EURASIAN EXPERIMENT JOURNAL OF PUBLIC HEALTH (EEJPH)

ISSN: 2992-4081 ©EEJPH Publications

Volume 7 Issue 2 2025

Blockchain in Health Records: Enhancing Security and Privacy

Nyakairu Doreen G.

Faculty of Science and Technology Kampala International University Uganda

ABSTRACT

The rapid digitization of healthcare has introduced significant challenges in maintaining the security and privacy of electronic health records (EHRs). Blockchain technology offers a promising solution to these issues through its decentralized, immutable, and transparent data storage capabilities. This paper explores the integration of blockchain into healthcare to address the vulnerabilities of current health record systems. It highlights the fundamental principles of blockchain, its advantages in ensuring data integrity, and the ability to enhance patient trust through secure access control. The study also examines implementation strategies, case studies, and regulatory considerations while addressing potential barriers and future trends. The findings suggest that blockchain technology has the potential to revolutionize health records management, improve interoperability, and establish a secure, patient-centric healthcare ecosystem.

Keywords: Blockchain, electronic health records (EHR), healthcare security, data privacy, decentralized systems, health informatics.

INTRODUCTION

Blockchain is a revolutionary technology for distributed databases. In a blockchain system, data is stored in the format of blocks, which are linked in the form of a chain. Unique copies of these chains are called a ledger. The users in a blockchain network are called nodes, and these nodes maintain a copy of the ledger. The updates of the blockchain data among the users are achieved through cryptographic security. This arrangement ensures decentralization of the data, which is one of the important concepts of a blockchain system. This feature plays a major role in advantages like enhanced security and transparency to the data, which is lacking in traditional database management systems. Blockchain provides a new opportunity for application development in fields involving sensitive data, such as finance and healthcare. The potential applications of blockchain are enormous. Key reasons for a high level of enthusiasm include the development of new cryptocurrencies and their investors' community, as well as the integration of health record data with blockchain technology to overcome the problems related to health services. The objective of a health record management system is not only to maintain a centralized record of a person but also to ensure the security and longitudinal sanctity of the data stored in the system. Thus, the health record system should be secured from both intrusion attacks and privacy issues. Blockchain technology-based systems have the potential to overcome these types of problems [1, 2].

Definition and Key Concepts

Blockchain is a word to describe digital systems, initially documented with accounting ledger practices. When transferred to digital, it represents a distributed ledger. The distributed ledger processes provide all participants with information about each transaction executed and stored in a block within a data channel that is very secure and cannot be changed. The fundamental design of blockchains, where data is aggregated into a block, verified via a consensus mechanism, and written into a public ledger, ensures integrity and immutability. Transactions written into a block become part of a true chain, unbreakable in

terms of its potential to be edited or manipulated by outside parties. Therefore, it is deemed that the blockchain is tamper-evident. Beyond cryptocurrencies, blockchains have been applied to many fields, including identity, supply chain, voting, healthcare records, and many more [3, 4]. The ongoing digitization in healthcare records and health delivery systems is complemented by the research on embedding blockchain within health administration and the healthcare delivery domain. As yet, there is no established definition of blockchain technology. Equally, the constituent components of blockchain systems, including those of distributed and decentralized networks, smart contracts, and consensus mechanisms, are not standardized and are perhaps too ethereal to have any practical effect. In the health sector, several organizations have explored the construction of blockchain systems, and many have published white papers. A common development, emerging from these conceptual designs, is the adaptation of these structurally diffused and solid databases to those structures particularly useful in health regime records [5, 6].

Fundamental Principles

The mainstay of blockchain's functionality is decentralization. Unlike centralized systems where a single party has control, blockchain creates a decentralized set of digital records that are linked together to create a chain. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. Any modification of the block's content will impact the hash, thus breaking the integrity of the entire chain. This fundamental design feature allows blockchain applications to eliminate the need for an intermediary trust broker since users can trust the system even when they do not trust each other. Indeed, in a blockchain platform, no single party has control of the data or information. Therefore, a user or organization cannot manipulate the data to their advantage, guaranteeing much higher levels of security and trust [7, 8]. Furthermore, consensus algorithms underpin blockchain platforms, ensuring that no single entity controls the outcome and verification process. Thus, endorsements and transactions are verified between all the participating nodes within the network. Blockchain transactions are validated by each node using cryptographic techniques before being aggregated and added permanently to the ledger. These cryptographic techniques secure the integrity of the data on the ledger and can be used for authentication while providing a mechanism for users to interact without relying on a central authority. Healthcare environments require fundamentally secure systems, as the impact of sensitive patient data being breached can have severe consequences for both the patient and the clinic or hospital. Security, transparency, and traceability offered by blockchain networks can provide considerable rewards for platforms seeking to streamline the healthcare process while respecting privacy and allowing patient control over who sees their data while preventing fraud [9, 10].

Challenges in Health Records Security and Privacy

In general, security and privacy are two major concerns in health record management, particularly with the increasing adoption of digital media. The total number of patient records that were affected due to data breaches doubled in 2019 compared to 2018, causing more than two-thirds of the affected patients to suffer because of medical identity theft. Data breaches can occur due to the lack of basic security hygiene, and cold-boot attacks can expose patient data to attackers for a long time, further deepening the threats of electronic health records (EHRs). Unauthorized access to EHRs can lead not only to misuse of the patient's information but also to potential fraud, causing the patient to be incorrectly billed for healthcare services not received. EHRs can be divided into various isolated or disparate health information systems, causing an increased threat of hacking, leading to service availability issues along with data breaches [11, 12]. HIPAA is one of the most well-known healthcare information privacy regulations; it sets forth different rules to regulate the issuance and enforcement of various security standards to protect EHRs and to ensure only authorized access. Organizations must comply with technical security services and physical safeguards to fully follow the HIPAA Security Rule. The fast development of technologies and cybersecurity paradigms, such as cloud computing and AI, poses challenges to HIPAA regulations for smaller healthcare organizations and agencies in terms of compliance. In general, the owner of the data determines the allocation and use of electronic patient data. The explicit consent of the patient is required in many cases for the usage and publication of electronic health information. The use of software to limit access to electronic health data only to authorized personnel can partially contribute to the security and privacy guidelines. As the use of selective encryption is often inefficient due to semantic security guarantees, quantum-proof selective encryption can be an efficient alternative to contribute to the security of electronic health data. Providing a solution for the security and privacy of the patient's data in

the health records, we aim to improve the trust and integrity of the EHR information and protect its confidentiality, including minimizing the cost of implementing specific security measures [13, 14].

Benefits of Utilizing Blockchain in Health Records

Blockchain can provide several valuable benefits to health records, making them more reliable and secure. Records stored on a blockchain are time-stamped with a unique cryptographic signature that makes them immune to modification or deletion. This means that once a health record is created, it cannot be retroactively altered without the consent of the entity that created it—the patient. This immutable data can be very useful and valuable for healthcare providers to build patient trust and privacy around aspects of their care. Records of visits, treatments, and tests can be captured permanently and transparently, which can help to avoid incomplete records, questions of trust, or concerns regarding inadequate documentation of patient history. The way transactions are recorded on the blockchain makes it an attractive option for health record management. The system can eliminate the need for intermediaries and expensive conversion processes, since transactions are available in near-real time, reducing the time and effort involved in audits of health records. Blockchain also presents a promising solution in reconciling differences in format for health records between different healthcare providers and across different countries, since the standard bytes transferred to hash functions for transactions allow for easy translation of the format to the viewer application. This potential to standardize data and improve interoperability can improve healthcare quality through digitally enabled patient care pathways, connecting people, services, and data to support patients in having more predictive, personalized, and responsive care. Lastly, patients can directly control and securely grant access to their health data to providers, insurers, and researchers, if and when they choose to do so [15, 16].

Implementation Strategies and Case Studies

There are several methodologies for implementing blockchain technology in healthcare to develop a secure and efficient electronic health records management system. Researchers and practitioners proposed a methodology that includes implementation, operational, and functional aspects for validating the successful deployment of a blockchain-based health records management system in healthcare settings. Based on a compiled vision of blockchain technology and novel approaches for the research community, an updated methodology to deploy the blockchain is proposed by parallelizing the steps. Such an implementation protocol is proposed with parallel steps; this allows supervisors or practitioners to quickly assess the feasibility of the new blockchain in the healthcare settings of software applications. To further enhance the quality of their solutions, many researchers used real case studies to which blockchain technology was applied. By drawing the lessons learned from the case study, this paper identifies best practices and developments for the integration of blockchain in electronic health records in a technological and operational context. Both studies illustrate the importance of collaborating with stakeholders to guarantee high deployment, in addition to technical factors. The analysis in these studies can be used as a guide to upcoming practices that will leverage blockchain's key characteristics and realize its advantages [6, 17].

Regulatory Considerations and Future Trends

Existing regulations could potentially restrict the application of blockchain technology in health records. With the need to comply with privacy laws, applications and companies that want to utilize blockchain in health records should clearly show how they are being compliant with the existing laws and data protection regulations. As we move forward, there is a need for proper guidance regarding the obfuscation of sensitive information contained in health records and an inducement to automatically delete stale records according to privacy laws in addition to the defined security features. Moreover, given that blockchain technology has unique challenges compared to other software due to its decentralized, semi-trusted trust model, a specific set of regulations might be needed for the underlying blockchain technology that powers institutions and companies [3, 18]. The adoption of blockchain technology in healthcare is expected to increase severalfold in the coming years. The frontiers of technology and patient care are expanding, and there is certainly a future for blockchain and healthcare. Throughout history, innovation has continued to shape the methods, materials, and beliefs associated with medical treatment on every level. In society, medical technology has advanced by leaps and bounds, entering territories that help not only those who are critically ill but also those who consume medical services in a theoretical way. Only time will tell. Personal views and ideological influences need to be translated as evidence before we expose the vulnerable data of patients transacting blockchain technology. The regulations take time to catch up with the technology. It may take years, or even government if the necessary steps are not taken

now. So, all stakeholders need to be aware and proactive in discussing such issues. Further pilot and testing phases are necessary to bring the blockchain to market. Crucial discussions are yet to be held not only about technology but also about ethics and rights. This roadmap could provide a starting point for discussion and pave the way for further research in this space [19, 20].

CONCLUSION

Blockchain technology offers an innovative approach to addressing the critical challenges of security, privacy, and interoperability in electronic health records. By decentralizing data storage, leveraging cryptographic techniques, and ensuring tamper-evident records, blockchain provides unparalleled levels of trust and transparency. The ability for patients to control access to their data while maintaining its integrity can transform the healthcare landscape, enabling a more secure and patient-focused system. However, significant regulatory, technical, and ethical considerations must be addressed before blockchain can achieve widespread adoption. Collaborative efforts among stakeholders, including healthcare providers, policymakers, and technology developers, are essential to overcome these challenges. Pilot studies and real-world applications demonstrate the potential of blockchain to improve healthcare delivery, but continuous research, testing, and refinement will be necessary to unlock its full capabilities. Blockchain's promise in healthcare is immense, but realizing its potential will require careful planning, robust governance, and proactive engagement with emerging challenges.

REFERENCES

1. Wenhua Z, Qamar F, Abdali TA, Hassan R, Jafri ST, Nguyen QN. Blockchain technology: security issues, healthcare applications, challenges and future trends. Electronics. 2023 Jan 20;12(3):546. mdpi.com
2. Qahtan S, Yatim K, Zulzalil H, Osman MH, Zaidan AA, Alsattar HA. Review of healthcare industry 4.0 application-based blockchain in terms of security and privacy development attributes: Comprehensive taxonomy, open issues and challenges and recommended solution. Journal of Network and Computer Applications. 2023 Jan 1;209:103529. [HTML]
3. Ghosh PK, Chakraborty A, Hasan M, Rashid K, Siddique AH. Blockchain application in healthcare systems: a review. Systems. 2023 Jan 8;11(1):38. mdpi.com
4. Odeh A, Keshta I, Al-Haija QA. Analysis of blockchain in the healthcare sector: application and issues. Symmetry. 2022 Aug 23;14(9):1760.
5. Govindan K, Nasr AK, Saeed Heidary M, Nosrati-Abarghooee S, Mina H. Prioritizing adoption barriers of platforms based on blockchain technology from balanced scorecard perspectives in healthcare industry: A structural approach. International Journal of Production Research. 2023 Jun 3;61(11):3512-26. [HTML]
6. Attaran M. Blockchain technology in healthcare: Challenges and opportunities. International Journal of Healthcare Management. 2022 Jan 2;15(1):70-83.
7. Zutshi A, Grilo A, Nodehi T. The value proposition of blockchain technologies and its impact on Digital Platforms. Computers & industrial engineering. 2021. [HTML]
8. Henninger A, Mashatan A. Distributed interoperable records: The key to better supply chain management. Computers. 2021 Jul 19;10(7):89.
9. Sivan R, Zukarnain ZA. Security and privacy in cloud-based e-health system. Symmetry. 2021 Apr 23;13(5):742.
10. Singh PD, Dhiman G, Sharma R. Internet of things for sustaining a smart and secure healthcare system. Sustainable computing: informatics and systems. 2022 Jan 1;33:100622. [HTML]
11. Shrivastava U, Song J, Han BT, Dietzman D. Do data security measures, privacy regulations, and communication standards impact the interoperability of patient health information? A cross-country investigation. International Journal of Medical Informatics. 2021 Apr 1;148:104401. [HTML]
12. Yeo LH, Banfield J. Human factors in electronic health records cybersecurity breach: an exploratory analysis. Perspectives in health information management. 2022;19(Spring). nih.gov
13. Szalados JE. Medical Records and Confidentiality: Evolving Liability Issues Inherent in the Electronic Health Record, HIPAA, and Cybersecurity. The Medical-Legal Aspects of Acute Care Medicine: A Resource for Clinicians, Administrators, and Risk Managers. 2021:315-42. [HTML]
14. Abbasi N, Smith DA. Cybersecurity in Healthcare: Securing Patient Health Information (PHI), HIPPA compliance framework and the responsibilities of healthcare providers. Journal of

Knowledge Learning and Science Technology ISSN: 2959-6386 (online). 2024 Sep 25;3(3):278-87. jklst.org

15. Meng L, Chen L. Analysis of client-side security for long-term time-stamping services. InInternational Conference on Applied Cryptography and Network Security 2021 Jun 9 (pp. 28-49). Cham: Springer International Publishing.
16. Majumder S, Zaha R, Manik MM, Alam KM. A Blockchain Based Scalable Framework for Academic Document Verification. In2023 26th International Conference on Computer and Information Technology (ICCIT) 2023 Dec 13 (pp. 1-6). IEEE.
17. Alzahrani S, Daim T, Choo KK. Assessment of the blockchain technology adoption for the management of the electronic health record systems. IEEE Transactions on Engineering Management. 2022 Apr 26;70(8):2846-63. pdx.edu
18. Reegu FA, Abas H, Gulzar Y, Xin Q, Alwan AA, Jabbari A, Sonkamble RG, Dziyauddin RA. Blockchain-based framework for interoperable electronic health records for an improved healthcare system. Sustainability. 2023 Apr 7;15(8):6337. mdpi.com
19. Habib G, Sharma S, Ibrahim S, Ahmad I, Qureshi S, Ishfaq M. Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing. Future Internet. 2022 Nov 21;14(11):341. mdpi.com
20. Li K, Liang C. Exploring the promotion of blockchain adoption in the healthcare industry through government subsidies. Kybernetes. 2024 Dec 9;53(12):5721-39.

CITE AS: Nyakairu Doreen G. (2024). Blockchain in Health Records: Enhancing Security and Privacy. EURASIAN EXPERIMENT JOURNAL OF PUBLIC HEALTH, 7(2):40-44.