

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/368755500>

Blockchain-based decentralized secure healthcare system using Ethereum smart contracts

Thesis · August 2022

DOI: 10.13140/RG.2.2.18633.42081

CITATIONS

0

READS

3

2 authors, including:



[Tariqul Islam](#)

Daffodil International University

16 PUBLICATIONS 3 CITATIONS

SEE PROFILE

**Blockchain-based decentralized secure healthcare system using Ethereum smart
contracts**

BY

Tariqul Islam
ID: 183-15-2250
AND

Md. Tanvir Rahman
ID: 183-15-2245

This Report Presented in Partial Fulfillment of the Requirements for the
Degree of Bachelor of Science in Computer Science and Engineering
Supervised By

Md. Mahfujur Rahman
Lecturer (Senior Scale)
Department of CSE
Daffodil International University

Co-Supervised By

Professor Dr. Md. Ismail Jabiullah
Professor
Department of CSE
Daffodil International University



DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

SEPTEMBER 2022

APPROVAL

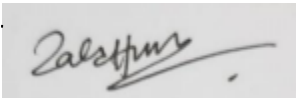
This Project titled “**Blockchain-based decentralized secure healthcare system using Ethereum smart contracts**”, was submitted by Tariqul Islam and Md. Tanvir Rahman to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation will be held on September 13, 2022.

BOARD OF EXAMINERS



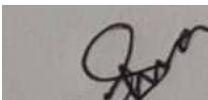
Dr. S M Aminul Haque
Associate Professor & Associate Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Chairman



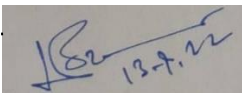
Dr. Md. Zahid Hasan
Associate Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



Ms. Taslima Ferdous Shuva
Senior Lecturer
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



Dr. Md Sazzadur Rahman
Associate Professor
Institute of Information Technology
Jahangirnagar University

External Examiner

DECLARATION

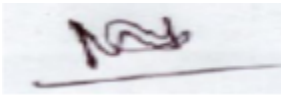
We hereby declare that this project has been done by us under the supervision of **Md. Mahfujur Rahman, Lecturer (Senior Scale), Department of CSE** Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere for any degree or diploma award.

Supervised by



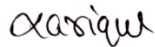
Md. Mahfujur Rahman
Lecturer (Senior Scale)
Department of CSE
Daffodil International University

Co-Supervised by

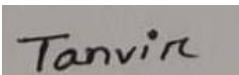


Professor Dr. Md. Ismail Jabiullah
Professor
Department of CSE
Daffodil International University

Submitted by:



Tariqul Islam
ID: 183-15-2250
Department of CSE
Daffodil International University



Md. Tanvir Rahman
ID: 183-15-2245
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

First, we express our heartiest thanks and gratefulness to Almighty God for His divine blessing makes it possible to complete the final year project/internship successfully.

We are grateful and wish our profound indebtedness to **Md. Mahfujur Rahman**, Lecturer (Senior Scale), Department of CSE Daffodil International University. Deep Knowledge & keen interest of our supervisor in the field of “*Blockchain*” to carry out this project. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior drafts, and correcting them at all stages have made it possible to complete this project.

We would like to express our heartiest gratitude to Md. Mahfujur Rahman, Professor Dr. Md. Ismail Jabiullah, and Head, Department of CSE, for his kind help to finish our project and also to other faculty members and the staff of the CSE department of Daffodil International University.

We would like to thank our entire course-mates at Daffodil International University, who took part in this discussion while completing the course work.

Finally, we must acknowledge with due respect the constant support and patients of our parents.

ABSTRACT

Blockchain for health care has the potential to standardize secure data exchange in a less burdensome way. Traditional data-sharing platforms rely on a third party. Owing to the consideration of a third party, such systems compromised transparency, trust, and integrity. To solve the aforementioned issues, we have proposed a smart contract-based secure data-sharing scheme in healthcare by leveraging the advantages of the interplanetary file system (IPFS). Our scheme achieves data confidentiality, integrity, and access control rules by implementing the access control policy written in a smart contract by active entities. This thesis is to attain higher levels of medical records security using Ethereum Blockchain methods. Finally, it also helps organ donation, to incentivize medical stakeholders such as researchers, health authorities, etc. to participate in the network as blockchain miners. This provides them with access to aggregate, anonymous data mining awards in return for sustaining, and securing the network.

Keywords: Blockchain, Ethereum, Medical Records, Storing System, IPFS

TABLE OF CONTENTS

CONTENTS	PAGE
BOARD OF EXAMINERS	i
DECLARATION	ii
ACKNOWLEDGEMENT	iii
ABSTRACT	iv
CHAPTER	
CHAPTER 1: INTRODUCTION	1
CHAPTER 2: RELATED WORK	2-7
CHAPTER 3: SYSTEM IMPLEMENTATION	8-13
3.1 Overview	8
3.2 Blockchain and Ethereum	8-10
3.3 Smart Contracts	10
3.4 Truffle	10
3.5 Ganache	10
3.6 Metamask	11-12
3.7 IPFS	12
3.7 Connecting to Ethereum Client	12-13
CHAPTER 4: EXPERIMENTAL METHODS	14-17
4.1 Policy Contract (PSC)	14-15
4.2 ETSC Verification & Data Addition Phase in the Blockchain Network	15-17
CHAPTER 5: RESULTS AND DISCUSSION	18-19

5.1 Communication Cost	18
5.2 Computation Cost	18-19
5.3 Blockchain Data Storage Cost	19
CHAPTER 6: IMPLEMENTATION OUTPUT	20-25
CHAPTER 7: FUTURE WORK AND CONCLUSION	26-27
CHAPTER 8: ACKNOWLEDGMENT	28
REFERENCES	29-30

LIST OF FIGURES

FIGURES	PAGE NO
Fig. 1: Structure and Workflow of Patient-Doctor System	8
Fig. 2: Blockchain Structure: a Continuously Growing List of Ordered and Validated Transactions	9
Fig. 3: Bitcoin Proof of Work Concept	9
Fig. 4: Import truffle-config.js	10
Fig. 5: Import Private Key from Ganache	11
Fig. 6: Add New RPC	11
Fig. 7: The Workflow of the Proposed Scheme	14
Fig. 8: Comparison of Data Storage Cost	19
Fig. 9: GUI of Application	20
Fig. 10: Admin Panel	20

LIST OF TABLES

TABLES	PAGE NO
Table 1: Comparison of Different Mining Techniques	7

CHAPTER 1

INTRODUCTION

Today's medical data is often scattered among various facilities and individuals. It is not very accurate and can be difficult to reconcile. Due to the complexity of the healthcare system, it is not always clear who recorded what in a health record. As a result, providers typically take a few days to respond to a request for an update or removal of a record. Beyond the time delay, maintaining a patient's records can be challenging as they are rarely reviewed or encouraged to review their full records. This issue also affects the ability to collaborate with other healthcare organizations. Due to the lack of coordinated data exchange and management, health records are fragmented. This means that patients and providers face significant obstacles in accessing and sharing their health information. Instead of just displaying data from one database, the health records could store data from every database in the ledger. The entire process would be automated. An Ethereum blockchain is used to create an immutable, time-stamped chain of content. The content is secured through a distributed proof of work algorithm known as the Proof of Work. These miners are responsible for keeping the blockchain secure. The work they do ensures that transactions are difficult to rewrite. The mining proof-of-work is a secure nonce that is utilized to verify the correctness of a particular calculation. The concept of the proof-of-work is that it is a method of keeping the blockchain secure in the future. Its goal is to provide a level of trust that the network will remain decentralized. The distribution model should be open and allow anyone to get involved. This is especially true if you are not a native developer or have no experience mining. The requirement for special hardware should be minimized or eliminated. This should make the distribution model more open, and it should make mining a simple process. An adversary can gain a large amount of the network's mining power by taking advantage of this feature.

CHAPTER 2

RELATED WORK

Novikov et al. [1] focus on the availability and quality of medical care for people by using blockchain technology. Information and communication technologies evaluate every sector of a person. In this paper, the authors will try to examine the prospect of making an infrastructure that will work based on blockchain and smart contracts. This paper works because of blockchain technology. In this work, the author tries to develop an integrated electronic medical record (IEMC). The main work of this is to store a large amount of patients' information in an electronic form. For making an efficient health management system we need to use a service model where we need to take the main place by IEMC. In this paper, the author uses smart contracts together with blockchain technology. The main advantages of blockchain technology are to ensure security, data processing, and implementation by using algorithms. That's why this technology has been chosen for this work.

Gürsoy et al. [2] aim to establish Ethereum smart contracts to preserve pharmacogenomics information with time and also memory effectiveness. Blockchain technology has been getting more popular in recent times. The main advantage of this technology is data integrity, security, and access control. Making an Ethereum-based smart contract is also challenging. That's why in this work the authors present a structure for this solution and also describe the procedure to store and querying the pharmacogenomics data with time and memory management. In this paper, the authors present a data structure and algorithm with remembering time and memory effectiveness to reserve pharmacogenomics data. Here the authors designed a smart contract to store all pharmacogenomics activities. In this case, all these pharmacogenomics activities are also noticed by a smart contracts trigger. This smart contract stores this observation data and reserves them in four nodes that are connected to a blockchain network. In this system, there is no permission for off-chain data storage. This designed system can finish a 2-AND query and it takes 35ms and takes 0.1 MB of memory. For a similar query, the fast query has 2 times improvement in time and 10 times improvement in memory. This work successfully shows that pharmacogenomics information can be reserved and queried in this designed Ethereum

blockchain. This solution can successfully be used for data integrity, security, time, and also memory efficiency.

Griggs et al. [3] focus on supplying a secure and self-operating remote patient observing system using blockchain technology. Nguyen et al. [4] make an efficient and secure electronic health record (EHRs) system. Yang et al. [5] use smart contracts to develop a management system that will contain medical records. In the paper [6] the target is to identify some suitable healthcare system applications based on Blockchain technology. Nowadays blockchain technology is one of the most popular technologies in the world. It makes a revolution in the field of medical infrastructure. The motivation of this work is to specify the use of blockchain technology in the medical sector. Besides, it also tells us about the challenges of using this technology. In this paper, the authors try to build a smart contract to contain the records of all medical entities. All records are gathered in a database to support the performance. This technology supports smart contracts and it helps automatically to track the transaction of data. Smart contract-based medical or healthcare management systems have made a revolutionary change. In this work the authors are successfully showing a creative procedure for healthcare record handling, supplying, accessing, observing, etc. using these smart contracts.

Javed [7] et al. propose an identity management system that is based on blockchain technology for far way healthcare. Nowadays Blockchain technology has created a revolutionary impact in the field of healthcare infrastructure. In this work, the authors have advised an identity management system that is based on blockchain technology that permits patients and doctors to indicate and verify themselves. To make the patient's information secure in this paper here we have used Health-ID. As a result, Patients and doctors are recognized by their health identifications (health IDs). In this work, the authors have executed a smart contract on Ethereum blockchain convenience recognition and confirmation methods. We additionally explore the performance by using various types of metrics such as transaction per second, blocks lost number, and block circulation time. Over the last few years, the identity management system has gotten outstanding attention. This paper presents a privacy-conserving identity management system for far way health care infrastructure. This advisable system by the authors permits patients and doctors to

verify themselves in various E-health domains Without depending on a central service provider.

Sharma et al. [8] aim to represent blockchain technology including smart contracts and also mention the importance of (IoMT) in healthcare infrastructure. We know that medical records must need to be private. Besides, it has to be easily accessible for the users and also has to be secure. In this case blockchain technology makes evolution in the healthcare system. In this paper, the author suggests a novel procedure for IoMT in healthcare with a blockchain network. This advisable method of the authors in this paper has more security, better performance, and data processing accuracy than other methods. This paper is working based on a blockchain network. smart contracts are self-authenticating systems and they can work independently with high-level security, good data processing, and access control accuracy also. Besides Smart contracts are very affordable to implement. Through smart contracts, this system can log in to patients' information records by the patient ID and see the patient-doctor relationship which is connected to the database. And data is stored in nodes and transactions are managed by algorithms. We can see that the representing algorithm of the authors performs better in terms of packet transfer ratio than traditional methods. This suggested method of this work has gained a 100% packet transfer ratio which is far better than other traditional methods. It has been noticed that using blockchain technology in e-healthcare is very advantageous. In this paper, our authors successfully showed how smart contracts on the blockchain can be used in IoMT in e-healthcare and solve challenges related to this.

Jabbar et al. [9] focuses on developing an efficient framework for amplifying data interoperability and integrity concerning electronic health record EHR sharing. The EHR sharing system is a sophisticated technology for providing healthcare. This advisable system can forecast results throughout the patient's lifespan. This system can observe the effectiveness of treatment and also find out human mistakes. This work demonstrates a structure for data integrity confirmation in decentralized infrastructure. The motivation of this work is to present and establish a health information system (HIS) and also talk about the Blockchain framework. The author's proposed method for enhancing data interoperability is institution-driven interoperability. This work shows a structure based on blockchain to make easier transactions between health providers who store all medical

events data and, in the cloud, and also share EHR. The author's advisable solution establishes a smart contract on Ethereum. The main theme of this paper is to set a foundation for future research and also establish a decentralized EHR system using blockchain because of its security, data processing, and authentication.

Omar et al. [10] focus on suggesting an Ethereum smart contract based on blockchain that will help to relieve data management. To innovate new medicine for successful therapy aiming to increase the quality of existing healthcare, clinical trials are very important. In this paper, the authors describe how we can apply blockchain technology in healthcare and also defend data management provocation in clinical testing management. In this work, the authors have described how Blockchain technology can improve clinical trial management. They suggest a framework [11] that apprehends participants of these given clinical trial methods. They also give the codes of Ethereum smart contracts for execution and also examine the overall system. This system permits only particular actors that can interconnect with the code. A green mark is shown that indicates that there is no error created when the patron tries to input data. This system also authenticates that the CT process is executed in sequential order. In the same way, the patient's enrollment stage will not work without completing the CT starting stage. It has been noticed that using blockchain technology in the CT process is very advantageous. It can also solve some challenges that are faced in this sector, especially data management.

Andola et al. [12] focus on examining the restriction of Ethereum based on blockchain with EHR sharing by using a third party. We know that medical records must need to be private. Besides, it has to be easily accessible for the users and also has to be secure. In this case, Ethereum-based blockchain permits seclusion conserves sharing of the decentralized database's cryptographic data with ambiguity and also controls the entrance. In this work, the authors have used dissymmetric and consistent key cryptography for preserving the privacy of records. They have implemented all activity record systems with the Ethereum blockchain. Each data is stored through smart contracts and connected persons with this network can justify data. In this work, the authors have suggested blockchain technology in healthcare infrastructure in which data integrity, processing, and security are confirmed by the use of Ethereum smart contracts.

Omar et al. [13] focus on providing a blockchain-based structure that interacts among different participants in a clinical trial method by using the smart contract. Clinical trials (CT) are very helpful for the innovation of various types of medicine. The aim of this is to increase the quality of the existing healthcare system as well as improve the efficiency of these new medicines. In this case, the authors suggest an outline of how this technology can authorize the CT data management method. In this work, the authors have suggested a system based on blockchain for this given CT data management with Ethereum smart contracts. In this system, all the documents of CT are gathered in the IPFS and it is very hard to disguise because they are given unique hashes. Here we provide this smart contract by using Remix IDE which is allowed in different situations. The main result of this paper is that it is very beneficial for all participants in the case of providing transparency, integrity, and also security. And our suggested solutions are also examining the Ethereum blockchain platform. The main result of this paper is that it is very beneficial for all participants in the case of providing transparency, integrity, and also security. And our suggested solutions are also examining the Ethereum blockchain platform.

Ekblaw et al. [14] aim to suggest a MedRec information management system to manage EHRs based on blockchain technology. Blockchain technology has successfully created a revolutionary impact in healthcare. In this paper, the authors present a reliable methodology for effective EHRs sharing among patients and doctors. They applied a blockchain network for this EHRs system. This MedRec system highly supports data integrity, security, improved data quality, and access control. Blockchain technology supports smart contracts that's why it permits the automatic tracking of transactions. Through smart contracts, this system can log in to patients' information records by the patient ID and see the patient-doctor relationship which is connected to the database. An algorithm manages this data transaction and after getting references this system permits database confirmation. This MedRec system successfully delivers secure and efficient EHRs sharing. It can log into the patient's records and also examine them. In this work, the authors made a great approach to establishing an efficient and secure EHRs sharing system for storing medical information.

Table 1: Comparison of Different Mining Techniques [14]

Mining Techniques	Resource	Examples	Miners	Reward
Proof of Work	High computation energy & power	No	Bitcoin	Yes
Proof of Stake	Assets or stake	Randomized selection of Blockchain	Ethereum	No
Proof of Space	Huge Storage	No	Ethereum	Yes
Proof of Importance	Significance of Node	No	NEM Wallet	Yes
Measure of trust	Reliability	No	No	Yes (Trust)

CHAPTER 3

SYSTEM IMPLEMENTATION

3.1. Overview

Smart contracts are used in our system to enable us to automatically track and record changes in viewership rights or the birth of new records. By linking a patient's record to a provider's database, we can log their viewing permissions and provide them with data retrieval instructions. Acquires medical information and casualties of people in a region and it can be monitored every week. Helps to know about the actual rate of spread of diseases, especially in backward areas. Add on the feature that helps organ donation. It also helps to share the data with insurance companies and organizations like the World Health Organization (WHO). For large storage of data IPFS (Inter-Planetary File System) is used. The goal of this system is to incentivize medical professionals to participate in the network as miners. They would receive mining rewards in exchange for keeping the network secure and operational.

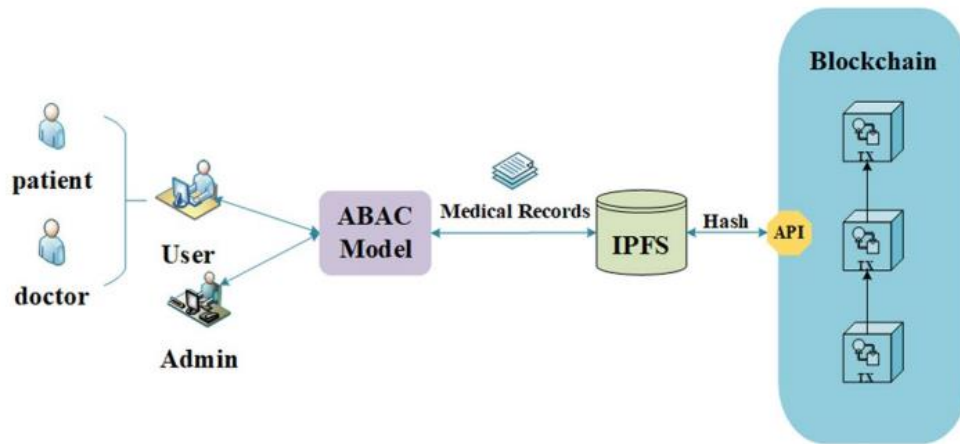


Fig. 1: Structure and Workflow of Patient-Doctor System

3.2 Blockchain and Ethereum

A blockchain is a decentralized computing architecture that maintains a growing list of ordered transactions grouped into blocks that are continually reconciled to keep the information up to date, as shown in Figures 1, and 2.

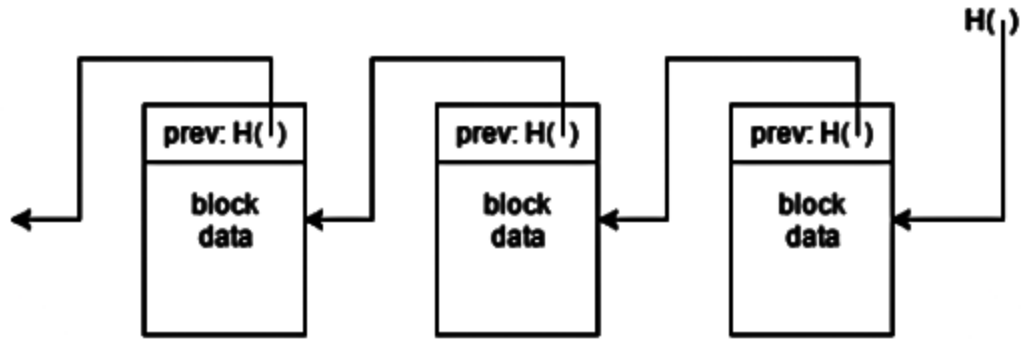


Fig. 2: Blockchain Structure: a Continuously Growing List of Ordered and Validated Transactions

Each block is verified using cryptography to make sure that it follows the sequence of its predecessors. The mining process is referred to as "mining" or "proof of work". The goal is to have the network's nodes compete to have their blocks added to the blockchain.

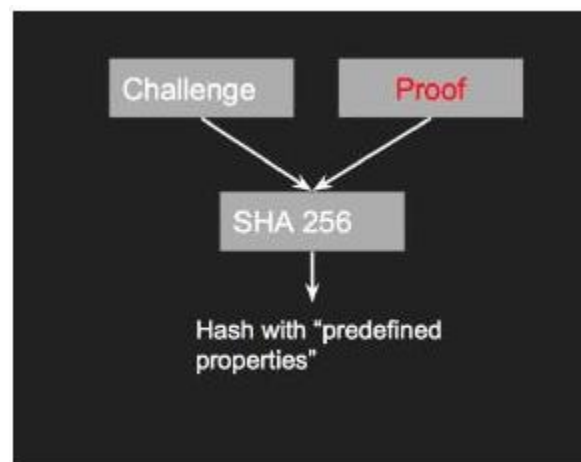


Fig. 3: Bitcoin Proof of Work Concept

The winning solution is a distributed mining system that uses game theory and cryptography to ensure that the network can reach a consensus regarding each block. All transactions are kept in the blockchain and are shared among all network nodes. Smart contract accounts are accounts that are associated with a specific contract code. These accounts can be triggered by functions or transactions from other contracts. To prevent exploitation, Ethereum has implemented a payment protocol that enforces a fee for processing transactions. Testnets are an Ethereum-based development environment that enables developers to create smart contracts without paying gas. Instead, they provide free or unlimited gas. lightweight testnets nodes are used for small-scale testnets. They are very fast and provide good error messages. Ethereum nodes are used for large-scale testnets.

These are typically referred to as Geth. Geth is a set of Ethereum nodes that are used for connecting to large-scale testnets. These are typically referred to as heavyweight nodes.

3.3 Smart Contracts

Ethereum smart contracts can be written in Solidity, a complete programming language that's built on top of the Ethereum Virtual Machine. It enables decentralized apps to run on the blockchain. Several smart contracts are made for the different functionalities such as for blood donation with features to search the donor by location, name, blood group, age, and request for blood. And, has similar features to organ donation, searching by name, organ, age, and location (PHC). The patient-Doctor record manager includes patient details, doctor details, medical prescriptions, and other reports. It also includes a Fitbit health tracker, tracking allergies, and medication procedures.

3.4 Truffle

Truffle is an Ethereum development environment that simplifies the work of developers. It features a robust testing framework and an asset pipeline. An automated contract testing pipeline that supports both web and console apps. It generates new contracts and tests that automatically rebuild assets during development. This tool supports both web and console apps.

3.5 Ganache

Ganache features a graphical user interface that can simulate Blockchain networks and live-test Smart Contracts without requiring you to set up real test networks or use a remote network.

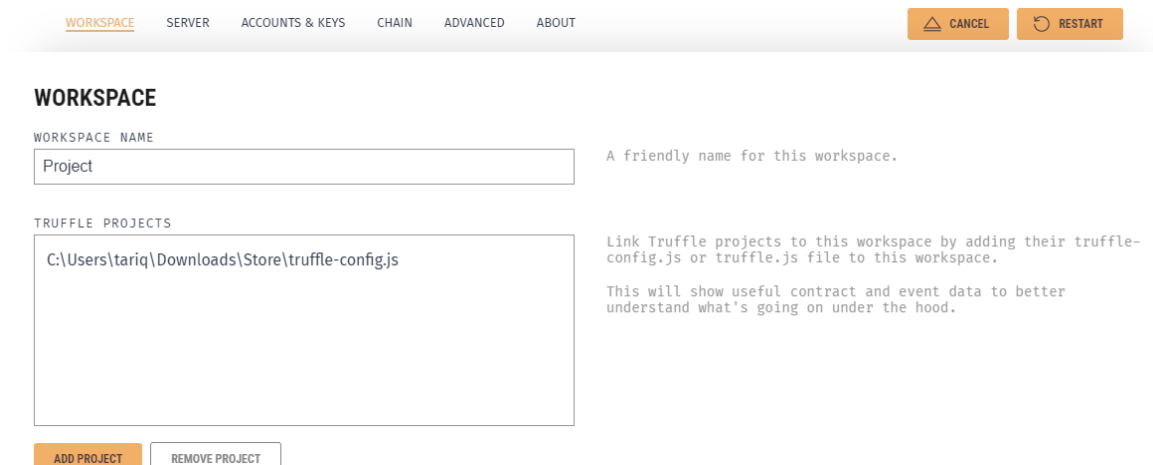
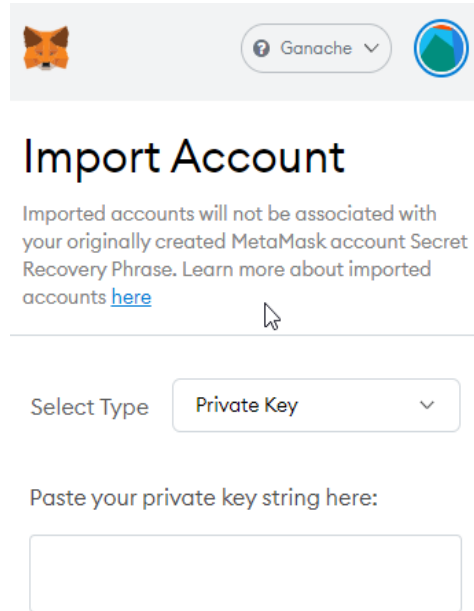


Fig. 4: Import truffle-config.js

3.6 Metamask

You do not register it on a website, but rather install it as an extension to your Chrome browser. Also, we will transact different blockchain-based coins like Ethereum.



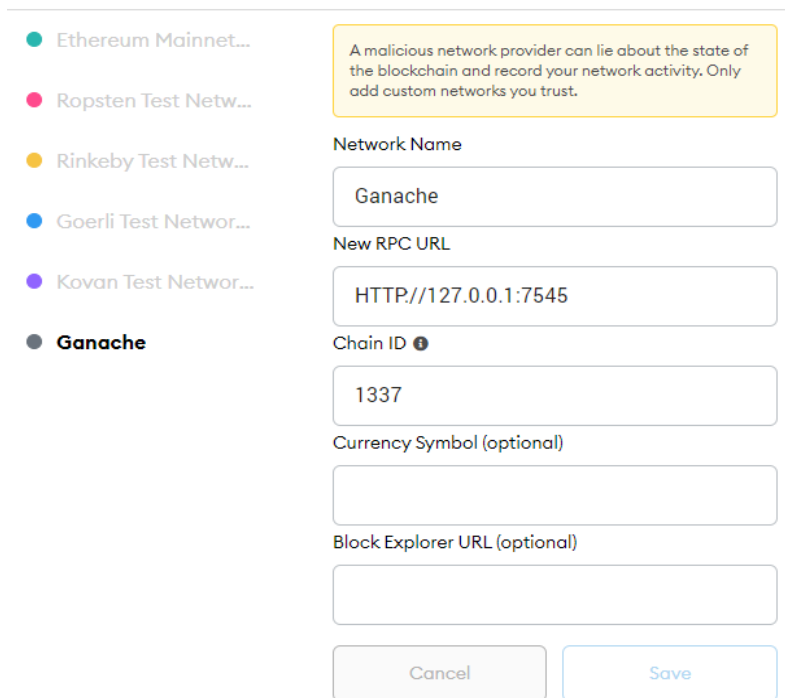
Import Account

Imported accounts will not be associated with your originally created MetaMask account Secret Recovery Phrase. Learn more about imported accounts [here](#)

Select Type: Private Key

Paste your private key string here:

Fig. 5: Import Private key from Ganache



Ethereum Mainnet...

Ropsten Test Netw...

Rinkeby Test Netw...

Goerli Test Networ...

Kovan Test Networ...

Ganache

A malicious network provider can lie about the state of the blockchain and record your network activity. Only add custom networks you trust.

Network Name: Ganache

New RPC URL: HTTP://127.0.0.1:7545

Chain ID: 1337

Currency Symbol (optional)

Block Explorer URL (optional)

Cancel Save

Fig. 6: Add New RPC

In metamask every transaction on the Ethereum blockchain the sender needs to pay some fees for performing that operation this fee is known as Gas. Every transaction contains the gas limit and gas price in it. Gas Price is the fee the transaction sender is willing to pay for gas and the Gas Limit is the maximum that could be paid for this transaction.

3.7 IPFS

IPFS was designed by Juan Benet and developed by Protocol Labs with the help of the open-source community in 2014, IPFS is a network transfer protocol designed to create persistent and distributed storage and sharing of files. IPFS combines features of existing technologies, including DHT, BitTorrent, Git, and SFS, to achieve the primary function of storing data locally and connecting nodes to each other for data transfer. IPFS was originally designed to build a better resource network than the now commonly used HTTP protocol to compensate for the shortcomings of HTTP. Compared to HTTP, IPFS exhibits advantages such as fast download speeds, global storage, security, and data perpetuation. IPFS is essentially a content-addressable, versioned, peer-to-peer hypermedia distributed storage, and transport protocol. It has the following features. Content Addressable: IPFS only cares about the content of the file, generating a unique hash mark from the file content, which is accessed by the unique mark and checked in advance to see if the mark has already been stored. If it has been stored, it is read directly from other nodes, without the need for duplicate storage, saving space in a sense. Slicing large files: Files placed in IPFS nodes do not care about their storage path or name. IPFS provides the ability to slice and dice large files, downloading multiple slices in parallel when used. Decentralized, distributed network structure: Such a network structure is suitable for solving bottlenecks in the blockchain's storage capacity by storing large amounts of hypermedia data on IPFS. Encrypted storage: IPFS adds a cryptographic hash unique to digital information to the encrypted data, and the corresponding hash of the stored file cannot be changed. The hash corresponds to the file one-to-one. In an IPFS network, there is no need to take into account the location of the server and the name and path of the file. When a file is placed in an IPFS node, each file is given a unique hash value calculated based on its contents. When access to a file is requested, IPFS finds the node where the file is located based on the hash table and fetches the file. IPFS combined with blockchain can be a good solution to the blockchain storage problem.

3.8 Connecting to Ethereum Client

Ethereum clients expose several methods over JSON-RPC for interacting with them from within an application. However, interacting directly over JSON-RPC passes on several burdens to the application developers, such as

- JSON-RPC protocol implementation
- Binary format encoding/decoding for creating and interacting with smart contracts

- 256-bit numeric types
- Admin command support - e.g. create/manage addresses, sign transactions web3.js

This JavaScript API is compatible with Ethereum. It can run as a Node module, a component, or an embeddable JS. web3j is a Java library that can run on the Ethereum network. Core features:

- Interaction with Ethereum clients over JSON-RPC via Java types
 - Supports all JSON-RPC method types
 - Supports all Geth and Parity methods for managing accounts and signing transactions
 - Sending of client requests both asynchronously and synchronously
 - Auto-generation of Java smart contract function wrappers from Solidity ABI files
- Currently, the go-Ethereum and Parity clients are supported.

CHAPTER 4

EXPERIMENTAL METHODS

The workflow of the proposed scheme mainly contains four parts. This section describes each part, and the specific workflow is shown in Figure 7. Smart contracts are not only related to the implementation of access control, but also the storage of medical information, and are therefore at the heart of this solution. There are three smart contracts in total: policy contract (PSC), access control contract (ASC), and medical record contract (RSC).

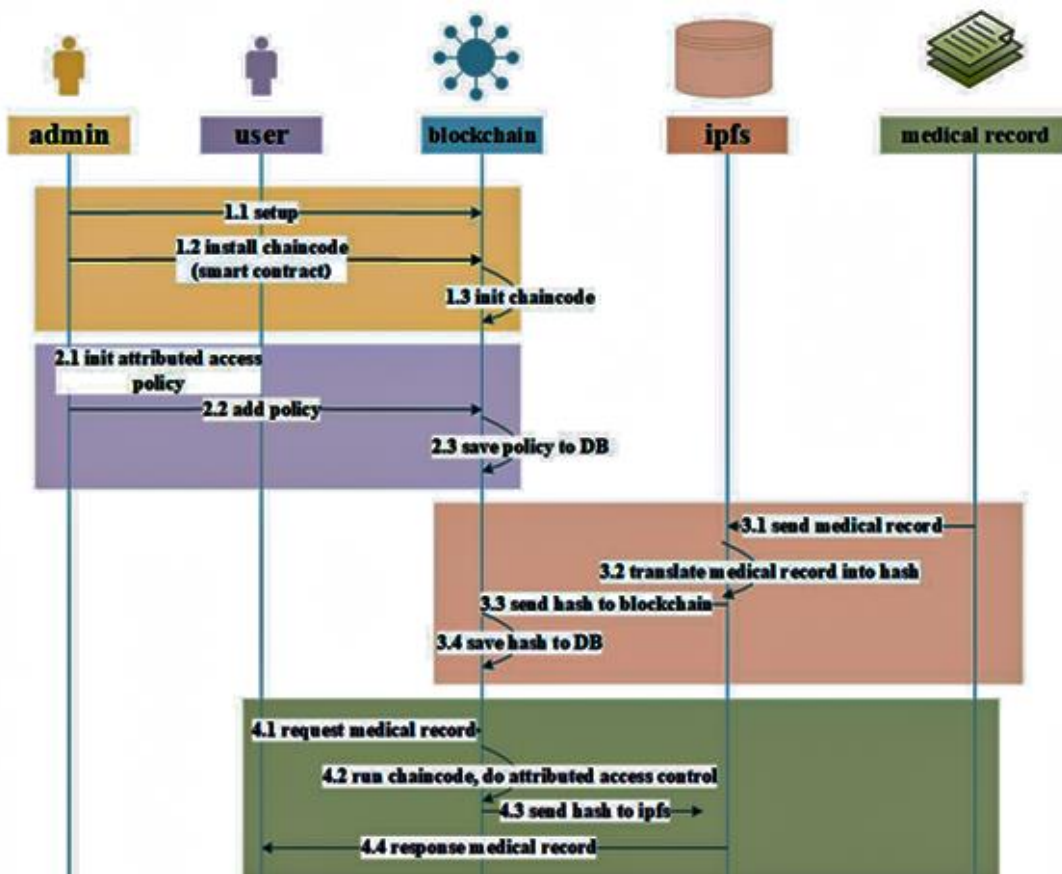


Fig. 7: The Workflow of the Proposed Scheme

4.1 Policy Contract (PSC)

The PSC provides the following methods to manipulate ABACPs.

CheckPolicy(): PSC needs to verify the validity of the ABACP by this method. Each ABACP should contain AS, AO, AP, and AE, and all four attributes should be satisfied for this policy to be valid.

AddPolicy(): The PSC needs to run the CheckPolicy() method before calling this method to add the policy, and only after the policy is legal can the policy be written to SDB and blockchain. The details are shown in Algorithm 1.

DeletePolicy(): This method will be called in two ways. Firstly, the administrator will call this method to delete an ABACP. Secondly, when the CheckAccess() method is executed and a policy is found to have expired, then this method will be called automatically to delete the useless policy. This is shown in Algorithm 2.

UpdatePolicy(): This method is called when an administrator needs to modify an ABACP. This method is called when the administrator needs to modify an ABACP. The modification record is also written to the SDB and the blockchain. This method also executes the AddPolicy() method at the end after the policy is updated, adding the modified policy back to the blockchain.

QueryPolicy(): all policies are stored in the state database CouchDB (a kind of key-value pair database) and the administrator can query the details of the desired ABACP by using the property AS or AO.

Algorithm 1 PSC.AddPolicy()

Require: ABACP

Ensure: Ok or Error

```
1: APIstub ChaincodeStub ← Invoke()
2: if CheckPolicy(ABACP) == False then
3:   return Error(BadPolicy)
4: end if
5: AS, AO ← ABACP
6: ABACPid ← HASHsha256(AS + AO)
7: err ← A APIstub.PutState(ABACPid, ABACP)
8: if err! = null then
9:   return Error
10: end if
11: return Ok
```

Algorithm 2 PSC.DeletePolicy()

Require: AS, AO**Ensure:** Ok or Error

```
1: APIstubChaincodeStub ← Invoke()
2: PolicyID ← HASHsha256(AS + AO)
3: err ← APIstub.GetState(Id)
4: if err! = null then
5:   return Error
6: end if
7: err ← APIstub.DelState(PolicyID)
8: if err! = null then
9:   return Error
10: end if
11: return Ok
```

4.2 ETSC Verification & Data Addition Phase in the Blockchain Network

ETSC is a program written in a particular programming language like solidity, Python, Kotlin, or Go. It is a self-inflicted, immutable, and self-authenticated program, that is helpful to designing real-world distributed problems simply.

Algorithm 1 Algorithm for Admin working

START

Input: Enrollment Certificate (EC) requested from CFA

Output: Access to P_E , and D_E transactions for all $(P_E, D_E) \in I_N$

Initialization: Admin should be valid node. Admin can Write / Read / Update / Add / Remove Nodes (P_{ID} , D_{ID} , PT_{ID} , C_{ID} , R_{ID})

```
1: procedure ADMIN(( $P_{ID}$ ,  $D_{ID}$ ,  $PT_{ID}$ ,  $C_{ID}$ ,  $R_{ID}$ ))
2:   while (True) do
3:     if ( $P_{ID}$  IS VALID) then
4:       if ( $P_{ID} \notin IPFS$ ) then
5:         Add_patient to the IPFS network
6:         Add_patient ( $I_N$ ,  $P_{ID}$ ),  $P_{details}$ 
7:         Grant_access ( $P_{ID}$ ,  $P_{details}$ ,  $U_{Name}$ ,  $Pr_k$ )
8:       else
9:         if ( $REC\_P \notin I_N$ ) then
10:          Create_Records ( $P_{ID}$ ,  $REC\_P$ ,  $I_N$ )
11:        else
12:          Update_Records ( $P_{ID}$ ,  $REC\_P$ ,  $I_N$ )
13:        end if
14:      end if
15:    else
16:      Not_exist ( $P_{ID}$ )
17:    end if
18:    if ( $D_{ID}$  IS VALID) then
19:      Add_doctor to the IPFS network
20:      Add_doctor ( $D_{ID}$ ,  $I_N$ )
21:      Grant_access ( $D_{ID}$ ,  $U_{Name}$ ,  $Pr_k$ )
22:    else
23:      Not_exist ( $D_{ID}$ )
24:    end if
25:    if int N; {0 means unpleasant behaviour, 1 means pleasant behaviour} then
26:      if (behaviour_node(N)) then
27:        Not update( $P_{ID}$ ,  $D_{ID}$ ,  $C_{ID}$ ,  $PT_{ID}$ ,  $R_{ID}$ )
28:      else
29:        Remove or update( $P_{ID}$ ,  $D_{ID}$ ,  $C_{ID}$ ,  $PT_{ID}$ ,  $R_{ID}$ )
30:      end if
31:    else
32:
33:    end if
34:  end while
35: end procedure
```

Although, the design is faultless. ETSC is challenging for language developers. In our proposed scheme, we determine the six types of entities $E = EP, ED, EA, EC, ER$, and EPT , which are linked with the ETSC via the Ethereum network. Each entity has an Externally Owned Account (EOA) to interconnect with the Ethereum blockchain. The Certificate Authority (CFA) in the ETSC describes illustrious health institutions, that accept or do not accept the doctor's experiences. It has the facility to verify the documents of a doctor who impulse to be qualified as a certified doctor.

CHAPTER 5

RESULTS AND DISCUSSION

This section computed the results mathematically by using some standard values for ID, Nonce, Hash function, Digital Signature, Timestamp, IPFS hash, and many more.

5.1 Communication Cost

The two entities are participating in ET transactions through the Admin Entity. The patient is having an ID of 128bit, and a 256bit hash code (generated using the SHA-256 algorithm). Now we compute the communication cost between Admin and Patient Entity. The communication cost of a block header is calculated as the sum of communication costs of the previous Hash (256 bits), Hash Root (256 bits), Digital Signature (320 bits), Timestamp (32 bits), Merkle Root (32 bits), and Version (32 bits) which is 928 bits. The hash output of 968 bits input after message digest (Block Header Value + nonce + Padding) is calculated using the SHA-256 algorithm which is 256 bits. Therefore, the total communication cost of PoW is the addition of the costs of every entity ID (128 bits) and Hash Output (256 bits) which is 384 bits. The total communication cost for the validation process is 992 bits including 384 bits for particular any entity present during the validation process, Digital signature of the entity is 320 bits, the hash (which is generated by IPFS) is 256 bits, and the Entity Timestamp 32 bits (File modification by the specific entity). Hence, the total communication cost for ET block creation and validation process is the sum of the costs of patient and doctor entity 968 bits (384 bits +384 bits). We concluded that the communication cost of the ET blockchain network is increasing with the increase in the number of transactions and entities.

5.2 Computation Cost

For computation time, the standard summation operation takes 1ms, the SHA-256 algorithm takes 2.7ms for block processing, the Hash algorithm takes 2.7-ms for the validation process in IPFS, and the data appended takes 0.5ms, Consequently, the computation cost (CC) from Patient to doctor is the summation of the patient's CC1 + Doctor's CC2 computation cost. The computation cost of the patient (CC1) is calculated as 6.9ms and the Doctor's computation cost (CC2) is 6.9ms, so the total computation cost total is the sum of the CCs of individual entities, for example, $CC1 + CC2 = 13.8ms$. Now, the computation cost increases as the block preparation and key transfer times increase for an increasing number of transactions.

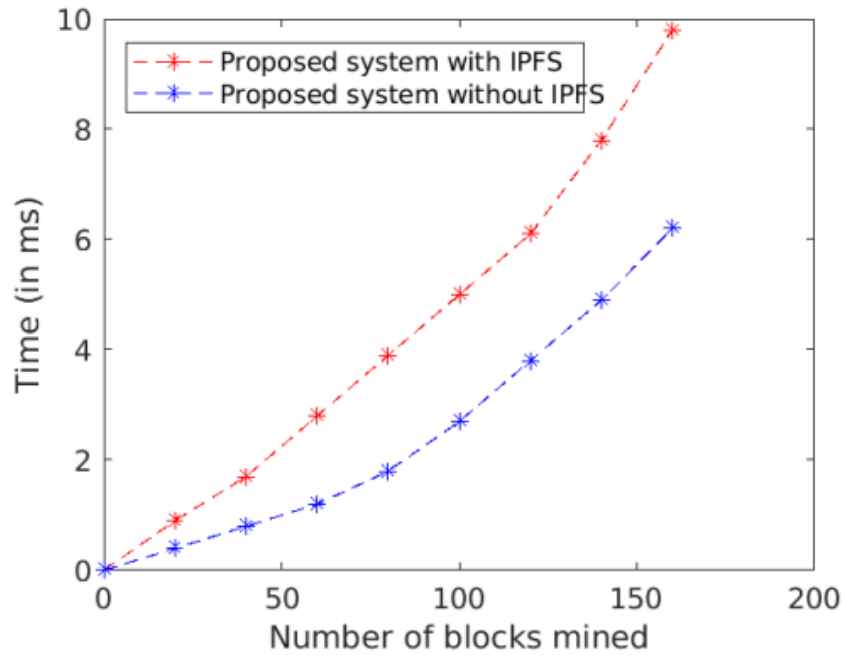


Fig. 8: Comparison of Data Storage Cost

5.3 Blockchain Data Storage Cost

In the proposed system, the transactions are stored in off-chain and on-chain storage locations. Blockchain also called on-chain storage keeps sensitive information such as keys, SSNs, and hash values. But, the off-chain storage, i.e, IPFS stores other information such as historical medical records and addresses, which are not sensitive information. To store data in the blockchain directly is very much costly, rather IPFS offers free storage. So, Keeping non-sensitive information in the IPFS network makes the system cost-efficient. Figure 8 shows the comparative analysis of the data storage cost of the FAIR approach with or without the IPFS system, which depicts that the approach with IPFS is cost-efficient.

CHAPTER 6

IMPLEMENTATION OUTPUT

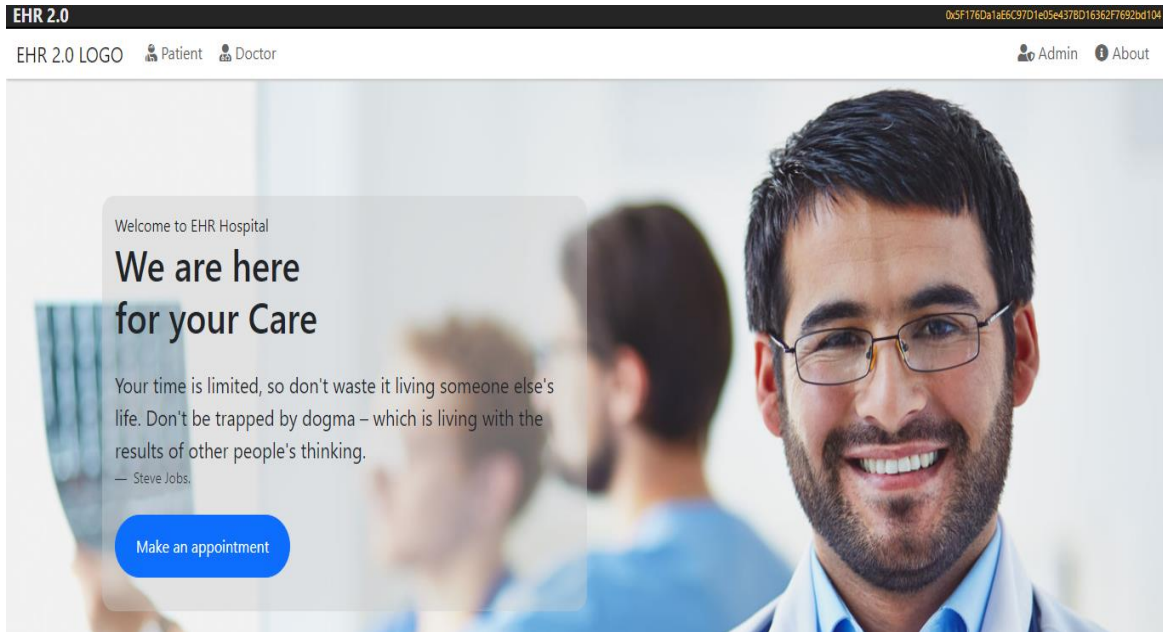


Fig. 9: GUI of Application

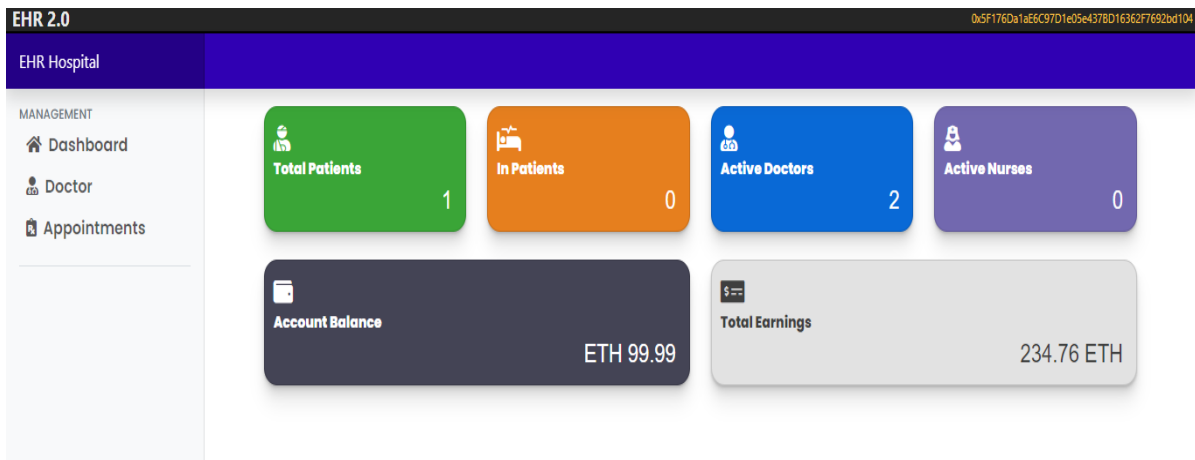


Fig. 10: Admin Panel

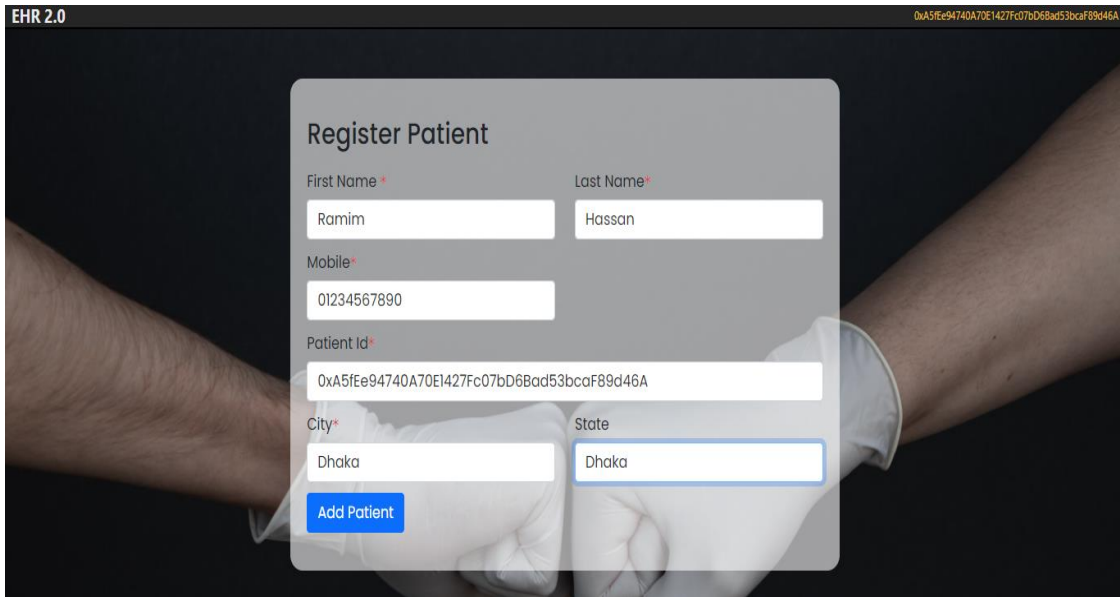


Fig. 11: Patient Register Page

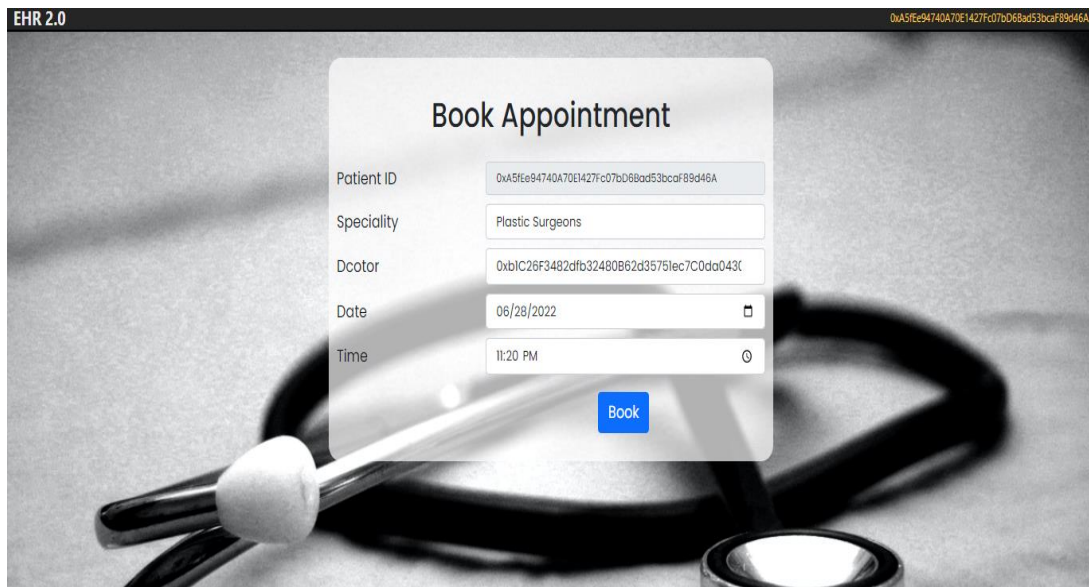


Fig. 12: Patient Book Appointment

```

▼ Object 1 register.component.ts:33
  city: "Dhaka"
  fName: "Ramim"
  lName: "Hassan"
  patID: "0xA5fEe94740A70E1427Fc07bD6Bad53bcaF89d46A"
  phone: "01234567890"
  state: "Dhaka"
  ▶ [[Prototype]]: Object

adding Patient blockchain.service.ts:143
IPFS hash : QmNXEic5joWfEm7ScDjggVXfptsLwau9XEycpnR81xCwF blockchain.service.ts:146
result 1 blockchain.service.ts:151
▶ Object register.component.ts:38
true 'Checking is Patient' progress_card.component.ts:29
▶ Array(2) appointment.component.ts:38
▶ AbstractContract blockchain.service.ts:114
1 blockchain.service.ts:120
1 appointment.component.ts:48
▶ Object appointment.component.ts:76
true 'Checking Patient....' progress_card.component.ts:29
1 patient-service.service.ts:38
QmNXEic5joWfEm7ScDjggVXfptsLwau9XEycpnR81xCwF patient-service.service.ts:70

```

Fig. 13: Data IPFS Hash

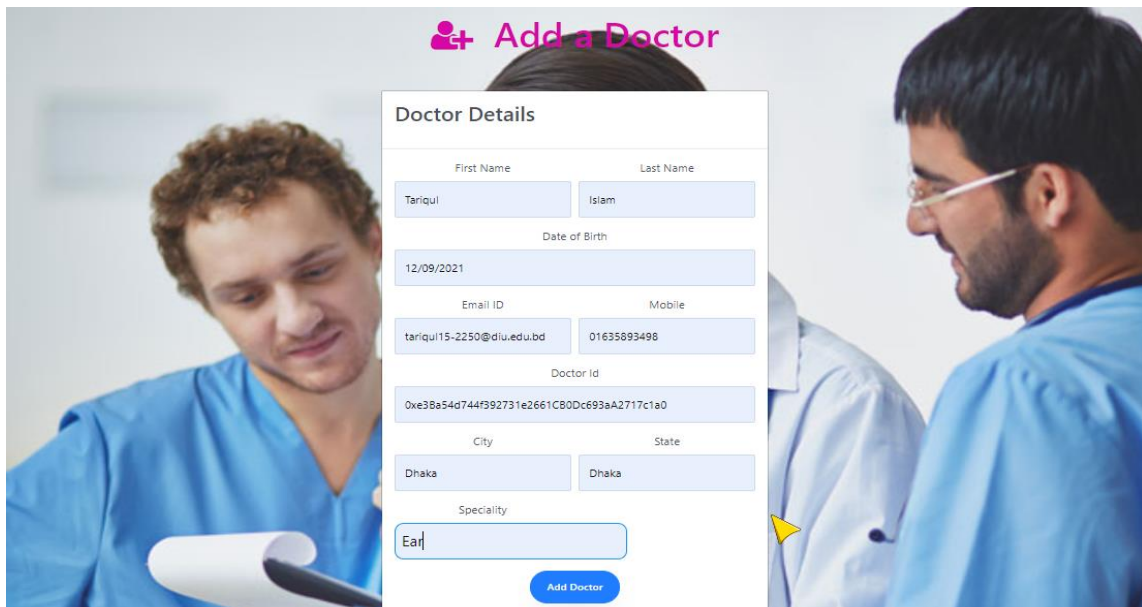


Fig. 14: Add a New Doctors

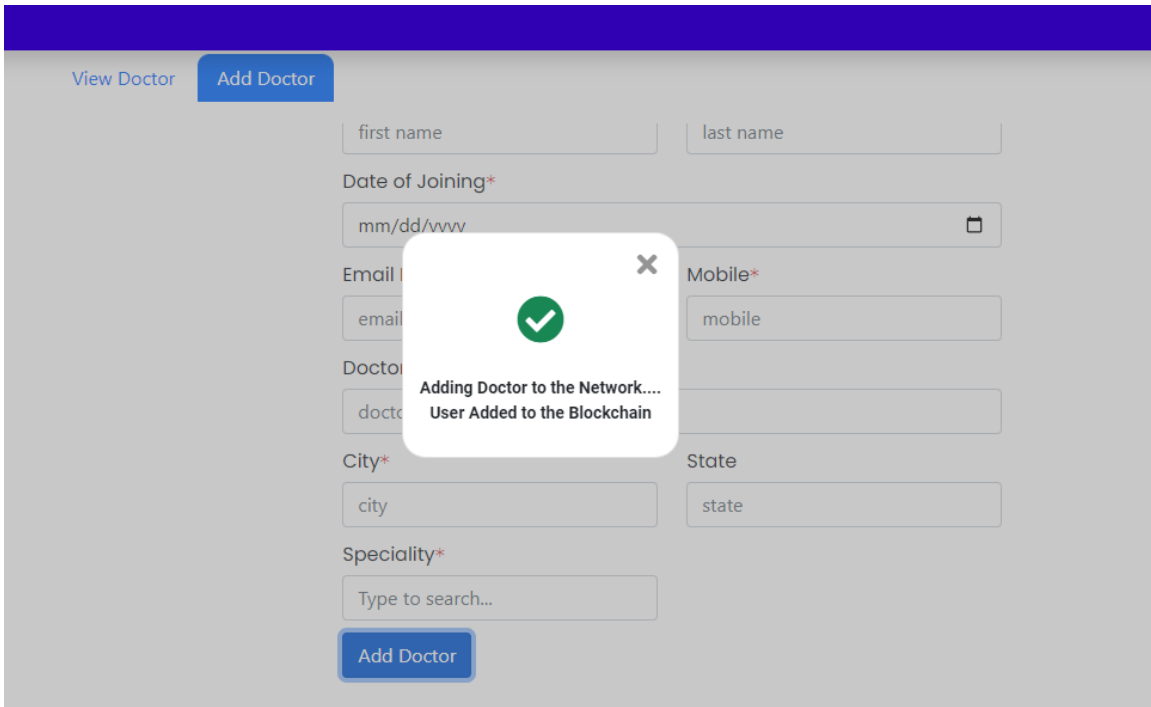


Fig. 15: Blockchain Transaction

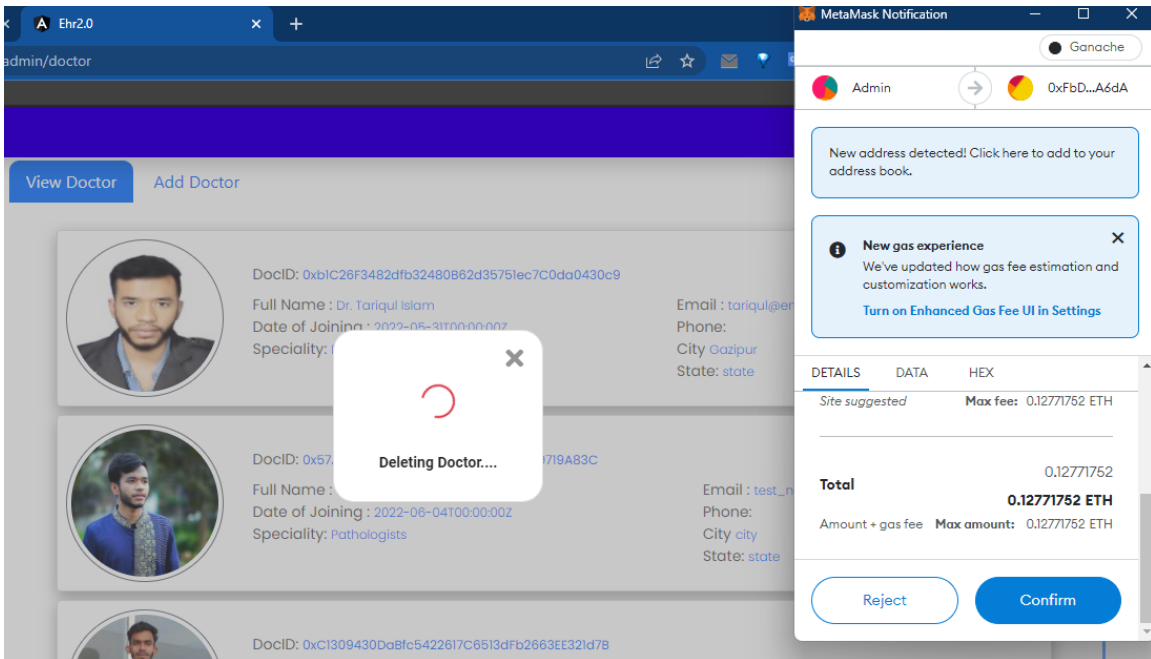


Fig. 16: Blockchain Total Amount with the Gas Limit

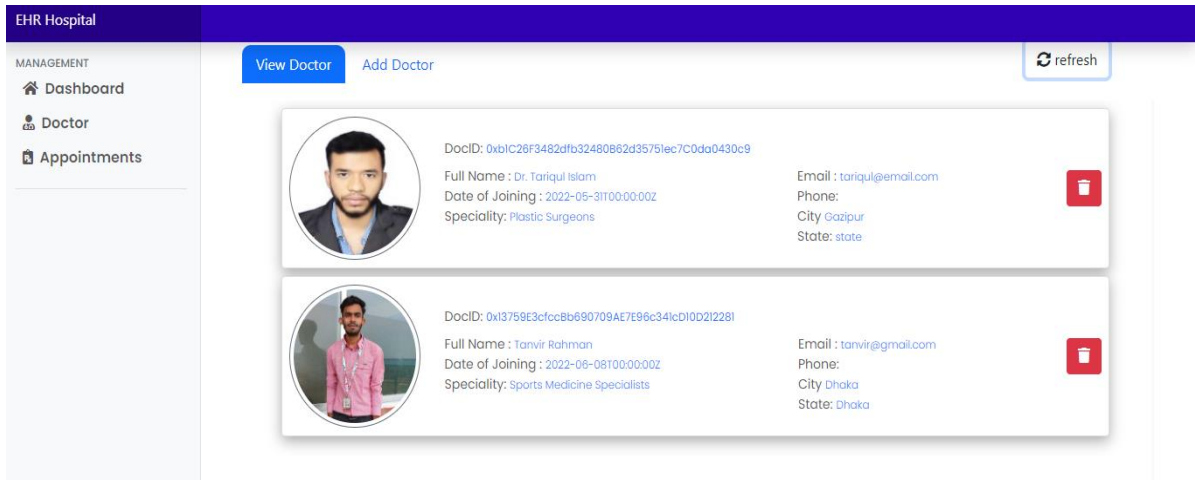


Fig. 17: Doctor Dashboard

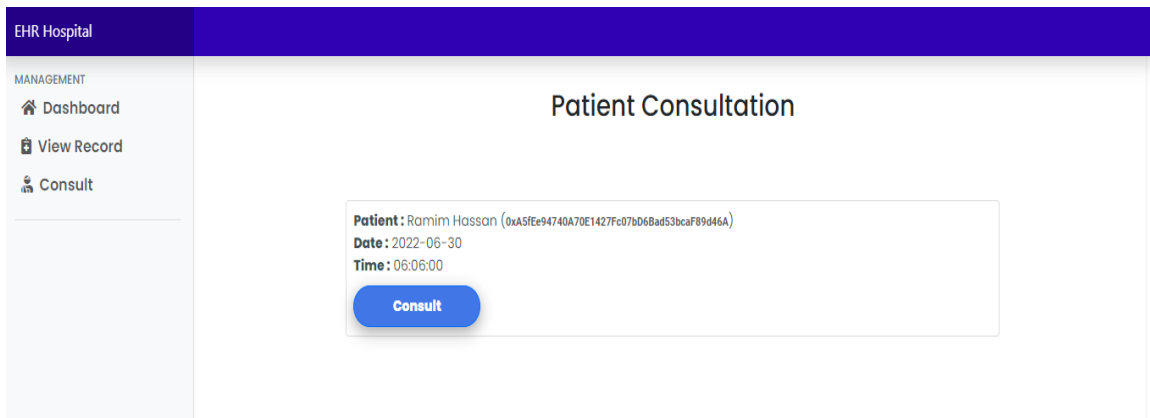


Fig. 18: Add a New Doctor to the Application

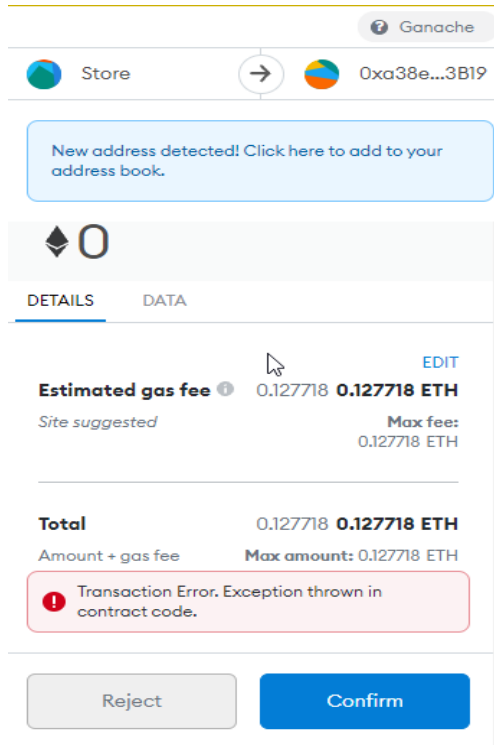


Fig. 19: Adding Cost by Ethereum in Metamask

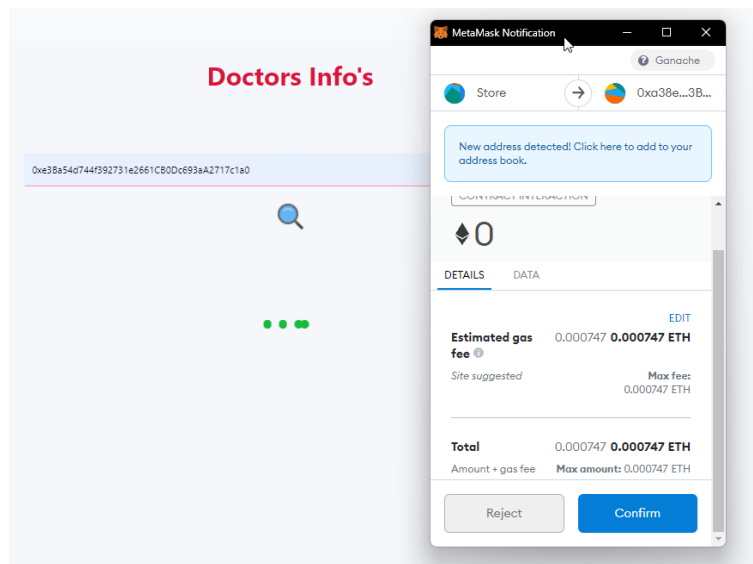


Fig. 20: Info's Check

CHAPTER 7

FUTURE WORK AND CONCLUSION

As we continue to work on our platform, we have identified several key areas of potential future work. First, we are engaging with various healthcare stakeholder groups across the industry. In the future, the system will be able to share information with insurance companies. Also, it provides a secure way for sponsors to donate money to people in need without the intervention of others (more trust in charity). The system is a proof-of-concept that shows how decentralized technology could enable secure, interoperability EHR systems. Its key component is a content-access system that authenticates patients' medical record access while allowing them to store and share their data. Our aim to unleash the possible applications of blockchain technology and also indicate the challenges and potential aspects of blockchain in health infrastructure. In recent years this technology has become trendy because of its cryptocurrencies. Blockchain technology has great potential in the field of healthcare. In this work, the author successfully represents a review of blockchain technology in healthcare which will be very helpful for further research in this field. This paper is based on the blockchain network. Here the healthcare system is made by creating an electronic record medical record management system called EHRs is created. Blockchain technology supports Ethereum and observes this data by itself. Here all the transactions are tracked by this system, It makes the system more secure. All the publications are independently examined by the reviewer. And this result describes that it has a higher quality of patents and journal papers compared with conferences and other literature papers. As blockchain technology has great potential in healthcare infrastructure that's why it should be used more in this field. Blockchain technology is very advantageous for its security, data processing, and access control. Pham et al. [15] aim to suggest a smart contract based on a blockchain network that makes a remote healthcare system that will manage all the information of doctors and patients. Blockchain technology has great potential in the field of healthcare infrastructure. That's why it has become popular and very much used in this sector. In this work, the authors propose a procedure to store medical information effectively that will be consistent with the patient's health situation. A smart contract is made by Ethereum based on

blockchain technology. First, Both the doctors and patients have to register in these smart contracts. As Ethereum can observe data by itself that's why it examines all data of patients and doctors. A sensor shows a patient's previous transaction in this system. Blockchain technology is very beneficial to use. This technology has created a great impact on healthcare. This technology is doing a fantastic job to make the system secure, data processing, and access control.

CHAPTER 8

ACKNOWLEDGMENT

The authors would like to thank Daffodil International University for your support and collaboration on this thesis.

REFERENCES

- [1] Novikov, Sergey P., et al. "Blockchain and smart contracts in a decentralized health infrastructure." 2018 IEEE International Conference "Quality Management, Transport, and Information Security, Information Technologies"(IT&QM&IS). IEEE, 2018.
- [2] Gürsoy, Gamze, Charlotte M. Brannon, and Mark Gerstein. "Using Ethereum blockchain to store and query pharmacogenomics data via smart contracts." *BMC medical genomics* 13 (2020): 1-11.
- [3] Griggs, Kristen N., et al. "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring." *Journal of medical systems* 42.7 (2018): 1-7.
- [4] Nguyen, Dinh C., et al. "Blockchain for secure ehers sharing of mobile cloud-based e-health systems." *IEEE Access* 7 (2019): 66792-66806.
- [5] Yang, Wei-Kai, Jie-Si Chen, and Yeong-Sheng Chen. "An electronic medical record management system based on smart contracts." 2019 Twelfth International Conference on Ubi-Media Computing (Ubi-Media). IEEE, 2019.
- [6] Khatoon, Asma. "A blockchain-based smart contract system for healthcare management." *Electronics* 9.1 (2020): 94.
- [7] Javed, Ibrahim Tariq, et al. "Health-ID: A Blockchain-Based Decentralized Identity Management for Remote Healthcare." *Healthcare*. Vol. 9. No. 6. Multidisciplinary Digital Publishing Institute, 2021.
- [8] Sharma, Ashutosh, et al. "Blockchain-based smart contracts for the internet of medical things in e-healthcare." *Electronics* 9.10 (2020): 1609.
- [9] Jabbar, Rateb, et al. "Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity." 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT). IEEE, 2020.
- [10] Omar, Ilhaam A., et al. "Exploiting Ethereum smart contracts for clinical trial management." 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA). IEEE, 2019.
- [11] Hölbl, M., Kompara, M., Kamišalić, A., & Nemeč Zlatolas, L. (2018). A systematic review of the use of blockchain in healthcare. *Symmetry*, 10(10), 470.

- [12] Andola, Nitish, et al. "SHEMB: A secure approach for healthcare management system using blockchain." 2019 IEEE Conference on Information and Communication Technology. IEEE, 2019.
- [13] Omar, Ilhaam A., et al. "Ensuring protocol compliance and data transparency in clinical trials using Blockchain smart contracts." BMC Medical Research Methodology 20.1 (2020): 1-17.
- [14] Ekblaw, Ariel, et al. "A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data." Proceedings of IEEE open & big data conference. Vol. 13. 2016.
- [15] Pham, Hoai Luan, Thi Hong Tran, and Yasuhiko Nakashima. "A secure remote healthcare system for a hospital using blockchain smart contract." 2018 IEEE Globecom Workshops (GC Wkshps). IEEE, 2018.

Plagiarism

ORIGINALITY REPORT

29%	27%	2%	22%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	dspace.daffodilvarsity.edu.bd:8080 Internet Source	16%
2	www.x-cart.com Internet Source	2%
3	Submitted to University of Wolverhampton Student Paper	2%
4	Submitted to Daffodil International University Student Paper	1%
5	Submitted to University of Greenwich Student Paper	1%
6	www.educba.com Internet Source	1%
7	jozilla.net Internet Source	1%
8	Submitted to Coventry University Student Paper	1%
9	www.freecodecamp.org Internet Source	1%

10	Submitted to Middle East College of Information Technology Student Paper	<1 %
11	Submitted to University of Liberal Arts Bangladesh Student Paper	<1 %
12	ir.msu.ac.zw:8080 Internet Source	<1 %
13	Submitted to Birzeit University Main Library Student Paper	<1 %
14	comprehensivofeltre.it Internet Source	<1 %
15	www.reyank.com Internet Source	<1 %
16	Submitted to Eastern Mediterranean International School Student Paper	<1 %
17	Submitted to University of Colombo Student Paper	<1 %
18	Submitted to The British College Student Paper	<1 %
19	Submitted to Universiti Teknikal Malaysia Melaka Student Paper	<1 %

20	Submitted to University of Central England in Birmingham Student Paper	<1%
21	www.herik.hanna.facit.edu.br Internet Source	<1%
22	Submitted to University of Bristol Student Paper	<1%
23	Submitted to University of Mauritius Student Paper	<1%

Exclude quotes On

Exclude matches Off

Exclude bibliography On