FrontiersinHealthInformatics www.healthinformaticsjournal.com
ISSN-Online: 2676-7104
2024; Vol13: Issue4 OpenAccess

# A Review on Blockchain Based Electronic Health Records (EHRs)

Pragneshkumar Patel[1], Zalak Rana[2], Zishan Noorani[1], Shraddha Modi[1], Prachi Pancholi[1], Archana Gondaliya[1], Esan Panchal[1], Shruti B. Yagnik [1]

[1]Assistant Professor, Computer Engineering Department, L. D. College of Engineering, Ahmedabad, Gujarat, India

[2]M.E., Computer Science and Technology, L. D. College of Engineering, Ahmedabad, Gujarat, India

[1] Lecturer, Information Technology Department, Government Polytechnic Gandhinagar, Gandhinagar, Gujarat , India

[1] Associate Professor, Indus Institute of Technology and Engineering, Indus University, Rancharda, Ahmedabad , Gujarat - India

Corresponding author- Pragneshkumar Patel, pragneshpatel@ldce.ac.in

**Article Info**

***Article type:***
*Research*

***Article History:***
*Received:2024-04-10*
*Accepted:2024-06-15*
*Published:2024-07-03*

***Keywords:***
Blockchain, EHR, Data Privacy, Access control

**ABSTRACT**

Electronic Health Record (EHR) is a data repository that contains sensitive health-related information of the patient such as disease and its diagnostic details, lab reports, contact information, which are sensitive and keeping it secure from any attacker is one of the challenging task. Conventional health care systems are utilizing based on the conventional central client-server approach, where full access rights of the system are given to the central authority. Here, the privacy and confidentiality of EHR data might be questionable, because the one who share data don’t have any right to access his data and neither control over their data with whom it has been shared with. Blockchain is a distributed, immutable, peer-to-peer, cryptographically secure ledger. Blockchain technology has shows potential solutions to address the challenges of the EHRs, such as data security, interoperability, confidentiality, and patient privacy. This paper reviewed blockchain based solutions for the EHRs, the role of smart contracts for managing data and automating process along with its integration for the cloud-based technology. It also explores the role of Internet of Thing (IoT)along with blockchain technology in the healthcare industry for addressing issues of Access control and Data security along with smart contract. Finally, it also provides outlook for the future direction to make blockchain based solution for the large scale EHR system in the healthcare industry.

## INTRODUCTION

The healthcare industry is rapidly changing, with digitization playing a critical role in enhancing patient care, operational efficiency, and access to medical services. A key part of the given digital transformation is the handling of Electronic Health Records (EHRs). Traditionally, EHRs have been managed through centralized database management system, which is only accessible by the providers and with patients. This centralized approach may create significant issues like data privacy, data security, interoperability, handling sensitive health information across multiple healthcare providers. Exchanging patients’ healthcare information such as disease details, treatment history, reports across multiple healthcare provides for providing effective and timely treatment. Key advantage of exchanging treatment history is that health care provides can easily get complete information about patient’s health treatment. During the emergency, selection of the treatment is critical, which also depends on the previous medical treatment for certain diseases. In such and any other situation, sharing of electronically stored health records can be done smoothly over a network with different health service provider. These stored health records are known as electronic health records (EHRs) [1].

An Electronic Health Record (EHR) is a detailed archive of all the health-related information about a person through in their life [2]. To create single continuous document for the individual patent's EHR record, we should place it at central location. The given documents contain individual's information about health as well as personal information. Any security threats on the availability of given information in the public domain can lead to data privacy and confidentiality. However, there is an advanced technology for handling this metadata, they still face many issues related to security, availability, data interpretability, data privacy. In the other side to improve medical diagnosis decisions, knowledge of a patient's health history like tests, previous diagnoses, and treatments can be useful. So EHR should be in such away that Health Information Exchange (HIE) and data access is reliable and secure with whole history of patient's treatment. If unauthorized users acquire access to data, it could be traded or leaked or exploited, putting personal information at risk of being revealed to anyone.

To archive a high level of security in any EHR system, there are many technical solutions such as Encryption, Authentication, Role-based access control (RBAC). In the EHR system, all the access event of the data must be documented in the log file, which should maintain historical access records and overall log records can be severs as a legal document. There are two major challenges to create patient centred approach for smooth exchange of information across the provider; one is time it takes to transfer past records while protecting the patient's confidential health information (PHI) from remote healthcare facilities and second is the risk of gaining access to patient's data by the health service provider without prior concern of the patient [3]. Apart from this, below are the challenges for the establishment of patient-centred approach:

(1) Security and privacy regarding data visibility, sharing, and accessibility concerns can lead to legal chastisement, (2) Unauthorized access to the health records may cause data breaches, (3) Discrepancy between the EHR data provided by the remote provider and the recipient can lead to data inconsistency.

## BACKGROUND

### *A. EHR Systems*

Health Information Exchange (HIE) or exchanging health information is one of the key features of EHR. Various health institutes have implemented EHR system with various levels of technical and operational proficiency with different structure and terminology. So, there are not any globally accepted standards exist. Hence, we need database system, that is compatible with different types of the data source, easily integrated and shared across different system.

### *B. BLOCKCHAIN TECHNOLOGY*

In 2008, Satoshi Nakamoto introduced concept of blockchain and it is recognized for use in the Bitcoin cryptocurrency network [4]. As shown in the figure-1, blockchain formed by connecting each block with its previous block using block's hash to form chain and each block contains three items – data, hash of the current block and hash of the prior block. The hash contains by block is SHA256 hash which is 64 characters long. Major services and techniques of the blockchain are Distributed P2P Networking, hash cryptography, Smart Contract, Immutable Ledger, and Consensus Protocol [5].

- Consensus protocol: Consensus protocol is the access rights mechanism to validate the transaction before adding to the blockchain network.
- Hash cryptography: Blockchain adds a transaction using SHA256 hash. The length of the hash is 64 characters.
- Immutable ledger: Immutable property of the blockchain indicates that once transaction is recorded, then it cannot be modified or edited.
- Distributed P2P network: It is useful to broadcast and distribute the transaction to updated data of other users.
- Provenance: In indicates that full data and its historical assessment log are accessible on the blockchain network.
- Smart contract: It contains set of self-executive codes stored in the blockchain network which executes when triggered event occurs.

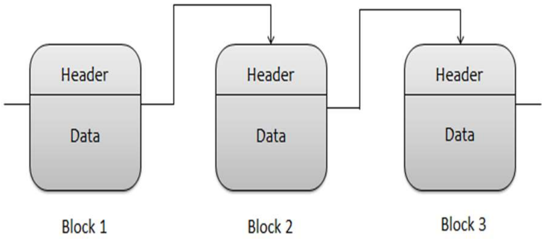

Figure 1. Chain of blocks in the Blockchain

The Benefit of blockchain:

- Decentralized: To avoid single point bottleneck, data are distributed on the network.
- Data Transparency: It ensures that data is of temper-proof when on blockchain network.
- Security and Privacy: Stored data and other information are secured using cryptographically
- Provenance: It ensures whole data and its assessment log availability on the network.
- Finality: Ensures about committed transaction on the blockchain network, which cannot be reversed or modified.

Along with above benefits, blockchain technology also have drawbacks. First one is that creation of blockchain network is a complex task and needs more time and technical in-depth knowledge [6]. Furthermore, data on the blockchain may be vulnerable to breaches and anonymity analysis attacks if suitable authentication procedures are not followed to protect privacy [7]. Improper management of private keys can lead to the "51% attacks" on the blockchain network [8].

## TYPE OF BLOCKCHAIN NETWORK

According to the network node's access right, we can classify blockchain system into three types.

**A. Public Blockchain:** Anyone who wishes to join the network can do so at any time and receive rewards by joining as a miner or join as a simple node. Ethereum and Bitcoin are popular public blockchain platforms.

**B. Private Blockchain:** There are access control rules to participate in the private blockchain network. To join the private blockchain participants must obtain an invitation or permission to join. Well-known examples of private blockchain are GemOS and MultiChain.

**C. Consortium Blockchain:** It is the semi-private lays between public and private blockchains. Group of organizations have access rights for managing the blockchain network and they are collaborated for the business application. Hyperledger Fabric is a business consortium blockchain framework. Ethereum also supports developing consortium blockchains.

## CONSENSUS

The mining process which validates the transaction of blockchain are known as consensus algorithm,

Consensus algorithm is the mining process used to validate the transaction of the blockchain. It defines set of protocols or rules to validate the nodes for inclusion in the network. Consensus protocol also ensures about suitable response will be received by the contributing nodes as per the transaction order. It takes the decision about inserting the block in the network [9][10].

Several protocols designed for validation of the block for adding nodes in the blockchain. Few of them are as below:

- Proof-of-work (PoW): It is consensus mechanism to validate nodes which gives complex mathematical puzzle to the miners. Amongst the miner, first one who solve puzzle will get the rights to validate node and its created nodes will be added into the transaction and miner will get rewards such as cryptocurrency. To solve complex puzzle, miner spent their energy.

- Proof-of-stake (PoS): Its an improved and energy saving version of PoW. The validation nodes are selected based on stake (e.g. currency) in the chain. Its likely that having more stake a node have higher likelihoods to validate node and it control the legitimacy of the block [11] [12].
- PBFT (Practical Byzantine Fault Tolerance): Its consensus protocol that allows a faulty node having a Byzantine fault [13]. It uses three phase protocol- one is pre-prepared, second is prepared, and third is commit. To attain consensus, it requires response from 2/3 valid nodes from each phase. This protocol generates valid nodes if quantity of malicious byzantine replicas nodes are less than 1/3. This consensus protocol is used by Hyperledger Fabric for the validation of the nodes.
- Raft: The core part of Raft algorithm is based on the leader-follower model. It works in two phase- leader election and log replication. In each peer organization of the Raft, ordered nodes are created and initialize them as leader node, follower node, or candidate node and periodically elect a leader node [14]. The decision of the selected leader node is broadcasted and replicated by follower node. After broadcasting transactions, the leader node waits for follower nodes to write the transaction. The transaction will be committed when leader node receives feedback from the follower node and perform log replication. Private/Consortium blockchain having 50% crash node tolerance capacity prefer Raft protocol.
- Proof of Authority (PoA): In PoA, each node needs to pass a preliminary authentication, only authenticated nodes have the right to generate new blocks. Though, centralized authentication mechanism is followed by this consensus mechanism.
- Proof of Capacity (PoC): Instead of computing resource, this protocol utilizes disk storage. The probability of creating a new block is higher for the miners having high storage capacity.
- Proof of Elapsed Time (PoET): This consensus algorithm selects block based on the waiting time of participant in the network.

## SMART CONTRACT

Every transaction must follow rules or protocols defines

Smart contract defines is a collection of rules or a protocol that must be adhered by transaction in an automated and digital way in the ecosystem of blockchain [15] [16]. It enhances security and reliability in the blockchain. Smart contracts provide role-based access that brings greater flexibility to transactions [17] [18]. Ethereum, the first open-source platform that enables smart contract executed in the decentralized way, without any need of central authority and provide facility to the developer for building solution.

## LITERATURE SURVEY

The given section classifies solution provided by the researcher for blockchain based solution for the healthcare industry.

### *A. Blockchain for EHR*

The integration of blockchain technology into Electronic Health Records (EHR) systems is rapidly gaining attention to address several long-lasting issues in the healthcare industry, particularly related to privacy, security, and interoperability. Traditional EHR system is based on the centralized storage server and with the technological advancement, it shifted paradigms to the cloud-based solution. For storing and managing electronics health data, cloud-based data sharing system emerges as the key promising solution. This system provides sharing of the Patient Health Information (PHI) across the multiple medical institutes in a convenient way, with keeping the privacy-preservation and security of the data intact. Despite the given advantages of the cloud-based solution, the chances of cloud hijacking or attack can create issues of possible abuse, loss, leakage, or theft of data despite the availability of the cryptographic techniques. To mitigate the security challenges of cloud-based solution, Blockchain has been suggested as a beneficial solution. It offers a decentralized and immutable method for maintaining and sharing a growing list of health records. In the e-Health system, where patients' records are managed are different health institute, Blockchain based Patient Health Information (PHI) sharing offers a secure distribution of EHR.

Blockchain overrides security challenges by maintaining auditable history of data access of hospital, patients and orderer. Existing systems are based on the central authority where patients did not have full control on the sharing of medical records across different stockholders. The ledger stores the transaction performed by the medical staff and patient and it contains different types of medical records generated at different time stamp. Thus, Ledger acts a registry for storing the patients record in EHRs [19] [20].

Tanwar et al. [5] proposed effective data sharing techniques using blockchain to overcome drawback of traditional client-server architecture. They have proposed access control policy and implemented it in the Hyperledger-based electronic healthcare record (EHR) sharing system [5]. They measured performance using blockchain evaluation and compared proposed methodology using Round Trip Time (RTT), latency, throughput. Zhuang et al. [3] presented novel concept of personalizing data segmentation using "allowed list" which contains list of clinicians allowed to access patient data and performed large scale simulation using patient-centric HIE -a programmable self-executing protocol running on a blockchain. This protocol ensures about patients' data privacy, data governance and gives full access to patients on their health records.

Shahnazet et al. [21] implanted blockchain based framework by defining granular access rules for the users to access the data and provide secure storage of electronic health records. Also discuss scalability issues of the blockchain and how off-chain storage of the data can be useful to overcome it. Christo et al. [22] proposed three phase blockchain based approach for granting access right on the medical reports of the patient. The three phases introduced by the researcher are - Authentication, Encryption, and Data Retrieval. Quantum Cryptography based authentical techniques are used while AES based encryption is performed and SHA algorithm-based data retrieval techniques are used to circumvent frequent attacks.

Hirtanet et al. [23] have proposed system design based on access policies defined by the patients to share medical analysis information across hospitals, medical clinics, and research institutes using blockchain. In the given system they involved two types of chain for protecting sensitive data- One is Private chain known as side chain to preserve information about read ID of patient and second is public chain- known as Main chain to store patients' health data marked with a temporary ID. Zhanget et al. [24] anticipated privacy-preserving PHI sharing protocol (BSPP) based blockchain based system to improve data sharing and diagnosis in the healthcare industry. They introduced two blockchains- Private blockchain, and Consortium blockchain to design secure health care sharing system. Based on the access rights given by the patients using PHI data sharing protocol, doctor can explore and search patients' historical health record to recommend better diagnosis.

Many research work has introduced to organise and handling electronics health records but little work has been done to manage uncertainties arise during emergency. In the conventional record keeping system, patients cannot give any access rights on his EHR data to emergency staff. Furthermore, there is a lack of secured EHR management system about patients' confidential information about his/her disease, symptoms, and who accessed it. To unravel the given problem, Rajput et al. [25] proposed smart contract rule-based system to share and define time limit on the emergency access of Personal health records (PHR) for managing the PHR permissions.

### *B. Cloud-based Blockchain in Healthcare*

For easy and convenient access to EHR or EMR data which are large, it is recommended to store them in the cloud-based storage system. Cloud based storage system is convenient and efficient for sharing EHR data across various health care provides. However, cloud servers also prone to security vulnerabilities such as authentication, data integrity, data privacy, and risk of reviling patients' information also there.

Chen et al. [26] proposed a blockchain-based searchable encryption scheme for EHRs. In the given work, logic expression-based index for EHR is created and stored in the blockchain. Users can utilize logical expression to search index. Index is propagated across the blockchain while original EHR data is stored in the public cloud in the encryption format to make it secure. This mechanism provides full access to the patient on their EHR data. Thus, integration of blockchain system with cloud can ensures about data integrity, and traceability of the EHR index.

Xia et al. [27] introduced access control challenge based blockchain data sharing platform for the sensitive data. They stored data using built-in autonomy and immutability properties of the blockchain in the cloud. Only invited and verified users are allowed to access data. Data are stored in the cloud while access log of the data is stored in the blockchain.

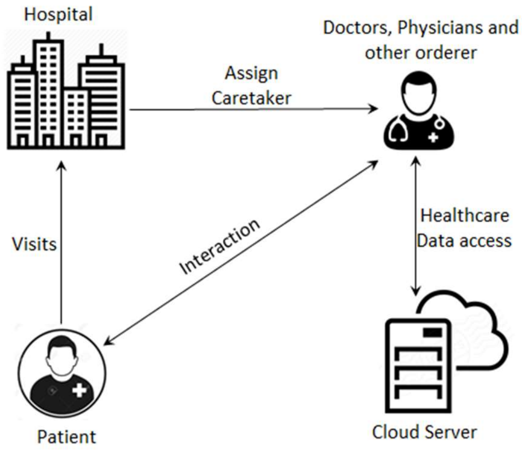

Figure 2. Blockchain with cloud server [40]

Xia et al. [28] designed Medshare system for sharing EHR data across the different users to provide security and data access control using cloud-based services and blockchain. Wanget et al. [29] proposed attribute-based encryption method for secured sharing of health records using blockchain. They ensured about traceability and data integrity of the EHR data using smart contract. Liu et al. [30] present a framework in which they proposed CP-ABE-based access control (CCAC) to store the EHR data using cloud for secure storage.

### *C. Blockchain in Log Management*

Blockchain stores data in the decentralized way and adding a block is independent of any blockchain platform. To make a secure health record management system, we need to store data in the secure storage, and keep all the access to the health data in the database. So, along with secured storage of data, we need to ensure about all logs of queries, such as select, alter, insert, delete, etc. must be secure and unchanged. Blockchain provides summary of all the logs and mechanism to store access logs in secured environment and maintain integrity of the logs.

Yang et al. [20] proposed blockchain based framework for safeguarding integrity of the data and tracks all the events of the data to advance interoperability of the system. Guoet et al. [31] proposed novel architecture using edge nodes and blockchain for access control on EHR data. In the given solution, role of blockchain is to manage identity and control policy and ensure about temper-proof log of access events. EHR data are stored using edge nodes and attribute-based access control policy specified by Abbreviated Language For Authorization (ALFA) is applied on the EHR data to manage logs.

### *D. Blockchain and IoT in Healthcare*

Recent development in the field of internet of things (IoT) has given rise to the number of connected devices for the enrichment of human life. One of the core aspects of human life is health, and it takes benefits from the various digital, smart, and comprehensive internet of things devices dedicated for the health care services, form a new dimension known as Internet of Health Things (IoHT) [32]. This kind of devices broadly contains three major components to form large digital healthcare system- One is wearable sensing devices, second is an internet gateway device and third is cloud-based data centre. The interaction among the given components is shown in figure-3. Patients' health data such as heart rate, oxygen level are collected through sensors of the wearable devices and observed by it and give alert message if it goes beyond threshold. Apart from it, these data are also stored in the chain and stored through transaction and alerted to the doctor.

Badr et al. [33] presented a novel protocol named - Pseudonym Based Encryption with Different Authorities (PBE-DA) to attain privacy preservation on the healthcare data using blockchain platform. Access rights to view and update patients' sensitive data on the EHRs system is given by PBE-DA.

Bhawiyugaet at el. [34] proposed different component-based system to integrate IoT with blockchain and cloud servers. The components are- HTTP based API gateways -works as gateway to blockchain interface, peer node, orderer, and membership service providers (MSP). Sensing data from IoT gateway devices are accepted by the API gateways. API gateway calls chain code which is installed in the each blockchain peer

By transmitting transaction to peers, API gateway, who perform role of client, calls chain code installed in each blockchain peer. As the transaction is received by the peers, it executes it and send approved transaction data to the client. When ordered received collected endorsement from various peers, it starts building a block having ordered transaction received from all the client and broadcast that block across all the peers. After receiving block by each peer, they perform a final verification and do commit all the ordered transaction of that block into its local ledger.

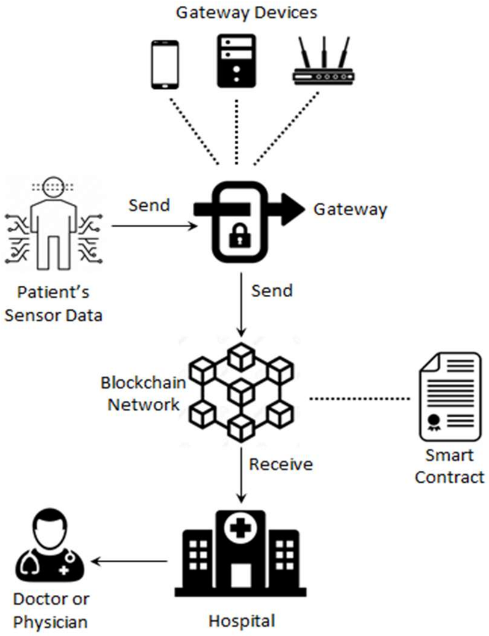

Figure 3. Sensor data interaction in IOT using blockchain

Griggs et al. [35] presented smart contract based IoT enabled Remote Patient Monitoring (RPM) system to secure and manage sensors and medical devices during communication. Record of all the events are stored in the blockchain with the secure ledger using smart contract. To resolve security vulnerabilities associated with RPM, automatic event notification is implemented and ensure about trustworthiness of the wearable medical devices to the patient.

To monitor big data and provide secure management in Remote Patient Monitoring (RPM) system, Dwivediet et al. [36] modified blockchain for the IoT devices based on the distributed and other network security characteristics. These security and privacy characteristics in the framework are the integration of private and public keys, blockchain, and other lightweight cryptographic primitives to enhance the access control of patients.

Table 1shows summary of security features of Blockchain-based EHR systems.

## TECHNICAL CHALLENGES OF USING THE BLOCKCHAIN IN HEALTHCARE

There are many different application areas and multi-disciplinary concept for the potential implementation of the blockchain, still many challenges are there. The researchers also endeavouring to overcome these challenges, herewith we have enumerated challenge when researcher applied blockchain technology in the healthcare area [37] [38] [39].

### *A. Security*

Blockchain based framework is prone to the one of the major security threat - "51% attack". It indicates that when any attacker/ group of them gains control of 51% of the network computation power, then its security could be conceded. The developer of the system should design framework such that it can mitigate such attacks on the healthcare system otherwise reliability of the organization vanished.

### *B. Resource consumption*

The mining process of the blockchain technology is highly computationally intensive and it requires large resource to make it active and alive. In the healthcare system, large number of devices varies from wearable devices to the large operational devices are required to monitor patients' health, which needs large computing, and energy costs. To manage the given devices, organization needs large investment.

### *C. Usability*

Handling of blockchain based solution is very complex and required in-depth technical expertise. To make it usable for the health care professionals, need to create user friendly features as well as require training to manage the system. Hence, usability is also one of the main challenges for the blockchain based healthcare solution.

### *D. Centralization*

Nature of the blockchain is the decentralized structure, but some blockchain based approaches require centralized miner. This dependency on the centralized miner creates a bottleneck when this node is vulnerable and its control is gained by the malicious attacker.

Table I SECURITY FEATURE(S) OF BLOCKCHAIN-BASED EHR SYSTEMS

| **Paper** | **Main security feature(s) provided by Blockchain** | **Method/ Objective** |
|---|---|---|
| Tanwar et al. [5] | Decentralization, Access control, Privacy | Proposed Hyperledger based EHR system that utilize chaincode concept |
| Zhuang Y et al. [3] | Encryption, Access control, Privacy | Presented allowed list to make personalizing data segmentation and access on health data |
| Shahnazet al. [21] | Secure storage, Scalability | Secure storage of health record by defining granular access rules. |
| Christo et al. [22] | Authentication, Encryption, and Data Retrieval | Quantum Cryptography to grant security in accessing medical reports. |
| Hirtan et al. [23] | Data security, Access control | To protect data they frame two types of chains: one isprivate and second is sidechain. |
| Zhang et al. [24] | Decentralization, Access control, Encryption, Data security | Presented PHI sharing protocol to improve diagnosis by preserving privacy |
| Rajput et al. [25] | Access control | Emergency access permission to PHR in emergency situation. |
| Chen et al. [26] | Integrity, Access control | Blockchain based searchable encryption scheme for EHRs. |
| Xia et al. [27] | Immutability, Access control, Log management | Blockchain based medical data sharing framework |
| Xia et al. [28] | Access control | Blockchain and cloud storage based data sharing framework |
| Wang et al. [29] | Encryption, Integrity, Traceability | Attribute based Blockchain cryptosystem for EHR system with Cloud. |
| Liu et al. [30] | Integrity, ABE based Access control | CP-ABE based Access control for data sharing and store EHR data on cloud |
| Yang et al. [20] | Log management, Access control, Integrity | To ensure the integrity and improve interoperability by tracking every event occurs in system |
| Guo et al. [31] | Attribute based Access control, Log management | Blockchain and edge node based hybrid approach to manage EHR data access. |
| Badr et al. [33] | Encryption, Access control | To enhance communication between healthcare entities in an e-health platform, proposed pseudonym based Encryption with multiple authorities, |
| Bhawiyuga et al. [34] | Access control, Decentralization | Proposed HTTP-based API gateway serves as the interface between devices and the blockchain. |
| Griggs et al. [35] | Data security, Access control, Decentralization | IOT-RPM based smart contract to manage medical device security while communicating with smart device |
| Dwivedi et al. [36] | Privacy, Access control, Data security, Encryption | Framework that modifies blockchain for IOT devices for distributed network security. |

## CONCLUSION

Integration of the Blockchain technology has shown a promising solution to the challenges associated with the Electronics Health Records (EHRs). Despite the significant advancement in Information Technology, existing EHR systems are service provider centric and faces critical issues related to patients' data management, integrity, reliability, and interoperability. Decentralized and immutable nature of the blockchain offers a unique approach to address given challenges by enhancing data privacy and security and integrity issue. Moreover, it enables patient's centric effective interoperability, and trustworthy system to offer solution to the issues such as data breaches, unreported clinical trials, and erroneous data. Through the systematic review existing research work, this paper highlights key innovations to address issues of the EHRs and ongoing challenges of the blockchain based solution for the healthcare industry.

Although blockchain has shown considerable potentials, still further research is needed to address several key challenges. Scalability is one of the major issues for blockchain based solution for the large volume of the data. For smooth interoperability across different health service provider, there is a need of standardized framework. In addition to this, also explore the legal and regulatory challenges of the patient's data and consent for the authorization. Despite the given challenges, integration of blockchain with internet of things (IoT) and cloud technology has the potential to create a more secure, transparent, and efficient healthcare system for both healthcare providers and patients.

## REFRENCES

[1] "Office of the National Coordinator for Health Information Technology,What is an electronic health record (EHR)?." [Online]. Available:https://www.healthit.gov/faq/what-electronic-health-record-ehr.

[2] "Electronic Health Record System from the Perspective of DataPrivacy." [Online]. Available: https://www.asianhhm.com/informationtechnology/electronic-health-record-system

[3] C. Y. S. Z. T. J. S. C. Zhuang Y, Sheets LR, "A patient-centric health information exchange framework using blockchain technology." no. Aug;24(8), 2020, pp. 2169–2176.

[4] S. Nakamoto, "https://www.healthit.gov/faq/what-electronic-healthrecord-ehr.Bitcoin: A peer-to-peer electronic cash system." [Online]. Available: https://bitcoin.org/ bitcoin.

[5] S. Tanwar, K. Patel, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," Journal of Information Security and Applications, 2020.

[6] M. N. Ahamad, Shaikshakeel and B. Varghese, "A survey on cryptocurrencies," In 4th International Conference on Advances in Computer Science AETACS, pp. 42–48, 2013.

[7] M. S. Ortega, "The bitcoin transaction graph—anonymity." PhD diss., Master's thesis, Universitat Oberta de Catalunya, 2013.

[8] G. Hileman and M. Rauchs, "Global blockchain benchmarking study." Cambridge Centre for Alternative Finance, University of Cambridge 122, 2017.

[9] G. Pîrlea and I. Sergey, "Mechanising blockchain consensus," in Proceedings of the 7th ACM SIGPLAN International Conference on Certified Programs and Proofs, 2018, pp. 78–90.

[10] J. Moore, J. S. Chase, and P. Ranganathan, "Weatherman: Automated, online and predictive thermal mapping and management for data centers,"in 2006 IEEE international conference on Autonomic Computing. IEEE, 2006, pp. 155–164.

[11] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proofof-stake," self-published paper, August, vol. 19, p. 1, 2012.

[12] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C.Qijun, "A review on consensus algorithm of blockchain," in 2017 IEEE international conference on systems, man, and cybernetics (SMC). IEEE, 2017, pp.2567–2572.

[13] M. Castro, B. Liskov et al., "Practical byzantine fault tolerance," in OSDI, vol. 99, no. 1999, 1999, pp. 173–186.

[14] Hyperledger, "The ordering service." [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-1.4/orderer

[15] A. K. G. Krishnendu Chatterjee and Y. Velner, "Quantitative analysis of smart contracts. in programming languages and systems," Springer International Publishing, no. 739–767, 2018.

[16] N. Szabo, "Formalizing and securing relationships on public networks," First Monday, vol. 2, no. 9, Sep. 1997. [Online]. Available: https://firstmonday.org/ojs/index.php/fm/article/view/548

[17] J. A. T. Fairfield, "Smart contracts, bitcoin bots, and consumer protection," Washington and Lee Law Review, 2014.

[18] S. Omohundro, "Cryptocurrencies, smart contracts, and artificial intelligence," AI Matters, vol. 1, no. 2, p. 19–21, Dec. 2014. [Online]. Available: https://doi.org/10.1145/2685328.2685334

[19] D. Tith, “Application of Blockchain to Maintaining Patient Records in Electronic Health Record for Enhanced Privacy Scalability and Availability,” pp. 2093–3681, 2020.

[20] K. Guang Yang, Chunlei li, “A blockchain-based architecture for securing electronic health record systems,” ACM Southeast Conference, 2019.

[21] U. Ayesha Shahnaz, “Using blockchain for electronic health records,” 2019.

[22] M. S. Christo, A. M. A., P. S. G., P. C., and R. K. M., “An efficient data security in medical report using block chain technology,” in 2019 International Conference on Communication and Signal Processing (ICCSP), 2019, pp. 0606–0610.

[23] L. Hirtan, P. Krawiec, C. Dobre, and J. M. Batalla, “Blockchain-based approach for e-health data access management with privacy protection,” in 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2019, pp.1–7.

[24] A. Zhang, “Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain,” in Journal of Medical Systems. Springer, 2018. [Online]. Available: https://doi.org/10.1007/s10916-018-0995-5

[25] A. R. Rajput, Q. Li, M. TalebyAhvanooey, and I. Masood, “Eacms: Emergency access control management system for personal health record based on blockchain,” IEEE Access, vol. 7, pp. 84 304–84 317, 2019.

[26] K. K. C. L Chen, N Zhang, “Blockchain based searchable encryption for electronic health record sharing,” Future Generation Computer Systems 95 (2019), p. 420–429, 2019.

[27] Q. Xia, E. Sifah, A. Smahi, S. Amofa, and X. Zhang, “Bbds: Blockchain based data sharing for electronic medical records in cloud environments,” Information, vol. 8, p. 44, 04 2017.

[28] 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,” IEEE Access, vol. 5, pp. 14 757–14 767, 2017.

[29] S. Y. Wang, H., “Secure cloud-based ehr system using attribute-based cryptosystem and blockchain.” Springer Science + Business Media, LLC, part of Springer Nature 2018, no. 42, p. 152, 2014.

[30] J. Liu, X. Li, L. Ye, H. Zhang, X. Du, and M. Guizani, “Bpds: A blockchain based privacy-preserving data sharing for electronic medical records,” in 2018 IEEE Global Communications Conference (GLOBECOM). IEEE, 2018, pp. 1–6.

[31] M. N. Huo Guo, Wanxin Li, “Access control for electronic health records with hybrid blockchain-edge architecture,” 2019 IEEE International Conference on Blockchain, no. 978-1-7281-4693-5/19, 2019.

[32] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. Kwak, “The internet of things for health care: A comprehensive survey,” IEEE Access, vol. 3, pp. 678-708, 2015.

[33] S. Badr, I. Gomaa, and E. Abd-Elrahman, “Multi-tier blockchain framework for iot-ehrs systems,” Procedia Computer Science, vol.141, pp. 159–166, 2018, the 9th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN-2018) / The 8th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH-2018) / Affiliated Workshops. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S187705091831812X

[34] A. Bhawiyuga, A. Wardhana, K. Amron, and A. P. Kirana, “Platform for integrating internet of things based smart healthcare system and blockchain network,” in 2019 6th NAFOSTED Conference on Information and Computer Science (NICS), 2019, pp. 55–60.

[35] K. B. H. Griggs, Ossipova, “Healthcare blockchain system using smart contracts for secure automated remote patient monitoring,” Journal of medical systems, no. 42, 2018.

[36] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, “A decentralized privacy-preserving healthcare blockchain for iot,” Sensors, vol. 19, no. 2,2019. [Online]. Available: https://www.mdpi.com/1424-8220/19/2/326

[37] H.-N. D. X. C. Zibin Zheng, Shaoan Xie and H. Wang, “Blockchain challenges and opportunities: A survey. international journal of web and grid services,” Journal of medical systems, vol. 4, no. 352–375, 2018.

[38] M. B. Hoy, “An introduction to the blockchain and its implications for libraries and medicine,” Medical Reference Services Quarterly, vol. 36, no. 3, pp. 273–279, 2017, pMID: 28714815. [Online]. Available: https://doi.org/10.1080/02763869.2017.1332261

[39] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He,“Blockchain in healthcare applications: Research challenges and opportunities,” Journal of Network and Computer Applications, vol. 135, pp. 62–75, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804519300864

[40] S. Ramachandran, O. Obu Kiruthika, A. Ramasamy, R. Vanaja and S. Mukherjee, "A Review on Blockchain-Based Strategies for Management of Electronic Health Records (EHRs)," 2020 International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2020, pp. 341-346, doi: 10.1109/ICOSEC49089.2020.9215322.