EHR dApp Report

(Electronics Health Record using ETH Blockchain)

HAMDAN ALKHOORI

ABSTRACT

Blockchain has been a captivating area of research for an extended period, offering numerous benefits that have been adopted by various industries. The healthcare sector, in particular, has the potential to greatly benefit from Blockchain technology due to its advantages in security, privacy, confidentiality, and decentralization. However, Electronic Health Record (EHR) systems face challenges related to data security, integrity, and management. In this essay, we will discuss how Blockchain technology can be utilized to transform EHR systems and provide a solution to these issues. We propose a framework that can be implemented in the healthcare sector for EHR, leveraging Blockchain technology. The primary goal of our framework is to incorporate Blockchain technology into EHR systems and ensure secure storage of electronic records by establishing granular access rules. Additionally, this framework addresses the scalability problem commonly faced by Blockchain technology through the utilization of off-chain storage for records. By implementing this framework, the EHR system can enjoy the benefits of a scalable, secure, and integrated Blockchain-based solution.

Index Terms: Blockchain, health records, electronic health records, decentralization, and measurability.

TABLE OF CONTENTS

I. INTRODUCTION

The rapid advancement of technology has had a profound impact on every aspect of human life, fundamentally changing the way we perceive and interact with the world. Just as technology has revolutionized various other sectors, it is now paving the way for advancements in the healthcare industry. Electronic Health Records (EHRs) have emerged as a significant development in this context. However, despite their numerous benefits, EHRs still encounter challenges pertaining to the security of medical records, user ownership of data, and data integrity, among others.

Blockchain technology provides a secure and transparent platform for storing medical records and other healthcare-related data. Prior to the advent of modern technology, the healthcare sector relied on paper-based systems for storing medical records, using manual documentation methods. This approach resulted in challenges related to data duplication and redundancy, as each institution the patient visited maintained multiple copies of their medical records. To address these issues, the healthcare sector transitioned towards Electronic Health Record (EHR) systems, which aimed to integrate paper-based and electronic medical records (EMR).

The goal of EHR systems is to address the challenges faced by paper-based healthcare records and provide an efficient system that can revolutionize the healthcare sector. EHR systems have been implemented in numerous hospitals worldwide due to the benefits they offer, particularly advancements in security and cost-effectiveness. They are considered a crucial component of the healthcare sector as they provide enhanced functionality and efficiency in healthcare operations.

1.1 STRUCTURE OF THESIS

1.2A. INTEROPERABILITY

The EHR system also encounters several other issues, including:

Interoperability is the process by which different data systems can exchange information and ensure that the data is usable for various purposes. In the context of EHR systems, an essential aspect is the Health Information Exchange (HIE) or data sharing functionality. However, due to the deployment of various EHR systems in different hospitals, there is a lack of universally defined standards in terms of terminologies and technical capabilities [6]. Furthermore, at a technical level, it is crucial that the exchanged medical records are interpretable, allowing the extracted information to be further utilized [6].

1.2B. INFORMATION ASYMMETRY

One of the significant challenges currently facing the healthcare sector, as highlighted by critics, is data asymmetry, which refers to one party having greater access to information compared to the other. This issue also affects EHR systems and the broader healthcare sector, as doctors or hospitals typically have centralized access to patient records. As a result, patients often face lengthy and cumbersome procedures when attempting to access their own medical records.

1.2C. DATA BREACHES

Data breaches in the healthcare sector highlight the need for a more robust platform. A study [7] analyzed data breaches in EHR systems and revealed that a staggering 173 million data entries have been compromised in these systems [8]. This demonstrates that hospitals have become targets of cyber-attacks, and the study observed an increasing trend in such incidents. Additionally, it is evident from the literature that many EHR systems fail to meet the needs and requirements of patients, leading to negative consequences in healthcare [2].

To address these issues, a suitable platform that can transform the healthcare sector into a patient-centered approach is needed, and Blockchain emerges as a promising solution. Blockchain provides security, transparency, and data integrity, making it an ideal choice for storing patients' medical records. This paper proposes a framework for a decentralized platform that securely stores patients' medical records and allows authorized individuals, including the patients themselves, to access the records.

Furthermore, our proposed work aims to tackle the aforementioned issues of data asymmetry and data breaches faced by EHR systems. The structure of this paper is as follows: Section II provides an overview of Blockchain technology and its dependencies, while Section III discusses the relevant existing work in this field.

1.2 AIM OF RESEARCH

1.3 A. BLOCKCHAIN TECHNOLOGIES AND DEPENDENCY

Blockchain technology was initially introduced by Nakamoto [13] for his groundbreaking work on digital currency or cryptocurrency, specifically Bitcoin. Nakamoto utilized blockchain to address the double spending problem in Bitcoin. However, this innovative technology soon found applications in various other domains. A blockchain is essentially a chain of interconnected blocks that continuously grows as transactions are stored on these blocks.

The distinguishing feature of this platform is its decentralized nature, allowing data to be distributed and shared among multiple participants. Each piece of distributed information, commonly referred to as data, has shared ownership. Transactions are grouped into batches and secured through hashing, and they are managed by peer-to-peer networks. Blockchain offers several advantages, including enhanced security, anonymity, and data integrity without the need for third-party intervention. These advantages make it an attractive option for storing patients' medical records, especially considering the increasing importance of technology in the healthcare industry.

Researchers have also identified the potential of utilizing blockchain technology in healthcare, as it can address the security concerns prevalent in the industry.

1.3 B . ARCHITECTURE

To comprehend the blockchain architecture, lets refer to use the subsequent figure, which illustrates an example of a blockchain and the block structure.

II. BLOCKCHAIN ARCHITECTURE

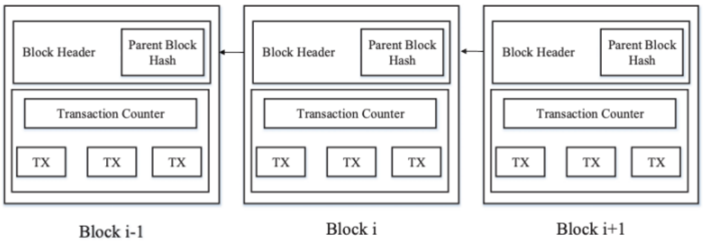


Fig. 1: An example of blockchain which consists of a continuous sequence of blocks.

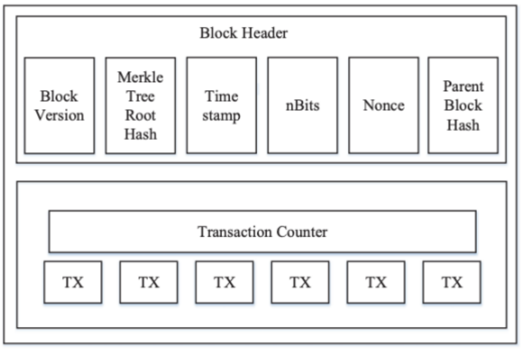


Fig. 2: Block structure

Blockchain is a sequence of blocks that functions as a decentralized and transparent public ledger. Figure 1 provides an illustration of a blockchain, showcasing its continuous sequence of blocks. Each block in the blockchain contains a reference to its parent block through the previous block hash. Additionally, in the Ethereum blockchain, the hashes of uncle blocks (children of a block's ancestors) are also stored. The very first block in a blockchain, known as the genesis block, does not have a parent block. Now, let's delve into the internal components of the blockchain in more detail.

A. Block

A block consists of two main parts: the block header and the block body, as depicted in Figure 2. The block header includes the following elements:

(i) Block version: Indicating the set of block validation rules to be followed.

(ii) Merkle tree root hash: A hash value representing all the transactions included in the block.

(iii) Timestamp: The current time in seconds since January 1, 1970, in universal time.

(iv) nBits: The target threshold for a valid block hash.

(v) Nonce: A 4-byte field that typically starts with 0 and increments for each hash calculation (explained further in Section III).

(vi) Parent block hash: A 256-bit hash value pointing to the previous block.

The block body consists of a transaction counter and the transactions themselves. The maximum number of transactions that a block can accommodate depends on the block size and the size of each transaction. Blockchain employs asymmetric cryptography, specifically digital signatures, to authenticate transactions. Each user possesses a private key and a corresponding public key. The private key is used to sign transactions, which are then broadcasted across the network. Digital signatures involve two phases: signing and verification. For instance, if user Alice wants to send a message to user Bob, (1) Alice encrypts her data with her private key and sends the encrypted result and original data to Bob. (2) In the verification phase, Bob validates the value using Alice's public key. This process enables Bob to determine if the data has been tampered with or not. The elliptic curve digital signature algorithm (ECDSA) is a commonly used digital signature algorithm in blockchains [17].

1.3 C. KEY FEATURES OF BLOCKCHAIN

1) DECENTRALIZATION

With blockchain, knowledge is distributed across the network instead of being stored at a central point. This decentralized nature of blockchain also extends to data management, which is collectively agreed upon by the nodes connected to the network. Unlike traditional systems where information is concentrated at a central point and managed by trusted entities, blockchain allows for a distributed and consensus-driven approach to data management.

2) DATA TRANSPARENCY

Achieving knowledge transparency in any technology relies on establishing a trust-based relationship between entities. The information or records stored on the blockchain are not centralized or controlled by a single node, but rather distributed across multiple nodes. This distributed nature of blockchain ensures that ownership of data is shared, resulting in increased transparency and enhanced security against third-party interventions. By removing the reliance on a central authority, blockchain technology enables a transparent and secure ecosystem for storing and managing data.

3) SECURITY AND PRIVACY

Blockchain technology utilizes cryptographic functions, such as the SHA-256 algorithm, to ensure security among the nodes connected on its network. By applying this algorithm to the hashes stored within the blocks, the integrity and immutability of the data are maintained. Transparency in data is achieved by fostering a trust-based relationship between entities. It is crucial to secure and safeguard the information or records involved. With blockchain, data is not centralized or controlled by a single node but is distributed across the network. This distributed nature of data ownership enhances transparency and provides security, protecting it from any unauthorized third-party intervention.

1.3E. CHALLENGES IN BLOCKCHAIN

1) SCALABILITY AND STORAGE CAPACITY

Storing information on the blockchain gives rise to two primary challenges: confidentiality and scalability. The nature of the blockchain makes the information visible to all participants on the chain, which compromises its confidentiality—a less desirable outcome for a decentralized platform. The data stored on the blockchain encompasses various patient medical records, including office results, X-ray reports, MRI results, and numerous other reports. With such voluminous data to be stored on the blockchain, scalability becomes a critical consideration.

2) LACK OF SOCIAL SKILLS

The workings of blockchain technology are currently understood by only a limited number of individuals. As a relatively new and evolving technology, blockchain is still in its early stages of development. Furthermore, transitioning from traditional trustworthy EHR systems to blockchain technology will require a significant amount of time, as hospitals and other healthcare institutions need to completely shift their existing systems to embrace blockchain.

3) LACK OF UNIVERSALLY DEFINED STANDARDS

Since blockchain technology is still in its early phases and constantly evolving, there is currently no well-defined standard for its implementation. Consequently, adopting this technology in the healthcare sector will also require additional time and effort. International authorities responsible for overseeing the standardization process of technologies, such as blockchain, would need to establish certified standards. These universal standards would play a crucial role in determining the data size, format, and types of information that can be stored on the blockchain. Furthermore, having well-defined standards would facilitate the adoption of blockchain technology within organizations, as they could easily implement and adhere to these established standards.

2. LITERATURE REVIEW

Blockchain technology, initially conceptualized by Nakamoto [13], was primarily designed as a cryptographically secure and decentralized currency for financial transactions. However, its application has expanded to various other domains, including the healthcare sector. Numerous researchers have conducted studies in this area, exploring the feasibility of using blockchain technology in healthcare and examining its associated advantages, threats, and challenges. These studies shed light on the potential benefits that can be derived from implementing blockchain in healthcare, as well as the issues and challenges that may arise when scaling up its usage.

2.1. THEORETICAL/ANALYTICAL RESEARCH

Bitcoin is a peer-to-peer distributed network used for conducting Bitcoin transactions. It operates through a proof-of-work consensus algorithm and utilizes the concept of blockchain mining. The authors also discuss important concepts related to operating systems and their connection to Bitcoin. Furthermore, they explore the potential of smart contracts in parallel blockchains, highlighting their role in achieving decentralization. In addition, the authors provide an explanation of the various layers of blockchain that work together to maintain the system's integrity.

2.2. PROTOTYPE / IMPLEMENTATION RESEARCH

Sahoo and Baruah [24] proposed a scalable framework to address the scalability issue in blockchain. They suggested leveraging the scalability offered by the underlying Hadoop infrastructure. In their approach, blocks are stored on the Hadoop system, while the blockchain built on top of this framework incorporates all the necessary blockchain dependencies. This storage arrangement on Hadoop enhances the scalability of the blockchain technology. To tackle the scalability challenges, the study recommends using the Hadoop data system along with SHA3-256 for hashing transactions and blocks.

The language used in this study helps understand how blockchain can be employed with other scalable platforms to enhance or resolve scalability issues. Another key feature of the proposed system is the validation process, which involves first validating the fixed-format correctness and then parsing the data to differentiate personal and specific information related to form operating systems and other essential concepts.

The authors also discuss the utilization of smart contracts in parallel blockchains, highlighting their benefits in terms of decentralization. They explain the various layers of a blockchain system, including data, network, consensus, and smart contracts. The paper not only explores the design and framework of smart contracts but also provides insights into their applications and challenges. Furthermore, it discusses an important future trend of parallel blockchains aiming to optimize two different yet crucial modules.

In a related work, [25] proposed a scalable solution that complies with the Office of the National Coordinator for Health Information Technology (ONC) standards. The challenges addressed in this technology primarily revolve around privacy, security, and scalability concerns associated with the transmission of massive volumes of datasets on this platform. However, there is currently no universally implemented standard for demonstrating a decentralized application (DAPP) based on the ONC requirements. The authors also shared the lessons learned and highlighted the security issues related to electronic health record (EHR) systems.

Additionally, [26] developed a system for managing medical questionnaires with the goal of data sharing and storage for medical and clinical research purposes. They emphasized the system's potential benefits in the development of EHR systems and addressed the associated security concerns.

3. APPROACH

3.1. SYSTEM DESIGN

A system was also chosen to be the foundation for the planned framework. This study contains two main functions: creating, storing, and sharing questionnaire data. One of the benefits of the system is the validation process, where the added data is first validated to ensure it follows the correct fixed format. It is then parsed to differentiate personal and specific information associated with the form. The graphical user interface (GUI) includes all the functions that can be accessed by the user based on their assigned role. Users can interact with other layers of the system through this GUI.

3.2. BLOCKCHAIN LAYER

The next layer in the system is the blockchain layer, which includes the code or mechanism for user interaction with the decentralized application (DAPP) running on the blockchain. This layer facilitates external users in updating the state of the record or data stored on the Ethereum blockchain network. These transactions are treated as assets within the Ethereum blockchain, as they consist of data that users can send to one another or store for their own use.

3.3. SYSTEM IMPLEMENTATION

As mentioned earlier in the preceding sections, the system was implemented utilizing the Ethereum blockchain and its associated dependencies. This section delves into the implementation of the system to provide a deeper understanding of its various functions.

3.4. SMART CONTARCTS

As mentioned previously, smart contracts play a crucial role in DAPPs as they are responsible for executing fundamental operations. The following contracts are included in this framework:

1. Patient Records: This smart contract focuses specifically on performing CRUD (Create, Read, Update, Delete) operations on patient records. It also defines roles to control access to these functions.
2. Roles: The second contract mentioned, named "Roles," is a predefined smart contract from the OpenZeppelin smart contract library. This library comprises multiple smart contracts that perform various functionalities. The reason for using this library was to leverage its benefits, such as pre-tested and commonly used contracts, ultimately enhancing the reliability and security of the system.

Additionally, it's worth noting that the Asset library, which is a sub-library of the OpenZeppelin library, was also utilized in this framework.

4. TESTING

4.1. ALGORITHM RULE

The first algorithm explains the functionalities of the smart contract related to defining roles and performing operations such as adding, viewing, updating, and deleting records.

This list of functionalities will soon be utilized to access the roles assigned to the recorded data. The assignment of roles to doctors is performed by the administrator. Additionally, this function ensures that the task is being executed by the genuine public address of the doctor's account and not by any unauthorized third party. In programming language, specifically Solidity, the term 'msg.sender' is used to indicate the address making the changes to the patient's saved records.

The validation process is repeated to ensure that only authorized users can access this function. The final function defined in algorithm one is 'delete patient records', which, as the name suggests, is responsible for deleting records. This function requires the unique ID associated with the record to be deleted.

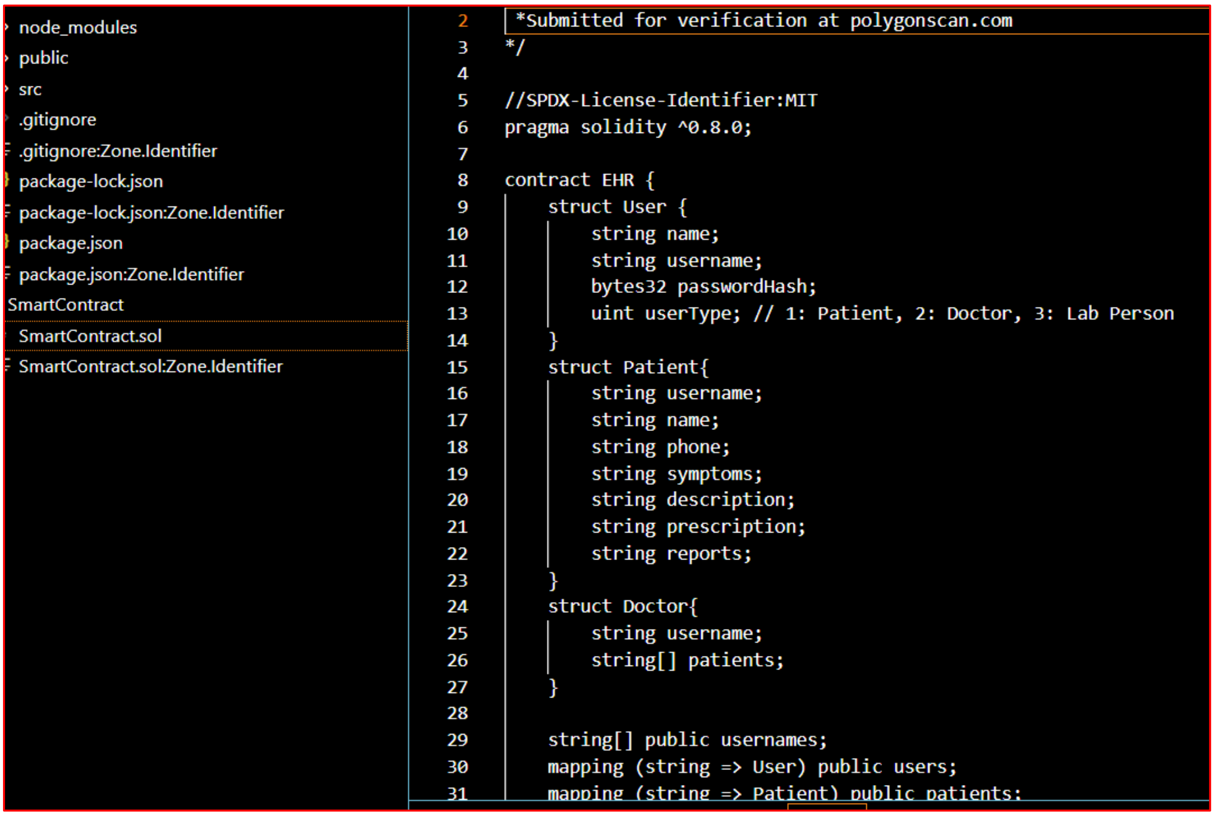
5. PROPOSED PROJECT

5.1. FRAMEWORK

In this project, there are three types of users: Patients, Doctors, and Labs. Patients will first register with the application, create their profiles, and grant access to doctors.

- Doctors will register with the application, log in, and gain access to the records of patients who have granted them permission. The doctor will have the ability to add prescriptions to the patient's profile.
- Lab personnel will log in to the application using the username 'Lab' and password 'Lab'. After successful login, they will be able to upload reports for patients.
- Patients can log in to the application and have the option to download or view their reports. They can filter the reports based on criteria such as viewing all reports or sorting them by date.

In this project author describe concept to store patient medical records using block chain technology as its provide inbuilt support to secure data store in it. To store details we are using the block chain ETHEREUM tool and using below code we generate solidity program:


node_modules
public
src
.gitignore
.gitignore:Zone.Identifier
package-lock.json
package-lock.json:Zone.Identifier
package.json
package.json:Zone.Identifier
SmartContract
SmartContract.sol
SmartContract.sol:Zone.Identifier

```
 *Submitted for verification at polygonscan.com
*/

//SPDX-License-Identifier:MIT
pragma solidity ^0.8.0;

contract EHR {
    struct User {
        string name;
        string username;
        bytes32 passwordHash;
        uint userType; // 1: Patient, 2: Doctor, 3: Lab Person
    }
    struct Patient{
        string username;
        string name;
        string phone;
        string symptoms;
        string description;
        string prescription;
        string reports;
    }
    struct Doctor{
        string username;
        string[] patients;
    }

    string[] public usernames;
    mapping (string => User) public users;
    mapping (string => Patient) public patients;
```

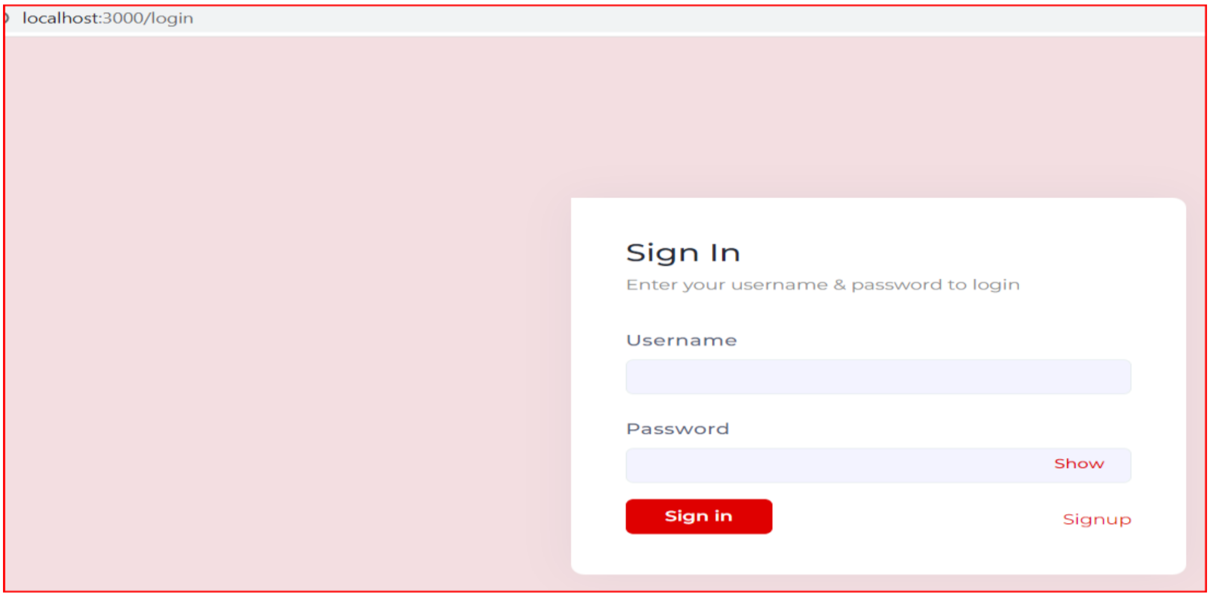
In above code snippet, functions are defined to store patient, doctors and prescription with report detailsS.

5.2 SOFTWARE INSTALLATION

Use following instructions to install nodejs software and then start it with blockchain.

- To implement EHR DAPP on localhost, you need to do following steps:
    - Download NodeJS here, and Install it.
    - Open frontend-ehr-dapp folder in command prompt or terminal
    - Run following commands npm install OR npm install --force npm start

- ○ Ensure you have installed the metamasks in the browsers and add some eth for accessing and authentications the transications.
- ○ It will automatically open the project in your default browser as below

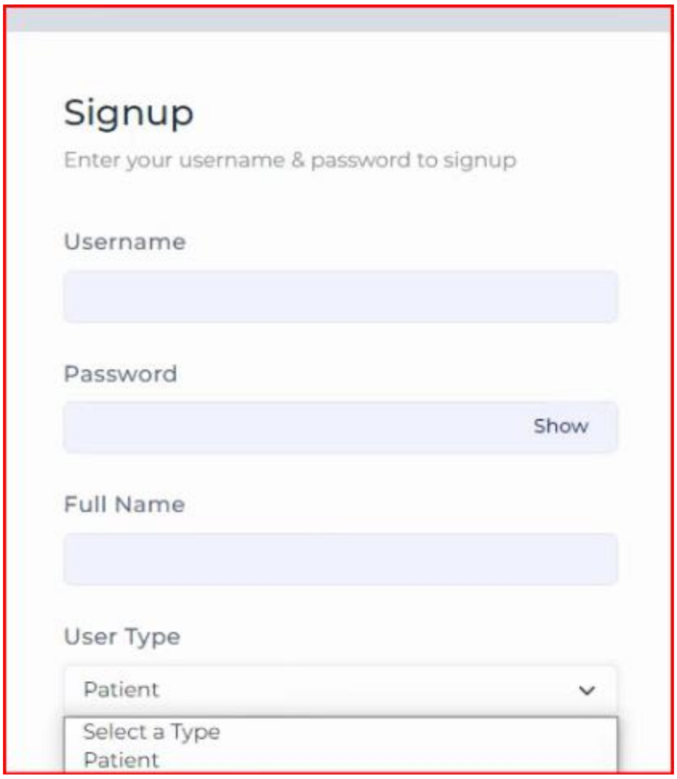


localhost:3000/login

Sign In

Enter your username & password to login

- Download the nodejs software and extract it and once you started it would be showing below screen in the browsers.



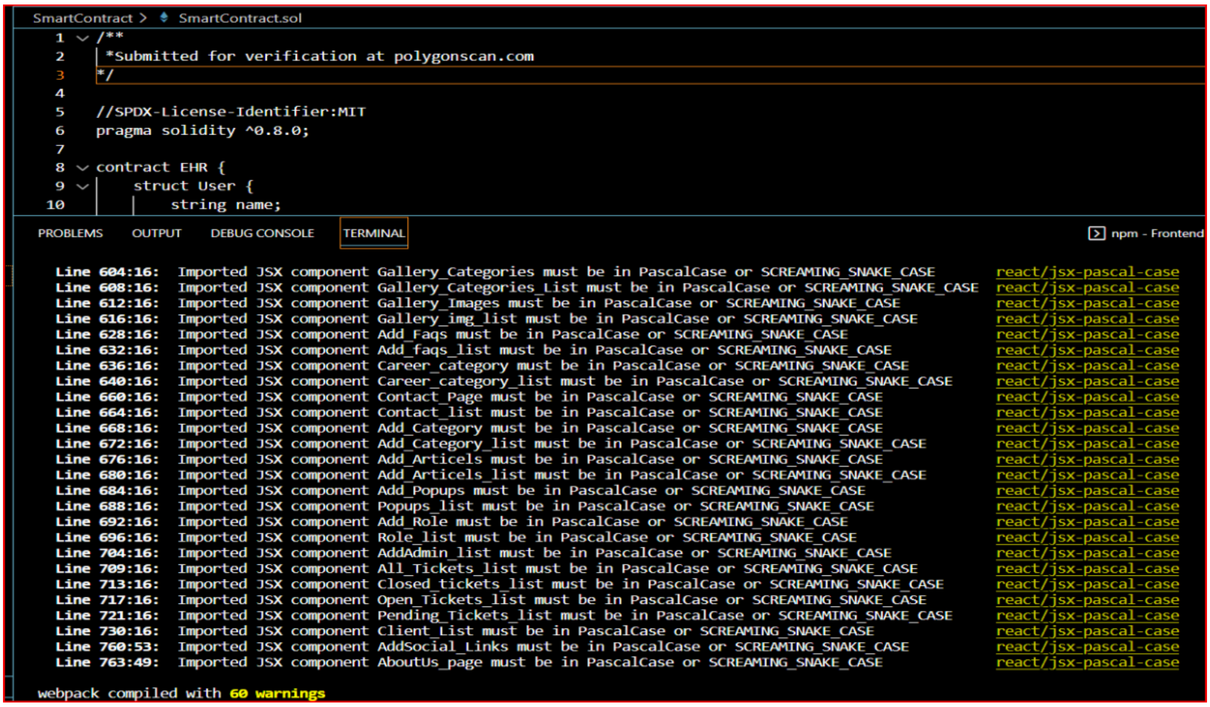
Signup

Enter your username & password to signup

User Type: Patient

To add the smart contract and codes, please follow these steps:

1. Download all the code files to a specific directory on your system.
2. Navigate to the directory where the code files are located.
3. Run the Node.js or npm start command in the command line or terminal to initiate the execution of the code.
4. After running the code, you should receive a message indicating that the smart contract has been deployed successfully.



```
/**
 *Submitted for verification at polygonscan.com
*/

//SPDX-License-Identifier:MIT
pragma solidity ^0.8.0;

contract EHR {
    struct User {
        string name;
```

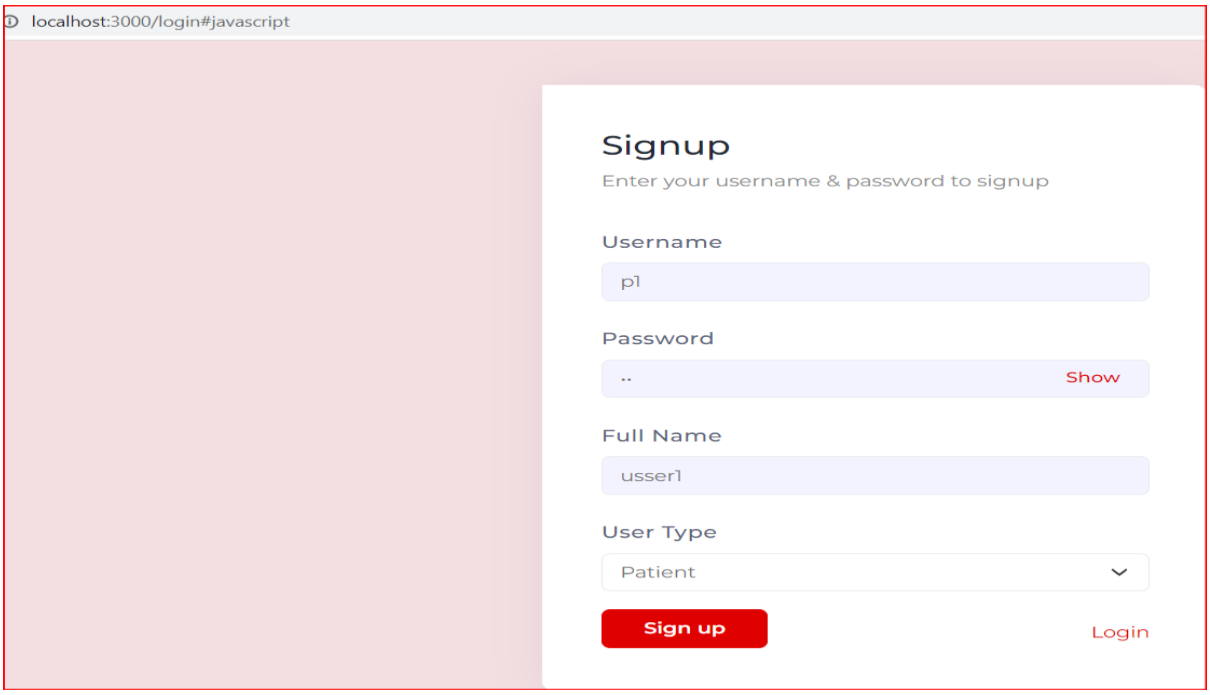
```
  Line 604:16:  Imported JSX component Gallery_Categories must be in PascalCase or SCREAMING_SNAKE_CASE       react/jsx-pascal-case
  Line 608:16:  Imported JSX component Gallery_Categories_List must be in PascalCase or SCREAMING_SNAKE_CASE  react/jsx-pascal-case
  Line 612:16:  Imported JSX component Gallery_Images must be in PascalCase or SCREAMING_SNAKE_CASE           react/jsx-pascal-case
  Line 616:16:  Imported JSX component Gallery_img_list must be in PascalCase or SCREAMING_SNAKE_CASE         react/jsx-pascal-case
  Line 628:16:  Imported JSX component Add_Faqs must be in PascalCase or SCREAMING_SNAKE_CASE                 react/jsx-pascal-case
  Line 632:16:  Imported JSX component Add_faqs_list must be in PascalCase or SCREAMING_SNAKE_CASE            react/jsx-pascal-case
  Line 636:16:  Imported JSX component Career_category must be in PascalCase or SCREAMING_SNAKE_CASE          react/jsx-pascal-case
  Line 640:16:  Imported JSX component Career_category_list must be in PascalCase or SCREAMING_SNAKE_CASE     react/jsx-pascal-case
  Line 660:16:  Imported JSX component Contact_Page must be in PascalCase or SCREAMING_SNAKE_CASE             react/jsx-pascal-case
  Line 664:16:  Imported JSX component Contact_list must be in PascalCase or SCREAMING_SNAKE_CASE             react/jsx-pascal-case
  Line 668:16:  Imported JSX component Add_Category must be in PascalCase or SCREAMING_SNAKE_CASE             react/jsx-pascal-case
  Line 672:16:  Imported JSX component Add_Category_list must be in PascalCase or SCREAMING_SNAKE_CASE        react/jsx-pascal-case
  Line 676:16:  Imported JSX component Add_Articels must be in PascalCase or SCREAMING_SNAKE_CASE             react/jsx-pascal-case
  Line 680:16:  Imported JSX component Add_Articels_list must be in PascalCase or SCREAMING_SNAKE_CASE        react/jsx-pascal-case
  Line 684:16:  Imported JSX component Add_Popups must be in PascalCase or SCREAMING_SNAKE_CASE               react/jsx-pascal-case
  Line 688:16:  Imported JSX component Popups_list must be in PascalCase or SCREAMING_SNAKE_CASE              react/jsx-pascal-case
  Line 692:16:  Imported JSX component Add_Role must be in PascalCase or SCREAMING_SNAKE_CASE                 react/jsx-pascal-case
  Line 696:16:  Imported JSX component Role_list must be in PascalCase or SCREAMING_SNAKE_CASE                react/jsx-pascal-case
  Line 704:16:  Imported JSX component AddAdmin_list must be in PascalCase or SCREAMING_SNAKE_CASE            react/jsx-pascal-case
  Line 709:16:  Imported JSX component All_Tickets_list must be in PascalCase or SCREAMING_SNAKE_CASE         react/jsx-pascal-case
  Line 713:16:  Imported JSX component Closed_tickets_list must be in PascalCase or SCREAMING_SNAKE_CASE      react/jsx-pascal-case
  Line 717:16:  Imported JSX component Open_Tickets_list must be in PascalCase or SCREAMING_SNAKE_CASE        react/jsx-pascal-case
  Line 721:16:  Imported JSX component Pending_Tickets_list must be in PascalCase or SCREAMING_SNAKE_CASE     react/jsx-pascal-case
  Line 730:16:  Imported JSX component Client_List must be in PascalCase or SCREAMING_SNAKE_CASE              react/jsx-pascal-case
  Line 760:53:  Imported JSX component AddSocial_Links must be in PascalCase or SCREAMING_SNAKE_CASE          react/jsx-pascal-case
  Line 763:49:  Imported JSX component AboutUs_page must be in PascalCase or SCREAMING_SNAKE_CASE             react/jsx-pascal-case

webpack compiled with 60 warnings
```

After getting that message follow the instructions below to run code, then open browser and enter the URL as ***http://localhost:3000/login#javascript*** to get above screen

5.3 WORKING IN PROPOSED FRAMEWORK

As mentioned in the previous section, we have implemented functions using Ethereum. When we refer to the block time, we are talking about the time it takes for a new block to be added. In the case of smart contracts, the confirmation time for a transaction is approximately 38 seconds, depending on the gas price set for the transaction. Unlike Bitcoin, Ethereum does not have a block size limit; instead, it has a gas limit.

The time taken for an append operation in the first rule, such as adding a patient record, would be around 1-2 minutes, depending on the data size. For retrieval operations, like the read patient record function in rule one, it would take approximately 50 seconds.



localhost:3000/login#javascript

Signup

Enter your username & password to signup

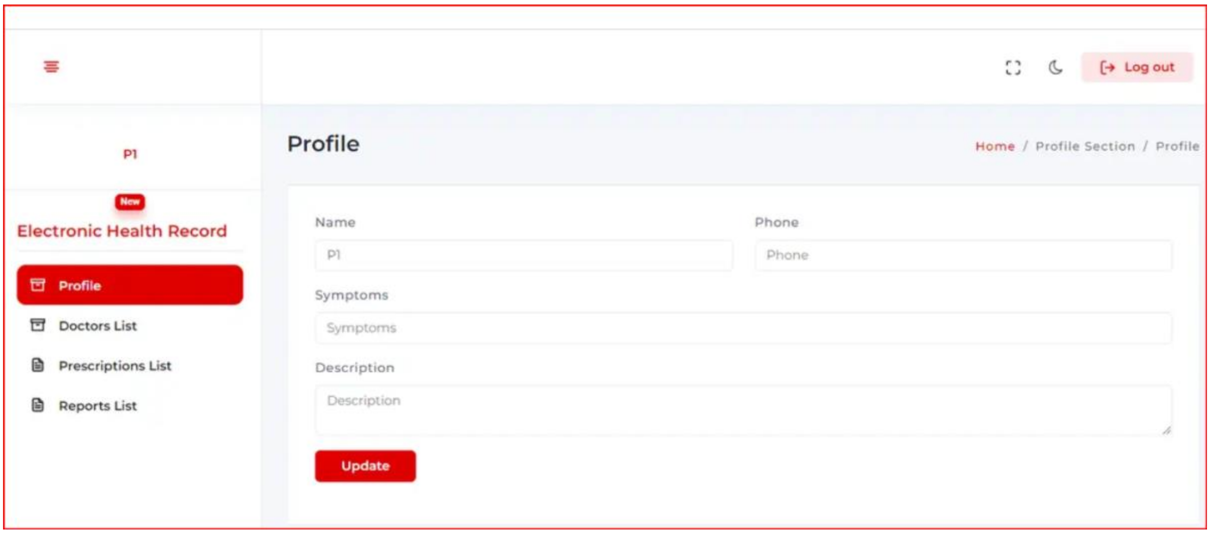
Username: p1

Password: ..

Full Name: usser1

User Type: Patient

In above screen, click on 'New User' and add different users



Profile

Home / Profile Section / Profile

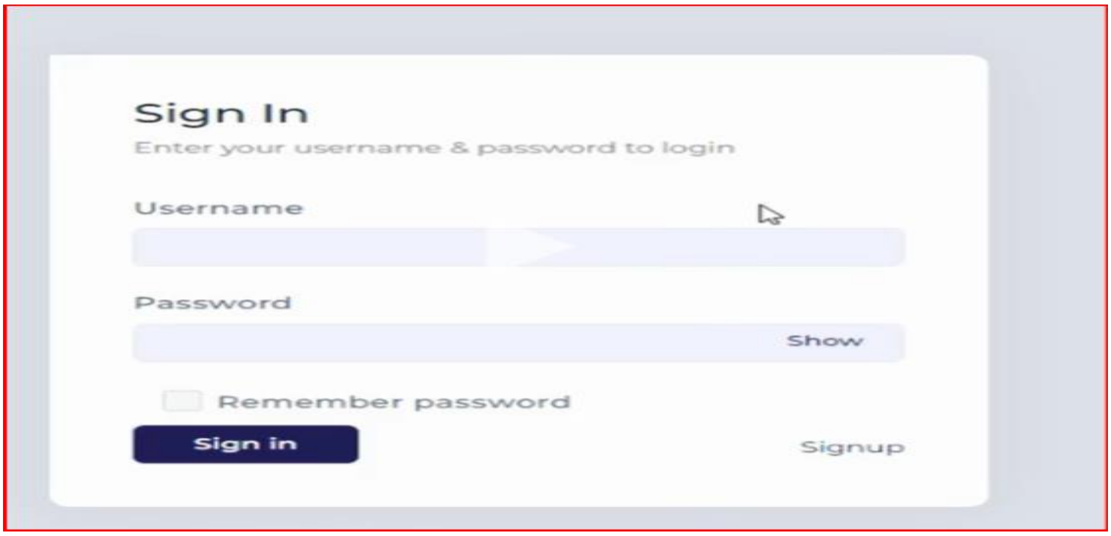
Name: P1

Phone: Phone

Symptoms: Symptoms

Description: Description

In the above scenario, when adding patient details, the DataOwner will be considered as the patient



Sign In

Enter your username & password to login

Username

Password

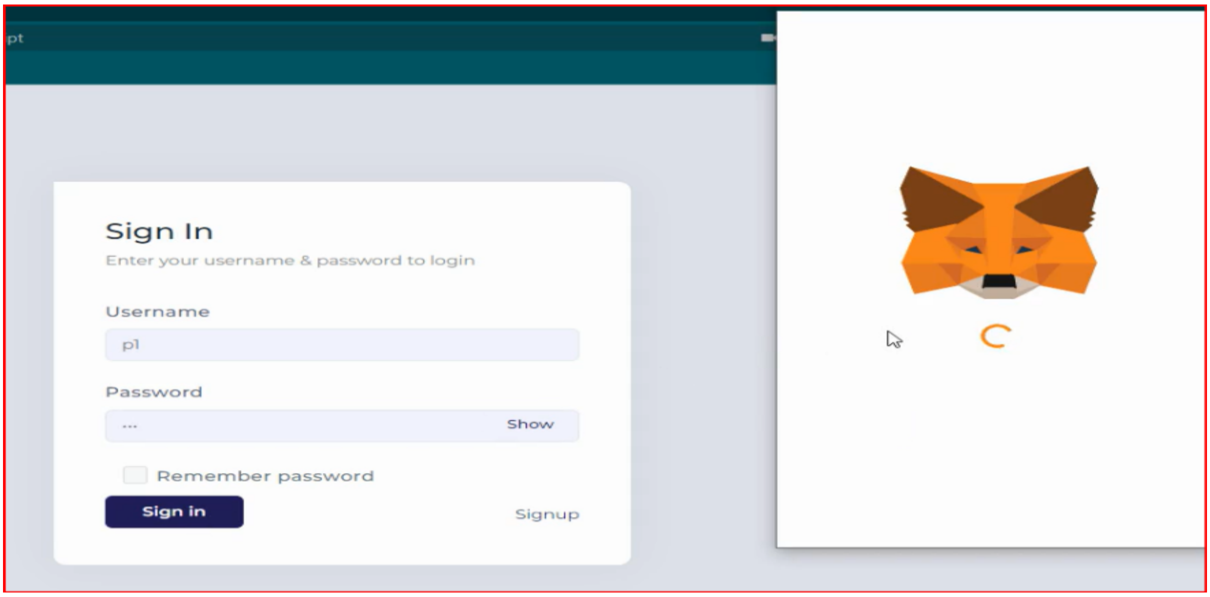
Show

□ Remember password

Sign in

Signup

For the sign in, users have to verify with the MetaMask confirmations as below –



Sign In

Enter your username & password to login

Username

p1

Password

...

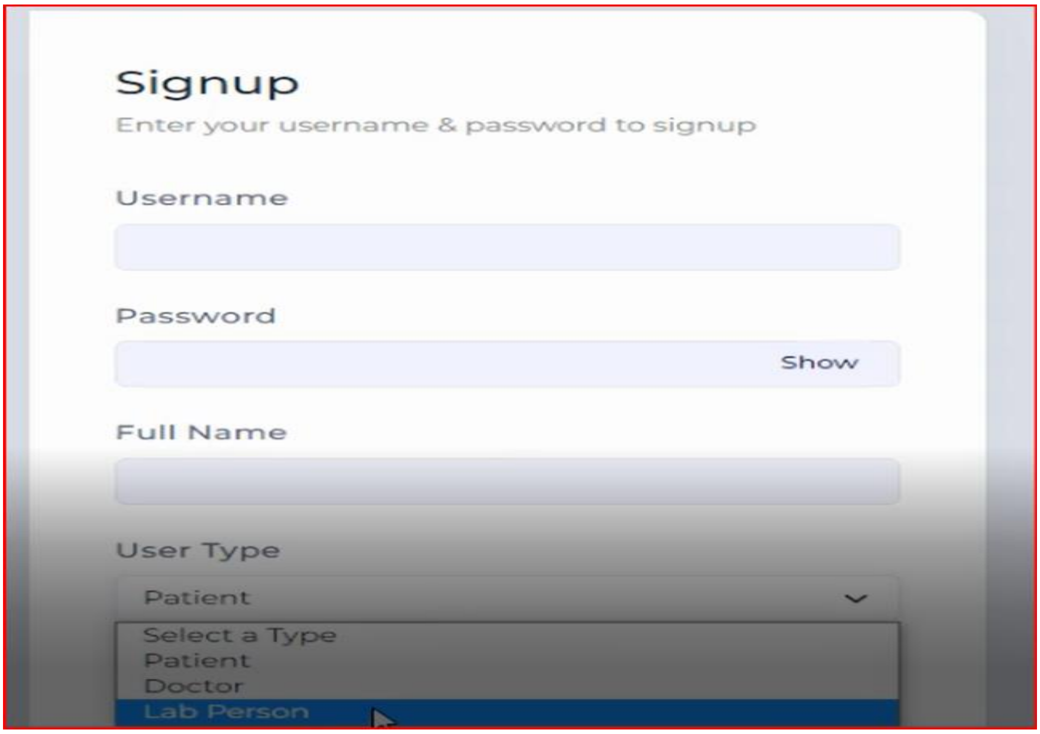
Show

□ Remember password

Sign in

Signup

Now go back to 'New User' link again and add one doctors


Signup

Enter your username & password to signup

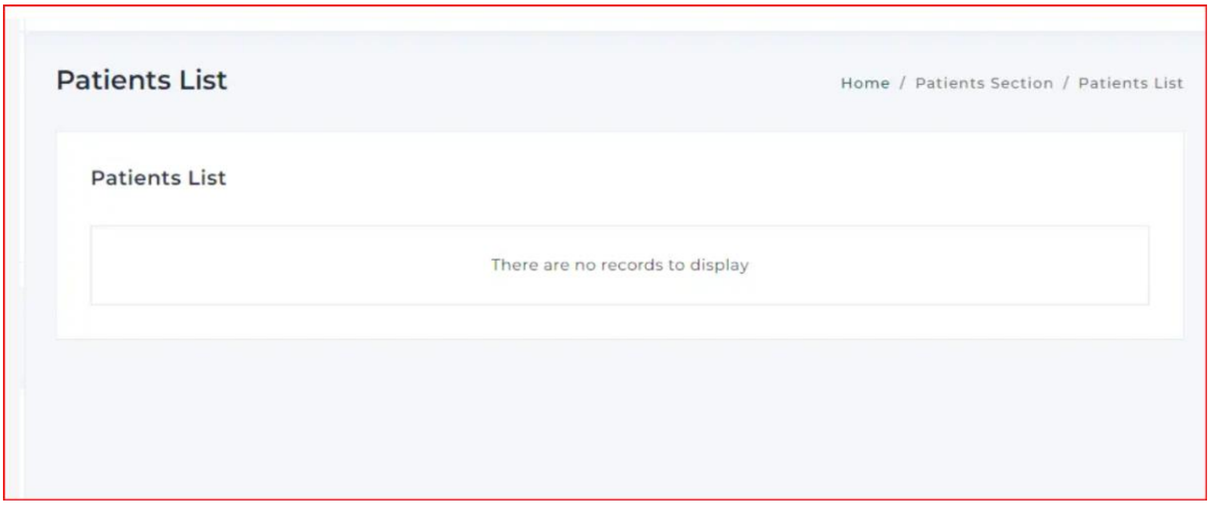
Username

Password

Full Name

User Type: Patient

In above screen I am adding one doctor details and selected user type as 'Physician' and after adding detail will get the below screen

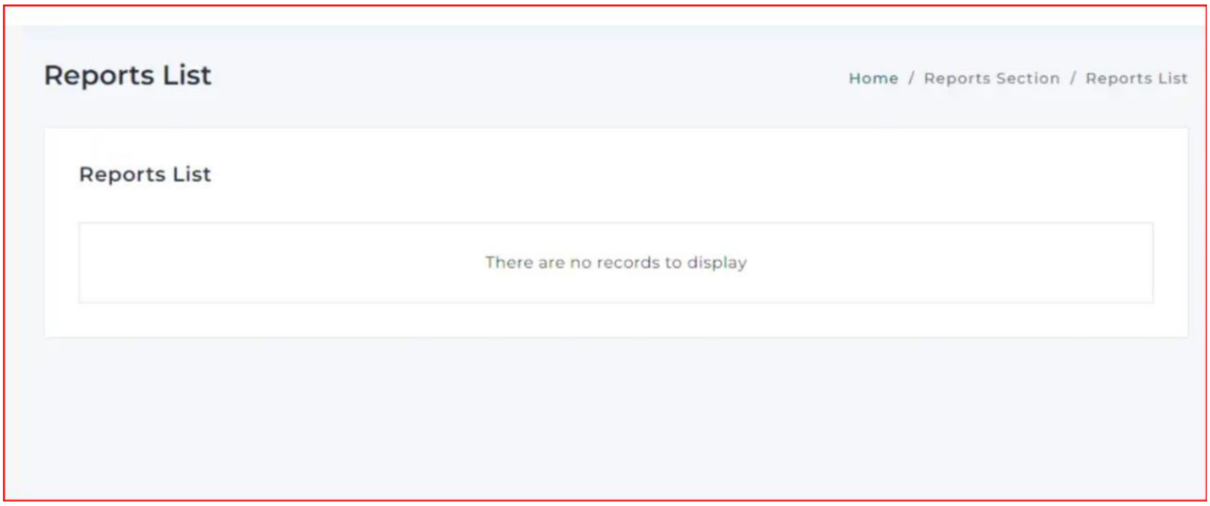

Patients List

Home / Patients Section / Patients List

Patients List

There are no records to display

Now click on 'Data Owner' to login as patient, see below screen

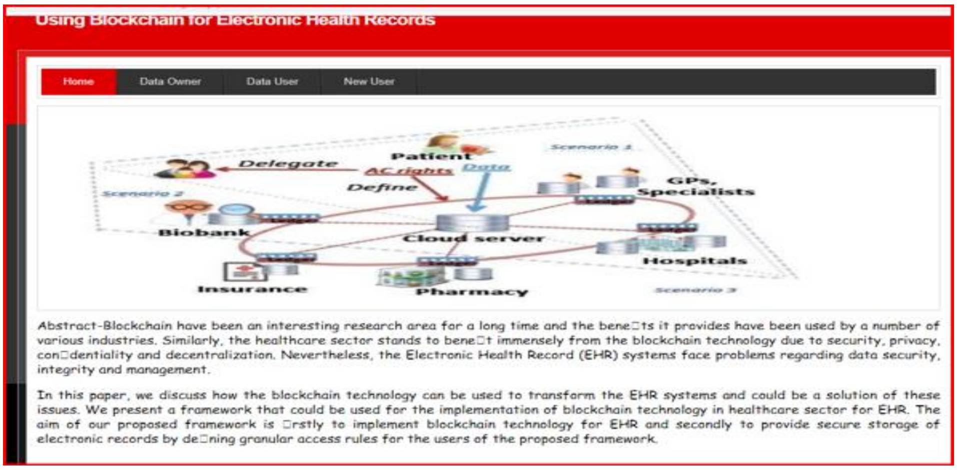


Reports List

Reports List

There are no records to display

In the above scenario, I am logging in as a patient by selecting the user type as 'Data Owner'. After logging in, the screen displayed will be as follows. In this screen, the patient can add their disease details and grant access to a doctor by selecting the doctor's name from the drop-down list. After adding the disease details, the message "Profile created" will be shown, and the patient can click on the 'View Profile' link to access the details. In the profile view, all the details will be visible, and in the last column, the message "Pending" indicates that no doctor has provided any prescription yet. To proceed, log out as the patient and log in as a doctor to prescribe medication for this patient.

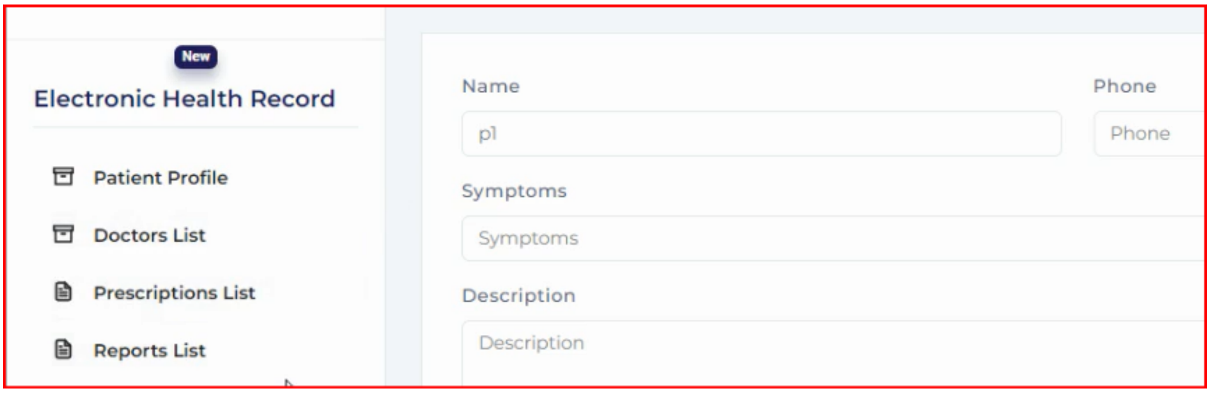


Using Blockchain for Electronic Health Records

Abstract-Blockchain have been an interesting research area for a long time and the benefits it provides have been used by a number of various industries. Similarly, the healthcare sector stands to benefit immensely from the blockchain technology due to security, privacy, confidentiality and decentralization. Nevertheless, the Electronic Health Record (EHR) systems face problems regarding data security, integrity and management.

In this paper, we discuss how the blockchain technology can be used to transform the EHR systems and could be a solution of these issues. We present a framework that could be used for the implementation of blockchain technology in healthcare sector for EHR. The aim of our proposed 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.

In the previous screen, click on the 'Data User' link to log in as a doctor. After logging in, the following screen will be displayed. To view all patient records, click on the 'View Medical Profile' link in the above screen



Name: p1

Phone: Phone

Symptoms: Symptoms

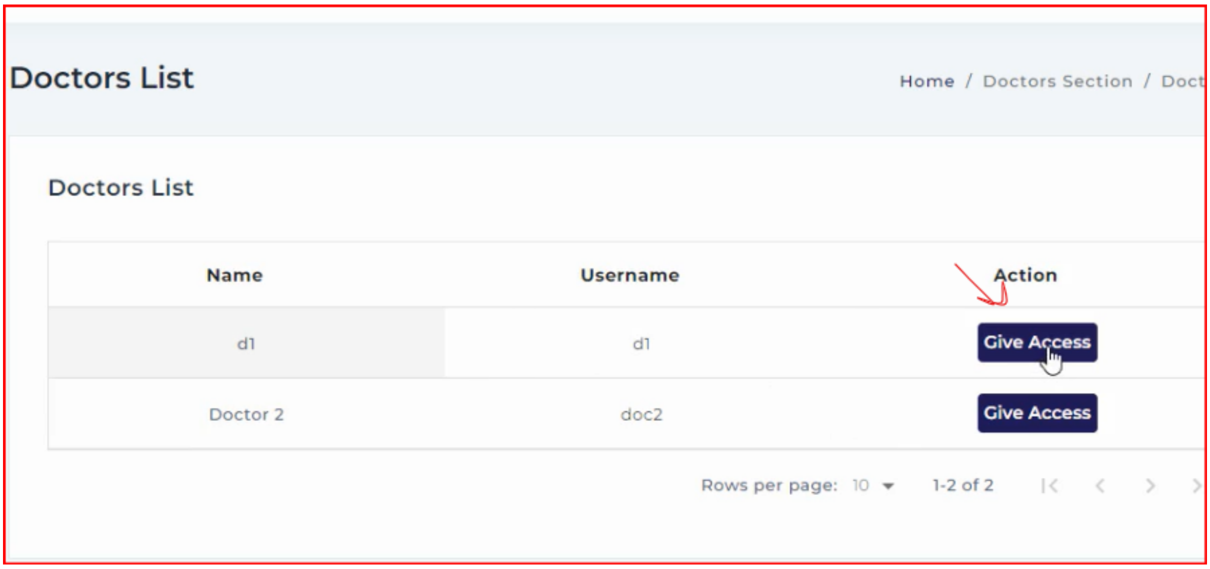
Description: Description

In above screen the doctor will click on ‘Add Prescription’ link to give a prescription to patient. After clicking on ‘Add Prescription’ you will get the below screen

In above screen doctor added some prescription and patient can login and see that prescription.

In above screen we can see status change to prescription from pending. Patient can view the prescription and go to lab for test. Now login as lab to upload report. Logout and click on ‘Data User’ link to get below screen

In the above screen, I have logged in as “Lab’ user and after login will get below screen



Doctors List

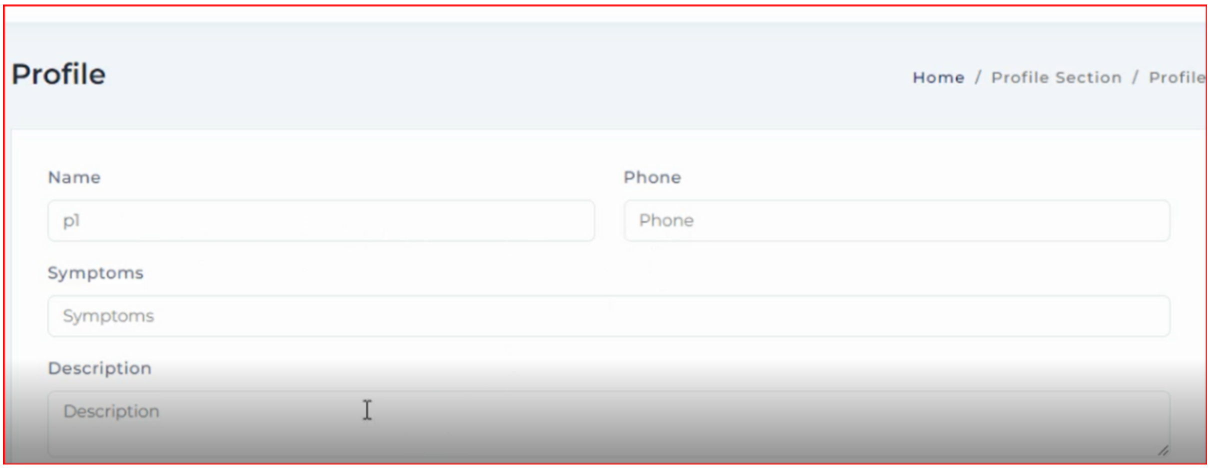
Home / Doctors Section / Doct

Doctors List

Name	Username	Action
d1	d1	Give Access
Doctor 2	doc2	Give Access

Rows per page: 10 ▾ 1-2 of 2

In above screen click on 'Add Reports' link to get below screen. In above screen lab person will select patient name and then upload report. In above screen I am uploading one PDF file and you can upload any type of file and after upload will get below screen



Profile

Home / Profile Section / Profile

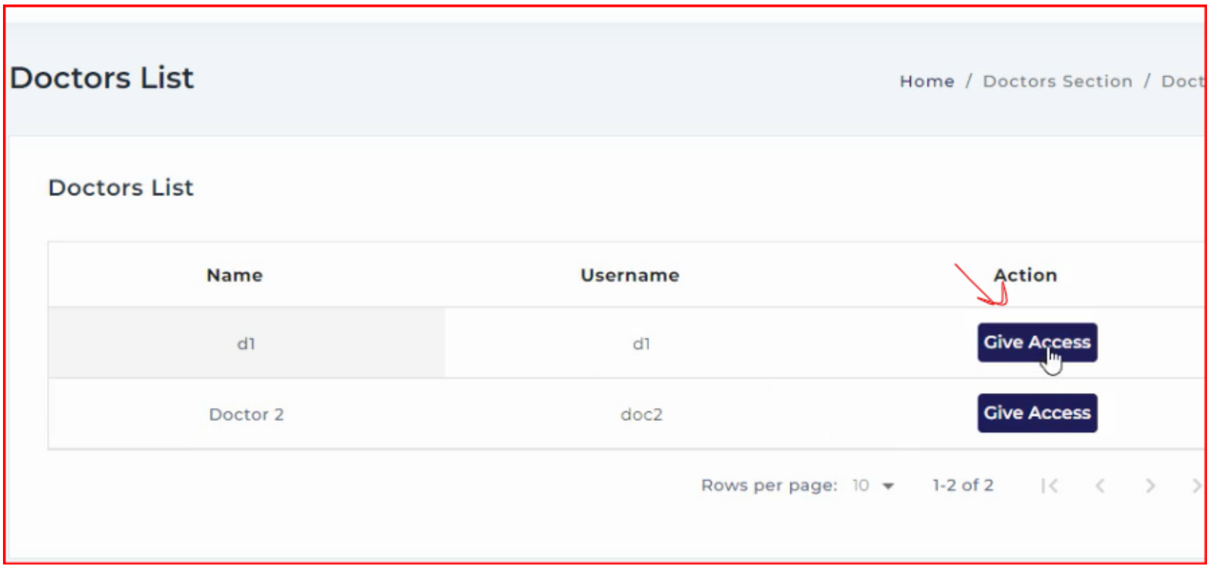
Name: pl

Phone: Phone

Symptoms: Symptoms

Description: Description

In above screen we can see report details added and now patient can login by clicking 'Data Owner' link and access reports.



Doctors List

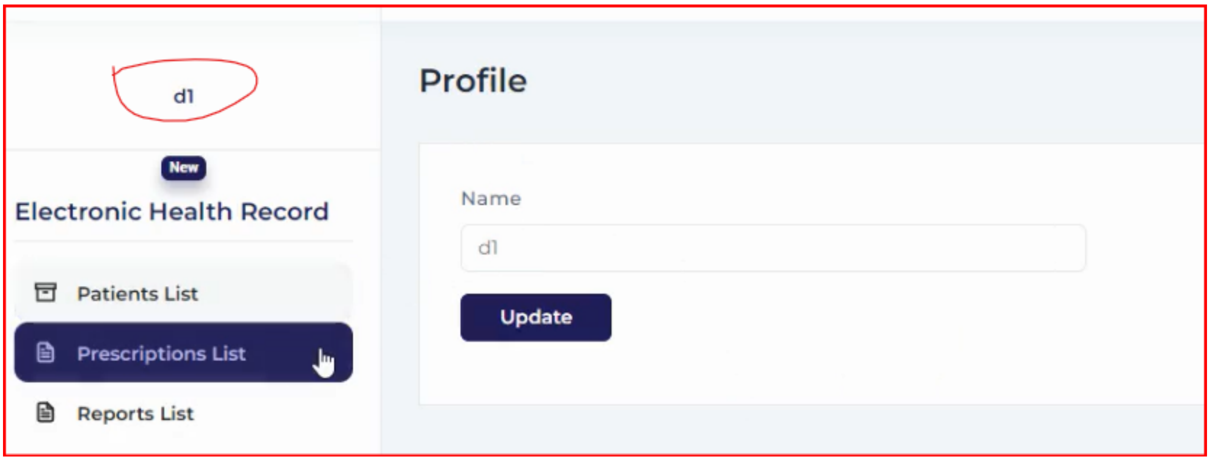
Home / Doctors Section / Doct

Doctors List

Name	Username	Action
d1	d1	Give Access
Doctor 2	doc2	Give Access

Rows per page: 10 ▾ 1-2 of 2

In above screen patient click on ‘View Reports’ link to get above screen and then select either option ‘All’ to get all reports or select from or to date option to select all reports between two date. After selecting ‘All’ Option user will get below screen upon click on ‘View Reports’ button



d1

New

Electronic Health Record

Patients List

Prescriptions List

Reports List

Profile

Name

d1

Update

In above screen patient can click on ‘Click Here’ link to download report , In browser status bar we can see file downloaded and similarly you can select date option and download files

5.4 FRAME WORK SCENARIO

The system primarily consists of two entities: the Administrator and the User. The Users are further divided into two categories for our proposed framework, namely, the Doctor and the Patient. These users are assigned roles by the system's Administrator, who belongs to the hospital's administrative staff. The Administrator is responsible for defining the granular access for the two main users of our system, i.e., the Doctor and the Patient. The initial task involves the Administrator assigning roles, which includes providing a Role Name and an Account Address for each role. This information is stored in a roles list for validation purposes in subsequent steps.

Once the roles are assigned, users can interact with the system through the blockchain layer. Users can access the DAPP browser, which provides a comprehensive view of the entire projected framework.

6. ANALYSIS AND DISCUSSION OF RESULTS

6.1 PERFORMANCE

In this section we tend to evaluate the performance of the projected framework.

By assessing the performance, we can effectively mitigate the risks associated with this novel technology. Understanding the performance metrics and evaluating the system's capabilities allow us to identify any potential issues and address them proactively. This assessment helps in ensuring the reliability, scalability, and security of the technology. Additionally, it enables us to optimize the system's performance, enhance user experience, and build trust among stakeholders. By continuously monitoring and evaluating the performance, we can stay ahead of any potential risks and make informed decisions to mitigate them effectively.

6.2 EXPERIMENTAL SETUP

For testing performance of the projected framework we've conducted experiments by victimisation the subsequent configurations:

- Intel Core i7-6498DU central processor @ a pair of.50GHz 2.60 gig cycle per second
- And 8.00 GB of memory with Operating System Windows 10 64-bit.

6.3 DATA COLLECTION FOR PERFORMANCE EVALUATION

This section provides an overview of the data used for analysing the performance of the projected framework. It also discusses the metrics employed to evaluate and justify the results of the performance analysis.

6.3. A. TRANSACTION DATA

To assess the performance of the projected framework, the following transaction data and its associated details are utilized. The first metric is the deployment time, which refers to the time it takes for a transaction to deploy a smart contract on the Ethereum blockchain. This deployment time is determined by the Ethereum network.

The second metric is the confirmation time, which is the time taken for the transaction to be completed and confirmed by the blockchain, specifically in the case of Ethereum. This metric indicates the time it takes for the transaction to be fully processed and included in the blockchain, ensuring its validity and immutability.

6.3. B. EVALUATION METRICS

The performance analysis of the projected framework includes the evaluation of three key metrics: execution time, latency, and throughput. These metrics are briefly explained as follows:

1. Execution Time: It is defined as the duration, measured in seconds, taken by the framework to execute a specific task or process. It indicates the speed and efficiency of the system in performing operations.

2. Latency: Latency refers to the time delay between the initiation of an action and the corresponding response or result. In the context of the framework, it can be understood as the difference between the deployment time and the completion time of a transaction. Lower latency indicates faster transaction processing.
3. Throughput: Throughput measures the rate at which data can be transferred from one location to another within a given time frame. It quantifies the amount of data that the framework can handle and process effectively. Higher throughput implies a greater capacity for data transfer.

By analyzing these metrics, we can gain insights into how the projected framework would perform in real-world scenarios, considering various users and their interactions with the system.

7. CONCLUSION AND FUTURE WORK

In this project, we explored the application of blockchain technology in the healthcare sector, particularly in Electronic Health Record (EHR) systems. We identified several challenges in traditional EHR systems that can be addressed through the integration of secure record storage and granular access control provided by blockchain.

By utilizing off-chain storage and implementing role-based access control, the proposed framework ensures that medical records are securely stored and accessible only to authorized individuals. This enhances data privacy and security in the healthcare ecosystem.

Looking ahead, we plan to further enhance the existing framework by implementing a payment module. This would require addressing certain considerations, such as determining the consultation fees patients would need to pay for accessing healthcare services through this decentralized system.

REFERENCES

[1] G. Jetley and H. Zhang, ''Electronic health records in IS research: Quality issues, essential thresholds and remedial actions,'' Decis. Support Syst., vol. 126, pp. 113-137, Nov. 2019.

[2] K. Wisner, A. Lyndon, and C. A. Chesla, ''The electronic health record's impact on nurses' cognitive work: An integrative review,'' Int. J. Nursing Stud., vol. 94, pp. 74-84, Jun. 2019. [3] M. Hochman,

‘‘Electronic health records: A ‘‘Quadruple win,’’ a ‘‘quadruple failure,’’ or simply time for a reboot?’’ J. Gen. Int. Med., vol. 33, no. 4, pp. 397-399, Apr. 2018.

[4] Q. Gan and Q. Cao, ‘‘Adoption of electronic health record system: Multiple theoretical perspectives,’’ in Proc. 47th Hawaii Int. Conf. Syst. Sci.,Jan. 2014, pp. 2716-2724.

[5] T. Vehko, H. Hyppönen, S. Puttonen, S. Kujala, E. Ketola, J. Tuukkanen, A. M. Aalto, and T. Heponiemi, ‘‘Experienced time pressure and stress: Electronic health records usability and information technology competence play a role,’’ BMC Med. Inform. Decis. Making, vol. 19, no. 1, p. 160, Aug. 2019.

[6] M. Riesman, ‘‘EHRs: The challenge of making electronic data usable and interoperable.,’’ PT, vol. 42, no. 9, pp. 572-575, Sep. 2017.

[7] W. Koczkodaj, M. Mazurek, D. Strzałka, A. Wolny-Dominiak, and M. Woodbury-Smith, ‘‘Electronic health record breaches as social indicators,’’ Social Indicators Res., vol. 141, no. 2, pp. 861-871, Jan. 2019.

[8] S. T. Argaw, N. E. Bempong, B. Eshaya-Chauvin, and A. Flahault,‘‘The state of research on cyber-attacks against hospitals and available best practice recommendations: A scoping review,’’ BMC Med. Inform. Decis. Making, vol. 19, no. 1, p. 10, Dec. 2019.

[9] A. McLeod and D. Dolezel, ‘‘Cyber-analytics: Modelling factors associated with healthcare data breaches,’’ Decis. Support Syst., vol. 108, pp. 57-68, Apr. 2018.

[10] L. Coventry and D. Branley, ‘‘Cyber security in healthcare: A narrative Review of trends, threats and ways forward,’’ Maturities, vol. 113,pp. 48-52, Jul. 2018.

[11] ‘‘The future of health care cyber security,’’ J. Nursing Regulation, vol. 8,No. 4, pp. S29-S31, 2018. [12] D. Spatar, O. Kok, N. Basoglu, and T. Daim, ‘‘Adoption factors of Electronic health record systems,’’ Technol. Soc., vol. 58, Aug. 2019, Art. no. 101144. [13] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System. 2008, pp. 1-9. [14] W. J. Gordon and C. Catalini, ‘‘Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability,’’ ComputStruct. Biotechnology. J., vol. 16, pp. 224-230, Jan. 2018.

[15] A. Boonstra, A. Versluis, and J. F. J. Vos, ‘‘implementing electronic health Records in hospitals: A systematic literature review,’’ BMC Health Services Res., vol. 14, no. 1, Sep. 2014, Art. no. 370.

[16] T. D. Gunter and N. P. Terry, ‘‘the emergence of national electronic health Record architectures in the United States and Australia: Models, costs, and Questions,’’ J. Med. Internet Res., vol. 7, no. 1, p. e3, Jan./Mar. 2005.

[17] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, ‘‘an overview Of blockchain technology: Architecture, consensus, and future trends,’’ in Proc. IEEE Int. Congr. Big Data (Big Data Congr.), Jun. 2017, pp. 557-564.

[18] C. Pirtle and J. Ehrenfeld, ‘‘Blockchain for healthcare: The next generation of medical records?’’ J. Med. Syst., vol. 42, no. 9, p. 172, Sep.2018.

[19]A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, ‘‘Applications of blockchain technology in medicine and healthcare: Chal- lenges and future perspectives,’’ Cryptography, vol. 3, no. 1, p. 3, Jan. 2019.
[20] J. Eberhardt and S. Tai, ‘‘On or off the blockchain? Insights on off- chaining computation and data,’’ in Proc. Eur. Conf. Service-Oriented Cloud Comput., Oct. 2014, pp. 11-45.

[21] D. Vujičić, D. Jagodić, and S. Randić, ‘‘Blockchain technology, bitcoin, and Ethereum: A brief overview,’’ in Proc. 17th Int. Symp. INFOTEH- JAHORINA (INFOTEH), Mar. 2018, pp. 1-6.

[22] S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin, and F.-Y. Wang, ‘‘An overview of smart contract: Architecture, applications, and future trends,’’ in Proc.IEEE Intell. Vehicles Symp. (IV), Jun. 2018, pp. 108-113.

[23] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, ‘‘Blockchain distributed ledger technologies for biomedical and health care applications,’’ J. Amer.Med. Inform. Assoc., vol. 24, no. 6, pp. 1211-1220, 2017.

[24] M. S. Sahoo and P. K. Baruah, ‘‘HBasechainDB—A scalable blockchain framework on Hadoop ecosystem,’’ in Supercomputing Frontiers. 2018,pp. 18-29.

[25] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom,''FHIRChain: Applying blockchain to securely and scalably share clinical data,'' Comput. Struct. Biotechnol. J., vol. 16, pp. 267-278, Jul. 2018.

[26] M. G. Kim, A. R. Lee, H. J. Kwon, J. W. Kim, and I. K. Kim, ''Sharing medical questionnaries based on blockchain,'' Proc. IEEE Int. Conf. Bioinf. Biomed. (BIBM), Dec. 2018, pp. 2767-2769.

[27] S. Gupta and M. Sadoghi, ''Blockchain transaction processing,'' in Ency-clopedia of Big Data Technologies. 2019, pp. 366-376.

[28] U. W. Chohan, ''Cryptocurrencies: A brief thematic review,'' SSRN Elec-tron. J., 2017.

[29] G. Wood, ''Ethereum: A Secure Decentralised generalised transaction ledger. EIP-150 revision,'' Tech. Rep., Aug. 2017, p. 33.

[30] N. Atzei, M. Bartoletti, T. Cimoli, S. Lande, and R. Zunino, ''SoK:Unraveling bitcoin smart contracts,'' in Proc. Int. Conf. Princ. Secur. Trust, Thessaloniki, Greece, 2018, pp. 217-242.

[31] I. Grishchenko, M. Maffei, and C. Schneidewind, ''A semantic framework for the security analysis of ethereum smart contracts,'' in Principles of Security and Trust. 2018, pp. 243-269.

[32] T. Dey, S. Jaiswal, S. Sunderkrishnan, and N. Katre, ''HealthSense: Amedical use case of Internet of Things and blockchain,'' in Proc. Int. Conf. Intell. Sustain. Syst. (ICISS), Dec. 2017, pp. 486-491.

[33] InterPlanatery File System (IPFS). Accessed: Feb. 4, 2019. [Online].Available: https://ipfs.io/.

[34] M. Niranjanamurthy, K. Kumar S, A. Saha, and D. D. Chahar, ''Comparative study on performance testing with jmeter,'' Int. J. Adv. Res. Comput. Commun. Eng., vol. 5, no. 2, pp. 70-76, 2016.