

A blockchain-based approach for securing Electronic Hospital Records

MSc Research Project
Cyber Security

Geetesh Vaswani
Student ID: X20194102

School of Computing
National College of Ireland

Supervisor: Mr. Ross Spelman

National College of Ireland
MSc Project Submission Sheet
School of Computing



Student Name: Geetesh Vaswani
Student ID: X20194102
Programme: MSc in Cybersecurity **Year:** 2021-22
Module: MSc Research Project
Supervisor: Mr. Ross Spelman
Submission Due Date: 15 December 2022
Project Title: A blockchain-based approach for securing Electronic Hospital Records
Word Count: 558
Page Count: 11

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Geetesh Vaswani

Date: 15 December 2022

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

| | |
|---|--------------------------|
| Attach a completed copy of this sheet to each project (including multiple copies) | <input type="checkbox"/> |
| Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies). | <input type="checkbox"/> |
| You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. | <input type="checkbox"/> |

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

| | |
|----------------------------------|--|
| Office Use Only | |
| Signature: | |
| Date: | |
| Penalty Applied (if applicable): | |

Configuration Manual

Geetesh Vaswani
X20194102

1 Introduction

This document is the configuration manual submitted as the supporting document for blockchain based approach of electronic health records. Documentation of all the steps taken to develop the model, the analysis and the hardware-software configuration is detailed in this document.

2 System Configuration

2.1 Hardware configuration

The Development and testing were done on a windows laptop, with the details of the hardware listed below.

| Feature | Description |
|--------------------|--|
| Operating System | Windows 10 version 22H2, November 2022 patch |
| System information | 64-bit |
| Processor | Intel i3 6 th gen with integrated radeon graphics |
| Memory | 8GB |
| Storage | 548GB OS drive, 2 x 191GB data drive |

2.2 Software configuration and requirements

The coding platform was setup on VScode (v1.73.0).
Nodejs (v18.12.1)
Ganache (v2.5.4)
Metamask chrome extension (v10.23.0)
Open Command prompt in project folder and install npm.

Run – “npm install –force”

Steps to run:

-Open command prompt as admin and install truffle.

Run – “npm install -g truffle”

```
Microsoft Windows [Version 10.0.19043.2130]
(c) Microsoft Corporation. All rights reserved.

C:\Users\vaswa>npm install -g truffle
npm WARN deprecated @types/keyv@4.2.0: This is a stub types definition. keyv provides its own type definitions, so you do not need this installed.
npm WARN deprecated mkdirp-promises@5.0.1: This package is broken and no longer maintained. 'mkdirp' itself supports promises now, please switch to that.
npm WARN deprecated har-validator@5.1.5: this library is no longer supported
npm WARN deprecated multicodec@1.0.4: This module has been superseded by the multiformats module
npm WARN deprecated uuid@2.0.1: Please upgrade to version 7 or higher. Older versions may use Math.random() in certain circumstances, which is known to be problematic. See https://v8.dev/blog/math-random for details.
npm WARN deprecated request@2.88.2: request has been deprecated, see https://github.com/request/request/issues/3142
npm WARN deprecated multibase@0.6.1: This module has been superseded by the multiformats module
npm WARN deprecated uuid@3.4.0: Please upgrade to version 7 or higher. Older versions may use Math.random() in certain circumstances, which is known to be problematic. See https://v8.dev/blog/math-random for details.
npm WARN deprecated uuid@3.3.2: Please upgrade to version 7 or higher. Older versions may use Math.random() in certain circumstances, which is known to be problematic. See https://v8.dev/blog/math-random for details.
npm WARN deprecated multibase@0.7.0: This module has been superseded by the multiformats module
npm WARN deprecated multicodec@0.5.7: This module has been superseded by the multiformats module
npm WARN deprecated cids@0.7.5: This module has been superseded by the multiformats module

added 749 packages, and audited 785 packages in 5m

36 packages are looking for funding
  run `npm fund` for details

9 moderate severity vulnerabilities

To address issues that do not require attention, run:
```

Fig 1.1: Install truffle.

-Next install yarn.

```
Microsoft Windows [Version 10.0.19043.2130]
(c) Microsoft Corporation. All rights reserved.

C:\Users\vaswa>npm install -g yarn

added 1 package, and audited 2 packages in 7s

found 0 vulnerabilities
npm notice
npm notice New patch version of npm available! 8.19.2 -> 8.19.3
npm notice Changelog: https://github.com/npm/cli/releases/tag/v8.19.3
npm notice Run npm install -g npm@8.19.3 to update!
npm notice

C:\Users\vaswa>npm install -g npm@8.19.3

added 1 package, and audited 212 packages in 21s

11 packages are looking for funding
  run `npm fund` for details

found 0 vulnerabilities

C:\Users\vaswa>npm config get prefix
C:\Users\vaswa\AppData\Roaming\npm

C:\Users\vaswa>
```

Fig 1.2: Install yarn

```

Microsoft Windows [Version 10.0.19043.2130]
(c) Microsoft Corporation. All rights reserved.

C:\Users\vaswa>npm install -g yarn

added 1 package, and audited 2 packages in 7s

found 0 vulnerabilities
npm notice
npm notice New patch version of npm available! 8.19.2 -> 8.19.3
npm notice Changelog: https://github.com/npm/cli/releases/tag/v8.19.3
npm notice Run npm install -g npm@8.19.3 to update!
npm notice

C:\Users\vaswa>npm install -g npm@8.19.3

added 1 package, and audited 212 packages in 21s

11 packages are looking for funding
  run `npm fund` for details

found 0 vulnerabilities

C:\Users\vaswa>npm config get prefix
C:\Users\vaswa\AppData\Roaming\npm

C:\Users\vaswa>

```

Fig1.3: Yarn and npm install

-Create new workspace in ganache and new project and select truffle-config.js in project folder and save the workspace.

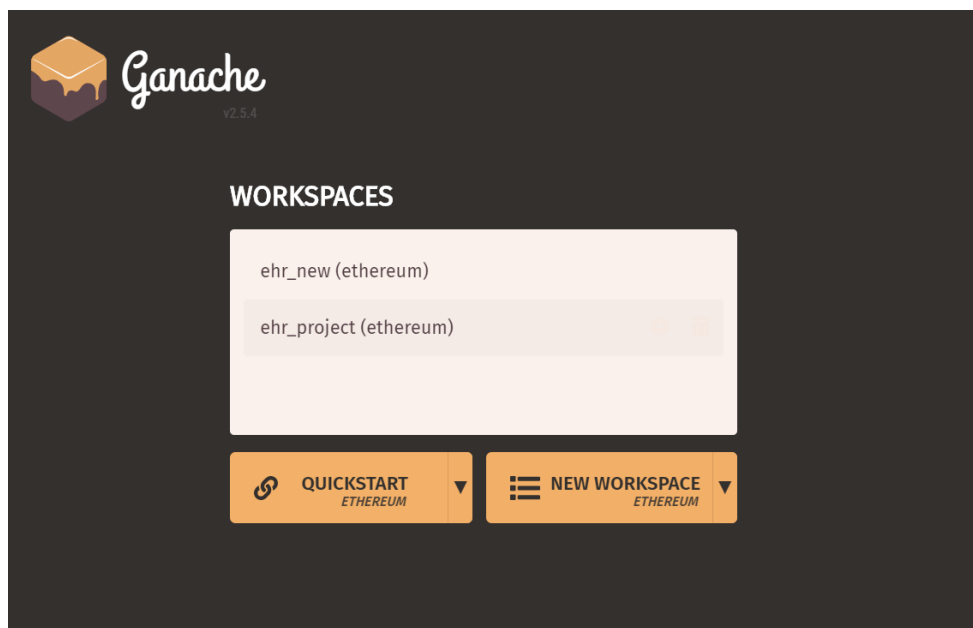


Fig 1.4: Ganache setup

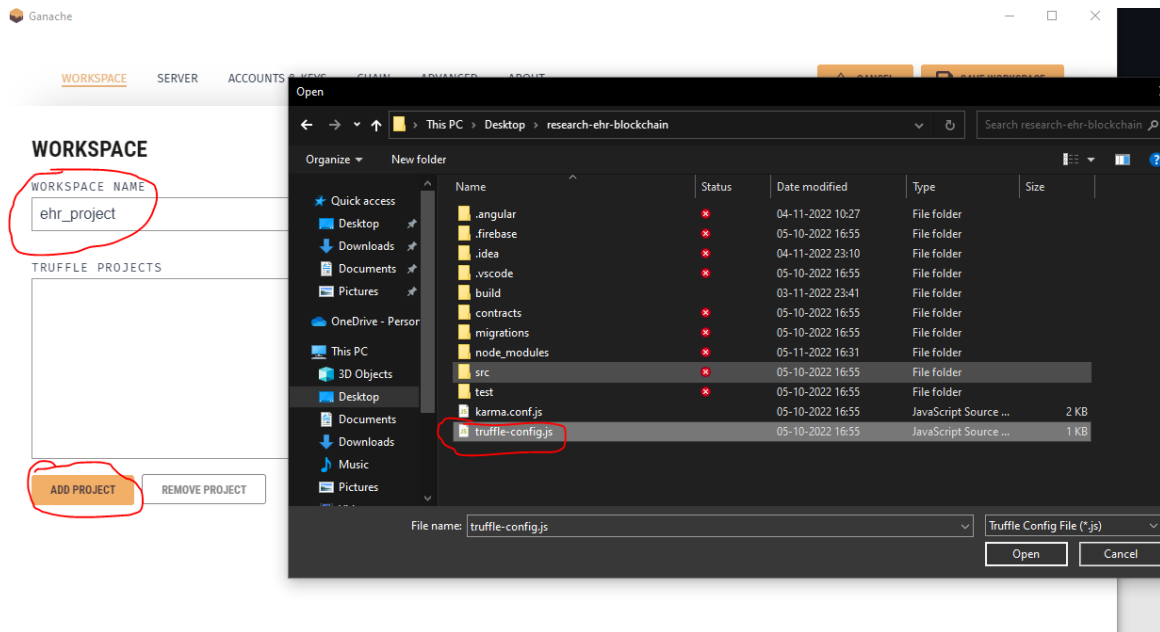


Fig1.5: Add project

-Open Command prompt again and migrate truffle.

```

Administrator: C:\WINDOWS\system32\cmd.exe
dity\dist\compilerSupplier\loadingStrategies\VersionRange.js:6:42)
  at processTicksAndRejections (node:internal/process/task_queues:95:5)
Truffle v5.6.4 (core: 5.6.4)
Node v18.12.0

C:\Users\vaswa\OneDrive\Desktop\research-ehr-blockchain>truffle migrate

Compiling your contracts...
> Compiling .\contracts\Contract.solc-bin. Attempt #1
> Compiling .\contracts\Migrations.sol
> Compiling .\contracts\Roles.sol
> Artifacts written to C:\Users\vaswa\OneDrive\Desktop\research-ehr-blockchain\build\contracts
> Compiled successfully using:
  - solc: 0.8.11+commit.d7f03943.Emscripten.clang
  _ Fetching solc version list from solc-bin. Attempt #1
  _ Fetching solc version list from solc-bin. Attempt #1
Starting migrations... Attempt #1.
=====
> Network name:    'ganache'
> Network id:     5777
> Block gas limit: 6721975 (0x6691b7)

1_initial_migration.js
=====
  _ Fetching solc version list from solc-bin. Attempt #1
  Deploying 'Contract' Attempt #1.
  -----
  > transaction hash:    0xd56a7e256daf5e4ae041ebe69667672deff8215c58247713e20cd973adf9377

```

Fig1.6: Migrate contracts

```

=====
_ Fetching solc version list from solc-bin. Attempt #1
  Deploying 'Contract' Attempt #1.
  -----
  > transaction hash:      0xd56a7e256dacf5e4ae041ebe69667672deff8215c58247713e20cd973adf9377
  > Blocks: 0              Seconds: 0 |c-bin. Attempt #1
  > contract address:     0x5d14568642F302D0FeB1B4393395818f4Ca78fD7
  > block number:         1 |econds: 0
  > block timestamp:      1667518946
  > account:              0x8AD14699c72D170F9Fd6F544a8cBe59d469d08CF
  > balance:              99.98875256
  > gas used:             562372 (0x894c4)
  > gas price:            20 gwei
  > value sent:           0 ETH
  > total cost:           0.01124744 ETH

  > Saving artifacts
  -----
  > Total cost:           0.01124744 ETH

Summary
=====
> Total deployments:    1
> Final cost:           0.01124744 ETH

```

Fig1.7: migrate complete

Run the development server by running the code

```

C:\Users\waswa\OneDrive\Desktop\research-ehr-blockchain>yarn start
yarn run v1.22.19
warning ..\..\..\package.json: No license field
$ ng serve
✓ Browser application bundle generation complete.

Initial Chunk Files                                         | Names
| Raw Size
vendor.js                                                   | vendor
| 4.06 MB |
polyfills.js                                               | polyfills
| 395.75 kB |
styles.css, styles.js                                     | styles
| 213.26 kB |
main.js                                                    | main
| 175.50 kB |
runtime.js                                                | runtime
| 12.79 kB |
| 4.84 MB | Initial Total

Lazy Chunk Files                                           | Names
| Raw Size
default-src, services, info, service, ts, src, utils, utils, module, ts, node, modules, angular, forms, fes-2ef177.js | admin-admin-mo

```

Fig1.8: yarn start

Open metamask extension and connect by inputting the same server settings as ganache:

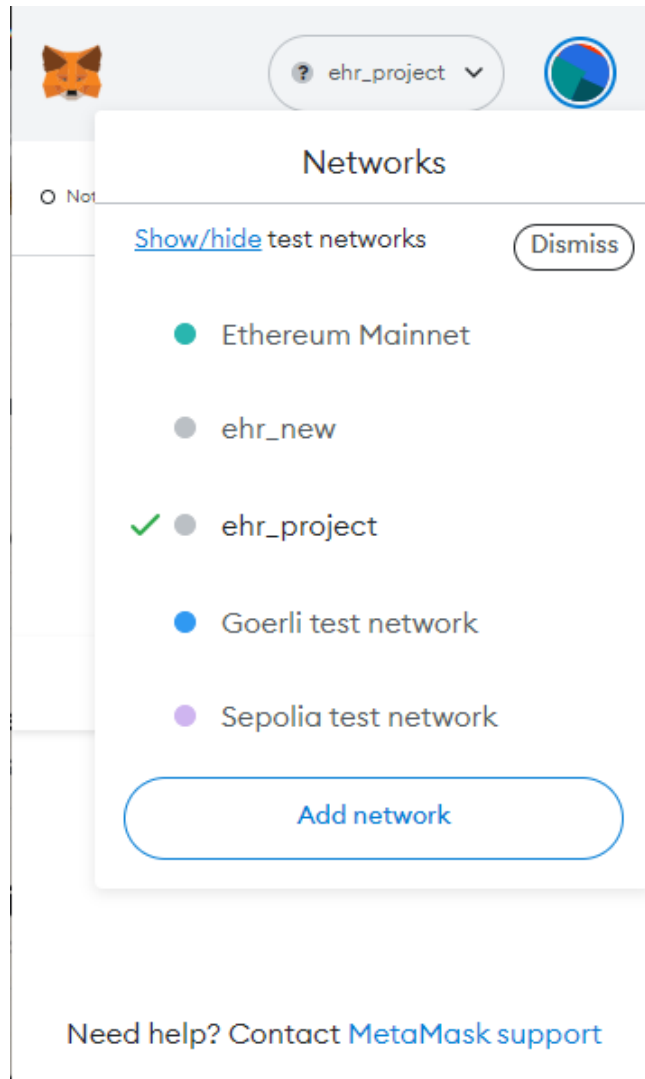


Fig 1.9: Metamask workspace

Import private key from ganache of one account to activate admin account:

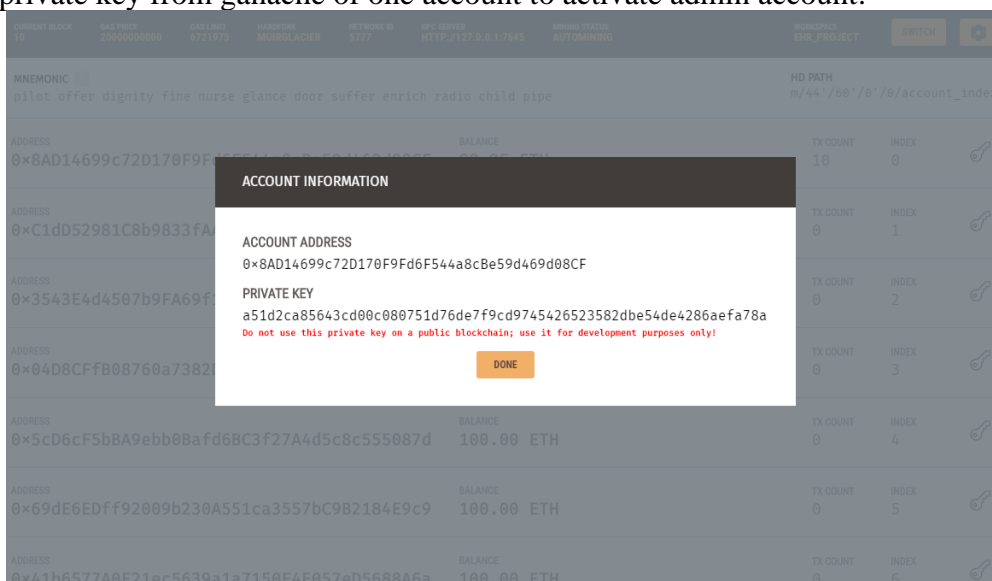


Fig1.10: Copy private key

Add the account and start browsing the website on the local host server.

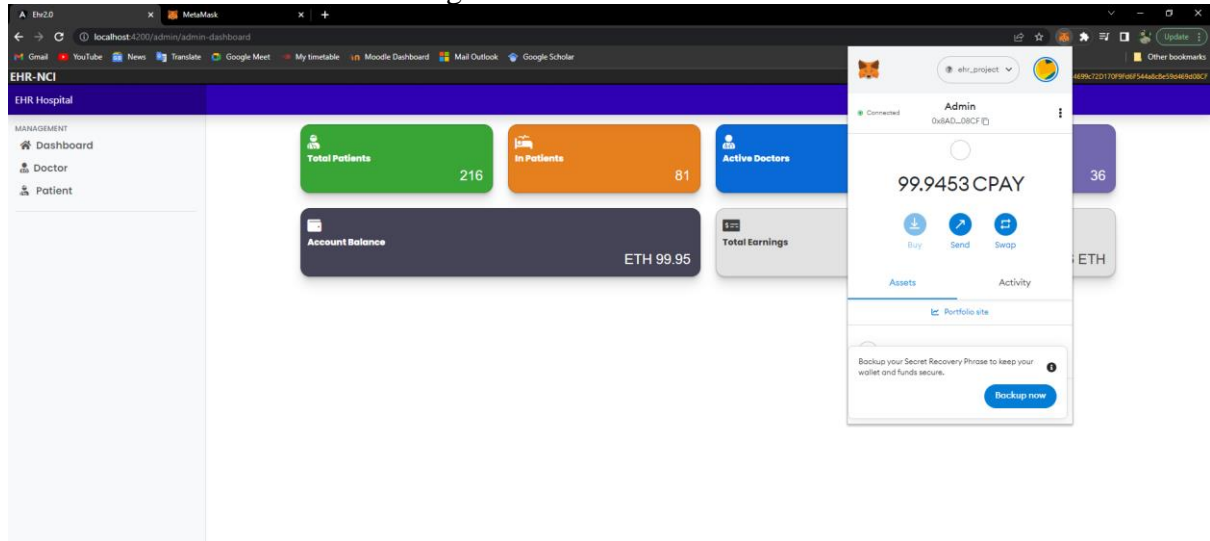


Fig1.11: admin has access to total number of users

- Users can book appointments from home page

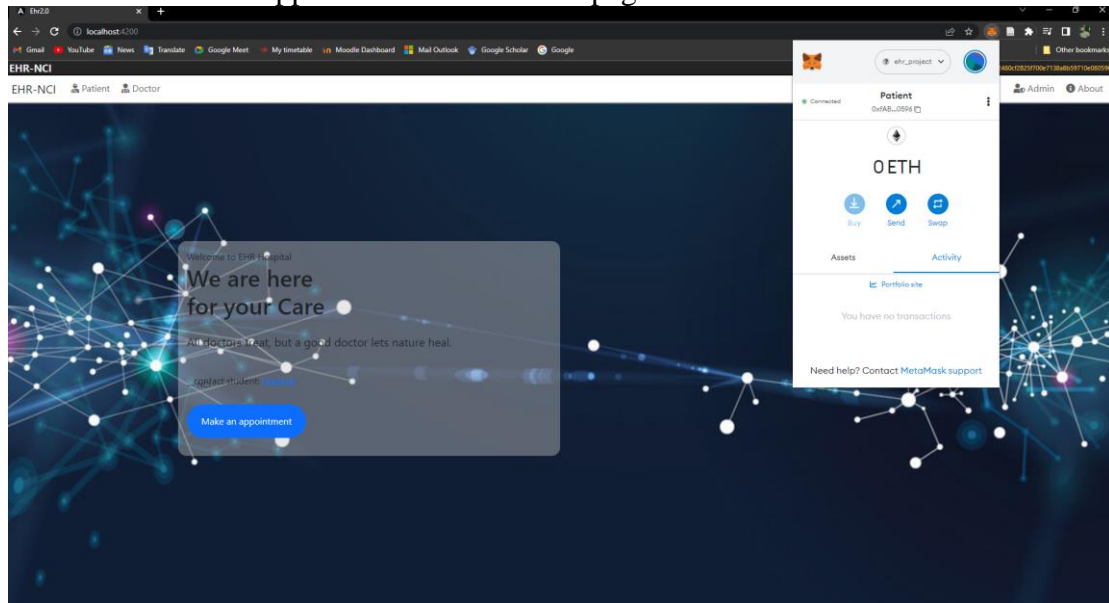


Fig 1.12: patient can book appointments

Patient and doctors do not have access to admin page:

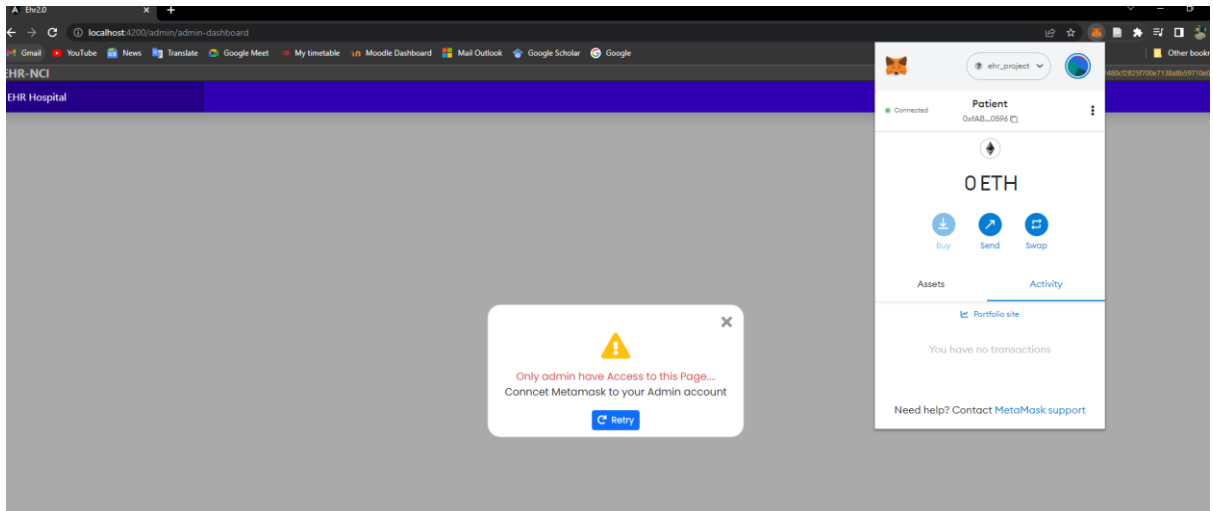


Fig 1.13: Access not granted

Only doctors have access to doctors page and to view shared records:

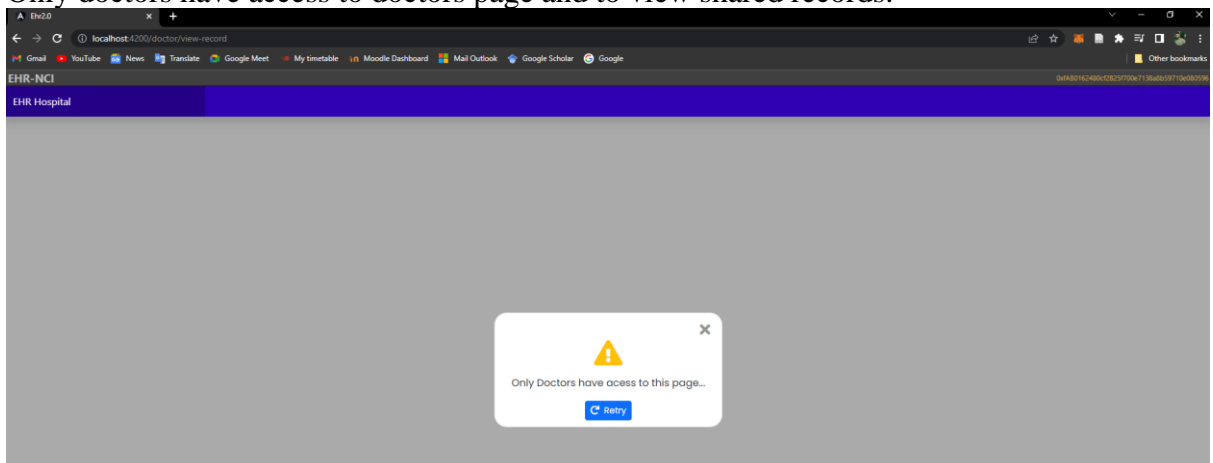


Fig 1.14: Doctors granted only

Blockchain transactions available in ganache:

| CURRENT BLOCK | GAS PRICE | GAS LIMIT | HARDFORK | NETWORK ID | RPC SERVER | MINING STATUS | WORKSPACE |
|--|------------|--|-------------|------------|-----------------------|---------------|-------------|
| 10 | 2000000000 | 6721975 | MUIRGLACIER | 5777 | HTTP://127.0.0.1:7545 | AUTOMINING | EHR_PROJECT |
| TX HASH | | | | | | | |
| 0x0bda8288c2486b425ab8a333e20811ec9d0c99720d86f28481f7b461b3ce631c | | | | | | | |
| FROM ADDRESS | | TO CONTRACT ADDRESS | | GAS USED | | VALUE | |
| 0x8AD14699c72D170F9Fd6F544a8cBe59d469d08CF | | Migrations | | 42290 | | 0 | |
| TX HASH | | | | | | | |
| 0x14728aab710be72558b6220a65b01d35c28bd9c6c6bd7c0e012a9ca46c0d786 | | | | | | | |
| FROM ADDRESS | | CREATED CONTRACT ADDRESS | | GAS USED | | VALUE | |
| 0x8AD14699c72D170F9Fd6F544a8cBe59d469d08CF | | 0x952c439093efdae7c222e0601fd3c47b2cf5b4F | | 153922 | | 0 | |
| TX HASH | | | | | | | |
| 0x356a7de96c72ea8027c37a1cbbf49f2e733fae5d0fbde442d527356ac0b3f5ef | | | | | | | |
| FROM ADDRESS | | CREATED CONTRACT ADDRESS | | GAS USED | | VALUE | |
| 0x8AD14699c72D170F9Fd6F544a8cBe59d469d08CF | | 0x5c51c976c693e6c2CF54c11586bd7987f9F280 | | 72217 | | 0 | |
| TX HASH | | | | | | | |
| 0xeec57f9e5cb24ba4d05b71fd735f7ea384cb285fd4543b18882a884664b09e8d | | | | | | | |
| FROM ADDRESS | | CREATED CONTRACT ADDRESS | | GAS USED | | VALUE | |
| 0x8AD14699c72D170F9Fd6F544a8cBe59d469d08CF | | 0x16A5e2331Af2aDa2d5D2E153eF0b6c98D0f314C7 | | 72217 | | 0 | |
| TX HASH | | | | | | | |
| 0x959a1cf2d05221627698559085ed891da0e7d67dcdc3c65a8aa38d88a8c6361 | | | | | | | |

Fig 1.15: Transactions

Contracts deployed:

The screenshot shows a blockchain explorer interface with a top navigation bar containing icons for ACCOUNTS, BLOCKS, TRANSACTIONS, CONTRACTS, EVENTS, and LOGS. Below the navigation bar, there are several data fields: CURRENT BLOCK (10), GAS PRICE (2000000000), GAS LIMIT (6721975), HARDFORK (MUIRGLACIER), NETWORK ID (5777), RPC SERVER (HTTP://127.0.0.1:7545), MINING STATUS (AUTOMINING), and WORKSPACE (EHR_PROJECT). A 'SEARCH FOR BLOCK NUMBERS OR TX HASHES' input field is also present. Below this, the path 'research-ehr-blockchain' is shown with its file location 'C:\Users\vaswa\OneDrive\Desktop\research-ehr-blockchain'. A table lists two deployed contracts:

| NAME | ADDRESS | TX COUNT | STATUS |
|------------|--|----------|----------|
| Contract | 0xf018B04A883224E973F6987150C6F479FF2B0b10 | 0 | DEPLOYED |
| Migrations | 0x952C439093efdae7c222e0601fD3cC47b2cf5b4F | 0 | DEPLOYED |

Fig 1.16: Contracts

Testing extensions were installed on google chrome:

The screenshot shows the Chrome extensions page with four extensions installed and enabled:

- Google Docs Offline 1.50.1**: Edit, create, and view your documents, spreadsheets, and presentations – all without internet access. ID: ghbmnjjoekpmoecnniinnbdlohkhi. Inspect views [background page \(Inactive\)](#).
- Load Testing in the Cloud from LoadFocu... 1.2.2**: Free Cloud Website and API Load Testing extension for creating and running free website and API load tests. ID: cehhldibjedpegllpigjckemnpkld.
- MetaMask 10.22.2**: An Ethereum Wallet in your Browser. ID: nkbihfbeogaeaoehlefnkodbefggknn. Inspect views [background.html](#).
- Selenium IDE 3.17.2**: Selenium Record and Playback tool for ease of getting acquainted with Selenium WebDriver. ID: mooikfkahbdckldjndioackbalphokd. Inspect views [background page](#).
- Zotero Connector 5.0.100**: Save references to Zotero from your web browser. ID: ekhagklcjbdpajgpjgmbionhlpdbjgc. Inspect views [background page](#).

Fig 1.17: Chrome extensions for testing

3 Conclusion

The steps shown above were successfully implemented to run the EHR system based on blockchain.