Review Open Access

Interoperability and Standards in Blockchain-based EHR

Hossien Aghahosseini [1], Mehdi Sakhaei-nia [1*]

1. Computer Engineering Department, Engineering Faculty, Bu-Ali Sina University, Hamedan, Iran

Abstract

Blockchain technology offers a decentralized database that enables the registration and maintenance of electronic health records (EHRs) through the implementation of encryption policies to ensure privacy. The inherent properties of decentralization and immutability in blockchains make them a practical choice for serving as a database for recording EHRs. Given that EHR files are typically generated by various entities such as hospitals, laboratories, clinics, and mobile applications, it is possible to store each set of collected data in separate blockchains adhering to different standards. However, due to the requirement for real-time access to medical records and concerns surrounding confidentiality and privacy, it is imperative that EHRs registered on different platforms are able to interact with one another online. Therefore, interoperability becomes a fundamental necessity for blockchain-based EHR systems. This paper aims to survey existing research on the implementation of interoperability in EHRs using blockchain technology. The study's findings suggest that achieving a comprehensive solution involves ensuring that all stakeholders follow standardized EHR protocols when recording information. Furthermore, it is advised to use cloud databases for storing large-scale EHR data, while limiting blockchain data storage to identity information and maintaining the integrity of cloud-stored data. To effectively enforce these processes, blockchain smart contracts are utilized. By employing these mechanisms, blockchain can serve as a suitable platform for recording and maintaining interoperable EHRs. Additionally, a detailed multi-layer software architecture is a common practice in the field, even though there is no consensus on the role of 3rd party auditors in it.

Keywords interoperability, blockchain, EHR

1. Introduction

Electronic Health Records (EHRs) refer to the digitized versions of patients' medical records, encompassing comprehensive information such as treatment history, medical prescriptions, radiology images, laboratory results, and allergies. EHRs are accessible online and patient-centric records while maintaining strict confidentiality. It is imperative that authorized users have the ability to real-time access and modify their own EHR data [1].

EHRs should be designed in such a way that they can be shared between different healthcare centers to improve coordination between centers and thus improve the quality of health care. [2]

The design of EHRs should facilitate seamless sharing between different healthcare centers to enhance coordination and improve the overall quality of healthcare [2].

* Correspondence:
sakhaei@basu.ac.ir

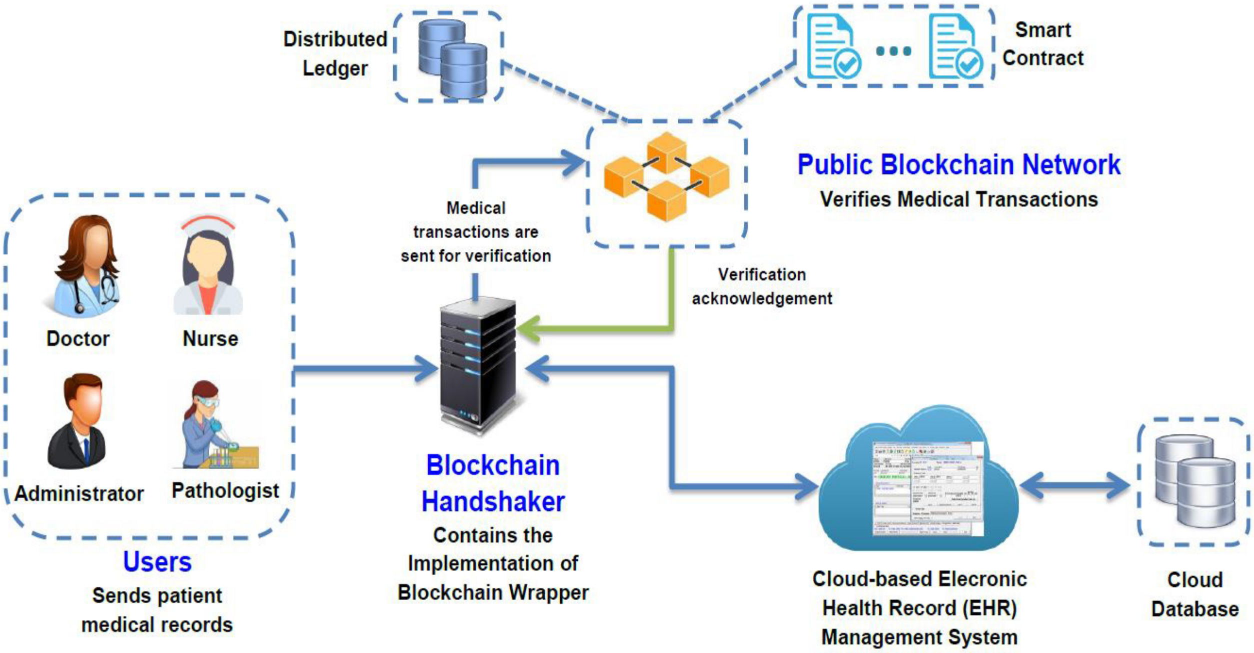
Distributed Ledger
Smart Contract
Public Blockchain Network
Verifies Medical Transactions
Medical transactions are sent for verification
Verification acknowledgement
Doctor
Nurse
Administrator
Pathologist
Users
Sends patient medical records
Blockchain Handshaker
Contains the Implementation of Blockchain Wrapper
Cloud-based Elecronic Health Record (EHR) Management System
Cloud Database

Fig 1. A System Architecture for Blockchain-based EHR Systems by Rahman et al. [11]

Blockchain technology, initially introduced as the foundation for Bitcoin cryptocurrency in 2009 by Satoshi Nakamoto [3], offers a decentralized database solution that possesses key features such as immutability, decentralized management and access control, and robust data security. Consequently, blockchain has emerged as a promising option for storing EHRs, leading to numerous research endeavors in this domain in recent years [4].

Leveraging blockchain as an EHR database can foster interoperability; however, it also presents its own set of challenges and issues. Firstly, the choice of blockchain type warrants consideration. The implementation can be based on existing open-source blockchains or a new blockchain can be developed from scratch. Additionally, determining whether the ownership of the blockchain should be private, public, or consortium-based is another crucial aspect that demands attention [5]. Using or not using smart contracts also makes another issue [6].

The next issue that should be considered is the EHR standard used, to register patients' health records. Different national and international organizations have each considered different standards for EHR registration, which should either be chosen as the standard for data registration in the blockchain, or a mechanism for converting EHRs based on different standards should be considered [7].

The storage location of medical records is another challenge; Since EHR data is voluminous, storing it inside the blockchain can be costly and slow down the speed of information access [8]. To solve this problem, cloud solutions can be used and combined with blockchain; however, in this way, EHRs will not be definitively immutable, and we will need other preventive mechanisms as well to maintain the integrity of EHR data [9].

In addition, the presence or absence of a third-party auditor should also be checked; should there be a member in the network who individually or collectively monitors the recorded data and requests on the blockchain side, or should all members have the same level of access? This issue should also be considered [10].

To overcome these problems, researchers have developed architectures and software platforms that include blockchain-based EHR with interoperability, and have provided different auxiliary mechanisms and components for it, each of which has covered the existing challenges in a way. The results of these investigations showed that, for this issue, a software architecture is used, which initially forces the stakeholders to use the same standards to record EHR information. Identity data and small information are stored on the blockchain, then to solve the scalability problem, a cloud database is used to record voluminous medical information, and a pointer to cloud data is recorded on the blockchain to maintain the integrity of the data. In order to access the data, permission to read the information will be granted to authorized users through encryption mechanisms. Smart contracts in blockchains are also used to enforce the above processes. By using these mechanisms, blockchain can be used as

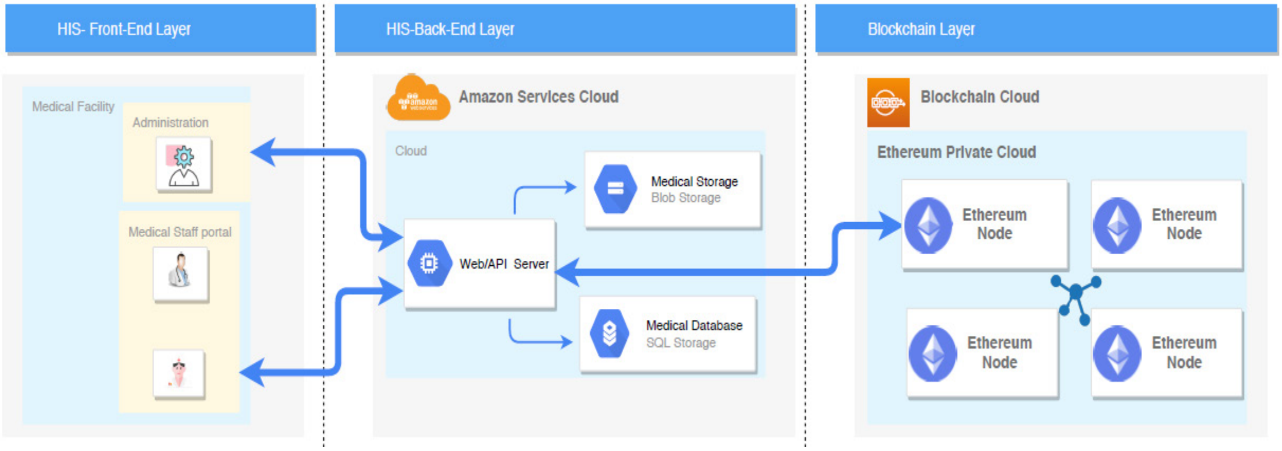

Fig 2. The architecture of Jaber et al.'s solution [15]

a suitable platform for recording and maintaining EHRs while considering interoperability.

The rest of the paper is organized as follows: the basic concepts are mentioned in the section 2. In section 3, the research works has been reviewed. In section 4, we compare the works done and then there is a discussion about the researches and in section 5, the summary and conclusion are presented.

2. Basic concepts

EHRs are necessary in today's world as EHR can create a platform for patients to access medical information, increase patient participation in medical decisions, and facilitate communication between patients and medical centers [1].

2-1- Interoperability in electronic health records

Interoperability is one of the quality features in software systems, which according to the IEEE definition refers to the ability to exchange information between two or more systems and use the exchanged information [12]. Medical organizations such as NAHIT have supplemented this definition for medical purposes and define interoperability as the ability to communicate and share data in a robust, efficient and accurate manner by software systems and information technology systems, along with the ability to use shared data [13].

Applying interoperability in maintaining and sharing EHRs is very important for the many reasons. Easy and fast access to EHR is one of these reasons. EHRs are created in different ways; Hospitals, laboratories, clinics, as well as body sensors, create EHRs separately in their databases [14].

In order to access this type of distributed data, each of the stakeholders of the system, including the patient, doctor, hospital, etc., should be able to easily and quickly access the files of other organizations, which can be even critical. Apart from the above, factors such as eliminating human error, increasing the efficiency of health service providers, reducing the costs of moving medical information are also among the benefits of applying EHR interoperability [15].

2-2- Blockchain and interoperability in EHR

A blockchain is a growing list of records maintained in a distributed manner by peer-to-peer groups. Due to the existence of features such as immutability, decentralized management and access, elimination of the single point of error, pseudo-anonymity, confidentiality, integrity and availability of data in the blockchain, this technology is suitable for use as a database for maintaining EHRs, and in recent years, many papers have been written in this area of research [4].

The blockchain can be maintained by stakeholders in a distributed manner and each stakeholder can record their medical data as a transaction within the blockchain and finally share it. It is also possible to access the medical records of other stakeholders (if permission is granted) using this blockchain. Through the consensus mechanism in the blockchain, all stakeholders can agree on medical data too.

Considering the above factors, blockchain can be considered a suitable platform for realizing interoperability in the field of EHR. However, many challenges such as implementation complexities, high volume of medical data, scalability, diversity of blockchains, data storage location, trade-off with security issues and lack of standard communication protocols can cause problems in achieving complete interoperability [16].

In addition, considering connection problems between different EHR based blockchains with different structures (such as different transaction structures) and also the variety of standards used in EHR, and different methods of sending data in blockchains, new issues are still created in the field of interoperability of blockchain-based EHRs [17].

3 - Conducted researches

In 2020, Jaber et al. [15] tried to solve the issue of interoperability in EHR by building a software architecture based on cloud and blockchain and the existence of a trusted distributed third-party auditor. The presented architecture consists of two main parts: Health information center (HIS) and BiiMED Blockchain.

The health information center itself includes two layers: The front-end layer is web portals that allow doctors to interact with medical information, and the back-end layer is the cloud system and web services that provide storage and access to medical information.

To record medical information, the ICD-10 standard provided by the World Health Organization (WHO) have been chosen and to record and store medical images the DICOM standard have been used.

The BiiMED blockchain is a private blockchain based on Ethereum and smart contracts [18] that is responsible for the management and validation of shared medical information and plays the role of a trusted distributed third-party auditor.

The system works as follows: users, who are health workers, register medical information in the cloud system using the front-end layer and simultaneously a hash of the data is stored in the blockchain. Each stakeholder, for example, each hospital, keeps its medical data separately, and normally they do not have access to the medical data of others.

If a user wants to access the medical file of a person located in another stakeholder database, he sends a request to the desired cloud system through the web portal and web services, and if permission is granted, the desired medical data will be shared for that user.

To validate the received data, the web services of the web portal first hash the data and then look up the data key in the BiiMED blockchain. If the created hash is equal to the hash in the blockchain, it means that the integrity of the information is preserved and the user can use the shared file.

The strength of this system is the use of the cloud to store and solve the problem of scalability and speed of data access in the blockchain [19], but since the data itself is not stored on the blockchain, there is no guarantee that the data will remain integrate forever; Because the permanent storage of data while maintaining integrity is guaranteed on the blockchain, not on the cloud, and this strength can also be a weakness of the system.

In addition, the existence of a trusted third-party auditor can also be a weakness; because this auditor has the ability to confirm and validate invalid medical data with the cooperation of stakeholders. Although due to the use of distributed blockchain, the third-party auditor can no longer be considered as a single point of failure, but the problem of intentional error still remains.

BiiMed has not been released in real world, but they used some metrics to evaluate the performance of their system. According to their results, when using a single 8GB RAM, Core i7 system with 10000 users, the average response time of read functions are between 1 to 20 milliseconds. As their result is based on a single system, the distributed nature of the blockchains is not addressed and their result should not be trusted in real world deployment of it.

Villarreal et al. [13] also presented another paper in this field which was published in 2023. This paper first reviews the interoperability issues in blockchain-based EHRs and then presents a blockchain-based EHR architecture using a domain-specific language (DSL) and smart contracts.

The proposed architecture is such that each stakeholder (for example, hospitals) has its own blockchain-based EHR database. Each of the blockchains can have different standards for accessing information, and also the mechanism of their smart contracts can also be different.

To access the medical information of other hospitals, Model Based Engineering (MBE) has been used to create interoperability features. In this way, a request to access information/add a record is created first. This request is then translated into a specific DSL-based format. Then this translated request, according to the type of blockchain in which the requested record is located, is converted into a smart contract inside that blockchain, and by using that smart contract, the end user can access the required medical record.

This paper only presents a model based on the translation of smart contracts, but does not implement it, it only introduces the Eclipse Modeling Framework as the platform for modeling smart contracts and converting them with Java language and in the XML format.

Sonkamble et al. [20] published another paper that examines and presents a solution on interoperability in blockchain-based EHR.

In this paper, the concept of interoperability is divided into two categories: structural interoperability and semantic interoperability. Structural interoperability defines the syntax, format and standard representation of data, but semantic interoperability means that the sender and receiver of the data, must have the same understanding of the shared information, and in the translations that take

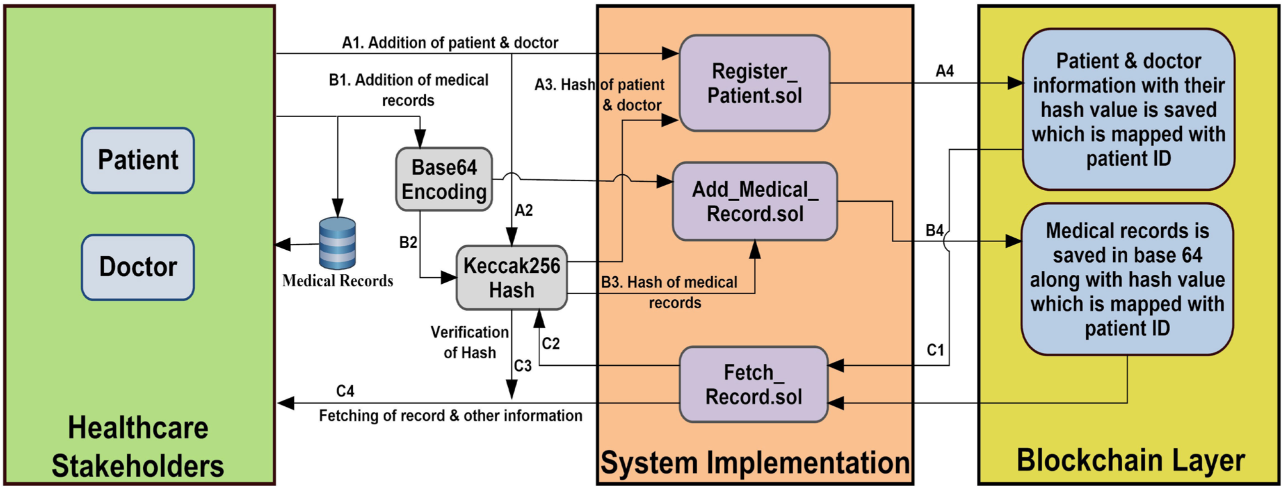
Patient
Doctor
Healthcare Stakeholders
A1. Addition of patient & doctor
B1. Addition of medical records
A3. Hash of patient & doctor
Base64 Encoding
A2
B2
Medical Records
Keccak256 Hash
B3. Hash of medical records
Verification of Hash
C2
C3
C4
Fetching of record & other information
Register_ Patient.sol
Add_Medical_ Record.sol
Fetch_ Record.sol
System Implementation
A4
B4
C1
Patient & doctor information with their hash value is saved which is mapped with patient ID
Medical records is saved in base 64 along with hash value which is mapped with patient ID
Blockchain Layer

Fig 3. User interaction in MyBlockEHR [20]

place during the sending and receiving of the data, the meaning of the data should not change [21].

One of the strengths of this paper is the systematic review of the standards presented in EHR sharing and the study of the most used ones. One of the most widely used EHR sharing standards is the OpenEHR standard, where patient and clinical trial records are maintained in a standardized format. The use of this standard can help ease the issue of interoperability in EHR. Apart from OpenEHR, the FHIR standard also provides a lightweight solution for EHR modeling using XML and JSON formats, which has higher portability.

This paper then examines the ways of interoperability between different blockchains and reaches three categories. The first category is based on the connection between two blockchains by a third-party auditor called a notary, which can be single or include several members with different digital signatures. The second category is based on side chains and smart contracts. In this way, through smart contracts, a blockchain can read the information of another blockchain and store the part of the information it wants on its side chain. The third category is called Hash Locking, which works by activating the same hash at a certain time in two blockchains.

After reviewing the existing solutions, they present their proposed solution called MyBlockEHR; In MyBlockEHR, users are divided into three categories: patients, doctors, and certificate authorities. Users are responsible for their data and are responsible for granting access to their data to doctors using cryptographic mechanisms.

In order to store data, EHR records are divided into two parts. The first part, which is stored on-chain, contains sensitive and light data plus the hash value of the second part, and the second part, which is stored off-chain, contains large data (eg, medical images) stored in the document-based NoSQL database MongoDB on the cloud storage. The reason for dividing the data into two parts is the greater scalability and the high cost of storing large chunks of data in the blockchain.

Smart contracts are used to access information and validate off-chain information received from MongoDB; In this way, the contracts receive the information and index needed to access medical data from the blockchain, and after receiving them from the off-chain database, it calculates its hash and compares it with the hash stored in the blockchain; If the two hashes are equal, the integrity of the information is confirmed and the data will be provided to the users.

MyBlockEHR hasn't been deployed in real world yet, but it is tested in an isolated platform using an Ubuntu PC with 7.6 GBs of RAM and an 8th gen Core i5 CPU. In its test they wanted to show the difference between the response time of storing EHR data on-chain or off-chain. To do so, they used Ethereum and its smart contracts written in Solidity Language and a local MongoDB database was used as EHR database. According to their results, accessing patient data while stored off-chain can be as fast as about 49 milliseconds, while accessing on-chain data can take as long as about 44 seconds, meaning that storing the actual data off-chain can greatly improve performance.

Carter et al.'s paper [22] has also solved the problem of interoperability in blockchain-based EHRs by using smart contracts and storing the original medical records in the cloud, and has reached the prototype architecture implementation stage. Each EHR provider (such as hospitals) is considered as a node in the Ethereum blockchain. When a provider wants to release a patient's medical record, they

Table 1. Comparison of the reviewed papers

Paper	Blockchain	EHR Standard	Data Storage	Software Architecture	Audit
Jaber et al. [15]	BiiMed Private blockchain based on Ethereum-Based	ICD-10 DICOM	Cloud. Data hash in blockchain	Two layers. Health information center and blockchain	Trusted distributed third-party auditor
Villarreal et al. [13]	Separate and arbitrary blockchain for each stakeholder (hospital)	Translation between different standards	Separate blockchains for stakeholders	Communication between blockchains by smart contracts	None
Sonkamble et al. [20]	MyBlockEHR private blockchain	OpenEHR, FHIR	Off-chain (MongoDB) along with their reference key on the blockchain	Access to off-chain data by smart contract	CA for membership and certification authority
Carter et al. [22]	Ethereum-Based	FHIR	Amazon cloud services	Bucket memory. Envelope encryption	None
Dagher et al. [23]	Ethereum-Based	unknown	Large data on mongo DB, its hash and query on blockchain, small data on blockchain	Three parts. Database, encryption, Ethereum Go client	None

first encrypt it using envelope encryption. Envelope encryption is done in such a way that first the original data is encrypted with a unique key of the data file itself, then the key of the file itself is encrypted once again with another key. After creating the file, it is uploaded to the bucket memory of a cloud storage. When a file is uploaded to the bucket memory, a smart contract is generated declaring that a node has published a medical data. Nodes that have received this message can try to decrypt the message with their key-pair. If they succeed in decryption, (they were given access) they get the key of the published EHR file and can use that key to decrypt the uploaded file.

Amazon AWS cloud service is used due to the existence of encryption services and Ethereum blockchain is used due to the existence of smart contracts. EHR files are created using the FHIR standard.

Their paper doesn't feature any implementation tests and results and any kind of implementation or real-world deployments are left for future works.

Dagher et al. [23] have also presented another blockchain-based EHR paper with interoperability. The provided software platform called Ancile consists of three components. The first component is the database manager. Ancile stores the query link to the database and its hash on the blockchain to maintain integrity, but the medical records themselves are kept off-chain on another database and can be accessed through the query link of the corresponding record in the blockchain. The database manager is in charge of the connection between the blockchain and the database through the creation of hashes and query links. The second component is the encryption manager, which is responsible for encryption and decryption. A public/private key mechanism is used to grant access, but symmetric cryptography is used to store large data. The third component is the Ethereum Go client.

Several smart contracts are used to communicate with the blockchain, which are also able to communicate each other. These contracts can determine the ownership of medical records using relationships between network nodes. In this way, a patient can grant a doctor access to information, revoke access by changing the key, see the history of access to his data and so on.

In order to access information, a user finds the owner of the desired data (for example, a hospital) through a smart contract, and then sends a request to that owner to receive the symmetric key of the corresponding data. If it is available, the key will be returned and the user can access the desired EHR medical record.

In addition, in this system, it is possible to store small medical files (for example, a medical prescription) on the blockchain itself.

In order to evaluate Ancile's performance, they compared its Ethereum gas cost to Medrec [24] which is another blockchain based EHR platform. According to their results, although Ancile has higher gas cost and even higher performance cost than Medrec, their security features are so much important and vital that they willingly pay its price as there is always a trade-off between performance and security.

4- Discussion

There are various ways for using blockchains to implement interoperability in EHR, and each of the reviewed papers has chosen one of them for implementation. Here, for each paper, the type of blockchain used, the EHR standard chosen to record medical records, the storage location of those medical records and the type of database used, the presence or absence of a third-party auditor and supervisor to the system, and finally their software architecture is checked and compared and the results are given in Table 1.

By examining and studying Table 1, you can get important results; First of all, all the papers reviewed by us have used a specific software architecture and intended to provide a complete software platform. In these software architectures, various encryption mechanisms are used to register and determine user access to EHR data. There is no agreement on the use of a trusted third-party auditor, two papers have used a trusted auditor while three papers have not. Also, the smart contracts available in blockchains are used in three out of five papers in order to enforce the above processes.

The software architecture in the presented papers has forced the users of the services to use a specific EHR standard, and apart from one paper that utilizes the ability to convert EHR standards, other papers have used a specific standard for EHR registration; FHIR standard is used in two out of five papers and other standards such as OpenEHR, ICD-10 and DICOM are also used once in other papers.

By checking the Table 1, you can also get tips about the storage location of EHR data; First of all, there are identity data that must be stored on the blockchain. But EHR documents, due to their high volume, are stored on a cloud database in four out of five reviewed papers, and only a pointer or a hash of that data is stored on the blockchain to maintain integrity. Other than them, one paper has also provided the ability to store small EHR data on the blockchain itself.

There is no definite consensus regarding the type of blockchain used. Two of the five papers have developed a private blockchain, two papers have used Ethereum, and one paper has allowed the use of any type of blockchain and solved the interoperability problem by translating between them.

4-1- Research limitations

In the process of obtaining the papers and information, we encountered some challenges that we will briefly mention. The first issue is the number of papers; Due to the novelty of the topic of examining interoperability in EHR registration on the blockchain, very limited groups have worked in this field in a professional manner, and much fewer people have published it as papers [25]. The second problem is the lack of implementation; Published papers often remain in the theoretical stage and none have been practically implemented and tested in the real world. This causes hidden weaknesses and challenges in using blockchain as a platform to implement interoperability in EHR records that have not been explored. The third issue is the excessive use of Ethereum and smart contracts by working groups; Instead of developing new blockchains with creative consensus mechanisms and using intra-blockchain solutions, the authors of most of the papers have been content with Ethereum smart contracts and finally, by storing the EHR in the cloud, they have only used the blockchain as a platform for registering smart contracts and the features of immutability and integrity that blockchain provides for data have not been used practically so that the integrity of EHR data is still at risk. The existence of these weaknesses creates areas for future researchers to solve the problems of storing EHR data on the blockchain, while providing interoperability.

5 – Future Research Areas

Blockchain integration to ensure interoperability of EHR data is still relatively new and there are still many unexplored aspects in this research area. Novel Blockchain technologies with new consensus methods, not only provide much better scalability, but also, they offer fast transaction confirmation time. Using these blockchains or developing specialized consensus methods for Interoperable EHR blockchains can increase performance by a far margin. Also, the removal of cloud services and using the blockchain as the sole distributed database can also be considered as it can ensure near perfect integrity of data and with these new blockchain technologies it can be possible. DAG based ledgers can be considered as the successors blockchains, DAGs help us achieve simultaneous transaction approval from different stakeholders using their directed acyclic graph structure, which can help us provide much better scalability. [26] Considering DAG as solution for interoperable EHR database can also be a new research area.

6 – Conclusion

Traditionally, EHRs are kept separately in the internal databases of different medical centers, and if a patient wants to transfer a part of his records to another medical center, he needs interoperability between the two medical centers. Blockchain, as a distributed platform for safe and unaltered data storage, can be a suitable database for storing and integrating patients' medical records that can improve interoperability between centers, and for this reason, in recent years, many solutions in this field has been provided.

Due to the problems of scalability and the high cost of storing large volumes of medical data on the blockchain, researchers have decided to store the medical data itself in the cloud and store its pointer and hash in the blockchain. In addition, medical data should be stored according to global EHR standards, like OpenEHR and FHIR, to improve interoperability and reduce or even eliminate the need for translation.

In this case, any provider of medical data (for example, a hospital) as long as it uses EHR standards can store its medical data on the cloud space of its choice and store only its hash and pointer in the main blockchain to ensure scalability through cloud storage and data integrity through blockchain.

In order to access blockchain data, the smart contracts available in Type 2 blockchains, such as Ethereum, are usually used to reduce human error and to enforce the information access process. It is also possible for the EHR to be stored in two different blockchains, in this case, it is necessary to interact between the two blockchains using methods such as smart contracts or a trusted interface.

Finally, it can be said that blockchains can help interoperability between EHR centers, provided that EHR standards and appropriate encryption techniques are used. The use of cloud space and NoSQL document-oriented databases to maintain EHR and store their pointer and hash in the blockchain is also very common in this area.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Declarations

Ethics approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Competing interests

The authors declare that they have no competing interests.

Received: Oct. 2023   Accepted: Nov. 2023
Published online: Dec. 2023

DOI: 10.22034/ASAS.2023.420797.1043

References

1. The Office of the National Coordinator for Health Information Technology. (2019, Sep 10). What is EHR. healthit.gov. https://www.healthit.gov/faq/what-electronic-health-record-ehr

2. Wang, Y., Zhang, A., Zhang, P., & Wang, H. (2019). Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain. Ieee Access, 7, 136704-136719.

3. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized business review.

4. Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. J. C. C. (2019). Analysis of Blockchain technology: pros, cons and SWOT. Cluster Computing, 22, 14743-14757.

5. Hussien, H. M., Yasin, S. M., Udzir, S. N. I., Zaidan, A. A., & Zaidan, B. B. (2019). A systematic review for enabling of develop a blockchain technology in healthcare application: taxonomy, substantially analysis, motivations, challenges, recommendations and future direction. Journal of medical systems, 43, 1-35.

6. Lee, J. S., Chew, C. J., Liu, J. Y., Chen, Y. C., & Tsai, K. Y. (2022). Medical blockchain: Data sharing and privacy preserving of EHR based on smart contract. Journal of Information Security and Applications, 65, 103117.

7. Mayer, A. H., da Costa, C. A., & Righi, R. D. R. (2020). Electronic health records in a Blockchain: A systematic review. Health informatics journal, 26(2), 1273-1288.

8. 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.

9. Cao, S., Zhang, G., Liu, P., Zhang, X., & Neri, F. (2019). Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain. Information Sciences, 485, 427-440.

10. Shi, S., He, D., Li, L., Kumar, N., Khan, M. K., & Choo, K. K. R. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. Computers & security, 97, 101966.

11. Rahman, M. S., Khalil, I., Mahawaga Arachchige, P. C., Bouras, A., & Yi, X. (2019, July). A novel architecture for tamper proof electronic health record management system using blockchain wrapper. In Proceedings of the 2019 ACM international symposium on blockchain and secure critical infrastructure (pp. 97-105).

12. Geraci, A. (1991). IEEE standard computer dictionary: Compilation of IEEE standard computer glossaries. IEEE Press.

13. Villarreal, E. R. D., García-Alonso, J., Moguel, E., & Alegría, J. A. H. (2023). Blockchain for healthcare management systems: A survey on interoperability and security. IEEE Access, 11, 5629-5652.

14. Wang, Y., Zhang, A., Zhang, P., & Wang, H. (2019). Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain. Ieee Access, 7, 136704-136719.

15. Jabbar, R., Fetais, N., Krichen, M., & Barkaoui, K. (2020, February). Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. In 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT) (pp. 310-317). IEEE.

16. Al Mamun, A., Azam, S., & Gritti, C. (2022). Blockchain-based electronic health records management: a

comprehensive review and future research direction. IEEE Access, 10, 5768-5789.

17. Reegu, F. A., Abas, H., Gulzar, Y., Xin, Q., Alwan, A. A., Jabbari, A., ... & Dziyauddin, R. A. (2023). Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System. Sustainability, 15(8), 6337.

18. Ethereum Foundation. (2014). Ethereum Whitepaper. ethereum.org. https://ethereum.org/en/whitepaper/

19. Mishra, R., Ramesh, D., Edla, D. R., & Qi, L. (2022). DS-Chain: A secure and auditable multi-cloud assisted EHR storage model on efficient deletable blockchain. Journal of Industrial Information Integration, 26, 100315.

20. Sonkamble, R. G., Phansalkar, S. P., Potdar, V. M., & Bongale, A. M. (2021). Survey of interoperability in electronic health records management and proposed blockchain based framework: MyBlockEHR. IEEE Access, 9, 158367-158401.

21. de Mello, B. H., Rigo, S. J., da Costa, C. A., da Rosa Righi, R., Donida, B., Bez, M. R., & Schunke, L. C. (2022). Semantic interoperability in health records standards: a systematic literature review. Health and technology, 12(2), 255-272.

22. Carter, G., Shahriar, H., & Sneha, S. (2019, July). Blockchain-based interoperable electronic health record sharing framework. In 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC) (Vol. 2, pp. 452-457). IEEE.

23. Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable cities and society, 39, 283-297.

24. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016, August). 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.

25. Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S. A., & Faxvaag, A. (2020). Blockchain in healthcare and health sciences—A scoping review. International Journal of Medical Informatics, 134, 104040.

26. Wang, Q., Yu, J., Chen, S., & Xiang, Y. (2023). Sok: Dag-based blockchain systems. ACM Computing Surveys, 55(12), 1-38.