iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** I **Month of publication:** January 2023

DOI: https://doi.org/10.22214/ijraset.2023.48808

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue I Jan 2023- Available at www.ijraset.com

A Literature Review of Blockchain Applications in Healthcare

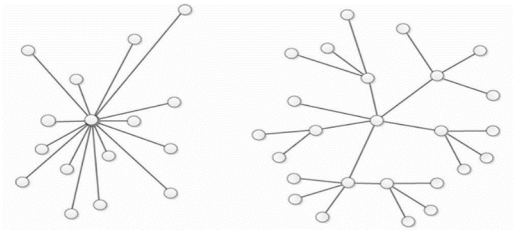
Govardhan R[1], Jagadeesh V Ranagatti[2], Lakshminath S M[3], Linganand Sangamad[4], Dr. Nagaraja J[5]
Dept. of Computer Science and Engineering, Dayananda Sagar College of Engineering

Abstract: ***Health data is usually in a scattered manner as they are usually gathered by various entities. The data's scatteredness develops a burden in designing adequate health bills which ensure the well-being of the patients. Moreover, the concerns in achieving synchronization and instantaneous access to such data worsens the problem all the more. So, designing a system that can ensure the integrity, security, preciseness, and accessibility of the patient's medical data is of paramount importance. Health systems based on blockchain can guarantee the above features and protect data from being tampered or from any kind of attacks. Blockchain also helps in management of data and its flawless integration. It makes most of its smart contracts feature to execute the several requests and queries related to the patients (medicine, appointments, medical procedures, lab tests or previous medical information). All the stakeholders in the system should be able to obtain the medical data preserved in a database not having to compromise on its credibility. In this survey, we examine the previous research work various authors have carried out on implementing blockchain in several aspects of healthcare.***

Keywords: Blockchain, Distributed systems, Electronic Health Records (EHR), Health Information Exchange (HIE), Healthcare, Private ledger

I. INTRODUCTION

Since the introduction of Blockchain in 2008, it has gained a lot of popularity. In a blockchain with a number of participants, it is possible to exchange information without any node governing this exchange. This decentralized nature of the blockchain has generated a lot of interest in different industry sectors. The nodes in the blockchain store and access data from a shared ledger that each node maintains a copy of [1].



a) Centralized b) Decentralized

Fig 1 [9]

One of the advantages of using blockchain is that, with peer-to-peer networks, the updates are in real-time, and there is no need for any intermediaries and their associated costs [2]. Due to the decentralized nature of blockchain, users can manage themselves. Fig 1 shows how a decentralized network is different from a centralized one. Since all transactions on the blockchain are immutable and fully transparent [3], the privacy and integrity of patient information will be preserved. The use of blockchain improves control and management of resources on the network. In the following section, we will discuss the existing work dedicated to blockchain applications in the healthcare sector. In the healthcare sector, a lot of data is generated and used. Storage and retrieval of such huge data is challenging but essential. Special importance must be given to the fact that the information is very sensitive, and proper security has to be maintained. Data has to be shared in an efficient manner among the required custodians so that the data is properly utilized. Using patient data without his/her consent can result in legal ramifications.

Several researches have been conducted to highlight various applications of blockchain in healthcare [4,5,6]. Mettler [7] discusses some areas of public health management where blockchain can be useful. In the field of legal medicine that includes the payment for medical services, the applications of blockchain have been surveyed and presented by Roman-Belmonte et al [8]. Tama et al. [9] explore different areas of application where blockchain can be used such as finance, healthcare, business etc.

A. Contribution

In this study, we aim to discuss the various applications of blockchain in healthcare and discuss some of the challenges. Our contributions are

1) We have surveyed existing literature works in the field of healthcare where blockchain can help improve the existing systems.
2) We have analyzed the different approaches used in the proposed solutions in those works, and have presented them in a simplified manner.

B. Paper Organization

We have organized the remainder of this paper as follows. Section II is survey of literary works on the use of blockchain in healthcare. It has been subdivided into 2 sections based on the storage techniques used - *On-chain* and *Off-chain.* Section III is the conclusion of this study.

II. LITERATURE SURVEY

We have divided the papers surveyed based on the 2 major data storage paradigms in blockchain – On-chain and Off-chain. The subsection that follows this discusses the works involving On-chain storage solutions. In the following subsection, we present the works with Off-chain storage mechanisms.

A. On-chain

Sudeep et. al. in [10] propose a system architecture for Hyperledger-based EHR sharing system for efficient and secure data sharing compared to traditional networks that use client-server-based architecture. Various Access Control Policy algorithms have been proposed and optimized to improve accessibility of data for participants in the system, avoiding the necessity of a central authority.
The system has four main participants - patients, providers or doctors, laboratory staff and system admin. The admin has complete control over the network and can perform CRUD operations. Admin can grant other participants access to patients' data. The performance metrics, which are measured using various tools and frameworks, show that the system has better performance and lower latency compared to current systems. The system however grants complete access to the patients allowing them to create, delete and modify health records which can be a drawback. The system also does not use any off-chain storage mechanism which is essential for storing high volume data like X-ray images.
Huirui Han et. al. [11] propose an architecture that uses hybrid blockchain which comprises of a private blockchain and a consortium blockchain. Asymmetric encryption is applied to health data of patients before this data is appended to the blockchain. The fully private blockchain is used to store medical data of individual medical facilities whereas shared medical data is present on consortium blockchain. Medical data can be of any type like laboratory results, X-ray images, prescriptions and other reports that may be larger in size. Use of a single blockchain to store this data will be a burden on the network, requiring nodes to have larger storage capacity and decreasing the performance. Hence only the necessary data of the patient is added to the main blockchain by the clinician. The major barrier for the proposed model is the deployment cost.

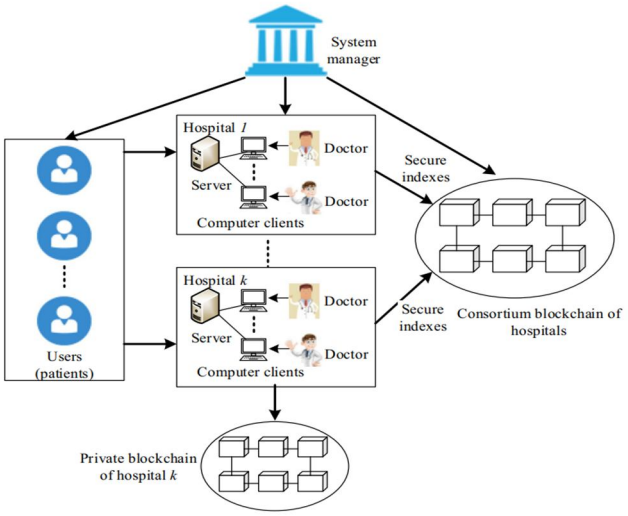


Fig 2 [12]

The authors [12] have designed a privacy-preserving and secure health data sharing scheme for enhancing the diagnosis process in e-Health using blockchain. Consensus mechanisms and data structures have been devised to construct 2 types of blockchains - one private and a consortium blockchain. The private one stores the personal health data while the consortium blockchain records the data's secure indices. Health data, identity of patient and various keywords are encrypted to achieve access control, security, secure search, and privacy. Block generators (like a hospital server) are used to produce proof of conformance, guaranteeing the availability of a system. The authors have also implemented this scheme on JUICE, a platform for smart contract designing, to evaluate the performance. The architecture of this scheme is shown in Fig 2. A. Murugan et.al. [13] in this paper proposed a distributed approach for Health Information Exchange blockchain technology (HIE). This technology is used in various healthcare fields, such as enhancing claims of insurance and ensuring accessible data for research, and exchange of health records between patients and doctors. Medical data is highly sensitive; hence the suggested system uses a permissioned block-chain like Hyperledger Fabric to maintain the essential privacy. The authors aim to transmit health information overcoming the boundaries both geographically and institutionally, so that a secure and suitable delivery mechanism is supplied.

B. Off-chain

This subsection is further divided according to the different mechanisms of data storage used.

1) Cloud

The authors in [14] propose a system for sharing of electronic healthcare information using a permissioned blockchain that allows only authorized users to join the network. The system comprises three layers, those are user, system manager and storage. The users of the system can add their data to the cloud repository that holds all the data and also can access the shared data of different medical facilities. The requests made by the users to read or write the data is considered as a transaction and this request can be made by the users using their private key. These transactions are then verified by the consensus nodes. Various protocols are also being discussed in this paper. The paper however does not focus more on the communication and authentication protocols that are being used. The paper [15] proposes a system whose main goal is to provide a productive way to collect quality health data for any kind of research and business reasons. Users should be able to own and control health data but they are usually managed by other organizations. And the authors propose an architecture involving blockchain technology using cloud storage in an easy and secure manner. In addition, they also have implemented machine learning to inspect the data quality. The main aim of this design is to provide control on their data and access to share the data securely in a General Data Protection Regulation (GDPR) way.

S. Wang et.al. [16] in this paper have proposed a scheme for securing personal health data stored on cloud platforms. Patients and users can access the encrypted data that is stored on the cloud. Here the user refers to an individual or healthcare provider. The data is encrypted, before storing it, to avoid modifications from external entities. Initiating a smart contract and sharing of private keys is done by the patients. The blockchain will have the details of the transaction along with the hash of the data that can be used to verify the integrity of data while accessing it. The operations like updation and deletion of a file in the cloud is not addressed in this paper.

The authors [17] have implemented a searchable encryption scheme for Electronic Health Records (EHRs) using blockchain. Healthcare agents can use queries to get access and interact with medical records. Monetary rewards among the parties on the network are traced using a smart contract deployed on Ethereum. Data owners are the ones who control the access to their data. This scheme proposed here allows complex queries when compared to the single keyword searches in earlier approaches.

X. Yue et.al. [18] have proposed an application called the Healthcare Data Gateway (HGD). The application gives patients total control over their shared medical data. They can access and monitor control to their data using this blockchain based application. This is a novel way in which patients interact with their data with ease, and it makes for better healthcare systems. A purpose-centric access control has been used to permit a third-party to securely process patient data. All the patient information is managed on the blockchain, and this data is thus immutable. A cloud backup of the data is maintained and synchronized regularly. Decisions regarding the legal aspects of patient data is simplified using this HDG system. It is also a very efficient and secure way to store sensitive medical information.

2) InterPlanetary File System

Solutions that use interplanetary file system for storage are discussed below.

Ayesha et. al. in [19] propose a framework that aims to provide a secure, decentralized, and scalable Electronic Health Record (EHR) system with the help of blockchain technology and discuss the challenges of EHR systems in terms of various aspects like data security, management, and privacy.

To address the problem of scalability the proposed framework makes use of off-chain storage of health records using IPFS. The security aspect is addressed by providing granular access rules for the nodes in the network by the administrator.

The availability of records only to trusted and related individuals is achieved by role-based access management. The paper mainly focuses on the internal operations like adding, updating and viewing patient records within the hospital network. The system does not include third parties like insurance agencies which are also an essential part of the healthcare system.

Buzachis et. al. [20] propose a HIE solution based on Blockchain-as-a-service (BaaS-HIE). Use of Blockchain helps in overcoming the security and interoperability challenges of patient-driven HIE between various healthcare providers. The proposed design uses a private blockchain and various smart contracts for access management. The system also uses InterPlanetary File System, a distributed file system, to store all the encrypted health data in a decentralized way. The blockchain will have a hash of these assets' URI. Personal data of the Patient from Internet of Medical Things (IoMT) devices are also stored in the EHR. The system uses Ethereum and clique, a proof-of-authority consensus protocol.

Nabil Rifi et.al. [21] discuss the importance of eHealth technology. Storing data from IoT devices i.e., sensors is not feasible, as it will result in a drop in performance. Sensor nodes send their data to a gateway which is then responsible for storing data off-chain, and the pointers to this data will appended as a transaction to the blockchain. The authors have expressed their concern regarding the consensus mechanism used in this system, and relevant questions must be asked and answered to build an optimized model with improved performance. Fig 3 shows the architecture.

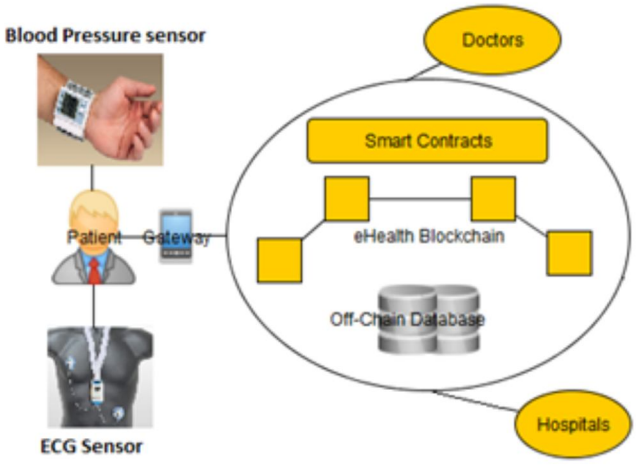


Fig 3 [21]

3) Existing Database

Solutions that use the providers existing databases for storage are discussed below.

In order to improve hospitals' electronic health system, the authors [22] suggest a healthcare data sharing system that makes use of a private blockchain. The approach can satisfy several security requirements, including decentralization, openness, and tamper resistance. Doctors are given a dependable way to maintain patient privacy while storing medical information or accessing patient history. Additionally, it enables patients with similar illness traits to be in touch with one another after mutual approval. This also achieves similar treatments to those patients with relatable symptoms.

Jayneel et. al. in [23] provides a framework based on blockchain for EHR storage. The framework focuses on requirements of patients and providers along with data confidentiality. Patients, healthcare providers and other parties are given access to health records of patients in a secure manner. The framework makes use of various encryption techniques and cipher manager before transmitting the records over the network. Thus, the measures taken above reduces unauthorized access of private data.

However, it has some limitations like difficulty of use for the users and time consuming for operations like adding new nodes and defining relationships between them. The authors [24] have proposed a system that uses the Ethereum blockchain to deploy smart contracts which records the relationship between patients and their healthcare providers. The stored medical records can be viewed with the specified permissions. The proposed system can be merged with the existing data storage solution used by the provider. Cryptographic hash of the data is stored on the blockchain to safeguard the data from unauthorized modifications. Researchers and other healthcare stakeholders are encouraged to take part in the network as miners to put transactions on the blockchain. A special function is written in the contract that gives miners anonymized medical data as rewards when they successfully append a block to the chain.

Using the Ethereum protocol, the authors [25] have created a private blockchain on which smart devices can call smart contracts and write records. Sensors in this system help in monitoring the patient in real-time. The sensitive healthcare data will not be recorded on the blockchain, but on secure storage databases, due to compliance reasons. The blockchain only contains transactions which can be linked to those databases to provide authentication.

The authors [26] here propose a framework called 'Ancile' which utilizes advanced cryptographic techniques and smart contracts to heighten access control and implement data obfuscation. Ancile has many smart contracts responsible for functions such as user registration, classification of nodes, maintaining relationship between nodes, specifying level of access, etc. Patients can manage the access to their private information using smart contracts. The blockchain is permissioned and Ancile controls who can participate in it by verifying user information before registration.

Yan Zhuang et. al. [27] propose a patient-centric blockchain system architecture to overcome the challenges in existing HIE systems. The architecture consists of two modules namely linkage module and request module. The latter is used by clinicians to request access from the patients and access their data. The blockchain adapter hashes the health data and stores it in a smart contract. The actual health data is stored in a secure database. To verify the integrity of data, the hashes and decryption keys are retrieved from the smart contract. The data is then hashed and compared with the original hash. For this system to work, hospital servers must be converted into blockchain adapters, and this is a major limitation. There is also the problem of scalability that is not addressed.

Guang Yang et.al. [28] present an architecture for EHR systems by using blockchain. This architecture can be combined with the existing databases of healthcare providers. Any operation that is being performed on these databases is recorded on the blockchain. In addition to this access permissions and ownership details are also stored on the contract. A new incentive mechanism is also being proposed based on significance. Selection of nodes that appends a new block to the existing chain is based on this mechanism.

Zhuang et. al. [29] propose a system that enables exchange of health information and monitoring of clinical trials. The system uses private blockchain and the miners are provided by the clinical facility. Smart contracts are designed for various scenarios and are deployed by the owner which is the FDA. Remote Procedure Call (RPC) servers are used to communicate with the databases in the clinical facilities. Patients give Clinicians access to their data. These servers fetch the data from various databases and give it to the smart contract that requested the data. Data transfer is encrypted by the RPC servers and the Encryption key is sent to the smart contract. This key is then sent to the requesting node and the data is decrypted.

Lee et. al. designed an HIE framework - MEXchange [30], that hides sender and receiver addresses to avoid privacy issues. This framework contains various smart contracts and workflows that use ring signature and stealth address for privacy by preventing inference problems. MEXchange is implemented on the Ethereum private network and PoW (Proof-of-Work) consensus algorithm is used. The framework's performance is evaluated based on various metrics. The main limitation of the proposed framework is increase in transaction delay as the number of transactions increase. The ring signature verification requires many operations and hence the system consumes a lot of time to process the requests.

K. Fan et. al. [31] have proposed MedBlock, a data management system based on blockchain, to handle the medical information of patients. The proposed system uses a distributed ledger that allows the efficient access and retrieval of electronic medical records (EMRs). In order to avoid high power consumption and congestion in the network, the authors have given an improved consensus algorithm. This algorithm uses symmetric cryptography along with customized access control protocols. MedBlock solves the issue of scalability and data sharing of medical records. Since there is a common blockchain, patients can retrieve their medical data from different hospitals. The architecture is shown in Fig 4.

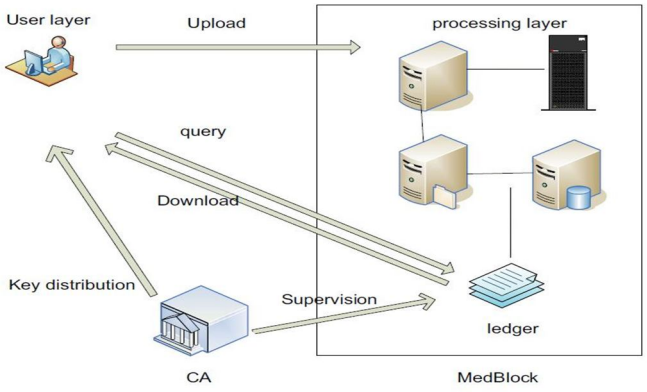


Fig 4 [31]

MeDShare [32] is a system for sharing medical data among the providers in an unreliable environment. The system has various layers that are responsible for performing various operations. Data is tracked using smart contracts and all transactions are performed in a tamper-proof manner. Deviation from usual behaviour is detected using the threat model. The model has two threat levels to ensure no data is being modified without the concern of responsible authority and to maintain confidentiality of medical reports. Whenever a violation is detected, access permissions are revoked. It aims to achieve auditing and data provenance when medical data is being shared with other entities to reduce privacy risks.

Author	Year	Blockchain type	Consensus Mechanism	Implementation	Performance Analysis
Han et. al. [11]	2018	Consortium Blockchain and Fully Private Blockchain as a Hybrid Blockchain	Proof of Work (PoW)	✘	✘
Zhang et. al. [12]	2018	Private blockchain and consortium blockchain	Proof of conformance	✔	✔
Buzachis et. al. [20]	2019	Private Blockchain	Clique - Proof-Of-Authority (PoA)	✔	✔
Liu et. al. [22]	2019	Private Blockchain	Improved delegated proof of stake	✔	✔
Azaria et. al. [24]	2016	Ethereum based Blockchain	Proof of Work (PoW)	✔	✘
Griggs et. al. [25]	2018	Private Blockchain	Practical Byzantine Fault Tolerance (PBFT)	✔	✘
Dagher et. al. [26]	2018	Permissioned Ethereum Blockchain	QuorumChain Consensus algorithm	✔	✔
Zhuang et. al. [29]	2018	Private Blockchain	Proof of Stake (PoS)	✔	✘
Jiang et. al. [34]	2018	Two loosely-coupled Blockchain	Proof of Work (PoW)	✔	✔
Purohit et. al. [35]	2021	Consortium Blockchain	Proof of Authorization (POA)	✔	✔

4) Other off-chain solutions

This paper [33] proposes a medical data preservation system (DPS) based on blockchain. To guarantee the primitiveness and authenticity of the data while safeguarding the privacy of users, DPS can be divided into two parts, the first one being the data access program which is responsible for submitting, manipulating, querying, and verifying the data. The second half, the blockchain interaction program is responsible for storing and extracting data to and from the blockchain.

Shan Jiang et. al. in [34] propose a Health Information Exchange platform, BlocHIE, based on blockchain. Two types of health data i.e., electronic health records and Personal Health data are considered. In order to store these data two loosely coupled blockchains EMR chain and PHD chain are designed respectively. The data that is signed by both patient and hospital are published on the first chain whereas data collected from smart IoT devices are stored on the second chain. Only the time stamped hash values with signatures are stored on the blockchain rather than complete information. This ensures data not being publicly accessible, thus preserving privacy of patients' data. This also improves throughput of the network by not storing the original records that are larger in size. Moreover, to increase throughput and fairness amidst the users, two fairness-based transaction packing algorithms are proposed. *Fig 5* shows the proposed architecture.

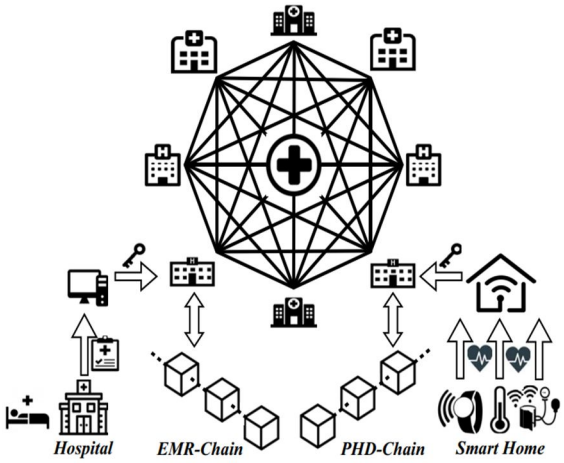


Fig 5 [34]

The authors propose HonestChain [35], a health information sharing system based on blockchain. The presented system makes use of consortium blockchain and interfaces with chatbot support. This helps to stick to data access standards and to gain reputation. Shorter deployment duration, less resource intensive properties are the reasons for deploying a permissioned blockchain.
Public blockchains on the other hand have open access and no barrier for participating nodes. The main contribution of this paper is reduced Loss of value/opportunity issues. Hyperledger Composer is used for implementing test bed and evaluation of the proposed system. Findings show that the system has better performance for service time and request resubmission rate metrics.
Zhang et al. [36] proposed a PSN-based healthcare system which enables wireless sensor devices to share medical data. The authors have designed two protocols to implement the system. One is to establish a secure communication link for the sensor nodes. Another protocol is to enable these devices to share data on the blockchain. The blockchain has addresses stored in them, and nodes can visit each other.
Dubovitskaya, A et.al. [37] provide their standpoints on EMR sharing among the medical facilities. The authors propose a framework on managing and exchanging the EMR for cancer patient's care. This framework can considerably reduce the turnaround time for EMR sharing, improve the decision-making process for medical care, and lower the overall cost. The authors also justify the selection of the permissioned blockchain technology for the implementation of the various scenarios.
Kevin Peterson et.al. [38] discuss the two main issues during exchange of the medical health record - security and data consistency. The authors outline a Blockchain-based method for sharing patient data. This strategy substitutes network consensus for a single, centralized source of trust and bases it on evidence of structural and semantic compatibility.

III.CONCLUSION

In this paper, we surveyed how blockchain can be pivotal in improving security, reliability, and availability of health data. Using this technology, we can create a shield against tampering and malicious attacks on a patient's personal medical information. It is also crucial in making the process of managing such data with ease and efficiency. We understand that we can use smart contracts, one of the very fine features of blockchain, to process various requests and queries related to patients. All the stakeholders should be able to view and retrieve the health data from a distributed data storage without having to compromise on its credibility.
We surveyed the relevant research papers on blockchain technologies and how blockchain is being employed in the field of healthcare. We have summarized some of the relevant papers in this domain into a literature review. The ultimate goal of this literature review was to explore the research topics of blockchain technology in the healthcare domain, along with its key impacts on this field. Our findings suggest that inclusion of blockchain in healthcare has capability to improve authenticity and transparency of medical data and to enhance and revolutionize healthcare services.

REFERENCES

[1] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), 2017, pp. 557-564, doi: 10.1109/BigDataCongress.2017.85.
[2] Zhang, P., Schmidt, D.C., White, J., & Lenz, G. (2018). Chapter One - Blockchain Technology Use Cases in Healthcare. Adv. Comput., 111, 1-41.

[3] Al Omar, A., Rahman, M.S., Basu, A., Kiyomoto, S. (2017). MediBchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data. In: Wang, G., Atiquzzaman, M., Yan, Z., Choo, KK. (eds) Security, Privacy, and Anonymity in Computation, Communication, and Storage. SpaCCS 2017. Lecture Notes in Computer Science(), vol 10658. Springer, Cham. https://doi.org/10.1007/978-3-319-72395-2_49
[4] Thomas McGhin, Kim-Kwang Raymond Choo, Charles Zhechao Liu, and Debiao He. 2019. Blockchain in healthcare applications: Research challenges and opportunities. J. Netw. Comput. Appl. 135, C (Jun 2019), 62–75. https://doi.org/10.1016/j.jnca.2019.02.027
[5] C. Agbo, Q. Mahmoud, and J. Eklund, "Blockchain Technology in Healthcare: A Systematic Review," Healthcare, vol. 7, no. 2, p. 56, Apr. 2019, doi: 10.3390/healthcare7020056.
[6] M. Hölbl, M. Kompara, A. Kamišalić, and L. Nemec Zlatolas, "A Systematic Review of the Use of Blockchain in Healthcare," Symmetry, vol. 10, no. 10, p. 470, Oct. 2018, doi: 10.3390/sym10100470.
[7] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), 2016, pp. 1-3, doi: 10.1109/HealthCom.2016.7749510.
[8] Juan M. Roman-Belmonte, Hortensia De la Corte-Rodriguez & E. Carlos Rodriguez-Merchan (2018) How blockchain technology can change medicine, Postgraduate Medicine, 130:4, 420-427, DOI: 10.1080/00325481.2018.1472996
[9] B. A. Tama, B. J. Kweka, Y. Park and K. -H. Rhee, "A critical review of blockchain and its current applications," 2017 International Conference on Electrical Engineering and Computer Science (ICECOS), 2017, pp. 109-113, doi: 10.1109/ICECOS.2017.8167115.
[10] Sudeep Tanwar, Karan Parekh, Richard Evans, Blockchain-based electronic healthcare record system for healthcare 4.0 applications, Journal of Information Security and Applications, Volume 50, 2020, 102407, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2019.102407.
[11] Han, H., Huang, M., Zhang, Y., Bhatti, U.A. (2018). An Architecture of Secure Health Information Storage System Based on Blockchain Technology. In: Sun, X., Pan, Z., Bertino, E. (eds) Cloud Computing and Security. ICCCS 2018. Lecture Notes in Computer Science(), vol 11064. Springer, Cham. https://doi.org/10.1007/978-3-030-00009-7_52
[12] Zhang, A., Lin, X. Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. J Med Syst 42, 140 (2018). https://doi.org/10.1007/s10916-018-0995-5
[13] Murugan, A. & Chechare, Tushar & Muruganantham, B. & Kumar, S.. (2020). Healthcare information exchange using blockchain technology. International Journal of Electrical and Computer Engineering (IJECE). 10. 421. 10.11591/ijece.v10i1.pp421-426.
[14] Xia Q, Sifah EB, Smahi A, Amofa S, Zhang X. BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments. Information. 2017; 8(2):44. https://doi.org/10.3390/info8020044
[15] X. Zheng, R. R. Mukkamala, R. Vatrapu and J. Ordieres-Mere, "Blockchain-based Personal Health Data Sharing System Using Cloud Storage," 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), 2018, pp. 1-6, doi: 10.1109/HealthCom.2018.8531125.
[16] S. Wang, D. Zhang and Y. Zhang, "Blockchain-Based Personal Health Records Sharing Scheme With Data Integrity Verifiable," in IEEE Access, vol. 7, pp. 102887-102901, 2019, doi: 10.1109/ACCESS.2019.2931531.
[17] Lanxiang Chen, Wai-Kong Lee, Chin-Chen Chang, Kim-Kwang Raymond Choo, and Nan Zhang. 2019. Blockchain based searchable encryption for electronic health record sharing. Future Gener. Comput. Syst. 95, C (Jun 2019), 420–429. https://doi.org/10.1016/j.future.2019.01.018
[18] Yue, X., Wang, H., Jin, D. et al. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. J Med Syst 40, 218 (2016). https://doi.org/10.1007/s10916-016-0574-6
[19] A. Shahnaz, U. Qamar and A. Khalid, "Using Blockchain for Electronic Health Records," in IEEE Access, vol. 7, pp. 147782-147795, 2019, doi: 10.1109/ACCESS.2019.2946373.
[20] A. Buzachis, A. Celesti, M. Fazio and M. Villari, "On the Design of a Blockchain-as-a-Service-Based Health Information Exchange (BaaS-HIE) System for Patient Monitoring," 2019 IEEE Symposium on Computers and Communications (ISCC), 2019, pp. 1-6, doi: 10.1109/ISCC47284.2019.8969718.
[21] N. Rifi, E. Rachkidi, N. Agoulmine and N. C. Taher, "Towards using blockchain technology for eHealth data access management," 2017 Fourth International Conference on Advances in Biomedical Engineering (ICABME), 2017, pp. 1-4, doi: 10.1109/ICABME.2017.8167555.
[22] X. Liu, Z. Wang, C. Jin, F. Li and G. Li, "A Blockchain-Based Medical Data Sharing and Protection Scheme," in IEEE Access, vol. 7, pp. 118943-118953, 2019, doi: 10.1109/ACCESS.2019.2937685.
[23] J. Vora et al., "BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records," 2018 IEEE Globecom Workshops (GC Wkshps), 2018, pp. 1-6, doi: 10.1109/GLOCOMW.2018.8644088.
[24] A. Azaria, A. Ekblaw, T. Vieira and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," 2016 2nd International Conference on Open and Big Data (OBD), 2016, pp. 25-30, doi: 10.1109/OBD.2016.11.
[25] Griggs, K.N., Ossipova, O., Kohlios, C.P. et al. Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. J Med Syst 42, 130 (2018). https://doi.org/10.1007/s10916-018-0982-x
[26] Gaby G. Dagher, Jordan Mohler, Matea Milojkovic, Praneeth Babu Marella, Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology, Sustainable Cities and Society, Volume 39, 2018, Pages 283-297, ISSN 2210-6707, https://doi.org/10.1016/j.scs.2018.02.014.
[27] Y. Zhuang, L. R. Sheets, Y. -W. Chen, Z. -Y. Shae, J. J. P. Tsai and C. -R. Shyu, "A Patient-Centric Health Information Exchange Framework Using Blockchain Technology," in IEEE Journal of Biomedical and Health Informatics, vol. 24, no. 8, pp. 2169-2176, Aug. 2020, doi: 10.1109/JBHI.2020.2993072.
[28] G. Yang and C. Li, "A Design of Blockchain-Based Architecture for the Security of Electronic Health Record (EHR) Systems," 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), 2018, pp. 261-265, doi: 10.1109/CloudCom2018.2018.00058.
[29] Zhuang Y, Sheets L, Shae Z, Tsai JJP, Shyu CR. Applying Blockchain Technology for Health Information Exchange and Persistent Monitoring for Clinical Trials. AMIA Annu Symp Proc. 2018 Dec 5;2018:1167-1175. PMID: 30815159; PMCID: PMC6371378.
[30] D. Lee and M. Song, "MEXchange: A Privacy-Preserving Blockchain-Based Framework for Health Information Exchange Using Ring Signature and Stealth Address," in IEEE Access, vol. 9, pp. 158122-158139, 2021, doi: 10.1109/ACCESS.2021.3130552.
[31] Fan, K., Wang, S., Ren, Y. et al. MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. J Med Syst 42, 136 (2018). https://doi.org/10.1007/s10916-018-0993-7

[32] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du and M. Guizani, "MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain," in IEEE Access, vol. 5, pp. 14757-14767, 2017, doi: 10.1109/ACCESS.2017.2730843.

[33] Li, H., Zhu, L., Shen, M. et al. Blockchain-Based Data Preservation System for Medical Data. J Med Syst 42, 141 (2018). https://doi.org/10.1007/s10916-018-0997-3

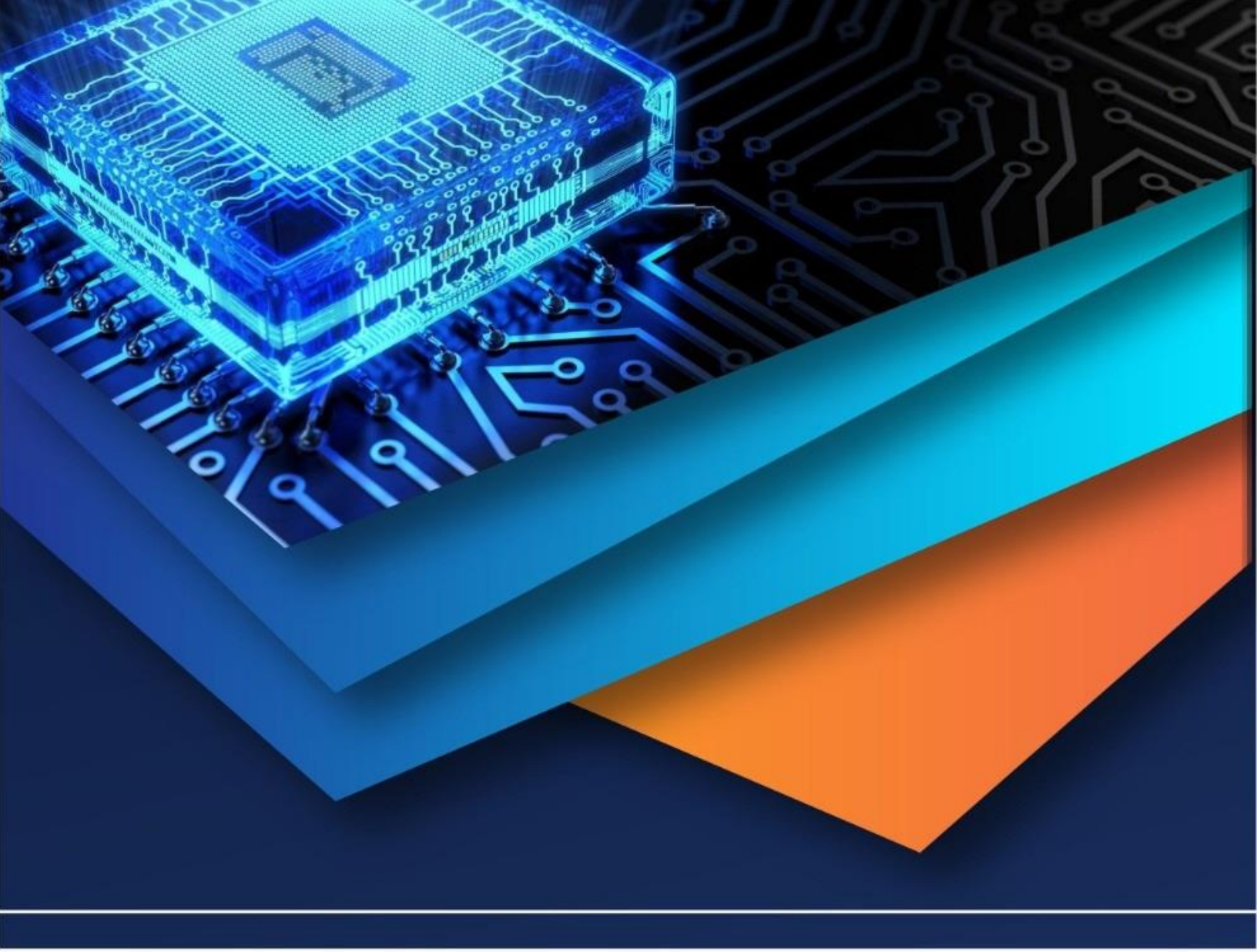
[34] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma and J. He, "BlocHIE: A BLOCkchain-Based Platform for Healthcare Information Exchange," 2018 IEEE International Conference on Smart Computing (SMARTCOMP), 2018, pp. 49-56, doi: 10.1109/SMARTCOMP.2018.00073.

[35] Purohit, S., Calyam, P., Alarcon, M.L. et al. HonestChain: Consortium blockchain for protected data sharing in health information systems. Peer-to-Peer Netw. Appl. 14, 3012–3028 (2021). https://doi.org/10.1007/s12083-021-01153-y

[36] J. Zhang, N. Xue and X. Huang, "A Secure System For Pervasive Social Network-Based Healthcare," in IEEE Access, vol. 4, pp. 9239-9250, 2016, doi: 10.1109/ACCESS.2016.2645904.

[37] Dubovitskaya A, Xu Z, Ryu S, Schumacher M, Wang F. Secure and Trustable Electronic Medical Records Sharing using Blockchain. AMIA Annu Symp Proc. 2018 Apr 16;2017:650-659. PMID: 29854130; PMCID: PMC5977675.

[38] Peterson, K.J., Deeduvanu, R., Kanjamala, P., & Mayo, K.B. (2016). A Blockchain-Based Approach to Health Information Exchange Networks.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY