BLOCKCHAIN: A DISTRIBUTED SOLUTION TO EXAM RESULT DATABASE SECURITY IN A DECENTRALIZED WAY

BY

MD. FERDOUS HAQUE
ID: 161-15-6753

This Report is about the Partial Fulfillment of the Requiring for the Degree of Bachelor of Science in Computer Science and Engineering

Supervised By

Narayan Ranjan Chakraborty
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science and Information Technology
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

DECEMBER 2019

APPROVAL

This Project/internship titled "BLOCKCHAIN: A DISTRIBUTED SOLUTION TO EXAM RESULT DATABASE SECURITY IN A DECENTRALIZED WAY", submitted by Md. Ferdous Haque, ID No: 161-15-6753 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 has been held on 06 December 2019.

BOARD OF EXAMINERS

Dr. Syed Akhter Hossain
Professor and Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Chairman

Saiful Islam
Senior Lecturer
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner

Shaon Bhatta Shuvo
Senior Lecturer
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner
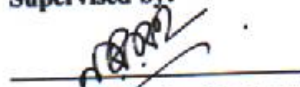
Dr. Dewan Md. Farid
Associate Professor
Department of Computer Science and Engineering
United International University

External Examiner

ii

DECLARATION

I hereby declare that this project has been done by us under the supervision of **Narayan Ranjan Chakraborty, Assistant Professor, Department of CSE** Daffodil International University. I also declare that neither this project nor any part of this project has been submitted elsewhere for the award of any degree or diploma.

Supervised by:

Narayan Ranjan Chakraborty
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Submitted by:

Md. Ferdous Haque
ID: 161-15-6753
Department of CSE
Daffodil International University

iii

ACKNOWLEDGEMENT

At first, I would like to express my heartiest gratitude and gratefulness to almighty Allah for His godly blessing that help in every aspect in completing the final year project successfully.

I also like to express my sincere gratitude, thankfulness and appreciation to my honorable project supervisor **Narayan Ranjan Chakraborty, Assistant Professor**, Department of CSE Daffodil International University, Dhaka, for his noteworthy, valuable advices, constructive suggestions and sincere guidance for my thesis with all the necessary facilities for assimilation, research and preparation for the project.

I also need to address my heartiest gratitude to **Professor Dr. Syed Akhter Hossain, Head,** Department of CSE, for his caring help to finish my project and also to other faculty member and the staff of CSE department of Daffodil International University.

The express of my gratitude to my family for their constant love and support is worth mentioning. Finally, I would like to take this chance to express my gratitude to one and all, who directly or indirectly, have lent their hand in this venture.

ABSTRACT

Blockchain is nowadays one of the most emerging fields in the computer science technology for data storage and transaction on online data among researchers and academics for the recent years. Hence, Blockchain implementation on exam result storage database is demandable field to work on. Aim of this thesis is to create a web application to store exam results data using blockchain that can perform to store data by an owner who have the authority to input the data and the other users would only view the data using their hash id. Here, I have used an Ethereum smart contract which is written by solidity programming language to create a contract that perform or execute the code based on some given conditions. I have used ganache framework for testing and debugging and development purpose of the smart contract. I have used the web3.js library which is the official Ethereum JavaScript API. It is used to interact with Ethereum smart contracts and some html and CSS codes for designing purpose. In this thesis I have successfully create a web application. And in the backend part it stores data using the blockchain cryptography. As in recent we are more concerned about securing our data storage because of tampering issues. Exam result tampering is nowadays a common problem in our country and so blockchain implementation in exam result storage database is a noteworthy task. Therefore, our study has highlighted the research studies in the field of decentralized and distributed ledger in exam results database.

TABLE OF CONTENTS

CONTENTS   **PAGE**

CHAPTER

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Introduction

We are living in an age where techniques of communicating are getting digitalized every moment. Almost everything is dependent on technology is a significant cause of it. The rapid growth in a reduction in size, computer electronics, interaction in a wireless medium in the technical environment has donated to incredible advances in our way of living [1]. People are getting used to technology to make their life easy and more comfortable. It is the result of our change in our way of living and interacting with others [1]. The current advancement in technology is simply a modifying version of previous expertise in the technical field, and the effect of digital technology is immense. Still, the way sometimes we use technology brings trouble in our way of living. Our social living gets threatened because of the negative use of technology. What is called modern technology, technically not so not up to date in most cases? For example, storing the kinds of data on the internet globally, locally, or in any private network technology has evolved with years, but there are some lacking in securing the data in the database.

The most striking attraction for illegal dwellers is databases because they comprise valued and delicate information, which can vary from economic or academic stuff to commercial data and individual employee data. Cybercrime is the issue that occurs due to this rupturing of the contents of the databases of the companies. For this, tampering problems in the database is common in recent years. A lot of examples that happened where illegal activity is done by hacking the database of large organizations can be described. Apple, Enron, eBay, and Equifax data holes were the topic in the newscast in recent times, for example, with the name of rare. Blockchain enables solutions not previously possible [2].

A specific technical environment provides the securing of the blockchain [3]. Blockchain follows the rule of distributed consensus. The mechanism which is known as distributed in

1

nature is disreputable because it has restricted scalability, which was perceived for ages as a primitive that is harmonized and applied in only those applications that are in frantic need of reliability and amongst only limited lumps [4]. The year that is passed, a person who is the doyen of capitalists of Silicon Valley named Marc Andreessen ranked the most significant creation, which is the distributed consensus mechanism of blockchain upper than the creation of the internet and the revolution of internet is suppressed by the blockchain [5].

The Internet is today's wrecked, and the data that we have used or store is not in our control, and also, we do not have the instinctive value reimbursement layer. It has been forty years since we are accepting internet for our digital communication, the styles of our data being following the rules of solitude database of the electronic device referred as the computing medium where the information is split into blocks and is centralized for storing these blocks of information by any individual or an organization where sometimes it gave the authority for serving and managing by any organization, read or write with the help of viewing. Sometimes it so happens that we lose control of our data because of the frequently accessed through the internet and so it is getting leaked, and the deal dweller gets them the power of storing our copy of data. As our everyday activities are dependent on an electronic device such as TV, car, digital watch, everything is sometimes linked with our personal data it happens for sometimes that hackers get into these personal data and private stuff and let ourselves for the threat of our privacy controlling under threat of tampering. Trust over the internet is getting questioned for this when it happens. It then scares the user of whether the data they have on the internet for using the advantage of interaction in wireless communication is secure or not. Providing security then becomes the most wanted concern. This is the type of problem that can be reduced if we implement blockchain in the way we transact, where there will be no centralized organization for the authorized purpose. Every transaction provides timestamp which cannot be changed or altered [6].

This technology has the advantages of robustness, but not like the web2, we know that the capability that is provided web2 is that we can read and write simultaneously in the web2, but we cannot execute anything in the web2 but the blockchain is different in the

performance capability of web2 instead storing information in blocks gives way to the new web interface where we can execute something which more of the technology provides then the web2. The block is created in the number of hashes which is linked together and make the way of immutability in the database that it generates. It also enables the feature of avoiding controlling by any single authority for manipulation of the blocks that contain data. It stores blocks of information that are linked across its network. And this reduces the risk of failing. Hashing data and properly stamping it gives the strengthening the way of security and also run the role of elimination of the risks that are originated due to data information of public data that is previously authorized centrally. The system that is provided by the blockchain restricts hackers who try to manipulate centralized data that is hackable. Today's biggest problem arises in securing data that is acknowledged to all and by all. Our dependency is on passcode and user information approvals in contacting our resources in the real-time internet transactions. The new emerging technology customs encrypting or data of information for ensuring security. The giving way to the new technology, which provides interaction in the name of web3, is the platform that is going to revolutionizes the way of our communication. In the name of a bitcoin transaction, the methodology of the blockchain is known. As it is providing transaction timestamp and other stuff like a connection to the previous blocks is the way that it creates is tracking capability. Tracking is mostly needed nowadays for a lot of organizations to understand or to get aware of the previous history about any transaction. So this gives a lot of benefits for the people who are doing commercial business or contract dwellers.

The importance of blockchain is not fully aware by a lot of companies who are badly in need of securing online transactions; it is, therefore, under the shadow of proper utilization[7]. As the transaction history is provided by the blockchain, it is, therefore, most needy technology for a lot of present organizational private applications [8]. In this study, we propose a database system that will run on blockchain cryptography. As for security concerns, there are no alternatives to blockchain implementation.

1.2 Objectives

The key expectation of this topic of the thesis is to have an environment where we can decrease the most unwanted problem of today's known as internet personal data security. I am mainly concerned about the securing of exam result storage data. As tampering with result data is somewhat a common issue in our country, there is no alternative to no think about that. Blockchain is nowadays known as the most emerging technology, which is based on the cryptographical algorithm. Linked of blocks that contain data and no way to tamper one data is possible in the chain of the blocks. So, it can be assumed that the blockchain implementation of the result database could give way to the new tamper-proof database.

1.3 Motivation

Data tampering is nowadays a common issue in our country, and it has its benchmark in tampering the exam results data. There is a lot of evidence which shows that the students are accused of being illegal in getting a chance in public universities and medical colleges by tampering their results. For this, the real talented students cannot fulfill their ambition and are not get treated in the right way, and thus, it brings a huge challenge in the growth of a country. A secure database is a must to reduce this kind of problem, and there is no alternative to blockchain implementation on the exam results database.

1.4 Rationale of the Study

The goal of this project is to implement blockchain-based database storage for the exam results in the sense of creating a tamper-proof environment for the database. In recent, there is a lot of case which shows the insecurity of exam results database due to this a lot well deserved students get missed out of their opportunity in getting their respective institution for their study.

1.5 Research Questions

➢ What is the role of blockchain in database storage?

➢ Can It give the solution to the security problem?

➢ How smart contracts can be created, and what is its role?

➢ Will the blockchain-based database work perfectly?

1.6 Expected Outcome

Today's era is about big data and how to handle it. The technology is getting digitalized day by day. In consideration of coping with this big data, there needs to be strong security to keep data away from tempering. The expectation of this research-based project is to create a web app for securing the exam results by using the blockchain technology in the backend of the web.

1.7 Report Layout

The whole study is well-ordered as follows, "Chapter 1" describes the key aims of this thesis, the inspiration behind this thesis. "Chapter 2" represented the literature review and related works in blockchain technology with the advancement of computer science. And the resources and methodology are described with the evaluation benchmark of different classification techniques in "Chapter 3". After that, the presented results and discussion are described with proper figures in "Chapter 4". And finally, the conclusions and future viewpoints of the research and recommendations are deliberated in "Chapter 5".

CHAPTER 2

BACKGROUND

2.1 Introduction

The advancement of technology makes it more rely on the fact that there needs to be a strong, secure database for keeping data and information safe from hackers and illegal dwellers. The most concerned aspect of this research-based project is to develop a database that is based on the technology named blockchain for storing exam results to ensure the security of the data. To do so, I need to study a lot on this topic to enhance the actual knowledge and why should it be implemented. Here, below, it is described my study on the various related works that are done all over the world.

2.2 Related Works

Blockchain nowadays has become one of the most promising fields to study because of its cryptographical algorithm that it is based on, which provides security in storing information or data. The most valuable thing of a business sector is the data of that organization that controls in every decision making process such as heaths, insurance, finance, and education [9]. Blockchain technology is the underlying concept of bitcoins [10]. It was in 2008 in the month of September when the idea first came into existence in the paper authorized by Satoshi Nakamoto, which was just a name and introduced the transaction idea using bitcoin in a way peer to peer to cashing [11]. The 2008 financial crisis caused a lot of people to lose trust in banks as trusted third parties [12]. In 2008, a person or group of persons known under the name of Satoshi Nakamoto published a paper [5] dealing with a new decentralized peer-to-peer electronic cash system [13]. This proposal was considered a unique idea to implement, and the working of bitcoin came into real-life transactions over the internet in the year 2009 onwards [14].

There are researches in the field of networks that are wirelessly connected and have the ability to sense the environment to introduce blockchain technology to enhance security. This field in computer technology requires a lot of study on securing purpose because there are way a lot of ways to harm this technology. In it, the decentralization of blockchain technology can play the most prominent role [13].

The voting sector is the field where we see that in our country, it is the most talkative issue that voting is not performed properly. Candidates' data on voting is said to be changed in most cases, which brings a lot of trouble. Sometimes electronic voting can be a threat of accuracy in voting. It seems that blockchain is the neediest technology in the voting technology in the online way [3].

Data integrity is said to be the most wanted factor in all the large companies and organizations; there is no denying the fact that if the data gets violated, it's a proper indication of the negative impact to rise on that organization [9]. Blockchain technology is built on the objective of providing data integrity, so it is effective clearly can be said.

There is no list of records for the food that we buy in general. And for this, there is no way we can detect the fraud whether they contaminate the food or not. If we implement blockchain for storing the record of the food in every transaction and the checking result of every contamination test, there would not be any possibility of being the target of the victim [2]. Moreover, the technology Blockchain can get us out of intermediaries who are in the look for collecting a lot of money in the interest of transacting [2]. Already the blockchain technology has come into existence in providing transaction safety of food, and it is Walmart the name of the organization that is using the blockchain technology [15].

Health is another talkative sector of implementing the blockchain technology to. There are a lot of reasons for that. For say, it is a must need to shortlist the problem of a patient, and it should be enlisted and get specific for every time a patient encounters a doctor [16]. The data that is provided by a doctor can come for good use in any other physician that the patient encounters.

7

2.2.1 Blockchain

Bitcoin came in the first place of discussion while we begin to think about blockchain [8]. Bitcoin actually the first implementation, which gives way for researches to think about the basis of the algorithm that is used nowadays named blockchain [17]. The main technicalities that the blockchain technology offers is that it is immutable tamper-proof and decentralized in the way it interacts transaction [6]. There is a specific condition that can be given to the blockchain how the method should perform on the internet or in the organization that uses it as in their database [18]. The database that is provided by blockchain has the nature of immutable and unalterable [19]. Every transaction in the blockchain is enlisted as a list of history, which then can be used for various purposes [6]. It's a linked list of blocks. Every block in the blockchain is linked to the previous block that contains a hash of that block, and there is a timestamp of the creation time of every block [6]. There is no way to alter or tamper a block, or if anyone does so, the whole blocks that are linked get damaged, and there needs to create a new chain of blocks. The database that is created using blockchain technology is decentralized, peer-to-peer, immutable, distributed. It has a consensus protocol.

2.2.2 Decentralization

Decentralization, which actually means there should be no central authority to use or manipulate the data without the acknowledgment of the participants who are in the blockchain network. The need for an intermediary for the help of transacting is valueless, and this can be diminished by the blockchain as it provides decentralization [20]. The impact of decentralization is that it reduces the cost also reduces the transaction time and finally provides the tamper-proof outcome [21].

2.2.3 Peer-to-peer database

The actual meaning of it is that there is no central controller in the network, and all participants talk to each other directly [20]. Peer-to-peer connections or transactions could be made using blockchain technology, which does not any help from intermediate

8

organizations, financial institutions, community organizations [17]. The peer-to-peer concept came int existence with the proposal of bitcoin, where the sender and receiver of bitcoin get transacted between two people without the help of any intermediaries [22]. After that, the algorithm is researched to give ways of peer-to-peer transactions on another transactional field of computer science [23].

2.2.4 Proof of Work

The term stands for validating the transaction by the participants of the network for the creation of a transaction [24]. All the participants agree on a certain condition, then it gets added on the blockchain. Proof of work provides a consensus mechanism that is given to the algorithm of the blockchain that is created, and the mechanism validates every transaction by the condition it provides [20]. The first application of proof of work came into existence with the establishment of bitcoin. Proof of work of the bitcoin provides the tracking result of every transaction [25].

2.2.5 Immutable Database

The term immutable means that it is once created cannot be changed or is impossible to change or delete [25]. In that sense, the immutable database refers to the database that is unchangeable or is impossible to change. Actually, it is not utterly immutable, but the way it shows the mechanism is considered to be immutable because no one can get into the blocks if anyone does so changing something would break the chain of the whole list of blocks [20]. Once the blocks of transactions are created, there needs to be an agreement for the users of the private network that they should remain as the contents and not be changed [26].

2.2.6 Consensus Mechanism

The consensus mechanism is the mechanism that is used for establishing proof of work [20]. It is the process where all the participants of the network come to the agreement that the transaction should be added or not. The steps are agreement, termination, validity, fault-

tolerant, integrity. The consensus mechanism is nothing but a way of validating a new transaction [26].

2.2.7 Distributed Ledger

The distributed ledger is the database that is distributed across all the participants who take part in the blockchain transactions [20]. It can be either a public blockchain or a private blockchain. Every participant in the blockchain transaction holds a copy of the shared ledger, but for accessing, he needs the crucial proper hash, and without this, he cannot even view the information of the block. This type of accounting restricts the method of data centralization, and there is no way that data gets centralized. The only blockchain does not provide a distributed ledger system; actually, the blockchain technology has this technique in the accessing process; that's why it is called to have distributed ledger [26].

2.2.8 Trust with Transparency

Trust in blockchain refers to the immutability mechanism of the blockchain, where anyone cannot easily change the transaction result and the blocks of information [20]. Transparency is that if the blockchain is public, anyone can view the result and get the results of the transaction that is made [16].

2.3 Research Summary

The above discussion has made it clear to us that as security is the primary concern of technology, there is a lot of implementation on the blockchain is proposed to impact significantly in the various fields of technology. The application of blockchain technology can surely be said in the growth, which is supposed to be rapid. And so, it is for not denying that it is going to revolutionize the advancement of technology by giving the most needed of recent times, which is security.

2.4 Scope of the Problem

Exam result is said to be the main achievement of a student to determine the hard work he put into learning things. Most of the results are stored in the SQL database or any kind of centralized database; it imagined to be secure, but there a lot of cases in our country where we have seen the big problem tampering results. It is because the database is not that secure, and hackers or illegal dwellers easily can access these databases and can-do tampering. The majority of the tampering happens during the varsity entrance examination, where deserving students lose their chance of passing the examination because of the illegal attempts done by illegal dwellers in changing the results with the interests of money.

2.5 Challenges

It is going to be a challenging task because the technology is a very new and emerging technology. We can hardly see some of the implementations that are done so far. The blocks that contain information about a student need to be chained properly, and the viewing of the results or tracing the previous information in the blocks is going to be a very difficult task. Another problem is to make a proper connection with the tools that I am using because there is a lot of issues that arise because of the version confliction.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Introduction

In this chapter, we are concerned about discussing the process of our implementation and the tools that I have used to perform our intended project. We will mainly focus on the architecture and the framework that I have made for the completion of our thesis. Here in the research subject instrumentation section, we will discuss the instrumental discussion of how it is done.

3.2 Research Subject and Instrumentation

Here I am going to discuss the research subject and the platform where I execute my project and, most importantly, how I will do the project. Instrumentation of the thesis will be discussed step by step.

3.2.1 Consortium Blockchain

Consortium blockchains can be realized if we have precise knowledge about the blockchain public. A consortium blockchain is the type of blockchain that holds no access restriction, which means that unconditionally, anyone with the connection of the internet can become a member of a blockchain that is public in nature. More precisely, we can say that anyone has the capability to read data that is included on the blockchain, and anyone is allowed to execute transactions on the blockchain, which is public. Significantly, there is a restriction too as to who can partake in the consensus procedure for blockchains that are the process that determines the individual who can add a block to the blockchain. Public blockchains are thought to be entirely decentralized, where control over the blockchain not in the hands of any individual. This is the type that we have created by the name, which is a smart contract.

3.2.2 Ethereum Platform

Ethereum is a platform that is the open-source, blockchain-based, user-friendly, public distributed decentralized environment, and operating platform featuring the smart contracts (scripting) rules. It is based on an improved kind of Nakamoto consent through a transaction-based way of conversions. Here I have used this platform to create a smart contract.

3.2.3 Creation of Smart Contract

This type of contract is a technique envisioned to simplify, legalize, the cooperation numerally, hence also the capability of a contract. Establishing the performance of trustworthy transactions without mediators is what this contract actually offers. These types of dealings are trackable and unchangeable. To create a smart contract, we need to use the online IDE named Remix. There are two evolving languages that are on the use of deploying contracts; one is solidity, and the other is Vyper. Solidity is the most used in this case. Solidity is a language that comes into existence in 2014. It is appropriately keyed, which lets complex, libraries, inheritance manipulator distinct kinds among all structures.
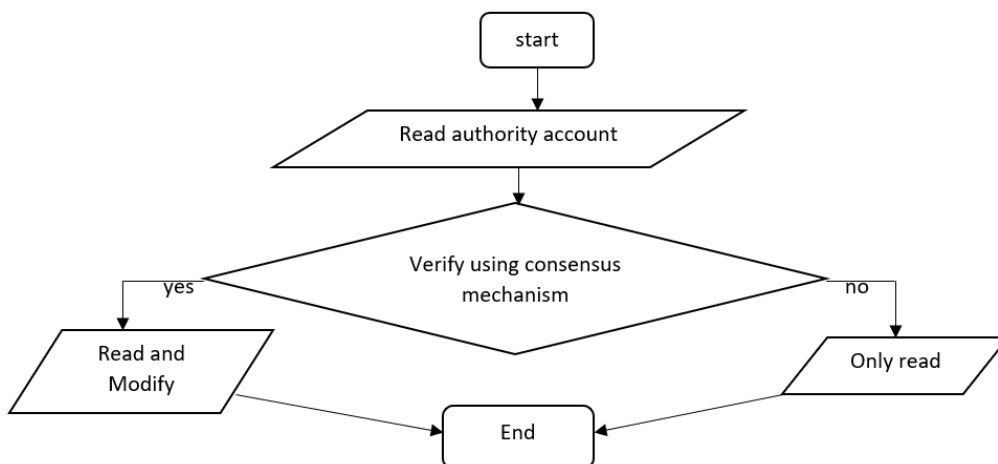

Figure 3.2.3.1: Defining the owner's requirement

At first, we have defined an address that can input the profile of a student and his result score, which can only be done with an address playing the role of owner. The exam result committee can play the task, and once the result is uploaded, it can be tampered with in later.
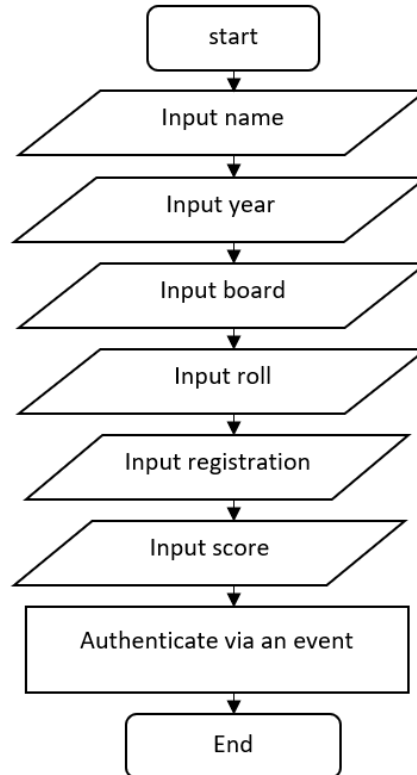

Figure 3.2.3.2: Student's information with proper event

Here, in the struct part, it holds the profile of a student. The blocks that are contained by a blockchain maintains the list of the history of all the transactions. Log tickets are the proof which is then contained by each block that contains every transaction. The contract manages the entries of every transaction. Events are dispatched signals the smart contracts can fire. Here we have used the event I indexed manner, which specifies that the history of the previous input profile of a student can be searchable.
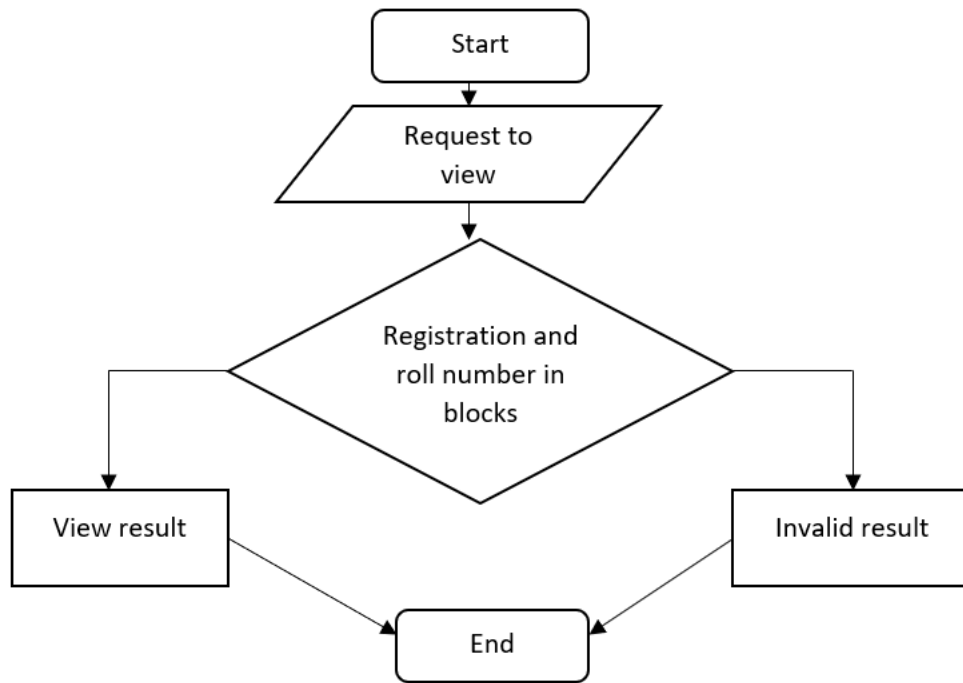
Figure 3.2.3.3: The functionality of the function

In the above scenario, it is seen that we have used functions. There are four types of Solidity functions: external, internal, public, and private. We have used the public functions because our intended program should work like anyone can view the result by accessing a hash address in the blockchain. There are two types of modifiers that we can use in functions one is a view, and the other is pure. By giving the function "view" modifier, we have made it a read-only function.

After working on the algorithm, we need to deploy our smart contract on the Ethereum online environment network. The address that we use to deploy our smart contract will be the owner's address, and our deploying of the smart contract will cost a very tiny amount of ether. There is a transaction cost that occurs, every time the authority input any student profile.
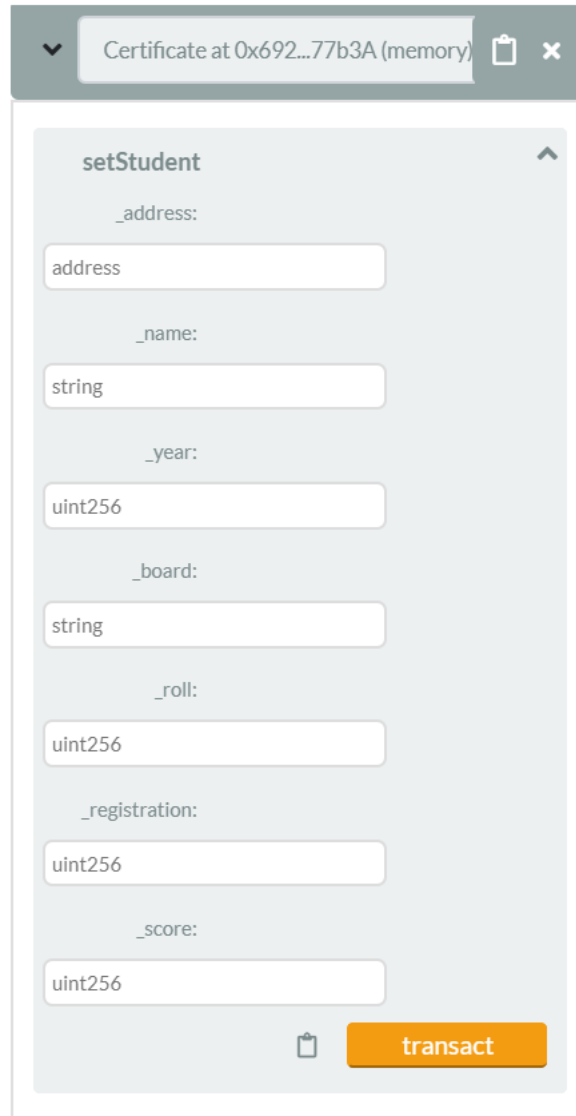
Figure 3.2.3.4: Owner's interface for creating transactions

Here it is the input of a profile that looks like, and every time after adding the student's info in it, the owners need to click on the transact button for the successful transaction of blocks.

```
transact to Certificate.setStudent pending ...

     [vm] from:0xca3...a733c
✅   to:Certificate.setStudent(address,string,uint256,string,uint256,uint256,uint256) 0x692...77b3a value:0 wei
     data:0x6f3...00000 logs:1 hash:0x573...3ac51

    status                          0x1 Transaction mined and execution succeed

    transaction hash                0x5732497895b59e76ec83294ce0250a509f47db7181f527b13c8599a8c833ac51 📋

    from                            0xca35b7d915458ef540ade6068dfe2f44e8fa733c 📋

    to                              Certificate.setStudent(address,string,uint256,string,uint256,uint256,uint256) 0x692a70d2e424a
                                    56d2c6c27aa97d1a86395877b3a 📋

    gas                             3000000 gas 📋

    transaction cost                178434 gas 📋

    execution cost                  152874 gas 📋

    hash                            0x5732497895b59e76ec83294ce0250a509f47db7181f527b13c8599a8c833ac51 📋

    input                           0x6f3...00000 📋

    decoded input                   {
                                            "address _address": "0x4B0897b0513fdC7C541B6d9D7E929C4e5364D2dB",
                                            "string _name": "Rakib",
                                            "uint256 _year": {
                                                    "_hex": "0x02"
                                            },
                                            "string _board": "Dhaka",
                                            "uint256 _roll": {
                                                    "_hex": "0x099b0e91"
                                            },
                                            "uint256 _registration": {
```

Figure 3.2.3.5: The actual backend mechanism of input transactions

After every transaction, this is the actual mechanism that happens as input. Here transaction, which is the block of the hash and the hash the generates from "from" is actually the owner's hash address. The gas represents the amount of gas that we can use, the limitation for say. Then comes the decoded input, which is the profile info that we have input. First, we have given the address under which a student or a user can only view the result of that particular individual.

```
decoded output                    {} ⎘
logs                              [
                                      {
                                          "from": "0x692a70d2e424a56d2c6c27aa97d1a86395877b3a",
                                          "topic": "0x8d2133c64cce6c939ae89265d421f83e098fa4815f9c0ab0d934c8fab0ae545
                                  e",
                                          "event": "StudentInfo",
                                          "args": {
                                              "0": "Rakib",
                                              "1": "2",
                                              "2": "Dhaka",
                                              "3": "161156753",
                                              "4": "53231547",
                                              "5": "93",
                                              "name": "Rakib",
                                              "year": "2",
                                              "board": "Dhaka",
                                              "roll": "161156753",
                                              "registration": "53231547",
                                              "score": "93",
                                              "length": 6
                                          }
                                      }
                                  ] ⎘ ⎘
value                             0 wei ⎘
```

Figure 3.2.3.6: The actual mechanism of output transaction

This is the framework of the output transactions

3.2.4 NodeJS

Node JS is a runtime environment. It is an open-source server environment that relies on JavaScript. Here we need to use this environment for creating the interaction of our smart contract with a user-friendly interface on the internet what the connection of the front end with the back end is. Node.js customs an event-driven, non-blocking I/O prototype that makes it trivial and efficient, faultless for data-intensive actual applications that route across distributed devices. Node.js is a slender, fast, cross-platform JavaScript runtime environment that is useful for both headwaiters and desktop applications.

3.2.5 Web3

If we go through the history of the web, we can get the idea that the first web, which was named web1, only holds the capability of a user to read, then came web2 where we could read and write; for example, we can say, Facebook. Web3 came with the real-life application of bitcoin, where we can read write and execute. Every invention in the web category revolutionizes our technology for interactions. The real-time environment of

©Daffodil International University

web2 gave way for the peer-to-peer transactions between two individuals or organizations with the help of intermediaries where the intermediaries act as the trusted unit, and they need to depend on the intermediary for the trusting issues. The problem arises because of getting a trusted environment. The web3 provides the solution to this problem. Here we have used the web3.js library. This new platform creates a new environment, which is the JavaScript Application Programming Interface. To install the web3.js library, we need to run the command that is given following in the command prompt of the node.js.

NPM install Ethereum/Web3.js — save

To run a web3 provider, we need to select it in the remix ide before deploying the smart contract.
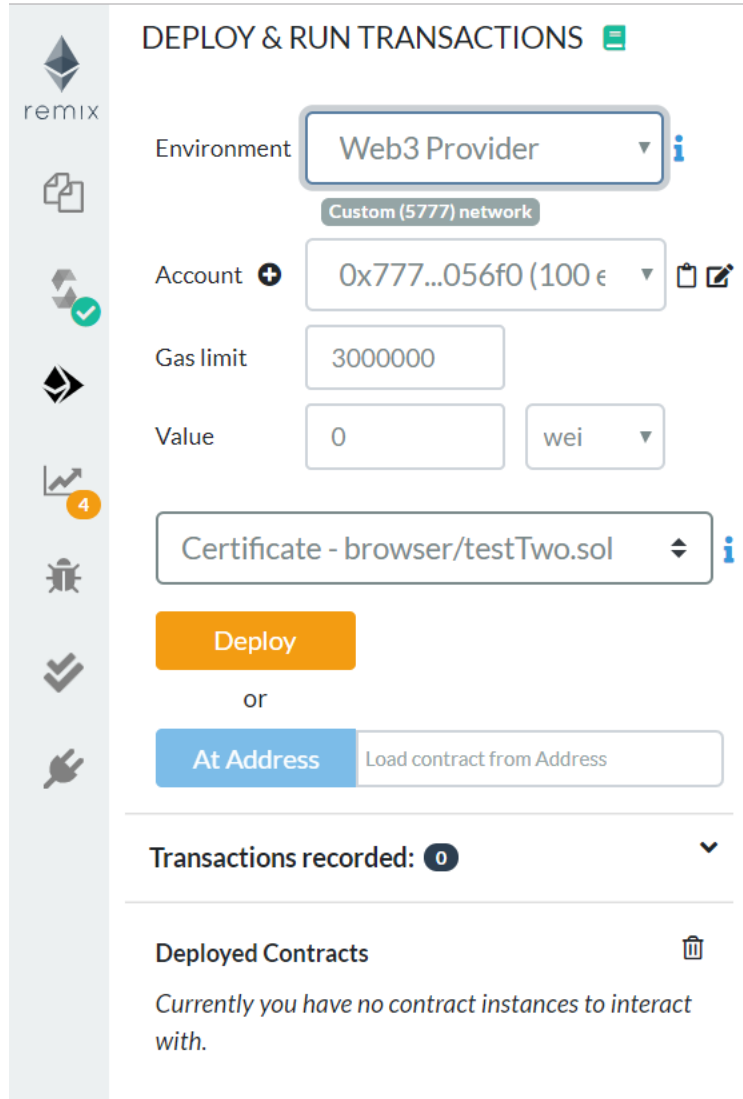
Figure 3.2.5.1: Selecting web3 provider environment in the DEPLOY & RUN TRANSACTIONS interface

To run the environment, we need to connect it with a node RPC. The platform that hosts the node RPC is provided by ganache. So, basically, we need to connect our smart contract by clicking the web3 provider environment where assign the host address, which is the RPC server of ganache CLI.

Figure 3.2.5.2: Selecting RPC SERVER in ganache

20

3.2.6 Ganache

Ganache is the platform which gives us ease in building a blockchain web app. It provides an RPC server that needs to be connected to the web3 provider. While we transact any information which actually is storing the student's information, it creates a new block in the ganache platform.
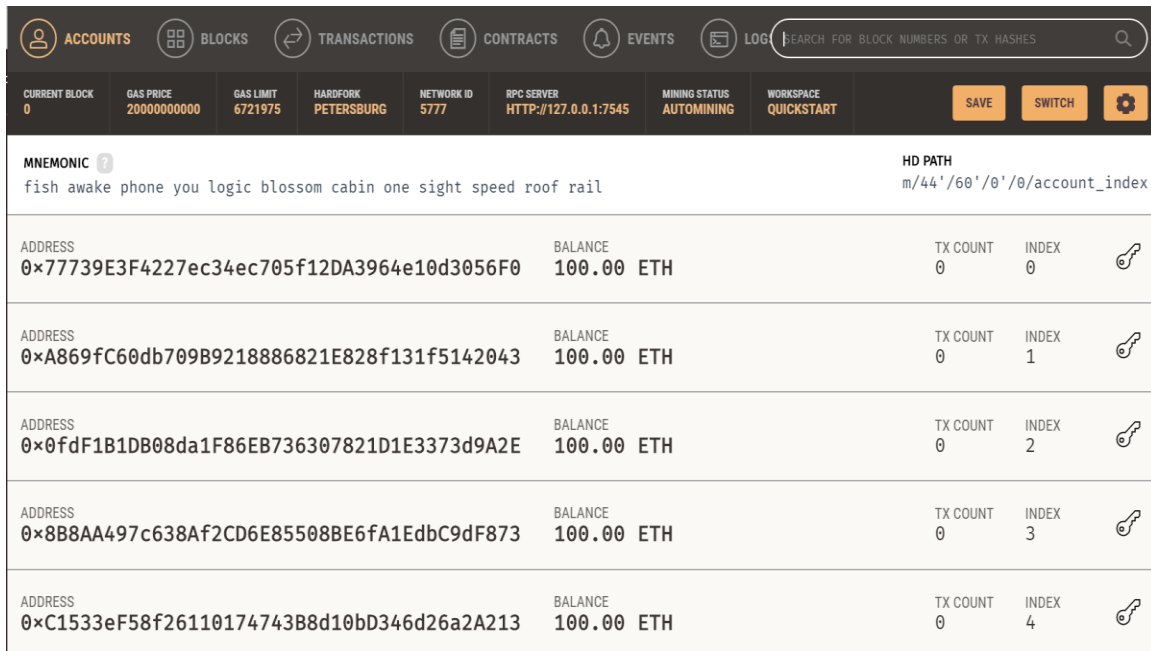

Figure 3.2.6.1: The interface of ganache

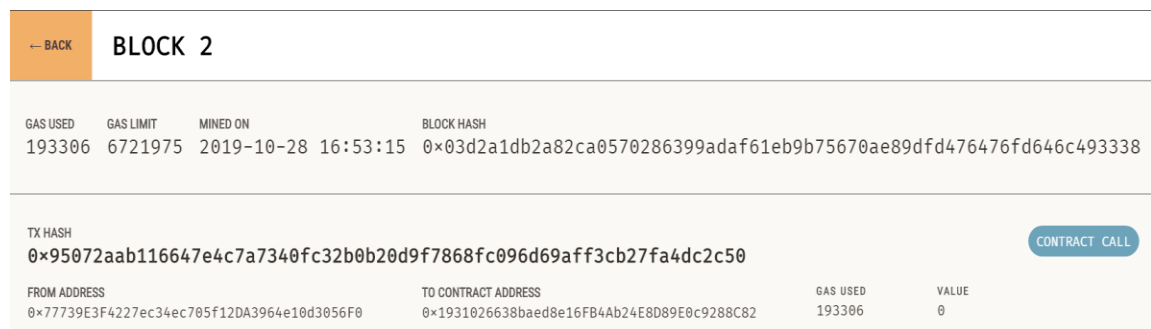We can use it for the testing of our implementation to see transaction ever is perfectly performing or not.

Figure 3.2.6.2: The blocks details in ganache

This is the example of a block that looks like after we generate a transaction in our smart contract.

3.2.7 MetaMask

It creates an environment that connects the web that is distributed. MetaMask lets to run the Ethereum decentralized application lacking running a full Ethereum node. It holds the identities of users or creators who deploy contracts; it helps in containing the allowing information for every user. It also works as the ether wallet to manage the balance of every user account. Every user who requests to see the outcome can view with the use of their MetaMask account, which provides a key.
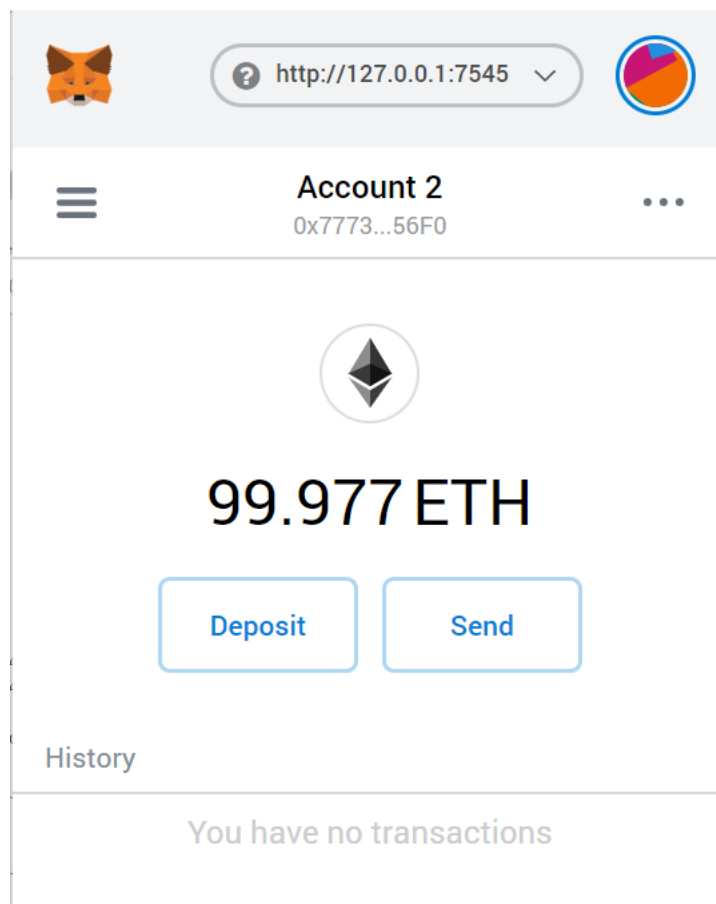

Figure 3.2.7.1: Example of account details in ganache

Here, for example, I am using this account as a possessor, and when I input a profile of a student and his score result, it cost me a tiny amount of ether for the transaction cost.

3.3 Implementation Requirements

In this implementation, we have used several tools and software to run our intended blockchain-based web app — the list of tools and software given below.

3.3.1 Hardware Specifications

- Operating System (Windows 7 or above)
- Hard Disk (minimum 4 GB)
- Ram (more than 2 GB)

3.3.2 Integrated Development Environments (IDE)

- Remix(online)
- Sublime
- Notepad++

3.3.3 Languages

- Solidity
- JavaScript
- HTML
- CSS

3.3.4 Software

- Firefox with the extension of MetaMask

CHAPTER 4

EXPERIMENTAL RESULTS AND DISCUSSION

4.1 Introduction

In this chapter, I will be discussing the final result of my experiment and some analysis on it. The final result of my implementation will be shown here. At first, I will show the owner interface who will input the profile and outcome of a student, and then I will be explaining the blocks that will be generated about the events of students. After that, I will discuss the user interface to interact with the user when an address is given.

4.2 Experimental Results

I have proposed to build a web application that runs on blockchain technology, which actually runs on a cryptographical algorithm. It is categorized as a consortium blockchain platform where the owner only has the authority to write about the profile of a student and his exam result, which is then stored in a decentralized blockchain database and is immutable and the owner himself cannot change it. When anyone wants to see the result, he will access to view the result through his hash address that is registered by the owner while creating the profile and giving the score.
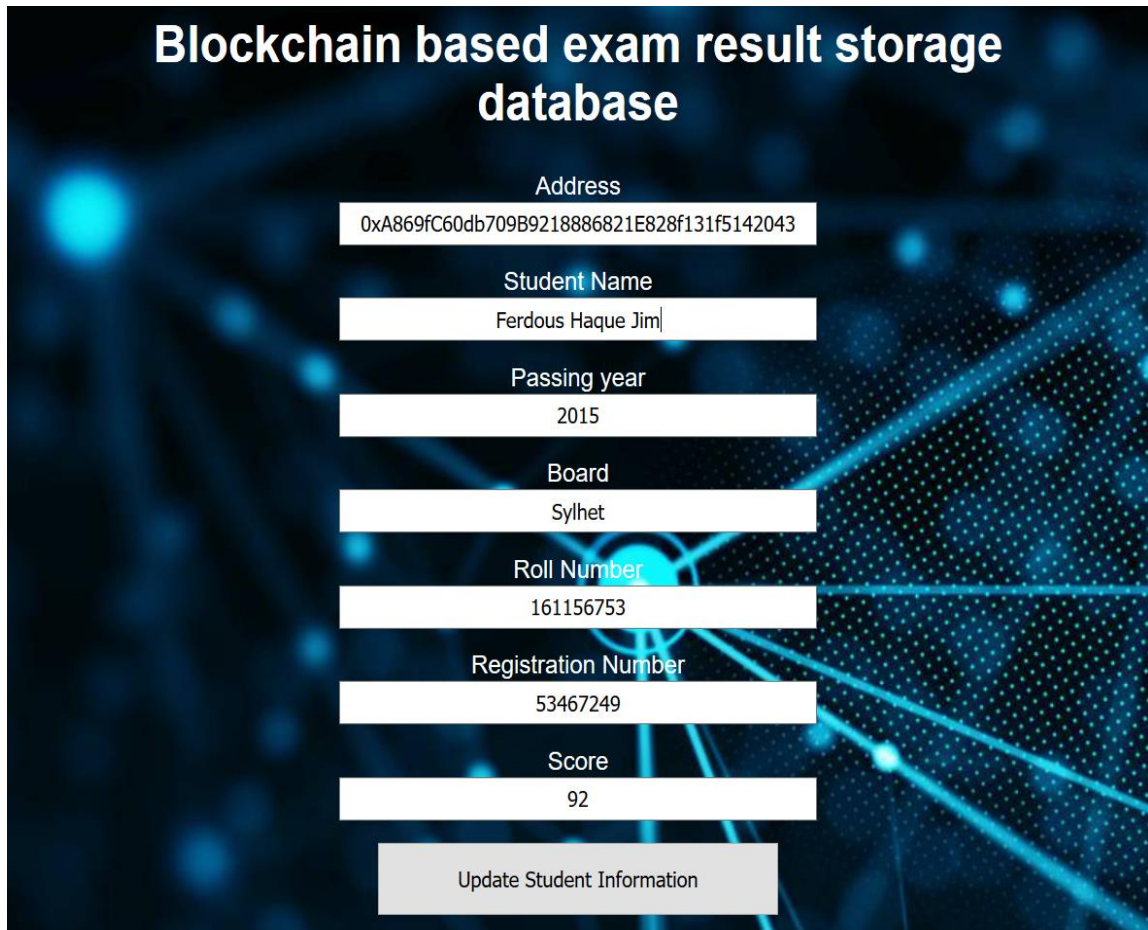
Figure 4.2.1: The web user interface for the owner

After clicking the update button above, the profile will be added as an event. The block of information that is added becomes immutable, and it cannot be changed or altered. And the information that is inserted one after another will be linked together as a chain of blocks. If anyone or any illegal dwellers try to change the score or any information, the chain of blocks will be disrupted, and all the information about all the students will be accessible, which will be known to the authority. So, firstly, it is really a very task to tamper the data, and if anyone does so, the hash will be changed of the block, and the chain will be disrupted. And so, it is called immutable in nature.
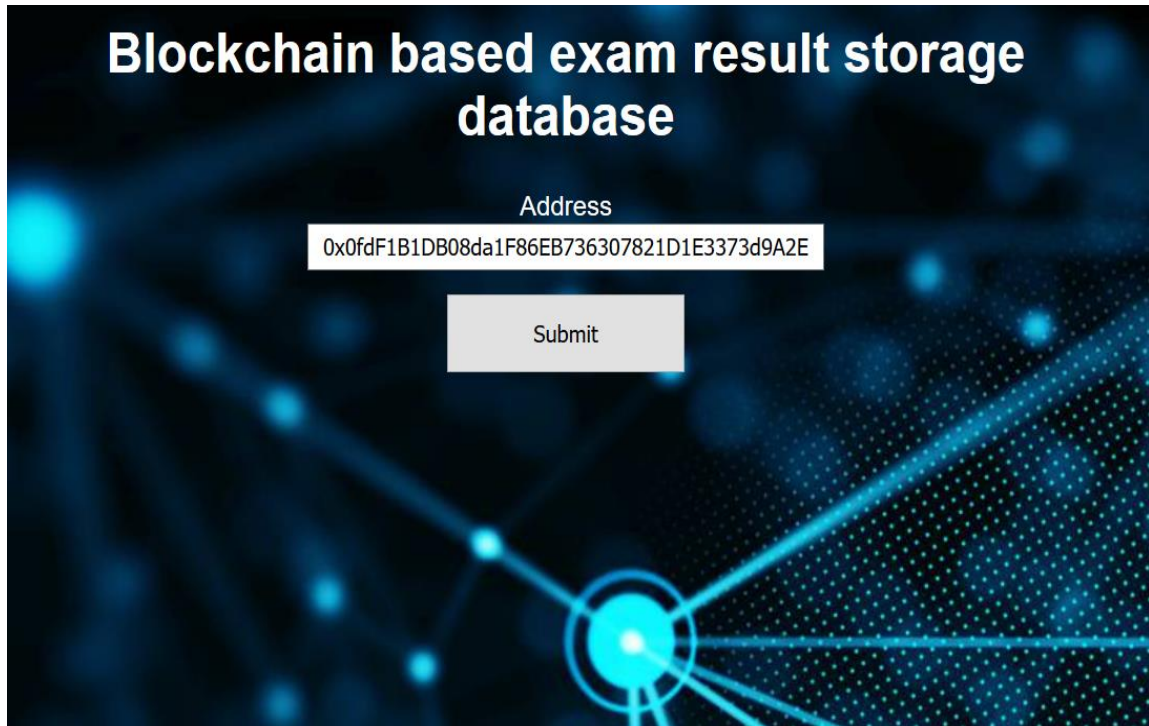
Figure 4.2.2: The web user interface for the viewer

The above figure is the user interface for anyone who wants to view the result by submitting the hash address. After submitting the address, he will get the following view,

Figure 4.2.3: The outcome of the resulting interface

4.3 Descriptive analysis

The motive of the implementation is to create a platform where we can clear out the most common problem of technology, which is security. We are advancing in technology, but the one question that we face in every phase of our advancement is security. As a result, it is not a fact of surprise that our database is no purely secure enough. In this thesis, I tried to use the most emerging technology in computer science, which is named blockchain, to secure our exam result database. Tampering in the exam result database is nowadays a widespread issue. It is most often seen that illegal dwellers always try to tamper the result score to benefit the student who is not hard-working or less deserving while getting a chance in the job field or good universities. Here we have used the consortium blockchain platform in the result database where the exam committee has the authority to input a profile of a student and his result score, and after clicking the input button, he cannot alter

or change the result. The user who wants to access to view the result of a particular student firstly, he will submit his address key and click on the submit button if it matches with the previous blocks of events generated by the exam committee authority, he will be able to view the result of a student.

4.4 Summary

The summary of all the explanation and implantation description is about to create a secure environment where we can store the result of our students in a clean and tamperproof database. There is no alternative to impose blockchain cryptography in the storage database to avoid tampering issues.

CHAPTER 5

SUMMARY, CONCLUSION, RECOMMENDATION, AND IMPLICATION FOR FUTURE RESEARCH

5.1 Introduction

In this chapter, we will discuss the summary limitation and future scope of blockchain implementation in real-time data storage environments.

5.2 Summary

There is no doubt that blockchain is one of the most demandable fields to study in computer science technology nowadays. The bitcoin transaction made the way to think about using the underlying technology of bitcoin in various areas of computer science to ensure security, robustness. There is no denying of the fact the coming years we will see more of the blockchain implantation in various fields of computer science.

5.3 Conclusion

In the end, one thing that should be concluded the consensus mechanism of the blockchain must be checked by the proper implementation. As Security is the best to concern at the present time, there is no other way of using or implementing blockchain technology for our data security.

5.4 Limitations

All the advancement that is done so far, we cannot say that every invention is 100% perfect for benefitting us. There are always some limitations that we must have to face. The main problem of the blockchain cryptography is its slow speed in the transaction; it takes time more than normal operation. Another significant limitation is the limitation of transactions in a given time. It cannot perform well in the fields where a deal of data needs to be done

very quickly. But we can surely say this blockchain cryptographical technology outperforms its limitations by giving us the security of our information if we store in a blockchain database.

5.5 Future scope

As the problem arises in securing the data of the user on the internet, it can be predicted that blockchain is going to revolutionize the way we keep track of our data. The cryptography algorithm is developed in such a way that the data we store inside the blockchain is hard to tamper with, and every transaction is recorded with the timestamp. So, it is clearly can be mentioned that data are secure enough if we store data inside blockchain-based database storage. And so, every database on the internet are in need to use the blockchain technology in the backend database storage.

References:

[1]   A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Futur. Gener. Comput. Syst.*, vol. 88, no. 2018, pp. 173–190, 2018.

[2]   D. Galen, N. Brand, L. Boucherie, R. Davis, and N. Do, "Social Impact - Moving Beyond the Hype Blockchain," *Blockchain Glob. Impact*, vol. 1, pp. 1–80, 2018.

[3]   P. Racsko, "Blockchain and Democracy," *Soc. Econ.*, vol. 41, no. 3, pp. 353–369, 2019.

[4]   M. Vukoli *et al.*, "RScoin: Centrally Banked Cryptocurrencies George," *BigchainDB*, vol. 1, no. February, pp. 1–65, 2017.

[5]   H. Baars and H.-G. Kemper, "Integration von Big Data-Komponenten in die Business Intelligence," *Controlling*, vol. 27, no. 4–5, pp. 222–228, 2015.

[6] L. García-Bañuelos, A. Ponomarev, M. Dumas, and I. Weber, "Optimized execution of business processes on the blockchain," *Lect. Notes Comput. Sci. (including Subsea. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10445 LNCS, pp. 130–146, 2017.

[7]   R. L. E. E. Twesige, "A simple explanation of Bitcoin," no. JANUARY, 2015.

[8]   S. Seebacher and R. Schüritz, "Blockchain Technology as an Enabler of Service Systems: A Structured Literature Review BT - Exploring Services Science," *Explor. Serv. Sci.*, vol. 279, no. Chapter 2, pp. 12–23, 2017.

[9]   E. Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "Blockchain-based database to ensure data integrity in cloud computing environments," *CEUR Workshop Proc.*, vol. 1816, pp. 146–155, 2017.

[10]   B. M. Lavanya, "Blockchain Technology Beyond Bitcoin: An Overview," *Int. J. Comput. Sci. Mob. Appl.*, vol. 6, no. 1, pp. 76–80, 2018.

[11]   M. Maccari, A. Polzonetti, and M. Sagratella, "Proceedings of the Future Technologies Conference (FTC) 2018," vol. 881, pp. 305–323, 2019.

[12]   A. Markelevich, "What is Blockchain Technology," *Account. Educ. News*, pp. 1–20, 2018.

[13]   A. Moinet, B. Darties, and J.-L. Baril, "Blockchain based trust & authentication for decentralized sensor networks," pp. 1–6, 2017.

[14]   Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, 2017.

[15]   R. Kamath, "Food Traceability on Blockchain: Walmart's Pork and Mango Pilots with IBM," *J. Br. Blockchain Assoc.*, vol. 1, no. 1, pp. 1–12, 2018.

[16]   A. Dubovitskaya, Z. Xu, S. Ryu, M. I. Schumacher, and F. Wang, "How Blockchain could Empower eHealth: an Application for Radiation Oncology," *VLDB Work. Data Manag. Anal. Med. Healthc.*, vol. 2, pp. 3–6, 2017.

[17]   Institute of Development Studies, "Blockchain for Development," *RapidResponse Brief.*, no. Issue

17, 2017.

[18] J. J. Sikorski, J. Haughton, and M. Kraft, "Blockchain technology in the chemical industry: Machine-to-machine electricity market," *Appl. Energy*, vol. 195, pp. 234–246, 2017.

[19] O. Jacobovitz, "Blockchain for identity management," *Tech. Rep. Ben-Gurion Univ.*, no. December, pp. 1–19, 2016.

[20] A. goleman, daniel; boyatzis, Richard; Mckee, 済無*No Title No Title*, vol. 53, no. 9. 2019.

[21] H. Subramanian, "Decentralized Blockchain-based electronic marketplaces," *Commun. ACM*, vol. 61, no. 1, pp. 78–84, 2018.

[22] M. Scherer, "Performance and Scalability of Blockchain Networks and Smart Contracts," p. 46, 2017.

[23] A. Grech and A. F. Camilleri, *Blockchain in Education - European Commission*. 2017.

[24] D. Mathijsen and K. Sadouskaya, "Adoption of Blockchain Technology in Supply Chain and Logistics 45 pages pages of appendices Commissioned by," *Reinf. Plast.*, no. October, pp. 3–18, 2017.

[25] P. R. Allen, *Joseph J. Bambara, Paul R. Allen, Kedar Iyer, Rene Madsen, Solomon Lederer, Michael Wuehler - Blockchain_ A Practical Guide to Developing Business, Law, and Technology Solutions-McGraw-Hill Education .pdf.* .

[26] A. Deshpande, K. Stewart, L. Lepetit, and S. Gunashekar, "Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards," *Br. Stand. Inst.*, no. May, pp. 1–34, 2017.

Appendix

Project reflection

Completion of this project was really hard a task for me, firstly it is a research-based project and there are not a lot to learn about implementation of this project. The frequent problem that I had to face while developing the project was the problem of framework version while connecting one to others. Had to face a lot of stress because of the lack of resources available in the internet. But it can be surely concluded that learn a lot about the new emerging technology named blockchain because of the effort I put on.

Plagiarism Screenshot: