

A Blockchain based Electronic Medical Health Records Framework using Smart Contracts

PROJECT REPORT

Submitted by

Rishi Sunder

Sathwik S

Suhaas Varma

CS6611 - CREATIVE AND INNOVATIVE PROJECT



COLLEGE OF ENGINEERING GUINDY

ANNA UNIVERSITY: CHENNAI 600 025

ANNA UNIVERSITY: CHENNAI 600 025

BONAFIDE CERTIFICATE

Certified that this project report “**Blockchain Based Health Records Framework**” is the bonafide work of “**Rishi Sunder, Sathwik S, Suhaas Varma**” who carried out the project work as a part of Creative and Innovative Project Laboratory.

SIGNATURE

SIGNATURE

HEAD OF THE DEPARTMENT

SUPERVISOR

Table Of Contents

Chapter	Title	Page no
	Abstract	4
1	Introduction	5
2	Literature Survey	7
3	Proposed System	
	3.1 Architecture Diagram	9
	3.2 Proposed Methodology	10
	3.2.1 Client Application	
	3.2.2 Ethereum Network	
	3.2.3 Smart Contract	
4	Result and Discussion	13
5	Conclusion	
	5.1 Future Works	18
	Appendices	19
	References	21

Abstract

The common issues in medical services within the country are mostly associated with doctors' referral process, data transfer between health institutions, and portals for patients to access their medical information. Specific issues arise, such as sharing health records across institutes or hospitals, problems with misuse of data once shared, no security, etc. Blockchain is an emerging distributed technology that can solve these issues due to its immutability and architectural nature that prevent records manipulation or alterations.

An Electronic Health Record (EHR) is a comprehensive system collection of patient personal information and health records that are stored electronically in a digital format.

This project aims to solve the healthcare sector's current problems by hosting medical record transactions on the Blockchain to create a smart ecosystem. The goal is to provide secure access to patient data, avoiding third party access to it without permission.

EHR Framework uses blockchain technology to securely store the records and maintain a single version of the truth. The stakeholders will have to request permission to access a patient's history and commit the transaction to the distributed ledger.

A solution centered on the blockchain, can permit large-scale availability, data confidentiality, cost-effectiveness, and belief in the information system.

Chapter 1

Introduction

Blockchain

A blockchain is a distributed database that is shared among the nodes of a computer network. As a database, a blockchain stores information electronically in digital format. Blockchains are best known for their crucial role in cryptocurrency systems, such as Bitcoin, for maintaining a secure and decentralized record of transactions. The innovation with a blockchain is that it guarantees the fidelity and security of a record of data and generates trust without the need for a trusted third party.

Smart Contract

A smart contract is a special account with associated data and code. The code is in an Ethereum-specific binary format (i.e., Ethereum Virtual Machine byte code) and deployed by an account to a global database known as blockchain. Smart contracts are an exciting application of blockchain. The smart contract of the blockchain can be understood as a piece of code (contract) that triggers execution when the two parties make a transaction transfer on the blockchain asset.

Problem Statement

The common issues in medical services within the country are mostly associated with doctors' referral process, data transfer between health institutions, and portals for patients to access their medical information. Specific issues arise, such as sharing health records across institutes or hospitals, problems with misuse of data once shared, no security, etc.

Issues include

- Interoperability
- Information Asymmetry
- Data breaches

Objective

This project aims to solve the healthcare sector's current problems by hosting medical record transactions on the Blockchain to create a smart ecosystem. The goal is to provide secure access to patient data, avoiding third party access to it without permission.

EHR Framework uses blockchain technology to securely store the records and maintain a single version of the truth. The stakeholders will have to request permission to access a patient's history and commit the transaction to the distributed ledger.

Chapter 2

Literature Survey

V. B, S. N. Dass, S. R & R. Chinnaiyan[7], 2021 Proposed system uses Hyperledger fabric to host smart contract called chain code in a containerized technology that integrates the application logic. The stakeholders will have to request permission to access a patient's history and commit the transaction to the distributed ledger. Since it is possible to distinguish the people engaged in the transactions, this could endanger their confidentiality and secrecy.

V. M. Harshini et al [8] ,2019 proposed an architecture to address-Health application challenges where Doctors and hospitals are considered as nodes which are connected to the eHealth Blockchain with the smart contract and even an off-chain database is maintained. Patients can interact with the Blockchain and medical sensors through the data gateway. The software gives real-time data access, keeps the data confidential, handles high volumes of data efficiently, and also authenticates and authorises the data. The system does not use role based access.

Akarca D et al [1], 2019 proposed model contains Data on a blockchain and is distributed across multiple servers so that each has a simultaneous ledger of all transactions. Lists of data, termed *blocks*, are linked chronologically by cryptographic hashes in an encrypted linear *chain*. This provides an auditable record unalterable by a single party once the network collectively has confirmed block validity. Blockchain can help in multiple ways; lowering transaction costs by the use of smart contracts to automate processes, reduce administrative burden and remove intermediaries. Distributed methods for data integrity validation are not alone

sufficient to solve all cybersecurity hazards.

N. Poonguzhali et al [4] ,2020 proposed system is a twofold process where first model focuses on the block creation and secondly secure the data using Elliptic Curve Cryptography (ECC) Algorithm. Scalability was ensured for the system. The immutability was also maintained in the system and it was ensured that the system was not altered by other stakeholders other than the role allotted. Communication is not possible between parties.

S. Alexaki et al [5] , 2018 proposed model validates Blockchain transactions by a miner network formed by the authority itself, healthcare providers, authorized medical stakeholders and other regulatory bodies. A permissioned platform facilitates the mandatory use of a trusted execution environment hardware for the computing nodes and the use of lightweight cryptography and password hashing to provide confidentiality of user credentials in clients. Governmental health authorities by virtue of their role as a regulator, can leverage the benefits of blockchains while retaining a sufficient degree of control over the blockchain application. This makes a common view of patient data accessible by all providers possible, while at the same time, ensures that patients retain complete control of their medical record. Sharing of records between providers is not possible.

B. L. Radhakrishnan et al [2], 2019 Proposed an application that connects associated healthcare providers to store and share the EHR using blockchain. This is divided into four layers such as User Management Layer, EHR Generation and View Layer, EHR Storage Layer, and EHR Access Management Layer based on the functionality. The proposed blockchain based healthcare system uses the multilevel authentication

scheme to address the user wallet attacks by adding one more level of security The blockchain-based healthcare system needs huge storage for storing the blockchain that is still a challenging task

U. P. Ellewala et al [6], 2020 Proposed instant messaging application based on blockchain technology consists of a message authentication model, a message end to end encryption model to protect the privacy of the user and a cryptographic hash mode to verify the integrity of the messages and smart contracts. Furthermore, each block is stamped with the correct timestamp to create a correct linked list in chronological order. Blockchain has shown its potential for viewing chat history in a safe manner and also by eliminating a centralised approach, users can assure the safety, confidentiality, availability of data and communication. Application is not scalable.

M. Abdulaziz et al [3], 2018 Proposed Decentralized messenger application utilizing the Ethereum Whisper protocol. Using the application, two users can engage in secure and anonymous communication which is encrypted end-to-end and resistant to network traffic analysis. The application is capable of sending end-to-end encrypted messages while ensuring that the identity of the sender and receiver are anonymous even with the presence of an adversary controlling most of the network. The application does not account for the possibility of the user being offline or in an unexpected network failure.

Chapter 3

Proposed System

3.1 Architecture diagram

The patient and the healthcare provider both interact with the same client application. The patient can see the list of doctors and choose to grant access. On granting access, a smart contract function is triggered to verify the identity of the provider and add them to the list of approved doctors on the patient side. The patient can also revoke the doctor's access, upon which another smart contract function is triggered to remove them from the list of authorized doctors.

On receiving access to the patient's records, the doctor can view and update them. To update the records requires another smart contract transaction after which the doctor's access is automatically revoked.

The client application also allows the parties to chat with each other, sending messages as transactions on the blockchain network.

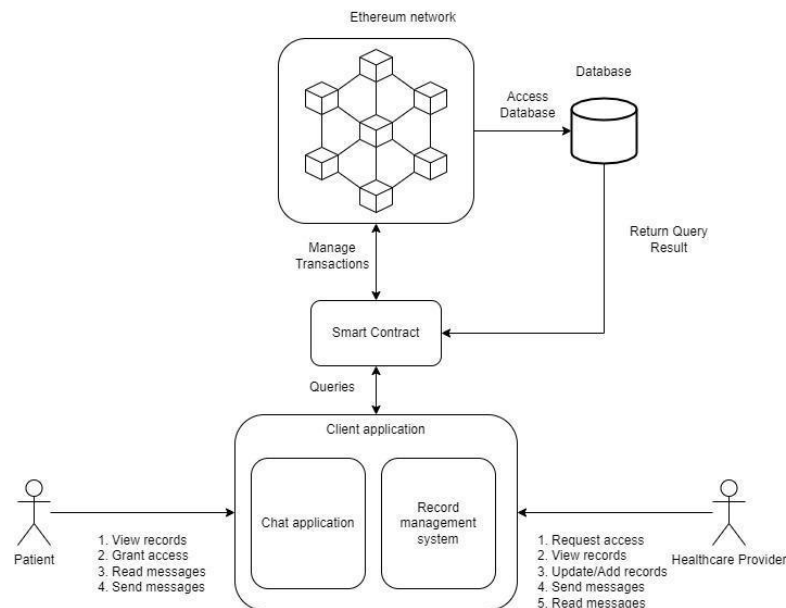


Fig 3.1 Architecture diagram

3.2 Proposed Methodology

The main problem of the current health care is that the organizations hold multiple and fragmented medical records of patients. The Proposed System aims to solve the health care sector's current problems by hosting medical record transactions on the Blockchain to create a smart ecosystem. The goal is to provide secure access to patient data, avoiding the third party accessing it without permission.

EHR Framework uses blockchain technology to securely store the records and maintain a single version of the truth. The stakeholders will have to request permission to access a patient's history and commit the transaction to the distributed ledger.

A solution centered on the blockchain, can permit large-scale availability, data confidentiality, cost-effectiveness, and belief in the information system. Yeah

Using Blockchain as the underlying technology to back the EHR provides the following features:

- All stakeholders involved with the patients will have time-limited access to the EHR. The EHR is shared in the form of a Smart Contract.
- The information is always kept private and secure.
- Blockchain being universal will ensure that the EHR framework will be compatible across multiple health applications.

List of Modules

- Client Application
- Ethereum Network
- Smart Contract

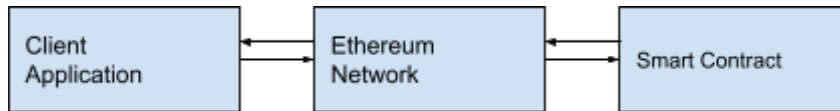


Fig 3.2 Interaction between different modules

3.2.1 Client Application

The users of this system could be patients, doctors etc. The main task of these users would be to interact with the system and perform basic tasks such as create and read the medical records. The users using this system would be accessing the system's functionality by a DApp. The GUI contains all the functions that could be accessed by a particular user. The user according to the assigned role could use this GUI for interacting with the other layer of the system, i.e., blockchain layer.

3.2.2 Smart Contract

Smart contracts are programs stored on a blockchain that run when predetermined conditions are met. They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement or time loss. Smart contracts are an important part of DApps as they are used for performing basic operations. Following contracts are included in this framework:

- Patient Records
- Roles

3.2.3 Ethereum Network

This layer contains the code or mechanism for interaction of user with the DApp which is functioning on the blockchain. This layer contains three elements inside it.

- **Blockchain Assets:** In Ethereum blockchain, transaction is the process by which external user can update the state of the record or information stored on the Ethereum blockchain network. These transactions are treated as *assets* by the Ethereum blockchain as they are piece of information that user can send to another user or to simply store it for using it later.
- **Governance Rules:** Blockchain technology in general follows some consensus rules for its transactions to be done and computed. For this purpose it needs some consensus algorithms to keep the blockchain temper-proof and secure. Ethereum blockchain uses Proof of Work (PoW) consensus algorithm, the reason behind using it is also for ensuring that *governance* of blockchain is maintained in a trusted manner which is through consent from all the trusted nodes attached to the blockchain network.
- **Network:** Ethereum blockchain uses the peer-to-peer network. In this network all the nodes are connected as *peers*. With no node acting as the central node controlling all the functions of the network. The reason behind using this network was because the idea was to create a distributed platform not a centralized. So, using a network where all the connected nodes have equal status and right was the best choice this technology could have done.

Chapter 4

Result and Discussion

Landing page

This is Landing page of the dMed application where the patient and doctor can login using their metamask account.

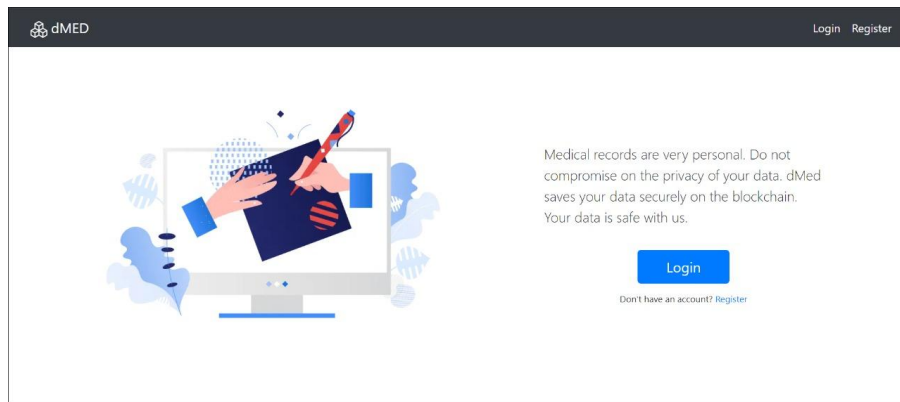


Fig 4.1 Landing page of the application where the user either logs in or registers

Register Page

This is the register page of the application where a new user can register as a doctor or a patient.

The screenshot displays the sign-up page of the dMed application. It has a dark header with the dMED logo and 'Login Register' links. The main content area contains a 'Sign Up' form. The form has three input fields: 'Name:' with the value 'Suhaas', 'Age:' with the value '40', and 'Registering as:' which is a dropdown menu. The dropdown menu is open, showing three options: 'Doctor' (selected), '--- Please Select ---', and 'Patient'. Below the dropdown, the word 'Doctor' is also visible.

Fig 4.2 The signup page for registering new users

Patient Page

This is the patient page where patient details are shown and their functionalities like giving access , revoking access can be done when the patient logs in using the account.

dMED chat Logout

Personal Information

Name:	Rishi
Age:	30

Your records are stored here: <http://localhost:8080/ipfs/QmbHwU43VHQmH4zGEGlXfgBzUxw4Cz4tP3MeK5kFiQjdVo>

[Hide Medical Records](#)

Name: Rishi
Public Key: 0xffdab8f1526e59a5e55bf849c7eb847156fdba82

Diagnosed By : sathwik
Diagnosis Time : 25/05/2022 18:15 PM
Diagnosis : Common Flu
Comments : isolate

Fig 4.3 The patient page where the patient can view his medical history

Doctor Page

This is the doctor page where the details of the doctor are shown and patients medical records can be added by the doctor.

dMED Chat Logout

Personal Information

Name:	Suhaas
Age:	40

Accessible EMRs

Patient	Public Key	Action
---------	------------	--------

Fig 4.4 The doctor page where the doctor can view the list of patients

Patient page giving access

This is a part of functionality in patient page where patient can give access to his medical record to a doctor or multiple doctors.

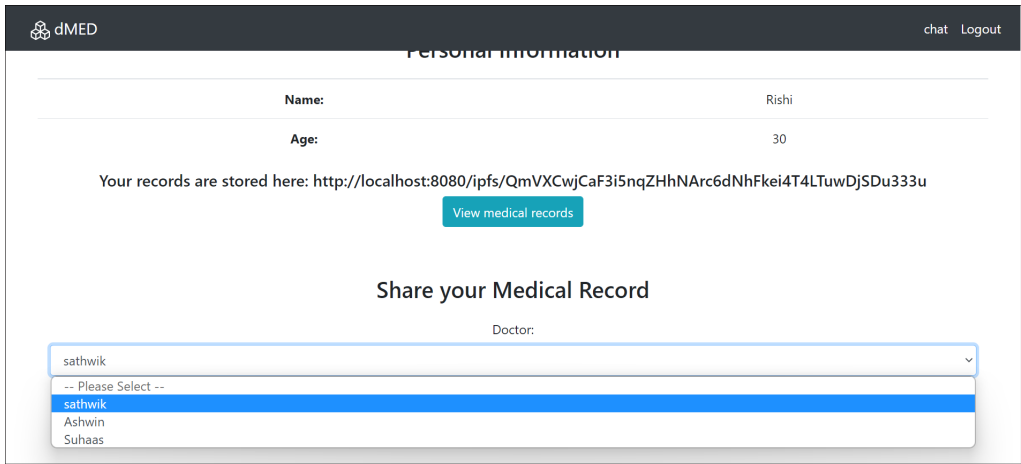


Fig 4.5 The page where patient can give access to a particular doctor

Patient page revoking access

This is a part of functionality in patient page where patient can revoke access to his medical record to a doctor or multiple doctors.

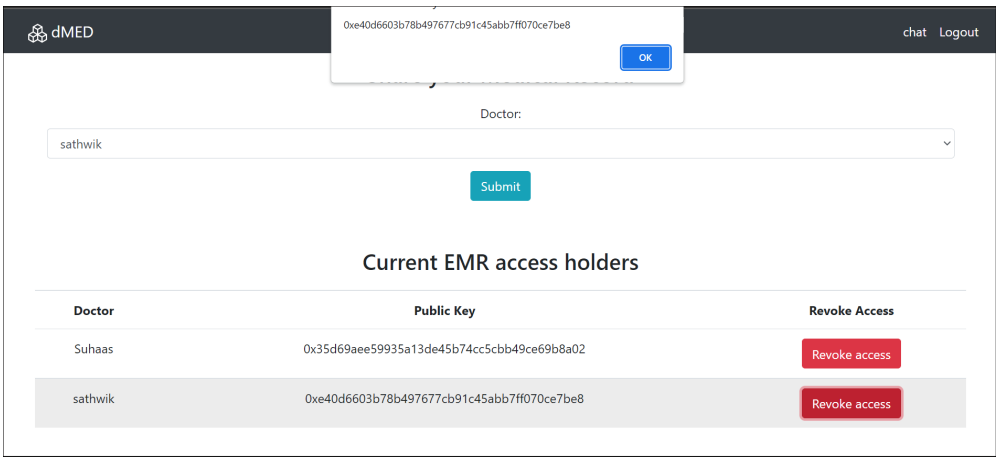
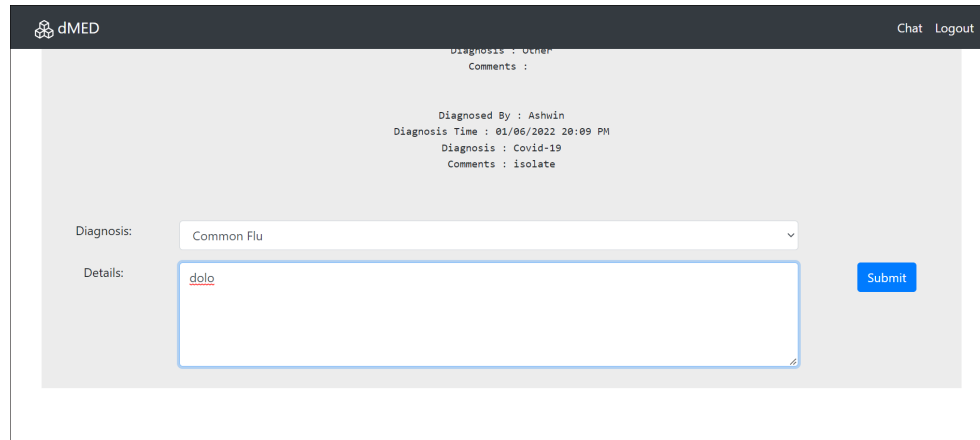


Fig 4.6 Page for revoking access of doctors

Doctor page report

This is functionality in the doctor page where doctor can submit the diagnosis of the patient who gave access to medical records.

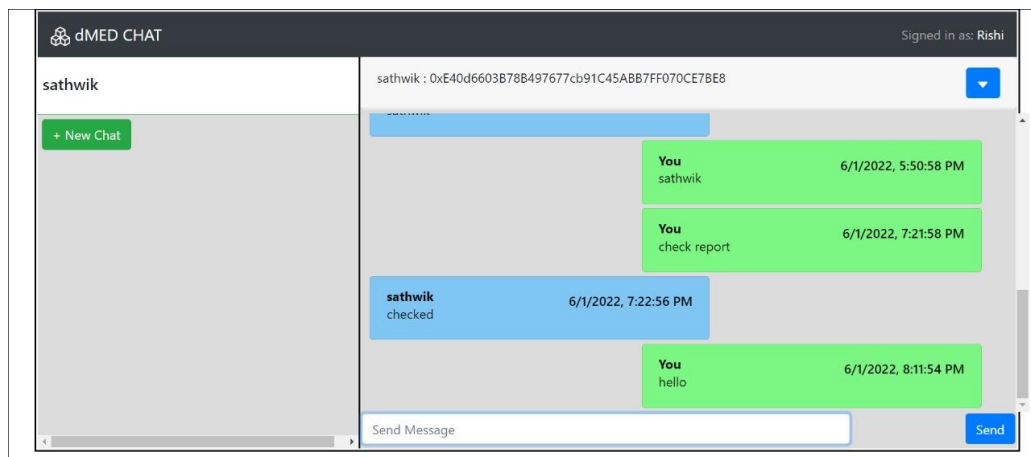


The screenshot shows a web interface for a doctor's report. At the top, there's a header with the dMED logo and 'Chat Logout' links. Below the header, there's a section for 'Diagnosis : Other' and 'Comments :'. The main content area contains a form with a 'Diagnosis:' dropdown menu set to 'Common Flu' and a 'Details:' text area containing the word 'dolo'. A blue 'Submit' button is located to the right of the text area. Above the form, there's a summary of the diagnosis: 'Diagnosed By : Ashwin', 'Diagnosis Time : 01/06/2022 20:09 PM', 'Diagnosis : Covid-19', and 'Comments : isolate'.

Fig 4.7 The page where the doctor adds health records for a patient

Chat Application

This is the chat application where doctor can chat with patient or patient can chat with doctor regarding any queries in the report.



The screenshot shows a chat application interface. On the left, there's a sidebar with the dMED CHAT logo and a '+ New Chat' button. The main chat area displays a conversation between 'sathwik' and 'You'. The messages are as follows: 'sathwik' (blue bubble) says 'checked' at 6/1/2022, 7:22:56 PM; 'You' (green bubble) says 'hello' at 6/1/2022, 8:11:54 PM; 'You' (green bubble) says 'check report' at 6/1/2022, 7:21:58 PM; and 'You' (green bubble) says 'sathwik' at 6/1/2022, 5:50:58 PM. At the bottom, there's a 'Send Message' input field and a 'Send' button. The top right corner shows 'Signed in as: Rishi'.

Fig 4.8 The chat application for communication between doctors and patients

Metamask Transaction

This is the transaction done in metamask when a patient revokes access where patient is charged in ethereum.

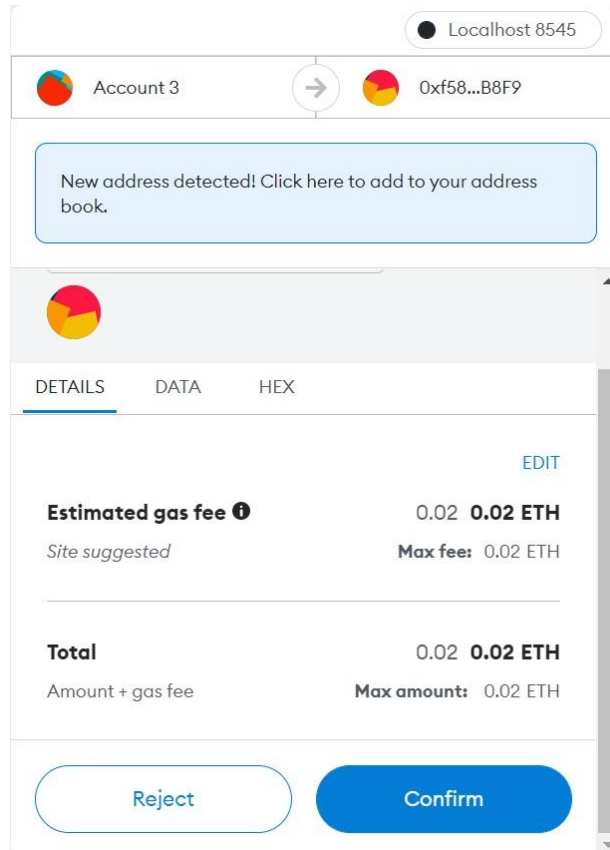


Fig 4.9 Metamask pop-up to authorize a transaction to revoke access to a doctor

Chapter 5

Conclusion

Adopting the Blockchain to deploy the EHR solves the significant issues of accessibility and authority. The Blockchain allows ease of access to the records as it is available to any personnel authorized to access them. Since it is deployed on a Distributed network, it can be accessed from anywhere. However, there are a few issues that could still be addressed in the future. Since it is possible to distinguish the people engaged in the transactions, this could endanger their confidentiality and secrecy. Although certain blockchains offer absolute anonymity, some sensitive details should clearly not be distributed in this way.

5.1 Future work

Including more features to the dApp where patient can give read-only access and doctor can request the access from patient.

Improving chat application functionalities to allow transfer of files,images.

The system can be improved by allowing the medical records to be accessed quickly during emergencies. Its structure could be modified to fit a specific disease or modeled on established standards.

Appendices

Code for giving access

```
function permit_access(address addr) payable public {  
  
    //require(msg.value == 0.02 ether);  
  
    creditPool += 2;  
  
    doctorInfo[addr].patientAccessList.push(msg.sender)-1;  
  
    patientInfo[msg.sender].doctorAccessList.push(addr)-1;  
  
}
```

Code for registering new user

```
function add_agent(string memory _name, uint _age, uint _designation, string  
memory _hash) public returns(string memory){  
  
    address addr = msg.sender;  
  
    if(_designation == 0){  
  
        patient memory p;  
  
        p.name = _name;  
  
        p.age = _age;  
  
        p.record = _hash;  
  
        patientInfo[msg.sender] = p;  
  
        patientList.push(addr)-1;  
  
        return _name;  
  
    }
```

```

else if (_designation == 1){

    doctorInfo[addr].name = _name;

    doctorInfo[addr].age = _age;

    doctorList.push(addr)-1;

    return _name;

}

else{

    revert();

}

}

```

Revoke access

```

function revoke_access(address daddr) public payable{

    remove_patient(msg.sender,daddr);

    creditPool -= 2;

}

```

References

1. Akarca D, and Xiu PY, Ebbitt D, Mustafa B, Al-Ramadhani H, Albeyatti A, "Blockchain Secured Electronic Health Records: Patient Rights, Privacy and Cybersecurity," 2019
2. B. L. Radhakrishnan, A. S. Joseph and S. Sudhakar, "Securing Blockchain based Electronic Health Record using Multilevel Authentication," 2019
3. M. Abdulaziz, D. Çulha and A. Yazici, "A Decentralised Application for Secure Messaging in a Trustless Environment," 2018
4. N. Poonguzhali, S. Gayathri, A. Deebika and R. Suriapriya, "A Framework For Electronic Health Record Using Blockchain Technology," 2020
5. S. Alexaki, G. Alexandris, V. Katos and N. E. Petroulakis, "Blockchain-based Electronic Patient Records for Regulated Circular Healthcare Jurisdictions," 2018
6. U. P. Ellewala, W. D. H. U. Amarasena, H. V. S. Lakmali, L. M. K. Senanayaka and A. N. Senarathne, "Secure Messaging Platform Based on Blockchain," 2020
7. V. B, S. N. Dass, S. R and R. Chinnaiyan, "A Blockchain based Electronic Medical Health Records Framework using Smart Contracts," 2021
8. V. M. Harshini, S. Danai, H. R. Usha and M. R. Kounte, "Health Record Management through Blockchain Technology," 2019