Review

Not peer-reviewed version

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

Kenan Kaan Kurt * , Meral Timurtaş , Sevcan Pınar , Fatih Ozaydin * , Serkan Türkeli

Posted Date: 21 August 2025

doi: 10.20944/preprints202508.1589.v1

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

Article

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
[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, Istanbul, Türkiye
[6] TESODEV Technology Solutions Development Company Ltd., Küçükyalı, 34840 İstanbul, Turkey
* Correspondence: fatih@tiu.ac.jp

Abstract

The integration of blockchain technology into healthcare systems has emerged as a transformative 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. The systematic review includes 80 core studies published between 2019 and 2025, identified through searches in PubMed, Scopus, and Web of Science (WoS) using the PRISMA method. 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, particularly in ensuring data integrity, enhancing patient autonomy, and fostering a more resilient healthcare ecosystem. Recent advancements in quantum science and 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

1. Introduction

The availability, storage, and synchronization of electronic health records (EHR) remain critical, with patient confidentiality at risk due to uncontrolled data sharing [1]. Protecting user privacy is essential as cloud storage and smart health devices increase cybersecurity threats. To address these challenges, blockchain in healthcare requires strict authentication protocols and compliance with regulations like the Health Insurance Portability and Accountability Act (HIPAA). Researchers explore smart contracts, fraud detection, and authentication, though blockchain vulnerabilities and governance remain concerns [2]. While smart contracts are widely used, their healthcare role has often been secondary to IoT and health data sharing [3]. Studies have examined blockchain applications in clinical trial transparency, data management, and authentication [4,5].

While systematic reviews have examined blockchain in healthcare, few have categorized its smart contracts in health policy [2]. This study introduces a classification framework, highlighting compliance challenges, cryptographic mechanisms, and policy implications to enhance understanding of blockchain's regulatory role in digital health governance. This research evaluates blockchain-based smart contracts in health policy, emphasizing their role in security, transparency, and efficiency in healthcare operations.

2. Background

2.1. Review Stage Blockchain-Based Smart Contracts in Health Management

Blockchain ensures encrypted, decentralized data storage, enhancing security, efficiency, and transparency in healthcare and insurance beyond cryptocurrencies [5,6]. Smart contracts automate secure transactions through predefined rules, digitizing legal processes and enabling verifiable, encrypted exchanges [7].

Cost analysis using Hyperledger Caliper shows that permissioned blockchains significantly reduce transaction costs and energy consumption compared to Ethereum's former proof-of-work (PoW) mechanism [8]. Ethereum and Solidity have enabled real-world applications, with SmartPy expanding development for Python [7]. However, blockchain networks vary in capabilities. Benchmarking studies confirm that permissioned blockchains like Hyperledger Fabric outperform Ethereum in transaction throughput and efficiency, achieving up to 1000 TPS with sub-second latency [9].

AI-driven blockchain optimization is improving smart contract security and transaction validation. Ref. [10] demonstrated that AI-enhanced blockchain-based patient monitoring strengthens fraud detection and network security in Hyperledger Fabric. Ref. [11] showed that AI-powered blockchain mechanisms enhance fraud detection in decentralized healthcare transactions. Hyperledger Fabric is preferred for its security and controlled access, while Ethereum supports more decentralized smart contracts [7]. Algorand and Bitcoin-NG offer higher transaction throughput for high-demand applications [12].

Smart contracts facilitate medical record auditing, secure data sharing, and patient-controlled encryption, ensuring authentication via public key cryptography [12]. Hyperledger Caliper performance analysis confirms that permissioned blockchain architectures like Hyperledger Fabric provide low-latency, scalable, and secure transactions [13]. Ref. [14] benchmarked Ethereum and Hyperledger Fabric, confirming Fabric's superior efficiency and lower energy consumption compared to Ethereum's PoW-based mechanism.

Ref. [15] validated Hyperledger Fabric's effectiveness in medical records management. Ref. [16] experimentally confirmed its efficiency in cross-chain medical data sharing. Ref. [17] developed an AI-driven permissioned blockchain system for secure IoT medical data sharing, proving its scalability. SVM models identified abnormal behavior in EHR access [18], while XGBoost was used for real-time fraud detection in blockchain-based healthcare supply chains [19].

3. Methods

A systematic review following PRISMA guidelines [20] was conducted to classify blockchain-based smart contracts in health policy using keyword-based searches in major academic databases. The study examined PubMed, WoS, and Scopus (2019–2025), including both open-access and subscription-based publications.

3.1. Study Design

Our design includes identifying and assessing promising research areas that do not require extensive analysis or consolidation. The systematic mapping research adhered to strictly defined empirical criteria, following the stages defined in [21], i.e.,

Research questions: Defining the research questions analyzed.

Methodology: Overview of the software libraries investigated for data collection.

3.2. Research Questions

The development of research questions is a critical component of any systematic review [22,23]. 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 is the taxonomy/classification for blockchain-based smart contracts in health management policy?

GQ2: What are the healthcare protocols and standards that should be implemented in blockchain-based smart contracts?

3.3. 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 [22], 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")).

3.4. Article Selection

Following the systematic review methodologies [22], this study refined 950 identified articles to 80 primary studies. Exclusion criteria focused on relevance to blockchain, smart contracts, and healthcare, eliminating studies with explicit implementation details, blockchain security evaluations, or unrelated topics. 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 unambiguous technical materail and inadequate research, leaving selecting 80.

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

3.5. Quality Assessment

Following Ref. [22], we evaluated

- research aims and contextualization
- literature review and methodology
- findings and policy relevance,

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

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. Ref. [24] found them ideal for EHR management and hospital transactions, while Ref. [25] confirmed Algorand's scalability via its Byzantine Agreement. Refs. [26–28] noted that Ethereum-based smart contracts, despite strong security, suffer from high transaction costs and delays. They suggested 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. 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 Networks (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 Machines (SVM)	Classification-based algorithm with kernel functions	80-88%	Medium	Medium	Behavioral fraud analysis

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 explained in Section 3.4, 80 are left. These 80 papers were selected as primary references for the study. Table 2 provides a structured overview of each study, including publication year, reference, publisher, and category.

Table 2. Overview of every original research, organized by year of publication and containing the study's unique identity, reference, publisher, and category.

ID	Ref.	Author(s)	Year	Publisher	Type
A20	[29]	Hang et al.	2019	MDPI	Journal
A04	[30]	Jamil et al.	2020	MDPI	Journal
A19	[31]	Dhillon	2020	Frontiers Media	Journal
A21	[32]	Malamas et al.	2020	IEEE	Conference
A26	[33]	Gong and Zhao	2020	Springer Nature	Journal
A11	[34]	Ali et al.	2021	MDPI	Journal
A15	[35]	Jabarulla and Lee	2021	MDPI	Journal
A17	[36]	Iqbal et al.	2021	IEEE	Conference
A02	[37]	Mohsan et al.	2021	MDPI	Journal
A03	[38]	Ali et al.	2022	MDPI	Journal
A06	[39]	Chondrogiannis et al.	2022	Elsevier	Journal
A07	[40]	Su et al.	2022	Elsevier	Journal
A10	[41]	Sutanto et al.	2022	MDPI	Journal
A12	[5]	Zhang et al.	2022	IEEE	Journal
A13	[42]	Careline and Godhavari	2020	SAI	Journal
A16	[43]	Salonikias et al.	2022	MDPI	Journal
A25	[44]	De Olivera et al.	2022	IEEE	Conference
A27	[45]	Bhandawat et al.	2022	Elsevier	Journal
A08	[46]	Haritha and Anitha	2023	IEEE	Conference
A18	[47]	Thantharate and Thantharate	2023	MDPI	Journal
A22	[48]	Abdelgalil and Mejri	2023	MDPI	Journal
A23	[49]	Chandini and Basarkod	2023	Springer Nature	Journal
A24	[50]	Karmakar et al.	2023	Elsevier	Journal
A43	[51]	Selvarajan et al.	2023	Springer Nature	Journal

A44	[52]	Liu et al.	2023	Elsevier	Journal
A45	[53]	Prajapat et al.	2024	IEEE	Journal
A46	[54]	Balasubramaniam et al.	2024	MDPI	Journal
A47	[55]	Venkatesh et al.	2024	IEEE	Conference
A01	[27]	Pu et al.	2024	Frontiers Media	Journal
A05	[56]	Kaur et al.	2024	Springer Nature	Journal
A09	[57]	Wang et al.	2024	Elsevier	Journal
A14	[58]	Li et al.	2024	Elsevier	Journal
A28	[59]	Bobrova et al.	2024	MDPI	Journal
A29	[60]	Igboanusi et al.	2024	Springer Nature	Journal
A30	[61]	Kaafarani et al.	2024	JMIR	Journal
A31	[62]	Liang et al.	2024	JMIR	Journal
A32	[63]	Mahdi et al.	2024	Springer Nature	Journal
A33	[64]	Takahashi et al.	2024	Springer Nature	Journal
A34	[65]	Wang et al.	2024	JMIR	Journal
A36	[66]	Yang and Li	2024	Springer Nature	Journal
A37	[67]	Duc et al.	2024	SAI	Journal
A38	[68]	Guerra et al.	2024	Taylor & Francis	Journal
A39	[69]	Li et al.	2024	Springer Nature	Journal
A40	[70]	Rekik et al.	2024	IEEE	Conference
A41	[71]	Saha et al.	2024	IEEE	Journal
A42	[72]	Vidhya et al.	2024	Wiley	Journal
A48	[73]	Arabnouri & Shafieinejad	2024	Springer Nature	Journal
A49	[74]	Bunia et al.	2024	IEEE	Conference
A50	[75]	Bieniek et al.	2024	Wiley	Journal
A51	[76]	Alharbi et al.	2024	MDPI	Journal
A52	[77]	Kumar & Ali	2024	Elsevier	Journal
A53	[78]	Rohini et al.	2024	PKP	Journal
A54	[79]	Li et al.	2024	Elsevier	Journal
A56	[80]	Zhu et al.	2024	MDPI	Journal
A58	[81]	Kar et al.	2024	IEEE	Journal
A59	[82]	Zhang et al.	2024	Elsevier	Journal
A62	[83]	Abid et al.	2024	OUP	Journal
A64	[84]	Ahmed et al.	2024	Univ. of New Mexico	Journal
A65	[85]	Ahmed et al.	2024	MDPI	Journal
A67	[86]	Akhyani et al.	2024	IEEE	Conference
A69	[87]	Ansar et al.	2024	ETP	Journal
A70	[88]	Badidi et al.	2024	IEEE	Conference
A71	[89]	Basudan	2024	Taylor & Francis	Journal
A73	[90]	Chegenizadeh & Tessone	2024	IEEE	Conference
A74	[91]	Devgun et al.	2024	IEEE	Conference
A77	[92]	Kumari et al.	2024	Elsevier	Journal
A78	[93]	Sun et al.	2024	IEEE	Journal
A79	[94]	Rani et al.	2024	Springer Nature	Journal
A80	[95]	Riahi et al.	2024	IEEE	Journal
A55	[96]	Cihan et al.	2025	Wiley	Journal
A57	[97]	Aakanksha & Sundaram,	2025	HICSS	Conference
A60	[98]	Ding et al.	2025	IEEE	Journal

A61	[99]	Abdunabi et al.	2025	SAGE	Journal
A63	[100]	Ahanger et al.	2025	Elsevier	Journal
A66	[101]	Ahmed et al.	2025	Elsevier	Journal
A68	[102]	Ali et al.	2025	ACM	Journal
A35	[103]	Mishra and Mehra	2025	Springer Nature	Journal
A72	[104]	Chaudhry et al.	2025	Elsevier	Journal
A75	[105]	Guo et al.	2025	MDPI	Journal
A76	[106]	Gupta & Lakhwani	2025	Springer Nature	Journal

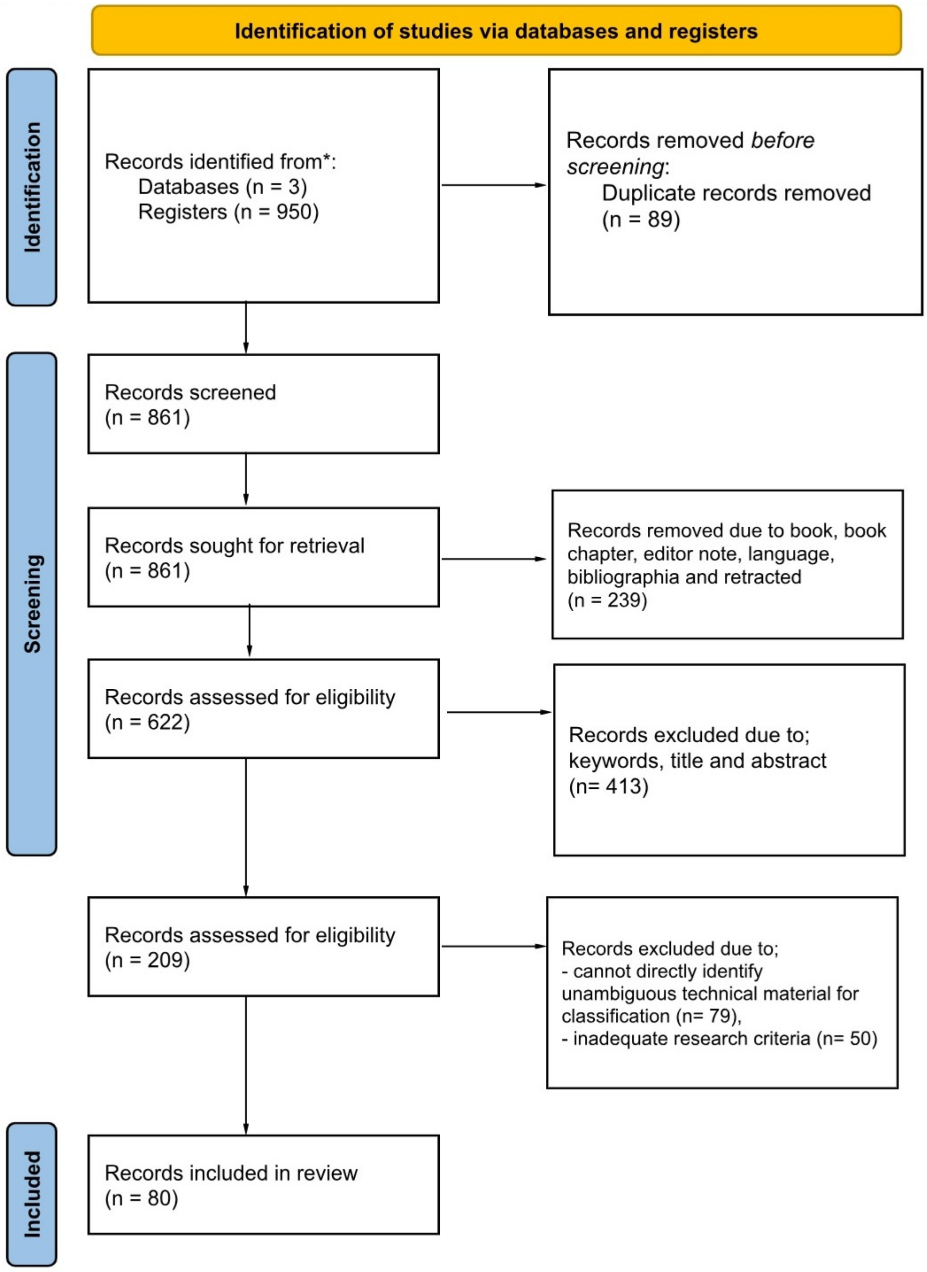
Identification of studies via databases and registers
Identification
Records identified from*:
Databases (n = 3)
Registers (n = 950)
Records removed *before screening*:
Duplicate records removed
(n = 89)
Screening
Records screened
(n = 861)
Records sought for retrieval
(n = 861)
Records removed due to book, book chapter, editor note, language, bibliographia and retracted
(n = 239)
Records assessed for eligibility
(n = 622)
Records excluded due to;
keywords, title and abstract
(n= 413)
Records assessed for eligibility
(n = 209)
Records excluded due to;
- cannot directly identify unambiguous technical material for classification (n= 79),
- inadequate research criteria (n= 50)
Included
Records included in review
(n = 80)

Figure 1. PRISMA flow diagram utilized in this review.

4.3. Conducting the Quality Evaluation

Each retrieved article was evaluated based on quality assessment criteria. The majority of studies met at least four out of 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. Discussions

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

GQ1. What is the taxonomy for blockchain-based smart contracts in healthcare?

Research has highlighted blockchain's potential in overcoming healthcare challenges, with smart contracts providing automated and secure solutions tailored to system requirements [26]. 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.

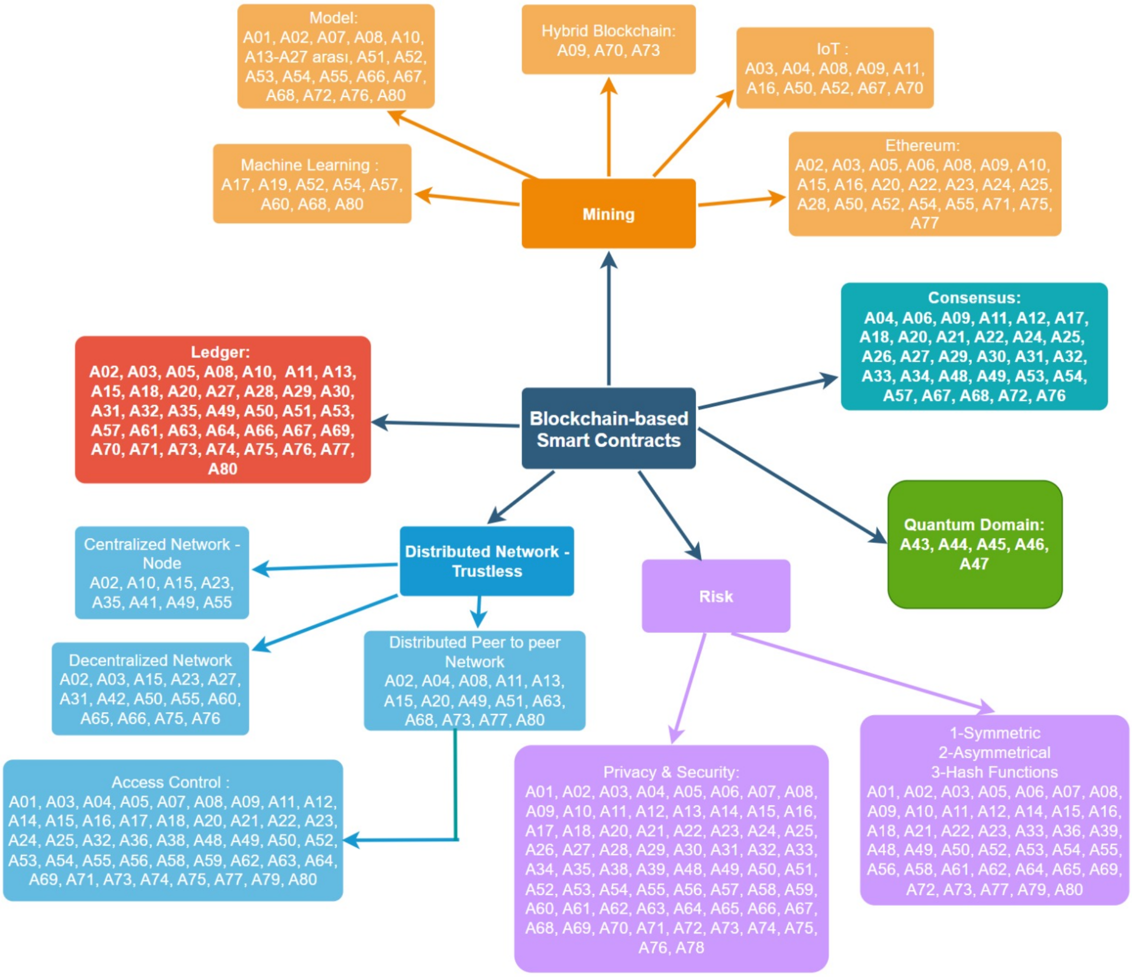
Model:
A01, A02, A07, A08, A10, A13-A27 arası, A51, A52, A53, A54, A55, A66, A67, A68, A72, A76, A80
Hybrid Blockchain:
A09, A70, A73
IoT :
A03, A04, A08, A09, A11, A16, A50, A52, A67, A70
Machine Learning :
A17, A19, A52, A54, A57, A60, A68, A80
Mining
Ethereum:
A02, A03, A05, A06, A08, A09, A10, A15, A16, A20, A22, A23, A24, A25, A28, A50, A52, A54, A55, A71, A75, A77
Consensus:
A04, A06, A09, A11, A12, A17, A18, A20, A21, A22, A24, A25, A26, A27, A29, A30, A31, A32, A33, A34, A48, A49, A53, A54, A57, A67, A68, A72, A76
Ledger:
A02, A03, A05, A08, A10, A11, A13, A15, A18, A20, A27, A28, A29, A30, A31, A32, A35, A49, A50, A51, A53, A57, A61, A63, A64, A66, A67, A69, A70, A71, A73, A74, A75, A76, A77, A80
Blockchain-based Smart Contracts
Centralized Network - Node
A02, A10, A15, A23, A35, A41, A49, A55
Distributed Network - Trustless
Quantum Domain:
A43, A44, A45, A46, A47
Risk
Decentralized Network
A02, A03, A15, A23, A27, A31, A42, A50, A55, A60, A65, A66, A75, A76
Distributed Peer to peer Network
A02, A04, A08, A11, A13, A15, A20, A49, A51, A63, A68, A73, A77, A80
1-Symmetric
2-Asymmetrical
3-Hash Functions
A01, A02, A03, A05, A06, A07, A08, A09, A10, A11, A12, A14, A15, A16, A18, A21, A22, A23, A33, A36, A39, A48, A49, A50, A52, A53, A54, A55, A56, A58, A61, A62, A64, A65, A69, A72, A73, A77, A79, A80
Access Control :
A01, A03, A04, A05, A07, A08, A09, A11, A12, A14, A15, A16, A17, A18, A20, A21, A22, A23, A24, A25, A32, A36, A38, A48, A49, A50, A52, A53, A54, A55, A56, A58, A59, A62, A63, A64, A69, A71, A73, A74, A75, A77, A79, A80
Privacy & Security:
A01, A02, A03, A04, A05, A06, A07, A08, A09, A10, A11, A12, A13, A14, A15, A16, A17, A18, A20, A21, A22, A23, A24, A25, A26, A27, A28, A29, A30, A31, A32, A33, A34, A35, A38, A39, A48, A49, A50, A51, A52, A53, A54, A55, A56, A57, A58, A59, A60, A61, A62, A63, A64, A65, A66, A67, A68, A69, A70, A71, A72, A73, A74, A75, A76, A78

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

5.1. Mining

Mining adds blocks to the blockchain, with miners verifying transactions based on consensus mechanisms [27,64,66]. Proof of Work (PoW) has been explored as an incentive model for healthcare providers, rewarding them with coins such as Ether [46,68]. To streamline data sharing, transactions are grouped into processing pools before mining [39]. 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 [44]. To lower costs, consortium blockchains are preferred over public blockchains [69]. Leader election algorithms improve efficiency in decentralized hospital networks [71]. 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 [68,69].

5.2. Consensus Mechanisms

Blockchain consensus mechanisms validate data before updates, with data controllers setting policies and processors ensuring compliance [27,30,31,35–37,40,46,47,49,50,67,70,72]. The choice of blockchain depends on the network type—public blockchains allow open participation, while private ones require approval [65]. Consensus mechanisms replace central authority reliance, ensuring secure and verified transactions across nodes [39]. Ref. [107] 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 [45]. Byzantine Fault Tolerance (BFT) enhances data integrity and security, with Istanbul BFT (IBFT) aiding health insurance fraud detection [57,61,103]. Reliable, Replicated, Redundant, and Fault-Tolerant (RAFT) consensus algorithm ensures secure health data storage and verification [71].

5.3. Security and Encryption

Encryption ensures confidentiality, integrity, and access control in healthcare blockchain systems, maintaining data integrity, traceability, and secure sharing [30,35–37,40,49,50,66–68,70–72]. Refs. [48,56–59,103,108] proposed a cryptographic authentication model for EMRs, enhancing identity verification and mitigating security threats. Public-key cryptography and Attribute-Based Encryption (ABE) enable user-controlled access, while Ref. [60] introduced a framework integrating ABE, Homomorphic Encryption (HE) for privacy-preserving computations, and Zero-Knowledge Proofs (ZKP) for secure identity verification. Consent management ensures privacy and compliance, while encrypted keyword indexing prevents unauthorized access [63]. CP-ABE restricts EHR access and maintains audit trails, while homomorphic encryption enables secure searches and data exchange [38]. Blockchain's immutability ensures long-term data accuracy, with consensus mechanisms validating and securely storing information [61].

5.4. Distributed Network

Distributed networks store health data across multiple nodes, eliminating central authority dependence while enhancing security and resilience [59,62,63]. 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 [32]. Smart contracts automate data management, while PoS resolves billing disputes. Decentralized networks improve organ donation transparency, fraud detection, and healthcare verification [60,61]. P2P architectures support hospital data decentralization, while IPFS-based solutions enhance security [30,36,37,40,47,49,50,70–72].

5.5. Ledger

Blockchain is a decentralized, immutable ledger ensuring data integrity, security, and transparency [33,35,47,61]. 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 [29,63,69]. Public blockchains allow open access, while private blockchains restrict entry [45,109]. Blockchain also enhances data sharing and computational efficiency [26].

Future research should validate the proposed taxonomy by implementing a prototype in EHR systems. Ref. [26] demonstrated a blockchain-based multi-hop permission delegation model, providing a foundation for healthcare-specific smart contract testing.

GQ2. What are the healthcare protocols and standards that should apply in blockchain-based smart contracts when it are applied to healthcare?

The healthcare protocols and standards related to smart contracts are presented in Figure 3. Research on blockchain and multi-certificate authority explores secure smart contract execution for health data access. Ref. [34] proposes 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 [56].

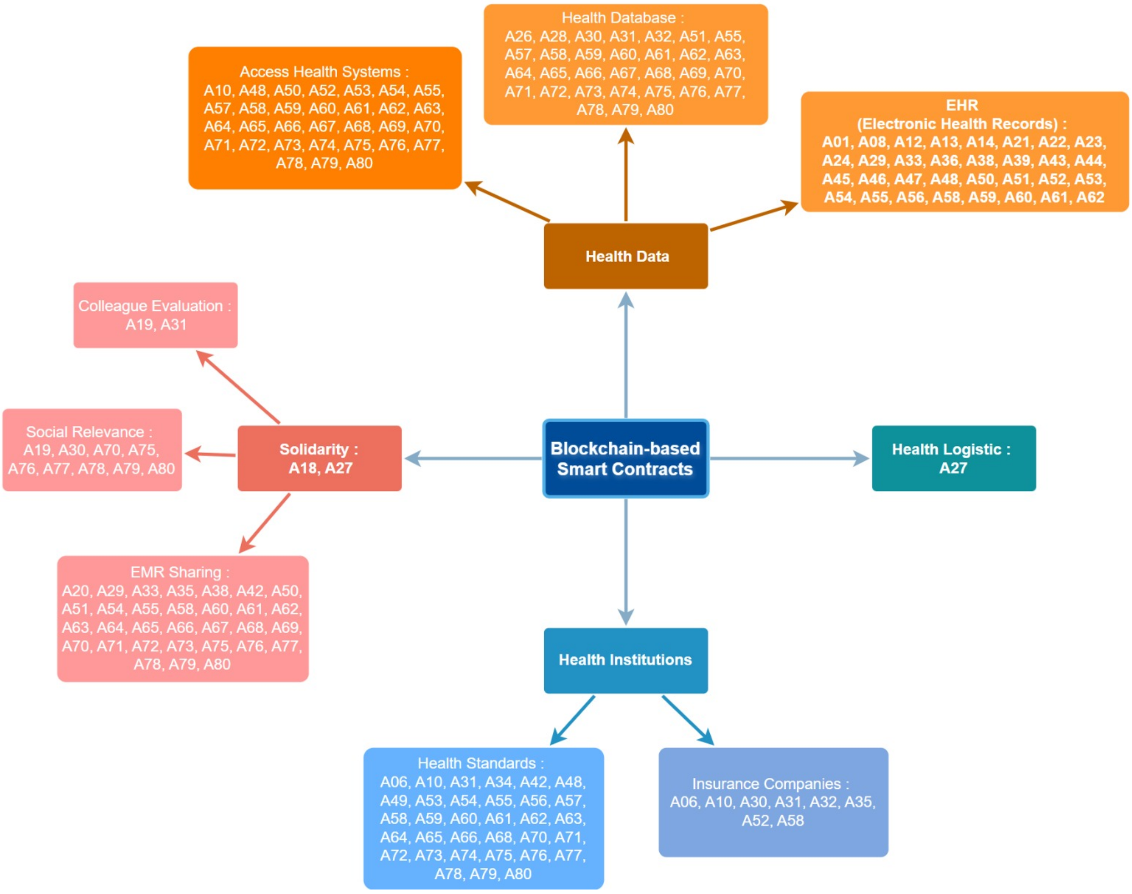
Health Database :
A26, A28, A30, A31, A32, A51, A55, A57, A58, A59, A60, A61, A62, A63, A64, A65, A66, A67, A68, A69, A70, A71, A72, A73, A74, A75, A76, A77, A78, A79, A80
Access Health Systems :
A10, A48, A50, A52, A53, A54, A55, A57, A58, A59, A60, A61, A62, A63, A64, A65, A66, A67, A68, A69, A70, A71, A72, A73, A74, A75, A76, A77, A78, A79, A80
EHR
(Electronic Health Records) :
A01, A08, A12, A13, A14, A21, A22, A23, A24, A29, A33, A36, A38, A39, A43, A44, A45, A46, A47, A48, A50, A51, A52, A53, A54, A55, A56, A58, A59, A60, A61, A62
Health Data
Colleague Evaluation :
A19, A31
Social Relevance :
A19, A30, A70, A75, A76, A77, A78, A79, A80
Solidarity :
A18, A27
Blockchain-based
Smart Contracts
Health Logistic :
A27
EMR Sharing :
A20, A29, A33, A35, A38, A42, A50, A51, A54, A55, A58, A60, A61, A62, A63, A64, A65, A66, A67, A68, A69, A70, A71, A72, A73, A75, A76, A77, A78, A79, A80
Health Institutions
Health Standards :
A06, A10, A31, A34, A42, A48, A49, A53, A54, A55, A56, A57, A58, A59, A60, A61, A62, A63, A64, A65, A66, A68, A70, A71, A72, A73, A74, A75, A76, A77, A78, A79, A80
Insurance Companies :
A06, A10, A30, A31, A32, A35, A52, A58

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

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 [59,61]. Enterprise blockchain ensures secure data exchange, as seen in Hyperledger Fabric, which supports inventory management without cryptocurrency reliance [45]. Smart contracts enable transparent transactions, strengthening collaboration and trust among stakeholders [31,47,57,62,63,68,70].

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 [29,110]. MedRec ensures secure data management with a transparent audit trail, while homomorphic encryption enhances privacy [38,49,111]. Blockchain streamlines insurance claims, reduces fraud, and enhances efficiency [61,62]. Hyperledger solutions improve security, and real-time access supports emergency response [63,64]. DiabeticChain aids chronic disease management [103]. Smart contracts ensure data verification, access control, and accountability, while an inter-nodal mechanism secures healthcare collaboration [39,43,66].

5.8. Participants

Blockchain's networking capabilities made participants capable of connecting with each other in a verifiable and safe way, even without a trustworthy medium [15,43,61]. Access control mechanisms regulate data retrieval for health institutions, laboratories, providers, and insurers [63,103]. RBAC and ABAC models ensure secure data sharing, privacy, and compliance among healthcare systems, pharmaceutical firms, and researchers [69,71].

5.9. Doctors

Doctors can securely access and manage patient records through encrypted communication and smart contracts [63,71]. Medical records are encrypted, stored in IPFS, and verified via blockchain hashes [31]. Physicians assist in organ donation verification and insurance claim validation, while emergency doctors use biometric authentication for rapid patient interventions [60,61,64].

5.10. Insurance Companies

Traditional insurance systems increase costs and data manipulation risks. Blockchain ensures secure, automated transactions with cryptographic protection [50]. It enables transparent access management, allowing secure transaction processing while protecting policyholder data [59,62]. Hyperledger Fabric enhances security and scalability [63]. Blockchain expedites insurance approvals and medical interventions, while decentralized management streamlines claims, prevents fraud, and strengthens trust through immutable records [41,64]. Ref. [13] 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 [112–114]. 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.

Ref. [115] proposes a blockchain framework based on quantum resources that maintains decentralization while defending against quantum adversaries, and demonstrates a proof-of-concept implementation on IBM's 5-qubit quantum computer with a very high fidelity. Ref. [116] presents 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. Ref. [51] introduces 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. Ref. [53] presents 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.

Ref. [52] proposes 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. In Ref. [54], a quantum-inspired blockchain (Qchain) is introduced alongside an entangled quantum medical record protocol, utilizing entangled states and quantum authentication to ensure privacy and auditability in Medical IoT systems. Finally, Ref. [55] proposes 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.

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 [73].

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 [74].

SecureCare introduces a blockchain-assisted wearable body area network (WBAN) architecture for IoT healthcare systems, offering enhanced data privacy, tamperproof security, and improved scalability for real-time patient monitoring through a decentralized and efficient framework [75].

Ref. [76] proposes 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 has been 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 [77].

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 [78].

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 [79].

A private permissioned blockchain framework based on Hyperledger Fabric has been 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 [96].

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 [80].

A decentralized autonomous organization (DAO)-driven framework has been 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 [97].

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 [81].

A consortium blockchain-based tunnel data bank has been 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 [82].

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 [98].

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 [99].

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 [83].

A decade-long analysis of intrusion detection systems (IDS) 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 [100].

A hybrid multi-criteria decision-making approach combining Type-2 Neutrosophic Numbers (T2NN), CRITIC, and MAIRCA is proposed to evaluate and rank blockchain platforms integrated with Large Language Models (LLMs), identifying Stellar, Klaytn, Openchain, and Hyperledger Fabric as top-performing platforms across technological, organizational, and environmental dimensions, thereby supporting more secure, automated, and user-friendly smart contract and data infrastructures [84].

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 UN Sustainable Development Goals through innovations like coin-toss-based data selection and service-based charity models [85].

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 limitations inherent in DLT consensus and participation [101].

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 [86].

A comprehensive survey of privacy-preserved and responsible recommender systems (RS) 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 [102].

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 [87].

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 [88].

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 [89]. The zk-DASTARK scheme combines zero-knowledge proofs 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 [104].

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 [90].

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 [91].

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 [105].

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 [106].

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 [92].

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 [93].

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 [94].

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 [95].

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.

6. Conclusions

Blockchain-based smart contracts enhance healthcare security, data privacy, encryption, and collaboration by improving data exchange, monitoring, and transparency while ensuring patient privacy [29]. Beyond cryptocurrency, blockchain supports healthcare, insurance regulations, and digital transformation, emphasizing security, interoperability, and institutional privacy frameworks. Regulatory compliance, particularly with HIPAA and GDPR, remains a challenge. Ref. [117] proposed a hybrid blockchain model integrating Attribute-Based Encryption (ABE) to improve patient data privacy and regulatory compliance. Ref. [118] explored blockchain-based prescription storage using IPFS to enhance healthcare database interoperability, stressing the need for standardized protocols aligned with FHIR and ISO/IEC 27799 frameworks. Permissioned blockchains with role-based access control can improve data governance in healthcare policy [26]. Blockchain's decentralized database facilitates disease research, drug development, and personalized treatments while reducing costs and increasing efficiency [111]. It enables real-time EHR management, secure provider communication, and automated insurance claims, streamlining administrative processes and reimbursement [26,32,111].

Future research should focus on policy integration, cost analysis, and scalability. Hyperledger technology may support multi-level security applications [46]. Smart contracts, DApps, and cloud-based solutions can optimize health data management, while further studies should explore blockchain's role in healthcare equity [42,43]. Blockchain-based data management systems significantly enhance healthcare insurance fraud prevention and ensure the secure storage of patient records. For example, the AI-driven blockchain encryption system developed by Ref. [119] has improved the secure access of hospitals to IoT-based healthcare devices, thereby increasing operational efficiency in medical services. AI-integrated blockchain systems are proving to be a game-changer in ensuring policy compliance and transparency in healthcare governance [120,121] highlight the role of blockchain in reducing fraud in healthcare insurance policies, leading to more reliable and fair healthcare governance [121]. Furthermore, Ref. [119] emphasizes the importance of secure searchable encryption frameworks in medical IoT systems to enable transparent data-sharing and automated compliance verification. These innovations underscore the growing synergy between blockchain and AI in policy-driven healthcare applications. Blockchain's immutability and transparency establish a secure digital trust system, requiring encrypted smart contracts for policy compliance [42]. In light of emerging quantum threats and evolving technological landscapes, there is a growing need to future-proof blockchain-based healthcare systems through quantum-resilient architectures and adaptive regulatory frameworks.

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.

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

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

ABE	Attribute-Based Encryption
EHR	Electronic Health Records
EMR	Electronic Medical Records
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
IoT	Internet of Things
NIH	National Institute of Health
NN	Neural Networks
PHR	Personal Health Records
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 Machines
WoS	Web of Science
ZKP	Zero-Knowledge Proofs

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. https://doi.org/https://doi.org/10.1371/journal.pone.0239946.
2. McGhin, T.; Choo, K.K.R.; Liu, C.Z.; He, D. Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications* **2019**, *135*, 62–75. https://doi.org/https://doi.org/10.1016/j.jnca.2019.02.027.
3. Ante, L. Smart contracts on the blockchain–A bibliometric analysis and review. *Telematics and Informatics* **2021**, *57*, 101519. https://doi.org/https://doi.org/10.1016/j.tele.2020.101519.
4. Christidis, K.; Devetsikiotis, M. Blockchains and smart contracts for the internet of things. *IEEE Access* **2016**, *4*, 2292–2303. https://doi.org/https://doi.org/10.1109/ACCESS.2016.2566338.
5. Zhang, L.; Zhang, T.; Wu, Q.; Mu, Y.; Rezaeibagha, F. Secure decentralized attribute-based sharing of personal health records with blockchain. *IEEE Internet of Things Journal* **2021**, *9*, 12482–12496. https://doi.org/https://doi.org/10.1109/JIOT.2021.3137240.
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 Transactions on Computational Social Systems* **2022**, *10*, 1642–1653. https://doi.org/https://doi.org/10.1109/TCSS.2022.3219256.
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. https://doi.org/https://doi.org/10.1109/ACCESS.2019.2896108.

8. Alammary, A.S. Building a sustainable digital infrastructure for higher education: A blockchain-based solution for cross-institutional enrollment. *Sustainability* **2024**, *17*, 194. https://doi.org/https://doi.org/10.3390/su17010194.
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. https://doi.org/https://doi.org/10.3390/math13030521.
10. Garg, S.; Kaushal, R.K.; Kumar, N. A novel design and performance assessment of a blockchain-powered remote patient monitoring system. *SN Computer Science* **2024**, *5*, 849. https://doi.org/https://doi.org/10.1007/s42979-024-03151-2.
11. Ali, K.; Unalp, A. Blockchain and AI Collaboration: Building Trust and Security in Decentralized Networks **2025**.
12. 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). IEEE, 2016, pp. 25–30. https://doi.org/https://doi.org/10.1109/OBD.2016.11.
13. Kaushal, R.K.; Kumar, N.; Kukreja, V.; Boonchieng, E. Hyperledger fabric based remote patient monitoring solution and performance evaluation. *Peer-to-Peer Networking and Applications* **2025**, *18*, 105. https://doi.org/https://doi.org/10.1007/s12083-025-01921-0.
14. Ucbas, Y.; Eleyan, A.; Hammoudeh, M.; Alohaly, M. Performance and scalability analysis of ethereum and hyperledger fabric. *IEEE Access* **2023**, *11*, 67156–67167. https://doi.org/https://doi.org/10.1109/ACCESS.2023.3291618.
15. Mnasri, S.; Salah, D.; Idoudi, H. A hybrid blockchain and federated learning attention-based BERT transformer framework for medical records management. *The Journal of Supercomputing* **2025**, *81*, 317. https://doi.org/https://doi.org/10.1007/s11227-024-06816-0.
16. 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). IEEE, 2024, pp. 338–342. https://doi.org/https://doi.org/10.1109/CCSB63463.2024.10735540.
17. 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). IEEE, 2024, pp. 1–6. https://doi.org/https://doi.org/10.1109/HealthCom60970.2024.10880766.
18. Bezanjani, B.R.; Ghafouri, S.H.; Gholamrezaei, R. Privacy-preserving healthcare data in IoT: a synergistic approach with deep learning and blockchain. *The Journal of Supercomputing* **2025**, *81*, 533. https://doi.org/https://doi.org/10.1007/s11227-025-06980-x.
19. Liu, Y.; Sharma, A.; Rani, S.; Yang, J. Supply Chain Security, Resilience and Agility in IoT-driven Healthcare. *IEEE Internet of Things Journal* **2025**. https://doi.org/https://doi.org/10.1109/JIOT.2025.3545962.
20. 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*. https://doi.org/https://doi.org/10.1136/bmj.n71.
21. Roehrs, A.; Da Costa, C.A.; da Rosa Righi, R. OmniPHR: A distributed architecture model to integrate personal health records. *Journal of biomedical informatics* **2017**, *71*, 70–81. https://doi.org/https://doi.org/10.1016/j.jbi.2017.05.012.
22. Keele, S.; et al. Guidelines for performing systematic literature reviews in software engineering. Technical report, Technical report, ver. 2.3 EBSE technical report. EBSE, 2007. https://doi.org/https://legacyfileshare.elsevier.com/promis_misc/525444systematicreviewsguide.pdf.
23. Petticrew, M.; Roberts, H. *Systematic reviews in the social sciences: A practical guide*; John Wiley & Sons, 2008. https://doi.org/https://fcsalud.ua.es/en/portal-de-investigacion/documentos/tools-for-the-bibliographic-research/guide-of-systematic-reviews-in-social-sciences.pdf.
24. Jain, A.K.; Gupta, N.; Gupta, B.B. A survey on scalable consensus algorithms for blockchain technology. *Cyber Security and Applications* **2025**, *3*, 100065. https://doi.org/https://doi.org/10.1016/j.jnca.2021.103020.
25. Yadav, J.; Shevkar, R. Performance-based analysis of blockchain scalability metric. *Tehnički glasnik* **2021**, *15*, 133–142. https://doi.org/https://doi.org/10.31803/tg-20210205103310.
26. 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-Confidence Computing* **2022**, *2*, 100084. https://doi.org/https://doi.org/10.1016/j.hcc.2022.100084.

27. 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. *Frontiers in Public Health* **2024**, *12*, 1358184. https://doi.org/https://doi.org/10.3389/fpubh.2024.1358184.
28. Marino, C.A.; Diaz Paz, C. Smart Contracts and Shared Platforms in Sustainable Health Care: Systematic Review. *JMIR Medical Informatics* **2025**, *13*, e58575. https://doi.org/https://doi.org/10.2196/58575.
29. Hang, L.; Choi, E.; Kim, D.H. A novel EMR integrity management based on a medical blockchain platform in hospital. *Electronics* **2019**, *8*, 467. https://doi.org/https://doi.org/10.3390/electronics8040467.
30. 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. https://doi.org/https://doi.org/10.3390/s20082195.
31. Dhillon, V. Blockchain based peer-review interfaces for digital medicine. *Frontiers in Blockchain* **2020**, *3*, 8. https://doi.org/https://doi.org/10.3389/fbloc.2020.00008.
32. 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. https://doi.org/https://doi.org/10.1109/ACCESS.2020.3011201.
33. Gong, J.; Zhao, L. Blockchain application in healthcare service mode based on Health Data Bank. *Frontiers of engineering management* **2020**, *7*, 605–614. https://doi.org/https://doi.org/10.1007/s42524-020-0138-9.
34. 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. *Applied Sciences* **2021**, *11*, 9999. https://doi.org/https://doi.org/10.3390/app11219999.
35. Jabarulla, M.Y.; Lee, H.N. Blockchain-based distributed patient-centric image management system. *Applied Sciences* **2020**, *11*, 196. https://doi.org/https://doi.org/10.3390/app11010196.
36. 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. https://doi.org/https://doi.org/10.1109/ACCESS.2021.3049325.
37. 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. *International Journal of Environmental Research and Public Health* **2022**, *19*, 14641. https://doi.org/https://doi.org/10.3390/ijerph192214641.
38. 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. https://doi.org/https://doi.org/10.3390/s22020572.
39. 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: Research and Applications* **2022**, *3*, 100049. https://doi.org/https://doi.org/10.1016/j.bcra.2021.100049.
40. 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 Generation Computer Systems* **2022**, *132*, 299–309. https://doi.org/https://doi.org/10.1016/j.future.2022.01.021.
41. Sutanto, E.; Mulyana, R.; Arisgraha, F.C.S.; Escrivá-Escrivá, G. Integrating blockchain for health insurance in Indonesia with hash authentication. *Journal of Theoretical and Applied Electronic Commerce Research* **2022**, *17*, 1602–1615. https://doi.org/https://doi.org/10.3390/jtaer17040081.
42. Careline, L.G.S.; Godhavari, T. Implementation of Electronic health record and health insurance management system using blockchain technology. *International Journal of Advanced Computer Science and Applications* **2022**, *13*. https://doi.org/https://doi.org/10.14569/IJACSA.2022.0130679.
43. Salonikias, S.; Khair, M.; Mastoras, T.; Mavridis, I. Blockchain-based access control in a globalized healthcare provisioning ecosystem. *Electronics* **2022**, *11*, 2652. https://doi.org/https://doi.org/10.3390/electronics11172652.
44. 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. https://doi.org/https://doi.org/10.1109/ACCESS.2022.3217201.
45. Bhandawat, R.; Casucci, S.; Ramamurthy, B.; Walteros, J.L. Cooperative Blood Inventory Ledger (CoBIL): A decentralized decision-making framework for improving blood product management. *Computers & Industrial Engineering* **2022**, *172*, 108571. https://doi.org/https://doi.org/10.1016/j.cie.2022.108571.

46. 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. https://doi.org/https://doi.org/10.1109/ACCESS.2023.3324740.
47. Thantharate, P.; Thantharate, A. ZeroTrustBlock: Enhancing security, privacy, and interoperability of sensitive data through ZeroTrust permissioned blockchain. *Big Data and Cognitive Computing* **2023**, *7*, 165. https://doi.org/https://doi.org/10.3390/bdcc7040165.
48. Abdelgalil, L.; Mejri, M. HealthBlock: A framework for a collaborative sharing of electronic health records based on blockchain. *Future Internet* **2023**, *15*, 87. https://doi.org/https://doi.org/10.3390/fi15030087.
49. Chandini, A.; Basarkod, P.I. Patient centric pre-transaction signature verification assisted smart contract based blockchain for electronic healthcare records. *Journal of Ambient Intelligence and Humanized Computing* **2023**, *14*, 4221–4235. https://doi.org/https://doi.org/10.1007/s12652-023-04526-8.
50. Karmakar, A.; Ghosh, P.; Banerjee, P.S.; De, D. ChainSure: Agent free insurance system using blockchain for healthcare 4.0. *Intelligent Systems with Applications* **2023**, *17*, 200177. https://doi.org/https://doi.org/10.1016/j.iswa.2023.200177.
51. Selvarajan, S.; Mouratidis, H. A quantum trust and consultative transaction-based blockchain cybersecurity model for healthcare systems. *Scientific Reports* **2023**, *13*, 7107. https://doi.org/https://doi.org/10.1038/s41598-023-34354-x.
52. Liu, A.; Chen, X.B.; Xu, G.; Wang, Z.; Feng, X.; Feng, H. Quantum-Enhanced Blockchain: A Secure and Practical Blockchain Scheme. *Computers, Materials & Continua* **2023**, *76*. https://doi.org/https://doi.org/10.32604/cmc.2023.039397.
53. 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 of Things Journal* **2024**. https://doi.org/https://doi.org/10.1109/JIOT.2024.3448212.
54. Balasubramaniam, A.; Surendiran, B. QUMA: quantum unified medical architecture using blockchain **2024**. *11*, 33. https://doi.org/https://doi.org/10.3390/informatics11020033.
55. 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). IEEE, 2024, pp. 1–6. https://doi.org/https://doi.org/10.1109/NMITCON62075.2024.10699120.
56. Kaur, J.; Rani, R.; Kalra, N. Attribute-based access control scheme for secure storage and sharing of EHRs using blockchain and IPFS. *Cluster Computing* **2024**, *27*, 1047–1061. https://doi.org/https://doi.org/10.1007/s10586-023-04038-2.
57. Wang, T.; Wu, Q.; Chen, J.; Chen, F.; Xie, D.; Shen, H. Health data security sharing method based on hybrid blockchain. *Future Generation Computer Systems* **2024**, *153*, 251–261. https://doi.org/https://doi.org/10.1016/j.future.2023.11.032.
58. Li, P.; Zhou, D.; Ma, H.; Lai, J. Flexible and secure access control for EHR sharing based on blockchain. *Journal of Systems Architecture* **2024**, *146*, 103033. https://doi.org/https://doi.org/10.1016/j.sysarc.2023.103033.
59. 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. https://doi.org/https://doi.org/10.3390/s24206582.
60. Igboanusi, I.S.; Nnadiekwe, C.A.; Ogbede, J.U.; Kim, D.S.; Lensky, A. BOMS: blockchain-enabled organ matching system. *Scientific Reports* **2024**, *14*, 16069. https://doi.org/https://doi.org/10.1038/s41598-024-66375-5.
61. 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. *Journal of Medical Internet Research* **2024**, *26*, e50730. https://doi.org/https://doi.org/10.2196/50730.
62. 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. *Journal of medical Internet research* **2024**, *26*, e46556. https://doi.org/https://doi.org/10.2196/46556.
63. 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. *Irish Journal of Medical Science (1971-)* **2024**, *193*, 2129–2137. https://doi.org/https://doi.org/10.1007/s11845-024-03728-z.
64. Takahashi, T.; Zhihao, Y.; Omote, K. Emergency Medical Access Control System Based on Public Blockchain. *Journal of Medical Systems* **2024**, *48*, 90. https://doi.org/https://doi.org/10.1007/s10916-024-02102-x.

65. 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. *Journal of Medical Internet Research* **2024**, *26*, e46160. https://doi.org/https://doi.org/10.2196/46160.
66. Yang, X.; Li, L. BPPKS: A blockchain-based privacy preserving and keyword-searchable scheme for medical data sharing. *Peer-to-Peer Networking and Applications* **2024**, *17*, 4033–4048. https://doi.org/https://doi.org/10.1007/s12083-024-01795-8.
67. Duc, T.; PHT, T.; DP, T.N.; et al. Developing a Patient-Centric Healthcare IoT Platform with Blockchain and Smart Contract Data Management. *International Journal of Advanced Computer Science & Applications* **2024**, *15*. https://doi.org/https://doi.org/10.14569/IJACSA.2024.01504115.
68. Guerra, K.; Koh, C.; Prybutok, V.; Johnson, V. A privacy perspective in adopting smart contract applications for healthcare. *Journal of Computer Information Systems* **2024**, pp. 1–15. https://doi.org/https://doi.org/10.1080/08874417.2024.2408003.
69. Li, H.; Li, D.; Liang, W. A smart contract-driven access control scheme with integrity checking for electronic health records. *Cluster Computing* **2024**, *27*, 11515–11535. https://doi.org/https://doi.org/10.1007/s10586-024-04524-1.
70. 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). IEEE, 2024, pp. 204–208. https://doi.org/https://doi.org/10.1109/WiDS-PSU61003.2024.00049.
71. 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 Transactions on Consumer Electronics* **2024**, *70*, 6975–6986. https://doi.org/https://doi.org/10.1109/TCE.2024.3391667.
72. 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. *International Journal of Network Management* **2024**, *34*, e2289. https://doi.org/https://doi.org/10.1002/nem.2289.
73. Arabnouri, A.; Shafieinejad, A. BACASE-SH: Blockchain-based authenticated certificate-less asymmetric searchable encryption for smart healthcare. *Peer-to-Peer Networking and Applications* **2024**, *17*, 2298–2314. https://doi.org/https://doi.org/10.1007/s12083-024-01687-x.
74. 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). IEEE, 2024, pp. 1–8. https://doi.org/https://doi.org/10.1109/SysCon61195.2024.10553424.
75. Bieniek, J.; Rahouti, M.; Xiong, K.; Ferreira Araujo, G. SecureCare: A blockchain-assisted wearable body area network for secure and scalable IoT healthcare services. *Security and Privacy* **2024**, *7*, e431. https://doi.org/https://doi.org/10.1002/spy2.431.
76. 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. https://doi.org/https://doi.org/10.3390/computers13070164.
77. Kumar, N.; Ali, R. A smart contract-based 6G-enabled authentication scheme for securing Internet of Nano Medical Things network. *Ad Hoc Networks* **2024**, *163*, 103606. https://doi.org/https://doi.org/10.1016/j.adhoc.2024.103606.
78. Rohini, K.; Subramanian, R.; Soman, G. Improving Data Security and Scalability in Healthcare System using Blockchain Technology. *Scalable Computing: Practice and Experience* **2024**, *25*, 3440–3452. https://doi.org/https://doi.org/10.12694/scpe.v25i5.3164.
79. Li, M.; Xue, J.; Liu, Z.; Suo, Y.; Lei, T.; Wang, Y. DAMFSD: A decentralized authorization model with flexible and secure delegation. *Internet of Things* **2024**, *27*, 101317. https://doi.org/https://doi.org/10.1016/j.iot.2024.101317.
80. Zhu, X.; Lai, T.; Li, H. Privacy-Preserving Byzantine-Resilient Swarm Learning for E-Healthcare. *Applied Sciences* **2024**, *14*, 5247. https://doi.org/https://doi.org/10.3390/app14125247.
81. Kar, J.; Liu, X.; Li, F. LA-IMDCN: A Lightweight Authentication Scheme With Smart Contract in Implantable Medical Device Communication Networks. *IEEE Access* **2024**. https://doi.org/https://doi.org/10.1109/ACCESS.2024.3429137.

82. 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. *Automation in Construction* **2024**, *167*, 105720. https://doi.org/https://doi.org/10.1016/j.autcon.2024.105720.
83. Abid, A.; Cheikhrouhou, S.; Kallel, S.; Tari, Z.; Jmaiel, M. A smart contract-based access control framework for smart healthcare systems. *The Computer Journal* **2024**, *67*, 407–422. https://doi.org/https://doi.org/10.1093/comjnl/bxac183.
84. 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 and Systems* **2025**, *83*, 25. https://doi.org/https://doi.org/10.5281/zenodo.15127966.
85. Ahmed, I.; Fumimoto, K.; Nakano, T.; Tran, T.H. Blockchain-empowered decentralized philanthropic charity for social good. *Sustainability* **2024**, *16*, 210. https://doi.org/https://doi.org/10.3390/su16010210.
86. 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). IEEE, 2024, pp. 1431–1436. https://doi.org/https://doi.org/10.1109/ICCWorkshops59551.2024.10615977.
87. Ansar, S.; Natarajan, P.; Guran, L.R.V.R. A New Encryption Scheme Using Blockchain for Secured Accessing of Sensitive Health Care Records. *Journal of Advances in Information Technology* **2025**, *5*, 510–526. https://doi.org/https://doi.org/10.12720/jait.16.4.510-526.
88. 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). IEEE, 2024, pp. 1–5. https://doi.org/https://doi.org/10.1109/DRCN60692.2024.10539174.
89. Basudan, S. IPFS-blockchain-based delegation model for internet of medical robotics things telesurgery system. *Connection Science* **2024**, *36*, 2367549. https://doi.org/https://doi.org/10.1080/09540091.2024.2367549.
90. 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). IEEE, 2024, pp. 346–353. https://doi.org/https://doi.org/10.1109/Blockchain62396.2024.00052.
91. 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). IEEE, 2024, pp. 204–210. https://doi.org/https://doi.org/10.1109/BCCA62388.2024.10844467.
92. 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. *Computer Networks* **2024**, *241*, 110223. https://doi.org/https://doi.org/10.1016/j.comnet.2024.110223.
93. Sun, L.; Liu, D.; Li, Y.; Zhou, D. A blockchain-based E-healthcare system with provenance awareness. *IEEE Access* **2024**. https://doi.org/https://doi.org/10.1109/ACCESS.2024.3440170.
94. Rani, P.; Sachan, R.K.; Kukreja, S. Educert-chain: a secure and notarized educational certificate authentication and verification system using permissioned blockchain. *Cluster Computing* **2024**, *27*, 10169–10196. https://doi.org/https://doi.org/10.1007/s10586-024-04469-5.
95. 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). IEEE, 2024, pp. 90–96. https://doi.org/https://doi.org/10.1109/IWCMC61514.2024.10592513.
96. Cihan, S.; Ozsoy, A.; Beyan, O.D. Managing Clinical Research on Blockchain Using FAIR Principles. *Concurrency and Computation: Practice and Experience* **2025**, *37*, e70005. https://doi.org/https://doi.org/10.1002/cpe.70005.
97. Aakanksha, A.; Sundaram, D. Optimizing Smart Ecosystems Using DAO: Collaborative Hospital Location Decision-Making. In Proceedings of the Proceedings of the 58th Hawaii International Conference on System Sciences, 2025. https://doi.org/https://scholarspace.manoa.hawaii.edu/10.24251/HICSS.2025.147.
98. 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 Journal of Biomedical and Health Informatics* **2025**. https://doi.org/https://doi.org/10.1109/JBHI.2025.3550261.

99. Abdunabi, R.; Al Amin, M.; Basnet, R. An authorization framework for body area network: A policy verification and smart contract-based integrity assurance approach. *Journal of Computer Security* **2025**, p. 0926227X241296435. https://doi.org/https://doi.org/10.1177/0926227X241296435.
100. Ahanger, T.A.; Ullah, I.; Algamdi, S.A.; Tariq, U. Machine learning-inspired intrusion detection system for IoT: Security issues and future challenges. *Computers and Electrical Engineering* **2025**, *123*, 110265. https://doi.org/https://doi.org/10.1016/j.compeleceng.2025.110265.
101. 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 Generation Computer Systems* **2025**, *168*, 107755. https://doi.org/https://doi.org/10.1016/j.future.2025.107755.
102. Ali, W.; Zhou, X.; Shao, J. Privacy-preserved and responsible recommenders: From conventional defense to federated learning and blockchain. *ACM Computing Surveys* **2025**, *57*, 1–35. https://doi.org/https://doi.org/10.1145/3708982.
103. Mishra, D.K.; Mehra, P.S. DiabeticChain: a novel blockchain approach for patient-centric diabetic data management. *The Journal of Supercomputing* **2025**, *81*, 166. https://doi.org/https://doi.org/10.1007/s11227-024-06589-6.
104. 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. *Computers and Electrical Engineering* **2025**, *123*, 110089. https://doi.org/https://doi.org/10.1016/j.compeleceng.2025.110089.
105. 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. https://doi.org/https://doi.org/10.3390/electronics14020345.
106. Gupta, A.; Lakhwani, K. Enhancing blockchain quality-of-service: a comparative analysis and novel smart contract mechanism. *Discover Applied Sciences* **2025**, *7*, 1–26. https://doi.org/https://doi.org/10.1007/s42452-025-07395-2.
107. 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 of Things Journal* **2025**. https://doi.org/https://doi.org/10.1109/JIOT.2025.3539428.
108. Huang, P.; Lin, C.; Ning, J.; Wu, W. Optimized Blockchain-Based EMR Sharing via Secure Channel-Free Universal Designated Verifier Signature Proofs. *IEEE Internet of Things Journal* **2025**. https://doi.org/https://doi.org/10.1109/JIOT.2025.3545913.
109. Jayachandran, P. The difference between public and private blockchain. *Blockchain Unleashed: IBM Blockchain Blog* **2017**, *2017*. https://doi.org/https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/.
110. Kamel Boulos, M.N.; Wilson, J.T.; Clauson, K.A. Geospatial blockchain: promises, challenges, and scenarios in health and healthcare. *International journal of health geographics* **2018**, *17*, 25. https://doi.org/https://doi.org/10.1186/s12942-018-0144-x.
111. Khatoon, A. A blockchain-based smart contract system for healthcare management. *Electronics* **2020**, *9*, 94. https://doi.org/https://doi.org/10.3390/electronics9010094.
112. Jurvetson, S. How a quantum computer could break 2048-bit RSA encryption in 8 hours. *MIT Technology Review, May* **2019**, *30*, 9. https://doi.org/https://www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/.
113. Denker, K.; Javaid, A.Y. Quantum computing as a threat to modern cryptography techniques. In Proceedings of the Proceedings of the International Conference on Foundations of Computer Science (FCS). The Steering Committee of The World Congress in Computer Science, Computer., 2019, pp. 3–8.
114. Aggarwal, D.; Brennen, G.K.; Lee, T.; Santha, M.; Tomamichel, M. Quantum attacks on Bitcoin, and how to protect against them. *arXiv preprint arXiv:1710.10377* **2017**. https://doi.org/https://doi.org/10.5195/ledger.2018.127.
115. Banerjee, S.; Mukherjee, A.; Panigrahi, P.K. Quantum blockchain using weighted hypergraph states. *Physical Review Research* **2020**, *2*, 013322. https://doi.org/https://doi.org/10.1103/PhysRevResearch.2.013322.
116. 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 Science and Technology* **2018**, *3*, 035004. https://doi.org/10.1088/2058-9565/aabc6b.

117. Alabdulatif, A. Blockchain-Based Privacy-Preserving Authentication and Access Control Model for E-Health Users. *Information* **2025**, *16*, 219. https://doi.org/https://doi.org/10.3390/info16030219.
118. 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. *Cluster Computing* **2025**, *28*, 255. https://doi.org/https://doi.org/10.1007/s10586-024-05054-6.
119. 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 Journal of Biomedical and Health Informatics* **2025**. https://doi.org/https://doi.org/10.1109/JBHI.2025.3538623.
120. Dutta, J.; Puthal, D. Advancing eHealth in society 5.0: a fuzzy logic and blockchain-enhanced framework for integrating IoMT, edge, and cloud with AI. *IEEE Access* **2024**. https://doi.org/https://doi.org/10.1109/ACCESS.2024.3520799.
121. 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. https://doi.org/https://doi.org/10.1109/ACCESS.2022.3194569.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.