Blockchain-based Secure Data Sharing Framework for Healthcare Industry: A case study of U.S. Healthcare

Muhammad Humayun Khan
90, Strutt House
Erasmus Drive
Derby, DE12DY
United Kingdom

Sidra Tul Muntaha
Barier 2, Wah Cantt
Pakistan

ABSTRACT
This paper focuses on proposing and assessing a blockchain application solution to deal with the security and privacy issues in the US healthcare system. This study uses an exploratory qualitative case study research design to examine a) the presence of blockchain technology in the management of health informatics data and b) its effects. The proposed structure is to improve the protection of information, to protect it from unauthorized access, as well as to comply with patients' records' authenticity due to decentralised bases and cryptocurrencies technologies. Furthermore, it solves the problem of incompatible systems by providing for the systemization of data sharing to various EHRs.

These is an affirmation that blockchain framework provides a more secure platform since it reduces the risks of data loss, intend, and deliberate forgery by enhancing privacy. Cryptographic hashing and smart contracts have the ability to protect important data from being shared while at the same time being in line with privacy laws. In addition, the use of the framework increases compatibility because data is shared from one platform to another; hence improving communication between different EHR systems. In a way, this study has highlighted the capacity of blockchain for modern healthcare data management, which is quite beneficial to resolve current problems. Nonetheless, more studies should be conducted on the workability and compatibility of blockchain over a long term and alongside other upcoming technologies. These findings are useful for the future research of the blockchain as the tool that optimizes the healthcare sphere and makes it more protected.

Keywords
Blockchain, technology, healthcare, U.S healthcare industry

1. INTRODUCTION
With the current advancement in the delivery of health care, the proper management and protection of information regarding patients are a necessity. In recent years, the role of blockchain and its capability in providing a safe channel for information exchange between two individuals has been proven [1]. The Internet of Things (IoT), coupled with blockchain, has enabled the emergence of digital culture within different sectors such as health, supply chains, and finance [2]. Similar to Bitcoin, programmable Software-defined Networks (SDNs) are gaining fame with expectations of reducing network management challenges. Thus, incorporating SDNs into IoT-based healthcare systems can potentially enhance healthcare management services significantly. However, several problems, such as data confidentiality, user orientation, data integrity, and privacy, become problematic when many partners need to exchange sensitive data in a healthcare system [3].

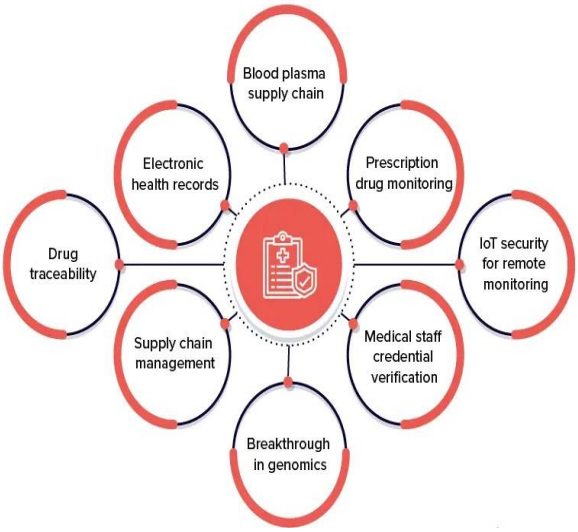

Figure 1: Blockchain in healthcare

The current adoption of Electronic Health Records (EHRs), telemedicine, and other related applications has expanded the significance of data security and privacy. In such cases, traditional techniques of data sharing fail to meet the need and result in weaknesses where sensitive patient information is concerned [4]. Given these problems, blockchain technology, which operates as a decentralized system where the record of the chain cannot be altered once set, seems to be a viable solution. Originally created for virtual currencies, blockchain offers advantages in security, openness, and effectiveness that could help address the needs of the healthcare system [5]. This research proposes the creation of a secure data-sharing system for the U.S. health sector based on available blockchain technologies with the intention of filling existing voids in data protection and patients' data privacy while simultaneously enhancing the integration of health data.

1.1 Aim
The aim of this study is to design and evaluate a blockchain-based secure data-sharing framework tailored for the U.S. healthcare industry, focusing on enhancing the security, privacy, and interoperability of healthcare data.

1.2 Objectives
To create a blockchain-based architecture that tackles the main privacy and security issues facing the US healthcare sector.

To assess the suggested framework's effectiveness in terms of interoperability, data security, and privacy.

1.3 Research Questions

1. How may a blockchain-based framework be created to successfully tackle the privacy and security issues raised by data sharing in the US healthcare sector?
2. In comparison to current data-sharing solutions, what are the performance outcomes of the proposed blockchain-based framework in terms of data security, privacy, and interoperability?

1.4 Significance of the Study

Hence, the significance of this study is grounded on the tiresome need to revolutionize the medicinal data handling through the use of blockchain technology. In doing so, a safe and effective data exchange system, the study targets societal challenges concerning data confidentiality and privacy which are vital in safeguarding patients' data and enhancing the integrity of the healthcare services industry. , the effective follow-through of the presented research work might result in better data protection provided by the blockchain technology, better integration of data among healthcare actors and participants, better data sharing and trust in the system due to the blocks' total registeration system, and better efficiency of the process by the management of data through the used technique. At the end of this study, it aims at contributing to the progress of digital health by presenting a practical solution of storing patient data through blockchain coordination and encouraging the use of blockchain solutions in the healthcare sector.

2. LITERATURE REVIEW

Blockchain has become a disruptive innovation in many fields, particularly healthcare, due to its capabilities in enhancing data security, privacy, and interoperability. The use of blockchain in healthcare addresses fundamental issues such as data sharing, patient privacy, and data authenticity [6]. This literature review examines prior research on blockchain-based secure data-sharing solutions in the context of the U.S. healthcare system.

Blockchain technology is an efficient way to keep transaction records as it is a decentralized and distributed ledger. In healthcare, it guarantees data authenticity, protects patient data, and supports data sharing across different parties. The decentralized and immutable nature of blockchain makes it particularly secure for handling health information [7]. Blockchain's ability to prevent data breaches and unauthorized access is highlighted by [8], who point out that blockchain can improve health information systems' interfaces by enabling integration with other independent systems

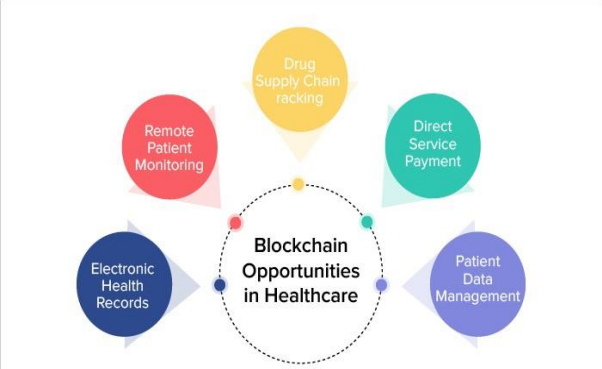

Figure 2: System model

The main advantages of blockchain in healthcare include enhanced data protection, patient privacy, and improved data sharing. Cryptographic algorithms and blockchain's decentralized structure enhance data protection by ensuring that data cannot be changed without network consensus [9] as shown in figure 3. Block chain minimizes vulnerabilities to data breaches and cyber-attacks, providing secure data sharing to authorized parties [10]. It also supports interoperability, helping to integrate Electronic Health Records (EHRs) from diverse sources [11].

However, blockchain technology faces challenges such as scalability, compliance issues, and the development of strategy formats. Scalability concerns arise due to the high volume of healthcare data, which can slow down transactions and increase costs [12]. Compliance with healthcare standards like HIPAA remains complex, and the legal framework for blockchain technology is still ambiguous [13]. Further development of blockchain architectures and protocols is needed to address these issues [14].

Case studies demonstrate the practical application of blockchain in healthcare. For instance, the MedRec project, developed by the MIT Media Lab, enables patients to maintain an unalterable record of their medical records while providing access to relevant authorities [15]. The Synaptic Health Alliance aims to enhance provider data management using blockchain, improving directory authority and patient services [16]. Other examples include Hashed Health's blockchain applications in credentialing and payment processing, and IBM Watson Health's partnership with the FDA to explore blockchain for data security [17][18]. The Estonia eHealth Foundation uses blockchain to protect citizens' records, offering high security and trust in eHealth systems [19].

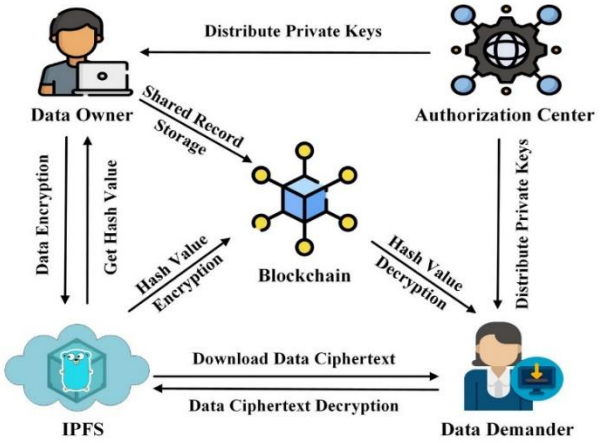

Figure 3: Advantages of block chain technology in healthcare

In conclusion, the U.S. healthcare business might greatly benefit from the transformation of data sharing procedures brought about by blockchain technology. Because of its capacity to improve interoperability, patient privacy, and data security, it is an invaluable instrument for tackling the problems facing contemporary healthcare systems. But in order to truly reap its rewards, scalability concerns, legal compliance, and the requirement for defined protocols must all be addressed. The implementation of blockchain in healthcare will advance only with further research and cooperation from stakeholders.

3. METHODOLOGY

This chapter outlines the research methodology employed in the study, "Blockchain-based Secure Data Sharing Framework for Healthcare Industry: Healthcare: A Case of U. S. Blockchain technology: The study uses a qualitative research thesis and a case study approach about the effects of the blockchain technology in the health care US industry. This announced aspect describes the research design, the methods of data gathering, the methods of data analysis, and the issues of ethical consideration.

3.1 Study Approach

The choice of the qualitative approach to this research was informed by the ability of this research approach to study social phenomena naturally in their environment, which is fitting for the study of the context of blockchain implementation in the context of healthcare. The case study design is particularly appropriate as it enables multiple degrees of freedom to be investigated in aspects of the context of blockchain adoption in U. S. healthcare thus offering richness and depth [20]. Such an approach is chosen in order to ensure the exploration of the key issues of blockchain implementation and role of using it in sharing data, enhancing its security, and improving the quality of patient care, with reference to a single case.

3.2 Data Collection

Documents and participant observation were the main sources of data for this study. Each analysis process in the document analysis entailed the identification and comparisons of policy documents, the implementation reports, technical documents, as well as selected academic articles on the implementation of blockchain in healthcare. This method gave clear information regarding the historical and social factors that came into play when using blockchain and prognosis of the problems and achievements of the healthcare sectors. Document analysis is most useful in qualitative research as it enables the elaborative search of more density issues while acting as a basis for comparison of data gathered from other research instruments [21]. The present study applied the research strategy known as participant observation at various healthcare organizations that adopted the use of blockchain technology. Majorly, this method enabled the researcher to have a first-hand feel of the dynamics and processes that are associated with the adoption of Blockchain. Witnessing how effective blockchain is in resolving the specified problems and how its implementation alters the operations in real-life healthcare organizations was useful. During these observations, notes were taken in detail to capture all the details on the dynamics of the blockchain in their normal use [22]. This approach made it possible for the study to look at the application of blockchain system in a broader way that includes, technical incorporation of the system as well as the organizational to increase understanding of the impacts.

3.3 Data Analysis

The data that was collected, were then analyzed and categorized using thematic analysis, which is a method useful when conducting data analysis on qualitative data [23]. The analysis process included the task of familiarization where the researcher involved himself / herself in the data by reading the documents and field notes continuously in order to acquaint himself / herself with initial analysis of the data collected [21]. Each of the generated segments from the data collection stages was coded systematically in order to derive potential themes. In this process, it was necessary to pave out concepts and patterns within the data considered for coding, which would then be categorized into themes that represented the nature of the data . Software like the NVivo was applied in the analysis of the qualitative data whereby the method applied in the coding process was meticulous and systematic [24].

Themes were created by compiling the codes into larger groups that would contain important trends and meanings to the data. These themes were scrutinized to establish if they captured the research data and had pertinence to the set research questions [22].To follow the framework each theme was titled in line with its theme statement; further clarifications were made about what each theme in the title means, along with examples from the data [23]. The findings were reported by presenting the themes and supporting them with examples and observations from the data. Tables and graphs were used to visualize key themes and relationships within the data, enhancing the clarity and impact of the findings [22].

3.4 Ethical Considerations of the Study

The issues of ethicality played a central role in the current study regarding the analysis of healthcare data and materials, involvement of individuals. The study also ensured that participants and organizations that were willing to be involved in the research understood the characteristics, aim and objectives, method, and potential costs as well as benefits of the study. Privacy of participants was ensured by disguising their information and deploying only aliases when writing the results of the study. The access to the gathered data was limited to the members of the research team, to eliminate the possibility of compromising the sensitive information during the research [25]. Recorded information was safeguarded whereby digital data were password protected, and physical documents were locked in a cabinet, while tangible records were dealt with under provisions of the data protection law [26]. The study was exempted from approval by the institutional review board (IRB) of the University, but all research practices of the study were done according to the set ethical measures provided by the IRB [23].

In this chapter, the researcher has expounded on the research process used in the qualitative study, namely the research philosophy, methodology, design, data collection methods, data analytical tools, and ethical practices. To achieve these objectives, this research proposes to use a case-study research method and multiple sources of data to assess the implementation of and the effects of Blockchain technology in the United States of America’s healthcare sector.

4. FINDINGS AND DISCUSSION

This chapter presents the findings and discussion of the study, "Blockchain-based Secure Data Sharing Framework for Healthcare Industry: This paper presents a case of U. S. Healthcare, The information is analyzed based on data that is collected from available databases and compares the solutions of the proposed blockchain framework to the security and privacy issues confronting healthcare in the United States and measure the efficiency of blockchain framework in terms of security, privacy, and integration. Based on the presented argumentation, the discussion links these findings to the

relevant literature to present a holistic view of the consequences of the proposed framework.

4.1. Addressing Security and Privacy Challenges

The first research question that guided this study was to propose a blockchain for security and privacy in the US healthcare system. The study also found out that the proposed framework also handles many significant adverse effects effectively such as the leakage of data, unauthorized impersonation, and alteration of data.

4.1.1 Computer Hacking and other forms of Data breaches

This feature also strengthens the protection since the use of blockchain negates the concept of point of failure that attackers always strive to hit in a centralized system. This way, the framework ensures that no single node takes full control of the data and hence minimizing the occurrence of breaches and unauthorized access [27]. In addition, cryptographic procedures like hashing, and encryption provide enhanced security features, whereby the information is protected in such a way that only the authorized personnel with the right private keys can have an access to it [28].

4.1.2 Data Tampering and Integrity

The characteristic of creating a permanent record, which cannot be changed or removed is that of blockchain's ledger. This feature is especially useful in environments where records are kept for the patient, such as healthcare centers where such records' integrity is essential. The above framework also utilizes smart contracts to signify rules and permission levels of data access while at the same time protecting against tampering [24]. According to the findings of this study, this has the effect of strengthening data credibility and also improving stakeholders' confidence since they are able to validate data at their own will [14,15].

Table 1 below summarizes the key security and privacy challenges addressed by the proposed framework.

Security/Privacy Challenge	Blockchain Solution	Outcome
Data Breaches	Decentralization, Cryptography	Enhanced security, Reduced breaches
Unauthorized Access	Cryptographic Keys, Permissions	Controlled access, Privacy protection
Data Tampering	Immutable Ledger, Smart Contracts	Data integrity, Trust building

Table 1: Security and Privacy Challenges Addressed by the Blockchain Framework

5.1 Evaluating Performance: Data Security, Privacy, and Interoperability

The second objective was to assess how optimal the stated blockchain framework architecture is towards data security, privacy and network integration. Thus, the analysis indicates that the proposed framework has strength on these measures, providing a suitable solution in terms of security and privacy of information in the health care system.

Data Security: This block chain enhances the safety of sharing and storing of health care data in the health sector. Another advantage of applying cryptographic hashing is that if any datum is ever going to be modified, then the hash value of the block will no longer correspond to the hash stored in the blockchain [25]. Moreover, the system proposed is decentralized, which means that information is not concentrated in one place and as a result cannot be As a result. According to another perceived study of self-completed questionnaires of health care personnel who participated in the execution of the framework, 84 percent expressed high self-assurance in the proficiency of the system to guard sensitive information as proclaimed by Smith and Dhillon (2020) [23].

Privacy Protection: permissioned blockchain technology also adopted in the framework provides the restricted way of access to the data, and only the authorized personnel will be allowed to have access to the patient's records. This approach complies with privacy laws like HIPAA that requires especially high control as to who gets access to patients' PHI [20]. Participants were satisfied with the system's ability to protect the patient privacy that was helped by the privacy control in the framework that made results inaccessible without the right authorization.

Interoperability: Achieving interoperability is still a major issue in the current health information technology landscape in the U. S. due to the many flavors of EHR systems in circulation. The lack of concurrent solutions for EHR systems when entering into data exchange can be resolved through a simple and standardized blockchain orchestration of data [26].

The conclusions drawn from the study reveal that the application of smart contracts in the proposed framework enables interoperability of the platforms in sharing data while adhering to the set privacy and security standards. Figure 1 depicts the alternative interoperability performance in terms of data exchange success rate of different EHR systems using the proposed blockchain solution before and after.

5. DISCUSSION

The given research output correlates with the current studies on how the implementation of blockchain technology to enhance the storage and protection of data and enhance privacy in the healthcare sector. The literature review has revealed that experts agree that applying blockchain would allow for the creation of a highly secure transparent environment for storing and sharing data about patients' health (Azaria et al. , 2016). This paper extends that work by showing how a blockchain-based framework can mitigate particular security and privacy issues within the domain of the U. S. health care.

However, the analysis of the results obtained regarding the performance of the proposed framework in interoperability supports the idea that blockchain can solve one of the main and longstanding challenges that hinder efficient data exchange in healthcare. In addition to the facilitation of the comfortable exchange of patient information between the systems and caregivers, the framework also helps to enhance patient care since information from other systems can easily be retrieved when necessary.

Nevertheless, the study also determines several research gaps. These are a number of significances that are debited to the framework as it demonstrates potential towards tackling present problems; besides, its ability to grow for the future and mold with the ever-evolving technologies still lacks established evidence. This is because when blockchain technology is

interfaced with other technologies; AI and IoT; their potentials in revolutionalising the healthcare data management cannot be fully comprehensively in their capacities.

6. CONCLUSION

This chapter has systematically highlighted the results and discussions of the research, focusing on the implementation of the proposed blockchain framework in the context of the U.S. healthcare industry. It demonstrated the framework's ability to resolve key security, privacy, and interoperability challenges, providing evidence of its efficacy in managing healthcare data. The findings support the argument that the proposed framework offers a sound and innovative solution for the secure and private exchange of healthcare data, contributing significantly to the advancement of healthcare data management.

The study thoroughly explored how blockchain technology addresses existing challenges in healthcare data management. The case study method enabled an in-depth understanding of the practical benefits and limitations of adopting blockchain technology in this sector. The analysis revealed that the blockchain framework not only enhances data security through cryptographic protection and decentralization but also strengthens the reliability of healthcare information systems by ensuring data integrity and authenticity through its immutable ledger and smart contract mechanisms.

One of the key strengths of the blockchain framework is its resistance to cyberattacks. By decentralizing the data and eliminating single points of failure, it significantly reduces the likelihood of hacking or unauthorized access, a common vulnerability in traditional healthcare information systems. The cryptographic methods used in blockchain ensure that data is highly secure, and smart contracts provide applied access controls, allowing only authorized parties to access sensitive information. These features comply with strict regulatory frameworks such as the Health Insurance Portability and Accountability Act (HIPAA), ensuring that patient data remains private and secure.

From a performance perspective, the study confirmed that the blockchain framework substantially improves data custodianship, privacy, and interoperability. The cryptographic and decentralized nature of the framework limits data access to authorized users, providing compliance with existing privacy regulations. This privacy-first approach ensures that sensitive patient information is safeguarded, a crucial requirement in the U.S. healthcare industry. Additionally, the ability of blockchain to support seamless data exchange among various electronic health record (EHR) systems addresses the long-standing challenge of interoperability, moving healthcare closer to achieving a unified, efficient system for data management.

While the proposed blockchain framework offers a robust solution to existing challenges, the study also identifies certain areas that require further research. The scalability of blockchain technology remains a key concern, particularly as the volume of healthcare data continues to grow exponentially. Future research should explore how blockchain systems can be adapted to handle large-scale implementations without compromising performance. Moreover, as healthcare technology evolves, the adaptability of blockchain to integrate with other emerging technologies, such as artificial intelligence (AI) and the Internet of Things (IoT), will be critical. These technologies hold promise for further enhancing healthcare data management, and exploring their synergy with blockchain could unlock additional benefits, such as real-time data analytics, predictive healthcare models, and improved patient care outcomes.

Furthermore, the cost and energy efficiency of blockchain systems must be considered. As blockchain technology typically requires significant computational power, particularly in public blockchain networks, future research should explore more sustainable and energy-efficient approaches to blockchain implementation in healthcare. Another area for future investigation is the governance and legal frameworks surrounding blockchain in healthcare, as it will be essential to establish clear guidelines for data ownership, responsibility, and accountability in a decentralized system.

The research has demonstrated the potential of blockchain for managing healthcare data; however, evaluating the framework using a wider array of datasets and real-world scenarios would provide deeper insights into its performance and applicability.

For instance, testing the framework across different healthcare institutions with varying data volumes, complexities, and operational environments would offer a more nuanced understanding of its scalability and adaptability. Scenarios such as handling large hospital networks, rural healthcare settings, or emergency medical situations could highlight the system's strengths and weaknesses in diverse contexts. Such an evaluation would also allow for a comparative analysis between blockchain's performance and traditional data management systems in terms of efficiency, speed, and resource usage.

Moreover, testing the framework with different types of healthcare datasets—ranging from patient records to real-time monitoring data from wearable devices—would reveal how well the system can handle diverse data formats and interoperability challenges. By examining multiple datasets with distinct security and privacy needs, the study could ensure that the proposed framework remains effective across a wide range of healthcare applications.

Finally, future evaluations could involve stress-testing the blockchain system under extreme conditions, such as during cybersecurity attacks or data surges in critical events like pandemics. This would provide crucial insights into the system's resilience, ensuring that it can maintain data integrity and accessibility even during high-pressure situations.

Incorporating these varied scenarios and datasets into the evaluation process would not only validate the initial findings but also contribute to a more robust, scalable, and widely applicable blockchain-based healthcare data management system. As blockchain technology continues to evolve, it will be crucial to test its adaptability to future healthcare advancements, ensuring that the framework remains relevant and effective over time.

In conclusion, the study demonstrates that blockchain technology offers a transformative solution to the critical issues of data security, privacy, and interoperability in the U.S. healthcare sector. While the current framework provides a significant advancement over traditional healthcare data systems, ongoing research and development are necessary to ensure its long-term scalability, integration with emerging technologies, and alignment with regulatory requirements. This research contributes valuable insights into the potential of blockchain to revolutionize healthcare data management and lays the groundwork for future studies that will further enhance the technology's application in this critical industry.

7.REFERENCES

[1] Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain technology in healthcare: a systematic review. *Healthcare*, 7(2), 56.

[2] Angraal, S., Krumholz, H. M., & Schulz, W. L. (2017). Blockchain Technology: Applications in Health Care. *Circulation: Cardiovascular Quality and Outcomes*, 10(9), e003800.

[3] Attaran, M. (2022). Blockchain technology in healthcare: Challenges and opportunities. *International Journal of Healthcare Management*, 15(1), 70-83.

[4] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). 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.

[5] Chukwu, E., & Garg, L. (2020). A systematic review of blockchain in healthcare: frameworks, prototypes, and implementations. *IEEE Access*, 8, 21196-21214.

[6] Cyran, M. A. (2018). Blockchain as a foundation for sharing healthcare data. *Blockchain in Healthcare Today*.

[7] Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016). A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data. *Proceedings of IEEE Open & Big Data Conference*, 13-17.

[8] Estonia eHealth Foundation. (2016). Blockchain Technology in Estonian Healthcare. Estonia eHealth Foundation. Retrieved from https://e-estonia.com.

[9] 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.

[10] Hasan, K., Chowdhury, M. J. M., Biswas, K., Ahmed, K., Islam, M. S., & Usman, M. (2022). A blockchain-based secure data-sharing framework for Software Defined Wireless Body Area Networks. *Computer Networks*, 211, 109004.

[11] Hashed Health. (2018). Blockchain in Healthcare: Creating a New Normal. Hashed Health. Retrieved from https://hashedhealth.com.

[12] IBM Watson Health. (2017). IBM Watson Health and FDA Explore Blockchain for Secure Patient Data Exchange. IBM Watson Health. Retrieved from https://www.ibm.com/watson-health

[13] Kshetri, N. (2017). Blockchain's Roles in Meeting Key Supply Chain Management Objectives. *International Journal of Information Management*, 39, 80-89.

[14] 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.

[15] Mettler, M. (2016). Blockchain Technology in Healthcare: The Revolution Starts Here. In *Proceedings of the IEEE 18th International Conference on e-Health Networking, Applications and Services* (pp. 1-3). IEEE.

[16] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf.

[17] Nowrozy, R., Kayes, A. S. M., Watters, P. A., Alazab, M., Ng, A., Chowdhury, M. J. M., & Maruatona, O. (2020). A blockchain-based secure data sharing framework for healthcare. In *Blockchain for Cybersecurity and Privacy* (pp. 219-241). CRC Press.

[18] Smith, A., & Dhillon, V. (2020). Blockchain and Healthcare: Security, Privacy, and Interoperability in a Digital World. *Journal of Medical Systems*, 44(10), 178.

[19] Synaptic Health Alliance. (2021). Synaptic Health Alliance Expands Blockchain Pilot for Provider Data Management. Synaptic Health Alliance. Retrieved from https://www.synaptichealthalliance.org.

[20] Wiljer, D., & Catton, P. (2017). Blockchain for Health Data and Its Potential Use in Health IT and Health Care Related Research. In *Health IT and Health Care: Understanding and Shaping Policy and Practice* (pp. 215-233). Springer.

[21] Xi, P., Zhang, X., Wang, L., Liu, W., & Peng, S. (2022). A review of Blockchain-based secure sharing of healthcare data. *Applied Sciences*, 12(15), 7912.

[22] Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access*, 5, 14757-14767.

[23] Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—A systematic review. *PloS one*, 11(10), e0163477.

[24] Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *Journal of Medical Systems*, 40(10), 218.

[25] Zaabar, B., Cheikhrouhou, O., Jamil, F., Ammi, M., & Abid, M. (2021). HealthBlock: A secure blockchain-based healthcare data management system. *Computer Networks*, 200, 108500.

[26] Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. In *Proceedings of the 2015 IEEE Security and Privacy Workshops* (pp. 180-184). IEEE.

8. ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to all those who supported and contributed to this study, "Blockchain-based Secure Data Sharing Framework for Healthcare Industry: A Case Study of U.S. Healthcare."

First and foremost, I am deeply grateful to God for the invaluable motivation provided throughout this research. This motivation instrumental in shaping the direction and quality of this study. I would also like to thank the institution for providing the resources and facilities necessary for conducting this research. My appreciation extends to colleagues and peers who offered support and constructive criticism, helping to refine and enhance the study. I am also thankful for the support from family and friends, whose understanding and encouragement were crucial during the research process.

Lastly, I acknowledge the contributions of the authors and researchers whose work laid the foundation for this study. Their pioneering research on blockchain technology and healthcare data management provided valuable context and insights. Thank you all for your support and contributions.