JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Transforming Healthcare: Harnessing Decentralized Ledger Technology to Secure Patient Information

[1]S.Sudeshna, [2]Ch.Sandhya Rani

[1,2]Assistant Professor
[1,2]Computer Science and Engineering, VNRVJIET,
Hyderabad, India

Abstract : This survey explores the complex field of health record management systems, with a particular emphasis on the common concerns of data security and patient privacy in centralized infrastructures. These systems frequently include flaws that expose patient data to different cyber threats and undermine the legitimacy of healthcare organizations. Decentralized ledger technology appears to be a viable answer to these problems. Using the Ethereum blockchain platform MediBlock as a case study, this survey examines the benefits of decentralized systems. Patients' privacy and data integrity are guaranteed by MediBlock's decentralized design, which grants patients total control of their health data. This survey highlights the many benefits of decentralized systems through a thorough examination, such as improved patient outcomes, simpler data management procedures, and the promotion of transparency, trust, and interoperability throughout the healthcare system.

IndexTerms **- Blockchain, Ethereum, medical records, smart contracts, decentralized technology**

I. INTRODUCTION

In the quickly changing healthcare environment, providing highquality medical care depends heavily on the effective and secure handling of patient data. But interoperability problems, data breaches, and a lack of patient control over their own health information have long plagued traditional centralized data management systems. A novel approach to addressing these issues is presented by MediBlock, a ground-breaking platform that uses blockchain technology's revolutionary potential to usher in a new era of decentralized patient data management.

Utilizing blockchain technology, a decentralized and secure ledger system with unmatched potential across numerous industries, is at the heart of MediBlock's innovation. This technology is used in the healthcare industry to build a strong, impenetrable ecosystem for patient data storage. An unchangeable chain of records is created by carefully encrypting and connecting each patient's medical data into a sequence of blocks. This creates a degree of tamper-resistance that makes it nearly impossible for bad actors to jeopardize patient information in addition to guaranteeing the data's integrity.

The blockchain's decentralized structure solves persistent problems with healthcare data management. Conventional systems frequently experience data breaches, making private data open to unwanted access. On the other hand, MediBlock uses blockchain technology to disperse patient data over a network of nodes, improving security. This offers a strong defense against unauthorized changes to patient records in addition to reducing the possibility of centralized breaches.

The use of smart contracts by MediBlock is one of its distinguishing characteristics. Patients are able to maintain control over who has accessto their health records and under what circumstances thanks to these self-executing contracts. Patients are empowered by their increased ownership and control over their health data, which promotes openness and trust throughout the healthcare system. MediBlock addresses privacy concerns and offers a collaborative, patient-centric approach to healthcare by giving individuals control over information access.

There are three main issues with using paper records in healthcare, starting with the major lack of accessibility. When people are in dire circumstances or are not in the presence of their primary healthcare professionals, it can be extremely difficult to obtain relevant medical information quickly. Manually locating paper records might take a long time, which hinders the quick decision-making that is necessary in emergency situations. This inaccessibility could jeopardize the efficacy and timeliness of medical interventions.

Another barrier is limited interoperability, which causes fragmentation in the healthcare system as a whole because paper records are frequently separated within the systems of particular healthcare providers. Inadequate protocols for information exchange amongst providers lead to inefficiencies and gaps in the provision of care. It becomes difficult for healthcare workers to collaborate and coordinate seamlessly, which impedes the continuity of care and may have an effect on patient outcomes.

These difficulties are made more difficult by security concerns because physical papers are prone to a number of hazards by nature. There are major risks to patient privacy when paper records are lost, damaged, or accessed without authorization. Paper records are not as secure as their digital equivalents because they do not have access controls and encryption, which makes private data more susceptible to hacking. In order to overcome these obstacles, digital health records must be implemented, utilizing technology to improve security, accessibility, and interoperability within the healthcare system.

II. RELATED WORK

Blockchain technology is revolutionizing the healthcare industry by offering creative answers to enduring problems. Numerous scholarly articles elucidate the potential uses, benefits, obstacles, and opportunities for incorporating blockchain technology into healthcare systems. Healthcare 4.0 addresses problems like professional information exchange gaps and the frequency of medical blunders. Blockchain seems as a promising solution that can handle fragmented data landscapes and give patients back control. Although telemedicine is acknowledged for improving the quality of care, issues like privacy and integration continue to be problems[1]. Healthcare is an essential service, particularly in developing nations like Zambia, Kenya, Pakistan, and India where the COVID-19 pandemic has made remote care more crucial. Numerous benefits of telehealth have been demonstrated, including lower costs, remote diagnosis, more effective medication procurement, and protection of patient privacy, security, and sensitivity. The distributed ledger technology known as blockchain holds promise for resolving security and privacy concerns in the healthcare industry. This research highlights the need for an integrated strategy towards a holistic healthcare system by presenting a comparative evaluation of current blockchain-based telehealth platforms. The BlockHeal framework integrates all healthcare industry players in order to include vital patient-critical services. The central health regulatory body oversees the BlockHeal system to guarantee certified and reliable participants.The BlockHeal framework is a cutting-edge method of telehealth that addresses the shortcomings of current systems by offering a platform that unifies all medical services. It offers different DApps for every possible user, including medical laboratories, patients, physicians, health ministries, pharmacies, drug makers, suppliers, and other players in the healthcare sector[2].

The conventional healthcare approach, patient data and treatment-related activities were managed independently, leading to potential issues such as unnecessary tests and medications recommended by doctors for personal gain. Patients often lacked access to their complete medical documentation when switching doctors, allowing illegal activities to go unnoticed.The proposed framework leverages blockchain technology to create a transparent and secure ecosystem. It ensures that patient records, medical diagnoses, prescriptions, lab tests, and medication purchases are stored on a blockchain, guaranteeing data integrity and preventing unauthorized access or manipulation. This blockchain-enabled system facilitates transparent and traceable communication among healthcare entities, mitigating the risk of fraud and misconduct.The proposed patient-centric digital healthcare framework integrates blockchain and AI technology for managing COVID-19 data[3]. The three basic modules in the blockchain , the client module, the blockchain network and distributed data store module define the structure. The client module is a simple ui application that consumes microservices to read and insert data. The blockchain network consists of authentication, consensus and security layer for the data and the distributed store is used to store static data. For the distributed data store a noSQL database is used, in this project virtuoso db has been used. The private blockchain network is implemented from scratch using apache kafka to create the data blocks, apache Storm for distributed processing and apache Zookeeper for synchronization of the communication between the nodes. Gradle is used for automation and application generation[4].

To combat the present breakout and subsequent sickness of the COVID-19 pandemic, MedHypchain was designed as a patientcentric, privacy-preserving medical healthcare data sharing system. Implemented over the Hyperledger Fabric, a permissioned blockchain, is the planned MedHypChain scheme. To improve the security of the proposed MedHypChain system, an identity-based broadcast group signcryption is implemented. Once the ordering process using PBFT as the consensus mechanism is successful, the signcrypted transaction is updated on the blockchain. Confidentiality, anonymity, traceability, and unforgeability are all achieved by the suggested MedHypChain. We deploy a PCI healthcare system in which the patient's medical information is stored on the blockchain and accessible only by authorized nodes[5].

The Healthchain framework is designed to secure electronic health records (EHRs) using blockchain technology. Its architecture includes components like Angular 4 for the frontend, Composer Rest Server for REST API interactions, Hyperledger Composer for smart contract modeling, and Hyperledger Fabric as the underlying blockchain platform. It employs a twofold approach with on-chain (Hyperledger Fabric and CouchDB) and off-chain (IPFS) solutions, ensuring both security and scalability. Access to EHRs is controlled through rolebased and rule-based access permissions, implemented using XML documents. The prototype implementation demonstrates user registration, record management, and access control, guaranteeing data privacy and integrity in healthcare. Secure and efficient storage of health records on IPFS with proper authentication and encryption measures in place. Patient-centric approach encrypts health records with patient public keys, ensuring data privacy.Efficient IPFS storage resolves scalability issues, enabling the system to process large datasets with low latency. Blockchain's immutability can make data recovery challenging in case of issues.Achieving network consensus can require substantial computational resources. Encouraging users to adapt to blockchain technology can be met with resistance[6]. Lack of standardized development practices leads to difficulties in exchanging information between applications developed on different blockchain platforms. Concerns about patient identity exposure and potential security breaches on public blockchains, along with conflicts with GDPR's "right to be forgotten." Storing large biomedical datasets on blockchain can cause performance degradation and operational impracticalities. Blockchain-based processing introduces delays, particularly in validation processes, impacting real-time operations. Encouraging patients, including the elderly and young, to actively manage their health data on blockchain poses a challenge. Blockchain allows for real-time monitoring of patient health, especially critical for immediate responses in emergencies. Blockchain enhances pharmaceutical supply chain management by ensuring traceability, preventing counterfeit drug incidents, and maintaining the integrity of the supply chain. Blockchain's immutability feature ensures the integrity and security of insurance records, while the distributed ledger system allows for decentralized storage and backup of these records across users' computers.Blockchain technology ensures data integrity, eliminates falsification, and allows for transparent replication of research data, making it a revolutionary tool for biomedical research and clinical trial data management[7].

Ethereum smart contracts are used to generate intelligent representations of current medical records that are kept on the network within separate nodes. We construct contracts with permissions, data integrity, and record ownership metadata. Cryptographically signed instructions for maintaining these properties are carried in the blockchain transactions of oursystem. Contract state transition

functions enforce policy solely through valid transactions that require data alteration. As long asa medical record can be computationally represented, these laws can be designed to enforce any set of rules governing that particular medical record. Before allowing a third party to view,a policy can, for instance, require sending separate consent transactions from patients and medical professionals[8]. The integration of healthcare into smart cities has enhanced life and health quality but raised concerns about security, particularly regarding patients' health data and mobile health app users. Traditional security measures like biometrics and passwords have proven insufficient against evolving cyber threats. Regulatory frameworks exist, but more mechanisms are needed to bolster healthcare information security. A survey showed widespread use of mobile health apps in healthcare, yet security and privacy remain significant concerns. Blockchain technology offers a promising solution, ensuring secure storage of patient data through decentralization, transparency, and resistance to tampering. The MedRec prototype and ModelChain illustrate how blockchain can safeguard electronic health records while granting patients control over data access permissions. However, challenges like public vs. private blockchain selection, security in smart contracts, and efficient data sharing need to be addressed for seamless blockchain integration in healthcare. A user-centric health data sharing solution is proposed, using permissioned Blockchain to protect privacy and enhance identity management. Smart contracts offer an efficient way for transactions, but security concerns must be minimized. A web-based application for personal health data management (PHDM) system is proposed, allowing individuals to synchronize sensor data from wearable devices with online accounts and control data access from third parties. The integration of information and technology with healthcare has significant impacts on improving health and medical services worldwide[9].

The study uses blockchain technology to securely transmit clinical trial data across institutions and researchers; although it is not exactly the same as our project, the underlying technologies and implementation are very similar. JavaScript user interface is utilized for user interaction, while the Ethereum blockchain powers the blockchain network. Blockchain is utilized for user registration and authentication as needed. Data access control is achieved by registry smart contracts. Data is kept in a database, and references to it are transferred in an encrypted format that can only be decrypted by the intended recipient using his private key. Next, using the sender's public key, the recipient must confirm that the data is truly coming from the intended sender..[10]. In a study, personal health records (PHRs) are integrated using a distributed architecture paradigm called OmniPHR. The concept attempts to solve the problems of giving healthcare professionals access to the most recent data and enabling a unified picture of disparate health information. OmniPHR gives patients the ability to manage their medical history from any device in a single, unified perspective, and gives healthcare providers access to connected patient data from many health organizations. The process utilized to create the OmniPHR model is not specifically mentioned in the publication. It does, however, discuss the use of natural language processing (NLP) to automate the conversion of old health records to the standard format used by the model and the creation of an equivalent ontology for every datablock kept in a semantic database. offers a distributed and compatible PHR architecture approach. gives patients a unified view of their medical history and healthcare professionals access to the most recent patient information. Encourages a cohesive perspective on PHRs that is both flexible and expandable[11].

By allowing patients to securely access and share their health information, blockchain technology is transforming the healthcare industry. In order to address security concerns in e- Health systems, this work tests a suggested strategy utilizing two databases: brain-development.org/ixi-dataset/ and www.microscopyu.com/galleries/pathology. The suggested picture segmentation technique prevents keyword deduction by using wavelet analysis to retrieve original image modalities. A consortium blockchain and a private blockchain make up the suggested blockchain architecture. The private blockchain is used to store patient data and enables medical professionals to create records on their behalf.The block header and the system payload are the two fundamental components of the suggested block structure. The system manager oversees the system and keeps a public key tree for physicians and patients. Medical service providers produce blocks pertaining to patients' health records and transmit the information to the hospital's private blockchain. In conclusion, blockchain technology can revolutionize healthcare by enabling patients to access and share their health information securely. The proposed block structure consists of two main parts: the block header and the system payload[12].

There are two types of healthcare interoperability that are becoming more popular: patient-driven and institution-driven. The foundation of institution-driven interoperability is the exchange of data between various healthcare organizations in response to commercial or legal incentives. By enabling patients to access their electronic health records via common protocols like APIs, patient-driven interoperability empowers patients to take charge of their digital health records. Issues with patient permission, governance, security, privacy, and participation are some of the problems this paradigm faces. Blockchain technology offers a safe framework for data sharing, which can assist in addressing these issues. Practical restrictions and difficulties still exist, though, including the need to scale blockchain for the volume of healthcare transactions, privacy and security issues, patient key management, and interoperability incentive programs. The transition from interoperability driven by institutions to that led by patients has the capacity to drastically modify attitudes and regulations regarding the exchange of clinical data[13].This problem was not addressed by the Health Information Technology for Economic and Clinical Health (HITECH) Act, which resulted in data theft that affected around 2.6 billion people between 2015 and 2017. Since individual clinicians usually handle EHRs, there are security, privacy, and control issues. Sensitive information has occasionally been incorrectly secured by hospitals, and it can be challenging to verify data integrity. Protecting the freedom to transfer or change health insurance, lowering fraud and abuse, establishing digital billing standards, and demanding privacy and security of protected health information are the four primary objectives of HIPAA, a rule for healthcare data systems. Healthcare data systems need to accomplish four things in order to be HIPAA compliant: grantingthe patient ownership and final control; securely limiting access; enabling safe transmission; and reducing the possibility that unauthorized parties will obtain PHI. Blockchain technology is adistributed ledger that replicates data throughout all nodes, eliminating any single point of failure and facilitating simple verification. Ethereum, a well-known cryptocurrency with millions of users, serves as its foundation. Patients now have more control over their medical data thanks to the framework, which uses permissioned blockchains and smart contracts for storage and access management. Hashed pointers and indices are stored on both blockchains, increasing system scalability and facilitatingfaster data transfer[14].

With the use of common protocols like APIs, patients may now access their electronic health records thanks to blockchain technology, which is revolutionizing healthcare interoperability. The transition to patient-centered interoperability raises issues with patient consent, governance, security, privacy, and engagement, among other things. By offering a high-level framework for safely

communicating with numerous stakeholders, identifying oneself across entities, and collecting health data in a durable format, blockchain can help with this shift. Practical restrictions and difficulties still exist, though, including managing patient keys, scaling blockchain to accommodate the amount of healthcare transactions, privacy and security issues, and patient involvement. Promoting interoperability is essential to the ongoing creation and upkeep of data interfaces that interact with patients. The transition from interoperability driven by institutions to that led by patients has the capacity to drastically modify attitudes and regulations regarding the ownership and exchange of clinical data[15]. A safe mechanism for exchanging data about electronic medical records is the Blockchain-Based Data Sharing Scheme (BBDS). Membership keys are generated by the issuer and shared with the verifier. After requesting and confirming membership, users are given a membership private key. After confirming their membership, the verifier sends a transaction private key. When a user sends a request, it gets signed by the user and added to a queue of unprocessed requests. This creates a block. Hashed with sha256, the block header guarantees security and immutability. A user's request for data access or contribution is processed by the consensus node, which also records the request's format and length and creates a chain[16].

III. METHODOLOGY

The alternative to the existing system is to use a blockchain for decentralized and secure approach.
The patient data can be managed and accessed by patients, healthcare providers, insurance companiesin an efficient manner.

•The primary interface for usersto access and manage their health information through web browsers.

• Users will need to authenticate securely to access their health records. Will implement Multi-Factor Authentication(MFA) for added security. Define access control policies to manage who can view and update health records.

• Users can input and update their health records, including medical history , test results, medications and other relevant information. Data input should be user friendly with structured forms and intuitive interfaces.

A. User Interface:

Developers may create fluid and engaging user interfaces for blockchain projects by combining Web3.js for blockchain connection with React for UI development. While Web3.js offers the tools required to interact with the Ethereum blockchain, enabling features like reading blockchain data, sending transactions, and deploying smart contracts directly from the web browser, React's component-based architecture makes it easier to create modular and dynamic user interface elements. This connection improves the usability and accessibility of decentralized applications by enabling users to interact with blockchain applications through user-friendly and responsive interfaces.

B. Smart Contracts:

Develop smart contracts to govern data access. Sharing , and consent management. Smart contracts can enforce rules, permissions, and facilitate secure data transactions while maintaining transparency.

C.Authentication and verification:

Metamask is a mobile app and browser extension designed to make it easier to interact with decentralized applications (dApps) based on Ethereum. Private keys are managed locally, Ethereum based assets are safely stored, and users can easily access and engage with a variety of dApps straight from their mobile devices or browsers. Before a transaction is broadcast to the Ethereum network, Metamask asks users to examine and approve it. It also provides features like network support, password protection, seed phrase backup, and phishing protection to further improve user security. Being an open-source project, Metamask promotes confidence and transparency in the cryptocurrency community, which makes it a well-liked option for Ethereum asset management and interacting with the expanding decentralized application ecosystem.

D. Blockchain Network:

Hardhat is a development environment with a set of tools for effective scripting, testing, debugging, and deployment that is designed for Ethereum smart contracts and decentralized apps (dApps). Hardhat makes building and deploying Ethereum-based projects easier with features like built-in plugins, automated testing, scripting capabilities, seamless integration with Ethereum networks, and robust community support. These attributes make Hardhat a preferred option for blockchain developers.

E. Data Storage

IPFS (InterPlanetary File System) is a decentralized protocol designed to facilitate peer-to-peer storage and sharing of content on the internet. Unlike traditional centralized storage systems, IPFS uses a distributed network of nodesto store and retrieve data, making it resilient to censorship and single points of failure. Content on IPFS is addressed using content-based addressing, where files are identified by their unique cryptographic hash, enabling efficient content distribution and retrieval. This approach enhances data redundancy, availability, and fault tolerance, as files are replicated across multiple nodes in the network. IPFS is particularly well-suited for applications requiring decentralized and censorship-resistant data storage, such as distributed applications, content delivery networks (CDNs), and decentralized finance (DeFi) platforms.

IV. CONCLUSION

To sum up , MediBlock is a ground-breaking development in medical technology that provides a thorough answer to the problems associated with effectively and safely managing patient data. MediBlock gives users unprecedented control over their health information while ensuring data integrity, privacy, and accessibility through the use of blockchain technology.
MediBlock reduces the dangers of medical errors and data breaches while streamlining patient and provider data sharing through its decentralized method. MediBlock's revolutionary influence goes beyond simple data administration; it signals a paradigm change in

healthcare toward a patient-centered approach where people are given the freedom to actively engage in their own treatment choices. MediBlock is leading the way in the healthcare industry's adoption of technological innovation, ushering in a new era of efficiency, transparency, and patient empowerment.

V. REFERENCES

[1] Stefano Abbate , Piera Centobelli , Roberto Cerchione , Eugenio Oropallo , and Emanuela Riccio [2022]. Blockchain Technology for Embracing Healthcare 4.0

[2] Narmeen Zakaria Bawany , Tehreem Qamar, Hira Tariq , And Saifullah Adnan[2022]. Integrating Healthcare Services Using Blockchain-Based Telehealth Framework.

[3] Krishna, P. R. ., & Rajarajeswari, P. . (2022). EapGAFS: Microarray Dataset for Ensemble Classification for Diseases Prediction. International Journal on Recent and Innovation Trends in Computing and Communication, 10(8), 01–15. https://doi.org/10.17762/ijritcc.v10i8.5664

[4] Mohamed Yaseen Jabarulla and Heung-No Lee [2021]. A Blockchain and Artificial Intelligence-Based, PatientCentric Healthcare System for Combating the COVID-19 Pandemic: Opportunities and Applications Student Dropout Prediction

[5] Alex Roehrsa , Cristiano André da Costaa, Rodrigo da Rosa Righia , Valter Ferreira da Silvab , José Roberto Goldimb , Douglas C. Schmidt [2019]. Analyzing the performance of a blockchain-based personal health record implementation

[6] Shekha Chenthara, Khandakar Ahmed , Hua Wang , Frank Whittaker, Zhenxiang Chen [2020].Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology.

[7] Cornelius C. Agbo, Qusay H. Mahmoud, J.Mikael Eklund [2019]. Blockchain technology in Healthcare: A systematic review

[8] Asma Khatoon [2020]. A Blockchain-Based smart contract system for healthcare management

[9] Jinglin Qiu, Xueping Liang,Sachin Shetty, Daniel Bowden ++ [2018]. Towards Secure and smart healthcare in smart cities using Blockchain

[10] Peng Zhang, Jules White, Douglass C.Schmidt, Gunther Lenz, S.Trent Rosenbloom[2018].FHIRChain : Applying Blockchain to securely and scalably share clinical data.

[11] Alex Roehrs, Cristiano André da Costa ⇑ , Rodrigo da Rosa Righi [2017]. OmniPHR : A distributed architecture model to integrate personal health records.

[12] Ahmed Faeq Hussein , Abbas K. ALZubaidi , Qais Ahmed Habash and Mustafa Musa Jaber [2018]. An Adaptive Biomedical Data Managing Scheme Based on the Blockchain Technique

[13]William J. Gordon, Christian Catalini [2018]. Blockchain Technology for Healthcare: Facilitating the transition to patient-driven interoperability

[14] Gaby G. Dagher, Jordan Mohler, Matea Milojkovic, Praneeth Babu Marella[2018]. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology.

[15] Abdullah Al Omar, Md Zakirul Alam Bhuiyan, Shinsaku Kiyomoto[2019]Privacy-friendly platform for healthcare data in cloud based on blockchain environment

[16] Emmanuel Boateng Sifah, Abla Smahi, Sandro Amofa[2017].BBDS: Blockchain-based data sharing for electronic medical records in cloud environments