Grenze International Journal of Engineering and Technology, June Issue

Blockchain based Medical Data Asset Management System

Akanksha Srivastava[1], Khalid Farooq[2], Rakshitha B[3], Rishika Kumari[4], Shruthi K[5], A. S. Poornima[6] and M. B. Nirmala[7]
[1-4]UG student, Computer Science and Engineering, Siddaganga Institute of Technology
Tumkur, India
Email: {akankshabsrivastava, wandererkhalid, rakshitabantwal1, rishikaojha1310}@gmail.com
[5]Assistant Professor, Computer Science and Engineering, Siddaganga Institute of Technology
Tumkur, India
Email: shruthik@sit.ac.in
[6]Professor, Computer Science and Engineering, Siddaganga Institute of Technology
Tumkur, India
Email: aspoornima@sit.ac.in
[7]Associate Professor, Computer Science and Engineering, Siddaganga Institute of Technology
Tumkur, India
Email: mbnirmala@sit.ac.in

***Abstract*—In today's health care management, medical health records are in the form of electronic medical record (EHR/EMR) systems. These systems store a patient's medical history in a digital format. However, a patient's medical data being acquired in an efficient and timely manner is proven to be difficult through these records. Health management is always hindered by the inability to acquire information, less usage of information acquired, unmanageable privacy controls, and poor data asset security. In this paper, we are introducing an efficient as well as a secure medical data asset management system using blockchain in order to resolve these issues. Blockchain technology eases the accessibility of all such records by maintaining a block for every individual patient. This paper proposes an architecture using an off-chain solution that will enable doctors, and patients to access records in a safe way. Blockchain makes medical records immutable and encrypts them for data integrity. Users can observe their health records, but only patients own the private key and can only share it with whom they desire. The smart contracts also help our data owners to manage their data access in a permissioned manner. The final result will be viewed as a web and mobile interface to easily access, detect as well as ensure high-security data.**

***Index Terms*— Medical data, Management, Blockchain, Web and mobile application.**

I. INTRODUCTION

One of the biggest issues faced worldwide in the healthcare and medical sector is the incapacity for medical data to be acquired in an efficient and timely manner. All electronic medical record or electronic health record (EMR/EHR) systems presume that each patient approaches medical practitioners in one clinic or in the common state or province. These systems are only centered around the same practitioner and the use of such information

Grenze ID: 01.GIJET.8.2.518

is not useful nor accurate. Patients visit multiple doctors per year for various reasons. The broader aspect of practitioners that usually aren't taken into account are chiropractors, pharmacists, etc. Patients also travel for vacation, work, and even relocate for a longer duration. In the present day, a large number of patients are vastly interested in recording their health status using wearable health devices. This health data generated by patients is easily acquired by the service providers or devices but never by medical practitioners. Therefore it is proven hard for a patient to get their multiple records accessed through a summarized EMR because of security and privacy concerns. Thus, regardless of patients being the rightful owners of their medical data assets, and in spite of practitioners, health facilities, and the government providing large medical investments, health management is always hindered by the inability to acquire information, less usage of information acquired, poor data asset security and unmanageable privacy controls. These are the key reasons for developing a health care management system using blockchain. For these security reasons, blockchain is implemented in this healthcare management system.

Blockchain is considered to be the immutable ledger which is decentralized, distributed and stores data in blocks. Each block of the blockchain is connected with its preceding block through the link. Since each header of the block has the hash value of the preceding one, it becomes computationally infeasible for a third party to change any data in the blockchain as it needs to be reflected on every node of the blockchain. This makes blockchain an immutable and secure database to store private information. As every node is independent in the blockchain and no node is superior to others, it technically forms a decentralized system that is robust for handling such big data-like medical records. In order to implement hashing of pointers, we use Merkle tree. Merkle tree on the other hand are cryptographic hash pointers represented as a binary tree. The construction of a Merkle tree is done by taking the hash of a pair of data as the leaf node, and its output is hashed till the root node. The usage of Merkle trees makes transaction verification easier and faster in the blockchain. But since permissionless blockchains are susceptible to being disruptive, permissioned chains are being implemented as they steer clear from expensive consensus mechanisms and work in environments that are trusted.

This paper implements a hyper ledger-based blockchain architecture that is more extensible and scalable. In this paper, we include mainly three components - an application user interface, an access control module as blockchain, and data storage based as off-chain. Any medical data being shared by an individual for their convenient exchange with the doctors needs to be secured from any sort of third-party intrusion. The data might hold crucial information regarding the patient's history which might affect them, thus any sort of change in the data by a third party intentionally or not may cause severe damage to the individual. Also at the time of emergency, a doctor might need all of the patient's history where an efficient database is required. Therefore, all medical data must be secured and efficiently available, which in this case is done using blockchain. All data assets like medical reports, prescriptions, treatment plans, drugs, etc. are kept in a safe cloud-based repository to maintain the level of performance and keep it economically feasible. The application interface makes the system smoothly available to access for doctors, patients, distributors, and manufacturers. The on and off-chain data are securely linked through the patent-pending method without any storage load in the blockchain architecture. Smart contracts provide data owners access to their records in a permissioned and safe manner.

II. Literature Survey

One research paper by Kai Fan, Shangyang Wang, Yanhui Ren, Hui Li and Yintang Yang titled "MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain" [1] aims to provide a familiar method of storing patients' information at hospitals. For a common patient, data is stored in multiple hospitals. Thus for a patient to get their multiple records accessible through a summarized EMR is proven hard because of security and privacy concerns. This paper provides a solution to the above problems by giving a blockchain-based information management system called 'MedBlock'. Here MedBlock's distributed ledger provides easy retrieval and access of data in electronic medical records. This paper also achieves an improved consensus mechanism and high data security by utilizing symmetric cryptography and customized access control protocols.

Catering to the needs of issues that arise in remote patient monitoring systems, Kristen N. Griggs, Olya Ossipova, Christopher P. Kohlios, Alessandro N. Baccarini, Emily A. Howson and Thaier Hayajneh published a paper titled "Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring" [2] for resolving security concerns related to exchange and recording of data transactions. In order to resolve these issues, this paper proposed a blockchain-based smart contract to ensure safe analysis and medical sensor management. The paper used the Ethereum protocol and created a system where the smart device is communicating with the sensors and calls smart contracts while at the same time logging every event on the blockchain. This benefits patients with real time tracking and intervention in the medical field by notifying

patients and practitioners, while simultaneously providing security. This paper resolves all security issues in medical smart devices health management in a HIPAA compliant manner.

Highlighting flaws in the centralized approach to maintaining health records, the research paper "Health Record Management through Blockchain Technology" by V. M. Harshini, S. Danai, H. R. Usha, and M. R. Kounte [3] brings out the issue of a data breach. There is a huge loss for institutions as well as patients when a data breach happens, in terms of monetary as well as health loss. Moving forward, this paper also reveals the flaws in institution-centralized data control and gives a decentralized system using blockchain as a solution. In health care, smart contracts help to make things simpler. Where Blockchain will be used for invocation, record production, and validation. The solution proposed could be used as a solution for various problems in the medical domain such as record maintenance, record sharing, billing, medical research, etc. It lays the theoretical base for a model of maintaining records with the help of blockchain, further research and practical implementation.

Similarly, research titled "A Secure and Scalable Data Source for Emergency Medical Care using Blockchain Technology" is a paper that focuses on the poor management and causes of failure of Emergency Medical care, written S. Hasavari and Y. T. Song [4] A lot of pre-hospital deaths are caused due to the lack of medical history of patients. A lot of patients' data is generated in some other hospital and later is relevant to some other hospital. It is very difficult for a different healthcare system to retrieve a patient's medical history from the previous healthcare system. In this paper, a safe filing system and blockchain is proposed as the remedy to emergency access to patients' records. All medical record concerns like authentication and privacy have been taken care of in this approach. With the help of the practical implementation of this paper, the ambulance crews can access patients' medical history and avail high-quality pre-hospital care which leads to a much less death rate.

Blockchain in the medical system has few healthcare systems that provide targeted sharing protocols for medical data and personal health data. The paper titled "MedBlock: Blockchain-based Multi-role Healthcare Data Sharing System" by Y. Yu, Q. Li, Q. Zhang, W. Hu, and S. Liu, [5] proposes a data management system for multiple users by combining blockchain and the InterPlanetary File System (IPFS).

Another work in similar literature, "Blockchain-based approach for e-health data access management with privacy protection" by L. Hirtan, P. Krawiec, C. Dobre and J. M. Batalla [6] provides a design where blockchain is used in the healthcare system for the storage of information in clinics, and hospitals based on the patients' access policies. The paper shows 2 types of chains i.e. a private sidechain and a public main chain, which either keeps information of the patients' real ID or information with a temporary ID.

Research, "Blockchain in Healthcare: A Patient-Centered Model", by Hannah S Chen, Juliet T Jarrell, Kristy A Carpenter, and David S Cohen, Xudong Huang [7] proposes a technology that could be utilized in many places for sharing and storing health records for both hospitals and application interfaces. After blockchain gained popularity in software research, it started providing data authority over to patients. This project thus created a change in authority for patients resulting in a patient-centered model.

A similar work titled "MedAccess: A Scalable Architecture for Blockchain-based Health Record Management" by M. Misbhauddin, A. AlAbdulatheam, M. Aloufi, H. Al-Hajji and A. AlGhuwainem, [8] aims for a decentralized medical structure using blockchain, though the price of storing information and records is overpriced on the blockchain. This price is due to the high amount of computaion required in a transaction prior to committing on the blockchain. Cost of managing patient's electronic health records (EHRs) is not feasible and costly on a blockchain service. Here, a project design solution is provided to reduce the high expenses on a blockchain. Furthermore, the usage of watermark as a way to store patients' media results in addition to the usage of encryption on IPFS objects stored in the network.

III. METHODOLOGY

A. Blockchain

A blockchain is a growing list of records, called blocks, that are linked together using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree) [9]. The timestamp verifies that the transaction data was there at the time the block was released, allowing it to be hashed. The blocks form a chain, with each new block reinforcing the preceding ones as it contains the information of the previous block. As a result, blockchains are resistant to data tampering since the data in any given block, once recorded, cannot be changed retrospectively without affecting all subsequent blocks.

Hyperledger Fabric, an open-source project from the Linux Foundation, is the modular blockchain framework and de facto standard for enterprise blockchain platforms [10].

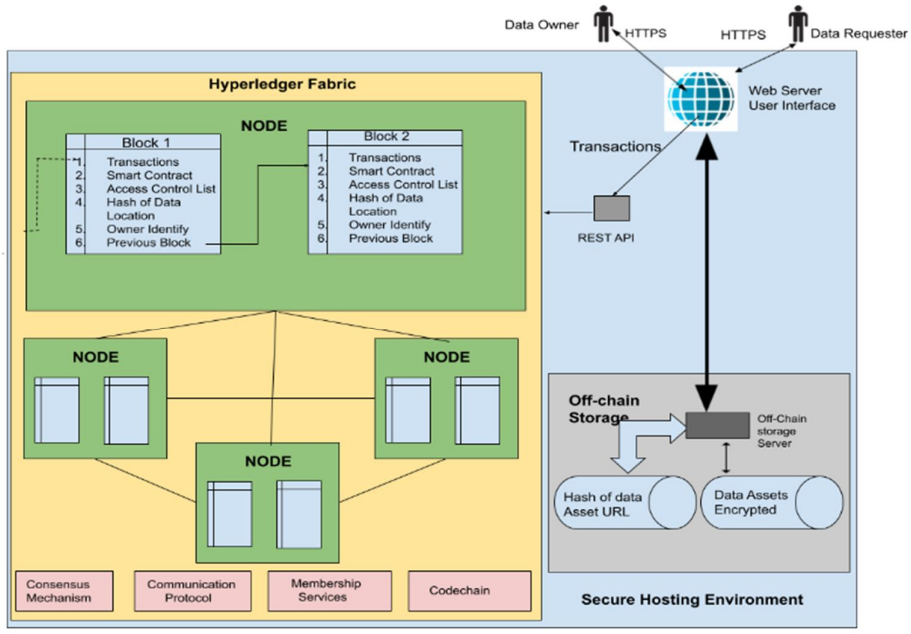

Fig. 1: Architecture

As shown in Fig. 1, We have two main entities, the data owner and the data requester who would be handling the data. The purpose of the project is to give the owner total control over their data, hence we will be using Discretionary Access Control (DAC) policy. The architecture is based on Hyperledger Fabric, which contains different nodes to store medical history. Hyperledger Fabric is a distributed ledger platform that is permissioned where all nodes in the network have an identity. Each node has a hash key which is used to securely access data from off-chain storage.

Each patient (the data owner) has its own blockchain and access to the blockchain can be given to the data requester, like doctors, pharmacies, and hospitals for a specified period of time. The patient can give permanent consent as well to a requester in order to facilitate emergency access to retrieve data. To maintain the integrity of the data, the patient will have the option to check consent details given till a certain point in time. The application would also facilitate the fetching of reports and prescriptions both by the patient as well as the data requestors.

The data requestors who have consent from the patient will have permission to add the blocks to the chain. The doctor can refer to tests and treatments which the patient has to go through and also prescribe drugs using the blockchain. In addition to this, the doctor can add comments and media to the blocks.

When a patient visits a hospital a new prescription is made. In a similar way, hospitals will have the permission to create a new report inpatient blockchain. In addition, hospitals will have the functionality to register a patient for the treatment recommended by the doctor and start the treatment.

B. Consensus

The model presented in this paper is patient-centric, and hence the patient holds the power of decision making in order to reach consensus. Once a patient gives permission, other entities like doctors, hospitals, and pharmacies can access the patient's data and participate in the consensus to agree upon a single, stable, and uniform state of the blockchain.

The technical freedom to create channels between the entities to further ensure safe and secure flow of data across entities allowed to participate in the channel. This in turn helps in creating a private network inside the blockchain between the chosen entities.

C. API Workflow

The following flow chart shown below in Fig. 2 displays the API workflow of the system. The description of each entity within the system is as explained.

Patient: The patient user registers to the network requiring their Aadhar number (a 12 digit individual identification number of India) and a consenter ID. This provides temporary consent to the doctors based on their ID.
Hospital: The hospital user creates a report for patients about their tests, details etc, using the patient ID.
Doctor: The doctor user refers tests to patients, along with the type of tests and treatment to be conducted.
PathLab: This user tests based on supervisor's ID and prescribes drugs to the patient
Pharmacies: Pharmacies give drugs along with a recommendation message. The refer treatments to patients accordingly.
Hospital: This user begins treatment based on the supervisor ID. Doctor further adds comments and media files to the patient's records.

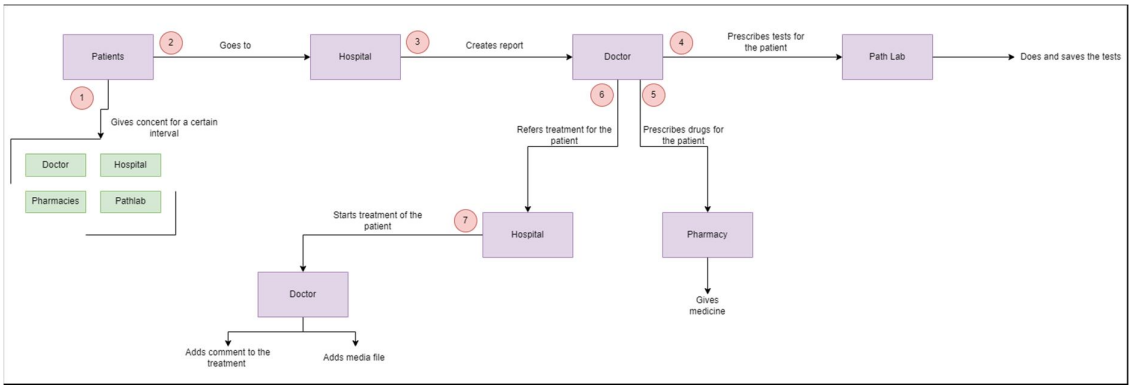

Fig. 2: Data Flow within the system

D. Off-chain Storage

The medical data management system will contain a huge amount of data which could not be accommodated on the block itself. In order to scale the system we would need storage off the blockchain. This storage is called off-chain storage. The off-chain storage can be a structured or unstructured storage which can contain a variety of data ranging from text to images.
There are various issues with current on-chain storage : access issue, performance issue, security issue, success issue, and cryptographic issue. In order to avoid all these we can use an off-chain storage which is shared and secure. To harness the advantages of distributed systems, the project will be using a nosql database named couchDB. CouchDb is a document based database which facilitates both structured as well as unstructured data. It also is highly compatible with hyperledger and highly responsive to HTTP requests which makes the transaction easier and faster. The couchDB also has a feature of replication and follows ACID property which prevents any kind of data loss and maintains the atomicity of each and every transaction happening in the chain.
The blocks in blockchain will contain a hash value which will refer to the partition where the data is stored in the database.

E. UI Description

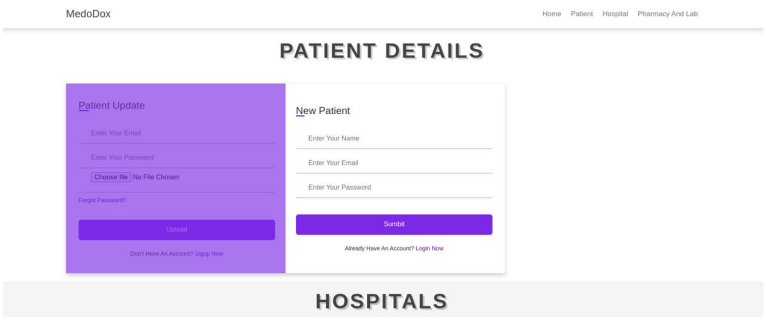

Fig. 3: UI for patient registration

The user interface of the medical data management system will have five activities, one for the data owner (the patient) and another 4 for the data requestors (doctor, hospital, pathLabs, and pharmacies). Each activity will have a registration and sign-in functionalities. During the time of registering each entity will be provided a unique id which will be referenced while accessing the blockchain.
The patient will have a page where they can view their medical records. On the other hand, the other entities (doctors, hospital, pathLab, and pharmacies) will have access to view as well as upload the designated details in the form of a new block to the blockchain.
In order to give a flawless experience to the users, a mobile application will be developed using a cross platform tool named flutter. This will make sure that the user outreach is not only limited to android or iOS users but to both.

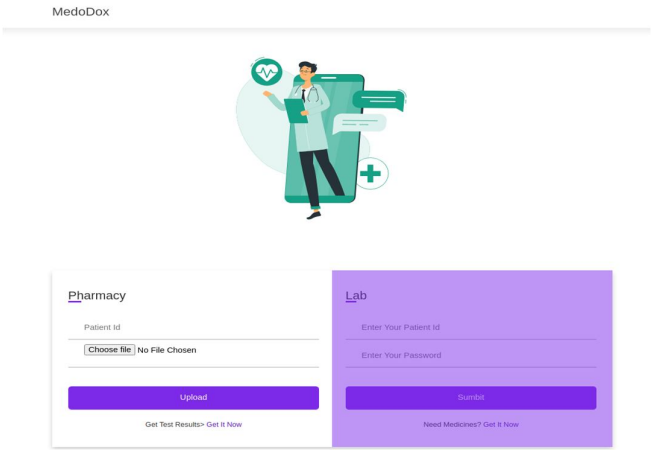

Fig. 4: UI for updation in patient blockchain by pharmacy and Lab

The undergoing UI of the working system is shown. As displayed in Fig. 3, it is the user interface for our patients to register themselves if they are new to the site and updating their new medical health records to the database through their ID and password. The hospital entity is where patients update their latest test results or prescription for any further comments from the doctor assigned. As shown in the Fig. 4, it is the phamacy and laboratory section where the respective departments function according. As the pharmacy provides the medicine as per the prescription provided and the laboratories perform the tests mentioned in the form submitted.

IV. Results

A. Secure an Enhanced Protocol for the Storage of Private Health Data

Implementing a blockchain data structure provides immutability of data and authenticity to the users accessing the data. The data stored can only be updated or inserted by the authority that owns the private key while others could access their own data for viewing. This ensures the authenticity that only authorized people like hospitals, caregivers and laboratories could update the data of a patient. The blocks in the data chain are linked to previous blocks using the hash of the block, thus any change in a block needs to be updated in every block to acquire an enhanced secure protocol for the storage of private health data as every block holds a copy of the entire blockchain. This makes our project a secure structure to store the medical data of every individual.

B. An Economically Feasible Health Data Management System

Maintaining an entire database that includes all medical records of every patient requires a large amount of space which directly requires a vast amount of storage thus increasing the cost of maintaining the blockchain exponentially. To reduce the cost of storage and provide an economically feasible health data management system, we have maintained an off-storage database where we keep the actual data of every individual, whereas the actual blockchain holds the link to the cloud storage where the medical assets are stored.
After the implementation of the solution proposed in the paper, we were able to give the data requesters (the hospital and doctor) a temporary access and it was tested using Postman, as shown in Fig. 5.
As shown in Fig.6, the changes in the blockchain can be visualized using Hyperledger-fabric explorer and secure the data within different channels.

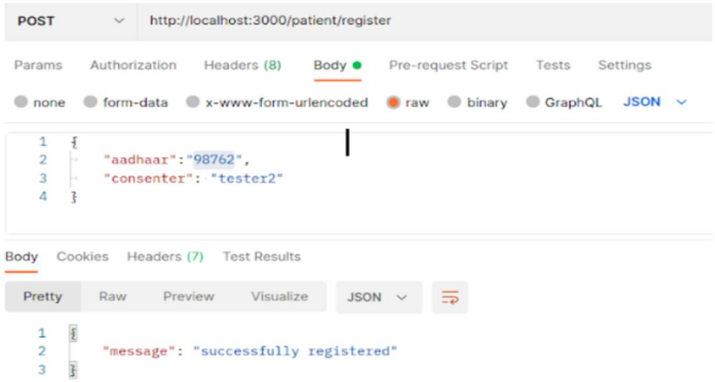

Fig. 5: API response for patient entity

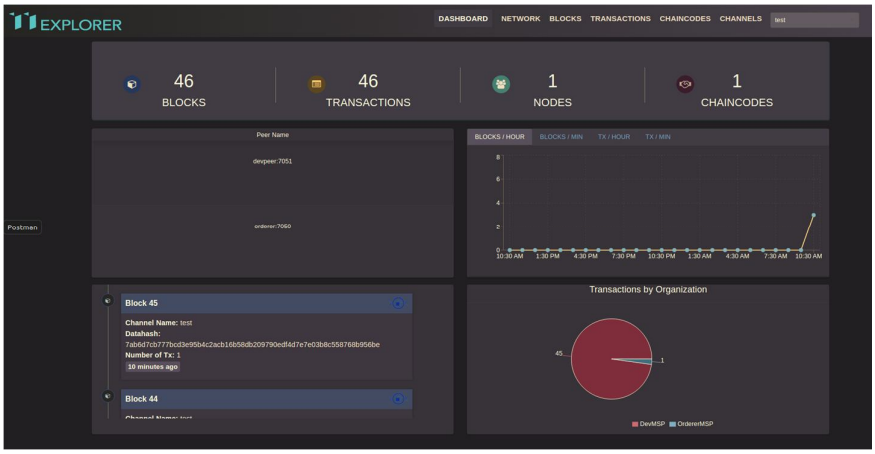

Fig. 6: Hyperledger Explorer for the blockchain

The existing system of healthcare is centralized and not secure while the proposed system provides decentralisation and gives appropriate amounts of security to the crucial medical data using consensus mechanisms. The decentralisation helps the access of medical data from any part of the world which would help in solving data loss problems during relocation and lack of input during treatment.

VI. Conclusion

As the world is moving forward, every aspect of life is measured in terms of time and energy consumption. In order to keep up with the status quo, the medical system needs to be upgraded. One form of healthcare upgrade is to facilitate efficient access and retrieval of data assets between patients, doctors, and caregivers while parallelly maintaining a secure protocol for the accessibility of private data assets.

This paper focuses on providing a convenient way of easing the retrieval and storage of an individual's health record using a blockchain data structure which makes data stored in each block to be immutable. In the blockchain, the blocks are linked to the previous block with a hash value and every block has a copy of the entire blockchain, and thus any change or update on any block needs to be reflected on every block which makes it computationally impossible to breach and resulting in blockchain to be a very secured data structure to store medical records.

Restricting who can update or add data to the blockchain also helps in providing security or resistance from any sort of impersonation. This is facilitated using public and private keys, where the private keys restrict only authorized users to updating the records. In the medical data asset, only the hospitals and doctors are allowed to update the test results, recommendations, or treatment analysis.

Ultimately, this paper aims to play an important role in the health care and management of data assets for patients to be able to update their new reports and get the needed report analysis and prescriptions from the medical practitioners while also ensuring that the integrity of their data is maintained.

REFERENCES

[1] Fan, K.,Wang, S., Ren, Y. et al. MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. J Med Syst 42, 136 (2018). https://doi.org/10.1007/s10916-018-0993-7.

[2] Griggs, K.N., Osipova, O., Kohlios, C.P. et al. Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. J Med Syst 42, 130 (2018). https://doi.org/10.1007/s10916-018-0982-x.

[3] V. M. Harshini, S. Danai, H. R. Usha, and M. R. Kounte, "Health Record Management through Blockchain Technology," 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 2019, pp. 1411-1415, doi: 10.1109/ICOEI.2019.8862594.

[4] S. Hasavari and Y. T. Song, "A Secure and Scalable Data Source for Emergency Medical Care using Blockchain Technology," 2019 IEEE 17th International Conference on Software Engineering Research, Management and Applications (SERA), 2019, pp. 71-75, doi: 10.1109/SERA.2019.8886792.

[5] Y. Yu, Q. Li, Q. Zhang, W. Hu, and S. Liu, "Blockchain-Based Multi-Role Healthcare Data Sharing System," 2020 IEEE International Conference on E-health Networking, Application & Services (HEALTHCOM), 2021, pp. 1-6, doi: 10.1109/HEALTHCOM49281.2021.9399028.

[6] L. Hirtan, P. Krawiec, C. Dobre and J. M. Batalla, "Blockchain-Based Approach for e-Health Data Access Management with Privacy Protection," 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2019, pp. 1-7, doi: 10.1109/CAMAD.2019.8858469.

[7] Hannah S Chen†, Juliet T Jarrell†, Kristy A Carpenter, David S Cohen, Xudong Huang* Department of Psychiatry, Massachusetts General Hospital and Harvard Medical School, USA.

[8] M. Misbhauddin, A. AlAbdulatheam, M. Aloufi, H. Al-Hajji and A. AlGhuwainem "MedAccess: A Scalable Architecture for Blockchain-based Health Record Management," 2020 2nd International Conference on Computer and Information Sciences (ICCIS), 2020, pp. 1-5, doi: 10.1109/ICCIS49240.2020.9257720.

[9] "Blockchain", 22:47, 11 April 2022, Wikipedia [Online]. Available: https://en.wikipedia.org/wiki/Blockchain

[10] "Hyperledger fabric", 22:57, 1 April, 2022, [online]. Available: https://www.ibm.com/topics/hyperledger