Saudi Journal of Medicine and Public Health

https://saudijmph.com/index.php/pub

https://doi.org/10.64483/202412556

Blockchain for Health Assistant Audit Trails and Consent Management: A Review of Implementations and Security Trade-offs

Saad Mutlaq Alluhaydan [1], Mohammed Obaid Alshammari [1], Yousef Jazaa Obaid Alshmilan [1], Ahmed Hamoud Alshammari [1], Abdulwahab Muaybid Abdullah Alrashdi [1], Raid Safg Alshammre [1], Tariq Khalifah Alshammari [1], Abdullah Salem Al-Azmi [1], Salman Mohammed Al-bashir [1], Faisal Abdullah AlAjami [1], Ali Ahmad Mohammed Aqeeli [2], Mohammed Saleem Marzouq Alhejaili [3]

(1) Ministry of Health, Saudi Arabia,
(2) Prince Mohammed bin Nasser Hospital, Ministry of Health, Saudi Arabia,
(3) King Salman Medical City, Ministry of Health, Saudi Arabia

Abstract

Background: The rise of AI health assistants and digital tools raises concerns about data security and consent management. Traditional systems are prone to failures and provide limited transparency in data sharing. Blockchain technology offers a decentralized, immutable, and secure solution to these issues. **Aim:** This narrative review critically examines the real-world implementations and security trade-offs of blockchain technology when applied specifically to health assistant audit trails and consent management, moving beyond theoretical propositions. **Methods:** A systematic search of peer-reviewed literature (2010-2024) was conducted across Scopus, IEEE Xplore, PubMed, and ACM Digital Library. Implementation case studies, prototypes, and theoretical frameworks were analyzed to assess technical architectures, performance metrics, and security evaluations. **Results:** Findings indicate an emerging landscape where blockchain proves useful for creating secure audit logs in AI decision-making and dynamic consent models using smart contracts. However, challenges persist, including performance and scalability issues, key management complexities, data linkage risks, and conflicts between immutability and regulatory requirements such as the GDPR's "right to be forgotten." **Conclusion:** Blockchain serves as a foundational layer to improve security and transparency in health assistant ecosystems. Its future potential relies on hybrid architectures, advanced cryptographic methods such as zero-knowledge proofs, and an awareness of the new security and operational challenges that arise. It is not merely a database but a comprehensive solution for integrity and control.

Keywords: Blockchain; Health Assistant; Audit Trail; Consent Management; Data Security

Introduction

The digital health revolution has ushered in an era of AI-driven health assistants, ranging from clinical decision support tools and virtual nursing aides to patient-facing wellness chatbots and remote monitoring platforms (Topol, 2019). These systems generate, process, and act upon vast amounts of sensitive personal health information (PHI), creating profound new challenges for data security, regulatory compliance, and ethical governance (Price & Cohen, 2019). Two interrelated challenges are paramount: the need for immutable and transparent audit trails and the imperative for dynamic, granular, and revocable patient consent.

Traditional, centralized architectures for managing health data and access logs present inherent vulnerabilities. Audit logs stored within a hospital's primary database can be altered, corrupted, or deleted, either maliciously or through error, compromising non-repudiation and forensic investigations (Kuo et al., 2017). Similarly, consent models are often static, captured at a single point in time via paper or a basic digital form, failing to accommodate the fluid nature of patient preferences and the complex data-sharing networks involved in modern care and research (Saini et al., 2020). This creates an accountability and trust deficit, particularly as AI assistants make increasingly autonomous recommendations affecting patient care.

In this context, blockchain technology has emerged as a candidate for a foundational security layer. Originally conceived for cryptocurrency, blockchain is a distributed ledger technology (DLT) characterized by decentralization, cryptographic hashing, consensus-based validation, and data immutability (Yaga et al., 2019). Its core propositions—creating a single, verifiable source of truth without a central authority—appear directly applicable to the problems of auditability and consent in digital health. Proponents argue it can provide an unchangeable record of every AI inference, data access request, and consent transaction, thereby

*Corresponding author e-mail: eng-saad-m@hotmail.com (Saad Mutlaq Alluhaydan).
Receive Date: 21 December 2024, Revise Date: 30 December 2024, Accept Date: 31 December 2024

ensuring transparency and empowering patients (Elangovan et al., 2022; Ekblaw et al., 2016).

However, the application of blockchain in healthcare, particularly for the nuanced use cases surrounding health assistants, is the subject of intense debate. Critics point to significant technical hurdles, including performance limitations, storage constraints, interoperability challenges, and the introduction of novel security and privacy trade-offs (McGhin et al., 2019; Zhang et al., 2020). Many publications remain conceptual, lacking real-world validation of proposed architectures.

Therefore, this narrative review aims to move beyond theoretical promise and critically analyze the concrete implementations, practical performance, and real security trade-offs of blockchain technology when applied to audit trails and consent management for health assistant ecosystems. This review synthesizes evidence from prototypes, pilot studies, and architectural analyses to answer a central question: In the operational reality of digital health, what does blockchain concretely deliver, and at what cost? By examining these implementations through the lenses of security, scalability, and usability, this review seeks to provide a balanced, evidence-based perspective on blockchain's role in securing the next generation of health assistants.

Methodology

This narrative review employed a systematic search and selection strategy to identify and synthesize relevant literature on blockchain applications for health data security, with a specific focus on audit trails and consent management. The search was conducted in January 2024 across four major electronic databases: Scopus, IEEE Xplore, PubMed/MEDLINE, and the ACM Digital Library. The search strategy combined terms from three conceptual clusters: (1) Blockchain/DLT ("blockchain," "distributed ledger," "smart contract"); (2) Health Application ("health data," "medical record," "EHR," "health assistant," "digital health," "mHealth"); (3) Security Function ("audit trail," "consent management," "access log," "data provenance," "integrity"). Boolean operators (AND, OR) were used to combine these terms.

Inclusion criteria comprised: peer-reviewed journal articles, conference proceedings, and authoritative technical reports published in English between 2010 and 2024; studies describing a specific blockchain-based implementation, architecture, or prototype for healthcare data auditability or consent management; and studies that included an evaluation of security, performance, or trade-offs. Exclusion criteria included: purely conceptual papers without technical detail, articles focused solely on cryptocurrency or non-health applications, and duplicate publications.

Given the heterogeneity in study designs (e.g., proof-of-concept implementations, simulation studies, security analyses), a narrative synthesis approach was adopted to thematically analyze the findings, compare architectural decisions, and distill the practical and security implications reported in the literature (Wong et al., 2013; Rees et al., 2023).

Foundational Concepts: Blockchain as a Security Primitive

To appreciate blockchain's application in securing health assistant ecosystems, it is essential first to dissect its core architectural properties and their specific relevance to audit and consent challenges. Unlike traditional centralized databases governed by a single authority, blockchain operates as a distributed ledger technology (DLT) (Roodbari et al., 2022). Its foundational innovation lies in decentralizing trust across a peer-to-peer network of nodes, each of which maintains an identical copy of the ledger. This structural decentralization is coupled with consensus mechanisms—such as Proof of Work, Proof of Authority, or Practical Byzantine Fault Tolerance—which collectively validate new transactions (e.g., logging "AI Assistant X accessed Record Y at time Z") without requiring a central arbiter. Consequently, this architecture theoretically eliminates single points of control and failure, preventing any sole actor, including the host healthcare institution, from unilaterally altering historical records, thereby establishing a bedrock for transparent accountability (Khatri et al., 2023).

Two further properties are paramount: immutability and programmability. Immutability is achieved through cryptographic chaining, where validated transactions are grouped into blocks, each containing a unique digital fingerprint (hash) of the previous block (Tullo et al., 2023). Altering any piece of data within a historical block would require recalculating all subsequent hashes and simultaneously subverting the network's consensus—a computationally prohibitive feat for a well-established chain. This creates a tamper-evident and non-repudiable ledger, ideal for maintaining pristine audit trails where the integrity of the log is as critical as the data it records (Recio-Saucedo et al., 2022). Complementing this is the capability for programmability through smart contracts. These are self-executing scripts stored on the blockchain that encode and automatically enforce complex business logic. For dynamic consent management, a smart contract can function as an autonomous policy engine, executing rules such as: "IF the data requester is an approved researcher AND the patient's consent status is 'granted for research type A,' THEN release an access key. IF consent is revoked, THEN immediately invalidate the key." This transforms static legal agreements into live, code-based enforcements.

A critical design imperative in all healthcare implementations is the strategic distinction between on-chain and off-chain data storage. Storing raw, voluminous Protected Health Information (PHI)—

such as medical imagery or comprehensive AI decision logs—directly on a blockchain is generally impractical. This is due to inherent limitations in transaction throughput, storage cost, and the privacy conflict arising from replicating sensitive data across all network nodes. Therefore, the predominant and rational model is a hybrid on-chain/off-chain architecture. In this model, the blockchain serves as a high-integrity anchor, storing only cryptographic proofs and essential pointers. This on-chain layer typically includes: (1) Hashes (Digital Fingerprints), which are unique cryptographic representations of the original PHI documents or audit logs—any subsequent tampering with the off-chain data will produce a mismatched hash, proving alteration; (2) Essential Metadata and Consent Tokens, which record transactional data like actor identities, timestamps, and digital tokens representing patient consent states; and (3) the Smart Contract Code itself, which houses the governance logic. Conversely, the actual, bulky PHI and detailed operational logs reside off-chain within traditional, performant, and access-controlled systems such as secure cloud storage, InterPlanetary File System (IPFS), or institutional data lakes. The on-chain hash thus acts as an immutable seal, providing a verifiable guarantee of the integrity and authenticity of the corresponding off-chain data. This separation of concerns allows blockchain to provide its unique security guarantees without being bogged down by the scale and sensitivity of primary health data.

Implementations for Immutable Audit Trails

The application of blockchain to create verifiable audit logs for health assistant activities has seen several concrete implementations, focusing primarily on data access provenance and AI decision traceability.

Several pilots have demonstrated the use of blockchain to log every access to patient records. For instance, MedRec (Azaria et al., 2016), a seminal prototype, used a blockchain to manage authentication and record data access events across different EHR systems, providing patients with a transparent log of who viewed their data. In the context of health assistants, similar architectures have been proposed where an AI module's query to a patient record triggers a blockchain transaction. This transaction logs the assistant’s ID (a pseudonymous public key), the patient record ID (hashed), the timestamp, and the purpose of access (e.g., "routine risk assessment") (Xia et al., 2017). Implementations like FHIRChain (Zhang et al., 2018) built upon this by integrating with the Fast Healthcare Interoperability Resources (FHIR) standard, using smart contracts to log and govern data exchange events in a standardized way. These systems shift the trust model: instead of relying on an institution’s internal log, a patient or auditor can verify the complete access history against the immutable blockchain (Zhang et al., 2023).

A more advanced application is auditing the behavior of AI health assistants themselves. This involves logging not just data access, but the AI’s inferences, the model version used, and the input data fingerprints. A proof-of-concept by Mamoshina et al. (2018) illustrated logging AI-powered analysis of genomic data to a blockchain, ensuring the results were traceable and reproducible. In clinical decision support, a blockchain can record a hash of the input vitals, the AI model’s identifier and version, and the resulting recommendation (e.g., "flag for sepsis risk") (Kuo & Ohno-Machado, 2018). This creates an immutable chain of causality, crucial for debugging algorithmic errors, investigating adverse events, and meeting regulatory requirements for explainability in AI (Zhu et al., 2022). Furthermore, smart contracts can enforce governance by only allowing certified, hashed model versions to be used in production, logging any updates or retraining events on-chain (Table 1). Figure 1 illustrates a hybrid on-chain/off-chain architecture for securing audit trails in AI-driven health assistants.

Table 1: Blockchain Implementation Models for Health Assistant Security

Model	On-Chain Data	Off-Chain Data	Primary Security Benefit	Exemplar Implementation/Concept
Access Provenance Ledger	Hashes of PHI, access event metadata (requester ID, timestamp, action).	Full PHI in secure databases/cloud.	Tamper-evident log of all data touches; prevents insider threat cover-ups.	MedRec (Azaria et al., 2016), FHIRChain (Zhang et al., 2018)
AI Audit Trail	Hashes of input data, AI model version ID, hash of output/recommendation.	Raw clinical data, full AI model binaries.	Ensures reproducibility & traceability of AI decisions; enables algorithmic accountability.	Mamoshina et al. (2018), Kuo & Ohno-Machado (2018)
Dynamic Consent Manager	Smart contract code, consent state	Detailed consent forms, research protocols.	Patient-centric, fine-grained, machine-	MeDShare (Xia et al., 2017), Patient-Centric Consent (Saini et al., 2020)

	(granted/revoked), patient & provider public keys.		enforceable consent; automatic revocation.	
Hybrid Integrity Anchor	Periodic "checkpoint" hashes of aggregated logs or database states.	Complete system databases and transaction logs.	Provides efficient integrity verification for bulk systems without logging every micro-transaction on-chain.	Various enterprise DLT platforms (e.g., Hyperledger Fabric applications).

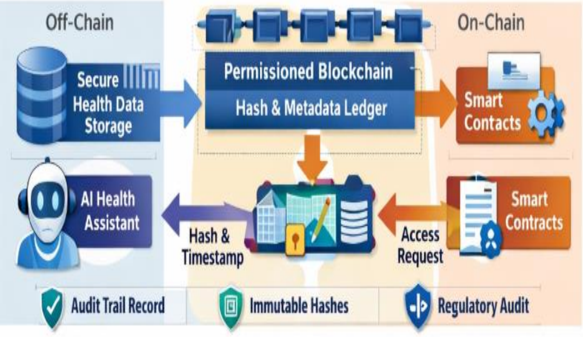

Figure 1. Blockchain-Enabled Architecture for Health Assistant Audit Trails

Implementations for Dynamic Consent Management

Blockchain and smart contracts offer a paradigm shift from static consent forms to dynamic, patient-controlled consent ecosystems.

The core innovation is encoding consent directives into smart contracts. A patient, via a user-friendly dApp (decentralized application), can set parameters such as: "My data from cardiology can be used by AI research project Alpha for 6 months," or "My virtual nursing assistant may share my medication adherence data with my primary care physician, but not with my insurer." These preferences are written into a smart contract deployed on the blockchain (Sharma et al., 2023). When a health assistant or researcher requests data, their application must interact with this smart contract. The contract automatically checks the request against the current consent rules. If valid, it can trigger an action, such as releasing a decryption key to a specific data enclave or returning a "permission granted" token. MeDShare (Marichamy & Natarajan et al., 2023) demonstrated this for data sharing between institutions, while later systems have focused on direct patient control (Jagtap et al., 2021).

Smart contracts enable unprecedented granularity. Consent can be tied to specific data attributes (e.g., lab results but not notes), purposes (research vs. quality improvement), time windows, and specific entities. Most importantly, revocation is immediate and globally enforced. A patient can update their consent status through the dApp, which sends a transaction to update the smart contract state. The next time any entity queries the contract, it will reflect the new, revoked permissions, automatically denying access. This solves a major flaw in traditional systems where revocation is a manual, error-prone process across disparate databases. Figure 2 depicts a patient-centric consent management workflow using blockchain smart contracts.

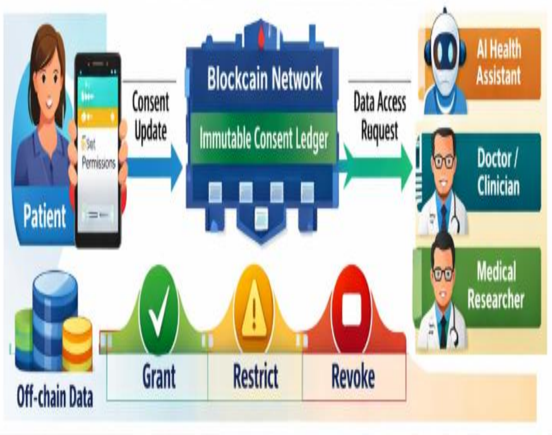

Figure 2. Smart Contract–Based Dynamic Consent Management in Health Assistant Ecosystems

Critical Analysis of Security and Operational Trade-offs

While the architectural benefits are clear, implementations reveal significant trade-offs that temper enthusiasm and dictate practical design choices.

Public blockchains like Ethereum suffer from low transaction throughput (tens per second) and high latency (minutes for confirmation), making them unsuitable for high-frequency health assistant interactions (McGhin et al., 2019). While permissioned/private blockchains (e.g., Hyperledger Fabric, Corda) offer higher performance by restricting validator nodes, they reintroduce a degree of centralization, arguably diluting the core trust model (Vukolić, 2015). Every on-chain transaction (consent change, audit log entry) also carries a cost ("gas fee" in Ethereum) or requires dedicated infrastructure, creating an ongoing operational expense. Storing even hashes on-chain for millions of patients and billions of micro-interactions presents a non-trivial scalability challenge (Ramzan et al., 2022).

Immutability conflicts with privacy regulations like the EU's General Data Protection Regulation (GDPR), which includes a "right to erasure" (Article 17). Data cannot be truly erased from an immutable ledger (Saeed et al., 2022). Mitigations include storing only hashes of consent *states* (not the form content) or using chameleon hashes that allow authorized "edits," but these complicate the design. Furthermore, if public keys are used as persistent identifiers for patients and assistants, sophisticated analysis of the blockchain's public metadata could deanonymize participants and reveal sensitive relationship patterns (e.g., which patients are seeing a specific oncologist's AI tool) (Almashaqbeh & Solomon, 2020).

Blockchain security is predicated on the protection of private cryptographic keys. If a patient loses the private key to their consent management wallet, they lose irrevocable control over their data—a catastrophic user experience. Conversely, if a health institution's key for its AI assistant is compromised, an attacker could illegitimately generate "valid" audit trails (Kuo et al., 2017). Robust, user-friendly, and recoverable key management systems are a critical unsolved challenge at scale.

Integrating blockchain layers with legacy EHRs, health assistant APIs, and identity management systems is a massive interoperability hurdle. The legal status of a blockchain-based consent smart contract as binding medical consent is still largely untested in most jurisdictions (Gordon & Catalini, 2018). Regulators like the FDA and EMA are still developing frameworks for evaluating these decentralized, algorithmically enforced systems (Table 2).

Table 2: Security Trade-offs of Blockchain in Health Assistant Applications

Promised Security Benefit	Associated Trade-off or New Risk	Mitigation Strategies
Immutability of Audit Logs	Conflicts with "Right to Erasure" (GDPR); storage of incorrect/malicious data is permanent.	Store only hashes; use privacy-aware consensus; employ mutable layers with on-chain integrity proofs (chameleon hashes).
Decentralization & Trust Minimization	Performance bottlenecks (low TPS, high latency); increased system complexity.	Use permissioned/private DLTs; employ hybrid/off-chain architectures; leverage layer-2 scaling solutions.
Transparent Provenance	Metadata on-chain can lead to patient/entity deanonymization through pattern analysis.	Use zero-knowledge proofs (ZKPs) for validation; employ mixing services; limit metadata granularity.
Cryptographic Integrity	Irrecoverable loss of private keys equals total loss of data control/identity.	Hierarchical deterministic (HD) wallets; social recovery mechanisms; secure hardware modules (HSMs).
Automated Enforcement via Smart Contracts	Bugs in contract code are immutable and can lead to irreversible, systematic policy failures (e.g., The DAO hack).	Extensive formal verification of contracts; use upgradeability patterns cautiously; implement multi-signature governance for critical functions.

Future Directions and Hybrid Solutions

The future of blockchain in health assistant security likely lies not in monolithic platforms but in purpose-built, hybrid architectures that leverage its strengths while mitigating weaknesses.

Zero-Knowledge Proofs (ZKPs) and Homomorphic Encryption

ZKPs allow one party to prove to another that a statement is true without revealing any underlying information (e.g., prove an AI assistant is certified without revealing its vendor, or prove a patient is over 18 without revealing their birthdate). Integrating ZKPs (e.g., zk-SNARKs) can dramatically enhance privacy while maintaining verifiability (Bernabe et al., 2019). Homomorphic encryption, which allows computation on encrypted data, could enable health assistants to analyze data that remains encrypted both off-chain and during processing, with only the result (or a hash of it) being logged to the blockchain.

Interoperability Frameworks and Standards

For blockchain to be viable, it must function as a lightweight interoperability and trust layer between existing systems. Efforts like the HL7 FHIR Blockchain Workgroup and the IEEE Standard for Blockchain in Healthcare are crucial to ensure different implementations can communicate and that core healthcare data standards are preserved (Zhang et al., 2018; Kumar et al., 2018).

The "Blockchain as a Security Sensor" Model

A pragmatic future model treats the blockchain not as the primary data store, nor even as the log for every event, but as a high-integrity "sensor" or "notary." Critical, high-value events—a major consent change, a formal deployment of a new AI model, a weekly integrity checksum of the primary audit database—are immutably recorded. This provides a trusted root of truth against which the performance and integrity of higher-throughput, more mutable operational systems can be periodically verified and audited.

Conclusion

This review confirms that blockchain technology presents a compelling and architecturally novel approach to addressing the twin challenges of auditability and dynamic consent in health assistant ecosystems. Concrete implementations demonstrate its viability for creating tamper-evident logs of data access and AI decisions, and for encoding patient consent into self-enforcing smart contracts. These applications move beyond theoretical promise, offering a technical pathway toward greater transparency, patient agency, and system integrity.

However, the analysis of these implementations reveals that the adoption of blockchain introduces a complex set of security and operational trade-offs. The immutability that guarantees audit integrity conflicts with data erasure mandates. The decentralization that eliminates central points of failure brings performance and scalability limits. The cryptographic model shifts the risk to key management. In essence, blockchain does not eliminate security problems; it transforms them into different, often more subtle, challenges.

Therefore, the ultimate utility of blockchain is not as a panacea or a replacement for existing health IT infrastructure. Its value is as a strategic security primitive—a foundational layer for verifiable integrity and controlled access in a hybrid architectural model. Future progress depends on the maturation of complementary technologies like zero-knowledge proofs, the development of clear regulatory and interoperability standards, and a sober, use-case-driven evaluation where blockchain is applied selectively to problems where its unique properties of decentralized trust and cryptographic assurance are genuinely required. For health assistants to be both intelligent and trustworthy, the security layer beneath them must be not only strong but also transparent and accountable; blockchain, with all its trade-offs, offers a pioneering path toward that goal.

References

1. Almashaqbeh, G., & Solomon, R. (2022, June). Sok: Privacy-preserving computing in the blockchain era. In *2022 IEEE 7th European Symposium on Security and Privacy (EuroS&P)* (pp. 124-139). IEEE. https://doi.org/10.1109/EuroSP53844.2022.00016
2. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016, August). Medrec: Using blockchain for medical data access and permission management. In *2016 2nd international conference on open and big data (OBD)* (pp. 25-30). IEEE. https://doi.org/10.1109/OBD.2016.11
3. Bernabe, J. B., Canovas, J. L., Hernandez-Ramos, J. L., Moreno, R. T., & Skarmeta, A. (2019). Privacy-preserving solutions for blockchain: Review and challenges. *Ieee Access*, *7*, 164908-164940. https://doi.org/10.1109/ACCESS.2019.2950872
4. Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016, August). A Case Study for Blockchain in Healthcare:“MedRec” prototype for electronic health records and medical research data. In *Proceedings of IEEE open & big data conference* (Vol. 13, No. 13).
5. Elangovan, D., Long, C. S., Bakrin, F. S., Tan, C. S., Goh, K. W., Yeoh, S. F., ... & Ming, L. C. (2022). The use of blockchain technology in the health care sector: systematic review. *JMIR medical informatics*, *10*(1), e17278. https://doi.org/10.2196/17278
6. Gordon, W. J., & Catalini, C. (2018). Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. *Computational and structural biotechnology journal*, *16*, 224-230. https://doi.org/10.1016/j.csbj.2018.06.003
7. Jagtap, S. T., Thakar, C. M., Phasinam, K., Garg, S., & Ventayen, R. J. M. (2021, August). A framework for secure healthcare system using blockchain and smart contracts. In *2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC)* (pp. 922-926). IEEE. https://doi.org/10.1109/ICESC51422.2021.9532644
8. Khatri, R. B., Erku, D., Endalamaw, A., Wolka, E., Nigatu, F., Zewdie, A., & Assefa, Y. (2023). Multisectoral actions in primary health care: A realist synthesis of scoping review. *Plos one*, *18*(8), e0289816. https://doi.org/10.1371/journal.pone.0289816
9. Kumar, T., Ramani, V., Ahmad, I., Braeken, A., Harjula, E., & Ylianttila, M. (2018, September). Blockchain utilization in healthcare: Key requirements and challenges. In *2018 IEEE 20th International conference on e-health networking, applications and services (Healthcom)* (pp. 1-7). IEEE. https://doi.org/10.1109/HealthCom.2018.8531136
10. Kuo, T. T., & Ohno-Machado, L. (2018). Modelchain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks. *arXiv preprint arXiv:1802.01746*. https://doi.org/10.48550/arXiv.1802.01746
11. Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, *24*(6), 1211-1220. https://doi.org/10.1093/jamia/ocx068
12. Mamoshina, P., Ojomoko, L., Yanovich, Y., Ostrovski, A., Botezatu, A., Prikhodko, P., ... &

Zhavoronkov, A. (2018). *Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. Oncotarget 9: 5665–5690.*

13. Marichamy, V. S., & Natarajan, V. (2023). Blockchain based securing medical records in big data analytics. *Data & Knowledge Engineering*, *144*, 102122. https://doi.org/10.1016/j.datak.2022.102122
14. McGhin, T., Choo, K. K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of network and computer applications*, *135*, 62-75. https://doi.org/10.1016/j.jnca.2019.02.027
15. Price, W. N., & Cohen, I. G. (2019). Privacy in the age of medical big data. *Nature medicine*, *25*(1), 37-43. https://doi.org/10.1038/s41591-018-0272-7
16. Ramzan, S., Aqdus, A., Ravi, V., Koundal, D., Amin, R., & Al Ghamdi, M. A. (2022). Healthcare applications using blockchain technology: Motivations and challenges. *IEEE Transactions on Engineering Management*, *70*(8), 2874-2890. https://doi.org/10.1109/TEM.2022.3189734
17. Recio-Saucedo, A., Crane, K., Meadmore, K., Fackrell, K., Church, H., Fraser, S., & Blatch-Jones, A. (2022). What works for peer review and decision-making in research funding: a realist synthesis. *Research integrity and peer review*, *7*(1), 2. https://doi.org/10.1186/s41073-022-00120-2
18. Rees, C. E., Crampton, P. E., Nguyenand, V. N., & Monrouxe, L. V. (2023). Introducing realist approaches in health professions education research. *Foundations of health professions education research: Principles, perspectives and practices*, 102-121. https://doi.org/10.1002/9781394322213.ch6
19. Roodbari, H., Axtell, C., Nielsen, K., & Sorensen, G. (2022). Organisational interventions to improve employees' health and wellbeing: A realist synthesis. *Applied Psychology*, *71*(3), 1058-1081. https://doi.org/10.1111/apps.12346
20. Saeed, H., Malik, H., Bashir, U., Ahmad, A., Riaz, S., Ilyas, M., ... & Khan, M. I. A. (2022). Blockchain technology in healthcare: A systematic review. *Plos one*, *17*(4), e0266462. https://doi.org/10.1371/journal.pone.0266462
21. Saini, A., Zhu, Q., Singh, N., Xiang, Y., Gao, L., & Zhang, Y. (2020). A smart-contract-based access control framework for cloud smart healthcare system. *IEEE Internet of Things Journal*, *8*(7), 5914-5925. https://doi.org/10.1109/JIOT.2020.3032997
22. Sharma, U., Ganapathi, A., Singh, A., & Singh, K. K. (2023). Blockchain in Healthcare: Use Cases. *Blockchain and Deep Learning for Smart Healthcare*, 147-169. https://doi.org/10.1002/9781119792406.ch7
23. Topol, E. J. (2019). High-performance medicine: the convergence of human and artificial intelligence. *Nature medicine*, *25*(1), 44-56. https://doi.org/10.1038/s41591-018-0300-7
24. Tullo, E., Wakeling, L., Pearse, R., Khoo, T. K., & Teodorczuk, A. (2023). Lost in translation: how can education about dementia be effectively integrated into medical school contexts? A realist synthesis. *BMJ open*, *13*(11), e077028. https://doi.org/10.1136/bmjopen-2023-077028
25. Vukolić, M. (2015, October). The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In *International workshop on open problems in network security* (pp. 112-125). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-39028-4_9
26. Wong, G., Greenhalgh, T., Westhorp, G., Buckingham, J., & Pawson, R. (2013). RAMESES publication standards: realist syntheses. *BMC medicine*, *11*(1), 21. https://doi.org/10.1186/1741-7015-11-21
27. Xia, Q., Sifah, E. B., Smahi, A., Amofa, S., & Zhang, X. (2017). BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. *Information*, *8*(2), 44. https://doi.org/10.3390/info8020044
28. Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. *arXiv preprint arXiv:1906.11078*. https://doi.org/10.6028/NIST.IR.8202
29. Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: applying blockchain to securely and scalably share clinical data. *Computational and structural biotechnology journal*, *16*, 267-278. https://doi.org/10.1016/j.csbj.2018.07.004
30. Zhang, P., Kelley, A., Schmidt, D. C., & White, J. (2023). Design pattern recommendations for building decentralized healthcare applications. *Frontiers in Blockchain*, *6*, 1006058. https://doi.org/10.3389/fbloc.2023.1006058

Zhu, S., Gilbert, M., Chetty, I., & Siddiqui, F. (2022). The 2021 landscape of FDA-approved artificial intelligence/machine learning-enabled medical devices: an analysis of the characteristics and intended use. *International journal of medical informatics*, *165*, 104828. https://doi.org/10.1016/j.ijmedinf.2022.104828

.