Research Output Journal of Public Health and Medicine 4(2):12-17, 2024

ROJPHM

ISSN ONLINE: 1115-9715
ISSN PRINT: 1115-6147

https://rojournals.org/roj-public-health-and-medicine/

https://doi.org/10.59298/ROJPHM/2024/421217

Blockchain in Healthcare: Ensuring Data Security and Integrity

Tukamuhebwa Richard

School of Engineering and Applied Science Kampala International University Uganda
Email: tukamuhebwa@kiu.ac.ug

ABSTRACT

The healthcare industry faces significant challenges in safeguarding data security and integrity, particularly with the rise of digital health systems and the sensitive nature of patient information. Blockchain technology offers a decentralized, immutable, and secure solution to address these issues, allowing healthcare organizations to protect and manage patient data effectively. This paper examines how blockchain can enhance data security and integrity within healthcare by examining its key features, such as immutability, transparency, and decentralized access, which collectively provide a robust framework for secure data management. The potential applications of blockchain in healthcare, including patient consent management, access control through smart contracts, and data-sharing solutions, are analyzed alongside challenges such as regulatory compliance, cost, and interoperability. By integrating blockchain, healthcare systems can achieve improved data security, fostering trust and resilience in patient data management. This paper concludes with case studies and discusses future trends in blockchain implementation within healthcare, underscoring its transformative potential for securing data while addressing privacy and ethical concerns.

Keywords: Blockchain, healthcare, data security, data integrity, patient data management, smart contracts.

INTRODUCTION

Blockchain is one of the fascinating technological innovations changing the way many industries operate. Although the concept of blockchain might be difficult to understand, it has some revolutionary aspects that make it different from traditional ledger systems. A blockchain is a continuously growing targeted list of records, secured and linked using cryptography. The blockchain is inherently resistant to modification of the data. All blockchains are decentralized and distributed across technology networks from peer to peer. This makes it extremely difficult to change or hack into the system. The blockchain has given a new perspective on the transparency and security present in the whole system, which is still missing in the healthcare industry [1, 2]. This is to why blockchain matters the most in the healthcare industry because data security and integrity are required at a high level. With various functions of blockchain in the healthcare industry, it is also getting into a number of discussions in Information Technology (IT) and healthcare domains. Blockchain in healthcare can create value and can be used to unlock new opportunities for the industry. Various concepts such as blockchain, smart contracts, Hyperledger, and Ethereum are briefly explained in this chapter [3, 4]. Blockchain: A chain of blocks in cryptography can be termed a blockchain, where each block has an arrangement of digital information and keeps records of transactions in a way that is made to be secure and transparent. A transaction is signed by the sender using a private key, which can be verified by a public key. Blockchain can be used as a distributed ledger that helps to minimize the overhead and cost of the ledger compared to the

traditional financial industry ledger. A blockchain is a data structure that is used to create a digital transaction. A blockchain is a sequence of blocks of a digital file, where each block contains a timestamp and a link to the previous block. The blockchain concept is not only restricted to Bitcoin but has been implemented across various industries. A blockchain is a distributed system that has a continuously growing database, where each record is connected with the other. It ensures that the held record is preserved from being forged or tampered with. Every block in the outward ring contains a cryptographic hash of the inner block, a timestamp, and transaction data. In the case of the inner block, it prevents the data from being manipulated once approved by the system. Blockchain removes the reliance on any one entity to approve the transactions. Once verified by the network, the transaction cannot be reversed. Tokens in the blockchain ledger system are transferred through a process called mining. Blockchain eliminates the middleman in a transaction and facilitates a decentralized performing system. In the blockchain system, the unlikely situation of having to use your data to recover dependability is mitigated by the federation. The hub group is designed to be trustworthy [5, 6].

Challenges In Healthcare Data Security and Integrity

The explosion of digital data in healthcare systems has revolutionized the ability to provide timely and precise care to patients. However, the current landscape is fraught with concerns about who has control, access, and manipulation, as well as who owns the data, as value creation increasingly gets attached and intertwined with the data being generated. Patient data shouldn't be allowed to be tampered with, should be electronically trackable, and should be severely shielded from prying eyes; consequently, the security and integrity of patient records in a healthcare system are paramount. A significant shortage of standard security procedures for ensuring reliable, sensitive healthcare data exposure makes it susceptible to breaches. A variety of management systems centralize patient information by either compromising the seclusion of each patient profile linked to the distinct patient care facility or exposing the entire group of patient profiles from the several patient care facilities they treated to all treating hospitals and physicians [7, 8]. This centralized style establishes entry points for both authorized and unauthorized users, as well as a central operating center of power. This data could potentially be mismanaged, exploited, or compromised. Adherence to guidelines, overseer requirements, and legal mandates makes it tough to govern in any centralized fashion. Healthcare services have increasingly become targets for hackers and an escalating number of cyber threats in the healthcare industry, whether to build networks, mobile devices, electronic health records, or to receive ransomware. Healthcare systems have applied multiple strategies to increase the level of their cybersecurity to adapt to these new hazards. To more effectively protect the data in healthcare systems, further and enhanced cybersecurity solutions are required to be implemented [9, 10].

Role of Blockchain in Addressing Healthcare Data Security and Integrity

In healthcare, ensuring data security and integrity is critical, but current e-health systems have yet to overcome existing challenges, including data tampering, unauthorized access, and data leakage. Blockchain technology presents a viable solution to address these challenges by assuring data integrity and security. Blockchain, a database that contains the history of all transactions, offers several unique features, such as immutability, traceability, and decentralization, which can improve healthcare data management. Firstly, immutability refers to the inability to alter data once it is recorded. Secondly, when data is written into the blockchain, the time, data, and owner of the data are visible to all of the blockchain participants who subsequently validate the data. Thirdly, data sharing and management are performed directly between peers without a need for intermediaries in a decentralized blockchain architecture [11, 12]. Several blockchain use cases have been developed to enhance data security and integrity in the healthcare domain. For instance, blockchain can be used to improve patient consent management, where patients are enabled to control their personally identifiable information between providers and choose to authorize or revoke access. In addition, the use of smart contracts on top of the blockchain architecture allows patients to define a set of usage policies for data access. Healthcare providers could use blockchain to manage authorized data access across various stakeholders. For instance, blockchain can implement access control for healthcare data, where only authorized professionals can access the patient's blockchain records. Secure data-sharing solutions, which implement both zero-knowledge proof and blockchain, have been proposed. In the proposed system, data privacy is preserved through zero-knowledge proof, and the blockchain helps all the stakeholders ensure data integrity. Any stakeholders who want to access data on the blockchain are required to request and obtain the data owner's verification. Therefore, any access to data is auditable, and the data access is ensured to be performed by the actual data owner [13, 14].

Existing e-health systems have various limitations concerning data management, particularly data security and integrity maintenance. Several unique features of blockchain make it suitable for healthcare data management, as it can provide data security and integrity. Blockchain can be integrated with existing healthcare data management systems by storing the hash of the data on the blockchain, while the actual data are stored in off-chain data repositories and warehouses. Data tampering events are then detected by comparing the stored hash in the blockchain with a regenerated hash of the data in the data repository. Nonetheless, the integration of blockchain with existing healthcare data management systems is affected by certain obstacles, such as data storage, technical ability, system cost, computational trust issues, and regulatory, and accountability concerns. Some of the e-healthcare systems developed in clinical trials and research projects have begun to consider blockchain in terms of data management [15, 16].

Implementing Blockchain Solutions in Healthcare Settings

For healthcare environments, different types of ecosystems, frameworks, and platforms can be implemented. These platforms have their own functionalities and settings; some of them also offer REST-based Application Programming Interfaces and development tools. Blockchain has the ability to foster security in healthcare systems to promote privacy while facilitating secure information exchange. Several platforms and technologies are vast now that can be customized to develop blockchain-based platforms. The users of these platforms as developers, owners, or users need to be specifically trained in these for developing the interface and dealing with them effectively as per their requirements [17, 18]. Challenges might be faced when moving from traditional to integrated blockchain solutions in healthcare and health research, such as data security and privacy, regulatory compliance, technical expertise, and interoperability. The use of blockchain in a healthcare workflow depends on understanding the optimal integration, security, and privacy goals of the system as a whole. Education and training are a must to use any technology extensively in healthcare. The development community needs guidance on how to use blockchain for secure data-sharing paradigms. Some pilot projects have begun that support digital research infrastructure investment. Platforms can facilitate secure and efficient data sharing and address challenges associated with data sharing in ways that will impact the management of data in healthcare and clinical research. These projects encourage best practices for integrating blockchain tools in healthcare workflows [19, 20]. When integrating blockchain tools in a workflow, the following stages should be considered. Pre-analysis helps to identify barriers and facilitate understanding. The beginning stage provides healthcare workers with initial information about the procedures. In the second stage, healthcare professionals should be educated on the blockchain system, taking into account the organization's use and the type of healthcare professional involved. In the third stage, implementation should be considered, and training modules and support for blockchain system use should be provided for selected healthcare professionals [21, 22].

Case Studies and Future Trends in Blockchain Integration in Healthcare

In this section, I will present some case studies explaining how blockchain has settled in the healthcare industry, potential benefits, results, and lessons learned. Moreover, I will outline the future possibilities concerning blockchain in healthcare and future development trends, such as machine learning, smart contracts, or consortium blockchains [23, 24]. The current state of blockchain is very promising with respect to healthcare. It has the potential to revolutionize approaches to data management and have very positive effects on security and patient care [25-27]. Together, the strategies proposed, combined with other trends, provide an outlook for the progress that blockchain can make for the future of healthcare [25, 26]. When we refer to blockchain technologies being transformative, we are referring to both legacy use cases of the technologies and imaginative approaches toward the future. One practical solution for implementing blockchain technologies is the integration of blockchains for healthcare alongside existing commercial entities [28-32]. These solutions typically strive to address better governance of healthcare data with some potential to share that data in a more controlled environment than typical health information exchanges [33-36]. There are many use cases, some of which promise to provide mainstream solutions for healthcare in the near future. Included are examples that range from whole cryptocurrencies designed for patient healthcare costs to the use of tokens as incentives for healthy activities [36-38].

CONCLUSION

Blockchain technology holds significant promise in addressing the healthcare industry's longstanding issues around data security and integrity. Its features of immutability, decentralized control, and secure access, offer unique solutions to current e-health system challenges, such as data tampering and unauthorized access. Through blockchain's application in patient consent management, secure data access,

and enhanced interoperability, healthcare organizations can achieve a more secure and transparent data management environment. However, for widespread adoption, the sector must overcome challenges related to technical expertise, cost, regulatory compliance, and system integration. Case studies demonstrate blockchain's tangible benefits in healthcare, indicating a promising path forward. As future advancements like machine learning and smart contracts develop within blockchain systems, healthcare can further improve data governance and patient trust.

REFERENCES

1. Satamraju KP. Proof of concept of scalable integration of internet of things and blockchain in healthcare. Sensors. 2020 Mar 3;20(5):1389.
2. Srivastava S, Mohit, Kumar A, Jha SK, Dixit P, Prakash S. Event-driven data alteration detection using block-chain. Security and Privacy. 2021 Mar;4(2):e146.
3. Duggineni S. Impact of controls on data integrity and information systems. Science and Technology. 2023 Jul;13(2):29-35.
4. Xu J, Wei L, Wu W, Wang A, Zhang Y, Zhou F. Privacy-preserving data integrity verification by using lightweight streaming authenticated data structures for healthcare cyber–physical system. Future Generation Computer Systems. 2020 Jul 1;108:1287-96. [HTML]
5. Akhtar MS, Feng T. Using blockchain to ensure the integrity of digital forensic evidence in an iot environment. EAI Endorsed Transactions on Creative Technologies. 2022 Jun 3;9(31):e2-. eai.eu
6. Mohammad A, Vargas S. Challenges of using blockchain in the education sector: A literature review. Applied Sciences. 2022 Jun 23;12(13):6380.
7. Boopathi S. Securing Healthcare Systems Integrated With IoT: Fundamentals, Applications, and Future Trends. InDynamics of Swarm Intelligence Health Analysis for the Next Generation 2023 (pp. 186-209). IGI Global. researchgate.net
8. Jaime FJ, Muñoz A, Rodríguez-Gómez F, Jerez-Calero A. Strengthening privacy and data security in biomedical microelectromechanical systems by IoT communication security and protection in smart healthcare. Sensors. 2023 Nov 3;23(21):8944. mdpi.com
9. Javaid M, Haleem A, Singh RP, Suman R. Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. Cyber Security and Applications. 2023 Dec 1;1:100016.
10. Bernard R, Bowsher G, Sullivan R. Cyber security and the unexplored threat to global health: a call for global norms. Global Security: Health, Science and Policy. 2020 Jan 1;5(1):134-41. tandfonline.com
11. Maariz A, Wiputra MA, Armanto MR. Blockchain technology: Revolutionizing data integrity and security in digital environments. International Transactions on Education Technology (ITEE). 2024 May 1;2(2):92-8. pandawan.id
12. Singh S, Hosen AS, Yoon B. Blockchain security attacks, challenges, and solutions for the future distributed iot network. Ieee Access. 2021 Jan 14;9:13938-59.
13. Singh S, Sharma SK, Mehrotra P, Bhatt P, Kaurav M. Blockchain technology for efficient data management in healthcare system: Opportunity, challenges and future perspectives. Materials Today: Proceedings. 2022 Jan 1;62:5042-6. [HTML]
14. Despotou G, Evans J, Nash W, Eavis A, Robbins T, Arvanitis TN. Evaluation of patient perception towards dynamic health data sharing using blockchain based digital consent with the Dovetail digital consent application: A cross sectional exploratory study. Digital health. 2020 May;6:2055207620924949. sagepub.com
15. Azbeg K, Ouchetto O, Andaloussi SJ. BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security. Egyptian informatics journal. 2022 Jul 1;23(2):329-43.
16. Jabbar R, Fetais N, Krichen M, Barkaoui K. Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. In2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT) 2020 Feb 2 (pp. 310-317). IEEE. researchgate.net

17. Mehta S, Grant K, Ackery A. Future of blockchain in healthcare: potential to improve the accessibility, security and interoperability of electronic health records. BMJ Health & Care Informatics. 2020;27(3).
18. Chenthara S, Ahmed K, Wang H, Whittaker F, Chen Z. Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. Plos one. 2020 Dec 9;15(12):e0243043.
19. Akram SV, Malik PK, Singh R, Anita G, Tanwar S. Adoption of blockchain technology in various realms: Opportunities and challenges. Security and Privacy. 2020 Sep;3(5):e109.
20. Zou J, He D, Zeadally S, Kumar N, Wang H, Choo KR. Integrated blockchain and cloud computing systems: A systematic survey, solutions, and challenges. ACM Computing Surveys (CSUR). 2021 Oct 4;54(8):1-36. nsf.gov
21. Khan AI, ALGhamdi AS, Alsolami FJ, Abushark YB, Almalawi A, Ali AM, Agrawal A, Kumar R, Khan RA. Integrating blockchain technology into healthcare through an intelligent computing technique. Computers, Materials & Continua. 2022 Jan 1;70(2):2835-60. researchgate.net
22. Fatoum H, Hanna S, Halamka JD, Sicker DC, Spangenberg P, Hashmi SK. Blockchain integration with digital technology and the future of health care ecosystems: systematic review. Journal of Medical Internet Research. 2021 Nov 2;23(11):e19846. jmir.org
23. Khatoon A. A blockchain-based smart contract system for healthcare management. Electronics. 2020 Jan 3;9(1):94.
24. Spanò R, Massaro M, Iacuzzi S. Blockchain for value creation in the healthcare sector. Technovation. 2023 Feb 1;120:102440.
25. Abbas A, Alroobaea R, Krichen M, Rubaiee S, Vimal S, Almansour FM. Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. Personal and ubiquitous computing. 2024 Feb;28(1):59-72. researchgate.net
26. Molli VL. Blockchain Technology for Secure and Transparent Health Data Management: Opportunities and Challenges. Journal of Healthcare AI and ML. 2023 Jan 1;10(10):1-5.
27. Tariq MU. Revolutionizing health data management with blockchain technology: Enhancing security and efficiency in a digital era. InEmerging Technologies for Health Literacy and Medical Practice 2024 (pp. 153-175). IGI Global. [HTML]
28. Chukwudi, O. F., Eze, V. H. U., & Ugwu, C. N. (2023). A Review of Cross-Platform Document File Reader Using Speech Synthesis. International Journal of Artificial Intelligence, 10(2), 104–111.
29. Enerst, E., Eze, V. H. U., Ibrahim, M. J., & Bwire, I. (2023). Automated Hybrid Smart Door Control System. IAA Journal of Scientific Research, 10(1), 36–48
30. Enerst, E., Eze, V. H. U., Musiimenta, I., & Wantimba, J. (2023). Design and Implementation of a Smart Surveillance Security System. IDOSR Journal of Science and Technology, 9(1), 98–106. https://doi.org/10.5120/cae2020652855
31. Enerst, E., Eze, V. H. U., Okot, J., Wantimba, J., & Ugwu, C. N. (2023). DESIGN AND IMPLEMENTATION OF FIRE PREVENTION AND CONTROL SYSTEM USING ATMEGA328P MICROCONTROLLER. International Journal of Innovative and Applied Research, 11(06), 25–34. https://doi.org/10.58538/IJIAR/2030
32. Enerst, E., Eze, V. H. U., & Wantimba, J. (2023). Design and Implementation of an Improved Automatic DC Motor Speed Control Systems Using Microcontroller. IDOSR Journal of Science and Technology, 9(1), 107–119.
33. Enyi, V. S., Eze, V. H. U., Ugwu, F. C., & Ogbonna, C. C. (2021). Path Loss Model Predictions for Different Gsm Networks in the University of Nigeria, Nsukka Campus Environment for Estimation of Propagation Loss. International Journal of Advanced Research in Computer and Communication Engineering, 10(8), 108–115. https://doi.org/10.17148/IJARCCE.2021.10816
34. Eze, M. C., Eze, V. H. U., Chidebelu, N. O., Ugwu, S. A., Odo, J. I., & Odi, J. I. (2017). NOVEL PASSIVE NEGATIVE AND POSITIVE CLAMPER CIRCUITS DESIGN FOR ELECTRONIC SYSTEMS. International Journal of Scientific & Engineering Research, 8(5), 856–867.

35. Eze, M. C., Eze, V. H. U., Ugwuanyi, G. N., Alnajideen, M., Atia, A., Olisa, S. C., Rocha, V. G., & Min, G. (2022). Improving the efficiency and stability of in-air fabricated perovskite solar cells using the mixed antisolvent of methyl acetate and chloroform. Organic Electronics, 107, 1–10. https://doi.org/10.1016/j.orgel.2022.106552
36. Eze, M. C., Ugwuanyi, G., Li, M., Eze, V. H. U., Rodriguez, G. M., Evans, A., Rocha, V. G., Li, Z., & Min, G. (2021). Optimum silver contact sputtering parameters for efficient perovskite solar cell fabrication. Solar Energy Materials and Solar Cells, 230(2020), 111185. https://doi.org/10.1016/j.solmat.2021.111185
37. Eze, V. H. U. (2023). Development of Stable and Optimized Bandgap Perovskite Materials for Photovoltaic Applications. IDOSR Journal of Computer and Applied Science, 8(1), 44–51.
38. Eze, V. H. U. (2024). Advancing Sustainable Energy Solutions in Uganda: A Comprehensive Exploration for Multi-Source Power Control Design. IAA Journal of Applied Sciences 11(1):73-86, 11(1), 73–86.

CITE AS: Tukamuhebwa Richard. (2024). Blockchain in Healthcare: Ensuring Data Security and Integrity. Research Output Journal of Public Health and Medicine 4(2):12-17. **https://doi.org/10.59298/ROJPHM/2024/421217**