Engineering Technology
Open Access Journal

Juniper PUBLISHERS
key to the Researchers

Research Article
Volume 5 Issue 3 - September 2023
DOI: 10.19080/ETOAJ.2023.05.555663

Eng Technol Open Acc
Copyright © All rights are reserved by Raza Nowrozy

Towards Secure and Efficient Healthcare: A Blockchain-Based Study on Patient Data Access, Control and Interoperability

Raza Nowrozy[1]* and Lubna Meer[2]

[1]*Victoria University, 295 Queen Street, Melbourne, VIC, Australia*

[2]*Air University, Service Road E-9, Islamabad, Pakistan*

Submission: August 11, 2023; **Published: September 1, 2023**

***Corresponding author:** Raza Nowrozy, Victoria University, 295 Queen Street, Melbourne, VIC, 3000, Australia, E-mail: raza.nowrozy@live.vu.edu.au

Abstract

In the rapidly evolving digital healthcare landscape, the secure and efficient management of Electronic Health Records (EHRs) is paramount and of significant concern. Although patient data is always sensitive, its privacy and security can sometimes be compromised when shared with others, such as doctors, hospitals, pharmacists, researchers, etc. To address this challenge, this study introduces a Blockchain- Based Data Sharing (BBDS) Framework that leverages the Ethereum platform to innovate the access control and distribution of patient records. Emphasizing a decentralized architecture, the research delves into the integration of blockchain technologies like Ethereum Swarm for data storage and the employment of smart contracts for diverse functionalities. A comparative analysis underscores the blockchain's superiority in terms of security, data ownership and accessibility. However, some challenges were identified concerning patient-based interoperability. The study's implications for patient consent management, drug traceability, clinical trial security and incentivization further showcase the transformative potential of the BBDS framework for healthcare systems. The findings mark a significant step towards a unified, secure and transparent healthcare data management system, fostering industry collaboration and amplifying patient control over their records.

Keywords: Blockchain; Cloud Computing; Data Sharing; Privacy; Personally Identifiable Information; Role-Based Access Control; Context-Aware Access Control; Electronic Medical Records; Electronic Health Records

Abbreviations: EHRs: Electronic Health Records; EMR: Electronic Medical Records; MHI: Mandatory Health Insurance; VHI: Voluntary Health Insurance; MIS: Medical Information System; PPR: patient-provider relationship; BBDS: Blockchain-Based Data Sharing; ABIs: Application Binary Interfaces; GDPR: General Data Protection Regulation; EDI: Electronic Data Interchange

Introduction

Healthcare is a field deeply reliant on data. However, the fragmentation of patient records within Electronic Health Records (EHRs) can pose significant challenges, including poor coordination of care, as well as concerns regarding data availability, privacy, confidentiality and integrity. Traditional methods of health information exchange have proven inefficient [1], prompting exploration into blockchains as potential solutions [2-4]. By facilitating secure and authenticated data sharing among stakeholders in healthcare, blockchains have the potential to notably transform the industry with attributes like decentralization, transparency, interoperability and enhanced accessibility [5,6].

Despite the promise of cloud-based solutions and other innovative technologies, persistent data security issues remain a paramount concern [7-10]. Blockchain technology, with its inherent features of immutability and decentralized control might present a solution to these challenges [11,12]. Blockchains serve as repositories of information that are both distributed and decentralized, secured by various cryptographic primitives. Participants, including providers, patients and payers upload data to these chains in a manner that ensures security and authentication. This process yields comprehensive medical records accessible to those granted permission by the patients with smart contracts ensuring this access. There are several use cases or applications for utilizing blockchain in healthcare. These include the storage of Electronic Medical Records (EMR), accounting of services within the insurance system and the sale of prescription drugs [13]. The most evident and suitable application of blockchain technology in healthcare currently is the establishment of a unified healthcare database. Firstly, this would facilitate the collection and accessibility of each patient's complete medical history, encompassing prescribed examinations, treatment courses, diagnoses and test results. Secondly, it would consolidate information on the entire population, capturing data not only from the Mandatory Health Insurance (MHI) system but also from Voluntary Health Insurance (VHI) and records of paid consultations. Presently, records detailing disease diagnoses or prescribed treatments often reside solely on the physician's computer or within the Medical Information System (MIS). Creating a centralized healthcare database on the blockchain would enable a comprehensive view of a patient's history [14], benefitting all stakeholders involved.

The applications of blockchain in healthcare can be grouped into various types each boasting unique levels of access and security. Public [8,15-19], private [18-24] and consortium [25-34] blockchains each present diverse potential applications in healthcare [8,35,36]. Moreover, integrating smart contracts within the blockchain infrastructure provides avenues for conditional logic and automatic transactions further enhancing the security of patient record management [25,37]. These smart contracts can be categorized as registrar, Patient-Provider Relationship (PPR) and summary contracts, each serving specific roles in managing patient information [14].

While the broad application of blockchain in healthcare is promising, challenges such as privacy, confidentiality and data integrity persist [8,38]. The potential applications and use cases for blockchain in healthcare extend to storing EMR service accounting in insurance systems and monitoring prescription drug sales [13]. Constructing a unified healthcare database with blockchain emerges as an especially promising domain. Such a unified healthcare base could offer advantages to all stakeholders, requiring tasks like identifying blockchain technology features, analyzing existing projects, outlining benefits, devising storage strategies and pinpointing potential utilization challenges [14,39]. Various nations are at the forefront, pioneering blockchain projects to enhance the reliability and transparency of their healthcare systems. Notable examples include Estonia's e-Health Authority, the Netherlands' Prescrypt initiative, BitHealth in the U.S., Alibaba's initiatives in China, Israel's ”Medrec” project and undertakings by Russia's Ministry of Health [37,40-42].

Although it's feasible to store medical data without employing blockchain, this technology introduces additional layers of integrity and security. These include preventing unauthorized data modifications and access, standardizing data, collecting reliable statistics and paving the way for new research opportunities [35,36]. Nevertheless, blockchain does have its limitations. These encompass challenges with key management, theoretical data security concerns and a relative lack of extensive real-world application experience [11,12,43].

In conclusion, blockchain technology harbors the potential to transform healthcare by addressing a myriad of security concerns. Although still nascent, it could lay the foundation for considerable advancements in the sector. Blockchain promises a more secure and efficient means of storing medical data, unifying health registers and empowering patients to control their medical data, safeguard against manipulations and access high-quality medical advice and treatment.

Objectives

The research aimed to develop a data-sharing framework using blockchain technology, addressing the current challenges in healthcare data sharing and providing improved data access control and security compared to traditional methods.

Materials and Methods

Combining robust security with the technological benefits blockchain offers has paved the way to address numerous security concerns prevalent in cyberspace. This technology is progressively being embraced to furnish patients with enhanced and secure healthcare services. However, given that the technology is still in its nascent stages, further analysis and time are required for its optimization. Overall, blockchain lays the groundwork for significant advancements in healthcare. Employing blockchain can assist the sector in ensuring more secure and efficient medical data storage. Moreover, it can establish a unified health register for patients, accessible across various healthcare facilities, enabling professionals to assess a patient's history from the onset. Furthermore, blockchain can serve as a centralized repository for all medical records of a patient, encompassing MRI scans, X-rays and test results. Patients gain control over the dissemination of their medical data, safeguarding them from potential data manipulations and ensuring they receive optimal medical advice and treatment.

Emphasizing the research goal, various aspects were considered to recommend and implement a blockchain framework in the healthcare industry. This alignment brought every institution in line with blockchain technology [9,44]. To address patient concerns regarding data sharing, we examined a case study of My Health Records Australia, specifically focusing on its data breaches and privacy issues. Furthermore, our research aims to ensure accountability and enhance workflow automation by leveraging the inherent characteristics of blockchain technology.

Case Study: Australian My Health Records

The My Health Records (MHR) system consolidates all health information data in a secure location. Primary users of the MHR include medical professionals such as doctors, hospitals and pharmacists. For secondary purposes, the system can be accessed by researchers and others for academic research. (Figure 1) depicts the UML of MHR.

How to cite this article: Raza N, Lubna M. Towards Secure and Efficient Healthcare: A Blockchain-Based Study on Patient Data Access, Control and Interoperability. Eng Technol Open Acc. 2023; 5(3): 555663. DOI: 10.19080/ETOAJ.2023.05.555663

MHR Use Cases: User login, Write prescriptions, Recommend patients to specialists, View data, Delete data and Account locked, etc.

MHR Misuse Cases: Alter record data, Alter prescription data, Improper recommendation, Steal data, Erase data illegally, Flood system and Brute force attack, etc.

The "user login" use case is the initial step for accessing the system. The MHR employs authentication to ensure that the user has the appropriate authorization. Every actor interacting with the system must employ this use case to gain access [45]. Doctors, hospitals, pharmacists and researchers all use their authentication credentials to log into the system through this use case. Users input their login credentials, which the MHR system then verifies. If the input is correct, access is granted; otherwise, the system displays an "Incorrect details. Authentication failed." message. After three unsuccessful attempts, the system locks the user's account for 24 hours to prevent unauthorized access attempts, such as brute force attacks.

Use Case Description: User login - (Actors: Doctors, Hospitals, Pharmacists and Researchers)

i. Actors input their login credentials.

ii. Authentication details (username and password) are entered.

iii. The system verifies the provided input.

iv. If the username and password are correct, the system grants access.

Extensions: If login credentials are invalid:

i. The system cannot verify the actor's input and notifies the actor.

ii. The actor is allowed three attempts to provide accurate login details.

iii. After three incorrect attempts, the account is locked for 24 hours. The system notifies the actor and ends the use case (Figure 1).

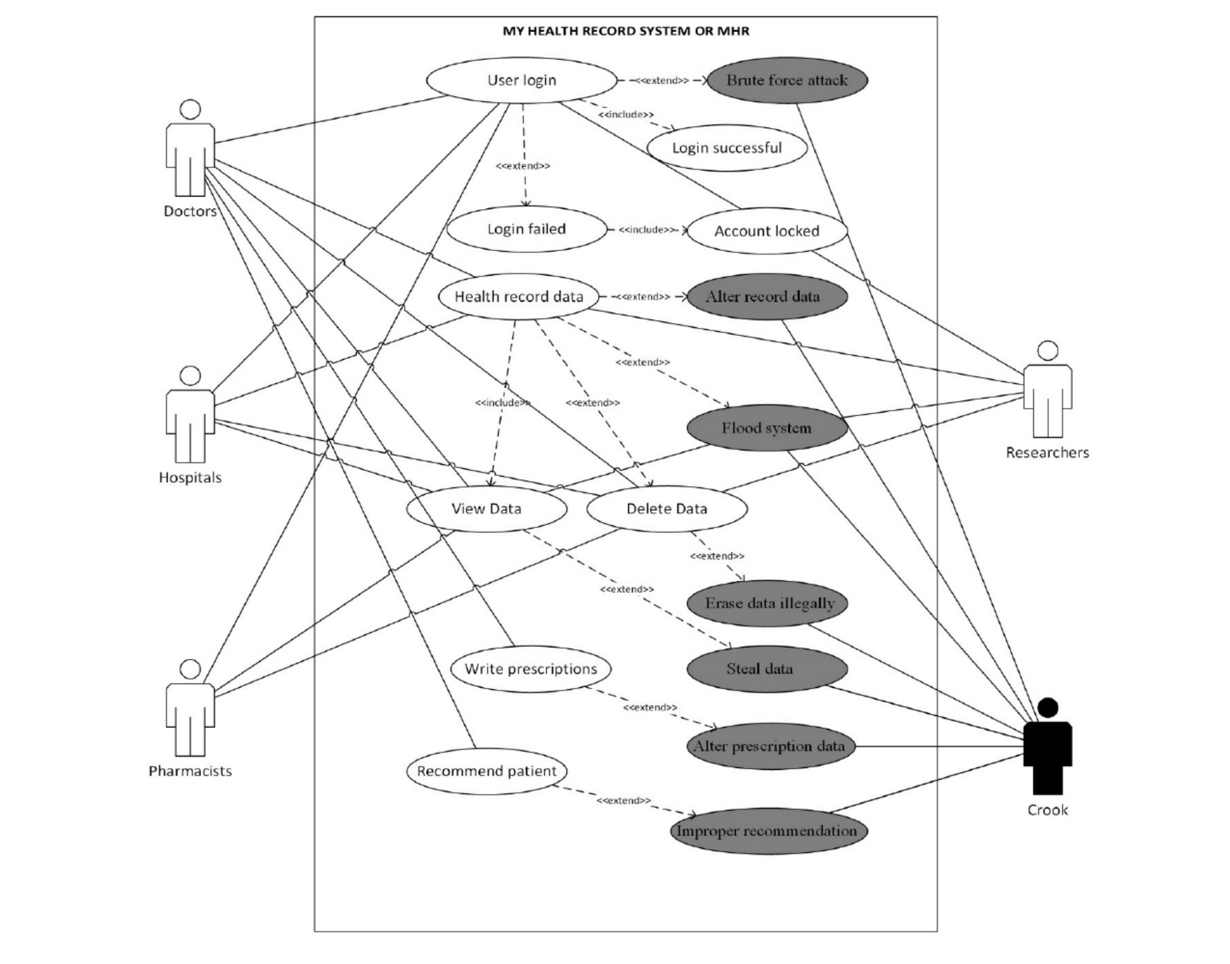
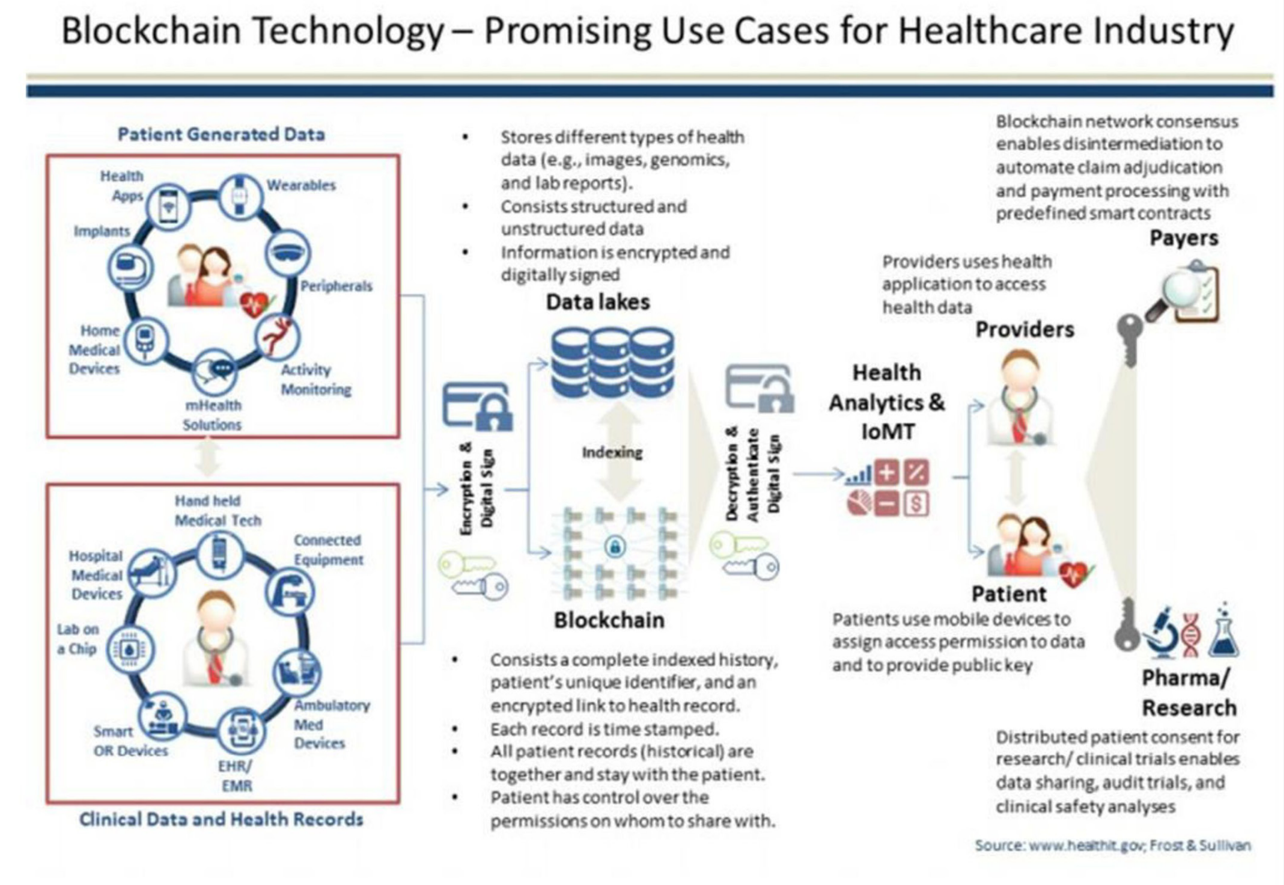


Figure 1: MHRUML Diagram.

MHR Security Requirements

Given the centralized data sharing model sensitive patient data can be easily manipulated or altered even potentially used against the patient. This could be achieved merely by possessing the database access credentials. Hence, block-based data sharing for MHR is intricately linked with technology vendors and the cybersecurity practices adopted by healthcare organizations. These practices might influence the system's design and implementation. By adopting a block-based data-sharing framework, MHR can ensure that its data-sharing system aligns with roadmap recommendations [46].

Blockchain-Based Data Sharing (BBDS) Framework



Blockchain Technology – Promising Use Cases for Healthcare Industry

- Stores different types of health data (e.g., images, genomics, and lab reports).
- Consists structured and unstructured data
- Information is encrypted and digitally signed

- Consists a complete indexed history, patient's unique identifier, and an encrypted link to health record.
- Each record is time stamped.
- All patient records (historical) are together and stay with the patient.
- Patient has control over the permissions on whom to share with.

Blockchain network consensus enables disintermediation to automate claim adjudication and payment processing with predefined smart contracts

Providers uses health application to access health data

Patients use mobile devices to assign access permission to data and to provide public key

Distributed patient consent for research/ clinical trials enables data sharing, audit trials, and clinical safety analyses

Source: www.healthit.gov; Frost & Sullivan

Figure 2: Blockchain framework for data sharing [47].

This is a data management system utilizing secure blockchain technologies that ensure patient data privacy while offering healthcare institutions easy access to the same information. The system leverages the Ethereum platform, a decentralized service that supports the deployment of applications by developers on custom foundations. Often, blockchains do not inherently offer adequate storage, leading to the need to store actual medical records on decentralized cloud storage platforms like Ethereum Swarm. Ethereum Swarm is a foundational layer of the Ethereum web3 stack serving as a distributed storage platform. A visual representation of the proposed data-sharing framework for healthcare stakeholders is presented in (Figure 2).

The graphic above illustrates a blockchain-based system designed for storing and sharing medical records, which entails collaboration between various healthcare entities and a central database [47] accessible via blockchain networks. Consortium blockchain technology [25] has been recognized as the most suitable network for the healthcare sector. This encompasses databases for healthcare service delivery institutions and research centers and supports functionalities like generating new information or retrieving existing data [26,48,49]. According to [50], healthcare stakeholders can access the consortium blockchain network utilizing cloud-based storage for secure data retention. The process to create new patient records encompasses storage by healthcare organizations in the cloud, data storage via blockchain in a home database and data transfer to the primary database through blockchain peer networks [46]. The information within the central security domain remains static and is open for review. Various architectural layers, interactions and components are integral to the proposed blockchain-based data-sharing model (Figure 3).

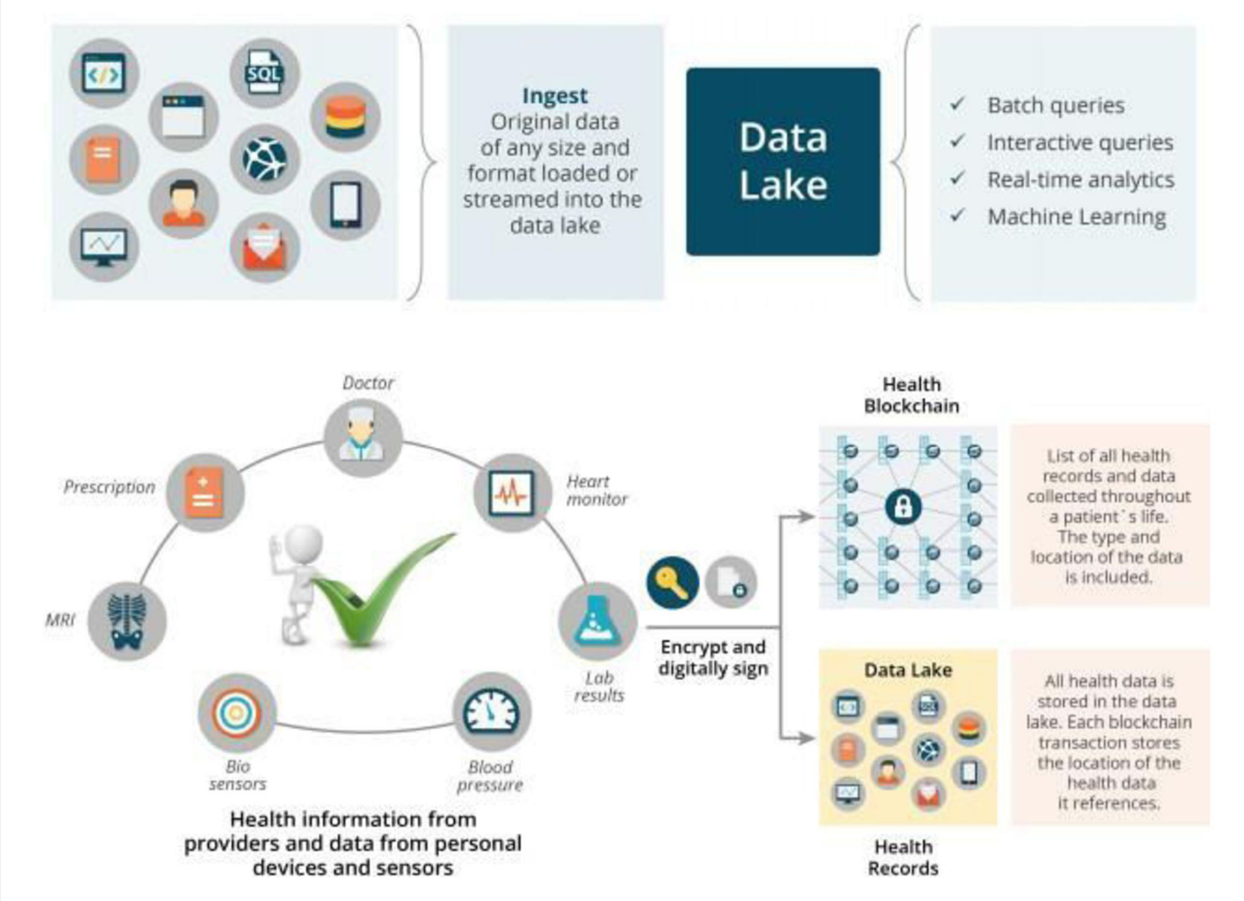

Ingest
Original data of any size and format loaded or streamed into the data lake
Data Lake
✓ Batch queries
✓ Interactive queries
✓ Real-time analytics
✓ Machine Learning
Doctor
Prescription
Heart monitor
MRI
Lab results
Bio sensors
Blood pressure
Health information from providers and data from personal devices and sensors
Encrypt and digitally sign
Health Blockchain
List of all health records and data collected throughout a patient`s life. The type and location of the data is included.
Data Lake
All health data is stored in the data lake. Each blockchain transaction stores the location of the health data it references.
Health Records

Figure 3: The layers in the Medical blockchain [47].

Medical records and data can reside off-blockchain in a scalable repository referred to as a data lake. These data lakes can house a variety of data types from textual documents to images and play a pivotal role in health investigations, feature extraction, optimal treatment decisions and preventative medicine research as depicted in (Figure 3). Enabled with functionalities like text analytics, machine learning and digital signatures data lakes maintain the authenticity and security of the information. Medical professionals produce digital signatures for health reports, subsequently encrypted and housed within the data lake. Each storage event prompts an update in the blockchain alerting the patient. Patients also have the facility to feed health data with digital signatures and encryption via mobile applications and sensors. (Table 1) details the EHR data transaction process showcasing how the proposed framework's blockchain fortifies data security as patient records become immutable post-creation. This exemplifies the mechanism of blockchain in safeguarding against unauthorized alterations.

Results

In the era of digital transformation managing healthcare data securely and efficiently has become imperative. Our proposed framework utilizes blockchain technologies to innovate the control and distribution of patient records. Based on the Ethereum platform this decentralized architecture allows developers to run customized applications while ensuring security and patient ownership of their records (Table 1).

Table 1: Illustrates the process of EHR data transaction.

Function	Scope	Design
Transaction	On-Chain	Exchange of data could be healthcare services, healthcare data and any other form of medical data that can be in a digital form.
Verification	On-Chain	The transaction will be verified instantly or will be queued in the pending transaction based on the defined parameters of the network to determine whether it is valid or not. In this case, nodes-the computes or servers in the network-determine if the transactions are legitimate. That is based on a set of rules the network has agreed on.
Structure	On-Chain	Each block will be identified by a hash, which will be a 256bit number, created using an algorithm agreed upon by the network. All block will contain a header, A reference to the previous block's hash and a transaction group. The sequence of Inked hashes creates a secure, interdependent chart.
Validation	On-Chain	Only validated blocks will be added to the blockchain. The most accepted form of validation for open source blockchains is proof of work (POW)-the solution to a mathematical puzzle derived from the block's header. Health researchers and medical institutes can provide this POW.
Blockchain Mining	On-Chain	Health researchers and medical institutes try to 'solve' the block by fitting multiple blocks to the chain until the solution satisfies a network-wide target. That is called -proof of work- because correct answers cannot be falsified. The appropriate level of computing power was drained in solving must prove potential solutions.
The Chain	On-Chain	Miners that solved the puzzle are rewarded when a block is validated and the block is then distributed through the network. Each node adds the block to the majority chain, which is the network immutable and auditable blockchain.
Built-In-Defense	On-Chain	If a malicious block is added to the blockchain, the hash function of that block and all the block following it will change. The other nodes will also detect these changes and will reject the block from being added to the majority chain, preventing corruption.
Communication	On-Chain	In the Hyperlinked Fabric blockchain, it functions as a back end with front-end applications to communicate with the network. SDK helps manage communication between front-end and back-end, such as Nodejs SDK and Java SDK. SDK provides a way to execute user chain code, carry out transactions on the network, monitor events, etc.
Data Storage	On-Chain	After validation and authentication in the chain, the data will then be stored in the Data Lakes

Although most blockchain implementations like Bitcoin inherently lack sufficient storage for large data such as medical records, our system integrates decentralized cloud storage solutions like Ethereum Swarm. This offers a robust platform for distributed data storage allowing pseudonym-masked entities within the blockchain to validate and execute transactions. The (Table 1) illustrates the process of EHR data transaction, showcasing how the blockchain aids in securing the data-given that patient records cannot be altered once created. This demonstrates the process of the blockchain securing the integrity of the entity.

Within Ethereum two types of accounts exist: contract and externally owned accounts. Both are defined by key pairs and indexed by 20-byte addresses enabling users to interact with the blockchain upon account creation. These accounts function as network entities and form the backbone of Ethereum's operations. One of the primary benefits of adopting Ethereum is its adaptability and flexibility. This allows for the development of diverse applications such as My Health Records. Ethereum's blockchain, comprising transaction blocks and smart contracts employs a proof-of-work algorithm to achieve a tamper-resistant consensus across its network nodes. Consequently, it ensures that in our proposed framework blockchain data remains unchangeable providing an unmatched security level.

Representing self-executing computer programs, smart contracts on the Ethereum blockchain trigger actions automatically when specific conditions align. They offer a multitude of programmable functions permitting users to interact through Application Binary Interfaces (ABIs). User-initiated transactions pave the way for various functionalities including request handling, data transmission and access control. A standard Ethereum transaction is a sophisticated data packet transferring ethers (Ethereum's native tokens) between accounts. In our proposed framework the data field is uniquely designated for declaring request IDs, streamlining data request transactions for cloud storage.

Blockchain For Secure Management of Electronic Health Records (EHRs)

By leveraging Enterprise Ethereum, the medical community can share data both securely and methodically. This strategy fortifies the safeguarding of patient data and privacy, granting physicians access to exhaustive medical histories. Additionally, it supports the scientific community by facilitating data sharing for research advancement.

Impact Of Blockchain on Patient Consent Management

This technology bestows structured data ownership with inherent permission tiers. While patients cannot modify specific medical entries, they possess the authority to regulate their records' access, selectively disseminating data to diverse healthcare stakeholders.

Impact Of Blockchain On Traceability Of Drugs

The clarity and interoperability of Enterprise Ethereum amplify the accountability and protection of drug supply chain operations enabling pharmaceutical firms to monitor products from inception to end-users efficiently.

Blockchain's Influence on Data Security In Clinical Trials

Ethereum mitigates the risk of data deceit through its consensus mechanism and centralized designs, delivering proof of existence and authentication validation. This cultivates confidence in trial outcomes ensures data's veracity and encourages cooperation within the research sphere.

Incentivization: Smart contracts facilitate the inception of micropayments to motivate patient actions. These contracts can distribute rewards for adhering to designated treatment regimens or contributing data for clinical exploration.

Summary

The insights underline the potential of a Blockchain-Based Data Sharing (BBDS) Framework for the secure exchange of healthcare data. The proposed system heralds a significant advancement in security offering robust defense against prevalent attacks, ensuring confidentiality and data accuracy and presenting features like tamper- evident data and storage space repurposing. The suggested BBDS Framework for My Health Record Australia is geared towards bolstering security, amalgamating data requestors and vouching for data integrity via blockchain infrastructure. It signifies a stride toward a consolidated solution, bridging the Australian government, MHR, patients, healthcare experts and other stakeholders.

Discussion

This study confirms the use of blockchain for secure and efficient healthcare data emphasizing a contrasting analysis between the blockchain mechanism and conventional systems. It also sheds light on the potential pathways blockchain offers when the BBDS framework discussed is applied to the healthcare system.

Security

Collectively one can infer that blockchain offers enhanced security for data sharing. G [2] reported that patient-driven interoperability achieved through blockchain technology, presents new challenges for security and data privacy. In contrast, [43,51-55] viewed it as a valuable tool that enhances the security of the data-sharing mechanism. Moreover, [56] highlighted blockchain as an emerging technology that offers superior data sharing security due to its transparency. This transparency is instrumental in tracing cyber-attacks given its capability to furnish vital audit information [57] also posited that blockchain's intimate interaction with role-based access controls facilitates secure data transactions and tailored access within organizations. The enforcement of the General Data Protection Regulation (GDPR) mandates institutions accessing such information to fortify their security by adopting stringent data access control policies in line with GDPR guidelines and operational efficacy [58]. Blockchain evidently provides superior privacy and security provisions for data owners as per literature survey cited in introduction section. The articles [2,51-55,59] also recognized blockchain technology as crucial in bolstering the cases for digital asset data ownership.

Data Ownership

This study posits that data ownership within the blockchain-supported framework in the healthcare sector is contingent upon the framework's intricate details. Data interoperability emerges as a pivotal indicator of data ownership within the blockchain system. Those with maximal data interoperability in a data-sharing framework possess data ownership. In the healthcare domain data ownership concerns are a primary deterrent to blockchain's adoption. Per the patient-driven data interoperability model for data sharing [2] both patients and institutions share data ownership. However, in the proposed framework data ownership is solely vested in the institution.

Data Breach

Stephen &Alex [60] emphasized that data ownership in blockchain is more robust compared to other alternatives especially in consortium and private blockchain setups. The amalgamation of trust, transparency, robust data ownership and data access control renders it a compelling choice for large-scale implementation. Yet, inherent limitations of blockchain technology act as impediments to its universal adoption. In a similar vein, [61] endorsed blockchain as unparalleled in ensuring data ownership noting its ability to return data ownership to users while allowing them the discretion over data sharing [4]. Presently, GDPR mandates businesses in the healthcare realm to bolster the security of systems utilizing blockchain technology. This enhancement amplifies the security quotient of electronic databases that store and transmit both personal and impersonal patient data granting patients data ownership rights [58]. Additionally, the healthcare system's design takes into account the myriad interactions different healthcare organizations have with the centralized database accessed via blockchain networks. The standard components of a blockchain system encompass databases for clinics and healthcare entities like small and large hospitals. These hospitals primary users of the blockchain-empowered healthcare system, either generate new data or retrieve extant information from the healthcare database. All these databases interconnect courtesy of blockchain technology aided by super peers enabling P2P engagement with other networked institutions.

Accessibility

The most optimal blockchain networks for a healthcare system accessible by numerous organizations are typically consortium or public blockchains. Concurrently the clinical database serves as the localized data repository for a given healthcare entity. Subsequently this data migrates to the central healthcare database which could operate at city, district or national levels, contingent upon the project's scope. Ideally this central database would leverage cloud- based storage facilitating the accommodation of voluminous data. The process of creating a new patient record involves a healthcare entity be it small or large generating data. This data is then stored in the local database via blockchain and eventually transferred to the central database through the blockchain's P2P network. The central database's content remains unalterable and always available for audit trails.

However, blockchain challenges persist. G [2] undertook research discussing blockchain's interoperability issue, revealing a growing trend of patient-centric interoperability via conventional Electronic Data Interchange (EDI) mechanisms employed in healthcare settings like hospitals and laboratories. While patient interoperability was deemed advantageous, it gave rise to privacy and security qualms owing to augmented access to patient data. This underscores the obstacles linked with patient-driven interoperability in the context of data sharing and patient engagement related to their health records. Consequently, the BBDS framework, inspired by Shen, Guo and Yang [55], calls for the translation of healthcare data records into immutable information stored in an appropriate blockchain-supported database. This paves the way for innovative solutions addressing the prevalent challenges of institutional interoperability in healthcare, integrating patient-centric interoperability via blockchain.

Conclusion

The integration of blockchain technology within healthcare data management offers a promising advancement toward enhanced security, transparency, data ownership and accessibility. This research has elucidated blockchain's potential in several key areas:

Security: By leveraging cryptographic principles and decentralized consensus mechanisms the proposed BBDS framework demonstrates superior security capabilities compared to conventional systems in alignment with GDPR guidelines [2,58].

Data Ownership: Through a patient-driven interoperability framework blockchain establishes a balanced data ownership model empowering both patients and institutions [2].

Data Breach Prevention: The study underscores the robustness of blockchain in preventing data breaches especially within consortium and private blockchain systems [60].

Accessibility: By utilizing various blockchain networks the research emphasizes the potential for fostering a seamless flow of information within the healthcare system addressing challenges associated with patient-based interoperability [2,55].

While the results are promising certain limitations and challenges such as barriers related to patient-based interoperability, emerged. Future research could prioritize resolving these barriers and investigating how to adapt blockchain-based systems for diverse healthcare settings. Moreover, the ramifications of blockchain on patient consent management, drug traceability, data security during clinical trials and incentivization expand the horizons for its implementation in healthcare [4]. In summation, this study marks a significant stride toward a unified healthcare data management solution, bridging the gap between patients, healthcare professionals and other stakeholders. Inspired by Shen, Guo and Yang, the proposed BBDS framework [55] heralds a transformative era for healthcare, bolstering security, integrity and collaboration within the sector. The continued exploration and development of blockchain applications in healthcare are essential for tapping into the full potential of this game-changing technology.

References

1. Pandey AK, Khan AI, Abushark YB, Alam MM, Agrawal A, et al. (2020) Key issues in healthcare data integrity:Analysis and recommendations. IEEE Access 8: 40612-40628.

How to cite this article: Raza N, Lubna M. Towards Secure and Efficient Healthcare: A Blockchain-Based Study on Patient Data Access, Control and Interoperability. Eng Technol Open Acc. 2023; 5(3): 555663. DOI: 10.19080/ETOAJ.2023.05.555663

2. Gordon WJ, Catalini C (2018) Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. Computational and structural biotechnology journal 16: 224-230.

3. Nepal S, Ranjan R, Choo KKR (2015) Trustworthy processing of healthcare big data in hybrid clouds. IEEECloud Computing 2(2):78-84.

4. Shen B, Guo J, Yang Y (2019) Medchain: Efficient healthcare data sharing via block chain. Applied sciences 9(6):1207.

5. Mettler M (2016) Blockchain technology in healthcare: The revolution starts here. 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), pp. 1-3.

6. Siyal AA, Junejo AZ, Zawish M, Ahmed K, Khalil A, et al. (2019) Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. Cryptography 3(1): pp. 3.

7. Ribitzky R, Broedl U, Mcfarlane C, Clauson KA (2018) Data Sharing? The Case for Blockchain at the GlobalConvergence of Healthcare, Life sciences, and Consumer Markets. Blockchain in Healthcare Today.

8. Yaqoob I, Salah K, Jayaraman R, Al-Hammadi Y (2021) Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Computing and Applications pages 34(7): 11475-11490.

9. Miyachi K, Mackey TK (2021) hocbs: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. Information Processing & Management 58(3): 102535.

10. Ullah A, Azeem M, Ashraf H, Alaboudi AA, Humayun M, et al. (2021) Secure healthcare data aggregation andtransmission in IOT- a survey. IEEE Access 9: 16849-16865.

11. Taylor PJ, Dargahi T, Dehghantanha A, Parizi RM, Choo KKR (2019) A systematic literature review of Blockchain cyber security. Digital Communications and Networks 6(2): 147-156.

12. Angraal S, Krumholz HM, Schulz WL (2017) Blockchain technology: applications in health care. Circulation: Cardiovascular quality and outcomes 10(9): 3800-3800.

13. Ouaddah A, Elkalam AA, Ouahman AA (2016) FairAccess: a new Blockchain-based access control framework for the Internet of Things. Security and Communication Networks 9(8): 5943-5964.

14. Ekblaw A, Azaria A, Halamka JD, 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: 1-13.

15. Hasselgren A, Kralevska K, Gligoroski D, Pedersen SA, Faxvaag A (2020) Blockchain in healthcare and health sciences-a scoping review. International Journal of Medical Informatics 134: 104040.

16. Abu-Elezz I, Hassan A, Nazeemudeen A, Househ M, Abd-Alrazaq A (2020) The benefits and threats of blockchain technology in healthcare: A scoping review. International Journal of Medical Informatics 142: 104246.

17. Capece G, Lorenzi F (2020) Blockchain and healthcare: Opportunities and prospects for the ehr. Sustainability 12(22): 9693.

18. Mehta S, Grant K, Ackery A (2020) Future of blockchain in healthcare: potential to improve the accessibility, security and interoperability of electronic health records. BMJ Health & Care Informatics 27(3): e100217.

19. Abdellatif AA, Al-Marridi AZ, Mohamed A, Erbad A, Chiasserini CF, et al. (2020) sshealth: toward secure, blockchain-enabled healthcare systems. IEEE Network 34(4): 312-319.

20. Soltanisehat L, Alizadeh R, Hao H, Choo KKR (2020) Technical, temporal, and spatial research challengesand opportunities in blockchain-based healthcare: A systematic literature review. IEEE Transactions on Engineering Management 70(1):353-368.

21. Wazid M, Bera B, Mitra A, Das AK, Ali R (2020) Private blockchain-envisioned security framework for AI-enabled IOT-based drone-aided healthcare services. In Proceedings of the 2nd ACM MobiCom workshop on drone assistedwireless communications for 5G and beyond, pp. 37-42.

22. Ghazal TM, Hasan MK, Abdullah SNHS, Bakar KAA, Al Hamadi H (2022) Private block chain-based encryption framework using computational intelligence approach. Egyptian Informatics Journal 23(4): 69-75.

23. Reda M, Kanga DB, Fatima T, Azouazi M (2020) Blockchain in health supply chain management: State of art challenges and opportunities. Procedia Computer Science 175: 706-709.

24. Anitha Kumari K, Padmashani R, Varsha R, Upadhayay V (2020) Securing internet of medical things (Iomt) using private blockchain network. Principles of Internet of Things (IOT) Ecosystem: Insight Paradigm pp. 305-326.

25. Xu B, Xu LD, Wang Y, Cai H (2022) A distributed dynamic authorization method for internet+ medical & healthcare data access based on consortium blockchain. Enterprise Information Systems 16(12): 1922757.

26. Purohit S, Calyam P, Alarcon ML, Bhamidipati NR, Mosa A, et al. (2021) Honestchain: Consortium blockchain for protected data sharing in health information systems. Peer-to-peer Networking and Applications 14(5): 3012-3028.

27. Ni W, Huang X, Zhang J, Yu R (2019) Healchain: A decentralized data management system for mobile healthcare using consortium blockchain. In 2019 Chinese Control Conference (CCC), Guangzhou, China, pp. 6333-6338.

28. Alsayegh M, Moulahi T, Alabdulatif A, Lorenz P (2022) Towards secure searchable electronic health records using consortium blockchain. Network 2(2): 239-256.

29. Thamrin A, Xu H (2021) Hierarchical cloud-based consortium blockchains for healthcare data storage. In 2021 IEEE 21st International Conference on Software Quality, Reliability and Security Companion (QRS-C), Hainan, China, pp. 644-651.

30. Wang Y, Zhang A, Zhang P, Qu Y, Yu S (2021) Security-aware and privacy-preserving personal health record sharing using consortium blockchain. IEEE Internet of Things Journal 9(14): 12014-12028.

31. Jiang S, Wu H, Wang L (2019) Patients-controlled secure and privacy-preserving ehrs sharing scheme based on consortium blockchain. In 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, pp. 1-6.

32. Li C, Liu J, Qian G, Wang Z, Han J (2022) Double chain system for online and offline medical data sharingvia private and consortium blockchain: A system design study. Frontiers in Public Health 10: 1012202.

33. Du M, Chen Q, Chen J, Ma X (2020) An optimized consortium blockchain for medical information sharing. IEEE Transactions on Engineering Management 68(6): 1677-1689.

34. Javed IT, Alharbi F, Bellaj B, Margaria T, Crespi N, et al. (2021) Health-id: A blockchain-based decentralizedidentity management for remote healthcare. In Healthcare 9(6): 712.

35. Hölbl M, Kompara M, Kamišalić A, Zlatolas LN (2018) A systematic review of the use of Blockchain in healthcare. Symmetry 10(10): 470-470.

36. Dammak B, Turki M, Cheikhrouhou S, Baklouti M, Mars R, et al. (2022) Lorachaincare: An iot architecture integrating blockchain and lora network for personal health care data monitoring. Sensors 22(4): 1497.

37. Carson B, Romanelli G, Walsh P, Zhumaev A (2018) Blockchain beyond the hype: What is the strategic business value. McKinsey & Company.

38. Kim KK, Joseph JG, Ohno-Machado L (2015) Comparison of consumers' views on electronic data sharingfor healthcare and research. Journal of the American Medical Informatics Association 22(4): 821-830.

39. Mettler M (2016) Blockchain technology in healthcare: The revolution starts here. In 2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom), Munich, Germany pp. 1-3.

40. Luu L, Narayanan V, Baweja K, Zheng C, Gilbert S, et al. (2015) Scp: A computationally-scalable byzantine consensus protocol for blockchains. Cryptology ePrint Archive.

41. Mcghin T, Choo KKR, Liu CZ, He D (2019) Blockchain in healthcare applications: Research challenges and opportunities. Journal of Network and Computer Applications 135: 62-75.

42. Kikitamara S, Van Eekelen MCJD, Doomernik DIJP (2017) Digital identity management on Blockchain for open model energy system. Unpublished Masters thesis-Information Science.

43. Peterson K, Deeduvanu R, Kanjamala P, Boles K (2016) A Blockchain-based approach to health information exchange networks. Proc. NIST Workshop Blockchain Healthcare 1: 1-10.

44. Theodouli A, Arakliotis S, Moschou K, Votis K, Tzovaras D (2018) On the design of a Blockchain- based system to facilitate Healthcare Data Sharing. 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, USA pp. 1374-1379.

45. Bhuiyan M, Haque F, Shabnam L (2018) Integration of organisational models and UML Use Case diagrams. Journal of Computers 13(1): 1-18.

46. Xia Q, Sifah E, Smahi A, Amofa S, Zhang X (2017) BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. Information 8(2): 44-44.

47. Chartier-Rueg T, Zweifel T (2017) Blockchain, leadership and management: business as usual or radical disruption. EUREKA: Social and Humanities 4: 76-110.

48. Tanriverdi M (2020) A systematic review of privacy-preserving healthcare data sharing on blockchain. Journal of Cybersecur Inf Management, 5(2-1): 31-37.

49. Hussien HM, Yasin SM, Udzir NI, Ninggal MIH, Salman S (2021) Blockchain technology in the healthcare industry: Trends and opportunities. Journal of Industrial Information Integration 22: 100217.

50. Guo R, Shi H, Zhao Q, Zheng D (2018) Secure attribute-based signature scheme with multiple authorities for Blockchain in electronic health records systems. IEEE Access 6: 11676-11686.

51. Patel V (2018) A framework for secure and decentralized sharing of medical imaging data via Blockchain consensus. Health informatics journal 25(4): 1398-1411.

52. Omar A, Basu A, Rahman MS, Kiyomoto S (2017) Medibchain: A Blockchain based privacy preserving platform for healthcare data. In International conference on security, privacy and anonymity in computation,communication and storage, pp. 534-543.

53. Vora J, Nayyar A, Tanwar S, Tyagi S, Kumar N, et al (2018) BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records. IEEE Globecom Workshops, Abu Dhabi, United Arab Emirates, pp. 1-6.

54. Chen Y, Ding S, Xu Z, Zheng H, Yang S (2019) Blockchain-based medical records secure storage and medical service framework. Journal of medical systems 43(1): 1-5.

55. Shen B, Guo J, Yang Y (2019) MedChain: Efficient Healthcare Data Sharing via Blockchain. Applied Sciences 9(6): 1207.

56. Gaetani E, Aniello L, Baldoni R, Lombardi F, Margheri A, et al. (2017) Blockchain-based database to ensure data integrity in cloud computing environments, Bengaluru, India.

57. Solanki N, Huang Y, Yen IL, Bastani F, Zhang Y (2018) Resource and role hierarchy based access control for resourceful systems. 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Tokyo, Japan, 2: 480-486.

58. Zheng X, Mukkamala RR, Vatrapu R, Ordieres-Mere J (2018) Blockchain-based personal health data sharing system using cloud storage. 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services(Healthcom), Ostrava, Czech Republic pp. 1-6.

59. Peterson K, Deeduvanu R, Kanjamala P, Boles K (2016) A Blockchain-based approach to health information exchange networks. Proc. NIST Workshop Blockchain Healthcare 1: 1-10.

60. Stephen R, Alex A (2018) A Review on BlockChain Security. IOP Conference Series: Materials Science and Engineering, Kerala, India 396: 12030.

61. Dias JP, Reis L, Ferreira HS, Martins A (2018) Blockchain for access control in e-health scenarios. arXiv preprint arXiv:1805.12267.

How to cite this article: Raza N, Lubna M. Towards Secure and Efficient Healthcare: A Blockchain-Based Study on Patient Data Access, Control and Interoperability. Eng Technol Open Acc. 2023; 5(3): 555663. DOI: 10.19080/ETOAJ.2023.05.555663