Journal of Positive School Psychology http://journalppw.com
2022, Vol. 6, No. 5, 42 – 55

Blockchain Technology Based Model to Secure Patient Data

[1]Tushar Ghumare, [2]Amit S. Savyanavar

[1]School of Computer Engineering & Technology, Dr. Vishwanath Karad MIT World Peace University, Pune, India, tusharghumare3@gmail.com
[2]School of Computer Engineering & Technology, Dr. Vishwanath Karad MIT World Peace University, Pune, India, amit.savyanavar@mitwpu.edu.in

Abstract

The research work explores the healthcare industry's possibilities to secure patient data using hyper ledger Fabric. The Electronic Health Record (EHR), which is highly sensitive, is the current option in healthcare for storing and sharing medical records. Due to a lack of trustworthy and dependable healthcare data sharing mechanisms, the majority of EHR data sharing is still done by mail. As a result, the patient-related is vulnerable to security breaches. Blockchain has the potential to revolutionize healthcare by bringing the patients at the center of the system and increasing health data protection and accessibility. Blockchain is a decentralized architecture that provides cryptographic data integrity, security, and anonymity, as well as smart contracts for data access. The paper covers several hyper ledger Fabric ideas and provides Based on the hyper ledger Fabric platform, a permission Blockchain system solution for storing and sharing healthcare records. Patients have complete control over their medical data and can grant or revoke access to clinicians using simple grant and revoke processes. It also discusses the challenges that must be overcome and issues Before Hyper ledger Fabric can be successfully adopted in healthcare systems, these issues must be handled.

Keywords: Hyper ledger fabric, Fabric SDK, Ledger, Smart Contract, Chain code.

1. INTRODUCTION

The healthcare services received at various hospitals and clinics have become prevalent. There's significant advancement in the healthcare services and also patient's mobility is dominant. Doctors with information about the patient's medical history can make precise decisions about the patient's medical condition and treatment. The ability to communicate clinical data with various healthcare facilities while maintaining confidentiality, data integrity and patient privacy are major issues that healthcare services are currently confronting [1].

Blockchain-based systems are a decentralized technology that is used in several industries Logistics, supply chain management, financial applications, and the Internet of Things are just a few examples (IoT)[2]. A secure distributed database is provided by Blockchain and queries related to the database can be resolved without the intervention of unauthorized identities. When multiple participants need to access the same database, it is extremely efficient. As a result, Blockchain when it comes to safely accessing the same database, could save a lot of time and money. HLF is a permissioned Blockchain system that makes use of CAs and MSPs to help network participants maintain trust. Healthcare systems rely on the storage and sharing of medical data. Sharing personal data across multiple parties via unprotected ways, on the other hand can result in important information being leaked. Furthermore, a lack of client control over their personal information has negative effect such as unauthorized identities being able to view and alter personal

medical information. Sharing of the patient details can lead to even more severe risks [11]. Maintaining interoperability among many involved identities is a major challenge in EHR/EMR stands for electronic health/medical data. This problem may create roadblocks in data exchange. There is a data processing and exchange systems are lacking among the identities, resulting in the Patient information is fragmented. Data privacy and security also are problems in the present techniques of storing and exchanging data through EHR/EMR systems [4], in addition to interoperability. Because of the risk of data leaking and the potential for security breaches, flaws, sharing and storing patient data has a number of risks. With smart contracts that enable certain characteristics among various identities in the system, Blockchain for healthcare can ensure the security of patients' personal and medical information. Only authorized identities can access/edit the data [21]. As a result, there is an obvious need for a distributed method of sharing and storing data in which patients can be confident in the confidentiality and privacy of their data. Additionally, the holistic view of the complete transactions and interactions is visible to all participating identities [12].

2. Literature Survey

N. Poonguzhali et al. [1] have designed architecture for the Electronic Medical Record utilising Blockchain s. They also developed a structure for the Blockchain and established a block to store the patient’s information in a decentralized health system for secure exchange. Ethereum was used to create the system. The user, the physician, and the admin are all members in the proposed model. Every member has a position to perform, such as user, physician, or admin, as well as the ability to update, add, remove, and see information. Throughput, delay, and processing time are the measures for the proposed model.

Harshini V M et al. [2] focused on Working of Blockchain. Also they have presented a framework for the Blockchain establishing a block to keep the patients' data in a decentralized health system for safe exchange and have designed a design for the EHR System using Blockchain technology. They employed the Elliptic Curve Encryption technique to assure data protection.

Shirin Hasavari and Yeong Tae Song [3] offered a method for creating a uniform, accessible, and secure data source for healthcare professionals like paramedics and ER physicians to access patient's critical clinical data for improved patient care. They created a secure and complete picture of critical medical information on the Blockchain by combining FTPS-based file transfer technologies with the hyper ledger Fabric Blockchain. Patients' clinical data may be gathered by establishing a chain of blocks that offers a consistent view of the patient's health status as they move through one clinic/medical institution to another.

Dr. B. Arunkumar et al.[4] in their survey paper have discussed in detail the impact of Blockchain in various applicable areas such as agriculture, funding , money transfer, lending and borrowing, stock market , education, healthcare, etc.

Istabraq M. Al-Joboury et al. [5] proposed to integrate Blockchain with IoT named Blockchain of Things based Fog layer for healthcare applications. This aids to remove the use of centralization of classical CC which makes the whole system crash at any failure. The proposed architecture consists of three layers: Things layer generates data from virtual wearable sensors on patients to broadcast it in peer-to-peer using Web Socket protocol, gateway layer transmits data from Things to upper layer using Wi-Fi and application layer that receives data and stores it in a Blockchain.

The methodology suggested by Bartoletti et al. [19] only allows data analytics on the Bitcoin and Ethereum platforms. The suggested technique allows relevant Blockchain data to be combined with data from other sources. The framework may also be used to arrange data in a database.

Vuckolic et al. [20] compared between proof of work based on Blockchain s and those based on

byzantine fault tolerance (BFT) in terms of scalability and performance. The paper showed that the performance of BFT based Blockchain s (such as hyper ledger) is better compared to those that are based on PoW (such as Bitcoin). On the other hand PoW based Blockchain s provide better scalability than BFT based Blockchain s.

Aniello et al. [21] presented implementation and evaluation for a two-layered Blockchain platform for a federated database. High performance and data integrity are provided by the suggested design, however scalability and data availability are lacking.

3. Methodology

Blockchain is divided into four types: public, private, consortium and hybrid Blockchains based on permission and assess.

3.1.1. Public Blockchain

It's a distributed technology that doesn't require permission [9]. Anyone with internet connection can access the public Blockchain and participate in transactions, as the name implies. This network's peers each have their own copy of the ledger. Proof of Work (PoW), Proof of Stake (PoS) and other consensus procedures are necessary to reach consensus when adding new blocks and verifying transactions. Because all peers have equal power, public Blockchain s are totally decentralized which makes them secure because no single entity has complete control over the Blockchain network. As a result, providing data security aids in the immutability of the ledger. Bitcoin, Litecoin and Ethereum are its examples.

• This Blockchain is public and open to the public and data may be accessed by anybody. Cryptocurrencies such as Bitcoin and Ethereum, for example.

• Consumers can save sensitive information and restrict access to specified individuals in both public and closed environments. Everyone can publish on this Blockchain but only certain entities have access to the reading privileges, voting for instance.

3.1.2. Private Blockchain

It is also known as permissioned Blockchain. There are limitations on who can be part of the network and who can contribute to the transactions. A private Blockchain is utilized by a firm or organization for internal purposes. Private Blockchain is centralized, meaning that just one entity controls the network. It provides transparency and security to the participants, for example hyper ledger Fabric [5].

• Private and Open: The data is accessible to all participants in the Blockchain network. For instance, take a look at a company's income statement.

• Private and Closed: The Blockchain network can only be read and written by known participants. For instance, tax returns and the Department of Defense.

3.1.3. Consortium Blockchain

In this Blockchain, more than one organization can manage the network and hence it is not fully centralized. It is used by organizations that need both public and private Blockchain functionality, for example, Quorum and Hyper ledger Fabric.[8]

3.1.4. Blockchain Hybrid

It is a hybrid Blockchain that combines private and public Blockchain applications. The peers on the Blockchain decide who gets access to which data. Some processes are kept private, while others are made available to the general public. Businesses can secure background transactions with business partners while still disclosing product details to customers via an open ledger, for instance Dragon chain [6].

To manage the medical records of patients, need to map fabric components to requirements of the EHR systems. All hospitals act as organizations in fabric network. Patient data has been treated as assets which is stored in the ledger. It is also feasible to keep the EHR data reference in the ledger but since the application is not maintained by real data, it will be

necessary to have a separate database with patient data. When combined with production or real-world hospital EHR data, this can be an excellent option. For now patient record has few fields like personal and medical details like age, address, allergies, symptoms, treatment, follow-up, etc. Patient history data will be available when a doctor is medicating a patient, which will assist doctors in assigning suitable therapy. To improve the privacy of records, it is designed to provide extra steps in application for patients. Patient can decide to have permission to access his/her data from a particular doctor. Doctor can view limited fields of assent means patient data like all medical fields along with age and allergies. Patient, on the other hand, can read all fields but only update personal ones. A comparable application method is already available in Blockchain Consensus [7], which prompted the development of this solution.

3.2 Use Cases

The system has three users with the roles of admin, patient, and doctor. Each user has its own use cases which are described in Figures 3.1, 3.2 and 3.3. Figure 3.1 is an interface for admin from every hospital to make necessary changes related to the users.

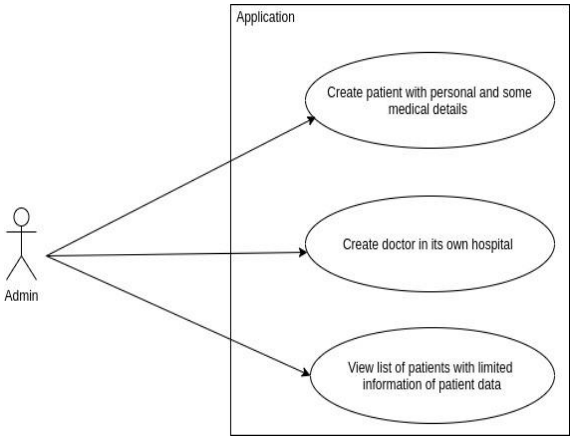

Figure 3.1: *Admin use case diagram [14]*

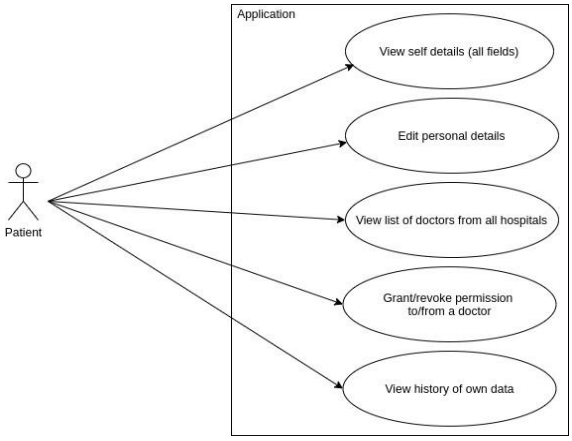

Figure 3.2: *Patient Use case diagram [14]*

3.3 Architecture

Figure 3.4 depicts the elevated architecture of a system. The architecture also shows the fabric network in detail with color schemes. The Blockchain operator sets up the network's steps required and gives the system's administrators the appropriate access and permissions [14]. All of the peers from the institutions are image hyper ledger /fabric-peer, ordered, and CA Docker containers. Because every component of the application is pluggable, the backend logic and smart contract are built in Js, and ExpressJS is used as the webserver to offer REST API. The Angular 11 framework was used to create the user interface. The communication between the front and back end is performed through REST calls with JSON web token for authentication. Backend code can also be written in Java, Go and Typescript which is officially supported languages by hyper ledger Fabric. A single channel named 'hospital channel' and two hospital organizations are adequate for the provided scenario. When the network is up and functioning, the third hospital can be added in the middle and connected with the same channel. LevelDB and CouchDB are the two databases that Fabric supports. Because CouchDB is more adaptable than LevelDB, it is utilised for the solution. Image handling is also possible. It supports indexes unlike LevelDB. Since all patient data is stored in CouchDB and does not maintain any separate EHR store, CouchDB fits well. LevelDB is a powerful in-memory database developed by Google to store

key-value pairs and in some cases, it is faster than CouchDB.

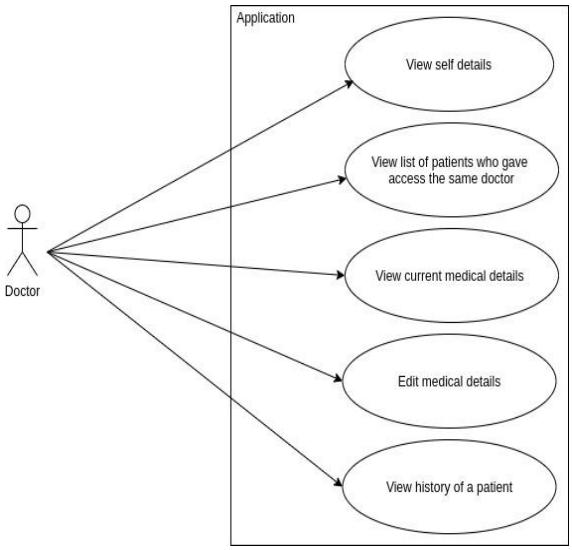

Figure 3.3: *Doctor Use case diagram [14]*

The other use case scenario where the EHR database of hospitals is used and only stores references (maybe in the form of API) to that record in LevelDB as a Blockchain ledger. Since use cases are simple here so CouchDB supports appropriately. The ledger is made up of the transaction log and the current world state. The world state is stored in CouchDB. Because of which there is no need to query the whole transaction log for every transaction request. All transactions are logged in the transaction log, starting with the first one in the genesis block.

3.3 Smart Contract & Chain code

In Hyper ledger fabric, a smart contract specifies the transaction logic that governs the lifespan of a business item in the world state [16]. Multiple smart contracts are combined into a single chain code before being deployed on a Blockchain network. In executable code, a smart contract specifies the regulations between multiple organizations. Fabric SDK invokes a smart contract to create transactions which then performs changes to the ledger. A chain code is where a smart contract is defined. Within a single chain code, many smart contracts may be established. All smart contracts included in a chain code are made available to apps once it is deployed. The application, as illustrated in Figure 3.5, consists primarily of three smart contracts packed into a single chain code. Every position (Patient, Doctor, and Admin) has its own shared ledger [13].

• AdminContract - This contract is invoked by the admin. The methods in the contract give the admin the ability to create/delete patients by adding/deleting patient object to and from the ledger. Admin can also view all the patients available throughout the network.

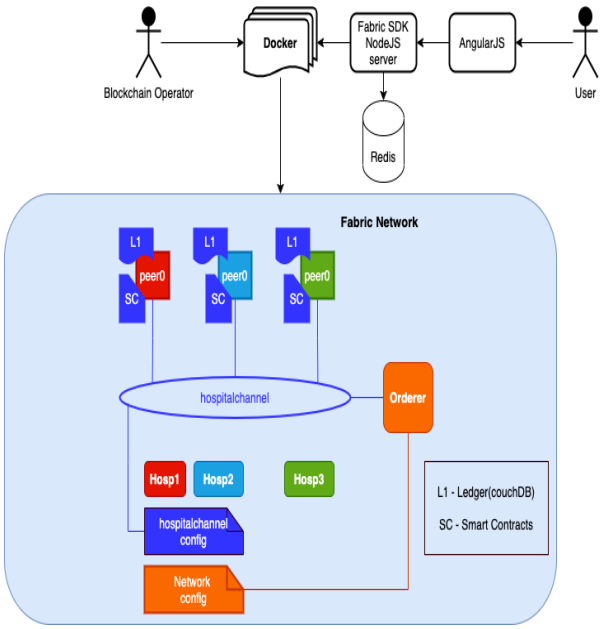

Figure 3.4: *Architecture [13]*

• PatientContract - The patient interacts with the ledger by invoking this contract. The contract contains the logic that is required for the patient. For instance, only the patient can update or view the personal details and password via the methods defined in the contract. Also patient contract contains methods to grant and revoke access to from a doctor.

• DoctorContract - The doctor contract has methods that allows the doctor to update or read the patients' medical details

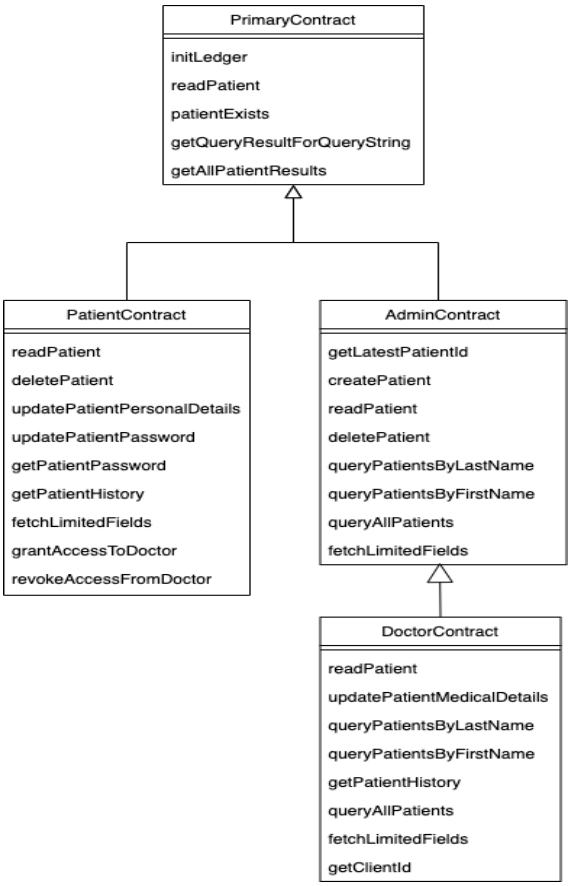

Figure 3.5: *Smart Contracts Hierarchy [13]*

4. Consensus Algorithms

Because all of the peers have equal authority, reaching an agreement is difficult. Before Bitcoin, a lot of decentralized currency systems failed because when it came to reaching a consensus, they were unable to resolve the most important problem [7].

4.1. Byzantine Generals Problem

Various army battalions' generals must decide whether to withdraw or attack. They must make a decision and establish an agreement by sending messages through messengers. There's a possibility that some of the messengers and/or generals are traitors. These traitorous generals can change the message and send a malicious response, causing the loyal generals' plan to be disrupted [10].

4.2 Consensus mechanisms

The following are the few consensus mechanisms that can be used to address the issue of the Byzantine Generals problem:

4.2.1 Proof of Work

Bitcoin uses PoW as the consensus mechanism. By solving cryptographic riddles, miners "mine" a block to connect to the Blockchain. This method necessitates a substantial amount of computation and energy. The riddles have been designed to be difficult and time-consuming for the system to solve. When a miner completes the puzzle, they send their block for verification to the network. It is fairly simple to determine if a block belongs in the chain or not. A 51 percent attack is a type of Blockchain assault in which a miner or a group of miners having more than 51 percent of the computational power prevents fresh blocks from being created and creates fraudulent transaction records in the attackers' favor [7].

4.2.2 Proof of Stake

RAFT is a distributed crash fault tolerance consensus technique that ensures that in the event of a breakdown, the system can make a decision and execute client requests. It's a log-processing consensus algorithm that works with replicated logs. Consensus in RAFT is reached through an elected leader. The server within a raft cluster is either a follower or a leader or a candidate. The leader is in charge of replicating logs with the followers [8].

4.2.3 Practical Byzantine Fault Tolerance (pBFT)

pBFT is used by Hyper ledger Fabric. It's a practical algorithm that accepts Byzantine flaws. To maintain the system stable, pBFT requires 3f+1 node, where f is the maximum number of faulty nodes the system can handle. As a result, approval from 2f+1 node is needed for the group of nodes to make any decision. Without performing complex mathematical computations (such as PoW), pBFT will achieve distributed consensus. Since they have been decided upon, the transactions do not need several confirmations. For example in Bitcoin's PoW, each node independently verifies all the transactions. Confirmations will take 10 to 60 minutes, depending on how many people are required to confirm the new block [10].

4.2.4 RAFT

All the peers have equal authority, hence it is difficult to reach consensus. Many decentralized money systems failed before Bitcoin because they couldn't establish a consensus on the most critical issue.

5. ANALYSIS AND RESULTS

5.1 Fabric SDK

APIs for interacting with the hyper ledger Fabric Blockchain are provided via the hyper ledger Fabric Client SDK. It offers APIs for interacting with smart contracts, submitting transactions to a ledger, and querying the ledger, for example [8]. The following packages are included in the Fabric SDK:

• Fabric-ca-client - Fabric-ca provides APIs for registering and enrolling participants (admin/patient/doctor) on the Blockchain network in order to create trustworthy identities. The package creates a new CA client for interacting with the CA server of the hospital to register and enroll the participants.

• Fabric-common - Wraps the common code shared by all fabric-sdk-node packages for fine-grained interactions with the Fabric network, such as sending transaction invocations. Provides APIs for monitoring events, logging and configuration settings of the environment variable, program arguments and in-memory settings.

• Fabric-network - The APIs necessary to join to the Fabric network, send transactions, query, and amend the ledger are included in this package. Provides APIs to manage the wallet which is used for managing identities and create a connection profile based on the connection profile JSON generated when CA is created.[13]

5.2 Bringing Up The Network

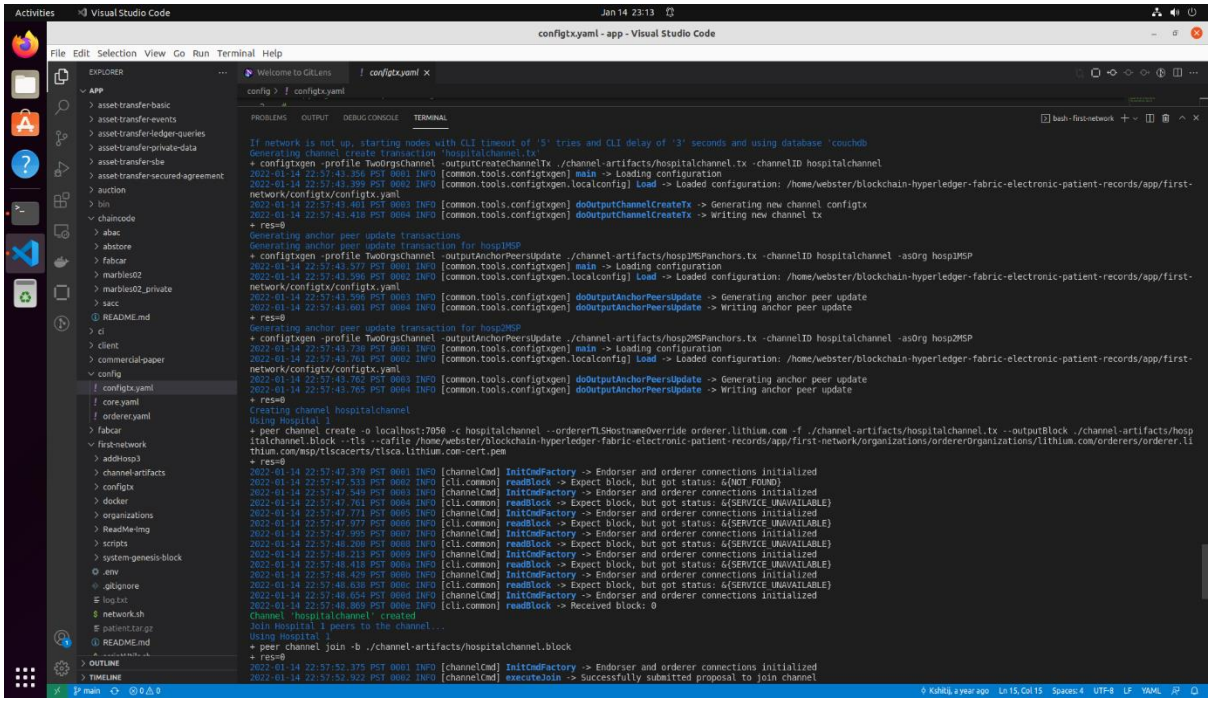

Fig.5.1 *Network start*

5.3 Creating Channel

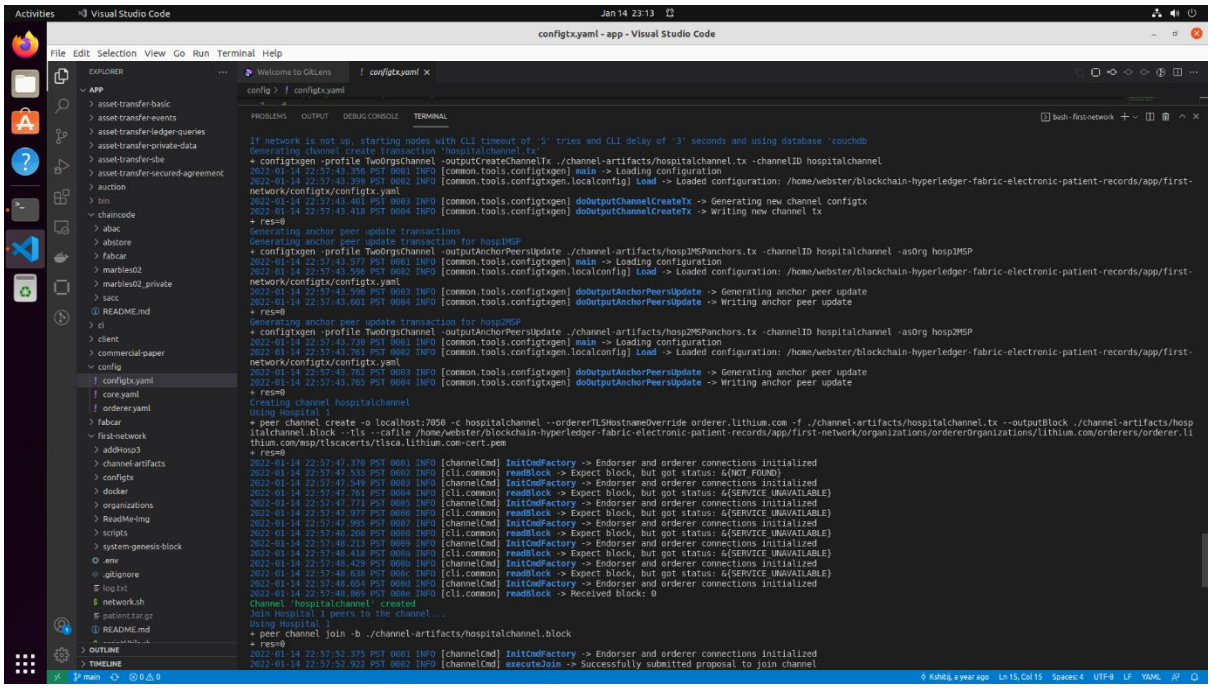

Fig 5.2 *Channel Creation*

5.4 Deploying Chain Code

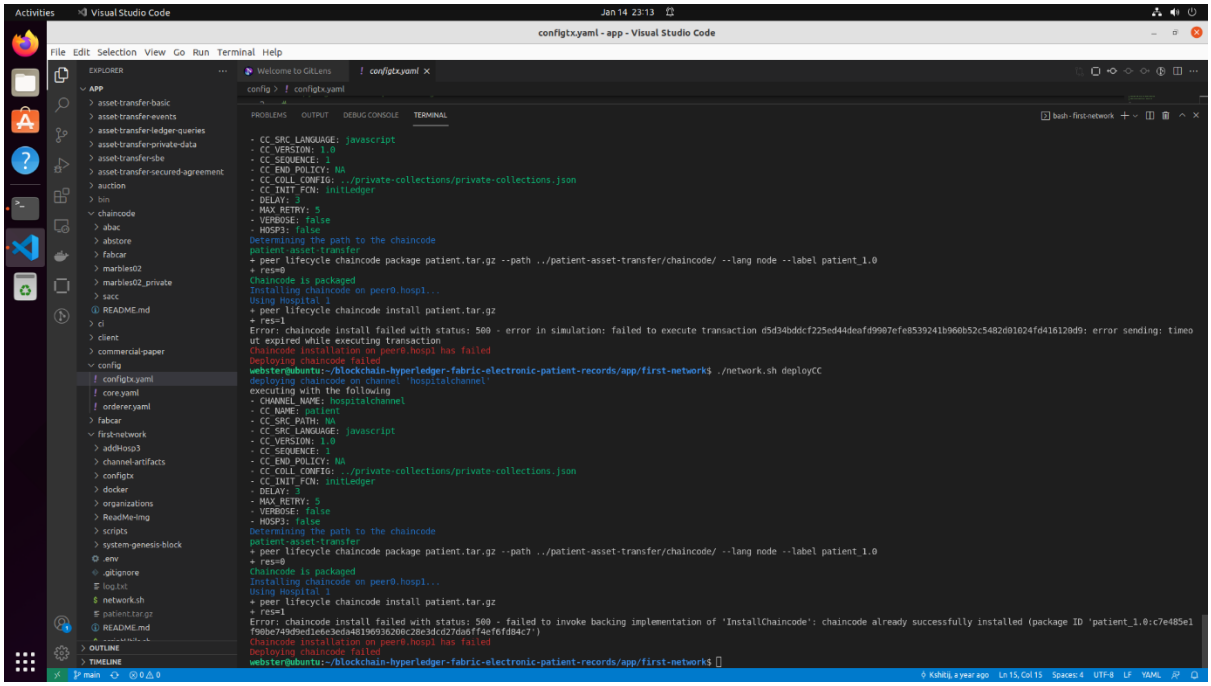

Fig 5.3 *Chain Code Deploy*

5.5 Login as an Administrator

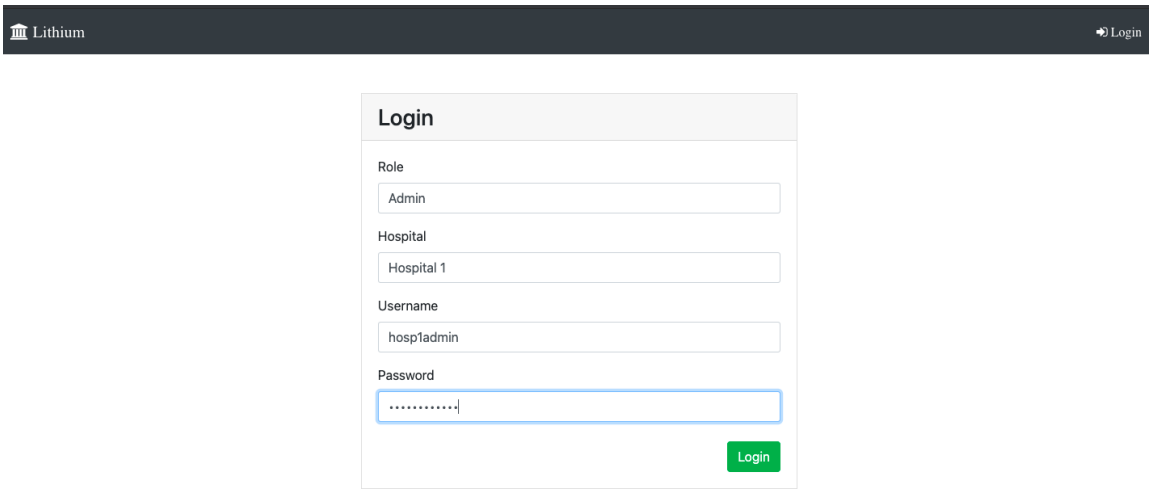

Fig. 5.4 *Admin Login screen*

5.6 Creating Patient Details and Patient Login Screen

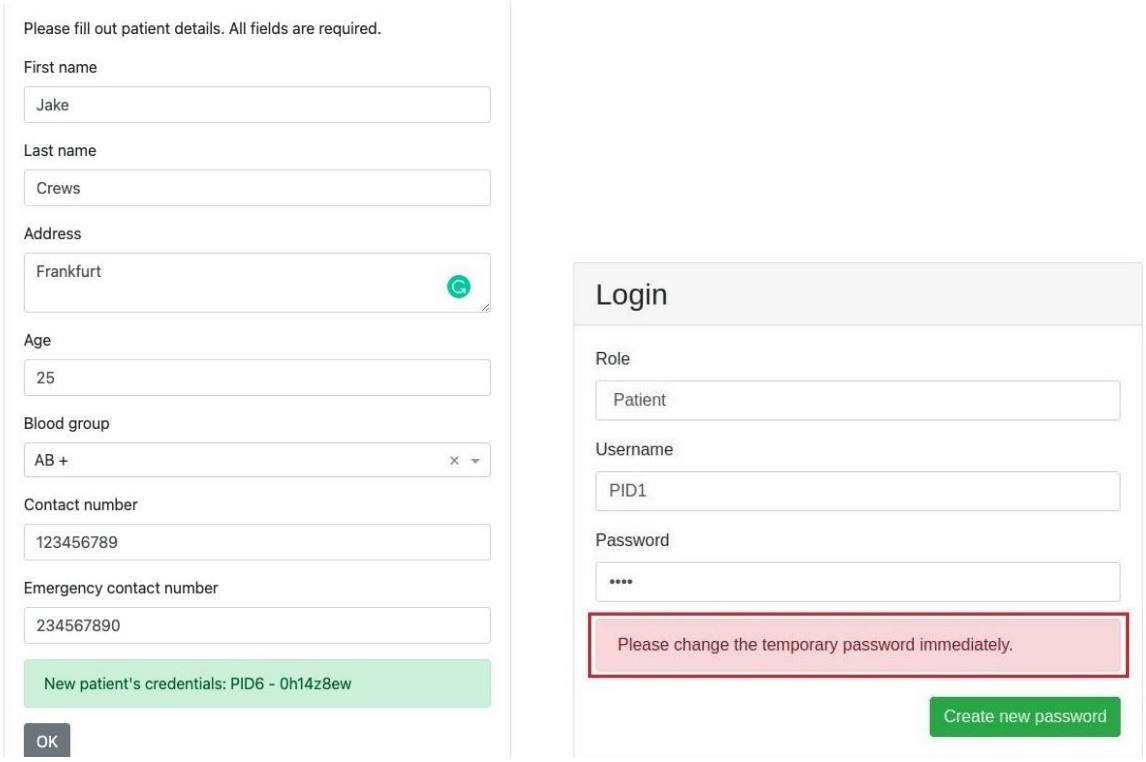

Fig. 5.5 *Creation patient details and patient login*

In package fabric-network - The main class that allows the Fabric SDK to interact with the network is the Gateway class. Once instantiated, the object creates a gateway/connection to a peer/user within the Blockchain network and enables access to the chain code and channels for which that peer/user is a member [8].

5.7 Creating Doctor Details and Login

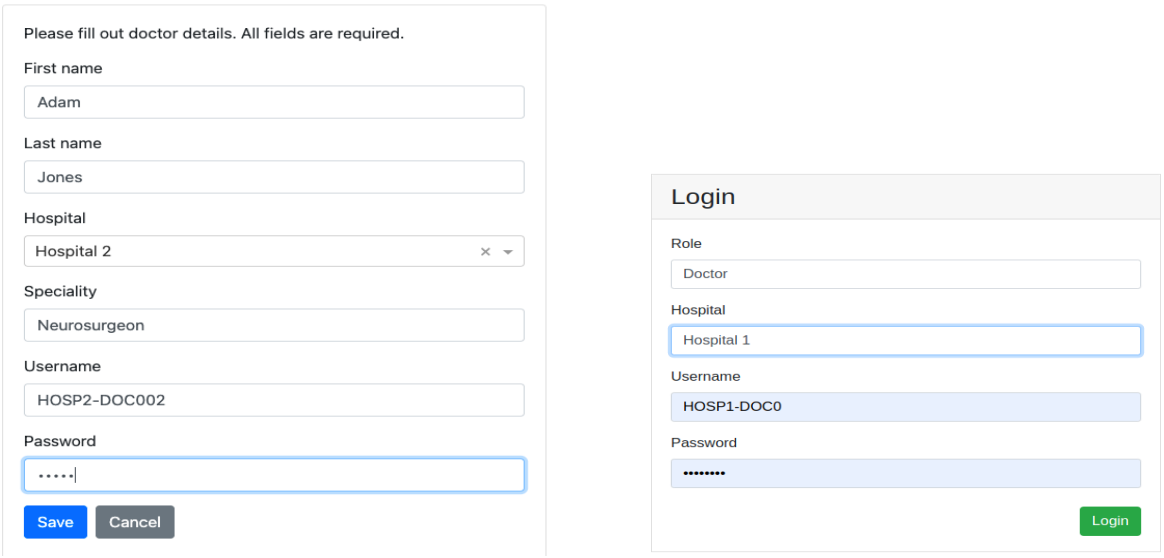

Fig. 5.6 *Creating Doctor details and login*

5.8 Performance Evaluation

By altering the number of transactions, the performance of two permissioned Blockchain systems [18]: Ethereum and Hyper ledger Fabric was compared (from 1 to 10000 transactions). Simple Electronic Health Records employ this system, which has three primary functions: Create Patient Account, Create Doctor Account, and Transactions.

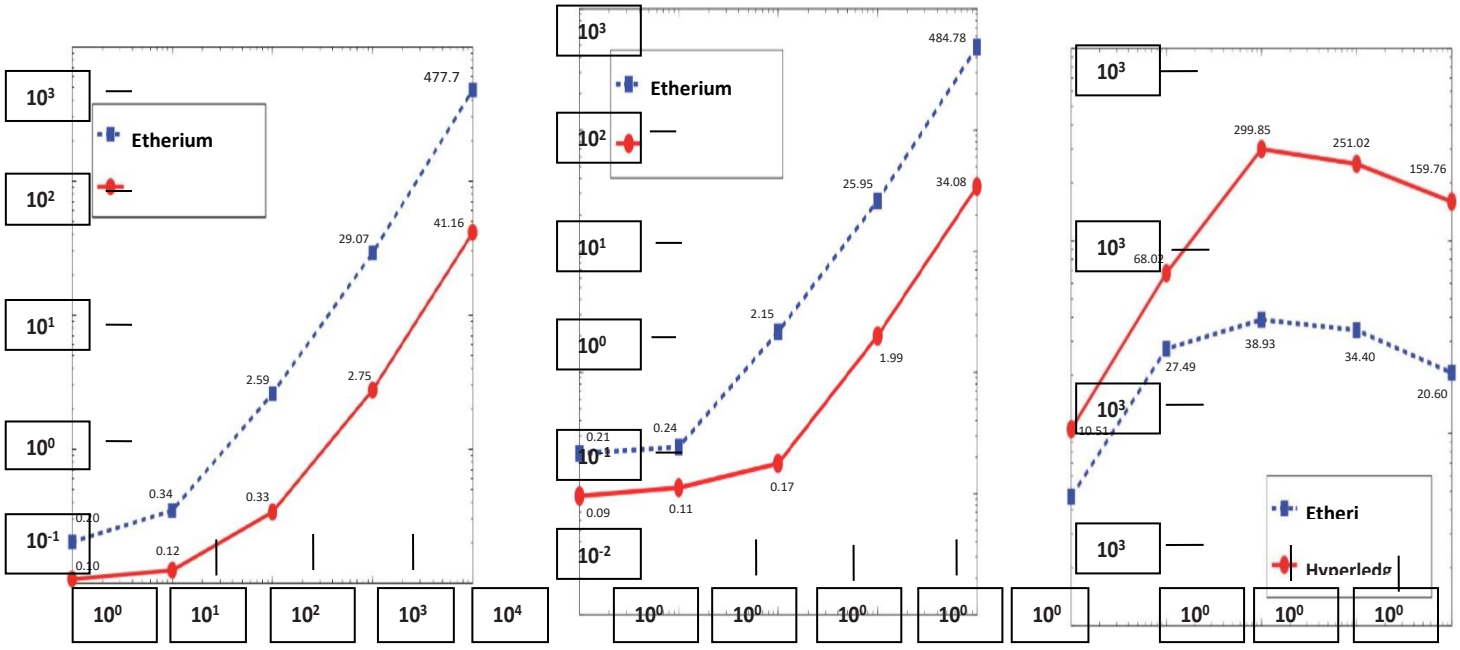

Fig 5.7: *Ethereum and Hyper ledger Fabric execution time, throughput, and latency, respectively. [18]*

According to the findings of this experiment, Hyper ledger surpasses Ethereum in all evaluation measures, including execution time, throughput, and latency, as shown in Figure 5.7.

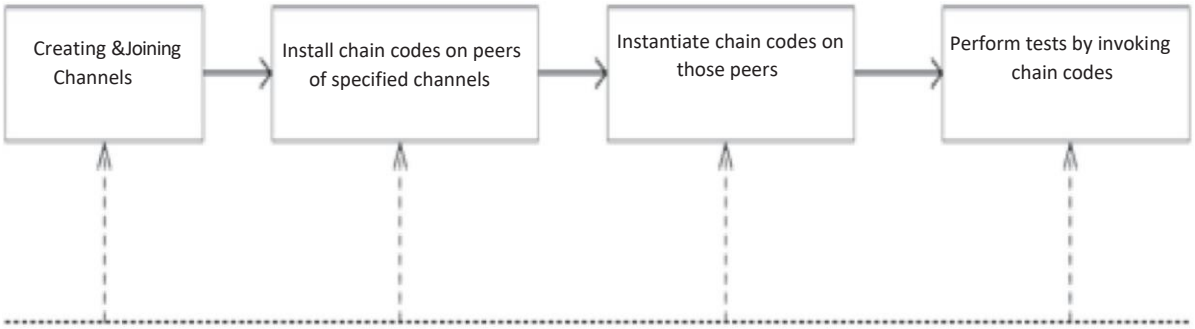

Fig 5.8: *Test flow for Fabric v1.0 [18].*

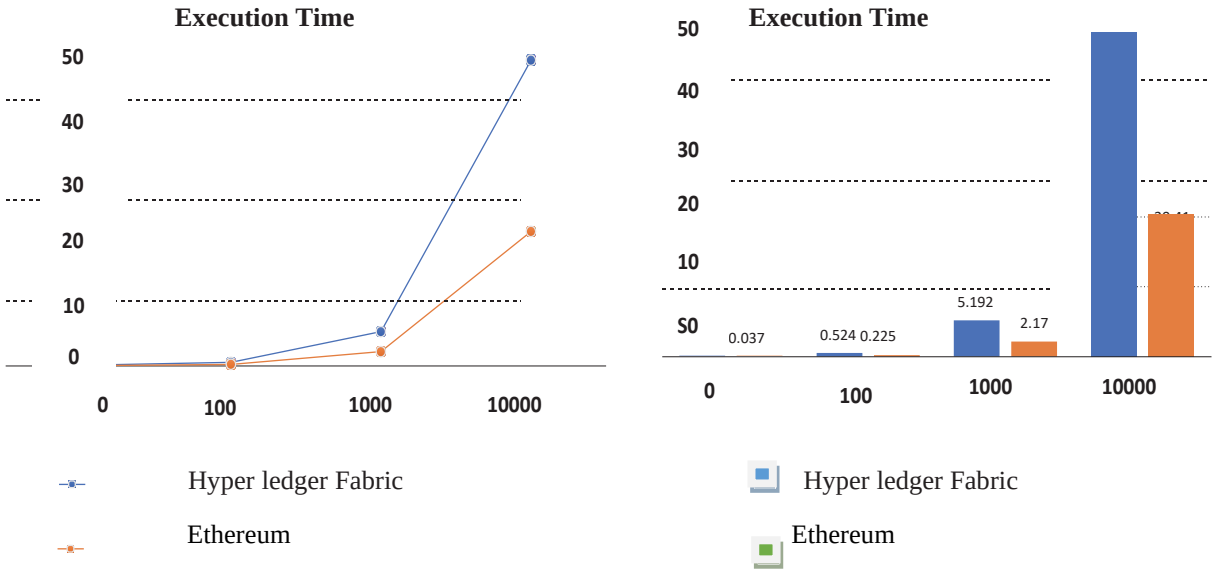

Fig 5.9: *Execution time for Fabric and Ethereum[18]*

5.9 Flow of Evaluation

The Blockchain platform under investigation determines the performance analysis test flow, with various test techniques for different Blockchain implementations. Fabric v0.6 and Fabric v1.0 test workflows are shown in Figures 5.8 and 5.9, respectively [18]. In all datasets, hyper ledger Fabric execution times are faster than Ethereum execution times, as demonstrated in Figure 5.9. As the datasets get larger, the disparity between the query execution times of both systems widens.

5.10 Considering Throughput

When the query function is executed on multiple datasets, Figure 5.10 shows the throughput of each implementation. Fabric has a better transaction throughput than Ethereum in all categories. We discovered that when the number of transactions rises, the difference in average throughputs between the two systems widens [19].

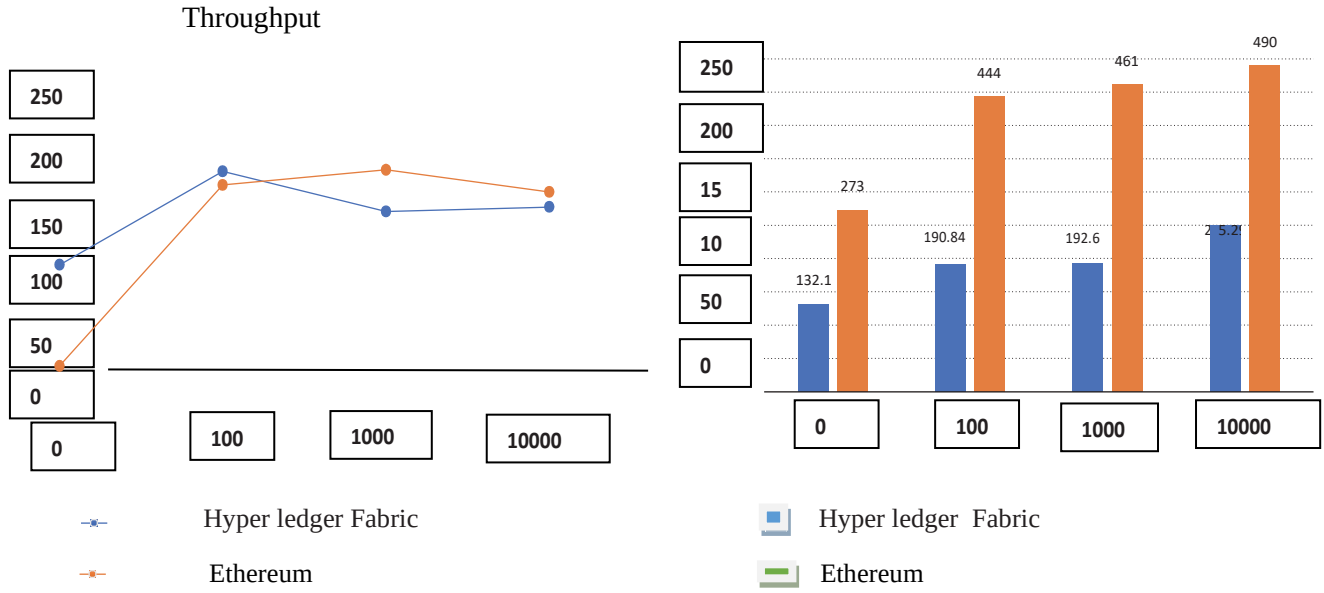

Fig 5.10: *Throughput for Ethereum and Fabric [20]*

6 Conclusion

Hyper ledger Fabric is a Blockchain framework that has a lot of potential has some concepts of policies, smart contracts and provision of secure identities which make the records secure and controlled. It enables the EHR systems to interoperable among multiple hospital organizations. Doctors can track history easily. Patients will no longer need to carry out paperwork related to medical history and digital records will vastly be adopted.

An EHR scenario comes under the private and closed Blockchain category and proposed solution can successfully conclude that it is an encouraging framework of this kind of Blockchain. It provides a reliable and secure solution in managing medical records [4].

This article also examines the performance of hyper ledger Fabric and Ethereum. Overall, the performance analysis findings show that hyper ledger Fabric routinely beats Ethereum in terms of throughput and execution time [18]. In the future, we intend to examine subsequent versions of hyper ledger Fabric and investigate further test scenarios, like as the influence of having many access points to the network's hospitals on overall performance. Furthermore, we want to compare the performance of permissioned Blockchain and public Blockchain systems to conventional databases [20].

Reference

[1] N. Poonguzhali, S. Gayathri, A. Deebika, R. Suriapriya. 2020. " A Framework for Electronic Health Record Using Blockchain Technology ". IEEE ICSCAN 2020. . https://doi.org/10.1109/ICSCAN49426.2020.9262369.

[2] Harshini V M, Shreevani Danai, Usha H R, Manjunath R Kounte. 2019. " Health Record Management through Blockchain Technology". (ICOEI 2019) https://doi.org/10.1109/ICOEI.2019.8862594

[3] Shirin Hasavari, Yeong_Tae Song. 2019. " A Secure and Scalable Data Source for Emergency Medical Care using Blockchain Technology "IEEE". https://doi.org/ 10.1109/SERA.2019.8886792.

[4] Dr.B.Arunkumar,Mr.T.Mohanraj,Mr.S.ShahulHammed, Dr.R.Santhosh. 2020. "A Stud of Blockchain Technologies and health Care Systems ".I-SMAC

https://doi.org/10.1109/ICSCAN49426.2020.9262369.

[5] Tyron Ncube, Nomusa Dlodlo and Alfredo Terzoli. 2020. "Private Blockchain Networks: A Solution for Data Privacy". IEEE Transactions on Electron Devices 59, no. 12 (december): 3273-79. DOI: 10.1109/IMITEC50163.2020.9334132.

[6] Jingkuang Liu, Lemei Yan, Dong Wang. 2021. "A Hybrid Blockchain Model for Trusted Data of Supply Chain Finance". Springer Nature 2021 (March 2021): 3273-79. https://doi.org/10.1007/s11277-021-08451-x.

[7] Amitai Porat, Avneesh Pratap, Parth Shah, and Vinit Adkar. 2012. "Blockchain Consensus: An analysis of Proof-of-Work and its applications". 2018 IEEE International Seminar on Research of Information Technology & Intelligent Systems (ISRITI 2018), Yogyakarta, 20-22 November 2019(November 2019): 3273-79. DOI:10.1109/ISRITI.2018.8864381.

[8] Omar Dib, Kei-Leo Brousmiche, Antoine Durand, Eric Thea, Elyes Ben Hamida. September 2018. "Consortium Blockchains: Overview, Applications and Challenges". International Journal on Advances in Telecommunications, vol 11 no 1 & 2, year 2018 (September): 3273-79. https://doi.org/10.1109/ted.2012.2219865.

[9] Eigelshoven, Felix, Ullrich, André, Bender, Benedict 2020. "Public Blockchain – A Systematic Literature Review on the Sustainability of Consensus Algorithms". IEEE Transactions on Electron Devices 59, no. 12 (june): 3273-79. https://doi.org/10.1109/ted.2012.2219865.

[10] Duan S., Meling H., Peisert S., & Zhang H. (2014). BChain: Byzantine Replication with High Throughput and Embedded Reconfiguration. In: Aguilera M.K., Querzoni L., & Shapiro M. (eds) Principles of Distributed Systems. OPODIS 2014. Lecture Notes in Computer Science,vol 8878, pp. 91-106. Springer, Cham. doi:10.1007/978-3-319-14472-6_(december): 3273-79. https://doi.org/10.1109/ted.2012.2219865.

[11] Elli Androulaki, Christian Cachin, Christopher Ferris, Manish Sethi, Chrysoula Stathakopoulou. Kim. 2018. "Hyper ledger Fabric: A Distributed Operating System for Permissioned Blockchain s". EuroSys '18: Proceedings of the Thirteenth EuroSys Conference, April 2018 Article No.: 30Pages 1–15 https://doi.org/10.1145/3190508.3190538.

[12] Dinh C. Nguyen1, Pubudu N. Pathirana, Ming Ding2, Aruna Seneviratne3. 2012. "Blockchain for Secure EHRs Sharing of Mobile Cloud based E-health Systems".IEEE TRANSACTIONS and JOURNALS Devices 59, no. 12 DOI 10.1109/ACCESS.2019.2917555.

[13] Adarsh Kumar, Rajalakshmi Krishnamurthi, Anand Nayyar, Kriti Sharma, Vinay Grover and Eklas Hossain. 2017. "A Novel Smart Healthcare Design, Simulation, and Implementation using Healthcare 4.0 Processes". IEEE DOI:10.1145/3152824.3152831

[14] Oluwaseyi Ajayi, Meryem Abouali, and Tarek Saadawi. 2020. "Secured Inter-Healthcare Patient Health Records Exchange Architecture". 2020 IEEE International Conference on Blockchain, https://doi.org/10.1007/s11277-021-08451-x.

[15] Muizz M. Mahdy, Khartoum, Sudan, 2020. "Semi-Centralized Blockchain Based Distributed System for Secure and Private Sharing of Electronic Health Records". 2020 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE) DOI: 10.1109/ICCCEEE49695.2021.942955

[16] Sabita Khatri, Fahad Ahmed Alzahrani, Md Tarique Jamal Ansari, Alka Agrawal, Rajeev Kumar, And Raees Ahmad Khan. 2021. "A Systematic Analysis on Blockchain Integration With Healthcare Domain: Scope and challenges".IEEE, DOI: 10.1109/ACCESS.2021.3087608

[17] Mamta, Brij B. Gupta, Senior Member, IEEE, Kuan-Ching Li, Senior Member. 2021. "Blockchain -Assisted Secure Fine-Grained Searchable Encryption for a Cloud-Based Healthcare Cyber-Physical System". CAA Journal of Automatica Sinica (Volume: 8, Issue: 12, December 2021) DOI: 10.1109/JAS.2021.1004003

[18] Qassim Nasir, Ilham A. Qasse, Manar Abu Talib, and Ali Bou Nassif1, IEEE, Kuan-

Ching Li, Senior Member. 2021." Performance Analysis of Hyper ledger Fabric Platforms". CAA Journal of Automatica Sinica (Volume: 8, Issue: 12, December 2021) https://doi.org/10.1155/2018/3976093

[19] Massimo Bartoletti, Andrea Bracciali, Stefano Lande, and Livio Pompianu. 2017. "A general framework for Blockchain analytics ". Conference: 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers, December 2017) DOI: 10.1109/JAS.2021.1004003

[20] Ahmed Afif Monrat, Olov Schelen, Karl Andersson IEEE, 2019 Kuan-Ching Li, Senior Member. 2021. " Performance Evaluation of Permissioned Blockchain Platforms". IEEE DOI:10.1145/3152824.3152831