Course code: CSE6041
Blockchain Development
J-Component Report

Title: Healthcare data management using Blockchain

Faculty: Prof. Vijaya Kumar K

Registration number: 20MCB0008

Name: Harpal Kaur Dhindsa

Abstract

Clinical history of a patient holds a significant and key job in recommending and counter the current medical conditions of a patient. Passing up a few details in history may make a colossal issue. Additionally, many time the patient may fail to remember his medicine, his tests and surprisingly the issues he confronted. Getting the information is fundamental however knowing the actuality of the information given is more significant. The specialist ought to have the certainty that the information he is taking a gander at isn't altered or mistaken.

The patient additionally should have the trust on the framework that its information will be secure and there will be no non approved admittance to it since it contains delicate clinical data. Another serious issue confronted is the refusal of a specialist endorsing a few medicine. There is a requirement for permanent history to which none of the gatherings getting to it can deny or question its legitimacy. This requirement can be fulfilled by utilizing Blockchain, to create a secure platform to store the patients data.

Literature Survey

Information security and accessibility are critical considerations for the combination and communication with Electronic Healthcare Record (EHR) systems when sharing private medical information. Taking this context into consideration context, selecting the foremost effective blockchain model for secure and trustworthy EHRs within the healthcare sector requires an accurate mechanism for evaluating the impact of various available blockchain models for its features. The authors in [1] present a study employing a scientifically proven approach for evaluating the impact of blockchain technology and provide an unique idea. As a part of the research analysis they garnered the feedback of 56 domain experts within the healthcare management for assessing the impact of various blockchain models. To dispose of the ambiguities that emerged due to various assessments of those specialists and for the externalization and association of information about the decision setting of the blockchain model, the investigation utilized a decision model. Fuzzy Analytic Analytical Network Process (F-ANP) method was accustomed calculate the weights of the standards also because the Fuzzy-Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) technique was accustomed evaluate the effect of different solutions. Further, the results obtained through this empirical investigation could be an instrumental reference for selecting the foremost appropriate Blockchain model for maintaining breach-free EHRs.

Personal Healthcare record stored in a healthcare institution remain in depository which isn't easily shared with other institutions thanks to technical and infrastructure related restrictions. In such some way, if a patient needs to visit distinct institutions/hospitals or physicians, there is no effective and privacy-preserving data sharing mechanism. Blockchain provides a shared, immutable and transparent history of all the transactions to create systems with trusty and decentralized environment. This provides a chance to develop a secure and trusty personal healthcare record data management system by blockchain technology. In [2] an answer was introduced focusing on the patient's control by holding the information on the encryption/decryption key which might be reasoned

from the past exchange in blockchain. In such the simplest way, a patient can control the private healthcare record by controlling key usage.

The authors in [3] this paper examine the state of the research in the field of blockchain implementation and integration in healthcare. Their primary contribution is an up-to-date classification of current research papers in the field of blockchain technology in Healthcare. They also identified understudied research areas, potential areas for future research work.

It is very challenging to create a robust AI model and use it in a real-time and real-world environment since most organizations don't want to share their data with other third parties because of privacy concerns, furthermore it's difficult to create a generalized prediction model thanks to the fragmented nature of the patient data across the healthcare system. to unravel the above problem, the authors in [4] present a solution supported blockchain and AI technologies. The blockchain will securely protect the information access and AI-based federated learning for building a sturdy model for global and real-time usage.

In medical services climate, IoT carries more comfort to specialists, attendants and patients. it's going to be more efficient for monitoring the illness patients and diagnosing very effective with reducing the worth. There are different security penetrates and dangerous attacks in medical care framework which are very weak like fraud, privacy leakage and so on. The aim of the authors in [5] is to simply investigate how Blockchain would improve the healthcare environment within the IoT context. It also amalgamates the potential of blockchain technology as a promising security measure, highlights potential challenges within the healthcare domain, and provides an analysis of varied blockchain based security solutions.

Technology does not stand still. Current advances are being presented in all circles of our life, including the medical care framework. The authors in [6] have examined the prospects for introducing 5G technology and blockchain into the healthcare system. From a technical point of view, they analyzed the key weak points in the healthcare system, analyzed the capabilities and advantages of 5G, blockchain and related technologies,

considered the benefits of their integration with the healthcare system. Based on the results obtained, they proposed a blockchain-based 5G healthcare architecture.

It has been demonstrated that blockchain applications are being used in medical care to convey secure information and to deal with the clinical information securely. Additionally, blockchain is changing the conventional clinical practices in successful manners, for example, diagnosing the issues adequately and treating through secure data sharing. The authors in [7] focus on security of healthcare applications, due to Covid-19, it has become challenging for healthcare officials and government to protect and record individuals sensitive data safely. Additionally, spread of deluding data has been likewise expanded during the pandemic and failure of existing stage for data approval prompts public frenzy. Execution of blockchain-based global positioning frameworks, substantial data dividing between individuals and Government. They have focused on information security issues raised by Covid-19 pandemic as well as implementation of blockchain-based platform in healthcare to record and protect covid-19 related information and contact tracing.

The authors in [8] have shown worry towards the area of Smart Healthcare, which has developed to a much prosperity in regards to the effective method of serving and directing clinical medical care to the patients with the purpose in keeping up with security of the patients' information and furthermore the way toward spreading out continuous precise and confided in information to the clinical experts. Yet, in the situation of Smart Healthcare, the essential concern emerges in the reality of privacy and security of the information of the patients because of the interoperability of different partners all the while. Hence, this concern of protection and furthermore relief of the precise information has been managed in the work by directing, checking and detecting worldview with agreement to the IoT and the Blockchain as an exchange and accessing executives framework and furthermore a proper mechanism for spreading out exact and confided in information for presenting with intentional clinical consideration and advantages to the patients.

The amount of healthcare data is increasing. Nonetheless, issues with unstandardized information designs and the unwavering quality of provenance make the data challenging to impart to different foundations. The authors in [9] propose a standards-based sharing framework, SHAREChain, which incorporates two features to deal with reliability and interoperability issues. To start with, it further develops unwavering quality by utilizing the information trustworthiness of a Blockchain-vault and comprises a Consortium Blockchain Network to share information exclusively between confirmed establishments. The subsequent element further develops interoperability with principles identifying with medical care information sharing: Fast Healthcare Interoperability Resources and Cross-Enterprise Document Sharing. They introduced blockchain and standards (FHIR and XDS) to solve these problems. Blockchain has a grip on this matter because it handles data so that it is consistent, timestamped, transparent, and immutable. Besides, they adopted the FHIR to solve interoperability issues. For example, the CDA is a standardized format, but the data is comparatively static, and it takes a specific work to obtain the information and make it available in any other format. FHIR rises above this document-based environment, staying away from traps of archive based trade, which regularly require separate information access.

In medical services applications, patient information are generally put away in the cloud, which makes it hard for the clients to have sufficient authority over their information. In any case, because of the General Data Protection Regulation (GDPR), it is the information subject's on the right track to know where and how his information has been put away, who can get to his information and to what extent. The authors in [10] have proposed a blockchain-based design for e-wellbeing applications which gives a productive protection safeguarding access control system. They have taken the benefit of Blockchain (BC) extraordinary highlights, i.e., permanence and secrecy of clients, while changing the exemplary blockchain structure to conquer its difficulties in IoT applications (i.e., low throughput, high overhead and idleness). They bunched the miners of BC, store and interaction information at the closest cluster to the patient.

To work on the exactness of conclusion and the viability of clinical treatment, a structure of Parallel Healthcare Systems (PHSs) in view of the counterfeit frameworks along with computational tests and parallel execution (ACP) approach is proposed by the authors in [11]. PHS utilizes counterfeit medical care frameworks to show and address patients' conditions, finding, and therapy measure, then, at that point applies computational analyses to break down and assess different restorative regimens, and carries out equal execution for dynamic help and continuous advancement in both real and fake medical services measures. Also, they join the arising blockchain innovation with PHS, through developing a consortium blockchain connecting patients, emergency clinics, wellbeing agencies, and medical care networks for far reaching medical services information sharing, clinical records survey, and care auditability. Finally, a model named parallel gout diagnosis and treatment framework is assembled and conveyed to check and show the adequacy and effectiveness of the blockchain-controlled PHS structure.

Experimental results

Medical Database while implementing Blockchain technology that can be accessed from wherever it is needed while still being secure and free from any sort of attempted fraudulence.

The main objective is to create a secure, user-friendly and appealing UI which could be accessed by the patient and the doctors at the hospital.

Many times, the patient forgets the medications he was given or even some problem he had in the past. So, this blockchain will have the data to overcome that problem. Also, sometimes patient does not want to reveal some information regarding health but hiding any of such details from a doctor may create a problem.

Tools used:

Ganache, Truffle, IPFS, React, and MetaMask.

Ganache: Ganache is an individual blockchain for quick Ethereum and Corda dispersed application development. It tends to be utilized across the whole development cycle; empowering to create, convey, and test the dApps in a protected and deterministic climate.

IPFS: IPFS represents Interplanetary File System. IPFS tries to make a lasting and conveyed web. It does this by utilizing a content tended to framework rather than HTTP's area based framework. Rather than utilizing an area address, IPFS utilizes a portrayal of the actual content to address the content. This is finished utilizing a cryptographic hash on a record and that is utilized as the location. The hash addresses a root object and different articles can be found in its way. This way the framework use actual nearness. IPFS interfaces every one of these diverse blockchains in a manner that is like how the web associates these load of sites together. The same way that you can drop a connection on one page that connects to another page, you can drop a connection in ethereum [for example] that connects to zcash and IPFS can resolve the entirety of that.

MetaMask: It is a browser extension that allows one to run dApps without being included in the Ethereum network as an Ethereum Node. All things considered, it allows one to associate with another Ethereum Node called INFURA and run shrewd agreements on that Node. MetaMask deals with a customized Ethereum wallet, which contains Ethers (or cash), and permits to send and get Ethers through a dApp of premium.

Overview:

- Blockchain works over various nodes in a distributed environment and are also in sync with each other. New nodes can also register and contribute over the blockchain. On registration they get the latest information and are also part of the distributed system. 3rd party applications can request any service of the blockchain from any of the nodes in the network.
- The reliability of the data is also high since the system is distributed.

- Functionalities provided by blockchain:
    - Save the entry.
    - Mine a block.
    - Access a block.
    - Access history of a patient or doctor.
- The project stores patient records on blockchain(hybrid). Hybrid since records are not put away on blockchain, however access data is put away on blockchain. There will be two members doctor and patient.
    - Doctor register by giving name.
    - Patient register by giving name and age.
    - Patient transfers records and gives irregular nounce to encode the document, record will be transferred to IPFS and mystery is put away in Ethereum.
    - Patient gives admittance to specific specialist.
    - Once doctor is given admittance by understanding, he will actually want to see patient's address in his landing page.
    - Doctor can get all records ipfs hash of patient and send solicitation to node application for viewing the document.
    - Node application will get document from ipfs and get secret from blockchain, unscramble record and send it to specialist.

Block diagrams:

Use Case diagram:

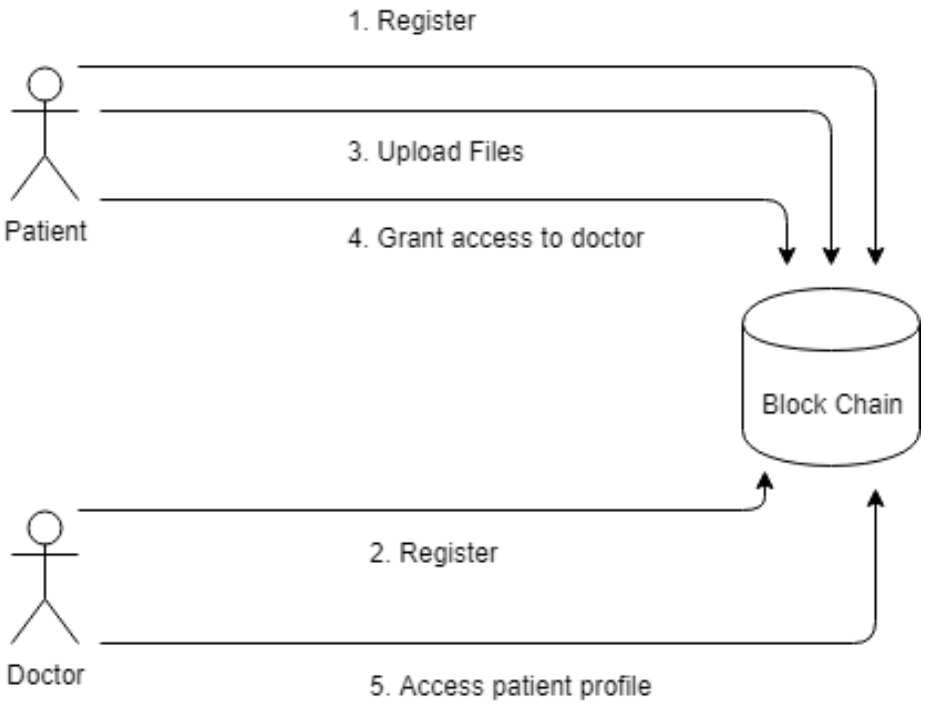

Figure 1. Use Case Diagram

The patient and doctor have an option to register for new users, and login option for the previous users. The patient has an option to upload the files, and it is the patients decision to grant access to doctor through the blockchain platform. Once granted access the doctor can access the patient's profile. This sets a patient centric boundary when concerned with privacy.

Upload files:

Here we have two layer of safety

1. hash given by ipfs(ie. records can be accessed only if document hash is known)

2. file transferred to ipfs is scrambled by secret (anyway secret isn't encoded in ethereum, ought to be done in future)

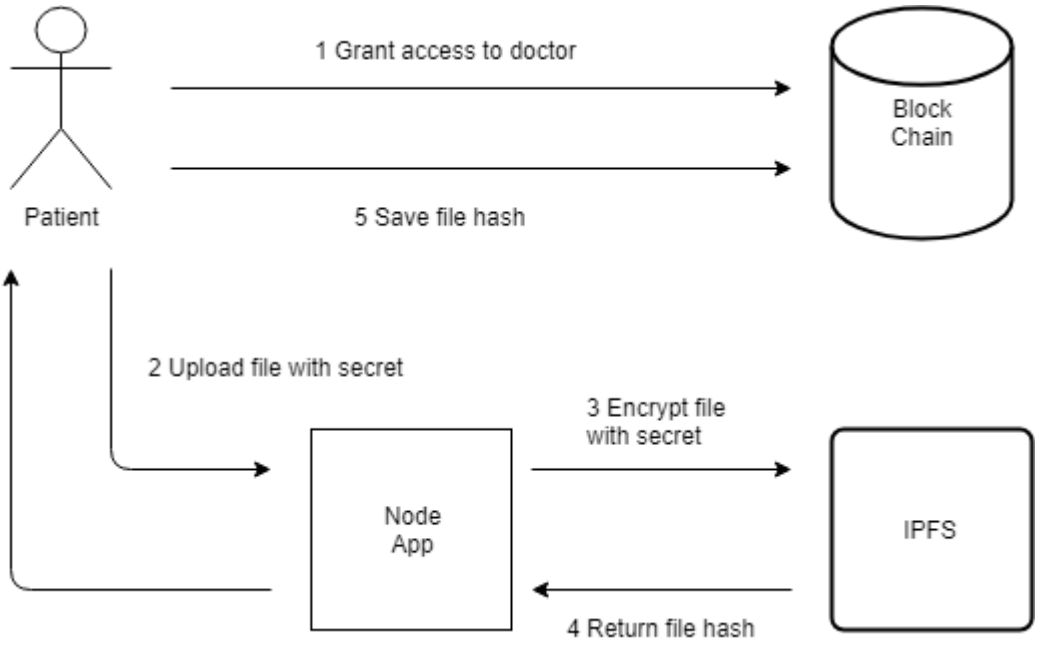

Figure 2. Upload files

Access files:

For the doctor to be able to access the patient's files.

1. The doctor has to request the patient list to the blockchain
2. The patient file list is provided to the doctor
3. The doctor then can send the file hash via the Node App
4. Hence, making a request secret to the blockchain
5. The blockchain on receiving the request provides the secret
6. The Node App gets the file on decrypting the key
7. And the doctor is able to access the file on the Node App

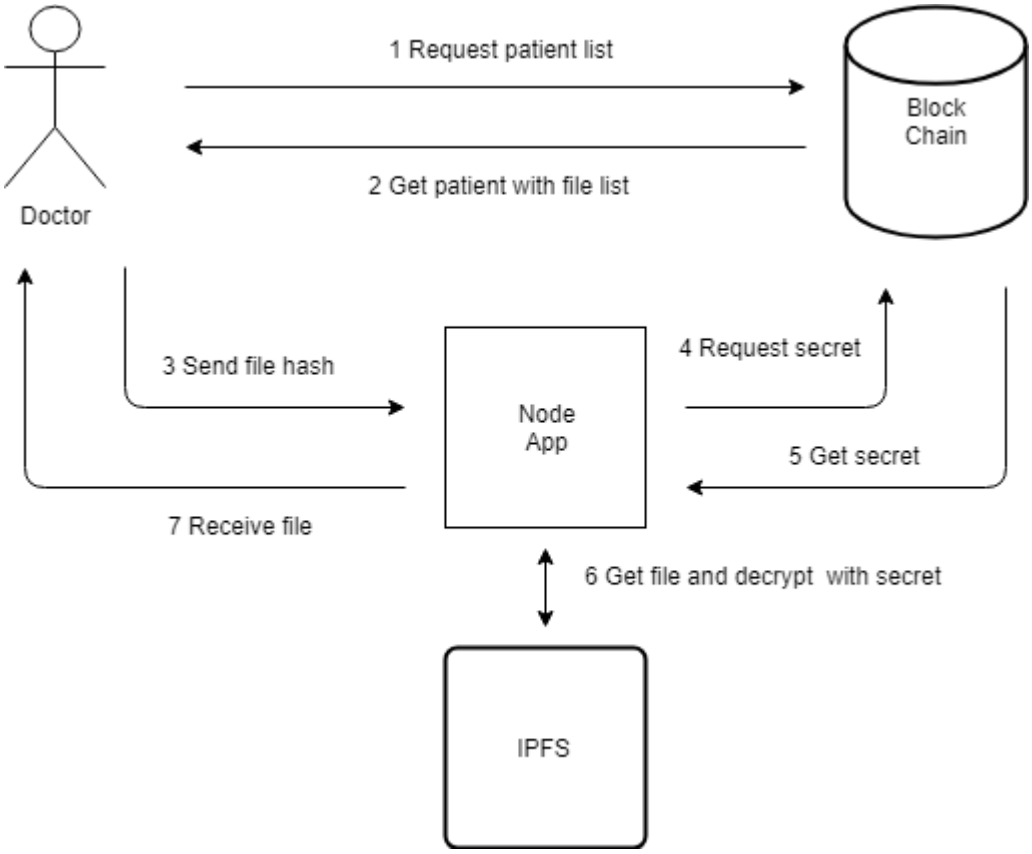

Figure 3. Access Files

Output

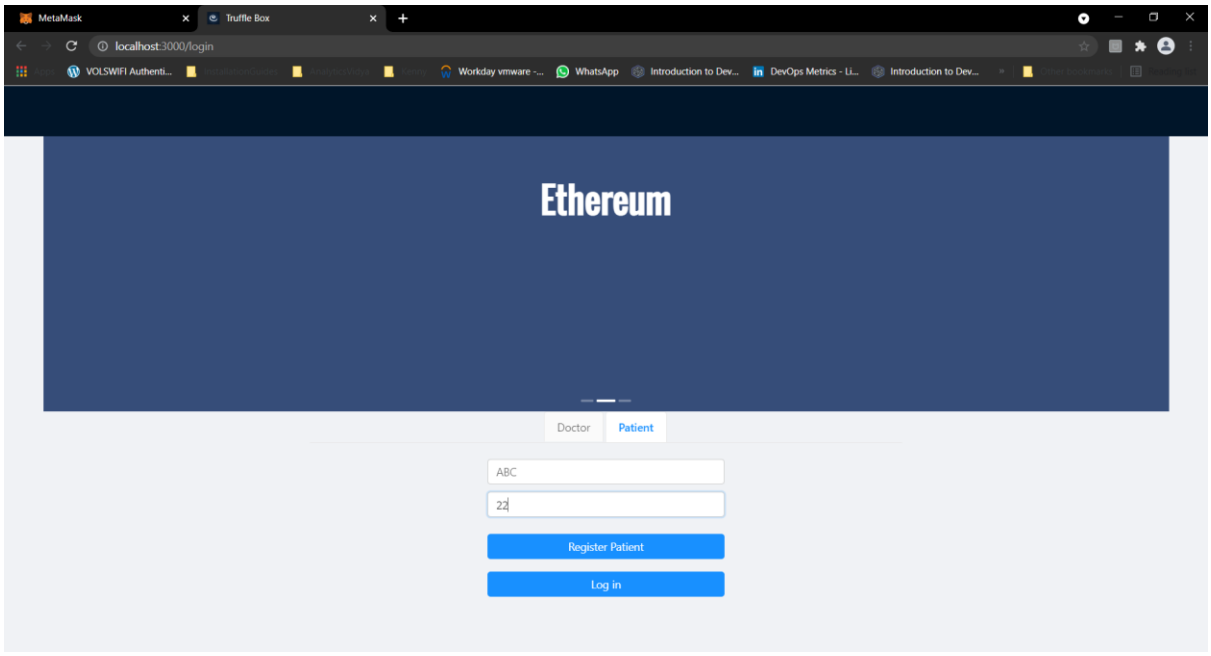

Figure 4. Home page for Patient

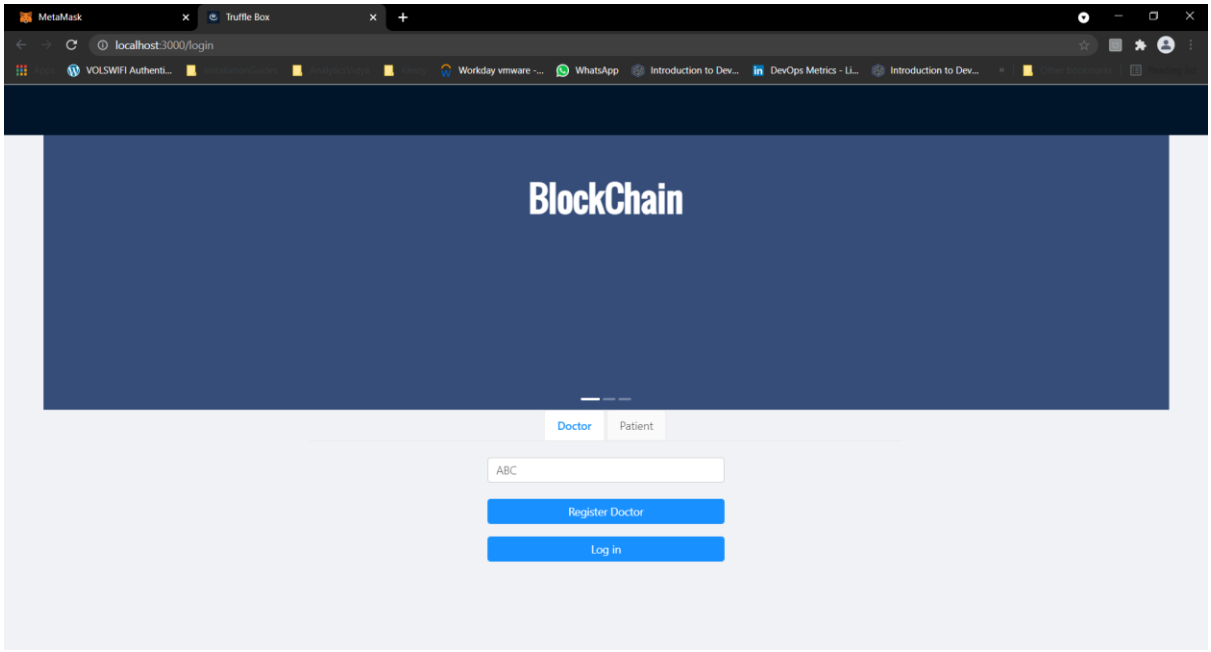

Figure 5. Home page for Doctor

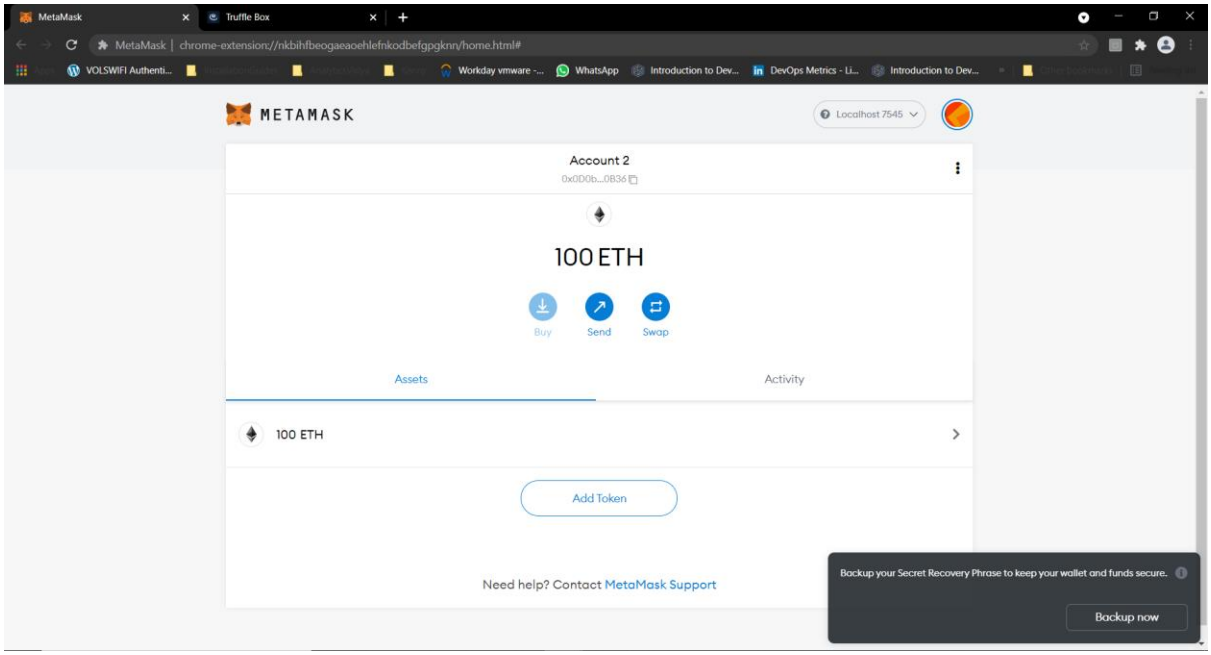

Figure 6. Ethereum account imported from Ganache in Metamask

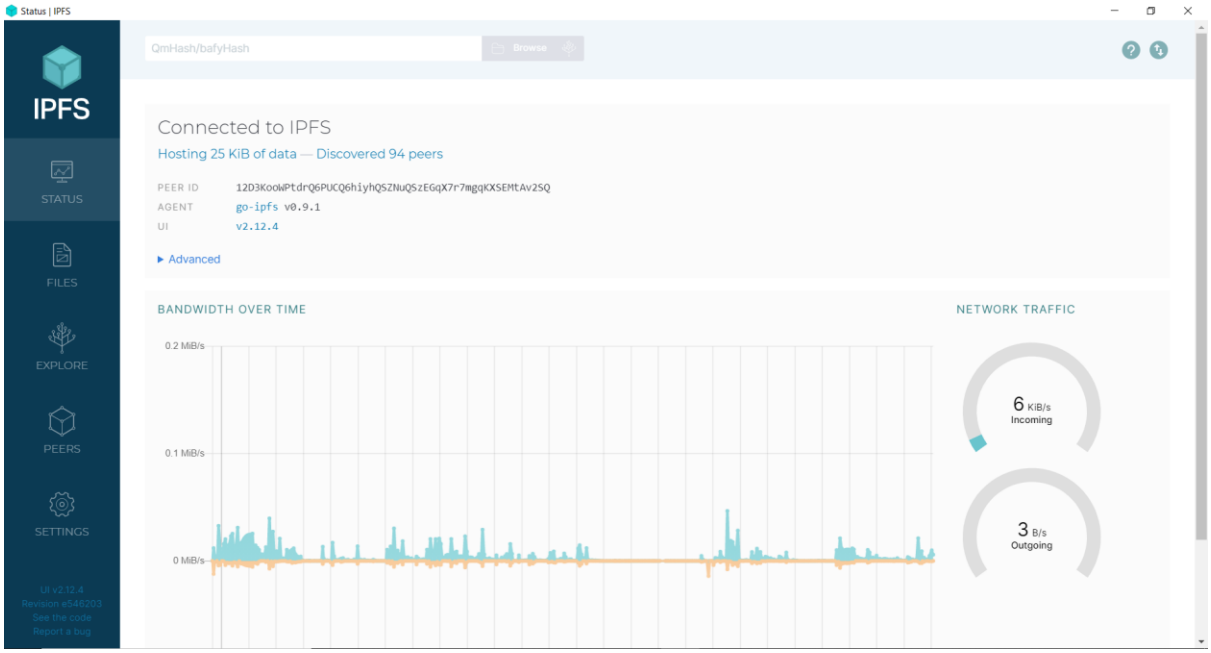

Figure 7. IPFS status

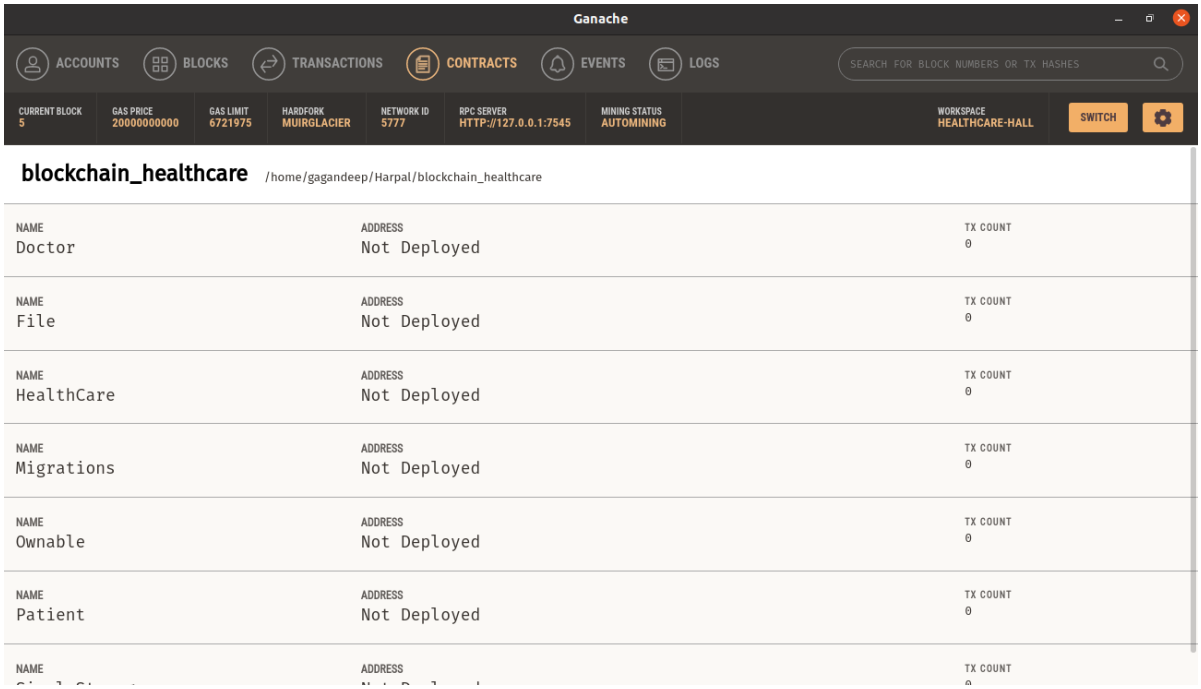

Figure 8. Contract Status in Ganache Workspace

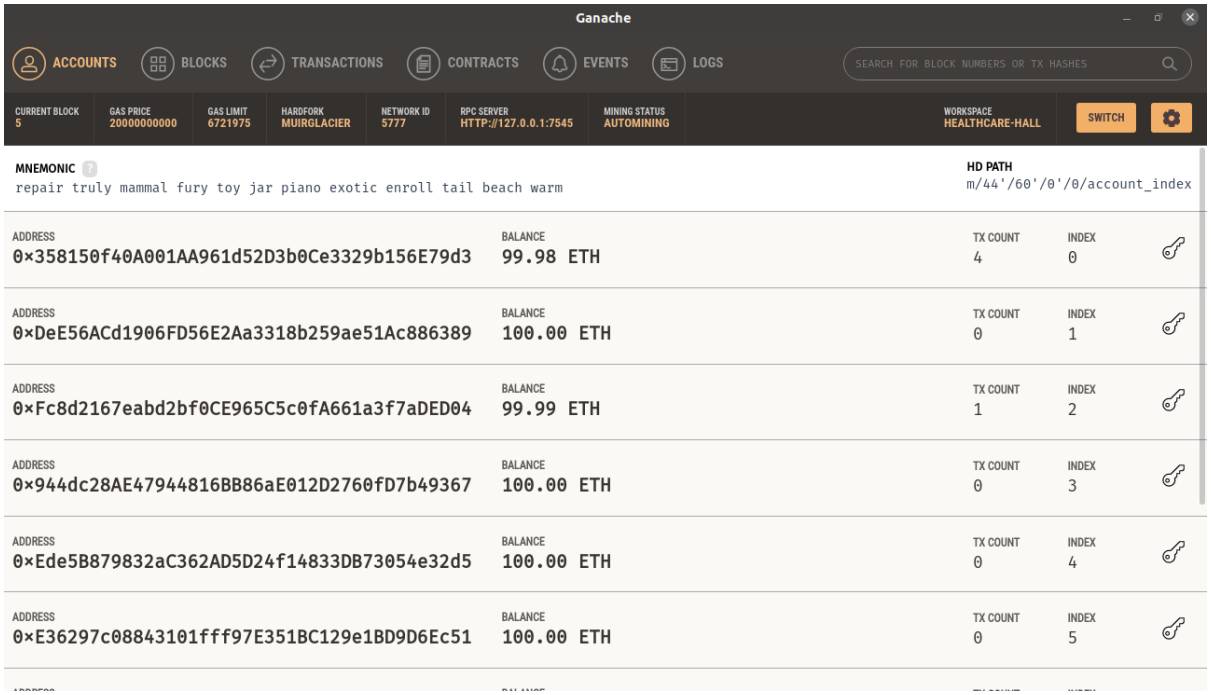

Figure 9. Accounts Status in Ganache

Conclusion

From the project we have demonstrated the use of blockchain to store data so that its integrity and authenticity is maintained along with non-repudiation of the sources providing data.

Since core medical data is stored on all the distributed nodes of the network, availability of the data is also high. And the application shows to be patient centric as the control over distributing the data is with the patient. And the data is being shared over secured links.

References

Bibliography

[1] M. T. J. A. M. A. A. K. S. M. F. A. A. R. K. R. A. K. Mohammad Zarour, "Evaluating the Impact of Blockchain Models for Secure and Trustworthy Electronic Healthcare Records," *IEEE Acces,* 2020.

[2] T.-H. C. Ting-Le Zhu, "A Patient-centric Key Management Protocol for Healthcare Information System based on Blockchain," *IEEE Conference on Dependable and Secure Computing (DSC),* 2021.

[3] G. P. C. William Bodeis, "Blockchain Adoption, Implementation and Integration in Healthcare Application Systems," *IEEE,* 2021.

[4] N. K. S. S. K. M. A. Y. R. C. M.-I. J. H.-C. K. Satyabrata Aich, "Protecting Personal Healthcare Record Using Blockchain and Federated Learning Technologies," *International Coference on Advanced Communications Technology (ICACT),* 2021.

[5] S. K. A.Yogeshwar, "Healthcare Domain in IoT with Blockchain Based Security- A Researcher's Perspectives," *Proceedings of the Fifth International Conference on Intelligent Computing and Control Systems (ICICCS),* 2021.

[6] E. R. N. A. D. K. Khalimjon Khujamatov, "Blockchain for 5G Healthcare architecture," *International Conference on Information Science and Communications Technologies (ICISCT),* 2020.

[7] M. M. M. H. Mansukhdeep Kaur, "Post study of Blockchain in smart health environment," *5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA),* 2021.

[8] S. A. H.-C. K. Sabyasachi Chakraborty, "A Secure Healthcare System Design Framework using Blockchain Technology," *International Conference on Advanced Communications Technology(ICACT),* 2019.

[9] M. G. K. I. K. K. Ah Ra Lee, "SHAREChain: Healthcare data sharing framework using Blockchain-registry and FHIR," *IEEE International Conference on Bioinformatics and Biomedicine (BIBM),* 2019.

[10] M. E. E. T. D. A. K. Koosha Mohammad Hossein, "Blockchain-Based Privacy-Preserving Healthcare Architecture," *IEEE Canadian Conference of Electrical and Computer Engineering (CCECE),* 2019.

[11] J. W. X. W. T. Q. Y. Y. L. O. Y. G. a. F.-Y. W. Shuai Wang, "Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach," *IEEE TRANSACTIONS ON COMPUTATIONAL SOCIAL SYSTEMS,* 2018.