Department of Computer Engineering

A **BLOCKCHAIN TECHNOLOGY**

PROJECT REPORT ON

BLOCKCHAIN FOR HEALTH RELATED MEDICAL RECORDS

SUBMITTED TO THE DEPARTMENT OF COMPUTER
ENGINEERINGAISSMS IOIT

BE Computer Engineering

SUBMITTED BY

STUDENT NAME	**ERP No:**
Onasvee Banarse	**09**
Kaustubh Kabra	**37**
Akash Mete	**50**
Harsh Shah	**65**

2022 -2023

AISSMS
INSTITUTE OF INFORMATION TECHNOLOGY
ADDING VALUE TO ENGINEERING

Department of Computer Engineering

CERTIFICATE

This is to certify that the project report

“BLOCKCHAIN FOR HEALTH RELATED MEDICAL RECORDS”

Submitted by

STUDENT NAME	ERP No:
Onasvee Banarse	09
Kaustubh Kabra	37
Akash Mete	50
Harsh Shah	65

is a bonafide students at this institute and the work has been carried out by them under the supervision of **Prof. Prashant Sadaphule** and it is approved for the partial fulfillment of the Department of Computer Engineering AISSMS IOIT.

(**Prof. Prashant Sadaphule**) (**Dr. S.N.Zaware**)

Mini-Project Guide Head of Computer Department

Place: Pune Date:

Abstract

The blockchain technology (BT) offers great potential to foster various sectors with its unique combination of characteristics, for example, decentralization, immutability, and transparency. We see promising possibilities in the use of this technology for science and academia. In this paper, we want to show why the BT suits specially to open sciences and medical fields. A blockchain-based system for medical records that can be linked into existing electronic medical record software and act as an overarching, single view of a patient’s record.

Patient can grant or revoke data access permission to/from any doctor. Patients can also add files to their profile/data like reports, X-rays etc. which will be stored over IPFS. Doctors are provided with facility to view the patient records to which they have access granted. Doctors can view their patients' files and previous consultations too and can accordingly provide consultation or treatment.

The major issues of security and functioning of medical records documentation has been solved by using the Blockchain Technology and developed a running website that provides with a demonstration of the same.

Contents

1. Introduction

The aim of this framework is firstly to implement blockchain technology for EHR and secondly to provide secure storage of electronic records by defining granular access rules for the users of the proposed framework. Moreover, this framework also discusses the scalability problem faced by the blockchain technology in general via use of off-chain storage of the records. This framework provides the EHR system with the benefits of having a scalable, secure and integral blockchain-based solution.

This project is developed with the aim to store patient healthcare records over blockchain. The DApp build provides a patient centric system in which patient has control over his data i.e. patient themselves decide who can view their profiles/data. The system classifies the users into two categories: Doctor and Patient.

In this scenario, every time there is an amendment to a patient record, and every time the patient consents to share part of their medical record, it is logged on the blockchain as a transaction. Medicalchain is a leading example of a company working with healthcare providers to implement blockchain enabled EMRs.

For this work, the given implementations are all in HTML, CSS and JAVASCRIPT, and have been thoroughly tested and analysed. However, it needs to be emphasised that focus does not lay on optimization for the given implementations. Instead, the implementations show what is possible in terms of increasing performance, through the results and analysis of this work.

2. Problem Statement

Develop a Blockchain based application for health related medical records

In this Project we will focus on following questions:

- Can Blockchain help improve any fields related to Healthcare?
- If yes, then what are the key aspects and roles Blockchain technology will play in this field?
- What are the key features and advantages does this application provide over traditional methods?
- What are the current requirements for a technical open science infrastructure, and how do they compare with BT features?
- What is the current status and perspectives for the use of BT in science and academia?
- What are the biggest challenges and obstacles that are preventing successful implementation and adoption of BT as supporting infrastructure for open science?

3. Software Requirement Specification

Software Used:

- **Ganache**
    - Ganache is used for setting up a personal Ethereum Blockchain for testing your Solidity contracts. It provides more features when compared to Remix. You will learn about the features when you work out with Ganache.

- **IPFS Desktop**
    - IPFS Desktop is built using the Electron framework (opens new window), so the application should work wherever Electron works. Or, if you'd rather use a package manager, check this list of third-party packages maintained by the IPFS community.

- **VScode or any IDE–**
    - Visual Studio Code is a source-code editor made by Microsoft for Windows, Linux and macOS. Features include support for debugging, syntax highlighting, intelligent code completion, snippets, code refactoring, and embedded Git.

4. Hardware Specification

The detailed hardware used for the project are:

Item	Description
System	HP OMEN 15 series
Processor	AMD Ryzen 5 4600H
RAM	8 GB
System Type	64-bit operating system, x64-based processor
SSD	256 GB Solid State Drive
HDD	1 TB Hard Disk Drive
Graphics	NVIDIA 4 GB Graphic Card
Operating System	Windows 11 Operating System

5. Theory

1. Introduction

The conventional medical record systems face the complicated administration procedure for data processing to ensure patients' privacy, leading to the enormous waste of human resources. Such an architecture is obviously inefficient for the medical record exchange. Blockchain technique [1] has recently been adopted to secure medical data sharing and management. The cryptographic property in the blockchain networks guarantees the patients' privacy. Data integrity and incorruptibility protect medical data from being tampered. The blockchain can be viewed as a distributed database, which stores data in each network nodes to avoid the halting problem. It thus provides higher stability, consistency and attack-resistance. The problem of distributed denial-of-service attacks (DDOS) in the conventional centralized framework can be solved by the blockchain technique. Deployment of blockchain in the medical record system not only provides the reliable service but also speeds up the medical record exchange. Owing to decentralization, the ownership of the medical record is returned to the patients, allowing them to manage the medical record directly and take care of their own health.

2. Methods

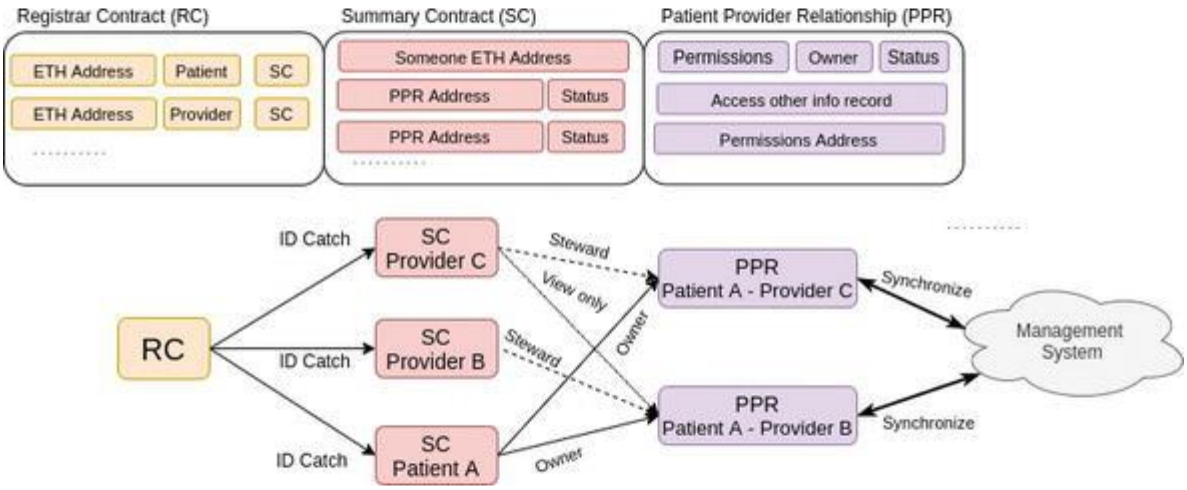
The BT is, besides the financial area, also emerging in many other sectors and gets continuously more popular. It is difficult to overview the market of existing and planned projects since there is no holistic public database or repository for it. Further, the range of visions, concepts, and prototypes is constantly increasing, which means that this review can only provide a snapshot and does not claim to be complete or exhaustive.

- **Proposed Ethereum-based framework for medical record management:**

Instead of using the traditional centralized databases, the Ethereum-based blockchain is applied to our designed system framework of medical record management to ensure the security of data. The medical records are stored within individual nodes in the blockchain networks by utilizing the smart contracts. The automatic smart contracts for the administration procedure are also designed with an aim to reducing the waste of human resource and speeding up the medical process.

- **Blockchain-based medical record management system**

Figure 1: illustrates the proposed medical record management system with smart contracts. There are three types of smart contracts, including registrar contract, patient-provider relationship contract and summary contract.



- **Registrar contract (RC)**

This contract maps member identification strings to the Ethereum address identity. All the registered members are divided into two groups, patients and medical personnel. Each identity has different access rights for the proposed system.

Authorized privilege of patients:

a) Review their own medical records.

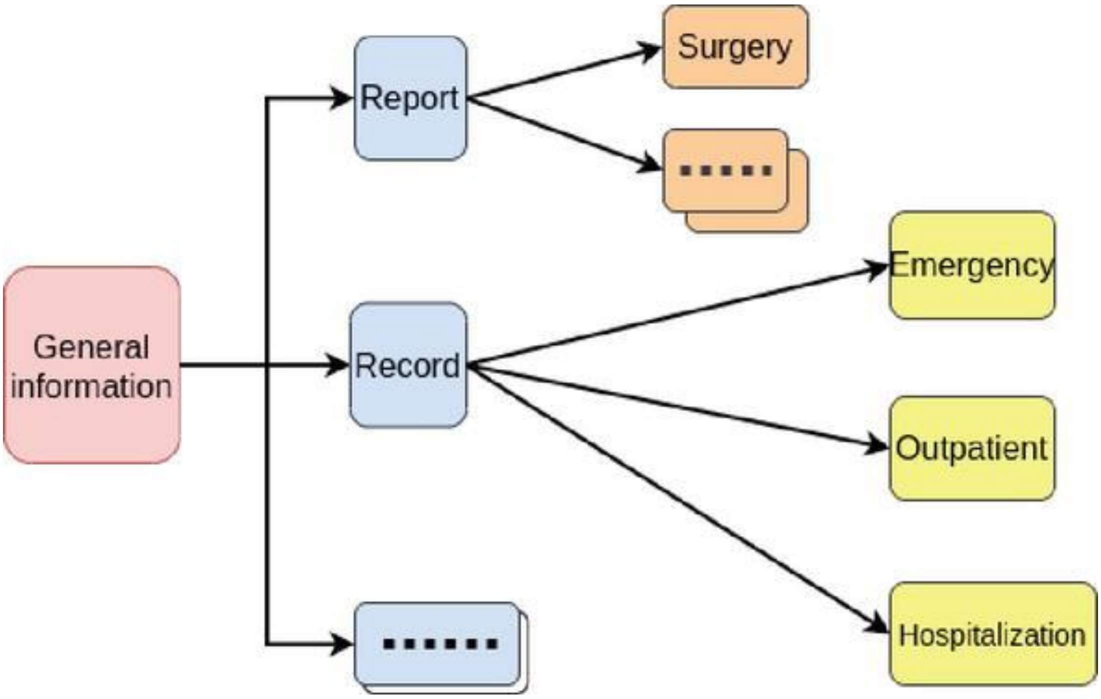
b) Authorize their own medical records.

Authorized privilege of the medical personnel:

a) Create/modify the authorized medical records.
b) Review the authorized medical records. Notice that different kinds of the medical personnel has different authorized or restricted rights.

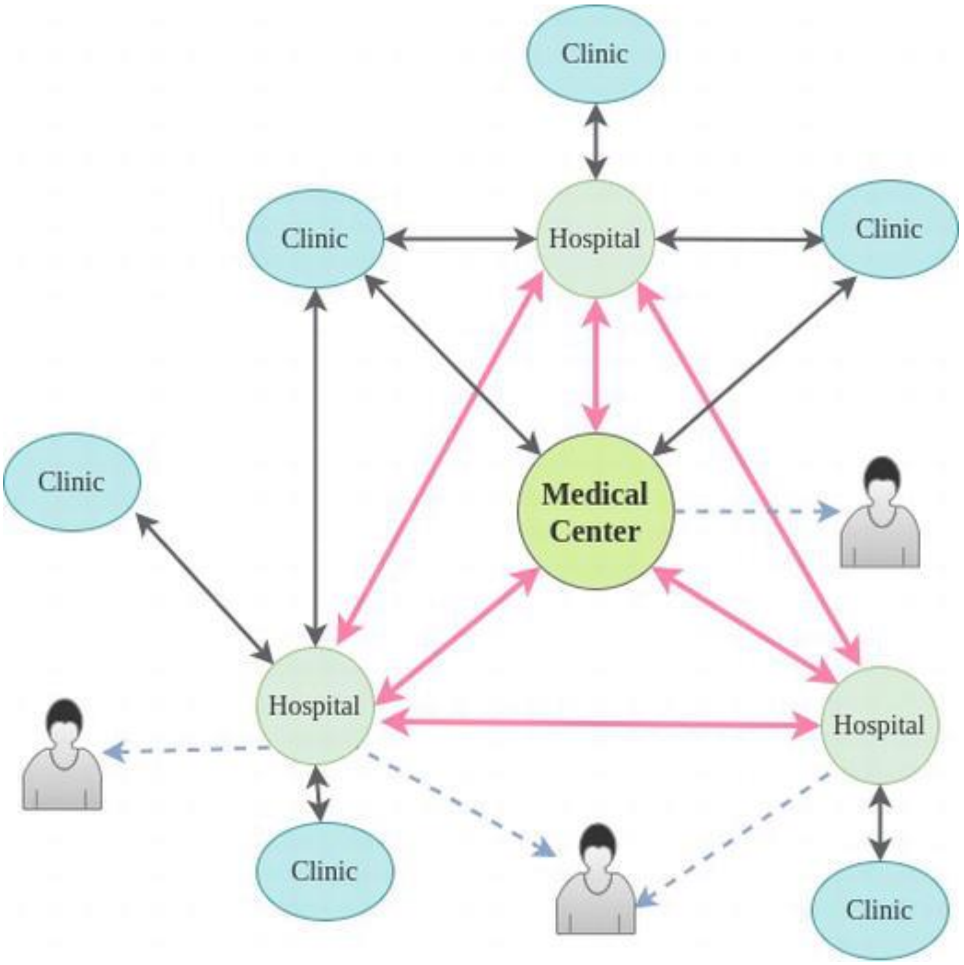
- **Summary contract (SC)**

This contract holds a list of references to PPRs, locating patients' medical record history. The patient-oriented medical record classification structure in the proposed system is designed. Each record is viewed as an PPR smart contract. The proposed medical record structure is shown in Figure



3. Private blockchain network

The deployment of the private blockchain network is illustrated in Figure, which is applied for the level of care. The main private blockchain network is plotted by the solid lines. The critical network devices are maintained by the medical centres or hospitals, and the distributed databases among them must be synchronized. The clinics only need to synchronize with the nearby blockchain network nodes to ensure their database stay latest and correct.

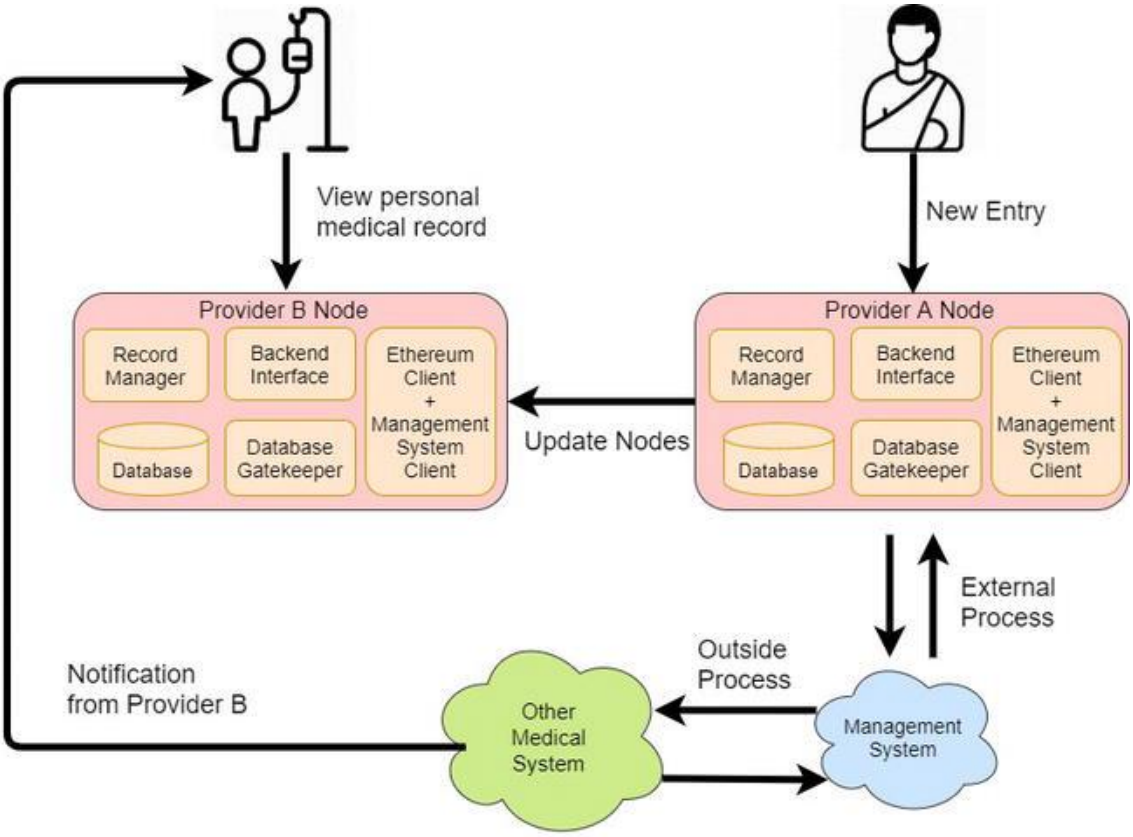


Deployment of private blockchain.

Dotted lines stand for the data requests to the blockchain network from patients whom made inquiry for medical record. In this case, the main blockchain network nodes (e.g. the medical center or hospital) are responsible to deal with the requests since their network equipments are capable of handling the heavy network traffic due to plenty of requests. As a primary node in blockchain network, the synchronization speed and correctness should be guaranteed.

4. System workflow

How the proposed management system works is presented in Figure



5. External process and outside process

The external management system detects the updates from the blockchain databases, automatically validates the latest data and notifies the patients of the new updates.

6. Update nodes

The blockchain network automatically synchronizes all nodes and offers the latest information to the patient node.

7. Limitations

With the blockchain-based technique for distributed databases, the additional network facilities and storage devices for network nodes are required to stabilize the whole system. However, it helps save human resource, reduce human errors and accelerate administration process.

6. Code and Output

Test environment

The computer specification used for the experiment was:

CPU: AMD Ryzen 5 4600H, 12MB cache, 6 cores, 12 threads

RAM: 8GB DDR4 RAM

OS: Windows 10 - 64-Bit Edition, installed on an SSD

Python: Version 3.9, x64

Code

Agent.sol

```
pragma solidity ^0.5.1;

contract Agent {

    struct patient {

        string name;

        uint age;

        address[] doctorAccessList;

        uint[] diagnosis;

        string record;

    }

    struct doctor {

        string name;

        uint age;

        address[] patientAccessList;

    }
    uint creditPool;
    address[] public patientList;
    address[] public doctorList;
    mapping (address => patient) patientInfo;
    mapping (address => doctor) doctorInfo;
    mapping (address => address) Empty;
    // might not be necessary
    mapping (address => string) patientRecords;
```

Migration.sol

```
pragma solidity ^0.5.1;
contract Migrations {
  address public owner;
  uint public last_completed_migration;
  modifier restricted() {
    if (msg.sender == owner) _;
  }
  constructor() public {
    owner = msg.sender;
  }
  function setCompleted(uint completed) public restricted {
    last_completed_migration = completed;
  }
  function upgrade(address new_address) public restricted {
    Migrations upgraded = Migrations(new_address);
    upgraded.setCompleted(last_completed_migration);
  }
}
```

Node modules

1. Move to the project directory and open it in your terminal.
2. Run npm install to install project dependencies.

Local server

Install Node lite-server by running the following command on your terminal npm install -g lite-server.

Metamask

1. Metamask is a browser extension available for Google Chrome, Mozilla Firefox and Brave Browser.
2. Go to the this link and add Metamask to your browser.

Configuration

1. Ganache

- Open Ganache and click on settings in the top right corner.
- Under Server tab:
  - Set Hostname to 127.0.0.1 -lo
  - Set Port Number to 8545
  - Enable Automine
- Under Accounts & Keys tab:
  - Enable Autogenerate HD Mnemonic

2. IPFS

- Fire up your terminal and run ipfs init
- Then run
  - ipfs config --json API.HTTPHeaders.Access-Control-Allow-Origin "['*']"
  - ipfs config --json API.HTTPHeaders.Access-Control-Allow-Credentials "['true']"
  - ipfs config --json API.HTTPHeaders.Access-Control-Allow-Methods "['PUT', 'POST', 'GET']"

3. Metamask

- After installing Metamask, click on the metamask icon on your browser.
- Click on TRY IT NOW, if there is an announcement saying a new version of Metamask is available.
- Click on continue and accept all the terms and conditions after reading them.
- Stop when Metamask asks you to create a new password. We will come back to this after deploying the contract in the next section.

Smart Contract

1. Install Truffle using npm install truffle -g
2. Compile Contracts using truffle compile

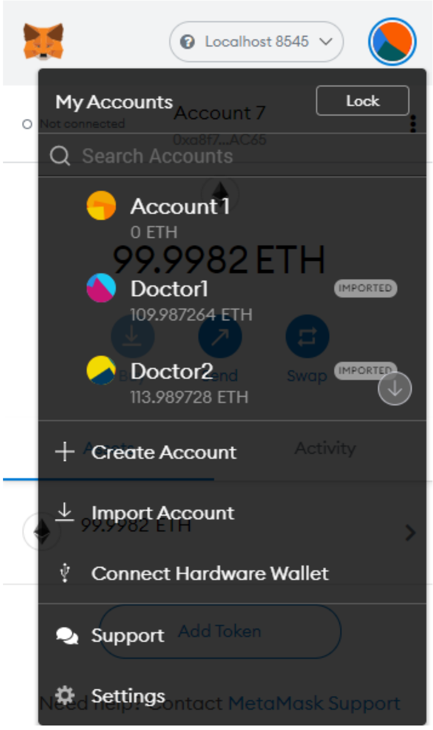
1. Starting your local development blockchain

- Open Ganache.
- Make sure to configure it the way mentioned above.

1. Open new Terminal and deploy contracts using truffle migrate
2. Copy deployed contract address to src/app.js alt text
3. If you change contents of any contract , replace existing deployment using truffle migrate --reset

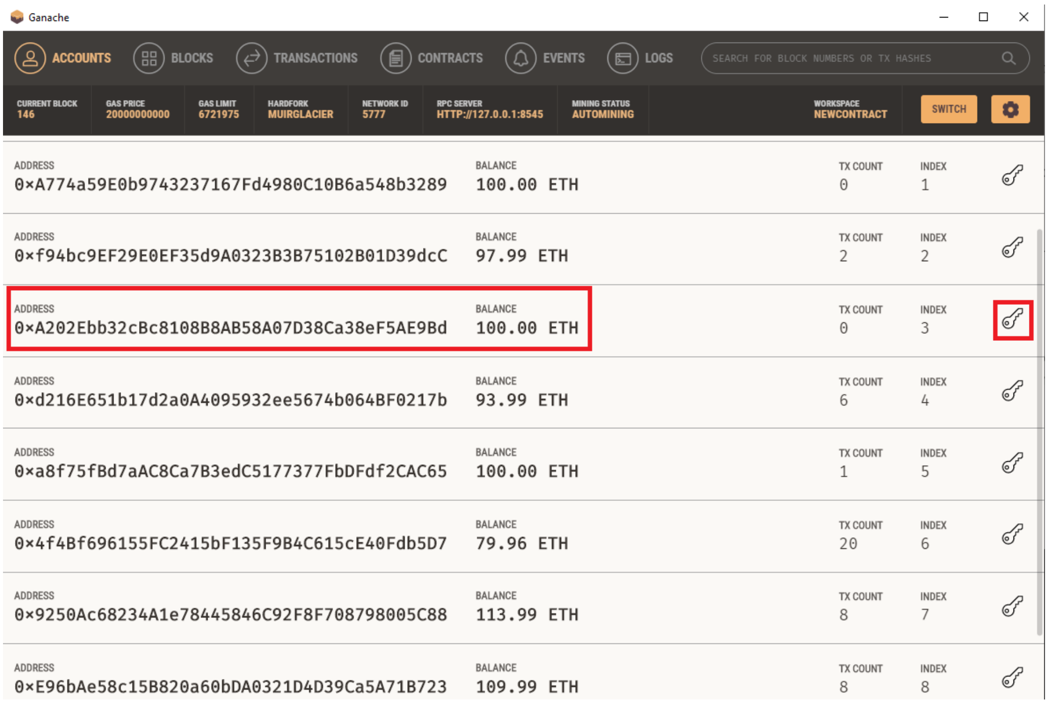
Running the dApp

1. Connecting Metamask to our local blockchain



- Connect metamask to localhost:8485
- Click on import account alt text

Select any account from ganache and copy the private key to import account into metaMask



CURRENT BLOCK 146 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK MUIRGLACIER | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:8545 | MINING STATUS AUTOMINING | WORKSPACE NEWCONTRACT

ADDRESS	BALANCE	TX COUNT	INDEX
0×A774a59E0b9743237167Fd4980C10B6a548b3289	100.00 ETH	0	1
0×f94bc9EF29E0EF35d9A0323B3B75102B01D39dcC	97.99 ETH	2	2
0×A202Ebb32cBc8108B8AB58A07D38Ca38eF5AE9Bd	100.00 ETH	0	3
0×d216E651b17d2a0A4095932ee5674b064BF0217b	93.99 ETH	6	4
0×a8f75fBd7aAC8Ca7B3edC5177377FbDFdf2CAC65	100.00 ETH	1	5
0×4f4Bf696155FC2415bF135F9B4C615cE40Fdb5D7	79.96 ETH	20	6
0×9250Ac68234A1e78445846C92F8F708798005C88	113.99 ETH	8	7
0×E96bAe58c15B820a60bDA0321D4D39Ca5A71B723	109.99 ETH	8	8

2. Starting IPFS

Start the IPFS Desktop Application

3. Start a local server

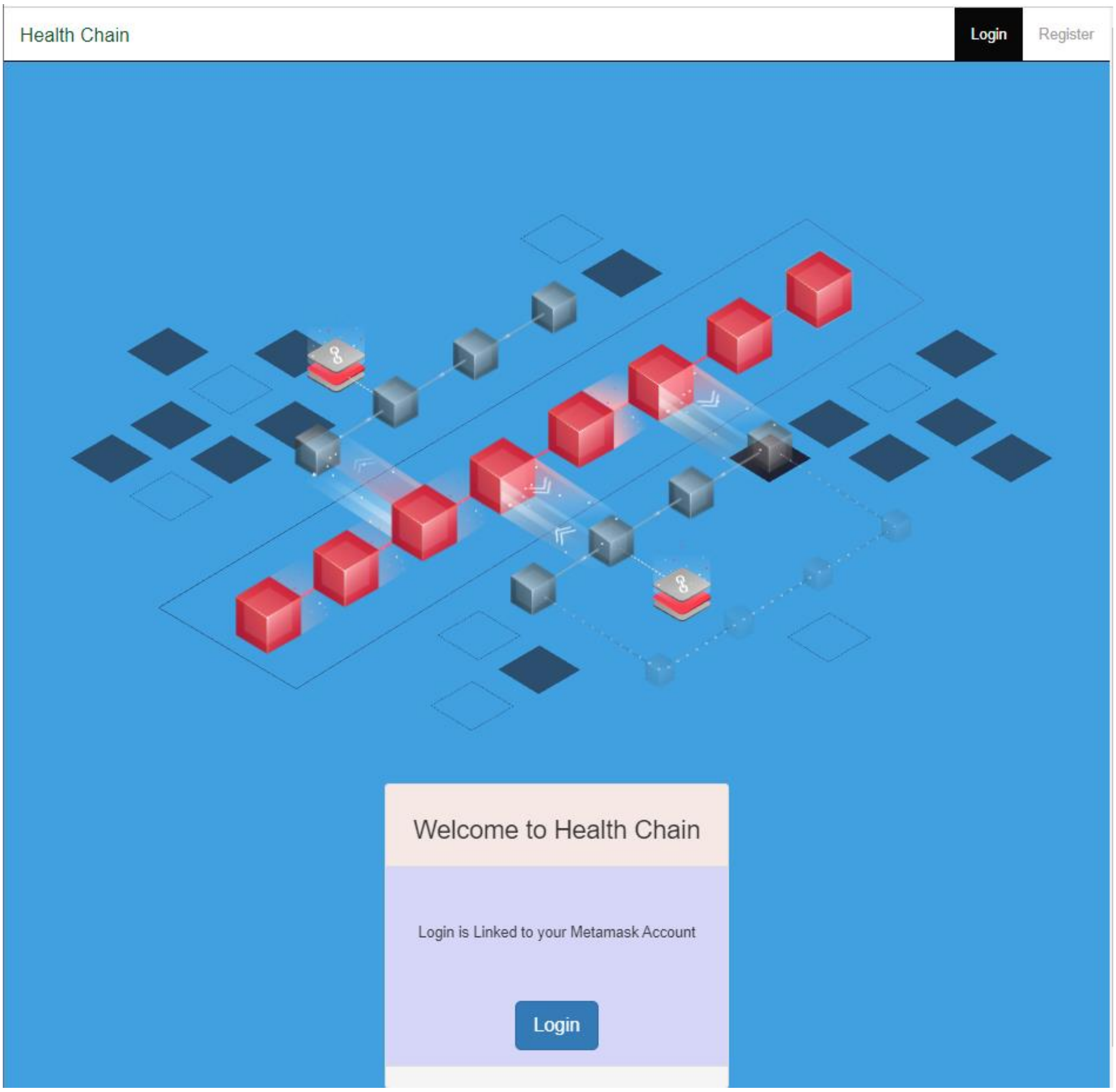
Open a new terminal window and navigate to /YOUR_PROJECT_DIRECTORY/app/.

Run npm start.

Open localhost:3000 on your browser.

That's it! The dApp is up and running locally.

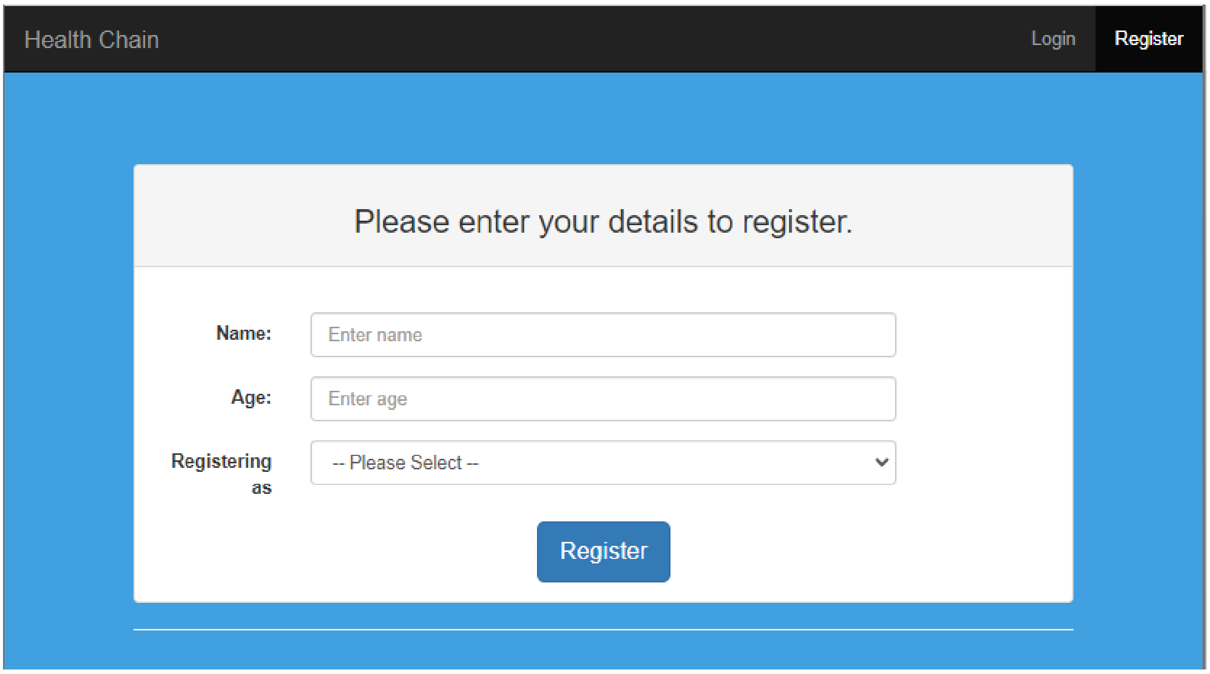
HOME PAGE



Welcome to Health Chain

Login is Linked to your Metamask Account

REGISTRATION PAGE



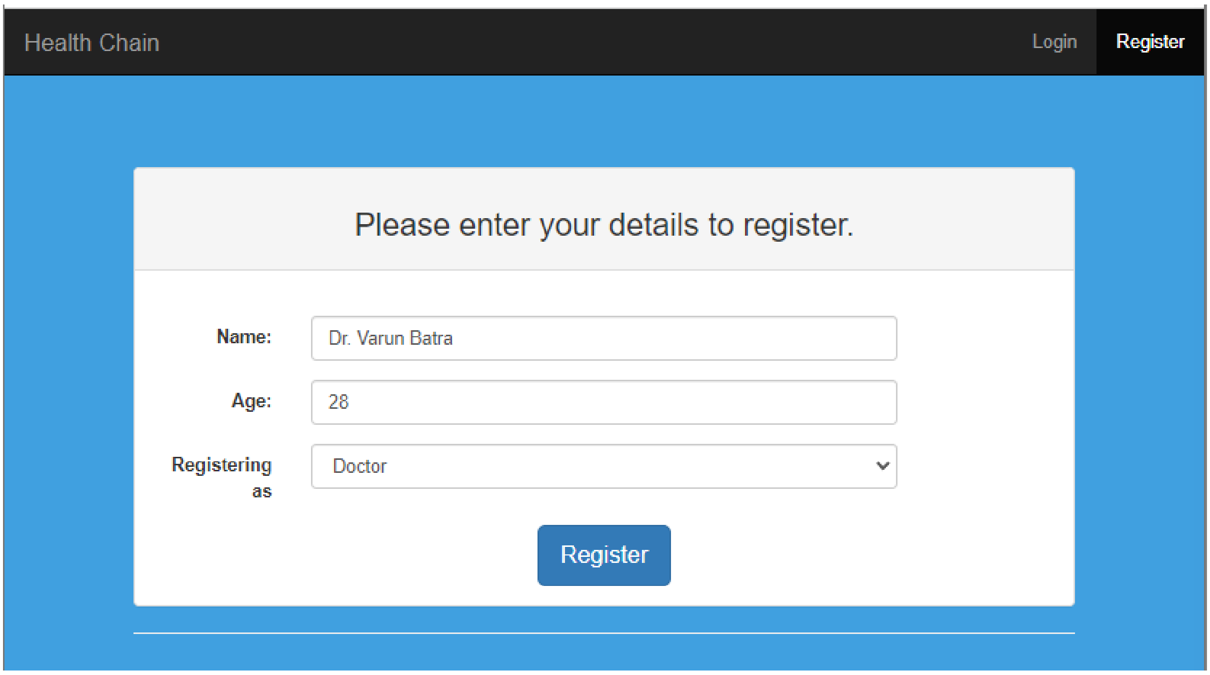
Please enter your details to register.

Name: Enter name

Age: Enter age

Registering as: -- Please Select --

DOCTOR REGISTRATION



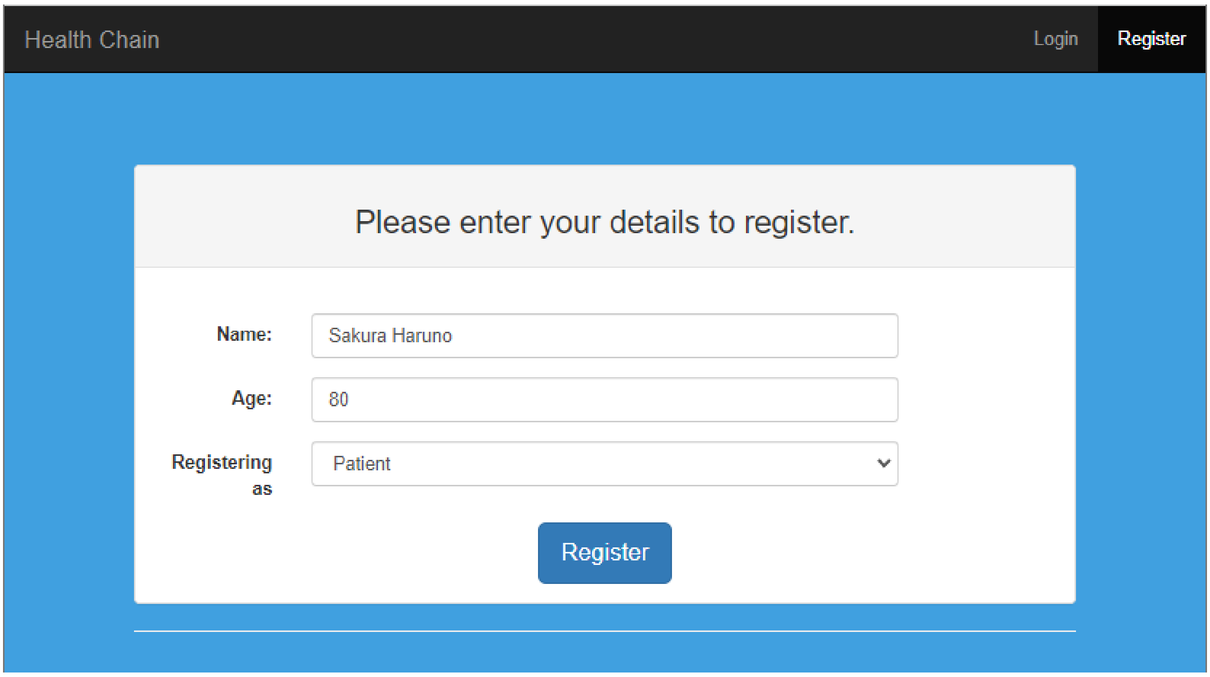
Please enter your details to register.

Name: Dr. Varun Batra

Age: 28

Registering as: Doctor

PATIENT REGISTRATION



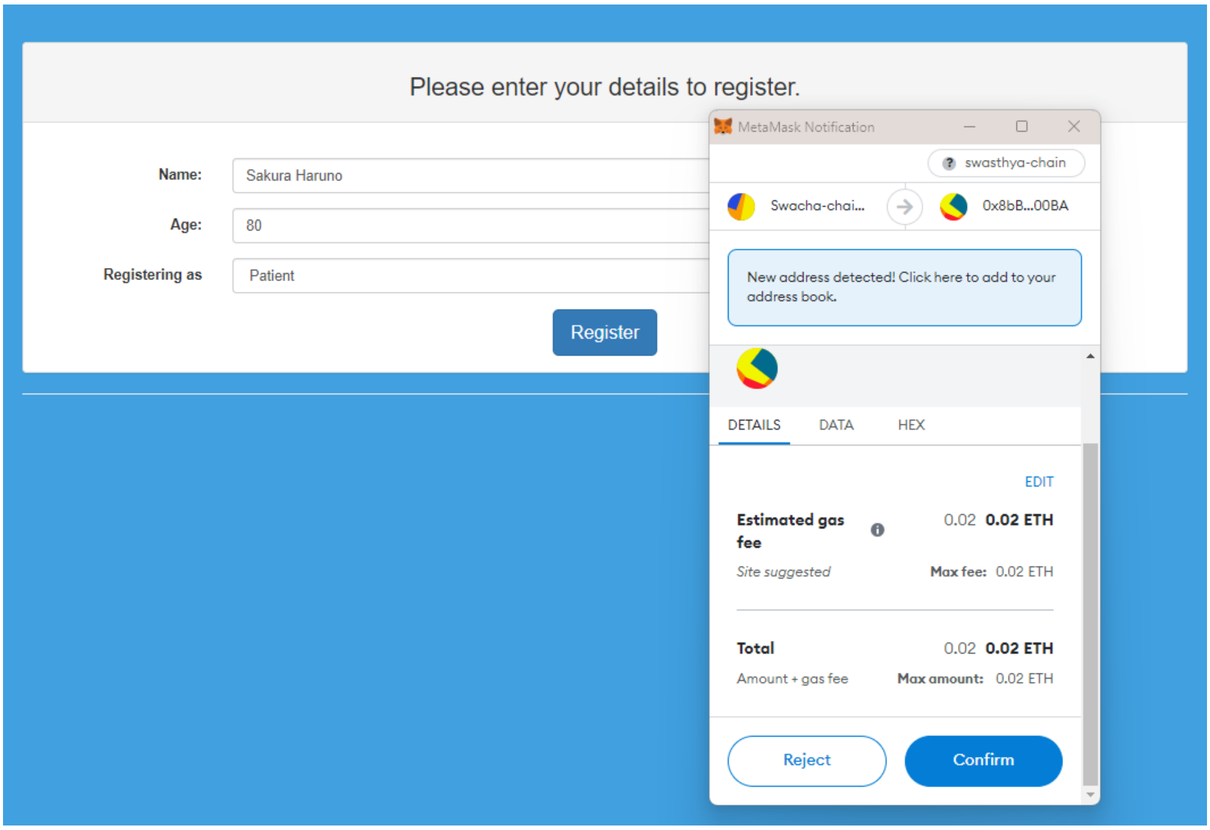
Please enter your details to register.

Name: Sakura Haruno

Age: 80

Registering as: Patient

SUCCESSFULL TRANSACTIONS



Please enter your details to register.

Name: Sakura Haruno

Age: 80

Registering as: Patient

New address detected! Click here to add to your address book.

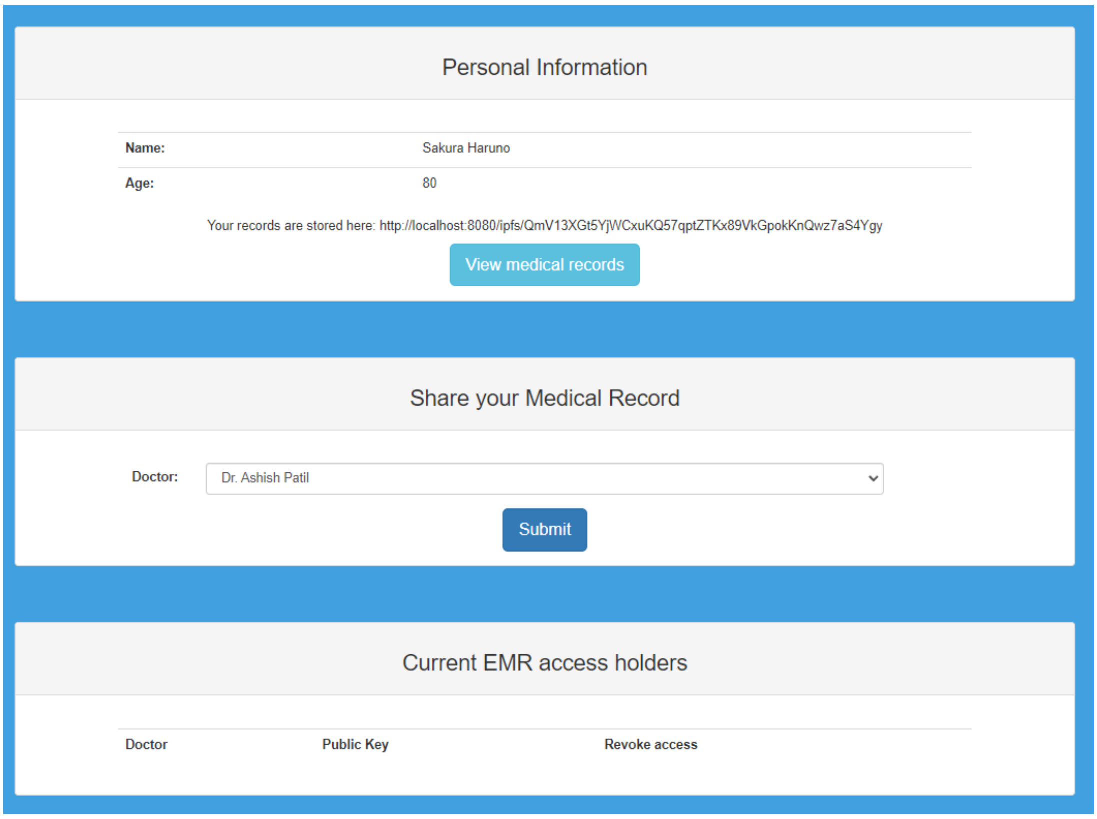
Estimated gas fee 0.02 **0.02 ETH**

Site suggested **Max fee:** 0.02 ETH

Total 0.02 **0.02 ETH**

Amount + gas fee **Max amount:** 0.02 ETH

VIEW AND SUBMIT MEDICAL RECORDS TO DOCTORS



Personal Information

Name:	Sakura Haruno
Age:	80

Your records are stored here: http://localhost:8080/ipfs/QmV13XGt5YjWCxuKQ57qptZTKx89VkGpokKnQwz7aS4Ygy

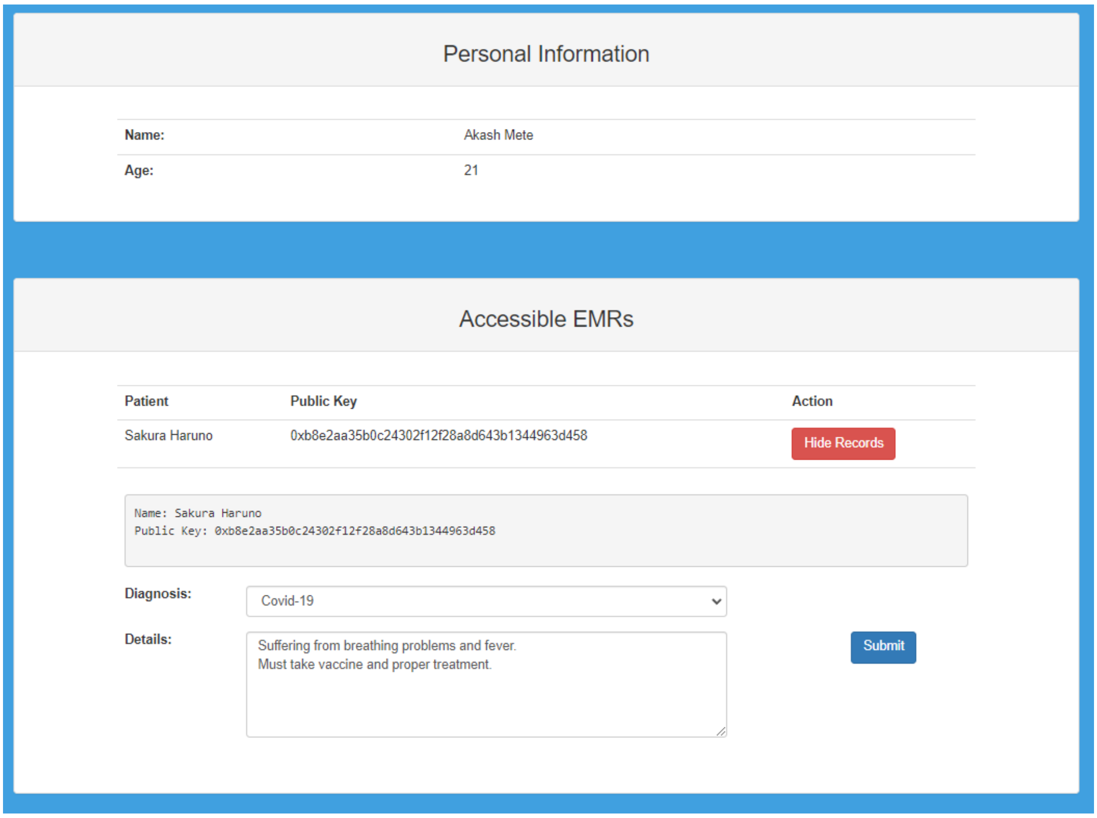
Share your Medical Record

Doctor: Dr. Ashish Patil

Current EMR access holders

Doctor	Public Key	Revoke access

DOCTORS ACCESSING PATIENT RECORDS AND GIVING PRESCRIPTION



Personal Information

Name:	Akash Mete
Age:	21

Accessible EMRs

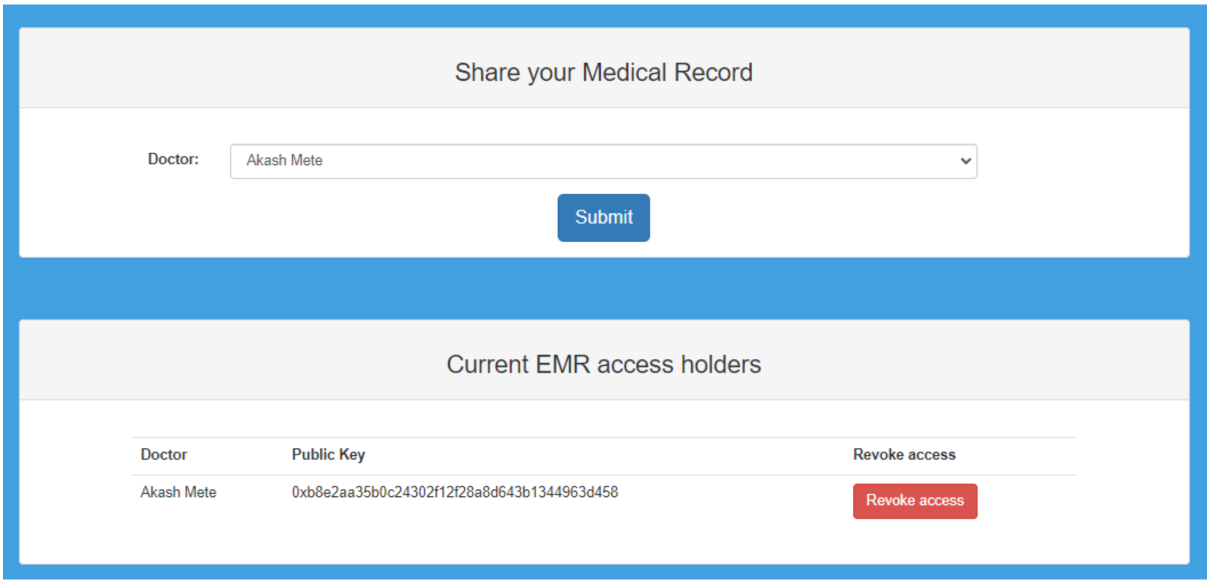
Patient	Public Key	Action
Sakura Haruno	0xb8e2aa35b0c24302f12f28a8d643b1344963d458	Hide Records

```
Name: Sakura Haruno
Public Key: 0xb8e2aa35b0c24302f12f28a8d643b1344963d458
```

Diagnosis: Covid-19

Details: Suffering from breathing problems and fever.
Must take vaccine and proper treatment.

OPTION TO REVOKE ACCESS FROM EMR ACCESS HOLDERS



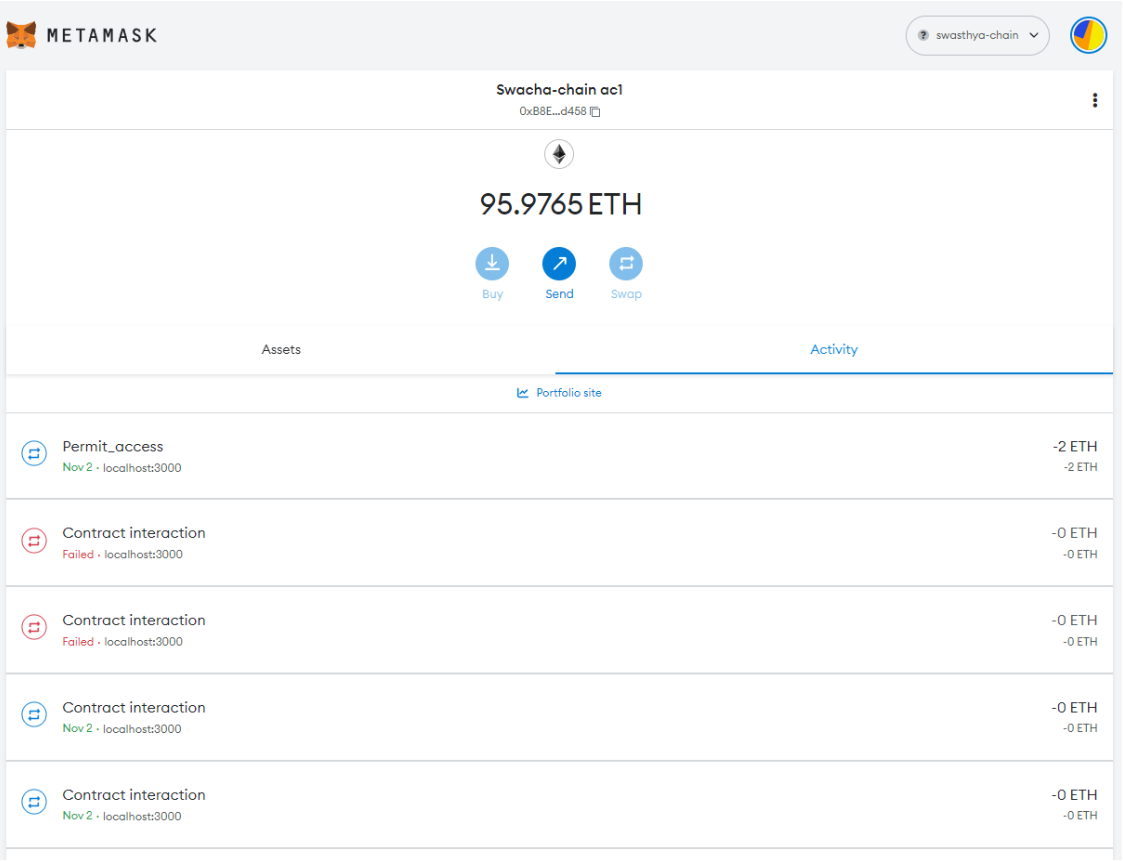
Share your Medical Record

Doctor: Akash Mete

Current EMR access holders

Doctor	Public Key	Revoke access
Akash Mete	0xb8e2aa35b0c24302f12f28a8d643b1344963d458	Revoke access

METAMASK ACTIVITY LOG OF ADMIN WALLET

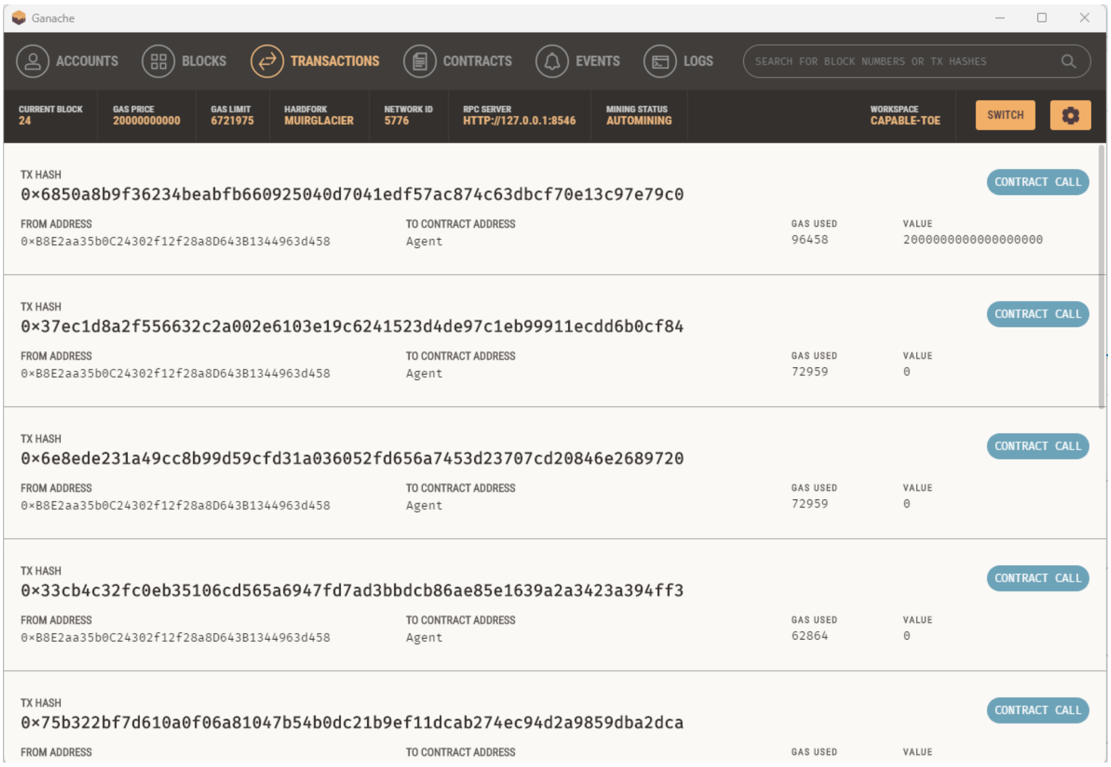


Swacha-chain ac1
0xB8E...d458

95.9765 ETH

Permit_access Nov 2 · localhost:3000	-2 ETH -2 ETH
Contract interaction Failed · localhost:3000	-0 ETH -0 ETH
Contract interaction Failed · localhost:3000	-0 ETH -0 ETH
Contract interaction Nov 2 · localhost:3000	-0 ETH -0 ETH
Contract interaction Nov 2 · localhost:3000	-0 ETH -0 ETH

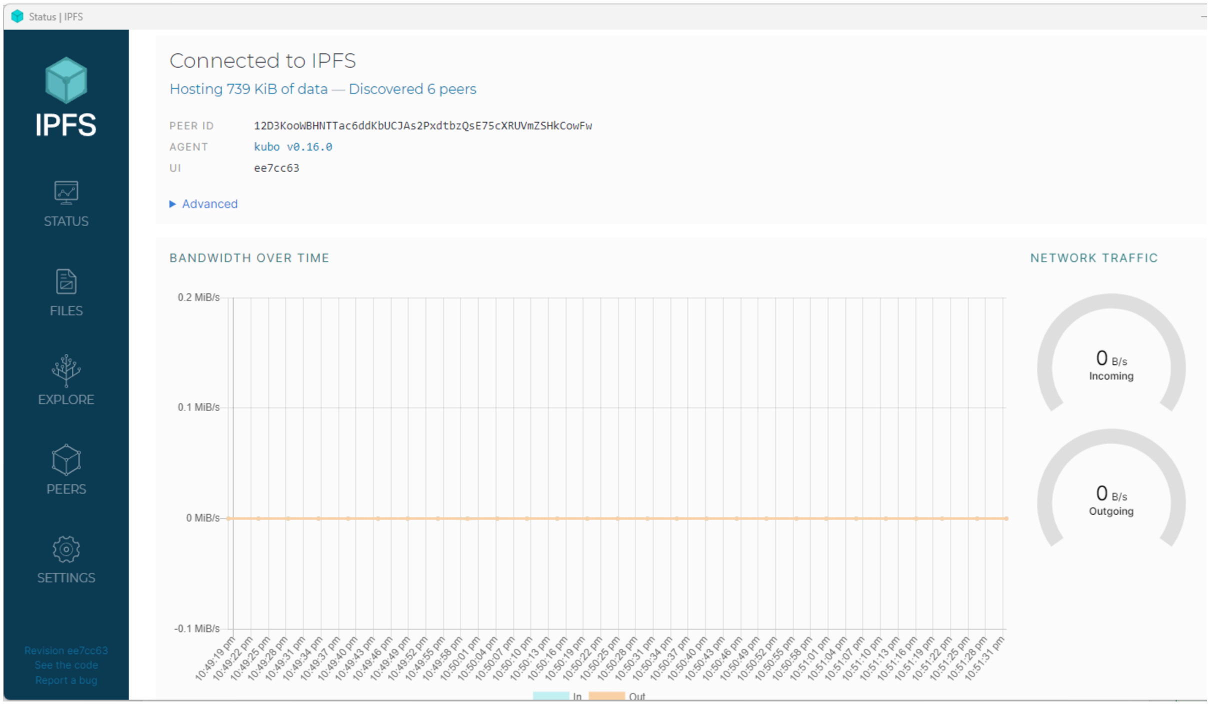
GANACHE LOG OF ALL TRANSACTIONS



CURRENT BLOCK 24 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK MUIRGLACIER | NETWORK ID 5776 | RPC SERVER HTTP://127.0.0.1:8546 | MINING STATUS AUTOMINING | WORKSPACE CAPABLE-TOE

```
TX HASH
0×6850a8b9f36234beabfb660925040d7041edf57ac874c63dbcf70e13c97e79c0          CONTRACT CALL
FROM ADDRESS                                  TO CONTRACT ADDRESS      GAS USED   VALUE
0×B8E2aa35b0C24302f12f28a8D643B1344963d458    Agent                    96458      2000000000000000000

TX HASH
0×37ec1d8a2f556632c2a002e6103e19c6241523d4de97c1eb99911ecdd6b0cf84          CONTRACT CALL
FROM ADDRESS                                  TO CONTRACT ADDRESS      GAS USED   VALUE
0×B8E2aa35b0C24302f12f28a8D643B1344963d458    Agent                    72959      0

TX HASH
0×6e8ede231a49cc8b99d59cfd31a036052fd656a7453d23707cd20846e2689720          CONTRACT CALL
FROM ADDRESS                                  TO CONTRACT ADDRESS      GAS USED   VALUE
0×B8E2aa35b0C24302f12f28a8D643B1344963d458    Agent                    72959      0

TX HASH
0×33cb4c32fc0eb35106cd565a6947fd7ad3bbdcb86ae85e1639a2a3423a394ff3          CONTRACT CALL
FROM ADDRESS                                  TO CONTRACT ADDRESS      GAS USED   VALUE
0×B8E2aa35b0C24302f12f28a8D643B1344963d458    Agent                    62864      0

TX HASH
0×75b322bf7d610a0f06a81047b54b0dc21b9ef11dcab274ec94d2a9859dba2dca          CONTRACT CALL
FROM ADDRESS                                  TO CONTRACT ADDRESS      GAS USED   VALUE
```

IPFS DESKTOP DATA TRAFFIC MONITOR



Connected to IPFS

Hosting 739 KiB of data — Discovered 6 peers

PEER ID 12D3KooWBHNTTac6ddKbUCJAs2PxdtbzQsE75cXRUVmZSHkCowFw
AGENT kubo v0.16.0
UI ee7cc63

▶ Advanced

7. Conclusion

In this project we have demonstrated the implementation of blockchain technology which is applied on a Healthcare based medical records holder called Health Chain.

Overall, the project as managed to answer the questions whether and how Blockchain Technology can be used in the field of Healthcare and have provided samples of output for available features which we have implemented in out mini project.

8. References

[1] H. Jin, Y. Luo, P. Li and J. Mathew, “A Review of Secure and Privacy-Preserving Medical Data Sharing,” in IEEE Access, vol. 7, pp. 61656-61669, 2019, doi: 10.1109/ACCESS.2019.2916503.

[2] Azaria, A. Ekblaw, T. Vieira and A. Lippman, “MedRec: Using Blockchain for Medical Data Access and Permission Management,” 2016 2nd International Conference on Open and Big Data (OBD), Vienna, 2016, pp. 25-30, doi: 10.1109/OBD.2016.11

[3] H. Yang and B. Yang, “A blockchain-based approach to the secure sharing of healthcare data”, Proc. Norwegian Inf. Secur. Conf., pp. 1-12, 2017

[4] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa and X. Zhang, “BBDS: Blockchain-based data sharing for electronic medical records in cloud environments”, Information, vol. 8, no. 2, pp. 44, 2017

[5] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du and M. Guizani, “MeDShare: Trust-less medical data sharing among cloud service providers via blockchain”, IEEE Access, vol. 5, pp. 14757-14767, 2017

[6] X. Liang, J. Zhao, S. Shetty, J. Liu and D. Li, “Integrating blockchain for data sharing and collaboration in mobile healthcare applications”, Proc. IEEE 28th Annu. Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC), pp. 1-5, Oct. 2017.

[7] McFarlane, M. Beer, J. Brown and N. Prendergast, Patientory: A Healthcare Peer-to-Peer EMR Storage Network v1, Addison, TX, USA:Entrust, 2017

[8] E. Daraghmi, Y. Daraghmi and S. Yuan, “MedChain: A Design of Blockchain-Based System for Medical Records Access and Permissions Management,” in IEEE Access, vol. 7, pp. 164595-164613, 2019, doi: 10.1109/ACCESS.2019.2952942

[9] R. Guo, H. Shi, Q. Zhao and D. Zheng, “Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems,” in IEEE Access, vol. 6, pp. 11676-11686, 2018, doi: 10.1109/ACCESS.2018.2801266