Blockchain in Healthcare: An EHR storage system

Rhea Rodrigues
IT Department
St. Francis Institute of Technology
Mumbai, India
rheasera@sfit.ac.in

Anshika Gupta
IT Department
St. Francis Institute of Technology
Mumbai, India
csendranshi123@student.sfit.ac.in

Ankita Tripathi
IT Department
St. Francis Institute of Technology
Mumbai, India
ankitatripathi424@student.sfit.ac.in

Reuben Coutinho
IT Department
St. Francis Institute of Technology
Mumbai, India
reuben211999@student.sfit.ac.in

Joanne Gomes
IT Department
St. Francis Institute of Technology
Mumbai, India
jgomes@sfit.ac.in

***Abstract*—Electronic health records (EHR) are digital versions of the traditional paper-based medical records. Blockchain is a type of distributed database that can be updated and is shared across multiple computers. The existing EHRs suffer from data manipulation, delayed communication, and trustless cooperation in data collection, storage, and distribution, making it arduous to achieve the ACID principles- atomicity, consistency, integrity and durability. The project proposes a blockchain-based mobile app with an integrated wallet to perform transactions to store and retrieve data on the blockchain network. The system interacts with the decentralized storage for the management of EHRs. Role-based access control plays a crucial role in the management of EHRs in the contract. Further, the project observes integration of role-based access control for the entities that interact with the contract. The Hospital is the default admin and assumes control to grant and revoke roles.**

***Index Terms*—blockchain, EHR, ethereum, ipfs, transactions**

I. Introduction

A digital counterpart of a patient's paper chart is called an Electronic Health Record (EHR). EHRs are patient-centered, real-time records that make information available to authorized users promptly and securely.

Blockchain is a peer to peer network of nodes, shared across multiple computers. The blockchain stores information similar to distributed file systems; in blocks that are inter-connected and each of them houses a copy of the entire transaction database. As new information is transacted, a new block is appended to the existing chain with reference of the hash value of the current last node. This results in a chronological chain of data.

The existing EHR management systems make use of the traditional relational databases or at the most NoSQL databases. These systems suffer from data inconsistency, latency, and integrity issues in data collection, storage, and distribution [1]. discussed various issues related to existing EHRs i.e data security and data accessibility. The data can be easily breached by hackers and unauthorized external parties jeopardizing the patient's privacy. The victim organization's data can be then used by the attackers for illegal and malicious intentions. The compromised data can then be further used for crime against those individuals, organizations or even the country as a whole depending on the size of the organization and sensitivity of the data.

A study of recent literature in Blockahin based EHRs shows that blockchain serves as a feasible solution to these challenges as it eliminates any possibility of server downtime, fraud, or third-party interference. The paper by A. Shahnaz *et al* provides a framework which is a combination of secure record storage along with the granular access rules for the records [4]. The records of the patient are stored on the IPFS, ensuring that the hash generated from it will be stored in the blockchain. Blockchain creates a ledger system that is immutable and allows the transaction to take place in a decentralized manner [2]. In the case of EHRs, a decentralized ledger is implemented so that no single person or group has control—rather, all users collectively retain control [4]. This decentralized legder works on a certain mechanism for block identity verification and block participation selection. Yang Guang *et al* have implemented an incentive based node selection algorithm based on the significance of each provider block [3]. They provided security analysis and extensive evaluations on various technical aspects of the proposed system, showing the advantages of their proposal over existing solutions. The smart contract code defines the rules and conditions for management and triggering the action of asset ownership [1]. A thesis aimed at designing a prototype for a simple blockchain based application for EHRs that satisfied requirements like information privacy, traceability, secure information access and sharing in a decentralized fashion has been proposed by A. Dubovitskaya *et al* [6]. The prototype was implemented with Hyperledger Fabric (HL Fabric) and served as an access control system to manage identities, provide traceability and preserve the privacy of users and patients. It also explored other factors in a crisis situation like the success rate, transaction commit, read latency, state read throughput(TPS) and resources consumption. Blockchain technology can use Ethereum for the implementation of the healthcare blockchain smart contract system. The authors A.

Khatoon *et al* [9] discussed different implementation workforces and analyzed the practical costs of deploying models such as issuing and filling of medical prescriptions, sharing laboratory test/results data, enabling effective communication between patients and service providers, data flow for healthcare reimbursement, etc.

The limitations in the existing solutions can be observed as scalability, network latency, data uploading privacy, and quality of service. The majority of the systems function on a web-based application which is not convenient in case of remote access requirements. The EHRs comprise heavy data volumes which are not feasible to store on a single blockchain and if done so, would increase the mining costs tremendously. The patients frequently lack control over their own data as the database systems are managed by the hospitals. The inefficient methods of transferring data between healthcare providers leads to deteriorated data quality and dissimilarity between the databases.

This project incorporates a secondary off-chain that overcomes the above-stated limitations. The blockchain privacy model keeps data records widely accessible, but the patients to whom they refer to are anonymized. For convenient remote access, the proposed EHR system is accessible through a mobile app that uses IPFS cloud storage for the secondary chain mechanism and Ethereum as the decentralized-distributed computing platform.

II. Related Work

A. Literature Survey

A study of recent literature in Blockahin based EHRs shows that most of the research works have been implemented

Blockchain for secure EHRs sharing of mobile cloud-based E-Health systems is proposed in the paper by Yang Guang *et al* [3], having a novel EHRs sharing scheme enabled by mobile cloud computing and blockchain. To investigate the performance of the proposed approach, they deployed an Ethereum blockchain on the Amazon cloud, where medical entities can interact with the EHRs sharing system via a developed mobile Android application. They provided security analysis and extensive evaluations on various technical aspects of the proposed system, showing the advantages of their proposal over existing solutions.

Paper [2] focuses on preserving the privacy of electronic health records using blockchain. The paper discussed various issues related to existing EHRs i.e data security and data accessibility. A Hyperledger Fabric has been used to create blockchain networks. The basic functionalities of the EHR system have been implemented and deployed.

In the paper by Yogesh Sharma *et al* [5], they've discussed a permission-based blockchain-based EHR systems for data integration and sharing with each hospital acting as its own node, with its own EHR system to form the blockchain network. Their approach was a hybrid data management system, where only management metadata was being stored on the chain and the actual EHR data was being encrypted to be stored on a (Health Insurance Portability and Accountability Act) HIPAA compliant cloud-based storage. The patient has the right to share his records with the hospital only. The analysis made was that it was a . Limitations mentioned were that during emergency situations like the unconsciousness of a patient would deny the access of EHR data to the hospital.

The next section gives an overview of EHRs and the implementation of blockchain systems on a public ledger.

III. Blockchain Based Approach

Electronic Health Records (EHRs) are the digitalized version of the conventional paper health records consisting of the medical history of the patient. These electronic records are real-time accessible and are relentlessly available to the authorized user entities. The fundamental feature of EHR systems is to facilitate inter-organizational switching through easy sharing among healthcare providers. This streamlines the healthcare service tremendously and offers the healthcare providers to take better care of the patient. EHRs contain sensitive information like diagnosis reports, treatment plans, immunization schedules, laboratory test results, etc and hence need to be secured from intruders over the network with malicious intentions.

Blockchain can be perceived as a peer-to-peer network of server nodes that store data, connect each node to other nodes and also perform computation operations when necessary. The whole system is governed by smart contracts which comprehensively lays down the specifics of each function and transaction. The network aspect of the blockchain if looked in one way can be observed as, the user needs to connect to any one single node through a URL to tap the entire blockchain network. As a database, the blockchain resembles a distributed file system. Each transaction creates a new node or block in the chain that appends to an existing node or starts a new chain. These nodes are immutable and the hash value of each node is calculated with reference to its previous node. Due to this property, even a minor edit in the data of an existing node will cause discrepancy in the hash value pattern of that node and rest of the chain. Every transaction taking place in the entire history of the system is stored and all users have complete access to each block. These blocks collectively form the public ledger. Finally, the blockchain can also serve as a computation entity which runs programs. Smart contracts are deployed on such chains that are responsible for generating and maintaining the records of all the transactions.

This can be recognized by any user on the chain and hence it forms a secure channel to store sensitive data like money, public records, health records, supply chain mechanisms, crowdfunding systems and many more relevant applications.

Every user on the blockchain has a unique identifier.

The role based access control mechanism offered by the blockchain, provides the extra layer of security to ensure that the data stays within the right entities, accessed immediately when required and are is misused. The said blockchain system is immutable and follows an append-only pattern which ensures that records exist in their original format at the time of upload. The complete patient history can be stored on the

blockchain nodes, hence eliminating the need to keep a hard-copy track of all the reports and prescriptions.

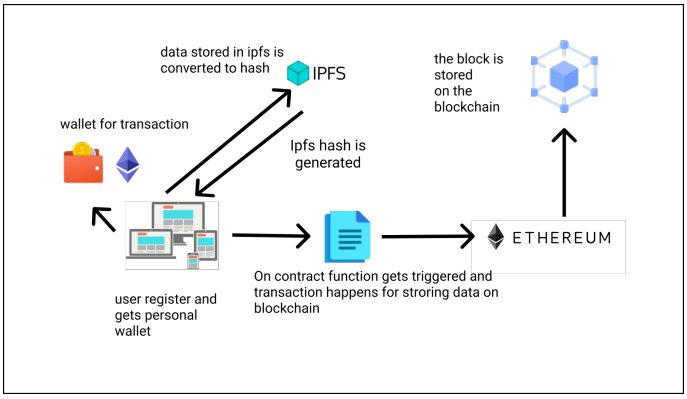


Fig. 1. The process of the system.

There are 2 methods of storing EHR in blockchain such as the off chain and on chain methods. But the most feasible method for storing massive amounts of data would be the off chain method IPFS is one of the off -chain storage methods used in many systems. The following figure 1 shows how the blockchain is related to the off-chain storage. Just like blockchain, it is a decentralized file storage system where a portion of the data is held by user-operator.

When an EHR is stored on a blockchain, a secondary storage known as an IPFS is used in order to store huge health information generated by multiple entities, thereby reducing transaction costs. When storing a health record on the blockchain system ,the data is first stored on IPFS which in turn generates a hash. Through the help of smart contracts and the transaction process, the hash is stored on the block. Before the block can be stored on the blockchain, the block has to be verified from all nodes and miners. This step can also be carried out by ethereum as it is a decentralized, open-source blockchain with smart contract functionality. In order to perform transactions on ethereum for execution contract functions It's necessary for a user to hold ethereum cryptocurrency. This thereby enables authorized entities to have access to past information stored in the blockchain. Once the Block is verified from Ethereum, It is stored onto the Blockchain holding the desired hash.

A. Terminology

Ethereum: Ethereum is a decentralized, open-source platform with smart contract functionality. This technology allows the user to send cryptocurrency to anyone for a small fee. The Ethereum network consists of a large number of computation nodes.

Ethereum Virtual Machine (EVM) : When a smart contract is run on Ethereum, It is executed by the EVM. The role of the EVM is to run smart contracts. It defines the rules for computing new valid states from block to block. The EVM is a powerful sandboxed virtual stack embedded in every full Ethereum node responsible for executing contract bytecodes.

Ether (ETH): is a cryptocurrency used to send transactions on the Ethereum platform. Smart Contracts: A smart contract is a computer program or transaction agreement designed to automatically execute, control or record legally relevant events and actions in accordance with the terms of the contract. Ethereum utilizes the Solidity Programming Language, thereby allowing developers to create and deploy smart contracts.

Nodes: These are real-life machines which are storing the EVM's state. They communicate with each other to tell information about the current state of EVM and new or updated state of EVM. Accounts: Similar to bank accounts, But used for Ether (ETH) cryptocurrency, which is stored in these accounts. Where Users can initiate it, deposit Ether into the account, transfer ether from one account to another. These accounts have account balances that are the Ether's. They are stored in a big table on the EVM and are a part of its overall state.

Transactions: A transaction is a form of request that is performed by the user, which may be for sending ether from one account to another , deploy smart contract or execute the code of smart contract on EVM. For the request to be affected on the EVM state, it must be validated, executed and "committed to the network"by another node. Blocks: A Block on the blockchain can have multiple transactions.

Gas: Gas refers to the unit of measurement, which is the amount of computational effort required to execute specific operations on the Ethereum network. They act as a certain transaction fee required to perform any transactions.

Inter-Planetary File System (IPFS): It is a protocol and peer-to-peer network for storing and sharing data in a distributed file system.

IPFS hash: IPFS uses a directed acyclic graph (DAG) to keep track of all the data stored in IPFS. A CID identifies one specific node in this graph. This identifier is the result of hashing the node's contents using a cryptographic hash function like SHA256

IV. Proposed System

A. Back-end of the Blockchain system

Development of smart contracts in solidity: Encapsulated smart contracts which focus on various role-based system functions. The contract also included functions for storing data about these various entities. Mappings were used which mapped the address to struct thereby acting as a database for each entity. Mappings were created for all entities which included Doctors, Patients, hospitals (admin), or Pharmacy personnel. The struct for patient record inculcated a mapping in it for the medical record. The medical record struct had an index, medical hash, verified status. These values are associated with each patient, where the patient or doctor could add medical records and update the data for that record.

Deployment of smart contracts: We made use of the Ganache CLI which acted as a Virtual Blockchain Environment, where we deployed the contracts. On deploying the contracts an ABI code is generated, which is basically a JSON

File needed by any frontend like a flutter to interact with the deployed contract.

B. Front-End User-Interface through Flutter

User Registration and Login: The system logs in the user through the flutter app and gets associated with the off-chain role-based access control parameter based on whether they are a Doctor, Patient, Hospital (admin), or Pharmacy personnel.

Creation of wallet credentials: On successful registration through firebase, the system randomly generates a new zero balance wallet account and assigns it to the user. For the user to now use the system and carry out transactions, they need ethers. To get ethers into the account, we import the private keys from ganache into the metamask, which contains 100 ethers by default. This facilitates the user to register as an entity on the blockchain. During the registration process, the user details get sent over to the IPFS server where it gets stored and the unique hash value of the stored data is transmitted back to the flutter app. On submitting this hash value, a smart contract function is triggered which stores it on the blockchain. This step involves a null ether transaction with charges only for the gas fee. Fig 2 shows the wallet screen and its various functionalities which also shows the counter for various entities like patient, doctor, hospital and pharmacy.

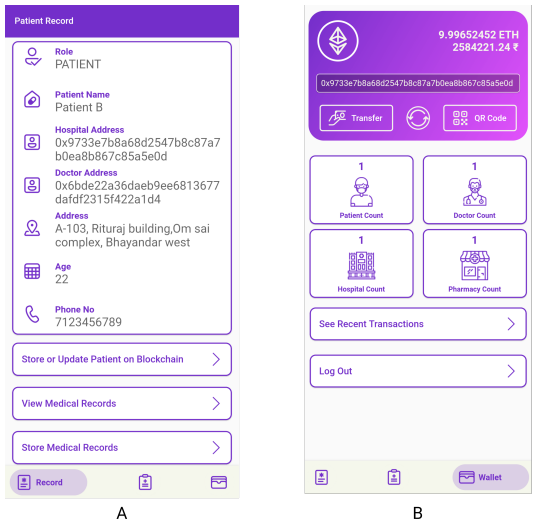


Fig. 2. Patient Record Screen after fetching data from the blockchain.

Working of the patient entity: After the user has signed in as a patient the user can now store their patient details on the blockchain, given that they have a balance in the wallet as visible in fig 3. After their details have been stored on the block chain, their details are fetched from the blockchain to display it on the main screen. The patient has the option to view their medical records and has another option for storing user medical records.The patient record is then verified by the doctor. The patient can add multiple medical records. Patients can also view previous medical records as shown in fig 4.The patient can update their medical records by re-submitting. Patients can also change the hospital and doctor by changing their address respectively. For storing any details or updating any details the patient must have ethers in their account to make transactions happen. Fig 3 shows all the patient details along with the necessary button to perform various functions like storing the medical record, view medical records, change hospital address, change doctor address.

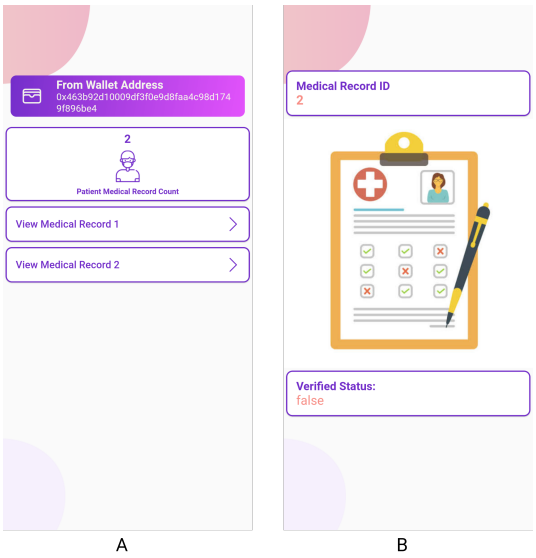


Fig. 3. shows the next screen as to what happens when clicked on viewing a single medical record.

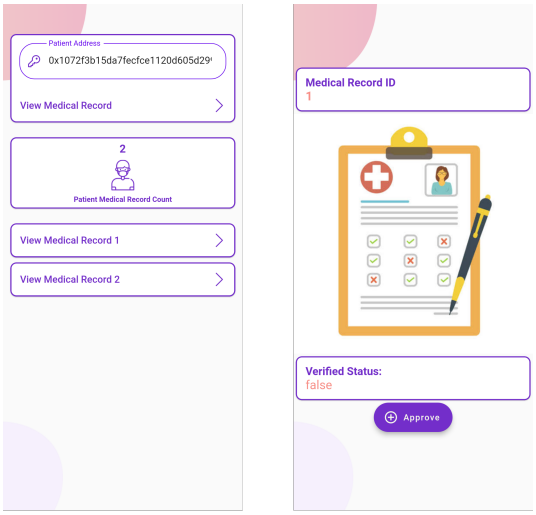
Working of the doctor entity: Similar to the patient entity, the doctor can also store his details on the blockchain which sets up the default role of the "DOCTOR". The doctor can view patient medical records and can also verify patients medical records, stating if they are correct or incorrect. Apart from this the doctor also has the option to change hospital on the blockchain.

Working of hospital entity: The hospital is the main user and also acts as the admin,when he stores his details on the blockchain he gets assigned the role of hospital admin. The hospital also has the ability to grant and revoke roles. The hospital interacts by granting and revoking roles to entites for further access to other functions on the contract. similarly the hospital can grant and revoke roles for the patient

V. Challenges in Blockchain based EHR

Among all the advanced features provided by the blockchain technology, it still isn't perfect. Key concerns being the security of the data being shared across nodes and handling the redundancy and discrepancies in the data at nodes across the blockchain network. All individual nodes are required to reach a consensus that the data they contain is the same and true. This is reached by implementation of census mechanisms. The current ethereum platform follows a proof-of-work concept non-repudiation at the nodes.

The contract to be deployed in real life scenario has a limited space of 24 Megabytes, thereby limiting the amount of code that can be written in a contract.



A B

Fig. 4. shows the next screen as to what happens when clicked on viewing a single medical record.

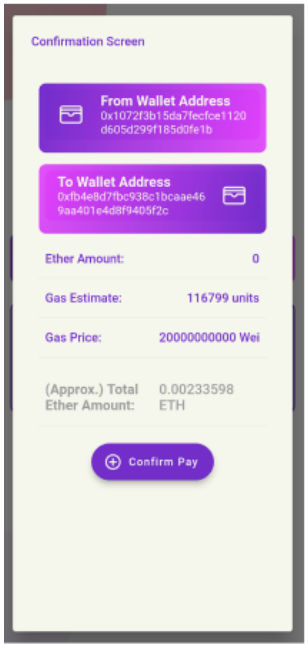


Fig. 5. Confirmation Screen

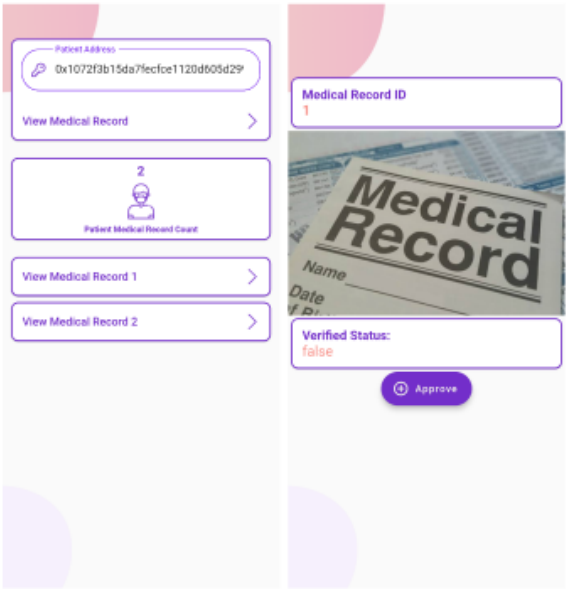


Fig. 6. The process of confirming patient record by doctor

With context to EHRs, the systems lack interoperability with hybrid systems that are currently in use, stand-alone projects, difficult integration with legacy systems, complexity of processes and lack of blockchain knowledge and awareness among people. As Blockchain is an unbreachable technology, hacking, unauthorized breaches and frauds can happen only on the frontend of the blockchain-based systems of while data transmission over the network. This can be resolved with encrypting the data before transmission and decrypting it at the final stage of display.

VI. Result

By incorporating a mobile application, the process of document uploading has been simplified. A patient can upload his medical record in the format of images as shown in figure After the image has been uploaded he enters a confirmation screen showing him the transaction cost of uploading the medical record on the blockchain. As shown in fig 5 a confirmation screen will appear after uploading an image .The user must have ethers in their wallet to make transaction happen.

VII. Conclusion and Future Scope

The EHR systems using blockchain serve as a decentralized and secure mode of patient data storage and provide convenient remote access to authorized users based on role based access control measures. The smart contracts govern the functions associated with each module. The system is highly scalable and hence makes a good investment for the health care institutions. Moreover, the inter-operability within organizations further simplifies the organization switching process and eliminates the requirement for the user to keep a track of all their medical history on paper. The digitization of the health records further mitigates the risk of document loss and hassle of maintaining the paperwork in case of relocation or travel. Since the blocks are immutable, the stored records cannot be modified once added which may serve as medical evidence in case of any legal mishaps. This provides immunity to the medical professional as well as the patient.

The project finds applications at places where the decentralization and immutability play a crucial role like hospital management, prescription tracking, crowdfunding, public records, and supply chain systems.

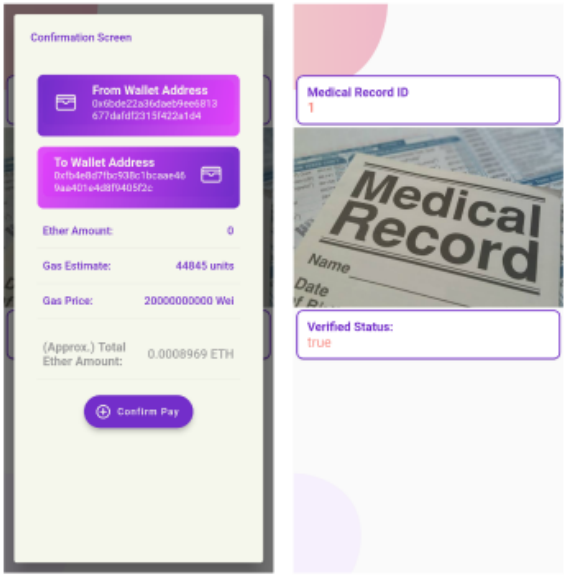


Fig. 7. Confirmation Screen

REFERENCES

[1] A. H. Mayer, C. A. da Costa, and R. da R. Righi, "Electronic health records in a Blockchain: A systematic review," Health Informatics J., vol. 26, no. 2, pp. 1273–1288, 2020.

[2] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for secure EHRs sharing of mobile cloud based E-health systems," IEEE Access, vol. 7, pp. 66792–66806, 2019

[3] G. Yang, C. Li, and K. E. Marstein, "A blockchain-based architecture for securing electronic health record systems," Concurr. Comput., vol. 33, no. 14, 2021.

[4] A. Shahnaz, U. Qamar, and A. Khalid, "Using blockchain for electronic health records," IEEE Access, vol. 7, pp. 147782–147795, 2019

[5] Yogesh Sharma,Prof. B. Balamurugan, "Preserving the Privacy of Electronic Health Records using Blockchain" .International Conference on Smart Sustainable Intelligent Computing and Application under ICITETM2020.

[6] A. Dubovitskaya et al., "ACTION-EHR: Patient-centric blockchain-based electronic health record data management for cancer care," J. Med. Internet Res., vol. 22, no. 8, p. e13598, 2020.

[7] A. Rejeb, H. Treiblmaier, K. Rejeb, and S. Zailani, "Blockchain research in healthcare: a bibliometric review and current research trends," J. of Data, Inf. and Manag., vol. 3, no. 2, pp. 109–124, 2021.

[8] F. Boiani, "Blockchain Based Electronic Health Record Management For Mass Crisis Scenarios: A Feasibility Study," Dissertation, 2018.

[9] A. Khatoon, "A blockchain-based smart contract system for healthcare management," Electronics (Basel), vol. 9, no. 1, p. 94, 2020.

[10] B. L. Radhakrishnan, A. S. Joseph, and S. Sudhakar, "Securing Blockchain based Electronic Health Record using Multilevel Authentication," in 2019 5th International Conference on Advanced Computing Communication Systems (ICACCS), 2019.

[11] N. Kshetri, "Blockchain and Electronic Healthcare Records [Cybertrust]," Computer (Long Beach Calif.), vol. 51, no. 12, pp. 59–63, 2018.

[12] "How Using Blockchain in Healthcare Is Reviving the Industry's Capabilities", Built In, 2022. [Online]. Available: https://builtin.com/blockchain/blockchain-healthcare-applications-companies.

[13] "Consensus Mechanism (Cryptocurrency)", Investopedia, 2022. [Online]. Available: https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp.

[14] e. Network, "Future of EHR in India: Challenges and Opportunities - Elets eHealth", Ehealth.eletsonline.com, 2020. [Online]. Available: https://ehealth.eletsonline.com/2020/11/future-of-ehr-in-india-challenges-and-opportunities/.

[15] A. Sharma and D. Bhuriya, "Literature Review of Blockchain Technology", IJRAR- International Journal of Research and Analytical Reviews, vol. 6, no. 1, p. 8, 2022.

[16] 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.