospects. *IEEE Access* **2022**, *10*, 79606–79627. [CrossRef]
14. Jain, A.K.; Gupta, N.; Gupta, B.B. A survey on scalable consensus algorithms for blockchain technology. *Cyber Secur. Appl.* **2025**, *3*, 100065. [CrossRef]
15. Yadav, J.; Shevkar, R. Performance-based analysis of blockchain scalability metric. *Teh. Glas.* **2021**, *15*, 133–142. [CrossRef]
16. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. Medrec: Using blockchain for medical data access and permission management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25–30. [CrossRef]
17. Ucbas, Y.; Eleyan, A.; Hammoudeh, M.; Alohaly, M. Performance and scalability analysis of ethereum and hyperledger fabric. *IEEE Access* **2023**, *11*, 67156–67167. [CrossRef]
18. Mnasri, S.; Salah, D.; Idoudi, H. A hybrid blockchain and federated learning attention-based BERT transformer framework for medical records management. *J. Supercomput.* **2025**, *81*, 317. [CrossRef]
19. Yang, S.; Zhang, G.; Feng, B.; Li, Y. A Cross-Chain Medical Data Sharing Scheme Integrating Ring Signature. In Proceedings of the 2024 4th International Conference on Computer Science and Blockchain (CCSB), Shenzhen, China, 6–8 September 2024; pp. 338–342. [CrossRef]

20. Qiao, Y.; Xue, Y.; Zhai, Y.; Zhang, D.; Vasilakos, A.V.; Hossain, M.S.; Mumtaz, S. A Controllable and Efficient Sharing Scheme for Medical IoT Data Based on Consortium Blockchain. In Proceedings of the 2024 IEEE International Conference on E-health Networking, Application & Services (HealthCom), Nara, Japan, 18–20 November 2024; pp. 1–6. [CrossRef]
21. Bezanjani, B.R.; Ghafouri, S.H.; Gholamrezaei, R. Privacy-preserving healthcare data in IoT: A synergistic approach with deep learning and blockchain. *J. Supercomput.* **2025**, *81*, 533. [CrossRef]
22. Liu, Y.; Sharma, A.; Rani, S.; Yang, J. Supply Chain Security, Resilience and Agility in IoT-driven Healthcare. *IEEE Internet Things J.* **2025**, *early access*. [CrossRef]
23. Prainsack, B.; Buyx, A. *Solidarity in Biomedicine and Beyond*; Cambridge University Press: Cambridge, UK, 2017; Volume 33.
24. Beauchamp, T.; Childress, J. Principles of biomedical ethics: Marking its fortieth anniversary. *Am. J. Bioeth.* **2019**, *19*, 9–12. [CrossRef]
25. Hess, C. Mapping the new commons. *SSRN Electron. J.* **2008**, *early access*. [CrossRef]
26. Ostrom, E. *Governing the Commons: The Evolution of Institutions for Collective Action*; Cambridge University Press: Cambridge, UK, 1990.
27. Daniels, N. *Just Health: Meeting Health Needs Fairly*; Cambridge University Press: Cambridge, UK, 2007.
28. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ* **2021**, *372*, n71. [CrossRef] [PubMed]
29. Roehrs, A.; Da Costa, C.A.; da Rosa Righi, R. OmniPHR: A distributed architecture model to integrate personal health records. *J. Biomed. Inform.* **2017**, *71*, 70–81. [CrossRef] [PubMed]
30. Keele, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; ver. 2.3 EBSE Technical Report; EBSE. 2007. Available online: https://legacyfileshare.elsevier.com/promis_misc/525444systematicreviewsguide.pdf (accessed on 20 June 2025).
31. Petticrew, M.; Roberts, H. *Systematic Reviews in the Social Sciences: A Practical Guide*; John Wiley & Sons: Hoboken, NJ, USA, 2008. Available online: https://fcsalud.ua.es/en/portal-de-investigacion/documentos/tools-for-the-bibliographic-research/guide-of-systematic-reviews-in-social-sciences.pdf (accessed on 20 June 2025).
32. Munn, Z.; Barker, T.H.; Moola, S.; Tufanaru, C.; Stern, C.; McArthur, A.; Stephenson, M.; Aromataris, E. Methodological quality of case series studies: An introduction to the JBI critical appraisal tool. *JBI Evid. Synth.* **2020**, *18*, 2127–2133. [CrossRef]
33. Nickerson, R.C.; Varshney, U.; Muntermann, J. A method for taxonomy development and its application in information systems. *Eur. J. Inf. Syst.* **2013**, *22*, 336–359. [CrossRef]
34. Huguet, A.; Hayden, J.A.; Stinson, J.; McGrath, P.J.; Chambers, C.T.; Tougas, M.E.; Wozney, L. Judging the quality of evidence in reviews of prognostic factor research: Adapting the GRADE framework. *Syst. Rev.* **2013**, *2*, 71. [CrossRef]
35. Gao, Y.; Zhang, A.; Wu, S.; Chen, J. Blockchain-based multi-hop permission delegation scheme with controllable delegation depth for electronic health record sharing. *High-Confid. Comput.* **2022**, *2*, 100084. [CrossRef]
36. Marino, C.A.; Diaz Paz, C. Smart Contracts and Shared Platforms in Sustainable Health Care: Systematic Review. *JMIR Med. Inform.* **2025**, *13*, e58575. [CrossRef] [PubMed]
37. Sittig, D.F.; Singh, H. A new sociotechnical model for studying health information technology in complex adaptive healthcare systems. *BMJ Qual. Saf.* **2010**, *19*, i68–i74. [CrossRef]
38. Jabarulla, M.Y.; Lee, H.N. Blockchain-based distributed patient-centric image management system. *Appl. Sci.* **2020**, *11*, 196. [CrossRef]
39. Iqbal, N.; Jamil, F.; Ahmad, S.; Kim, D. A novel blockchain-based integrity and reliable veterinary clinic information management system using predictive analytics for provisioning of quality health services. *IEEE Access* **2021**, *9*, 8069–8098. [CrossRef]
40. Mohsan, S.A.H.; Razzaq, A.; Ghayyur, S.A.K.; Alkahtani, H.K.; Al-Kahtani, N.; Mostafa, S.M. Decentralized patient-centric report and medical image management system based on blockchain technology and the inter-planetary file system. *Int. J. Environ. Res. Public Health* **2022**, *19*, 14641. [CrossRef]
41. Ali, A.; Almaiah, M.A.; Hajjej, F.; Pasha, M.F.; Fang, O.H.; Khan, R.; Teo, J.; Zakarya, M. An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network. *Sensors* **2022**, *22*, 572. [CrossRef]
42. Hang, L.; Choi, E.; Kim, D.H. A novel EMR integrity management based on a medical blockchain platform in hospital. *Electronics* **2019**, *8*, 467. [CrossRef]
43. Jamil, F.; Ahmad, S.; Iqbal, N.; Kim, D.H. Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals. *Sensors* **2020**, *20*, 2195. [CrossRef]
44. Dhillon, V. Blockchain based peer-review interfaces for digital medicine. *Front. Blockchain* **2020**, *3*, 8. [CrossRef]
45. Malamas, V.; Kotzanikolaou, P.; Dasaklis, T.K.; Burmester, M. A hierarchical multi blockchain for fine grained access to medical data. *IEEE Access* **2020**, *8*, 134393–134412. [CrossRef]
46. Gong, J.; Zhao, L. Blockchain application in healthcare service mode based on Health Data Bank. *Front. Eng. Manag.* **2020**, *7*, 605–614. [CrossRef]

47. Ali, A.; Rahim, H.A.; Ali, J.; Pasha, M.F.; Masud, M.; Rehman, A.U.; Chen, C.; Baz, M. A novel secure blockchain framework for accessing electronic health records using multiple certificate authority. *Appl. Sci.* **2021**, *11*, 9999. [CrossRef]
48. Chondrogiannis, E.; Andronikou, V.; Karanastasis, E.; Litke, A.; Varvarigou, T. Using blockchain and semantic web technologies for the implementation of smart contracts between individuals and health insurance organizations. *Blockchain Res. Appl.* **2022**, *3*, 100049. [CrossRef]
49. Su, J.; Zhang, L.; Mu, Y. BA-RMKABSE: Blockchain-aided ranked multi-keyword attribute-based searchable encryption with hiding policy for smart health system. *Future Gener. Comput. Syst.* **2022**, *132*, 299–309. [CrossRef]
50. Sutanto, E.; Mulyana, R.; Arisgraha, F.C.S.; Escrivá-Escrivá, G. Integrating blockchain for health insurance in Indonesia with hash authentication. *J. Theor. Appl. Electron. Commer. Res.* **2022**, *17*, 1602–1615. [CrossRef]
51. Careline, L.G.S.; Godhavari, T. Implementation of Electronic health record and health insurance management system using blockchain technology. *Int. J. Adv. Comput. Sci. Appl.* **2022**, *13*, 668–673. [CrossRef]
52. Salonikias, S.; Khair, M.; Mastoras, T.; Mavridis, I. Blockchain-based access control in a globalized healthcare provisioning ecosystem. *Electronics* **2022**, *11*, 2652. [CrossRef]
53. De Oliveira, M.T.; Reis, L.H.A.; Verginadis, Y.; Mattos, D.M.F.; Olabarriaga, S.D. SmartAccess: Attribute-based access control system for medical records based on smart contracts. *IEEE Access* **2022**, *10*, 117836–117854. [CrossRef]
54. Bhandawat, R.; Casucci, S.; Ramamurthy, B.; Walteros, J.L. Cooperative Blood Inventory Ledger (CoBIL): A decentralized decision-making framework for improving blood product management. *Comput. Ind. Eng.* **2022**, *172*, 108571. [CrossRef]
55. Haritha, T.; Anitha, A. Multi-level security in healthcare by integrating lattice-based access control and blockchain-based smart contracts system. *IEEE Access* **2023**, *11*, 114322–114340. [CrossRef]
56. Thantharate, P.; Thantharate, A. ZeroTrustBlock: Enhancing security, privacy, and interoperability of sensitive data through ZeroTrust permissioned blockchain. *Big Data Cogn. Comput.* **2023**, *7*, 165. [CrossRef]
57. Abdelgalil, L.; Mejri, M. HealthBlock: A framework for a collaborative sharing of electronic health records based on blockchain. *Future Internet* **2023**, *15*, 87. [CrossRef]
58. Chandini, A.; Basarkod, P.I. Patient centric pre-transaction signature verification assisted smart contract based blockchain for electronic healthcare records. *J. Ambient Intell. Humaniz. Comput.* **2023**, *14*, 4221–4235. [CrossRef]
59. Karmakar, A.; Ghosh, P.; Banerjee, P.S.; De, D. ChainSure: Agent free insurance system using blockchain for healthcare 4.0. *Intell. Syst. Appl.* **2023**, *17*, 200177. [CrossRef]
60. Selvarajan, S.; Mouratidis, H. A quantum trust and consultative transaction-based blockchain cybersecurity model for healthcare systems. *Sci. Rep.* **2023**, *13*, 7107. [CrossRef]
61. Liu, A.; Chen, X.B.; Xu, G.; Wang, Z.; Feng, X.; Feng, H. Quantum-Enhanced Blockchain: A Secure and Practical Blockchain Scheme. *Comput. Mater. Contin.* **2023**, *76*, 259–277. [CrossRef]
62. Balasubramaniam, A.; Surendiran, B. QUMA: Quantum unified medical architecture using blockchain. *Informatics* **2024**, *11*, 33. [CrossRef]
63. Venkatesh, R.; Darandale, S. Enhancing Healthcare Security with Quantum Blockchain: Electronic Medical Records Protection. In Proceedings of the 2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON), Bengaluru, India, 9–10 August 2024; pp. 1–6. [CrossRef]
64. Pu, X.; Jiang, R.; Song, Z.; Liang, Z.; Yang, L. A medical big data access control model based on smart contracts and risk in the blockchain environment. *Front. Public Health* **2024**, *12*, 1358184. [CrossRef]
65. Kaur, J.; Rani, R.; Kalra, N. Attribute-based access control scheme for secure storage and sharing of EHRs using blockchain and IPFS. *Clust. Comput.* **2024**, *27*, 1047–1061. [CrossRef]
66. Wang, T.; Wu, Q.; Chen, J.; Chen, F.; Xie, D.; Shen, H. Health data security sharing method based on hybrid blockchain. *Future Gener. Comput. Syst.* **2024**, *153*, 251–261. [CrossRef]
67. Li, P.; Zhou, D.; Ma, H.; Lai, J. Flexible and secure access control for EHR sharing based on blockchain. *J. Syst. Archit.* **2024**, *146*, 103033. [CrossRef]
68. Bobrova, P.; Perego, P.; Boiano, R. Design and Development of a Smart Fidget Toy Using Blockchain Technology to Improve Health Data Control. *Sensors* **2024**, *24*, 6582. [CrossRef]
69. Igboanusi, I.S.; Nnadiekwe, C.A.; Ogbede, J.U.; Kim, D.S.; Lensky, A. BOMS: Blockchain-enabled organ matching system. *Sci. Rep.* **2024**, *14*, 16069. [CrossRef] [PubMed]
70. Kaafarani, R.; Ismail, L.; Zahwe, O. Automatic Recommender System of Development Platforms for Smart Contract–Based Health Care Insurance Fraud Detection Solutions: Taxonomy and Performance Evaluation. *J. Med Internet Res.* **2024**, *26*, e50730. [CrossRef]
71. Liang, X.; Alam, N.; Sultana, T.; Bandara, E.; Shetty, S. Designing A Blockchain-Empowered Telehealth Artifact for Decentralized Identity Management and Trustworthy Communication: Interdisciplinary Approach. *J. Med Internet Res.* **2024**, *26*, e46556. [CrossRef]

72. Mahdi, S.S.; Ullah, Z.; Battineni, G.; Babar, M.G.; Daood, U. The Telehealth chain: A framework for secure and transparent telemedicine transactions on the blockchain. *Ir. J. Med. Sci.* **2024**, *193*, 2129–2137. [CrossRef] [PubMed]
73. Takahashi, T.; Zhihao, Y.; Omote, K. Emergency Medical Access Control System Based on Public Blockchain. *J. Med. Syst.* **2024**, *48*, 90. [CrossRef]
74. Wang, G.; Chen, C.; Jiang, Z.; Li, G.; Wu, C.; Li, S. Efficient Use of Biological Data in the Web 3.0 Era by Applying Nonfungible Token Technology. *J. Med. Internet Res.* **2024**, *26*, e46160. [CrossRef]
75. Yang, X.; Li, L. BPPKS: A blockchain-based privacy preserving and keyword-searchable scheme for medical data sharing. *Peer-to-Peer Netw. Appl.* **2024**, *17*, 4033–4048. [CrossRef]
76. Duc, T.; Trung, P.H.T.; Trong, N.D.P.; Phuc, N.T.; Khoa, T.D.; Khiem, H.G.; Nam, B.T.; Bang, L.K. Developing a Patient-Centric Healthcare IoT Platform with Blockchain and Smart Contract Data Management. *Int. J. Adv. Comput. Sci. Appl.* **2024**, *15*, 1139–1146. [CrossRef]
77. Guerra, K.; Koh, C.; Prybutok, V.; Johnson, V. A privacy perspective in adopting smart contract applications for healthcare. *J. Comput. Inf. Syst.* **2024**, 1–15. [CrossRef]
78. Li, H.; Li, D.; Liang, W. A smart contract-driven access control scheme with integrity checking for electronic health records. *Clust. Comput.* **2024**, *27*, 11515–11535. [CrossRef]
79. Rekik, S.; Alsulaiman, N.; Albadrani, N. A Health Record Management System Using Blockchain and Smart Contract. In Proceedings of the 2024 Seventh International Women in Data Science Conference at Prince Sultan University (WiDS PSU), Riyadh, Saudi Arabia, 3–4 March 2024; pp. 204–208. [CrossRef]
80. Saha, S.; Das, A.K.; Wazid, M.; Park, Y.; Garg, S.; Alrashoud, M. Smart contract-based access control scheme for blockchain assisted 6G-enabled IoT-based big data driven healthcare cyber physical systems. *IEEE Trans. Consum. Electron.* **2024**, *70*, 6975–6986. [CrossRef]
81. Vidhya, S.; Siva Raja, P.; Sumithra, R. Blockchain-Enabled Decentralized Healthcare Data Exchange: Leveraging Novel Encryption Scheme, Smart Contracts, and Ring Signatures for Enhanced Data Security and Patient Privacy. *Int. J. Netw. Manag.* **2024**, *34*, e2289. [CrossRef]
82. Arabnouri, A.; Shafieinejad, A. BACASE-SH: Blockchain-based authenticated certificate-less asymmetric searchable encryption for smart healthcare. *Peer-to-Peer Netw. Appl.* **2024**, *17*, 2298–2314. [CrossRef]
83. Bunia, S.; Campbell, O.; Carvalho, A.; Alluri, V. SCeFSTA: Smart Contract enabled Fair, Secure, and Transparent Auction for Healthcare Transportation. In Proceedings of the 2024 IEEE International Systems Conference (SysCon), Montreal, QC, Canada, 15–18 April 2024; pp. 1–8. [CrossRef]
84. Bieniek, J.; Rahouti, M.; Xiong, K.; Ferreira Araujo, G. SecureCare: A blockchain-assisted wearable body area network for secure and scalable IoT healthcare services. *Secur. Priv.* **2024**, *7*, e431. [CrossRef]
85. Alharbi, S.H.; Alzahrani, A.M.; Syed, T.A.; Alqahtany, S.S. Integrity and privacy assurance framework for remote healthcare monitoring based on IoT. *Computers* **2024**, *13*, 164. [CrossRef]
86. Kumar, N.; Ali, R. A smart contract-based 6G-enabled authentication scheme for securing Internet of Nano Medical Things network. *Ad Hoc Netw.* **2024**, *163*, 103606. [CrossRef]
87. Rohini, K.; Subramanian, R.; Soman, G. Improving Data Security and Scalability in Healthcare System using Blockchain Technology. *Scalable Comput. Pract. Exp.* **2024**, *25*, 3440–3452. [CrossRef]
88. Li, M.; Xue, J.; Liu, Z.; Suo, Y.; Lei, T.; Wang, Y. DAMFSD: A decentralized authorization model with flexible and secure delegation. *Internet Things* **2024**, *27*, 101317. [CrossRef]
89. Zhu, X.; Lai, T.; Li, H. Privacy-Preserving Byzantine-Resilient Swarm Learning for E-Healthcare. *Appl. Sci.* **2024**, *14*, 5247. [CrossRef]
90. Kar, J.; Liu, X.; Li, F. LA-IMDCN: A Lightweight Authentication Scheme With Smart Contract in Implantable Medical Device Communication Networks. *IEEE Access* **2024**, *12*, 99694–99703. [CrossRef]
91. Zhang, D.M.; Nie, C.; Zhang, J.Z.; Huang, H.W.; Huang, X. Consortium blockchain-based tunnel data bank for traceable sharing and treatment of structural health monitoring data. *Autom. Constr.* **2024**, *167*, 105720. [CrossRef]
92. Abid, A.; Cheikhrouhou, S.; Kallel, S.; Tari, Z.; Jmaiel, M. A smart contract-based access control framework for smart healthcare systems. *Comput. J.* **2024**, *67*, 407–422. [CrossRef]
93. Ahmed, H.; Gamal, A.; Abdelmouty, A. Optimizing Blockchain Platform Selection: A Decision-Making Approach Using LLMs, Type-2 Neutrosophic Numbers, CRITIC, and MAIRCA. *Neutrosophic Sets Syst.* **2025**, *83*, 25. [CrossRef]
94. Ahmed, I.; Fumimoto, K.; Nakano, T.; Tran, T.H. Blockchain-empowered decentralized philanthropic charity for social good. *Sustainability* **2024**, *16*, 210. [CrossRef]
95. Akhyani, J.; Patel, J.; Desai, V.; Gupta, R.; Tanwar, S.; Bhatia, J. GRACE: Blockchain and Game-Based Resource Allocation Scheme for SDN Controllers in ioT. In Proceedings of the 2024 IEEE International Conference on Communications Workshops (ICC Workshops), Denver, CO, USA, 9–13 June 2024; pp. 1431–1436. [CrossRef]

96. Ansar, S.; Natarajan, P.; Guran, L.R.V.R. A New Encryption Scheme Using Blockchain for Secured Accessing of Sensitive Health Care Records. *J. Adv. Inf. Technol.* **2025**, *16*, 510–526. [CrossRef]
97. Badidi, E.; Lamaazi, H.; El Harrouss, O. Toward a Secure Healthcare Ecosystem: A Convergence of Edge Analytics, Blockchain, and Federated Learning. In Proceedings of the 2024 20th International Conference on the Design of Reliable Communication Networks (DRCN), Montreal, QC, Canada, 6–9 May 2024; pp. 1–5. [CrossRef]
98. Basudan, S. IPFS-blockchain-based delegation model for internet of medical robotics things telesurgery system. *Connect. Sci.* **2024**, *36*, 2367549. [CrossRef]
99. Chegenizadeh, M.; Tessone, C.J. PAVA: Privacy-Preserving Attribute-Based Verifiable Authentication in Healthcare using Smart Contracts. In Proceedings of the 2024 IEEE International Conference on Blockchain (Blockchain), Copenhagen, Denmark, 19–22 August 2024; pp. 346–353. [CrossRef]
100. Devgun, T.; Kumar, G.; Conti, M. FASALKA: Offloaded Privacy Classification for Blockchain Smart Contracts. In Proceedings of the 2024 6th International Conference on Blockchain Computing and Applications (BCCA), Dubai, United Arab Emirates, 26–29 November 2024; pp. 204–210. [CrossRef]
101. Kumari, D.; Parmar, A.S.; Goyal, H.S.; Mishra, K.; Panda, S. Healthrec-chain: Patient-centric blockchain enabled ipfs for privacy preserving scalable health data. *Comput. Netw.* **2024**, *241*, 110223. [CrossRef]
102. Sun, L.; Liu, D.; Li, Y.; Zhou, D. A blockchain-based E-healthcare system with provenance awareness. *IEEE Access* **2024**, *12*, 110098–110112. [CrossRef]
103. Rani, P.; Sachan, R.K.; Kukreja, S. Educert-chain: A secure and notarized educational certificate authentication and verification system using permissioned blockchain. *Clust. Comput.* **2024**, *27*, 10169–10196. [CrossRef]
104. Riahi, A.; Erbad, A.; Bouras, A.; Mohamed, A. RL-Based Incentive Cooperative Data Learning Framework over Blockchain in Healthcare Applications (RL-ICDL-BC). In Proceedings of the 2024 International Wireless Communications and Mobile Computing (IWCMC), Ayia Napa, Cyprus, 27–31 May 2024; pp. 90–96. [CrossRef]
105. Cihan, S.; Ozsoy, A.; Beyan, O.D. Managing Clinical Research on Blockchain Using FAIR Principles. *Concurr. Comput. Pract. Exp.* **2025**, *37*, e70005. [CrossRef]
106. Aakanksha, A.; Sundaram, D. Optimizing Smart Ecosystems Using DAO: Collaborative Hospital Location Decision-Making. In Proceedings of the 58th Hawaii International Conference on System Sciences, Waikoloa Village, HI, USA, 7–10 January 2025. Available online: https://scholarspace.manoa.hawaii.edu/10.24251/HICSS.2025.147 (accessed on 18 June 2025).
107. Ding, X.; Liu, Y.; Ning, J.; Chen, D. Blockchain-Enhanced Anonymous Data Sharing Scheme for 6G-Enabled Smart Healthcare with Distributed Key Generation and Policy Hiding. *IEEE J. Biomed. Health Inform.* **2025**. [CrossRef]
108. Abdunabi, R.; Al Amin, M.; Basnet, R. An authorization framework for body area network: A policy verification and smart contract-based integrity assurance approach. *J. Comput. Secur.* **2025**, *33*, 119–162. [CrossRef]
109. Ahanger, T.A.; Ullah, I.; Algamdi, S.A.; Tariq, U. Machine learning-inspired intrusion detection system for IoT: Security issues and future challenges. *Comput. Electr. Eng.* **2025**, *123*, 110265. [CrossRef]
110. Ahmed, W.; Iqbal, W.; Hassan, A.; Ahmad, A.; Ullah, F.; Srivastava, G. Elevating e-health excellence with IOTA distributed ledger technology: Sustaining data integrity in next-gen fog-driven systems. *Future Gener. Comput. Syst.* **2025**, *168*, 107755. [CrossRef]
111. Ali, W.; Zhou, X.; Shao, J. Privacy-preserved and responsible recommenders: From conventional defense to federated learning and blockchain. *ACM Comput. Surv.* **2025**, *57*, 1–35. [CrossRef]
112. Mishra, D.K.; Mehra, P.S. DiabeticChain: A novel blockchain approach for patient-centric diabetic data management. *J. Supercomput.* **2025**, *81*, 166. [CrossRef]
113. Chaudhry, U.H.; Arshad, R.; Khalid, A.; Ray, I.G.; Hussain, M. zk-DASTARK: A quantum-resistant, data authentication and zero-knowledge proof scheme for protecting data feed to smart contracts. *Comput. Electr. Eng.* **2025**, *123*, 110089. [CrossRef]
114. Guo, R.; Liao, S.; Zhu, J. CrowdBA: A Low-Cost Quality-Driven Crowdsourcing Architecture for Bounding Box Annotation Based on Blockchain. *Electronics* **2025**, *14*, 345. [CrossRef]
115. Gupta, A.; Lakhwani, K. Enhancing blockchain quality-of-service: A comparative analysis and novel smart contract mechanism. *Discov. Appl. Sci.* **2025**, *7*, 807. [CrossRef]
116. Chen, X.; Ma, Y.; Cheng, Q.; Chen, X.; Luo, X. LB3AS: Lightweight Blockchain-Assisted Anonymous Authentication Scheme for Fog-Cloud-Based Internet of Medical Things. *IEEE Internet Things J.* **2025**, *12*, 18098–18114. [CrossRef]
117. Huang, P.; Lin, C.; Ning, J.; Wu, W. Optimized Blockchain-Based EMR Sharing via Secure Channel-Free Universal Designated Verifier Signature Proofs. *IEEE Internet Things J.* **2025**. [CrossRef]
118. Jayachandran, P. The difference between public and private blockchain. *Blockchain Unleashed: IBM Blockchain Blog* **2017**, *2017*. Available online: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/ (accessed on 20 June 2025).
119. Kamel Boulos, M.N.; Wilson, J.T.; Clauson, K.A. Geospatial blockchain: Promises, challenges, and scenarios in health and healthcare. *Int. J. Health Geogr.* **2018**, *17*, 25. [CrossRef]
120. Khatoon, A. A blockchain-based smart contract system for healthcare management. *Electronics* **2020**, *9*, 94. [CrossRef]

121. Jurvetson, S. How a quantum computer could break 2048-bit RSA encryption in 8 hours. *MIT Technol. Rev.* **2019**, *30*, 9.
122. Denker, K.; Javaid, A.Y. Quantum computing as a threat to modern cryptography techniques. In Proceedings of the International Conference on Foundations of Computer Science (FCS), Las Vegas, NV, USA, 29 July–1 August 2019; pp. 3–8.
123. Aggarwal, D.; Brennen, G.K.; Lee, T.; Santha, M.; Tomamichel, M. Quantum attacks on Bitcoin, and how to protect against them. *arXiv* **2017**, arXiv:1710.10377. [CrossRef]
124. Banerjee, S.; Mukherjee, A.; Panigrahi, P.K. Quantum blockchain using weighted hypergraph states. *Phys. Rev. Res.* **2020**, *2*, 013322. [CrossRef]
125. Kiktenko, E.O.; Pozhar, N.O.; Anufriev, M.N.; Trushechkin, A.S.; Yunusov, R.R.; Kurochkin, Y.V.; Lvovsky, A.; Fedorov, A.K. Quantum-secured blockchain. *Quantum Sci. Technol.* **2018**, *3*, 035004. [CrossRef]
126. Alabdulatif, A. Blockchain-Based Privacy-Preserving Authentication and Access Control Model for E-Health Users. *Information* **2025**, *16*, 219. [CrossRef]
127. Khan, A.; Litchfield, A.; Alabdulatif, A.; Khan, F. BlockPres IPFS: Performance evaluation of blockchain based secure patients prescription record storage using IPFS for smart prescription management system. *Clust. Comput.* **2025**, *28*, 255. [CrossRef]