Blockchain Integration in Healthcare Information System: A Secure and Efficient Approach

Taiye Muktar [1] and Timur Inan [2][0000-0002-6647-3025]

[1] Department of Computer Science, Altinbaş University, Republic of Türkiye
[2] Department of Computer Engineering, Marmara University, Republic of Türkiye
213721006@org.altinbas.edu.tr
timur.inan@marmara.edu.tr

Abstract. In the realm of healthcare blockchain technology offers an approach, to storing records facilitating medical transactions and fostering trust within a decentralized healthcare network. While the healthcare sector has shown interest in technology concerns persist regarding the security and privacy implications associated with sharing medical information. This piece delves into the issues surrounding security and privacy, in utilizing blockchain within healthcare focusing on studies conducted from 2018 to 2023.This study aims to tackle challenges and explore real world uses by assessing existing literature. The goal is to offer an evaluation that sheds light on directions, for future research and advancements.

Keywords: Blockchain, Healthcare, Medical Data, Security and Privacy.

1 Introduction

Blockchain technology has been increasingly prominent, in sectors with healthcare being no exception. It's not surprising since blockchain acts as a transparent and decentralized distributed database establishing trust in the value chain. As the healthcare industry embraces transformation the development of medical information systems becomes essential. Healthcare holds importance in people's lives and data plays a role in diagnosing illnesses and guiding treatment decisions. Traditionally data was recorded on changeable or insecure mediums. However, with advancements, like technology, secure and efficient data transmission is now achievable [1-7]. Furthermore, these technologies are expected to enhance user anonymity, privacy, and access control. Without adequate security, privacy, and trust, individuals may be hesitant to share sensitive information or delay seeking necessary medical treatments[8]. Hence, data security becomes paramount, leading to the emergence of blockchain technology, a cutting-edge solution that promises to safeguard data from breaches and vulnerabilities[9]. The inherent decentralized nature of blockchain technology enables it to resist setbacks and attacks in a distributed and steadfast manner. These technologies will also be expected to advance user anonymity, privacy and control.

Thus, inadequate security, trust and privacy can make individuals reluctant to share personal information or delay seeking important medical attention[10]. Therefore, data

safety is critical; hence the advent of blockchain technology. This technology is particularly known for its decentralized character which makes it resistant to failures and attacks at large. Besides this, it documents data ownership and validates that it's genuine[11]. In the last years blockchain has been recognized as an adjustable technology with numerous applications in industry specific solutions such as identity management, supply chain management, healthcare, insurance and contract administration [12] Notable characteristics of blockchain are decentralization, openness, traceability and reliability.

Thus, Blockchain comes in handy when one needs to tackle issues of security confidentiality and interoperability. It allows for transactions within networks among untrusted parties while acting as means of collecting distributed networked device data[13].

It has been largely recognized that blockchain technology has the potential to revolutionize how patient data is exchanged and stored in the healthcare sector, thereby improving metrics like process security and efficiency. Nonetheless, in terms of medical field there are challenges with regard to security and privacy particularly in safeguarding confidential patient data. A review of literature on this topic is aimed at providing a preview for various scholars who are involved in making contributions into research on this issue. The study by Hasselgren et al. involved a scoping review about blockchain utilization in healthcare where they noted the existence of unresolved issues such as regulatory environment and interoperability requirements [13]. However, they concluded that blockchain can improve the security and privacy levels within healthcare. Azaria et al make an important point regarding the security or privacy of patient data during modern times – it matters a lot [14]. They suggest that tracking medical data using blockchain technology will help meet objectives related to authenticity, accountability, and certainty. In general, from available evidence one can deduce that blockchain technology could potentially enhance the safety features around transfer of patients' health information storage as well as its privacy.

However, there are still some issues that need to be sorted out such as proper access controls, regulatory concerns and interoperability. More studies should be done in order to fully explore what blockchain might do in the health care system in relation to the protection of patient privacy and confidentiality. This paper presents a review that was critically carried out based on these factors. Although other useful investigations can be found in literature [16-18], this work looks at the issue from a different angle and purpose.

2 Background

2.1 Blockchain Technology

The blockchain technology, which became popular through Bitcoin's success, provides a safe and dependable way of doing business without relying on a central third party over decentralized networks. Here then are the key elements in blockchain [19]-[21].

2.2 Blockchain Systems' Types

There are four types of blockchain systems depending on whether the network nodes have been given permissions or not:

Private Blockchain: In this case, the network is restricted to those who are invited or authorized. Network control through access restriction.

Public Blockchain: Anybody that wants to be a node or miner can join a public blockchain and it is widely accessible and participatory.

Hybrid Blockchain: these combined elements of public and private blockchains they allow for control over who can see and access the information on the blockchain.

Consortium blockchain: This is also known as "semi-private" blockchain lies between public and private blockchains. It is accessible to a selected number of authorized organizations often helping companies in achieving their goals.

2.3 Blockchain in Healthcare

It is crucial to ensure that medical records are secure in the healthcare industry. Healthcare organizations employ multiple security measures to protect patient data, and blockchain technology has the potential of transforming the healthcare sector by securely storing and transmitting sensitive patient data. In healthcare, data security becomes important because it keeps confidential information like test results, prescriptions details, and medical histories [14-17,22-24].

The safekeeping of medical records is crucial in healthcare. Medical organizations use various security measures to protect patient data; secure storage and transmission of sensitive patient data using blockchain technology may revolutionize healthcare sector. In healthcare, as it helps to guard confidential information like diagnostic test results, prescriptions, and family histories.[14-17, 22-24]

Confidentiality of medical records is a big issue in healthcare industry also. Blockchain technology could be used to improve healthcare privacy because it has many advantages. It minimizes the chances for a single point of failure or target by making the ledger decentralized and distributed. This allows smart contracts that are compliant with privacy laws and which automate sharing of data to be established on a blockchain protocol system. However, pseudonymization and encryption methods provide ways through which private data stored on blockchains can be protected while still allowing authorized parties access to that particular information. Nevertheless, several challenges remain in using blockchain for privacy in health care particularly, how different blockchain platforms can interoperate among themselves and dealing with the challenges related to implementation process itself (Fernandez et al., 2018).14 25 27

2.4 Interoperability Challenges

Incorporating blockchain technology into healthcare is a major challenge, with interoperability being one of the biggest technical hurdles. The diverse nature of such systems as they employ different electronic health record (EHR) system and medical devices with dissimilar data formats and standards make complicated healthcare data exchange challenging. These interoperability difficulties can be overcome through careful planning and transformation of information particularly when dealing with legacy systems that are not compatible with blockchain technology.

To realize the full potential of blockchain in healthcare, there are several ways to address these challenges. They include creating standardization for medical data within the network, employing middleware to facilitate communication between the networks of blockchains and existing systems, and reaching consensus on data standards by collaborating amongst healthcare organizations, regulators and technology providers.

3 Methodology

In this review a systematic search was conducted in different bibliographic databases such as MEDLINE, Embase, Cochrane Library, Scopus, Google Scholar, Compendex, Inspec ACM IEEE etc. The search strategy combined the terms “blockchain” AND “health” using Boolean operator AND. The selection process involved filtering titles, abstracts, and full papers based on inclusion and exclusion criteria, with a reviewer and supervisor reviewing and discussing publications to ensure consistency.

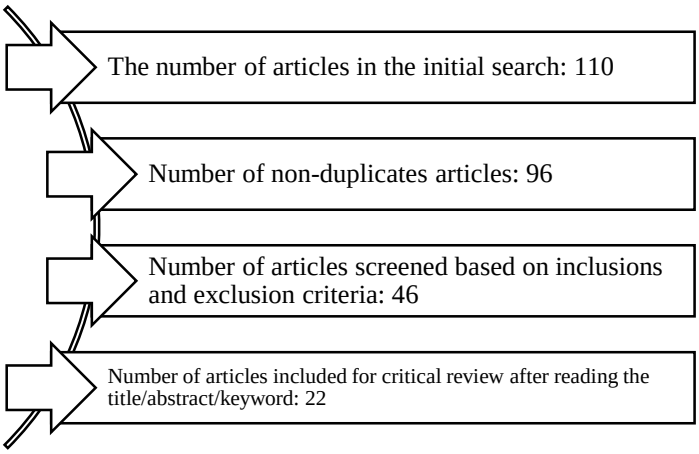


Fig. 3.1. Selection process.

3.1 Inclusion and Exclusion Criteria

Inclusion Criteria

1. Research was published from 2018 to 2023.
2. The research's exclusive domain is the journal.
3. The two primary areas of research should be "blockchain" and "healthcare."
4. Articles that put forth a framework, paradigm, or system.

Exclusion criteria

1. Press pieces being pulled.
2. Articles in languages other than English.
3. Books, dissertations, monographs, conferences, reviews, and works derived from interviews are not included.

3.2 Data Extraction

The collected research data was utilized to construct a preliminary development matrix. Once the reviewer had extracted the majority of the data, the supervisor reviewed it again. The data was extracted, organized, and condensed into a matrix format, which was subsequently converted into tables and graphs. The data matrix was initially created in Google Sheets and later converted to Microsoft Excel 2023 for the convenience of the study group.

3.3 Data Analysis

After extracting relevant quantitative data, the data analysis was carried out using Microsoft Excel 2023. When applicable, the standard deviation (SD) and mean, indicated by ±, were calculated. All numerical values were rounded to the nearest whole number. Categorical statistics were presented as percentages unless otherwise specified.

4 Results and discussion

This study shows that blockchain can provide information security, confidentiality as well as integration in the healthcare industry. The main aim of this research is to tackle the persistent security and privacy issues within the domain. The findings show that these technologies can protect patient and doctor's privacy by efficiently distributing and limiting access to medical information. The suggested processes satisfy the expected safety norms and have competitive computation and communication overheads. For example, (Kumar et al., 2022).'s work outlines a new model for sharing decentralized medical image data using blockchain technology through federated learning[31]. Also, it mentions an off-chain health data storage architecture based on Interplanetary File System (IPFS) which demonstrates its extraordinary security, scalability, and resilience. It also demonstrates that sending data to blockchain only affects processing time and effort because of the anonymous nature and encryption provided by design [32-44].

Many research papers proposed methods where patients are able to decide whether or not their data should be accessed [45-50] Technology advances can be used to help healthcare organizations and healthcare providers conform better with the privacy regulations. Additionally, these solutions are able to provide secure payment options thus allowing patients and hospitals to pay for storage and diagnostic services without any risks. According to a comprehensive security study and rigorous testing, these solutions have shown great resilience against various attacks such as impersonation, collusion or middle man attack. Finally, in terms of secure transmission and storage of health privacy data within or outside the health system, the findings demonstrate high-security encryption performance, balanced storage space allocation as well as robust anti-attack capabilities by the suggested approaches. In order to ensure safe searching in IoT medical applications like IoMT (Internet of Medical Things) framework 5; we propose using custom-made smart contracts that rely on modified attribute-based cryptographic primitives.

The development of Internet of Things (IoT) technology has led to increased interest in Wireless Sensor Network (WSN) systems.[52] Further studies have improved their techniques for small sensors nodes found in IoT devices.[53] The sophistication level

involved in different sensors depends on factors such as cost efficiency, power consumption, sensing range among others. There are some important technologies that are employed by WSNs' energy management system under this field.

This paper presents several developments which have been carried out with an intention of conserving energy through utilization of wireless sensor networks. In many cases a miniaturization technique is used when trying to produce ultra-small sensors which do not need any battery or even wire.

Furthermore, researcher may wish to experiment with different types photovoltaic materials such as organic cells instead of silicon-based cells

Additionally, researchers might want to explore other sorts photovoltaic elements like organic ones rather than silicon based cells.

Another research (Yugha et al., 2022, p. 52) concludes that the suggested method is a secure and efficient way for transmitting medical data in IoT while maintaining privacy of patients. Another study by (Yugha et al., 2022) shows that the proposed approach provides a secure and efficient means to facilitate the transfer of IoT medical data while preserving patient privacy. The above studies collectively demonstrate how blockchain technology can be used to enhance efficient, safe and secured healthcare data sharing and access control. A major reason why these methods are suitable for IoMT applications is because they meet the expected security standards, as well as provide competitive communication and processing costs. These findings show how these technologies can effectively solve longstanding security and privacy problems faced by health industry.

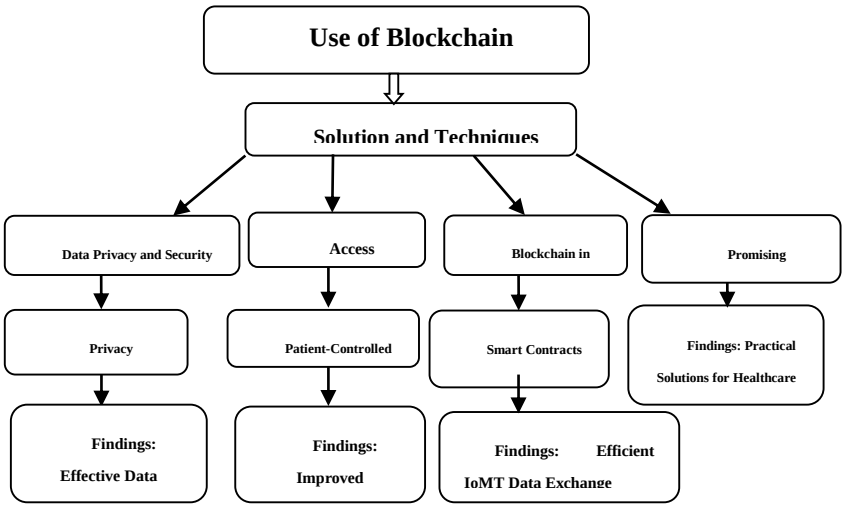


Fig. 4.1. Blockchain and cryptography for privacy and security in healthcare

TABLE 1. HEALTH RECORDS APPLICATIONS

Use Case
1. Electronic health records (EHRs)[43]
2 Personal health records (PHRs) management and sharing [22]
3 Management of EHRs [23]
4 Blockchain technology for EHR management [44]
5 Enhancing EHR privacy using blockchain [45]
6 Automation of EHR and related services [46]
7 Integration of bitcoin payments and smart contracts in EHR systems [47]
8 PHR [48]
9. EHR sharing [49]
10. Patient record management [50]

Robust security and privacy measures are essential for the sharing and administration of Personal Health Records (PHRs). PHRs store sensitive health information such as test results, diagnoses, and medical histories. By employing blockchain technology for data sharing, patient privacy can be protected, and access to the data can be restricted to authorized personnel (Table 2). Enhancements in healthcare data security and privacy can be achieved through privacy-preserving Knearest Neighbors (K-NN) training for Internet of Things (IoT) data, and the exchange of electronic health records (EHRs) can contribute to privacy protection.[50,51]

Patients' medical information can be exchanged and stored securely on blockchain platforms that use the technology offering confidentiality and data integrity (“Table 4.3”). Thus, additional security options such as authorization or authentication mechanisms improve healthcare data protection through blockchain (“Table 4”). While Table 4.5 contains publications that address improvement of security methods, table 4.6 separately lists all applications per each use cases.

TABLE 2. DATA MANAGEMENT

Use Case and Reference
1. Sharing of IoT data in health. [42]
2. Safe communication of data. [44]
3. Sharing.[52]
4. Sharing of medical data.[53]
5. Data sharing using blockchain assistance. [56]
6. Sharing of medical data. [57]
7. Healthcare data transfer with privacy preservation provided by IoT. [41]
8. Information exchange. [58]
9. Sharing of health information. [56]
10 Safe exchange of health information between various organizations. [58]
11. method for protecting privacy and sharing medical data.[59]
12 Data management in healthcare.[60]
13 Group decision-making in medicine. [61]
14 Big data management in healthcare.[62]
15 Sharing of protected health information (PHI).[63]
16 Transfer of data.[64]
17 Information management in healthcare.[30]
18 Storage of data.[26]
19 COVID-19 medical record protection facilitated by blockchain technology.[65]
20. Medical data transmission enabled by AI and blockchain.[66]

TABLE 3. PRIVACY ENHANCEMENT

Use Case
1. Preserving privacy [67]
2. Improvement of privacy [68]
3. An e-health system that protects privacy [69]
4. Sharing of data while protecting privacy [70]
5. Protection of privacy [71]
6. Better location sharing in healthcare that protects privacy [72]
7. Protection of medical data privacy [73]
8. Protection of medical privacy [74]
9. Sharing medical data while protecting Privacy [75]
10. Sharing of electronic health data while protecting privacy [76]
11. IoT data privacy-preserving K-NN training [79]
12. Privacy of health data [77]
13. Medical data privacy protection program [78]
14. Blockchain privacy in healthcare [85]

4.0 Authentication and Security Enhancement

These include identity authentication, machine learning authentication, blockchain-based healthcare data authorization and authentication, authentication, PPBA authentication, and anonymity on the Internet of Things.[78-82] A key component of this use case in the healthcare industry is security enhancement, with particular attention paid to areas like biomedical security, medical data security, collaborative analysis, and enhanced security and privacy in the patient healthcare framework.[83-87] This use case takes into account a number of additional applications in addition to the main focus. Verifiable data classification, contact tracing, IoT healthcare security and privacy, and federated learning are some of these applications. [87, 45, 35,22]

4.1 Research question 1: What healthcare-related blockchain applications for security and privacy are there?

In healthcare industry, patient confidentiality and security have become crucial concerns.Electronic health records (EHRs), which contain sensitive and private data, must be secure and private in order to protect patients' rights and stop data breaches. One of the biggest problems facing the healthcare industry is patient information privacy. Blockchain-based EHR systems could offer a secure, ‘unhackable’ system that patient information transfers and storage. While intelligent contracts and cryptocurrency payments will ensure only permitted individuals gain access to the information, the decentralized structure of blockchain has proven capabilities not to allow data compromise and provide assurance to data authenticity. Another way that patients can choose who gained full or limited control to their information and revoke or grant access as needed is through patient-controlled access. Blockchain-based access control may also improve data privacy by letting patients grant or revoke access to their data whenever they choose and ensuring that only authorized parties may access it. They don't both show off how to use smart contracts

4.2 Research question 2: What security and privacy issues does blockchain present for the healthcare sector?

The issue of security and privacy is a delicate matter in medical data due to the possibility of harm and damage through unauthorized access or data breaches. In response to these challenges, blockchain technology presents itself as providing an alternative decentralized, secure platform for sharing and storage of data. Cryptographic primitives are useful for secure search and customized access control; whereas smart contracts offer information confidentiality as well as access control. The validity, efficiency, and safety have been proven by numerous suggested solutions during simulation and experimental investigations. Additionally, several empirical studies have demonstrated that blockchain-based systems can meet expected security requirements without escalating computation and communication expenses. By way of example, Modified attribute based cryptographic primitives together with certificateless public-key encryption may be suitable for protecting privacy in hospital settings where users need customizable access control. To this effect organizations must carefully assess such proposals to ensure they are feasible within real-life healthcare settings while at the same time meeting necessary privacy concerns.

4.3 Research question 3: How can blockchain technology protect patient privacy and security in the healthcare sector?

In the years ahead, healthcare is set to concentrate more on improving privacy and security. The potential of blockchain technology to secure medical data is growingly admitted nowadays. A smart medical cloud platform ensures that a user's privacy can be protected while allowing for data consumption without borrowing. Such new technologies like edge computing, federated learning, and blockchain are among others that could help improve data security and privacy. Access control is made secure while data manipulation is stopped by use of blockchain technology while supporting private information federation through cooperative analysis of data in federated learning. Moreover, edge computing can reduce the possibility of data breach by processing it closer to its source unlike centralizing it. Alternatively, regulations could be made stronger as part of ensuring safety of personal health information. This becomes more critical today because the amount of health-related information becoming available has multiplied exponentially over time leading to increased chances of cyber terrorism or hacking into such databases or networks if they are not adequately protected from unauthorized intrusion as well as other types or forms of breaches which people might not even imagine at first glance which would cause tremendous damages once done. Two acts that help protect personal health information are Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR). More laws will probably be established in the future with a view to ensure the security of health issues hence there may exist several regulations therefore requiring diverse measures in different countries during this period when quite a number of countries have already developed their own legal frameworks in respect to privacy matters only waiting for discussions among stakeholders so as their enactment process can eventually begin too under certain circumstances given that e-PHI includes any medium used by organizations to record patients' conditions such as paper records or electronic systems storing patients' test results plus doctors' diagnostic findings among others thereby making one wonder what specific measures ought to be taken here apart from just securing such details?

5 Conclusion

Efforts should focus on developing state-of-the-art technologies that enable efficient management of the substantial volume of healthcare data within blockchain networks while ensuring seamless connectivity across multiple networks. Scalability and interoperability should be prioritized in healthcare blockchain networks to facilitate efficient data processing and seamless network connectivity. The dynamic interaction between blockchain technology and the healthcare sector presents numerous research opportunities and practical applications. Resolving interoperability and scalability challenges is the most pressing issue. Blockchain's security features can facilitate secure global transmission of healthcare data, particularly when treating patients from different countries. Blockchain has the potential to revolutionize the management of the medical supply chain by ensuring patient safety and validating the authenticity of medications. Additionally, combining blockchain technology with artificial intelligence can unlock powerful data analytics capabilities while protecting data privacy. Patients may have more control over their medical records and even earn income from them through the use of blockchain technology. However, careful consideration is needed for patient consent and identity management. Blockchain technology can assist healthcare organizations in complying with regulations, particularly those related to data security. It can also enhance the security of IoT medical devices by protecting the integrity of patient data collected by these sensors. Improving user interfaces and seamless integration of telemedicine and blockchain-based electronic health records with existing healthcare infrastructure is another potential avenue. This review highlights key research topics and demonstrates how blockchain technology can transform the healthcare field. It emphasizes the potential of blockchain technology in addressing longstanding issues in the sector. Blockchain technology offers a novel approach to medical data storage, transaction processing, and integration and sharing within a decentralized healthcare network. However, the security and privacy challenges associated with sharing information using blockchain need to be carefully addressed. The paper presents research conducted between 2018 and 2023 on the privacy and security of blockchain in healthcare.

The aim of this research review is to assess the current state of affairs, focusing on practical applications and challenges. The analysis concludes that blockchain technology holds promise for addressing practical privacy and security issues in the medical domain. By providing a decentralized and tamper-proof platform for exchanging and storing sensitive patient data, blockchain technology enhances the privacy and security of PHRs and EHRs. It also enables patients to have more control over their data through patient-controlled authentication. Healthcare organizations and practitioners need to carefully evaluate the suitability of blockchain solutions for their specific contexts to ensure practicality and compliance with privacy requirements. While blockchain technology has significant potential, it is not a one-size-fits-all solution and may require customization to meet specific needs. Overall, the study identifies areas that require further research and development to unlock the full potential of blockchain technology in healthcare.

Carefully addressed privacy and security concerns on blockchain-based sharing of information, though. This implies that sharing any health information on a blockchain should be treated with care because there are inherent risks associated with it. The article presents work done between 2018 and 2023 about the privacy and security of blockchain technology regarding healthcare. Blockchain technology can also help in

complying with regulations, especially those concerned with data security for healthcare providers. In addition, this can secure IoT medical devices by ensuring patient data which was gathered from such sensors is kept intact. Furthermore, the improvement of user interfaces as well as seamless integration into existing health infrastructure could also be considered as a possibility presented herein. By doing so, the current issue points out some important directions for research and outlines how blockchain might change the medical field through several case studies suggesting an array of potential impacts to various stakeholders within that sector. It highlights how blockchain might address long-standing problems within healthcare systems. This enables medical data to be stored, processed, transacted or shared in a decentralized manner across the Internet as its key attributes without any third party intervention – thereby making Blockchain Technology revolutionary in EHRs storage as compared to other traditional record keeping approaches like EMR/EHR systems built over centralized databases (Nakamoto, 2008).

The primary objective of this research review is to assess the current situation focusing on applications and challenges. The study concludes that blockchain technology has the potential to address practical privacy and security issues in healthcare. Therefore, blockchain technology improves PHR's and EHR's privacy and security by providing a decentralized and tamper-proof platform for sharing sensitive health information. It also allows patients to maintain more control over their data through patient-controlled authentication. In a bid to be practical and meet with various privacy requirements, healthcare organizations should evaluate how appropriate it would be to apply block chain solutions in their organizations as well as adhere with legal considerations relating to patient information rights among other things. Nevertheless, while blockchain technology has great potential, it is not a universal solution that can be used without customization. This paper however pinpoints specific areas which require further investigation regarding blockchain technology's full potential in medical field.

6 Recommendations

1. Interoperability and Scalability: Urgently address interoperability and scalability challenges in healthcare blockchain networks. Focus on developing innovative solutions that enable efficient data processing and seamless network connectivity across multiple networks. Explore approaches that can effectively manage the substantial volume of healthcare data while ensuring secure and reliable connectivity.

2 International Data Transmission: Investigate the benefits of using blockchain's security features for transmitting medical data across borders, particularly when treating patients from different countries. Explore how blockchain can enhance the security, privacy, and integrity of data in international medical transactions.

3 Revamping the Medical Supply Chain: Analyze the possible consequences for healthcare supply chain management that may arise from using blockchain technology. Elucidate on how blockchain is capable of enhancing patient's safety and validating the genuineness of drugs. Propose viable approaches that will safely embed blockchain in extant supply chain practices, which will continue to be responsible, liable and open.

Disclosure of Interests. Both Author A (Taiye Muktar) and Author B (Timur Inan) have no known competing interest anywhere.

References

1. McGhin T, Choo K-KR, Liu CZ, He D. Blockchain in healthcare applications: Research challenges and opportunities. J Netw Comput Appl. 2019;135:62–75.
2. Esposito C, De Santis A, Tortora G, Chang H, Choo K-KR. Blockchain: A panacea for healthcare cloud-based data security and privacy? IEEE Cloud Comput. 2018;5:31–37.
3. Epiphaniou G, Daly H, Al-Khateeb H. Blockchain and healthcare. In: Blockchain and Clinical Trial: Securing Patient Data. Springer; 2019. pp. 1–29.
4. Ahram T, Sargolzaei A, Sargolzaei S, Daniels J, Amaba B. Blockchain technology innovations. In: Proceedings of the 2017 IEEE Technology & Engineering Management Conference (TEMSCON); 2017 Jun 8–10; Santa Clara, CA, USA. pp. 137–141.
5. Kuo T-T, Zavaleta Rojas H, Ohno-Machado L. Comparison of blockchain platforms: A systematic review and healthcare examples. J Am Med Inform Assoc. 2019;26:462–478.
6. Hölbl M, Kompara M, Kamišali´c A, Nemec Zlatolas L. A systematic review of the use of blockchain in healthcare. Symmetry. 2018;10:470. 7. Khan FA, Gumaei A, Derhab A, Hussain A. A novel two-stage deep learning model for efficient network intrusion detection. IEEE Access. 2019;7:30373–30385.
7. Liang X, Zhao J, Shetty S, Liu J, Li D. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In: Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC); 2017 Oct 8–13; Montreal, QC, Canada. pp. 1–5.
8. Yaqoob S, Khan MM, Talib R, Butt AD, Saleem S, Arif F, Nadeem A. Use of blockchain in healthcare: A systematic literature review. Int J Adv Comput Sci Appl. 2019;10:644–653.
9. Khalid U, Asim M, Baker T, Hung PC, Tariq MA, Rafferty L. A decentralized lightweight blockchain-based authentication mechanism for IoT systems. Clust Comput. 2020;23:2067–2087.
10. Burniske C, Vaughn E, Cahana A, Shelton J. How Blockchain Technology Can Enhance Electronic Health Record Operability. Ark Invest: New York, NY, USA; 2016.
11. Taherdoost H. Blockchain-Based Internet of Medical Things. Appl Sci. 2023;13:1287.
12. Hasselgren A, Kralevska K, Gligoroski D, Pedersen SA, Faxvaag A. Blockchain in healthcare and health sciences—A scoping review. Int J Med Inform. 2020;134:104040.
13. 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); 2016 Aug 22–24; Vienna, Austria. pp. 25–30.
14. Zhang R, Xue R, Liu L. Security and privacy for healthcare blockchains. IEEE Trans Serv Comput. 2021;15:3668–3686.
15. Roman-Belmonte JM, De la Corte-Rodriguez H, Rodriguez-Merchan EC. How blockchain technology can change medicine. Postgrad Med. 2018;130:420–427.
16. Kuo T-T, Kim H-E, Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applications. J Am Med Inform Assoc. 2017;24:1211–1220.
17. Engelhardt MA. Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector. Technol Innov Manag Rev. 2017;7:22–34.
18. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Decentralized Bus Rev. 2008;21260.
19. Ma S, Deng Y, He D, Zhang J, Xie X. An efficient NIZK scheme for privacy-preserving transactions over account-model blockchain. IEEE Trans Dependable Secur Comput. 2020;18:641–651.

20. Lin C, He D, Huang X, Khan MK, Choo K-KR. DCAP: A secure and efficient decentralized conditional anonymous payment system based on blockchain. IEEE Trans Inf Forensics Secur. 2020;15:2440–2452.
21. Mohanasundaram S, Ramirez-Asis E, Quispe-Talla A, Bhatt MW, Shabaz M. Experimental replacement of hops by mango in beer: Production and comparison of total phenolics, flavonoids, minerals, carbohydrates, proteins and toxic substances. Int J Syst Assur Eng Manag. 2022;13:132–145.
22. Sriram G. Edge computing vs. Cloud computing: An overview of big data challenges and opportunities for large enterprises. Int Res J Mod Eng Technol Sci. 2022;4:1331–1337.
23. Hassan NH, Ismail Z. A conceptual model for investigating factors influencing information security culture in healthcare environment. Procedia-Soc Behav Sci. 2012;65:1007–1012.
24. Yaqoob I, Salah K, Jayaraman R, Al-Hammadi Y. Blockchain for healthcare data management: Opportunities, challenges, and future recommendations. Neural Comput Appl. 2021;34:11475–11490.
25. Zhang P, Schmidt DC, White J, Lenz G. Blockchain technology use cases in healthcare. In: Advances in Computers. Elsevier; 2018. Volume 111, pp. 1–41.
26. Appelbaum D, Cohen E, Kinory E, Stein Smith S. Impediments to blockchain adoption. J Emerg Technol Account. 2022;19:199–210.
27. Alnafrani M, Acharya S. SecureRx: A blockchain-based framework for an electronic prescription system with opioids tracking. Health Policy Technol. 2021;10:100510.
28. Leng J, Chen Z, Huang Z, Zhu X, Su H, Lin Z, Zhang D. Secure blockchain middleware for decentralized iiot towards industry 5.0: A review of architecture, enablers, challenges, and directions. Machines. 2022;10:858.
29. Hasan MR, Deng S, Sultana N, Hossain MZ. The applicability of blockchain technology in healthcare contexts to contain COVID-19 challenges. Libr Hi Tech. 2021;39:814–833.
30. Kumar R, Kumar J, Khan AA, Zakria, Ali H, Bernard CM, Khan RU, Zeng S. Blockchain and homomorphic encryption based privacypreserving model aggregation for medical images. Comput Med Imaging Graph. 2022;102:102139.
31. Wang Y, Zhang A, Zhang P, Qu Y, Yu S. Security-Aware and PrivacyPreserving Personal Health Record Sharing Using Consortium Blockchain. IEEE Internet Things J. 2022;9:12014–12028.
32. Jayabalan J, Jeyanthi N. Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy. J Parallel Distrib Comput. 2022;164:152–167.
33. Kumar R, Tripathi R. Towards design and implementation of security and privacy framework for Internet of Medical Things (IoMT) by leveraging blockchain and IPFS technology. J Supercomput. 2021;77:7916–7955.
34. Majdoubi DE, Bakkali HE, Sadki S. SmartMedChain: A BlockchainBased Privacy-Preserving Smart Healthcare Framework. J Healthc Eng. 2021;2021:4145512.
35. 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;15:e0243043.
36. Younis M, Lalouani W, Lasla N, Emokpae L, Abdallah M. Blockchain -Enabled and Data-Driven Smart Healthcare Solution for Secure and Privacy-Preserving Data Access. IEEE Syst J. 2022;16:3746–3757.
37. Wu G, Wang S, Ning Z, Li J. Blockchain-Enabled Privacy-Preserving Access Control for Data Publishing and Sharing in the Internet of Medical Things. IEEE Internet Things J. 2022;9:8091–8104.

38. Alzubi OA, Alzubi JA, Shankar K, Gupta D. Blockchain and artificial intelligence enabled privacy-preserving medical data transmission in Internet of Things. Trans Emerg Telecommun Technol. 2021;32:e4360.
39. Dagher GG, Mohler J, Milojkovic M, Marella PB. Ancile: Privacypreserving framework for access control and interoperability of electronic health records using blockchain technology. Sustain Cities Soc. 2018;39:283–297.
40. Yue X, Wang H, Jin D, Li M, Jiang W. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. J Med Syst. 2016;40:218.
41. Mohammad Hossein K, Esmaeili ME, Dargahi T, Khonsari A, Conti M. BCHealth: A Novel Blockchain-based Privacy-Preserving Architecture for IoT Healthcare Applications. Comput Commun. 2021;180:31–47.
42. Barka E, Al Baqari M, Kerrache CA, Herrera-Tapia J. Implementation of a Biometric-Based Blockchain System for Preserving Privacy, Security, and Access Control in Healthcare Records. J Sens Actuator Netw. 2022;11:85.
43. Boumezbeur I, Zarour K. Privacy Preservation and Access Control for Sharing Electronic Health Records Using Blockchain Technology. Acta Inform Pragensia. 2022;11:105–122.
44. Karunakaran C, Ganesh K, Ansar S, Subramani R. A privacy preserving framework for health records using blockchain. Pertanika J Sci Technol. 2021;29:3081–3098.
45. Egala BS, Pradhan AK, Badarla V, Mohanty SP. Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things with Effective Access Control. IEEE Internet Things J. 2021;8:11717–11731.
46. Shanthashalini K, Nithya M. Blockchain based healthcare system to ensure data integrity and security in green computing environments. J Green Eng. 2020;10:10244–10260.
47. Thwin TT, Vasupongayya S. Blockchain-Based Access Control Model to Preserve Privacy for Personal Health Record Systems. Secur Commun Netw. 2019;2019:8315614.
48. Cao Y, Sun Y, Min J. Hybrid blockchain–based privacy-preserving electronic medical records sharing scheme across medical information control system. Meas Control. 2020;53:1286–1299.
49. Tith D, Lee JS, Suzuki H, Wijesundara WMAB, Taira N, Obi T, Ohyama N. Application of blockchain to maintaining patient records in electronic health record for enhanced privacy, scalability, and availability. Healthc Inform Res. 2020;26:3–12.
50. Ul Haque R, Hasan ASMT, Jiang Q, Qu Q. Privacy-preserving knearest neighbors training over blockchain-based encrypted health data. Electronics. 2020;9:96..
51. Al-Otaibi YD. K-nearest neighbour-based smart contract for internet of medical things security using blockchain. Comput Electr Eng. 2022;101:108129.
52. Zhang D, Wang S, Zhang Y, Zhang Q, Zhang Y. A Secure and Privacy -Preserving Medical Data Sharing via Consortium Blockchain. Secur Commun Netw. 2022;2022:2759787.
53. Nie X, Zhang A, Chen J, Qu Y, Yu S. Blockchain-Empowered Secure and Privacy-Preserving Health Data Sharing in Edge-Based IoMT. Secur Commun Netw. 2022;2022:8293716.
54. Chen Z, Xu W, Wang B, Yu H. A blockchain-based preserving and sharing system for medical data privacy. Future Gener Comput Syst. 2021;124:338–350.
55. Elhoseny M, Haseeb K, Shah AA, Ahmad I, Jan Z, Alghamdi MI. IoT solution for AI-enabled privacy-preserving with bigdata transferring: An application for healthcare using blockchain. Energies. 2021;14:5364.
56. Lee D, Song M. MEXchange: A Privacy-Preserving BlockchainBased Framework for Health Information Exchange Using Ring Signature and Stealth Address. IEEE Access. 2021;9:158122–158139.

57. Huang H, Zhu P, Xiao F, Sun X, Huang Q. A blockchain-based scheme for privacy-preserving and secure sharing of medical data. Comput Secur. 2020;99:102010.
58. Zou R, Lv X, Zhao J. SPChain: Blockchain-based medical data sharing and privacy-preserving eHealth system. Inf Process Manag. 2021;58:102604.
59. Omar AA, Bhuiyan MZA, Basu A, Kiyomoto S, Rahman MS. Privacyfriendly platform for healthcare data in cloud based on blockchain environment. Future Gener Comput Syst. 2019;95:511–521.
60. Yang J, Onik MMH, Lee NY, Ahmed M, Kim CS. Proof-of-familiarity: A privacy-preserved blockchain scheme for collaborative medical decision-making. Appl Sci. 2019;9:1370.
61. Dwivedi AD, Srivastava G, Dhar S, Singh R. A decentralized privacypreserving healthcare blockchain for IoT. Sensors. 2019;19:326.
62. Zhang A, Lin X. Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. J Med Syst. 2018;42:140.
63. Miyachi K, Mackey TK. hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. Inf Process Manag. 2021;58:102535.
64. Huang Z, Guo Y, Huang H, Duan R, Zhao X. Analysis and Improvement of Blockchain-Based Multilevel Privacy-Preserving Location Sharing Scheme for Telecare Medical Information Systems. Secur Commun Netw. 2022;2022:1926902.
65. Tan L, Yu K, Shi N, Yang C, Wei W, Lu H. Towards Secure and Privacy-Preserving Data Sharing for COVID-19 Medical Records: A Blockchain-Empowered Approach. IEEE Trans Netw Sci Eng. 2022;9:271–281.
66. Zhao J, Wang W, Wang D, Wang X, Mu C. PMHE: A wearable medical sensor assisted framework for health care based on blockchain and privacy computing. J Cloud Comput. 2022;11:96.
67. de Moraes Rossetto AG, Sega C, Leithardt VRQ. An Architecture for Managing Data Privacy in Healthcare with Blockchain. Sensors. 2022;22:8292.
68. Zhang G, Yang Z, Liu W. Blockchain-based privacy preserving ehealth system for healthcare data in cloud. Comput Netw. 2022;203:108586.
69. Xu L, Lin M, Feng Y, Sun Y. BPDST: Blockchain-Based PrivacyPreserving Data Sharing on Thin Client for Electronic Medical Records. J Comput Inf Technol. 2022;29:235–250.
70. Upadhyay S, Kumar M, Kumar A, Karnati R, Mahommad GB, Althubiti SA, Alenezi F, Polat K. Feature Extraction Approach for Speaker Verification to Support Healthcare System Using Blockchain Security for Data Privacy. Comput Math Methods Med.n 2022;2022:8717263.
71. Lee TF, Chang IP, Kung TS. Blockchain-based healthcare information preservation using extended chaotic maps for HIPAA privacy/security regulations. Appl Sci. 2021;11:10576.
72. Wang B, Li Z. Healthchain: A privacy protection system for medical data based on blockchain. Future Internet. 2021;13:247.
73. Wu H, Dwivedi AD, Srivastava G. Security and Privacy of Patient Information in Medical Systems Based on Blockchain Technology. ACM Trans Multimed Comput Commun Appl. 2021;17:60.
74. Chen Y, Meng L, Zhou H, Xue G. A Blockchain-Based Medical Data Sharing Mechanism with Attribute-Based Access Control and Privacy Protection. Wirel Commun Mob Comput. 2021;2021:6685762.
75. Jia X, Luo M, Wang H, Shen J, He D. A Blockchain-Assisted PrivacyAware Authentication Scheme for Internet of Medical Things. IEEE Internet Things J. 2022;9:21838–21850.
76. Sarier ND. Privacy Preserving Biometric Authentication on the blockchain for smart healthcare. Pervasive Mob Comput. 2022;86:101683.

77. Wen H, Wei M, Du D, Yin X. A Blockchain-Based Privacy Preservation Scheme in Mobile Medical. Secur Commun Netw. 2022;2022:9889263.
78. Rao KR, Naganjaneyulu S. Permissioned Healthcare Blockchain System for Securing the EHRs with Privacy Preservation. Ing Des Syst Inf. 2021;26:393–402.
79. Luong DA, Park JH. Privacy-Preserving Blockchain-Based Healthcare System for IoT Devices Using zk-SNARK. IEEE Access. 2022;10:55739–55752.
80. Deshmukh V, Pathak S, Bothe S. MobEdge: Mobile blockchainbased privacy-edge scheme for healthcare Internet of Thingsbased ecosystems. Concurr Comput Pract Exp. 2022;34:e7210.
81. Ranjith J, Mahantesh K. Blockchain-based Knapsack System for Security and Privacy Preserving to Medical Data. SN Comput Sci. 2021;2:245.
82. Liu H, Crespo RG, Martínez OS. Enhancing privacy and data security across healthcare applications using Blockchain and distributed ledger concepts. Healthcare. 2020;8:243.
83. Zhou Z, Liu Y. Blockchain-Based Encryption Method for Internal and External Health Privacy Data of University Physical Education Class. J Environ Public Health. 2022;2022:7506894.
84. Ali A, Rahim HA, Pasha MF, Dowsley R, Masud M, Ali J, Baz M. Security, privacy, and reliability in digital healthcare systems using blockchain. Electronics. 2021;10:2034.
85. Zhang C, Xu C, Sharif K, Zhu L. Privacy-preserving contact tracing in 5G-integrated and blockchain-based medical applications. Comput Stand Interfaces. 2021;77:103520.
86. Zheng X, Zhao Y, Li H, Chen R, Zheng D. Blockchain-based verifiable privacy-preserving data classification protocol for medical data. Comput Stand Interfaces. 2022;82:103605.