FINAL YEAR THESIS REPORT

A BLOCKCHAIN-BASED GOVERNMENT FUND MANAGEMENT SYSTEM

Submitted By

SHUAIB
ID: 201-15-14062

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

Supervised By

DEWAN MAMUN RAZA
Lecturer (Senior Scale)
Department of CSE
Daffodil International University

Co-Supervised By

Syada Tasmia Alvi
Lecturer
Department of CSE
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

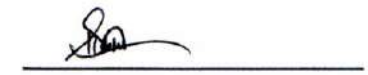
JANUARY 19, 2023

APPROVAL

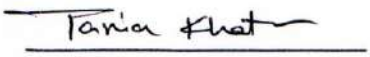
This Thesis titled "**A BLOCKCHAIN-BASED GOVERNMENT FUND MANAGEMENT SYSTEM**", submitted by **SHUAIB** to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on January 19, 2023.

BOARD OF EXAMINERS

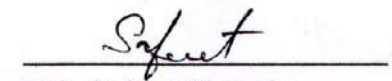
Dr. Touhid Bhuiyan — **Chairman**
Professor and Head
Department of CSE
Faculty of Science & Information Technology
Daffodil International University



Subhenur Latif — **Internal Examiner**
Assistant Professor
Department of CSE
Faculty of Science & Information Technology
Daffodil International University



Tania Khatun — **Internal Examiner**
Assistant Professor
Department of CSE
Faculty of Science & Information Technology
Daffodil International University

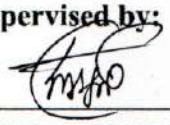


Md. Safaet Hossain — **External Examiner**
Associate Professor & Head
Department of Computer Science and Engineering
City University

DECLARATION

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

Supervised by:



DEWAN MAMUN RAZA
Designation: Lecturer (Senior Scale)
Department of CSE
Daffodil International University

Co-Supervised by:

SYADA TASMIA ALVI
Lecturer
Department of CSE
Daffodil International University

Submitted by:

Shuaib

SHUAIB
ID: 201-15-14062
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

First, I express my heartiest thanks and gratefulness to almighty ALLAH for the divine blessing makes me possible to complete the final year thesis successfully.
I am grateful and wish my profound gratefulness to **DEWAN MAMUN RAZA**, **Lecturer (Senior Scale)**, Department of CSE Daffodil International University, Dhaka.

Deep Knowledge & keen interest of our supervisor in the field of *"*Blockchain*"* to carry out this thesis. His endless patience, scholarly guidance, continual constant, energetic supervision, valuable advice, and reading many drafts and correcting them at all stages have made it possible to complete this thesis.

I would like to express our heartiest gratitude to DR. TOUHID BHUIYAN, Professor, and the Head**,** Department of CSE, for his kind help to finish my thesis and also to other faculty members and the staff of the CSE department of Daffodil International University.

Finally, I must thank my parents and especially my Mother for always being there for me with her support, attention & blessings throughout my entire life so far. I must thank my father for motivating me to work on this platform.

ABSTRACT

Blockchain is a technology that can provide us with features like immutability, transparency, traceability, decentralization, and many more. Blockchain is being used in identity management, cryptocurrency, supply chain management, and many more. In recent years using of blockchain in finance, supply chain, and data-storing sectors has increased significantly. As it provides immutability and openness, it can be used in government fund supply. When government allocates funds for specific purposes and people, in most cases there is no knowledge of the recipient's identity. Some corrupt people take advantage of the handwritten system and put the wrong people's names for their benefit. To solve these issues, a Blockchain-based platform(DAPP) has been proposed in this research. A decentralized identity proof and fund transfer system has been proposed here. People who need the fund can apply through this DAPP with the proper documentation. The authority can verify these documents and provide approval decisions on the DAPP. For example, the election commission office can confirm if the provided NID is original or not, the land office can confirm if that person has any land or not. After collecting approval, a candidate list will be sent to the admin and the admin will allocate a hash for the candidate. After providing this hash to integrated mobile banking, one can collect cash. A prototype of this DAPP is discussed at the end of this thesis. I have used the Ethereum blockchain platform for this prototype. In the future, this can be developed using any kind of public or private blockchain platform.

TABLE OF CONTENTS

Contents PAGE

LIST OF FIGURES

LIST OF FIGURES

Chapter 1
INTRODUCTION

1.1 Introduction

In today's world, everything is getting digitalized. From personal to public and private to government, everyone is adopting digitalization. Even the Bangladesh government has taken several initiatives for Digital Bangladesh. The road to 2041 is one of them[1]. But still, if the government wants to provide some helping fund or any kind of fund, they have to depend on the root-level workers and they use mostly handwritten documents. From selecting the fund receiver to verifying the documents, authorities have to do it physically. Here comes the corruption part. In most cases, the root-level workers along with the politicians allocate government funds to their supporters, friends, and family. Besides, there is a huge problem of corruption in Bangladesh. Bangladesh ranks 147 out of 180 on Corruption Perception Index[2]. Countries like South Sudan and Syria are at the bottom of this list. Research by G. Locatelli, G. Mariani, T. Sainati, and M. Greco shows that 1% corruption reduces the 0.72% growth rate and 2% productivity of a country [3].

1.2 Why Blockchain

So there is a crying need for digitalization in the government funding supply. But even after digitalization, there is a lot of scope for corruption. Like data tempering. The passport application platform is a perfect example of that. Even though it's a web-based platform, some people can take advantage of this technology. For example, some agents can change the appointment date of a candidate for some money. Even some government department uses their own digital documents for their own fund supply. But in these cases, anyone can change the recipient list and user data. Sometimes honest officials can't even stop this corruption.

In these situations, blockchain brings revolutionary changes. Blockchain's immutability nature can solve digital corruption. Blockchain stores data in blocks and these blocks are connected with each other with one-way hash functions. Blockchain is mainly used in

cryptocurrency transactions. But nowadays, blockchain can be used in the supply chain, data storing, Identity management, and many more sectors[4]. Blockchain is popular in every sector because of its transparency, immutability, decentralized nature, non-corruptibility, etc. Corruption can be reduced by using immutability and transparency features[5]. If we integrate blockchain into the fund management system, everyone working with the system can track everything. Using blockchain in the government sector can contribute to the growth and improvement of Bangladesh's economy. To improve our ranking in several humanitarian and corruption indexes, these kinds of technology can directly contribute.

1.3 Research Introduction

In this research, I will be discussing the basics and applications of blockchain in fund management. Besides that, I will be discussing how it can work in our government system and how can people adopt this platform. A platform based on blockchain has been proposed in this research. A prototype of a DAPP has been discussed here. The prototype idea is developed based on a covid-19 fund (a government fund to support the people affected by covid-19) supply system. The concept of this DAPP is to verify documents to choose deserving people for the fund and a secure way to transfer the fund to the right people. The objective of this whole research is to keep these things transparent. But even if there is any kind of misuse of information and data tempering occurs in the system we will be able to find where and by whom these misusages occurred.

1.4 Motivation

After the global hit of the ransomware attack in 2017[6], I came to learn about blockchain technology for the first time. The peer-to-peer electric cash flow system motivates me a lot[7]. From Satoshi Nakamoto's paper on "Bitcoin: A Peer-to-Peer Electronic Cash System", I learned about the decentralized nature of the blockchain. After the hit of the covid-19 pandemic, the Bangladesh government declared several funds to support the people whose earnings are dependent on working in the open market. Lots of misuse of this fund came out in the news.

After that, a need for a decentralized, non-corruptible platform was felt. It could be made with traditional database and backend system. But that's just a matter of time to manipulate Now, this blockchain-based fund management can contribute to reducing corruption.

1.5 Objective

The key expectation of this research is to introduce a non-corruptible digital platform where the Bangladesh government can manage its funds easily. I am mainly concerned about the corruption in Bangladesh. If we have a tamperproof and easily trackable platform, we can easily eliminate corruption. For this tamperproof platform, we need digital verification. Blockchain can provide us with immutability and transparency features. Thus we can achieve our objective through this research.

1.6 Features

My proposed platform has several features. Although the platform is not ready yet, I have done all my research based on these features. I chose some features to start my research with. The rest of the features I have added in the middle of my research because they were necessary for this research and proposed platform.

- Verify documents through the platform. With blockchain hash signature, if a document is verified, it can be used in several places.
- Create digital ids of people to verify who he/she is.
- Record every transaction in an immutable ledger.
- Submit physical verification reports through the platform so that everyone concerned with the fund can see these reports and documents.
- Connect the deserving fund recipient directly to the authority. There is no need for a third party here.
- Transfer the fund directly to the recipient by collaborating with banks and mobile banking services.

1.7 Rationale of Study

In a country like Bangladesh, corruption is very common. The government allocated funds for several projects. But the root-level workers take advantage of the handwritten fund management system. So a new tamperproof system is a must to change these scenarios. In this case, blockchain can provide us the immutability and transparency. This research on

fund management with blockchain will fulfill the requirement of the new system. Now the question is 'Is it viable?' The answer is yes. But it seems irrational now. But the financial sectors are already adopting blockchain technology. It's a matter of time to adopt this technology. My research may help to find a way to make it possible.

1.8 Research Questions

- Can this project solve the corruption problem?
- Is using blockchain a viable option for this project?
- Can we use another technology other than blockchain?
- Will officials adopt this technology?
- Will people adopt this technology?

1.9 Expected Outcome

The expected outcome of this research-based project is to build a DAPP based on blockchain technology for government fund supply management. The other expected outcomes are-

- We will be able to see if such a system can be made with blockchain or not.
- We will find out if this system makes any complications or not.
- We can observe how blockchain transactions work and how we can use these transactions for tracking data tempering.

1.10 Report Layout

The study of this research is ordered into 4 chapters.

Chapter 1 contains an introduction, motivation, and purpose of this research.

In chapter 2 I have discussed the previous study on blockchain and fund management systems. I have presented the literature review in this chapter. Besides, I have mentioned previous work on this specific topic from other researchers.

I have discussed resources and used methodologies and analysis in chapter 3. A demo of the proposed DAPP is shown in this chapter.

Chapter 4 contains experimental outcomes and analysis.

In chapter 5 I discussed the impact of this project on the society and environment. Finally, chapter 6 contains a conclusion summary and future scopes. I have also discussed some issues in this chapter.

Chapter 2
LITERATURE REVIEW

2.1 Introduction

As we are witnessing the advancement of technology, we are also witnessing new ways of forgery. It also appears in technological sectors. We can see different types of data theft, fake document making, illegal hacking, etc. To manage a government fund through a digital platform, it must be checked continuously. Besides illegal hacking or data theft, corruption is a big problem here. So a strong fund management system is a must. To prevent corruption and data theft, we can use blockchain technology. It can reduce both data theft and corruption. This research aims to develop a platform based on the blockchain so that data stays safe and there is always transparency. This research has 2 main topics i. Digital Identity and Document Verification and ii. Maintain the supply of allocated funds.

2.2 Corruption in Fund Management

Corruption in Fund management appears in form of bribery. When government allocates a fund, it goes through several offices and procedures. While traveling the fund from one office to another office, there is a chance that the corrupt officials will get some percentage for themselves. In handwritten documents, it's really hard to track. Major corruption occurs at a local level. The root-level workers make a list of the people who will receive the government fund. In this process, the dishonest list makes puts their close one's name on the list whether they need the fund or not. Sometimes they select the people who are willing to pay them an amount after receiving the fund. Even sometimes higher officials take some percentage for granting the fund.

2.3 Blockchain Technology

Blockchain is a decentralized, distributed ledger technology that is used to securely store and record data across a network of computers. It stores data in blocks and the blocks stay connected with each other with a hash function. It is used to create a secure, permanent

record of digital transactions and data records that are resistant to tampering and revision. Blockchain technology is especially useful when it comes to storing financial information and digital assets such as cryptocurrency.

The technology was first implemented by Bitcoin and other cryptocurrencies to secure data and verify transactions[7]. In the coming chapters, I will be discussing the different features and characteristics of blockchain technology.

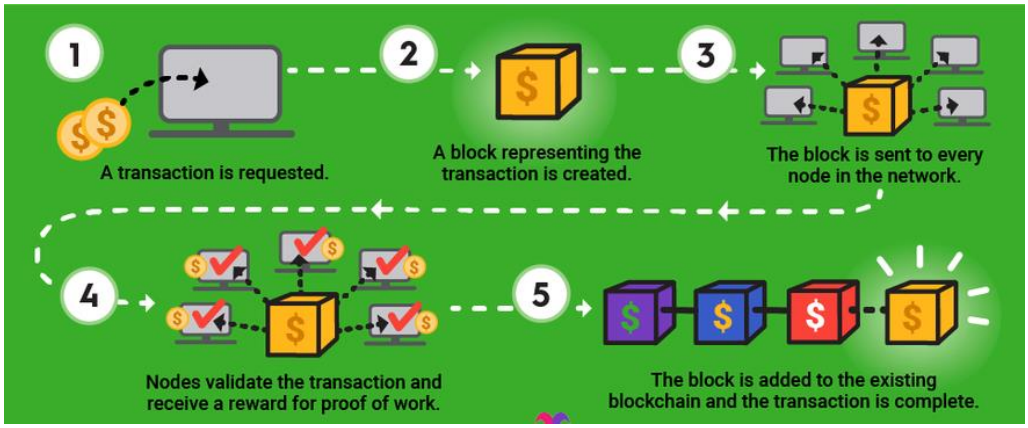


Figure 2.3.1: How a blockchain system works

2.3.1 Private and Public Blockchain

There are two types of blockchains. Private and Public. The first-ever blockchain is a public blockchain.

A private blockchain is a blockchain platform where the participants are known and trusted. It is a distributed ledger technology (DLT) that allows for permission access to the data for a select group of users. Private blockchains have a single organization controlling access to the network and determining who can participate in the network, create new blocks, and validate transactions. Private blockchains are typically used within organizations to ensure secure data sharing and processing among members of a specific group. Hyperledger is the most common private blockchain.

A public blockchain is a decentralized, distributed ledger technology that anyone can read, write, or audit. It is an immutable, transparent, and secure ledger of transactions and data that is accessible to everyone in the network. Unlike a private blockchain, anyone can join the public blockchain network and no permission is required to participate. Transactions are recorded on the public ledger and are secured by cryptographic algorithms, which

makes them difficult to modify or tamper with. This makes public blockchains extremely secure and resilient against malicious attacks and tampering. Bitcoin and Ethereum is the most common public blockchain.

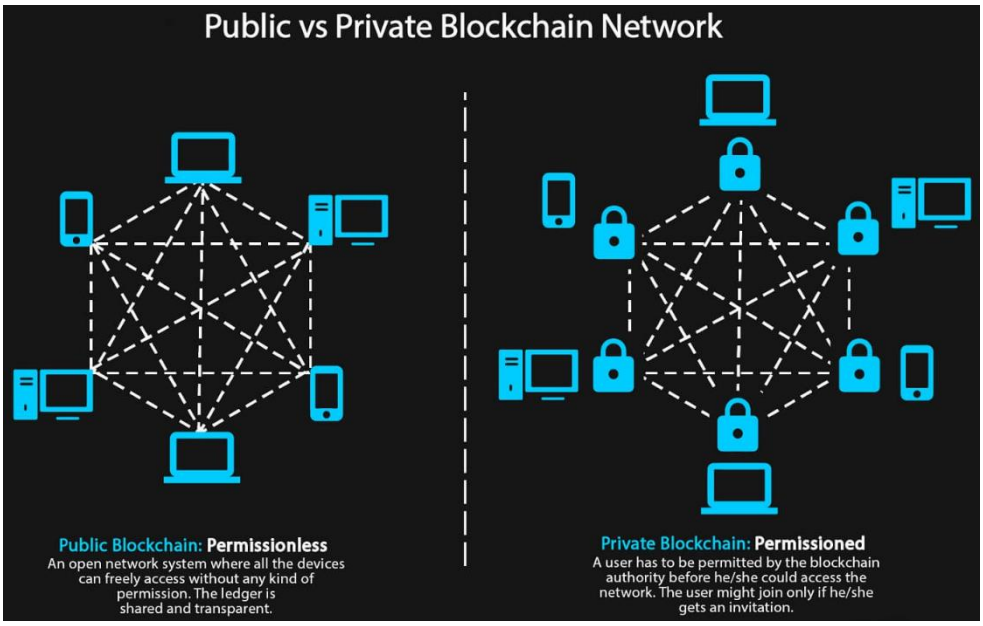


Figure 2.3.1.1: Private and Public Blockchain

Although public blockchain looks more secure, sometimes organizations like banks and financial institutes may need to keep things between them. This is where private blockchain is very useful. Besides private blockchain is much faster than public blockchain.

There is another type of blockchain called consortium blockchain. In this case, several private blockchain banded together to ensure a more security, transparency and accountability.

2.3.2 Hashing Algorithm

A typical blockchain has several parts. Like block number, data, previous block hash, and current block hash. Like I said before blocks stay connected with each other with a hash function. Now when a block is created it needs the hash of the last block. Everyone in the blockchain knows the last block's hash whether they have the block or not. In these cases, the SHA256 hashing algorithm is used. This hash algorithm uses a cryptographic algorithm to generate hashes. A hash is generated through data or string and it is impossible to get the original data from a hash. The only way to temper data is by guessing the hash which

is basically impossible. Even it is computationally impossible to collide between hashes. It would require so much computational power[19].

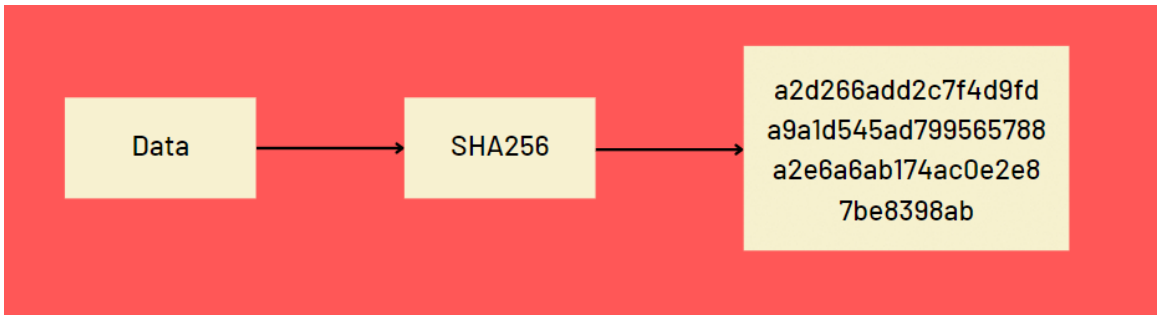


Figure 2.3.2.1: SHA256 hashing algorithm

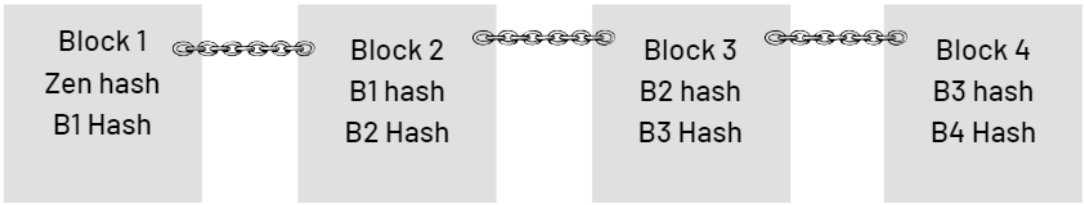


Figure 2.3.2.2: Hashes in blockchain blocks

2.3.3 Peer-to-Peer Network

A blockchain P2P network is a distributed network of computers that use a distributed ledger technology called blockchain to maintain a shared ledger of transactions in a secure, distributed, and immutable manner. The blockchain P2P network allows users to securely transfer value without the need for a third-party intermediary, such as a bank. The peer-to-peer network was first introduced in Bitcoin[7].

2.3.3.1 Distributed P2P Network

A distributed peer-to-peer (P2P) network in a blockchain is a network of computers that are connected to each other in a decentralized manner. The computers in the network are called nodes and each node can communicate with any other node in the network. The main purpose of a distributed P2P network in a blockchain is to enable the secure and trustless

transfer of data and value between two or more parties. This type of network is used in various blockchain technologies, such as Bitcoin and Ethereum.

2.3.4 Immutable Ledger

In chapter 2.4.2 I discussed how blocks stay in the blockchain with the help of hashing algorithm. A block depends on the previous block. If someone tries to manipulate data in one block, then the hash of the block will be changed. If the hash of a block changes, the blocks after them will not be able to find the block. As a result, the whole chain will fall off.

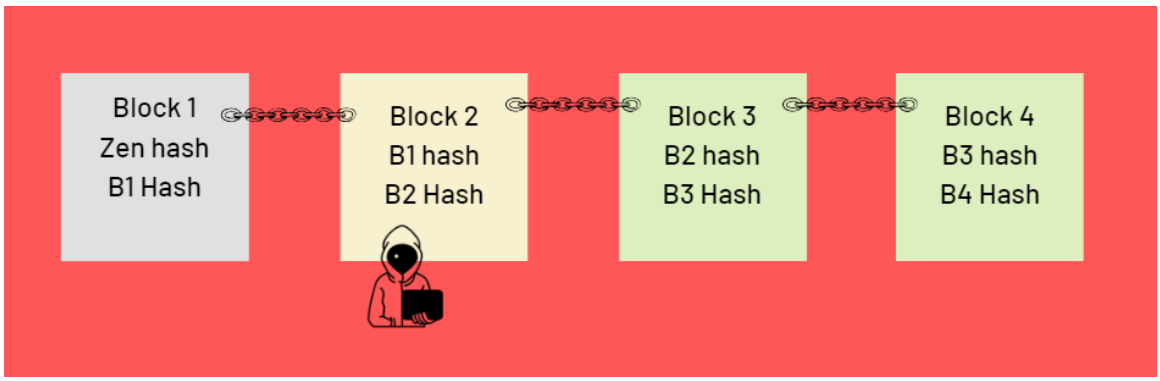


Figure 2.3.4.1: Example of attack in block

In figure 2.3.4.1 we can see, someone is trying to tamper with block2. If he tampers the data of block2, the hash of block2 will be changed. Then block 3 will not be able to find the hash with which he has been connected from the first. From this incident, the authority will be able to find the problem and take action. This is why blockchain is an Immutable Ledger.

2.3.5 Consensus Protocol

A consensus protocol is a mechanism that a distributed system uses to reach an agreement among its participants. In blockchain technology, the consensus protocol is used to validate the authenticity of the data stored on the blockchain. It is the mechanism by which all nodes (computers) in the network come to an agreement on the current state of the blockchain. Now in this case even if someone tries to add a fake block or attack the last block the Consensus Protocol will prevent them from doing it.

The most popular consensus protocol used in blockchain networks is the proof-of-work (PoW) protocol. Under this protocol, miners compete to solve complex mathematical puzzles in order to add new blocks of data to the blockchain. The miner who solves the puzzle first is rewarded with a small amount of cryptocurrency.

Other consensus protocols used in blockchain networks include proof-of-stake (PoS), delegated proof-of-stake (DPoS), and proof-of-authority (PoA).

But in a private blockchain, there is no manner. Here fault-tolerant distributed consensus is used. In this protocol, all the nodes reveal their identity and agreed upon the state of the blockchain[20]. Byzantine Fault Tolerant Consensus is a very popular protocol for private blockchain validation.

2.3.5.1 Longest Chain Rule

The longest chain rule is a consensus mechanism used by blockchain networks to determine which blockchain is the valid one. Under this rule, the blockchain with the most blocks (the "longest" chain) is considered to be the valid one and all other blocks are discarded. This rule is based on the assumption that the longest chain is the one that the majority of nodes in the network have worked on and is thus the most secure.

2.3.6 Transparency

Blockchain technology is known to be a transparent system. This is because it is a distributed ledger technology, which means that the data stored on the blockchain is public and can be seen by anyone who has access to the network[21]. Every transaction that is recorded on a blockchain is visible to all participants on the network, creating a level of transparency and accountability that is not available with traditional systems.

2.3.6 Blockchain Traceability

We already know that blockchain is immutable. If a block enters into a chain, it is impossible to change. Does that mean we can’t even edit our data? Well, actually we can. But when an authorized node changes something, a new block is added and with the help of consensus protocol, the nodes agreed that the last block has the latest information. Now the problem is, anyone can tamper with data. Not really. Only authorized users can change

data by adding new blocks. Even if a block enters the chain, the previous block stays. So if any such issue occurs, we can check the previous block data. Every transaction in the blockchain stores the information that was edited during the operation. The transactions also store timestamps, nonce, sender and receiver addresses, and many more.

2.4 Blockchain for fund management

Different organizations like banks and venture capitalists are going on a new way of blockchain application. One such architecture is shown below. In this architecture, the bank will help us to manage the cash flow. Here I am suggesting mobile banking. User and official will be connected through a smart contract. Officials will validate documents through the smart contract. Banks will contact the management through another smart contract. The whole system will run on a blockchain network.

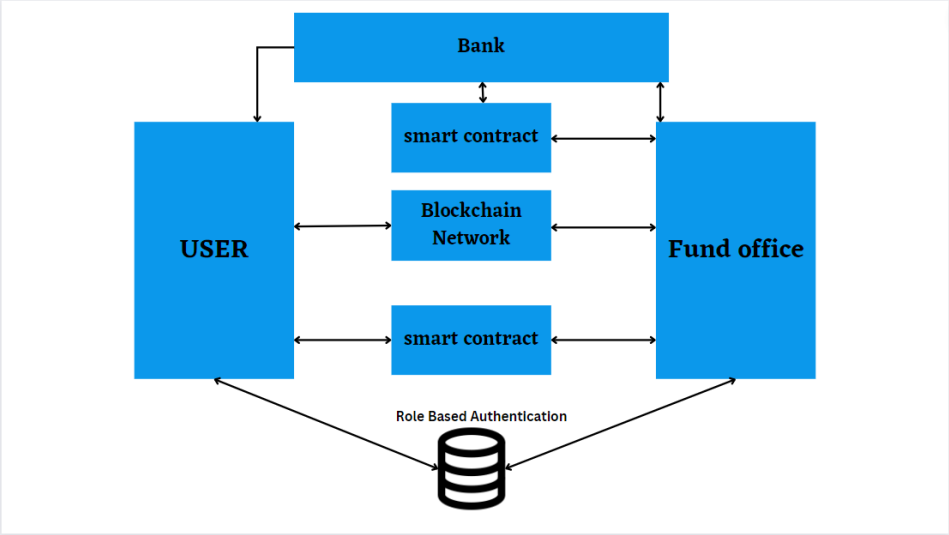


Figure 2.4.1: A blockchain architecture for fund management

A. Digital Identity

To transfer the fund to the right people and perform verification through the blockchain, we need a digital identity system. From the user database, we can validate the user's status and documents. Based on these validations we can make a list of people who is eligible to receive the fund. Then we can send the list to the bank.

B. Fund Transfer

For fund transferring we can use mobile banking as Bangladeshi authorities already using it to transfer the funds. For this, we can generate a unique token for the recipients. They can submit the token in mobile banking and withdraw money.

2.5 Related Works

As I mentioned earlier, this research project is divided into two parts. The first one is digital identity and document verification for selecting the deserving person for the fund. The second one is to supply funds to the right people.

Yang Liu et al provides brief details of the digital identity system and its patents in their research. In this paper, the authors suggested 3 types of participants, i. User, ii. ID provider and iii. Service providers[8]. The authors also discussed 3 main Blockchain-based Digital Identity Management Systems. i. Sovrin ii. uPort iii. ShoCard[8].

Estonia is currently the pioneer Digital Identity System at the national level. Nathan Heller described the digital identity system of Estonia in The New Yorkers[12].

In my research project, I have used a similar identity system. Here a user will register with a unique hash. Then they can add different types of identity documents. Unlike the systems mentioned above, users can add the documents which are necessary for fund receiving and get verified by the concerned authority. I am proposing a NoSQL-based authentication system.

Omar s. Saleh et al discussed the blockchain-based certificate verification system. The authors proposed an off-chain database for storage. A central database is necessary for storing confidential documents [13]. But we can store user documents in the distributed file system (IPFS) and verify the document with a digital signature[14]. Later users can use these verified documents in another place by providing a digital signature.

There are very few studies on fund management using blockchain. Ajay Acharya and Apporva Mohite mentioned such a system on the hyperledger platform[15]. But they didn't mention anything about identity verification.

Dr. S. S. Prasada Rao et al proposed a DAPP where investors and RTA will be able to exchange mutual funds[16].

Hadi Saleh et al have mentioned a platform for tracking donations of charitable foundations based on blockchain technology[17]. Managing donations and government funds are two different things. Government fund management has much more parameters.

Nibula Bente Rashid et al have proposed a very good platform for government fund management. But they have used cryptocurrency[18]. First of all, crypto is not legal in Bangladesh, and in general, people can't handle crypto.

2.6 Research Summary

Our main purpose of this research is to build a non-corruptible and secure platform for government fund management. Blockchain provides decentralization and transparency features which will help us implement the platform. Private and public blockchains can provide different features for these types of systems. But which one is better, it can be said after testing the system in both environments. There may be some issue that occurs during and after developing the platform. But these issues should be easily manageable. Blockchain technology is going to revolutionize the technology world. So today or tomorrow we need to adopt this amazing technology.

2.7 Scope of the Problem

Government funds are meant for some specific group of people. Most of these funds go through handwritten documents. These documents are easily corruptible. Even if we digitalized the system, there is still a chance for data tampering. Here blockchain can provide us with a system with transparency and immutability.

2.8 Challenges

Blockchain technology is very new. Very few implementations of blockchain are seen yet. In a blockchain network, every node (computer/smartphone) need to participate in the system. The real challenge will be bringing different offices into a single platform. Besides, it is very hard to explain new technology to the users.

One other problem is, we need lots of computers to host the blockchain data. If the users refuse to participate in that, we have to go for expensive data storage.

Chapter 3
RESEARCH METHODOLOGY

3.1 Introduction

In this chapter, we will be discussing implementing our project. Blockchain can be implemented using several methods. In this research, I have experimented with a public blockchain. So I will be discussing tools and components of public blockchain technology. I have discussed the requirements in the last section of this chapter. In the next chapter, I have discussed the results of my prototype.

3.2 Proposed Solution

I already have discussed the problems of government fund management. I have also discussed how blockchain can eliminate these issues. In this project, I am proposing a transection-based network. The purpose of this transection-based solution is to store all the transaction history and use them when needed. In this way, it will be so easy to investigate any queries if needed later. I will be using the Ethereum blockchain network for this project. I will write the smart contract in solidity programming language and deploy it Ethereum blockchain. But as Ethereum is a very sensitive and expensive network, I will be using ganache as a testing network.

3.3 Applied Mechanism

I have used the Ethereum blockchain for the fulfillment of this research. Ethereum is a public blockchain. I have tested the system on the ganache test network. There are several other blockchains to work with. The reason I choose it because of its main net and testnet availability. Some of the Most popular blockchain networks and their properties are given below-

Table 1: Most used blockchain networks and their types.

Network Name	Network Type	Cryptocurrency	Consensus Mechanism
Ethereum	Public	Ether, dogecoin (uses ethereum platform)	PoS Consensus
IBM Blockchain	Private	N/A	Selective Endorsement
Hyperledger Fabric	Private	N/A	Endorsement, Ordering, and Validation
Hyperledger Sawtooth	Public	N/A	Practical Byzantine Fault Tolerance (PBFT) and Proof of Elapsed Time (PoET)
Bitcoin Network	Public	Bitcoin	Proof of Work (PoW)
R3 Corda	Private	N/A	Transaction validity

The further discussion is based on the requirement of Ethereum blockchain network.

3.3.1 Ethereum Blockchain Network

The Ethereum blockchain is a distributed ledger technology (DLT) based on the Ethereum protocol. It enables the development of decentralized applications (dApps) and smart contracts on the Ethereum network. The Ethereum blockchain is an open, permissionless ledger that records all transactions that take place on the platform. It is secured by a network of computers (nodes) that validate the transactions and create an immutable record of them on the blockchain. Ethereum is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud, or third-party interference. These apps run on a custom-built blockchain, an enormously powerful shared global infrastructure that can move value around and represent the ownership of property. In the coming chapter, I will be discussing the Ethereum blockchain for government fund management.

3.4 Proposed Model in Blockchain

In the previous chapter, I proposed a blockchain-based platform for Government fund supply management which is a distributed ledger, transparent and non-corruptible. The proposed platform will be able to verify documents and identity and transfer funds. This asymmetric cryptography and consensus technique have achieved user security as well as record consistency. My goal is to introduce a distributed model that is flexible, accessible from anywhere, and most secure. The primary characteristics are better security, quick settlement, and anonymity.

I have made an exertion to reduce corruption and reduce unauthorized data tampering. The system dispenses with the requirement for any central specialist within the confirmation and organization of character data, which diminishes the time went through on assignments requiring user identity confirmation. Blockchain innovation is respected as one of the viable ways to store and convey confidential information, where miners ceaselessly confirmed the advanced record. The project's workflow is given below-

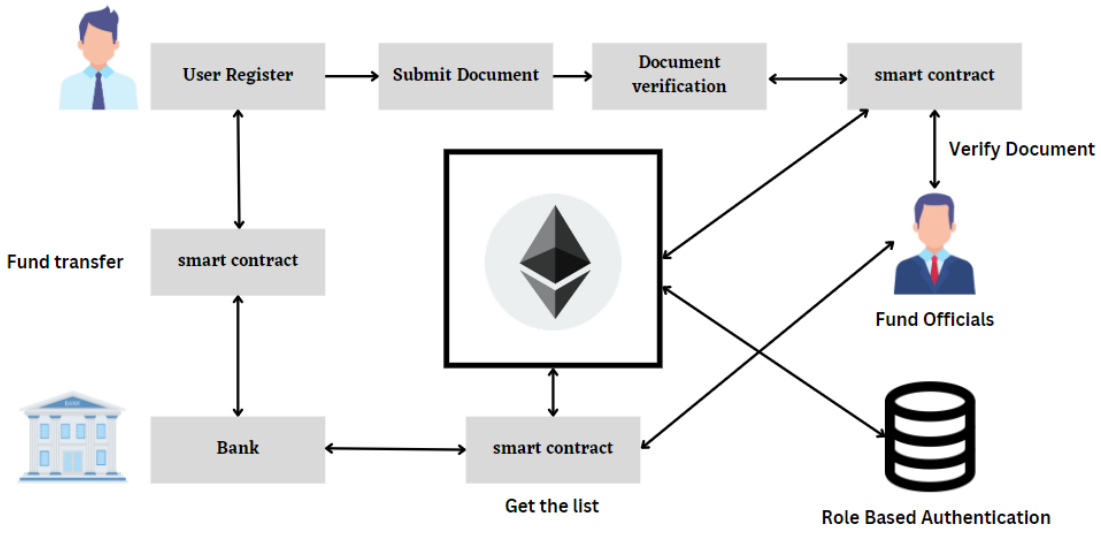


Figure 3.4.1: Blockchain model for proposed platform

Figure 3.4.1 shows the steps of the proposed blockchain model. Users can register themself on the platform with specific parameters. They can submit the necessary documents for fund application. These user data will be stored in IPFS. Miners will add a block with a digital signature of the document. In this case, miners will solve some complex

mathematical problems which are also known as consensus protocol[7]. The officials will be able to view the documents and investigate them. For viewing, no mining is required. The officials can validate the documents sent by fund seekers. For validating, mining is required. After validating the documents, the officials will send a list of data to the banks. Then the bank will transfer the fund to the fund seeker.

A smart contract written in solidity will be responsible for all these works. A smart contract in Ethereum is a programmable contract that is written in Ethereum's native programming language, Solidity[23]. The code of the smart contract is stored on the Ethereum blockchain, and when it is initiated, it will execute according to the rules of the contract. I am proposing a NoSQL database for role-based authentication and access to them through a smart contract. In this way, the blockchain network will be much faster. A simple smart contract can have a mapping for storing identities for specific users.

Ethereum and smart contracts will perform all these operations through a transaction. Transactions on the Ethereum network are sent using Ether, the network's own cryptocurrency. To send a transaction on the Ethereum network, a user must have Ether in their account. Transactions are broadcast to the network and are added to the blockchain. Ethereum transactions are processed by miners, who use their computing power to solve cryptographic puzzles. When a miner solves a puzzle, they are rewarded with a small amount of Ether. Ethereum transactions are secure and immutable and can be used to transfer value, store data, and execute smart contracts[22].

Now to access these data and methods on a webpage we need web3 technology. Web3.js is a collection of libraries that allow you to interact with a local or remote Ethereum node, using an HTTP or IPC connection. It is the official Ethereum Javascript API that implements the Generic JSON RPC spec. It allows you to send transactions, accesses smart contract data, and much more. Web3.js can be used to create powerful decentralized applications (DApps) on the Ethereum network[24].

3.5 Implementation of the Model

This section will present an algorithm and flowchart that will function as the suggested model predicts.

Algorithm for Smart Contract

Step 1: start

Step 2: call setter_data(hashid, name, nid, mobile, home_address, document)

Step 3: set approval[hid] = true/false. //False by default

Step 4: if approval[hid] = true

Send hid to the approved list

Step 5: call get_approval_list(hid) and check validation

Step 6: if get_approval_list(hid) = true

Send fund

Step 7: Finish

This algorithm is just an overview of how the platform will work. Lots of things like user data editing and document crossmatching parts were ignored here.

Flowcharts-

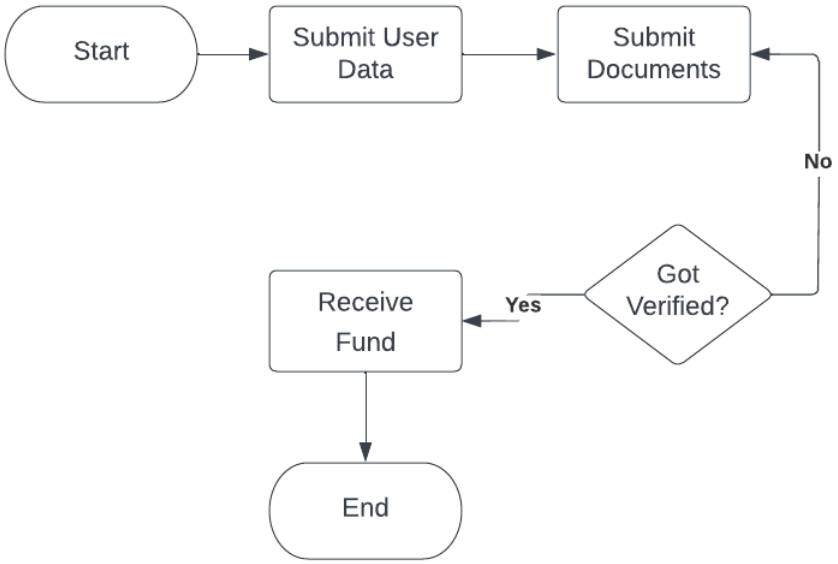


Figure 3.5.1: User flowchart

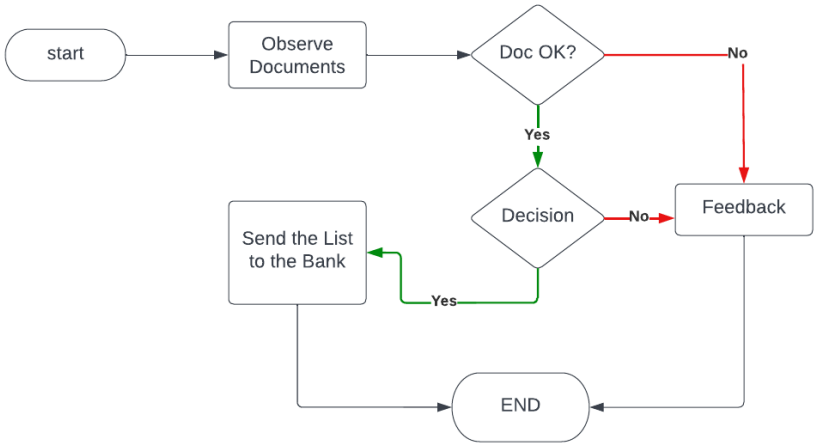


Figure 3.5.2: Document Verification flowchart

Smart Contract

```
pragma solidity >=0.7.0 <0.9.0;

contract Storage {

    mapping(int => string) private name;
    mapping(int => string) private nid;
    mapping(int => string) private mobile;
    mapping(int => string) private homeadd;
    mapping(int => string) private document;
    mapping(int => bool) private approval;
    mapping(int => int) private wallet;
    mapping(int => bool) private approved_list;

    function gettername(int hid) public view returns(string memory){
        return name[hid];
    }

    function getternid(int hid) public view returns(string memory){
        return nid[hid];
    }

    function gettermobile(int hid) public view returns(string memory){
        return mobile[hid];
    }

    function getterha(int hid) public view returns(string memory){
        return homeadd[hid];
    }
    function getterdoc(int hid) public view returns(string memory){
```

```
        return document[hid];
    }
    function getterapp(int hid) public view returns(bool){
        return approval[hid];
    }
    function getterwallet(int hid) public view returns(int){
        return wallet[hid];
    }
    function setter_data(int hid, string memory nm, string memory _nid,
string memory _hmoead, string memory _mobile, string memory doc) public
    {
        int wal = 0;
        name[hid] = nm;
        nid[hid] = _nid;
        homeadd[hid] = _hmoead;
        mobile[hid] = _mobile;
        document[hid] = doc;
        wallet[hid] = wal;
        approval[hid] = false;
        approved_list[hid] = false;
    }
    function approval_setter(int hid, bool app) public
    {
        approval[hid] = app;
        if(app){
            approved_list[hid] = true;
        }
        else{
            approved_list[hid] = false;
        }
    }
    function send_money(int hid, int am) public
    {
        if(approved_list[hid]){
            wallet[hid] = wallet[hid] + am;
        }
    }
}
```

Ganache Test Network

Implementing blockchain directly into the Ethereum main net is quite risky. That's why we use a testing network. In this case, I am using the ganache test network. For the ganache, we have to select Ganache Provider from remix ide.

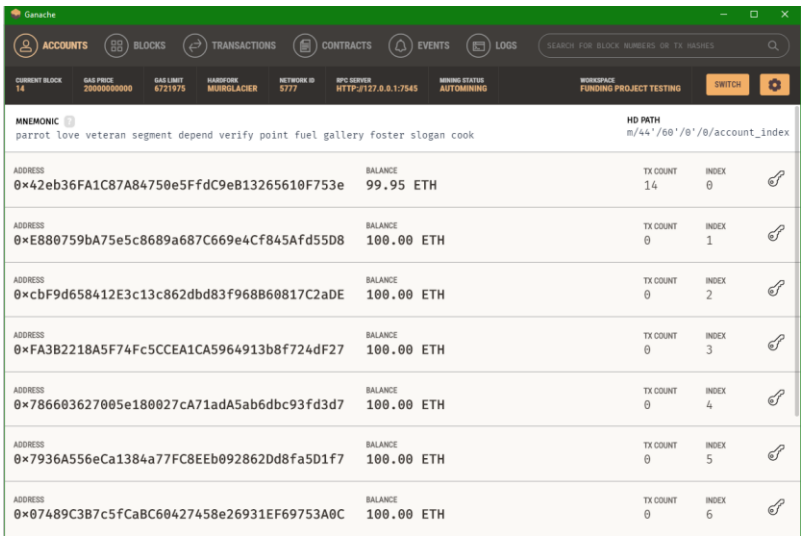


Figure 3.5.3: Ganache desktop view

Metamask connection

Metamask is a browser extension for the Ethereum network. It allows users to connect to Ethereum-enabled websites, Dapps, and other platforms. Web3 is an application programming interface (API) for interacting with the Ethereum blockchain. With Metamask, users can use web3 to send Ether and interact with Ethereum smart contracts.

```
const connectMetamask = async () => {
    if(window.ethereum !== "undefined") {
        const accounts = await ethereum.request({method:
"eth_requestAccounts"});
     account = accounts[0];
     document.getElementById("accountArea").innerHTML = account;
}
```

Connecting Smart Contract

```
const ABI = [];
const Address = "0x2c1f488483317B2221a71543E28b47222E5c4B79";
window.web3 = await new Web3(window.ethereum);
cont = window.contract = await new window.web3.eth.Contract( ABI, Address);
document.getElementById("balance").innerHTML = "connected to smart contract";
```

3.6 Implementation Requirements

To implement this project all we need is a web development environment. We can build api of the application and show it on mobile, computer, or any other frontends. There is a

dedicated library for web3 for these works. I am proposing an app with react as frontend and smart contact as backend. A summary of requirements is given below_

1. Smart contract in solidity.
2. React library of javascript.
3. Moralis for user authentication.
4. Help of NID and other documents api.
5. Database like bigchaindb for further scaling of the application.
6. Metamask.
7. Pinata for media storage (IPFS).
8. Infura for the deployment of the smart contract.

Chapter 4

RESULT AND DISCUSSION

4.1 Introduction

During the implementation, I tried to develop a fund management system based on blockchain technology and the architecture mentioned in chapter 3.4. For that, I have built my DApp on the Ethereum blockchain network. The Ethereum blockchain is a public blockchain network, which can provide us with a transaction-based system. From the transaction, we can detect any kind of data tampering and corruption. Ethereum uses smart contracts for operations.

4.2 Experimental Setup

I have used a javascript web framework for the front end and smart contract as the backend. A details description is given below-

1. I have written the smart contract in solidity language.
2. Simple HTML, CSS, and javascript have been used here to interact with the smart contract and present data on a web page.
3. IPFS has been used for media purpose.
4. Ganache has been used for testing the ethereum blockchain testing.

4.3 Experimental Results

From the beginning of this research, I have to mention a decentralized and non-corruptible fund management platform. In this platform users can apply for funds and officials can validate documents and provide recipient lists. The users and officials will connect to the platform with metamask. After entering the record in a transaction no one can change it.

Figure 4.2.1: Smart Contract deployment transaction

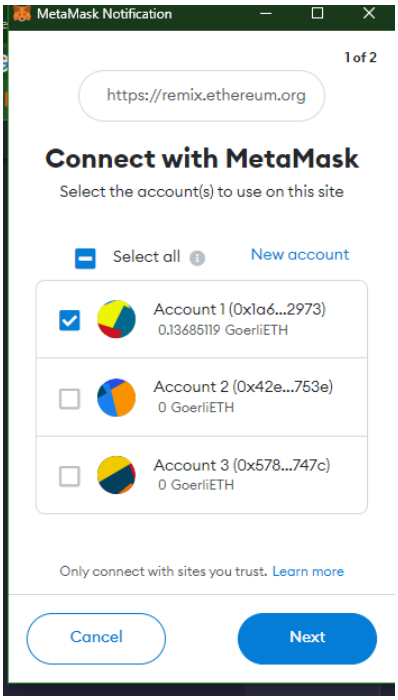


Figure 4.2.2: Metamask connection

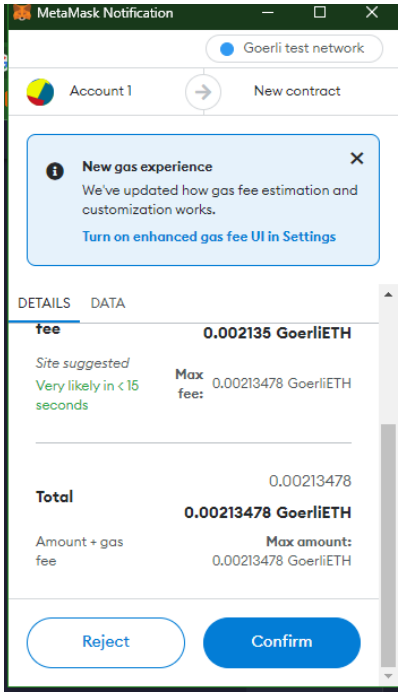


Figure 4.2.3: Mining fees through metamask

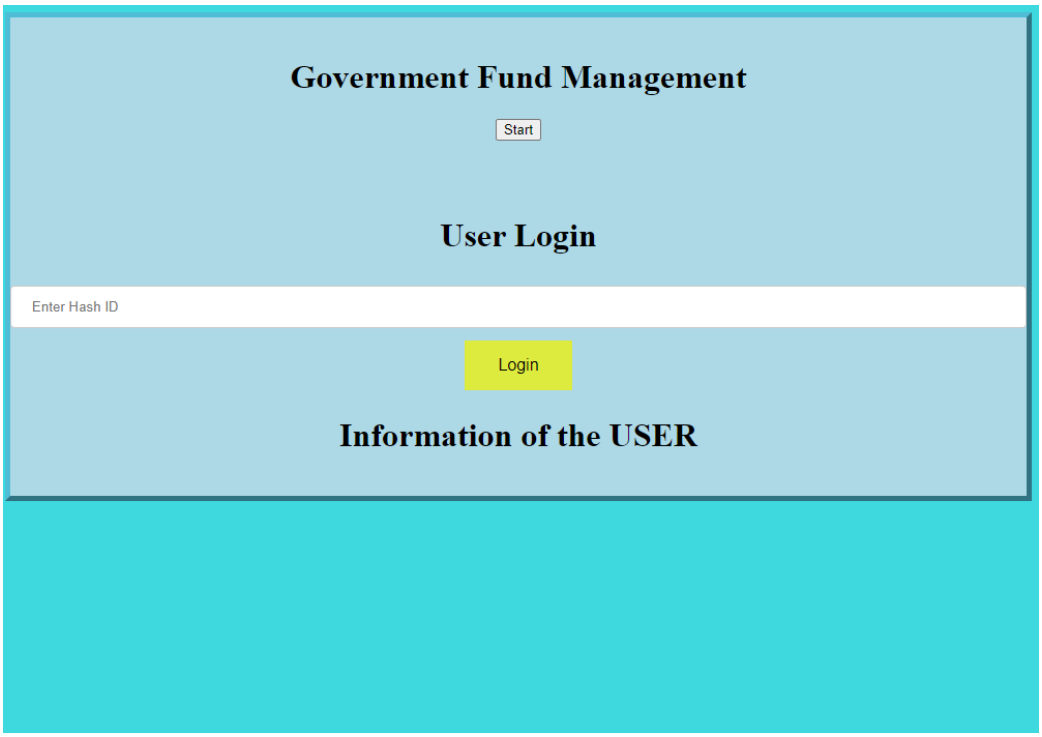


Figure 4.2.4: Initial Web layout

In figure 4.2.4 we can see the login option. Basically, these logins will be done with metamask. Now we can see user info with this login option.

Figure 4.2.5: User info searching with hashID

Figure 4.2.6: Transaction for adding new user

Figure 4.2.6 show the transection in remix ide after adding a new user. Figure 4.2.7 show the deployment transection of our smart contract in etherscan. I have deployed this from remix ide but I still can see this in etherscan and these transactions are immutable.

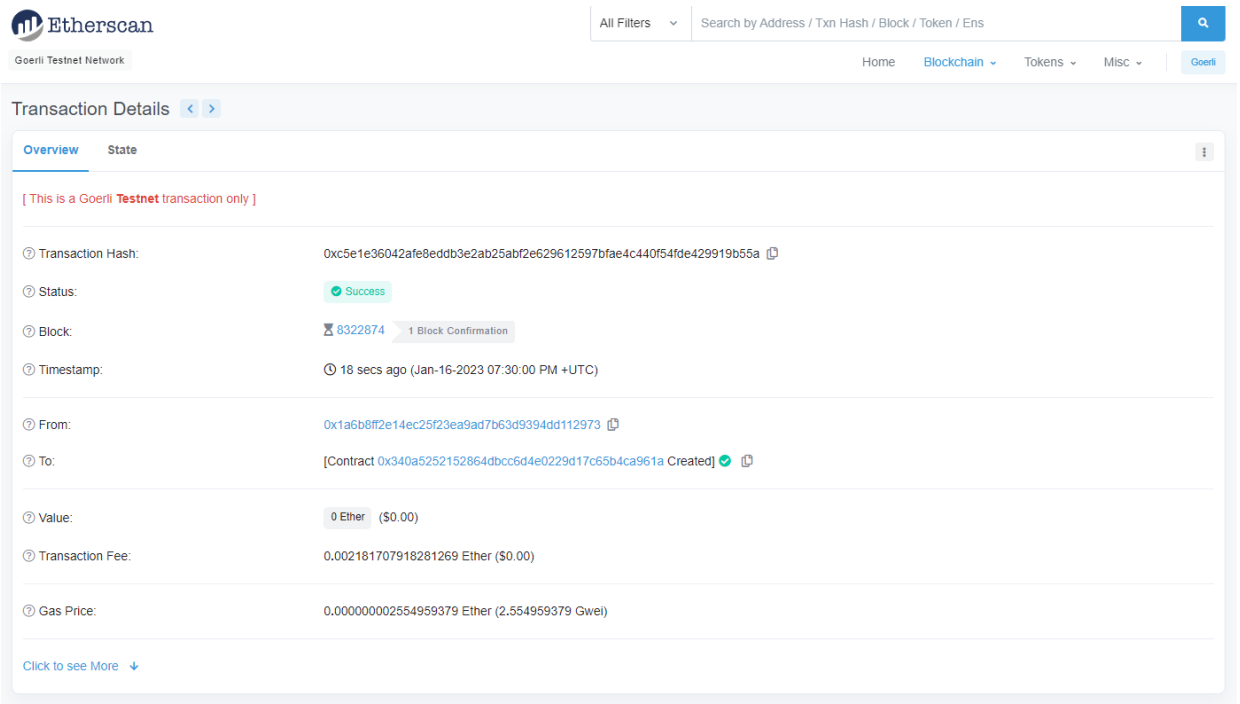


Figure 4.2.7: Our Deployment transection in Etherscan

In figure 4.2.8 we can see how media files are being stored in IPFS through piñata.

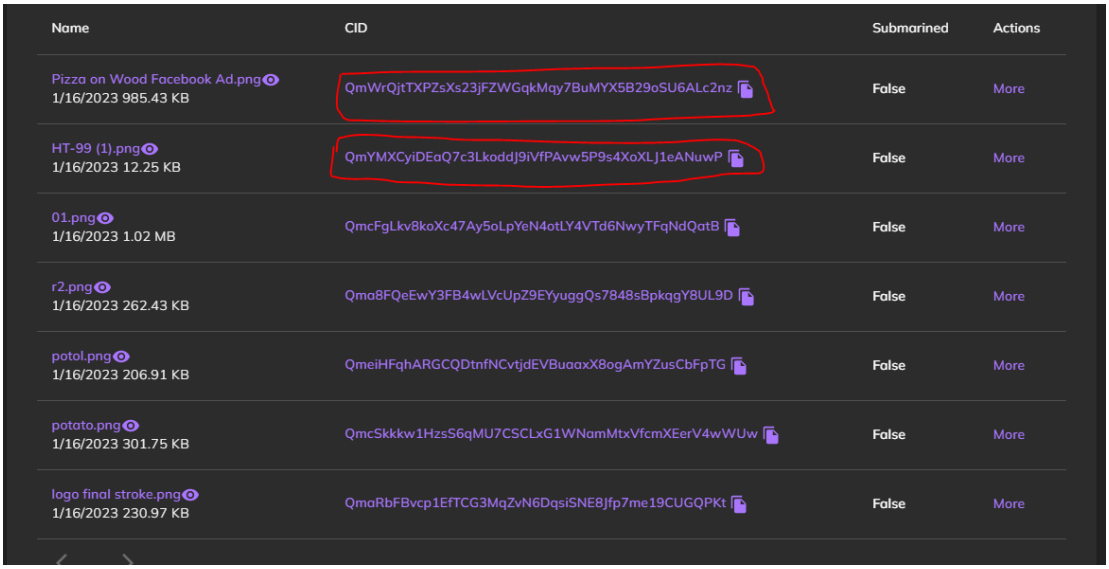


Figure 4.2.8: Image storing in IPFS through piñata.

The red marked areas are the CIDs of the uploaded media. The images here are uploaded from react frontend. In figure 4.2.9, we can see how piñata api looks like and in figure 4.2.10, we can see pinata's own cid verifier. We can use the same verifier for our document verification.

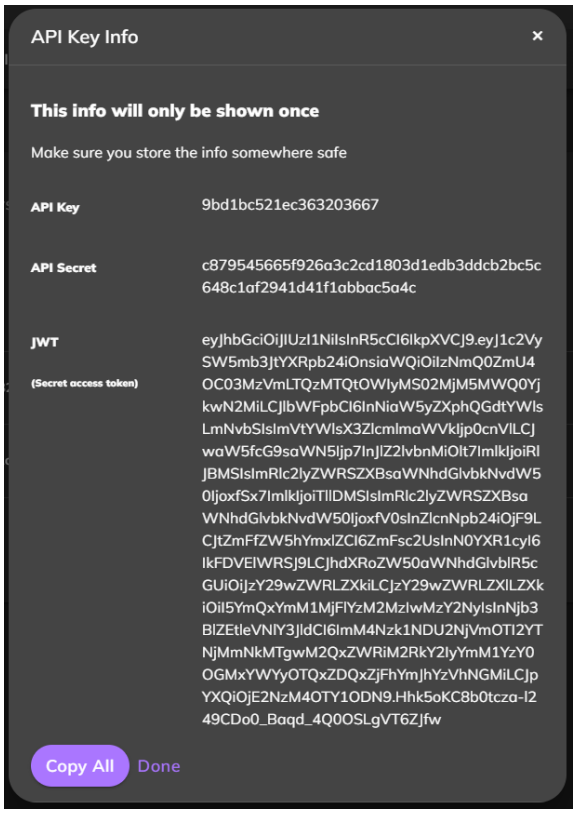


Figure 4.2.9: Pinata API key

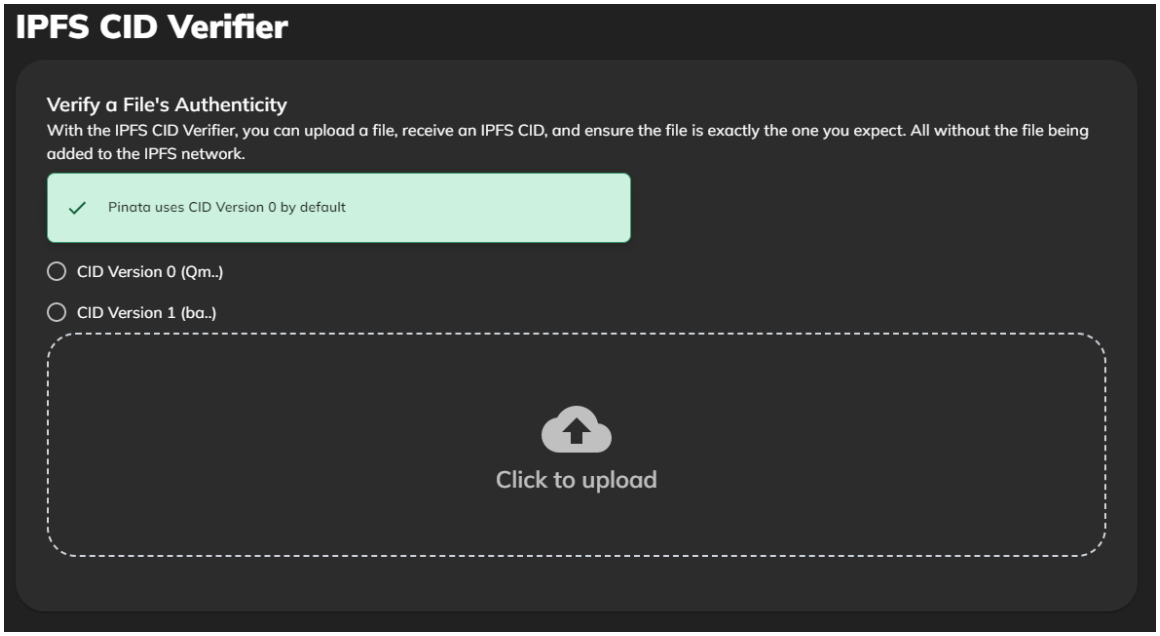


Figure 4.2.10: Pinata CID verification system

4.4 Descriptive analysis

My aim is to create a transparent platform for fund management. With the current update of my project, we can see how the Ethereum blockchain is storing data in a transaction. From these transactions, we can see what types of changes were made. These transactions are also available in the test network. If we deploy this system in Ethereum main net, we can see these transactions on the etherscan website.

Chapter 5

IMPACT ON SOCIETY, ENVIRONMENT, AND SUSTAINABILITY

5.1 Social Impact

Corruption in anything, even in the tiniest places can play a direct role in our society. For example, let's take corruption in fund management. In most cases, the corrupt officials along with the local politicians usually allocate the fund to the people close to them or the people who will provide them with a commission. Thus the real needy people suffer and these things directly affect the local as well as the country's economy. Rich and powerful people are being richer and more powerful and poor people are being poorer.

My research and proposed platform can directly help to change this scenario. If deserving people get the financial help that was allocated to them, their socioeconomic scenery will change completely. If the root-level people can improve their economic status it will directly affect the country's economy. The officials and politicians will think twice before they harass any person and commit any corruption. And if there is no option for corruption the officials and politicians will be forced to work for the people. On the other hand, we can use this concept for project fund management and NGO fund (foreign funding) management.

5.2 Impact on the environment

Blockchain can play both a good and bad role in the environment. Blockchain networks like bitcoin can transfer electronic cash from peer to peer. But these transactions required electricity consumption[25]. Nevertheless, de Vries asserted that, upon examination of the sales of Bitcoin miners, it can be determined that the Bitcoin network was consuming 87.1 TWh per annum on September 30, 2019, surpassing estimates acquired from the two indexes, and coming close to the energy expenditure of a country such as Belgium[24].

In our project, we are not using cryptocurrency. Yet it will consume significant energy through the Ethereum blockchain network. But on the other hand, it will replace hand-written documents. Thus we can even reduce our carbon footprint. Less paper use means

less cutting of trees. Besides, if we digitalize the process without blockchain, it will also consume electricity.

5.3 Ethical Aspect

The ethical aspect is very important for this platform. Blockchain provides us with the anonymity feature. This anonymity can be used for money laundering, financial crime, and even tax fraud. But compared to the facility that blockchain is providing, we need to think about countering these types of issues rather than abandoning the technology. Besides government or fund officials can regulate the platform for any kind of unethical activities.

5.4 Sustainability Plan

Blockchain itself can be a sustainability plan for data centers. With the help of peer-to-peer data storing and accessing we can reduce the use of data centers. Thus there is a possibility of energy and plastic use reduction.

Besides, we can focus more on solar, wind, and other sustainable energy sources. A private blockchain network can be a good solution. For example, we can build a blockchain network with users who use only sustainable energy.

However, bitcoin and other cryptocurrency miners are using sustainable energy sources especially solar energy for mining.

Chapter 6

CONCLUSION AND RECOMMENDATION

6.1 Findings

There's a gigantic opportunity for upgrading blockchain advancement to handle data exchanges all the more quickly. Blockchain innovation upgrades across the nation interrelation and diminishes the centralized approach which could be a major key component within globalization. For the financial sector, it’s not just an opportunity. It’s necessary.

I have proposed a new method for government fund distribution during this research. I have proposed a decentralized app using Ethereum blockchain technology. My suggested DAPP was tested with the ganache testing network. We don't need to worry about mining as we have developed our Dapp in the Ethereum blockchain. The nodes connected with Ethereum will mine our blocks. Besides, Ethereum will use proof of work consensus.

6.2 Conclusion

I have tested the model with a public blockchain. To make a conclusion about which blockchain is suitable for these types of systems, we still need to test it in a private blockchain network.

6.3 Future-Related Work

As we are going deeper into internet use, it is very important to secure our data. Blockchain is going to play a role in every data-related field. Medical, banking, identity, etc sectors are already adopting blockchain technology. I have already proposed a theory about document validation, we can implement the theory into land distribution. Like fund supply, land distribution is very complex in Bangladesh and these are mostly dependent on handwritten documents.

References:

[1] Chowdhury, Anil 2021, Digital Bangladesh to Innovative Bangladesh: The road to 2041, UNDP, 25 December, last accessed 2nd December 2022 < https://www.undp.org/bangladesh/blog/digital-bangladesh-innovative-bangladesh-road-2041>.

[2] Transparency International 2021, CORRUPTION PERCEPTIONS INDEX, Transparency International, accessed 11 August 2022, < https://www.transparency.org/en/cpi/2021>.

[3] G. Locatelli, G. Mariani, T. Sainati, and M. Greco, "Corruption in public projects and megaprojects: There is an elephant in the room!" International Journal of Project Management, vol. 35, no. 3, pp. 252–268, 2017.

[4] Massimo Di Pierro, "What Is the Blockchain?". Computing in Science & Engineering, Issue No. 05 - September/October (2017 vol. 19) pp: 92-95

[5] Sharma, Toshendra Kumar 2018, "HOW CAN BLOCKCHAIN REDUCE CORRUPTION?" < https://www.blockchain-council.org/blockchain/how-can-blockchain-reduce-corruption/>

[6] Zoha, Tanvir Hasan, 2017, "Ransomware attack affects 30 PCs in Bangladesh", The Daily Star, May 15, < https://www.transparency.org/en/cpi/2021>.

[7] Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, p.21260.

[8] Liu, Y., He, D., Obaidat, M.S., Kumar, N., Khan, M.K. and Choo, K.K.R., 2020. Blockchain-based identity management systems: A review. *Journal of network and computer applications*, *166*, p.102731.

[9] A. Tobin, D. Reed, The inevitable rise of self-sovereign identity, The Sovrin

Foundation 29.

[10] C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, M. Sena, Uport: A platform for self-sovereign identity, URL: https://whitepaper. uport. me/uPort whitepaper DRAFT20170221. pdf.

[11] Shocard: The premier blockchain-based mobile identity platformhttps: //shocard.com.html.

[12] Heller, N., 2017. Estonia, the digital republic. *The New Yorker*, *18*.

[13] Saleh, O.S., Ghazali, O. and Rana, M.E., 2020. Blockchain based framework for educational certificates verification. *Journal of critical reviews*, *7*(03), pp.79-84.

[14] Nyaletey, E., Parizi, R.M., Zhang, Q. and Choo, K.K.R., 2019, July. BlockIPFS-blockchain-enabled interplanetary file system for forensic and trusted data traceability. In *2019 IEEE International Conference on Blockchain (Blockchain)* (pp. 18-25). IEEE.

[15] Mohite, A. and Acharya, A., 2018, December. Blockchain for government fund tracking using Hyperledger. In *2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS)* (pp. 231-234). IEEE.

[16] Manda, V.K. and SS, P.R., 2018, November. Blockchain technology for the mutual fund industry. In *National Seminar on Paradigm Shifts in Commerce and Management* (pp. 12-17).

[17] Saleh, H., Avdoshin, S. and Dzhonov, A., 2019, November. Platform for tracking donations of charitable foundations based on blockchain technology. In *2019 Actual Problems of Systems and Software Engineering (APSSE)* (pp. 182-187). IEEE.

[18] Rashid, N.B., Saha, J., Prova, R.I., Tasfia, N., Shanto, M., Huda, N. and Noor, J., 2022. Towards Devising A Fund Management System Using Blockchain. *arXiv preprint arXiv:2211.03613*.

[19] Di Pierro, M., 2017. What is the blockchain?. Computing in Science & Engineering, 19(5), pp.92-95.

[20] Xiao, Y., Zhang, N., Lou, W. and Hou, Y.T., 2020. A survey of distributed consensus protocols for blockchain networks. IEEE Communications Surveys & Tutorials, 22(2), pp.1432-1465.

[21] 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.

[22] Chan, W. and Olmsted, A., 2017, December. Ethereum transaction graph analysis. In 2017 12th international conference for internet technology and secured transactions (ICITST) (pp. 498-500). IEEE.

[24] Wackerow, Paul 2022, INTRODUCTION TO SMART CONTRACTS, Ethereum.org, September 22, accessed December 2, 2023< https://ethereum.org/en/developers/docs/smart-contracts/>.

[23] Ethereum.org, 2022, Introduction to Web3, Ethereum.org, November 22, accessed December 2, 2023< https://ethereum.org/en/web3/>.

[24] Belkhir, L. and Elmeligi, A., 2018. Assessing ICT global emissions footprint: Trends to 2040 & recommendations. Journal of cleaner production, 177, pp.448-463.

[25] Badea, L. and Mungiu-Pupăzan, M.C., 2021. The economic and environmental impact of bitcoin. IEEE Access, 9, pp.48091-48104.

Appendices

Experimental Results

The experimental results of the research are shown according to how blockchain works. The complete platform will take much time to build. Besides, testing with private blockchain is yet to be tested.

Project Reflection

Completing this project was quite challenging. Firstly it was a research based project and secondly the resource on blockchin is not much available. On the other hand, testing of blockchain technology is difficult as we can’t directly test our project directly on the mainnet.

A BLOCKCHAIN-BASED GOVERNMENT FUND MANAGEMENT SYSTEM

ORIGINALITY REPORT

13%	10%	6%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Daffodil International University Student Paper	2%
2	dspace.daffodilvarsity.edu.bd:8080 Internet Source	2%
3	kipdf.com Internet Source	1%
4	coin98.net Internet Source	1%
5	Submitted to National College of Ireland Student Paper	1%
6	Submitted to Sim University Student Paper	1%
7	ebin.pub Internet Source	<1%
8	eprints.utem.edu.my Internet Source	<1%
9	Submitted to CSU, San Jose State University Student Paper	<1%