Blockchain in Healthcare for Achieving Patients' Privacy

Esraa Elgamal
Information System
Benha University
Cairo, Egypt
esraa.Kamal@fci.bu.edu.eg

Walaa Medhat
Benha University, Nile University
Cairo, Egypt
wmedhat@nu.edu.eg

Mohamed Abd Elfatah
Benha University
Cairo, Egypt
mohamed.abdo@fci.bu.edu.eg

Nashwa Abdelbaki
Nile University
Cairo, Egypt
nabdelbaki@nu.edu.eg

***Abstract*—Heath data are sensitive and valuable for individuals. The patients need to integrate and manage their medical data continuously. Personal Health Record (PHR) is introduced as a solution for managing their health information. It gives patients ownership over their medical data and provides physicians with realignment data. However, it does not achieve reliability, traceability, trust, nor security of patient control. Centralization of any data is vulnerable to the problem of hacking and single failure in addition to control from one organization. So, the centralization of data is the common problem that all current healthcare systems suffer from. Even in the Metaverse world, the application of Metaverse in healthcare services loses users' privacy as one of its challenges. In this study, we suggest using blockchain in healthcare to improve security and privacy in medical records. The proposed system employs the advantages of blockchain technology to give patients full control over their data with low throughput, high overhead, and latency. We present a security analysis of our suggested architecture as well as blockchain issues in healthcare systems.**

Keywords—blockchain, Ethereum, healthcare, big data, smart contract, EMRs' access control.

I. INTRODUCTION

Healthcare systems have changed recently from 1.0 to 4.0. It has started from version 1.0 where it was physicians centric and manual records to evolve to Healthcare 2.0 where Electronic Healthcare Records (EHRs) are found. Healthcare 3.0 was aimed at the patient, but Healthcare 4.0 was focused on data sharing across many stakeholders through the use of technologies such as Telehealth, Internet of Things (IoT), Cloud Computing and Fog Computing[1]. The IoT and wearable technologies have significantly changed the healthcare sector of the IT industry. Patients in general use PHR (Personal Health Record) and EMR/EHR (Electronic Medical Record /Electronic Health Record) to manage their healthcare data. TABLE I. demonstrates the main differences between EHR and PHR. The healthcare sector has witnessed an increase in both opportunities and challenges[2]. EHR market, nowadays, may be counted in tens of billions of dollars [3]. However, EHR suffers from many security issues such as transparency, trustfulness, traceability, immutability, auditing, and privacy. Fig. 1 shows the types of problems in healthcare applications summarized in data security, privacy, integrity, and interoperability problems [4]. This is in addition to access control in medical systems and management of the massive volumes of patient data.

TABLE I. COMPARISON BETWEEN EMR/PHR

	EMR/EHR	**PHR**
Controlled by	Physicians	Patients
Definition	The patient's medical history, including diagnoses, prescriptions, treatment plans, allergies, and laboratory test results, is digitally captured.	This digital service's purpose is to provide a user-friendly interface and assistance for many MIS (Management Information Systems).
Examples	Athenahealth AdvancedMD drchrono	Apple Health Google Health Practice Fusion
Disadvantages	- High upfront acquisition costs -Ongoing maintenance cost. - Workflow interruptions result in a loss of productivity.	- Time and effort needed for collecting data from MIS. -Sharing data with third party. -Centralization which leads to lose immutability, privacy, traceability.

The rest of this paper is divided into six sections. Section II focuses more on blockchain-based features and their significance to the healthcare sector. Section III summarizes prior research on the use of blockchain technology in healthcare. Section IV focuses on the suggested systematic architecture, its components, and interaction scenarios. Section V examines the suggested approach in terms of security and privacy analysis, as well as how it might tackle blockchain challenges in EHR systems. Section VI summarizes the article and discusses future research.

979-8-3503-0030-7/23/$31.00 ©2023 IEEE

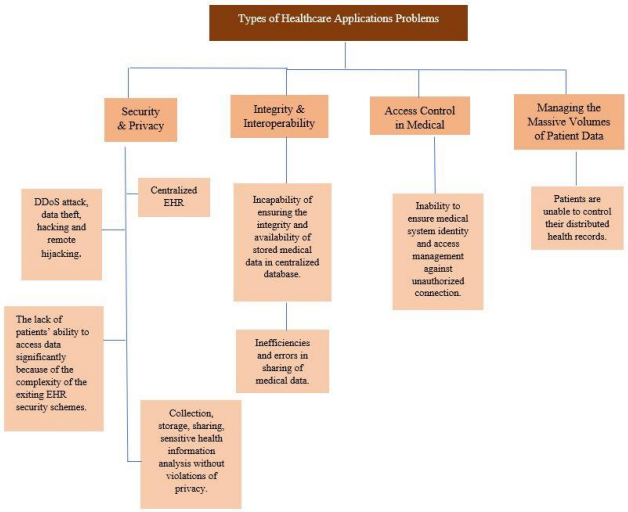

Fig. 1. Types of Healthcare Applications problem

II. Blockchain Overview

Blockchain is a hybrid of two technologies: cryptography and peer-to-peer networking. It was introduced in 2008 for Bitcoin by Satoshi Nakamoto [5] and increased its need with each technical advancement. Bitcoin is the first digital cryptocurrency. It does not rely on a third party but requires massive computational power from linked nodes and use SHA-256 hashing. Blockchain has caused a huge technological uproar, especially with the advent of the virtual world and the emergence of metaverse. Blockchain technology is being used extensively in the implementation of the metaverse system. It achieves digital assets, digital currency, and the digital market for the metaverse [6]. Node, transaction, block, chain, miners, and consensus are the most important concepts in blockchain [7]. Fig. 2 shows the sequence of processes for adding a new block to the blockchain. A new block contains the latest transactions that occurred since the last block. Participants compete to validate the block and the first node compute the hash is rewarded. Finally, the verified block is added to the chain, and all authorized participants can access it.

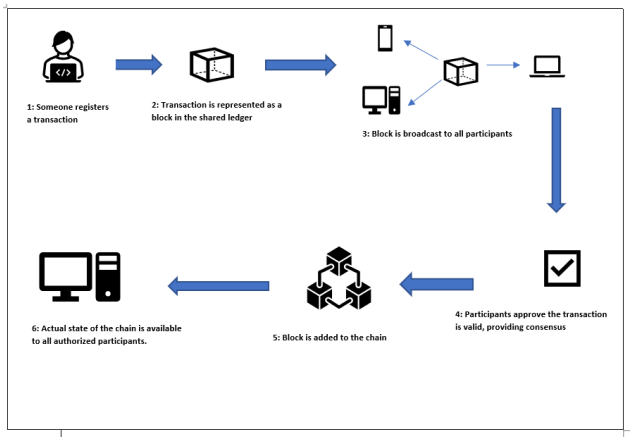

Fig. 2. The Blockchain Process

From these blocks the blockchain is made up. Fig. 3 shows the blockchain architecture. The blocks are linked together by the hash value of the preceding block.

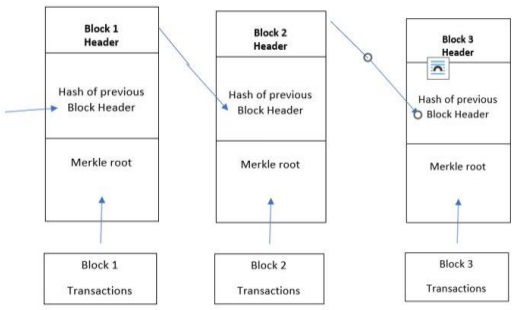

Fig. 3. Blockchain Architecture

Blockchain enables users to exchange and track their data as well as other actions that take place in the healthcare system without having to seek additional integrity and security options [4]. Three types of blockchain namely public blockchain, private blockchain, and consortium blockchain [8], can be utilized based on the access needs and permissions of network members. Fig. 4 shows to what extent blockchain is needed in healthcare systems. Introducing blockchain to any software system [9] leads to three choices: no need for blockchain, needed permissioned blockchain, or permissionless blockchain. Permissioned blockchain may be private or consortium blockchain, but permissionless blockchain is public blockchain [4]. Blockchain can achieve many benefits for healthcare data management system. It can eliminate the threat of data theft or mishandling. Natural disasters do not pose a threat to health data held on blockchain. [10]. It enables medical institutions to share access and traceability and the auditors may readily check transactions using blockchain. It prevents excessive data redundancy and keeps healthcare organizations compliant with essential legal requirements and laws [11].

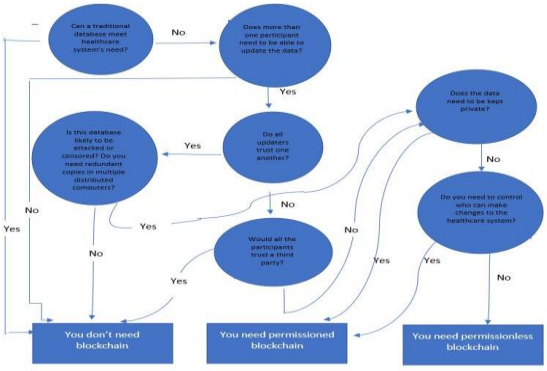

Fig. 4. The Need for Blockchain in Healthcare

III. Literature Review

security and privacy problems in Healthcare 4.0 were discussed by authors in [1].Theoretically, they demonstrated that the blockchain technology can solve the security and privacy issues of healthcare 4.0 by investigating attacks on several layers of healthcare systems.

In [4] authors recommended to researchers to investigate how to monitor a certain user and collect all of the communications he or she has sent while keeping the individual's sensitive information hidden. They claimed that the secure multiparty computation is a potential method for letting an unreliable third party use medical data for calculations without invading the patients' privacy.

The authors in [7] explained how consortium blockchain as MedChain, ModelChain, and BlockInsure are more suitable for health information security. It can eliminate redundancy and provide caretakers with consistent records about their patients.

According to [12], healthcare data are vulnerable to violations such as 6% data loss, 10% unknown data, 10% theft of data, 12% unauthorized or disclosure, and 62% hacking/IT incidents. It demonstrated the research efforts made to control health data integrity and proposed that the blockchain is the most priority data integrity technology.

As shown in [13], two significant security issues have arisen in Electronic Health Systems (EHS). The first is choosing an access control method without considering previous users' data. The second question is how much data the healthcare services practitioner will disclose. The authors proposed an access control model based on the user's level of confidence in the healthcare provider.

The authors of [14] discussed risks relating to EHRs, these risks are unauthorized users trying to access patients' record and missing of trust between different parties. Blockchain is presented as a solution for authorization and access control problem in healthcare system-based on cloud technology.

In [15] authors categorized blockchain applications in healthcare into three categories. First category is Electronic Medical Record (EMR) improvement for scalability, security, and data duplication. The second is to improve insurance claim procedures, such as smart health profiles, and medical records sharing using smart contracts. Facilitating data exchange among researchers is the third category and allowing private engagement between consumers and caregivers is the fourth.

According to the survey study in [16], problems of access control, data integrity and interoperability, privacy, and security for patient health records are the biggest challenges facing blockchain integration in healthcare authors discussed.

In [17] the authors provided an overview of blockchain-based healthcare applications. MedRec handles medical records and provides patients with access to them through record reviews, care auditability, and data sharing. The BlockHie application is used to share healthcare information for EMR and PHR. The MedShare enables cloud service providers to share data. It lowers latency, which aids data processing and anonymization. To handle personal health data, applications for data sharing and privacy leverage batching and a tree-based data processing architecture based on the Hyperledger. Their study focused on merging medical data with personal health data.

Blockchain applications for healthcare have lately appeared in many countries, as highlighted in [18]. For example, the Estonian government began a blockchain-based project in 2016 to ensure that 95%-99% of the country's patients had access to electronic health information. The UAE Ministry of Health and Prevention (MoHAP) has announced the development of a blockchain-platform for storing healthcare data in order to enhance storage and strengthen data security across national healthcare systems. Swiss hospitals have developed a blockchain-based system to track medical devices in a reliable and efficient manner. On the other hand, the Patientory Dapp that is an online platform that provides patients with safe, flexible access to EMR in a private, permissioned blockchain environment.

In [19] The authors introduced a blockchain-based Self-Sovereign Identity (SSI) architecture for healthcare. That gave users complete control over their personal data across multiple authorities. This design enabled the changing of shared data in near real time.

In [20] the authors proposed an access control system based on Blockchain that protects patients' privacy. They developed a strategy based on reducing data redundancy by mining clustering, which lowers network overhead and makes transactions small enough to be transmitted across blockchain. Each patient in this model has a pseudonym, and their data has been stored and processed at the nearest location to them.

The Systematic Literature Review in [21], answered three main questions in blockchain-based healthcare. First, what are the structures and issues of integrating blockchain to the healthcare sector, as well as the uses of blockchain in healthcare systems? Second, what are the temporal, technological, and geographical characteristics of recently existing blockchain applications? Third, what are the study's next steps in building and implementing a blockchain-based healthcare system?.

In [22], the authors proposed a smart contract system to provide patients authority over their records. To securely store, retrieve, and distribute patients' medical data, they used the Interplanetary File System (IPFS) and trusted reputation-based re-encryption oracles.

From our survey study, we conclude that there is still a problem with patients' privacy and how to control their data access in EMR. According to the systematic analysis on blockchain integration with healthcare [16], Access Ccontrol is a major challenge with percentage of 17% of total challenges.

IV. Blockchain-Based solution Proposed

In this part, we explain the details of our proposed blockchain-based access control architecture for providing patients with privacy and total control over their data. We describe the system components and the system architecture.

A. Ethereum

It is launched following bitcoin's success as a blockchain platform for digital currency. Ethereum first launched as an open-source and blockchain platform [23] in 2013. Ethereum's native cryptocurrency is ether, which is used to fuel the Ethereum ecosystem. The Ethereum network is well-known for its ability to run smart contracts on a custom-built blockchain. When invoked with certain parameters, the smart contract functions similarly to a vending machine. It performs some actions or computation if certain conditions are satisfied [24]. Any developer may write a smart contract and publish it to the network, with the blockchain serving as its layer data. Then, for a charge paid to the network, any user may call this smart contract and have it perform its function again. Ethereum used to use Proof of Work (PoW) consensus algorithm like bitcoin, but on September 15, 2022, at 2:45 am EST, Ethereum has transitioned to a consensus mechanism called Proof-of-Stake (PoS), which uses far less power and should make the network about 99% more energy-efficient [25]. Well, Ethereum is trying to be the computer of the Internet, and the main component of any computer is its operating system which is the EVM (Ethereum Virtual Machine) in our case. EVM is a single entity maintained by numerous connected computers running on an Ethereum client. It is a runtime environment for smart contracts. It consists of stack, memory, storage, and gas balancer [26].

B. *Interplanetary File System (IPFS)*

IPFS is a distributed file system that uses a peer-to-peer network to store and share data . HTTP address locations points to an IP address of a machine hosting the content. IPFS flips this. Based on content addressing, it identifies each file in a global namespace that connects all computing devices. It identifies each file in a global namespace connecting all computing devices based on content addressing [27]. IPFS uses filecoin cryptocurrency as a reward to encourage people to share their hard disk in IPFS network. IPFS has no Single Point of Failure since nodes do not need to trust each other.

C. *Practical Byzantine Fault Tolerance (PBFT)*

Over all other consensus algorithms, PBFT offers a distinct advantage. In POW, each block required its own pow round, while in PBFT, no miner is solving the typical hashing algorithm. As a result, it consumes less energy and does not require confirmation. [28] [29]. PBFT allows only 1/3 faults, if total nodes=3f+1 then it handles f Byzantine faults.

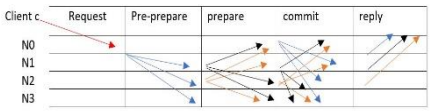

Fig. 5. PBFT consensus algorithm

PBFT composes of three phases pre-prepare, prepare, and finally commit phases. PBFT begins when the client submits a request to the primary node. Advocating for the client's request is the responsibility of the primary node. As illustrated in Fig. 5, N0 is the principal node in our scenario. It contains four nodes, which means that each node should be able to hold 1 fault. If N3 drops out due to a spotty Internet connection, the other three nodes may not realize it and continue to transmit messages to him/her. N0 transmits the pre-prepared message to everyone on the network during the pre-prepare stage. A node is considered "prepared" in the prepare stage if it has seen the initial request from the primary node, has pre-prepared, and has seen 2f prepare messages that match its pre-prepared, resulting in 2f+1 prepares. The client waits for f+1 of the same reply since we allow for at most f fault. We need to wait for at least f+1, and this ensures the response to be valid.

D. *Overall System Architecture*

In our suggested design, we modify in the architecture of Ethereum blockchain and depend on choosing miners within the hospitals and grouping them in to decrease the network overhead and reduce the data redundancy. We encrypt the medical record data using symmetric key (patient public key (K_{pp}), patient private key (K_{sp})) and then store the encrypted data in IPFS. On smart contracts, blockchain is utilized to store hashes of patients' healthcare data as well as patients' access policies to their data.. The doctor can access these data if he has privilege and can decrypt the symmetric key using his private key. Fig. 6 The diagram depicts the system's key components.

a) *Regulatory Orgnization:* is in responsibility of users' registration (hospitals, medical staff, patients).

b) *Insurance company:* is responsible for the finance system.

c) *Hospitals:* are in responsibility of assigning a health wallet to each patient and medical staff member, as well as allocating a cluster miner to each patient. They are transferring the medical record files and patients' symmetric keys to their patients.

f) *Blockchain:* is used to store data hashes and access controls.

g) *Decentralized* Database storge IPFS: stores encrypted medical record files off-chain.

h) *Miners*: can be from hospital and healthcare centers or outside.

i) *Patient Smart Contract (PSC):* is responsible for storing metadata (title, creation data, description of the file, access policies, a log of all requests for access) for the patient record.

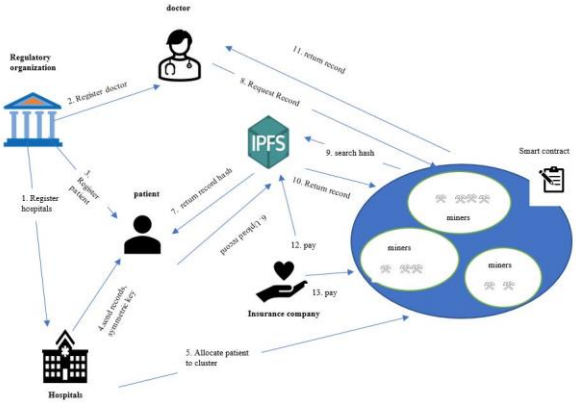

Fig. 6. The major components of our system

E. *Interaction Scenario*

A simple use-case scenario for sharing a medical file with a doctor is shown in Fig. 7. This sequence starts after the patient has received a symmetric key and the medical records from a hospital, and all the entities have been registered by regulatory agency. The following is the sequence of actions:

1. The patient: has public key (K_{pp}) and private key (K_{sp}) then uploads the encrypted medical records on IPFS.
2. IPFS sends record hash value, the hash of the encrypted medical data is saved on-chain.
3. The doctor: asks for access to the patient's medical record.
4. According to access policies for this record file in PSC, the doctor will receive the accepted response or rejected.
5. PSC: fetches the required file from IPFS. This file contains medical record data and symmetric key downloaded as a bundle.
6. If the request is accepted: PSC informs the doctor That a data request has been granted and transmits the encrypted medical record.
7. The doctor: uses his private key (K_{SD}) to decrypt the symmetric key.

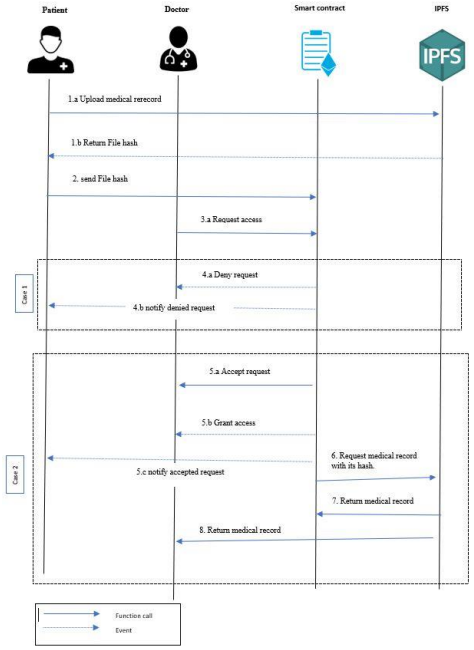

Fig. 7. medical record access sequence diagrams

F. *Patients' Data Policies*

Patients send the policies for data access to cluster miners as a transaction in this form:

< $Patient_{ID}$, $Request_{ID}$, DataType, $Time_e$, validity >

- $Patient_{ID}$: the ID of the patient.
- $Request_{ID}$: the ID for the individual who has access to the data (medical staff).
- DataType : data kind accessed by $Request_{ID}$.
- $Time_e$: the policy expiration date.
- Validity : the binary value 1 or 0 for valid or invalid policy.

V. Analysis and Discussion

In this section, we analyze and evaluate the proposed solution in terms of security and privacy and analyze the blockchain problems of healthcare systems. Theoretically, we explain how our suggested method may overcome several security issues for EMRs as well as other issues for blockchain applications in the healthcare area.

A. *Analysis of Security and Privacy*

In this section, we discuss how the suggested system architecture may address privacy and security issues that were mentioned earlier in Fig. 1. TABLE II. discusses the security and privacy performance of our proposed architecture in healthcare applications.

B. *Blockchain problems in EHR*

When we combined blockchain revolution technology with healthcare systems, which is one of the most important sectors in our everyday lives, we encountered several obstacles that we attempted to address in our suggested solution.TABLE III. shows these challenges and our solutions for them.

TABLE II. PROPOSED ARCHITECTURE SECURITY ANALYSIS

Threat	Definition	Defense	Flexibility
Centralization	Centralized data can be exposed to Single Point of Failure.	Ethereum blockchain and IPFS makes this system completely decentralized.	High
DDoS attack	To disrupt the network, the attackers produce a high number of transactions.	To make its DNS infrastructure impervious to DDoS assaults, it is using the Ethereum blockchain and IPFS, a distributed alternative to HTTP's centralised structure.	Moderate
Data theft & hacking	Hackers try to steal or alter sensitive data through transmission.	Blockchain's immutability is a key feature, since the patients' record data is encrypted before being transmitted to the patient and saved as encrypted data in IPFS and hash value in blockchain, making it harder to hack this data.	High
Access Control	The lack of patients' ability to access data significantly.	The smart contract's patient policies transaction determines who can access data also the system will notifying the patient with all requests access.	High
Confidentiality	only authorised users should be able to view the messages.	The requested data is transmitted encrypted to the doctor.	High

TABLE III. BLOCKCHAIN ANALYSIS OF OUR PROPOSED ARCHITECTURE

Challenge	Definition	Defense
Limited size	Large documents, such as comprehensive electronic medical records or genetic data records, would be inefficient and costly to store on the blockchain.	Using IPFS as a datastore for medical records and only the file hash is stored in the blockchain.
High energy consumption	The amount of computing power required to manage all the data in blockchain is very high.	We use PBFT which is characterized by lower energy consumption compared to PoW and PoS.
Transaction throughput	Because Ethereum mining does not use parallel computing, the number of successful transactions per second remains low.	Because of clustering and allocating each patient transaction to a different cluster. This causes transactions to run in parallel and increases the number of transactions.
51% attack	The attacker has control of more than 51% of the miners and is attempting to construct a fake block.	Choosing the miners from various health centers and hospitals and using PBFT consensus algorithm makes it difficult to occur.

Public blockchain modification	The attacker declares a fake ledger and makes it the longest.	Because of the miners are known, so they are unable to construct harmful blocks..
Denial of Service (DOS)	The attacker generates a huge number of transactions in order to disrupt the blockchain network.	Because of clustering, Instead of affecting all nodes in the network, trace flooding will only affect a selection of clusters.
Sybil attack	The attacker operates several active fake identities from a single node, gaining the majority of network impact.	Users cannot construct false blocks due to each cluster has a large number of miners.

VI. Conclusion

In this paper, we propose a new architecture based on the blockchain technology to enable patients to control their sensitive health data. In this architecture, we depend on private blockchain and make set of clusters of miners and integrated our solution with IPFS that store encrypted data to securely store, fetch, and share patients' healthcare data. Patients can store access policies over their data to control who has access to it. We discuss our solution in terms of security and privacy and show how our solution can solve the problems of integrating blockchain with EHR. We will implement the architecture and assess its performance in the future.

References

[1] J. J. Hathaliya and S. Tanwar, "An exhaustive survey on security and privacy issues in Healthcare 4 . 0," *Comput. Commun.*, vol. 153, no. January, pp. 311–335, 2020.

[2] A. G. ALEXANDRU, I. M. RADU, and M.-L. BIZON, "Big Data in Healthcare - Opportunities and Challenges," *Inform. Econ.*, vol. 22, no. 2/2018, pp. 43–54, 2018.

[3] N. Tariq, A. Qamar, M. Asim, and F. A. Khan, "Blockchain and smart healthcare security: A survey," *Procedia Comput. Sci.*, vol. 175, no. 2019, pp. 615–620, 2020.

[4] H. M. Hussien, S. M. Yasin, S. N. I. Udzir, A. A. Zaidan, and B. B. Zaidan, "A Systematic Review for Enabling of Develop a Blockchain Technology in Healthcare Application: Taxonomy, Substantially Analysis, Motivations, Challenges,Recommendations and Future Direction," *J. Med. Syst.*, vol. 43, no. 10, 2019.

[5] S. Www, "S ato shi N a k a m oto A Peer-to-Peer Electronic Cash System," 2020.

[6] Q. Yang, Y. Zhao, H. Huang, Z. Xiong, J. Kang, and Z. Zheng, "Fusing Blockchain and AI With Metaverse: A Survey," *IEEE Open Journal of the Computer Society*, vol. 3. pp. 122–136, 2022.

[7] Z. Alhadhrami, S. Alghfeli, M. Alghfeli, J. A. Abedlla, and K. Shuaib, "Introducing blockchains for healthcare," *2017 Int. Conf. Electr. Comput. Technol. Appl. ICECTA 2017*, vol. 2018-Janua, pp. 1–4, 2017.

[8] B. D. Puthal, N. Malik, and S. P. Mohanty, "Everything You Wanted to Know About the Blockchain," *IEEE Consum. Electron. Mag.*, vol. 7, no. july 2018, pp. 6–14, 2008.

[9] B. World, "5.Block_chart," 2017.

[10] J. Vora *et al.*, "BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records," *2018 IEEE Globecom Work. GC Wkshps 2018 - Proc.*, pp. 1–6, 2019.

[11] S. Chakuu et al., "Signature redacted redacted Signature Signature redacted," SSRN Electron. J., vol. 1, no. 2012, pp. 1–117, 2017.

[12] A. K. Pandey *et al.*, "Key Issues in Healthcare Data Integrity: Analysis and Recommendations," *IEEE Access*, vol. 8, pp. 40612–40628, 2020.

[13] A. Singh and K. Chatterjee, "An adaptive mutual trust based access control model for electronic healthcare system," *J. Ambient Intell. Humaniz. Comput.*, vol. 11, no. 5, pp. 2117–2136, 2020.

[14] L. J. Kittur, R. Mehra, and B. R. Chandavarkar, *The Dependency of Healthcare on Security: Issues and Challenges*, vol. 698. Springer Singapore, 2021.

[15] A. A. Mazlan, S. M. Daud, S. M. Sam, H. Abas, S. Z. A. Rasid, and M. F. Yusof, "Scalability Challenges in Healthcare Blockchain System-A Systematic Review," *IEEE Access*, vol. 8, pp. 23663–23673, 2020.

[16] S. Khatri, F. A. Alzahrani, M. T. J. Ansari, A. Agrawal, R. Kumar, and R. A. Khan, "A Systematic Analysis on Blockchain Integration with Healthcare Domain: Scope and Challenges," *IEEE Access*, vol. 9, pp. 84666–84687, 2021.

[17] H. Rathore, A. Mohamed, and M. Guizani, *Blockchain applications for healthcare*. Elsevier Inc., 2020.

[18] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, "Blockchain for healthcare data management: opportunities, challenges, and future recommendations," *Neural Comput. Appl.*, vol. 0123456789, 2021.

[19] M. Shuaib, S. Alam, M. Shabbir Alam, and M. Shahnawaz Nasir, "Self-sovereign identity for healthcare using blockchain," *Mater. Today Proc.*, 2021.

[20] K. M. Hossein, M. E. Esmaeili, T. Dargahi, and A. Khonsari, "Blockchain-Based Privacy-Preserving Healthcare Architecture," *2019 IEEE Can. Conf. Electr. Comput. Eng. CCECE 2019*, pp. 1–4, 2019.

[21] L. Soltanisehat, R. Alizadeh, H. Hao, and K.-K. R. Choo, "Technical, Temporal, and Spatial Research Challenges and Opportunities in Blockchain-Based Healthcare: A Systematic Literature Review," *IEEE Trans. Eng. Manag.*, pp. 1–16, 2020.

[22] M. M. Madine *et al.*, "Blockchain for Giving Patients Control over Their Medical Records," *IEEE Access*, vol. 8, pp. 193102–193115, 2020.

[23] G. Wood, "Ethereum: a secure decentralised generalised transaction ledger," *Ethereum Proj. Yellow Pap.*, pp. 1–32, 2014.

[24] M. Wohrer and U. Zdun, "Smart contracts: Security patterns in the ethereum ecosystem and solidity," *2018 IEEE 1st Int. Work. Blockchain Oriented Softw. Eng. IWBOSE 2018 - Proc.*, vol. 2018-Janua, pp. 2–8, 2018.

[25] E. Kapengut and B. Mizrach, "An Event Study of the Ethereum Transition to," vol. 0253, no. 908, 2022.

[26] S. H. Jeong and B. Ahn, "Implementation of real estate contract system using zero knowledge proof algorithm based blockchain," *J. Supercomput.*, vol. 77, no. 10, pp. 11881–11893, 2021.

[27] A. Al Mamun, M. U. Faruk Jahangir, S. Azam, M. S. Kaiser, and A. Karim, A combined framework of interplanetary file system and blockchain to securely manage electronic medical records, vol. 1309. Springer Singapore, 2021.

[28] E. Indhuja and M. Venkatesulu, A Survey of Blockchain Technology Applications and Consensus Algorithm, vol. 55. Springer Singapore, 2021.

[29] Y. Zhang *et al.*, "Research on electronic medical record access control based on blockchain," *Int. J. Distrib. Sens. Networks*, vol. 15, no. 11, 2019.