

Blockchain Based E-Procurement System to Eradicate Corruption in Public Sector



by

- 1) Rabana Tajrin - 18101687
- 2) Lubaba Tasnia - 18101292
- 3) Shabab Masiat - 18101680
- 4) Md.Alkawser Rahman - 18101602

A thesis submitted to the Department of Computer Science and Engineering
in partial fulfillment of the requirements for the degree of
B.Sc. in Computer Science

Department of Computer Science and Engineering
Brac University
January 2022

Declaration

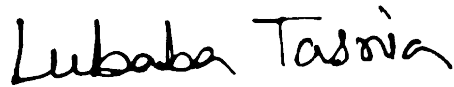
It is hereby declared that

1. The thesis submitted is my/our own original work while completing degree at Brac University.
2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. We have acknowledged all main sources of help.

Student's Full Name & Signature:



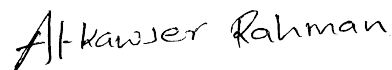
Rabana Tajrin
18101687



Lubaba Tasnia
18101292



Shabab Masiat
18101680



Md. Alkawser Rahman
18101602

Approval

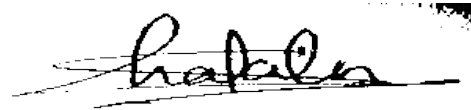
The thesis titled “Block-chain Based E-Procurement System to Eradicate Corruption in Public Sector” submitted by

1. Rabana Tajrin
2. Lubaba Tasnia
3. Shabab Masiat
4. Md.Alkawser Rahman

Of Fall, 2021 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on January, 2022.

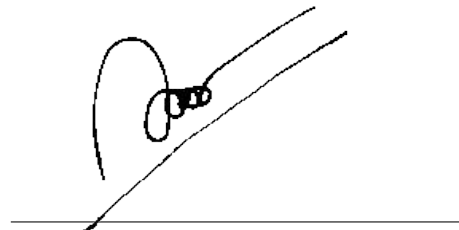
Examining Committee:

Supervisor:
(Member)



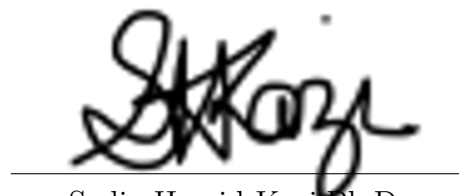
Shakila Zaman
Lecturer
Department of Computer Science and Engineering
Brac University

Co Supervisor:
(Member)



Dr. Muhammad Iqbal Hossain
Assistant Professor
Department of Computer Science and Engineering
Brac University

Head of Department:
(Chairperson)



Sadia Hamid Kazi, Ph.D.
Chairperson and Associate Professor
Department of Computer Science and Engineering
Brac University

Abstract

Public procurement is a basic function of the government for providing services to its citizens. A digitalized, tamper proof public-procurement function not only helps a country to make progress but also helps in economic growth of that country. We analyze the importance of having a blockchain based e-procurement system to maintain transparency and make the e-procurement process more effective and less complex, in this research. We identified the current problems Bangladesh are facing in this process like, tempering in transactional records , documents, complex process structures, intervention of multiple parties, massive corruption etc. So, we propose to have a blockchain based e-procurement system where public procurements will be monitored using Delegated Proof of Stake (DPoS) and Proof of Work (PoW) consensus algorithms. Implementation of this technology helps in efficiency when compared to the traditional way of working and adds a layer of transparency among the stakeholders and government authorities, which will eventually contribute to the development of our country, Bangladesh. In this paper we will use the health ministry as an example. As health is one of our most basic rights, our government allocates a huge budget every year in this sector. Our proposed blockchain based allocation system in the health ministry will ensure effective and rightful distribution of money.

Keywords: Blockchain; Public Procurment; DPoS; PoW, GETH, SHA256,

Acknowledgement

All praise to almighty the Allah by whose blessings we have completed our Thesis. And also we are really grateful to our Supervisor Shakila Zaman and Co-supervisor Dr.Muhammad Iqbal Hossain for sharing their valuable knowledge with us and most importantly giving us their precious time and guidelines. Their availablity to our needs and kind support has made this journey possible. We also thank our Parents for their support and with their prayer we are now on the verge of our Graduation.

Table of Contents

Declaration	i
Approval	ii
Ethics Statement	iii
Abstract	iii
Acknowledgment	iv
Table of Contents	v
List of Figures	1
1 Introduction	2
1.1 Motivation	3
1.2 Research Problem	3
1.3 Research Objectives	4
1.4 Thesis Structure	4
2 Literature Review	5
2.1 Delianiting Blockchain	5
2.1.1 Block	6
2.1.2 Types of Blockchain	7
2.2 Related Works	9
3 Methodology and Case Study	12
3.1 Case Study	13
3.1.1 Case In Point	14
3.2 Proposed Model	15
3.2.1 Genesis Block	15
3.2.2 Data Block	16
3.2.3 Previous Hash	17
3.2.4 Current Hash	18
3.2.5 Timestamp	18
3.2.6 Nonce	18
3.2.7 Consensus	19
3.2.8 Proof of Work (PoW)	20
3.2.9 Distributed Ledger	20
3.2.10 Decentralized System	20

3.2.11	Smart Contract	21
3.2.12	On Chain and Off Chain	21
3.2.13	Mining	23
3.2.14	Cryptography	23
3.2.15	Revocation	24
3.3	Store and Retrieve Files	25
3.4	Reasons behind choosing DPoS over PoS.	27
4	Implementation and Analysis	29
4.1	Configuration	29
4.2	Result	36
4.3	Cost Analysis	38
5	Conclusion	41
	Bibliography	45

List of Figures

2.1	Blockchain networks of 4 blocks	5
2.2	Block creation and Mining	6
2.3	Block creation	7
2.4	Types of Blockchain	8
3.1	Flow chart of blockchain based e-procurement system (User Side) . .	12
3.2	Threatening areas of corruption and its end result.	13
3.3	Blockchain based E-procurement System (health sector) [17]	14
3.4	Activity diagram of Proposed Model (Government Side)	15
3.5	Data block	16
3.6	Hash and Previous hash	17
3.7	Nonce [18]	19
3.8	Storing file in the server	26
3.9	Retrieving file from the server	27
3.10	Working process of PoS and DPoS	28
4.1	Account Creation	29
4.2	Genesis block pseudo code	30
4.3	Creating the genesis block	31
4.4	Creation of private blockchain network	31
4.5	Mining to validate block	32
4.6	Connecting remix ide to geth private network to deploy smart contract	32
4.7	Contract Deployment using web3 injection	33
4.8	Pseudo code for smart contract 1	34
4.9	Pseudo code for smart contract 2	35
4.10	Contract 1	36
4.11	Contract 2	36
4.12	Successful transaction confirmation	37
4.13	Comparison Between Contracts	38
4.14	Graph of Contract 1	39
4.15	Graph of Contract 2	40

Chapter 1

Introduction

We are all free citizens of the People's Republic of Bangladesh. Any country in the world needs to provide goods and services to its own citizens as it is one of its core functionalities, which is known as public procurement. A digitised and temper proof public-procurement function can help a country to make progress and moreover it helps in economic growth of that country. Though we have all these gains from the public procurement system, for developing countries like Bangladesh, it is a huge problem to finish the process efficiently and transparently. This only happens due to a scarcity of trust and lucidity among the contributors to this process. Tempering in transaction records, documents, intervention of multiple parties, massive corruption, etc., are the main causes behind the weak and ambiguous procurement system. After distributing or exchanging corruption money between companies, government officials, and other parties, only a very small part is left to fulfill the public's demands or needs, which is not sufficient at all. To overcome all these issues and to keep transparency and trust, a fresh application to track all the particular features of public procurement is needed. This is where the concept of blockchain comes into play. A blockchain is a localized, allocated, and oftentimes public, digital registry containing data called blocks that are used for recording transactions across many devices so that any involved block cannot be changed retroactively, without the changing of all following blocks. So, blockchain has the potential to make a positive change in the e-procurement system and make it more authentic and trustworthy.

are all free citizens of the People's Republic of Bangladesh. Any country in the world needs to provide goods and services to its own citizens as it is one of its core functionalities, which is known as public procurement. A digitised and temper proof public-procurement function can help a country to make progress and moreover it helps in economic growth of that country. Though we have all these gains from the public procurement system, for developing countries like Bangladesh, it is a huge problem to finish the process efficiently and transparently. This only happens due to a scarcity of trust and lucidity among the contributors to this process. Tempering in transaction records, documents, intervention of multiple parties, massive corruption, etc., are the main causes behind the weak and ambiguous procurement system. After distributing or exchanging corruption money between companies, government officials, and other parties, only a very small part is left to fulfill the public's demands or needs, which is not sufficient at all. To overcome all these issues and to keep transparency and trust, a fresh application to track all the particular features of public procurement is needed. This is where the concept of blockchain comes into

play. A blockchain is a localized, allocated, and oftentimes public, digital registry containing data called blocks that are used for recording transactions across many devices so that any involved block cannot be changed retroactively, without the changing of all following blocks. So, blockchain has the potential to make a positive change in the e-procurement system and make it more authentic and trustworthy. That is why in this paper we are proposing a blockchain-based e-procurement system to ensure the success and actual objective of public procurement, using Bangladesh as a case. After conducting various research about how procurement systems allocation and process flow go on in Bangladesh, we came up with some drawbacks and problematic issues with this process. Agreeing to our proposal, we would attempt to ease the mistakes and blemishes of the current framework and make it successful by utilizing blockchain-based e-procurement frameworks. In countries like Bangladesh, where people have many health issues and disabilities, As a developing third world country, we need more manpower to develop our economy, and people with health issues can't help in the country's development, rather they hinder the process. For this purpose, the government spent a large sum of money on the development of the health sector. As corruption and mismanagement occur in every sector of the country, ours is no different. In most cases, mismanagement or corruption has a huge effect on quality, equity, efficiency, access, and the success of health care services. Though it affects everyone, the poorer sections of society suffer more. There have been many health rights movements and many articles show that doctors and other health professionals in public hospitals are accountable for all this mismanagement or corruption. With a view to this, we will be considering the health ministry's allocation process, for example, and try to build a block-chain based allocation system for them so that we can ensure the proper and rightful distribution of money while maintaining proper transparency.

1.1 Motivation

Singapore, a country that everyone dreams of, it literally got recognition from a dying land to first society rank within 10-20 years of its independence, it became everything to nothing. So, why is our country lagging behind? Almost 50 years after becoming independent, our country's structure is still very fragile. Pondering over this matter, one thing came to our mind, which is that our public procurement sector is not strong enough. Look at the "Padma Shetu" project, which is taking so much time. Though the funding from the government in all those sectors is good enough, the fact is that it lacks proper usage only because of proper transparency. So, our proposed model will ensure the proper and rightful distribution of public procurement, thus contributing to the country's development.

1.2 Research Problem

A public procurement system is one of the main functionalities for any government of any country, and a digitized, tamper-proof public procurement function not only helps a country to make progress but also helps in the economic growth of that country. Trust and transparency are missing between the contributors. That is why it is a massive mess to end the procedure efficiently and transparently. Tempering in

transactions, records, documents, intervention of multiple parties, massive corruption, etc., are the main causes behind the weak and ambiguous procurement system. Our existing procurement process lacks the ability to ensure transparency and security of transactions, and it is very cumbersome and complex. In our paper, we use the health sector as an example. Each year the government allocates a sufficient amount of public revenue for the health sector, but as there is a lack of accountability, those allocated resources flow through different stages of national and local governmental institutions on their way to health facilities, which means facilities are not rightfully distributed. Our current system cannot ensure that allocated funds are used for their intended purpose.

1.3 Research Objectives

This research aims to create a blockchain based e-procurement system for monitoring public procurement using Delegated Proof of Stake (DPoS) and Proof of Work (PoW) consensus algorithms. Maintaining transparency in a huge budget procurement and reducing corruption by adapting blockchain can make the process more efficient. Hence, the main idea of having a blockchain based procurement system is to eradicate the current system's drawbacks and corruption, thus making the system more secure and trustworthy. The objectives of this research are:

- Implementing blockchain in the public sector to eliminate corruption.
- Increase performance of current processes with the help of online based procurement processes.
- Creating a layer of transparency between different government bodies.
- Making the process faster and easier than the current traditional process.
- Build a system to ensure rightful and proper distribution of allocated money for the health sector.

1.4 Thesis Structure

In our paper, the first chapter consists of four parts: motivation, research objective, research problem, and thesis structure. Here the reason behind choosing this topic is described. On the other hand, the second chapter described what blockchain is and a summary of some papers that are similar to our paper. Chapter 3 has a case study and a scenario where there is a clear vision of how the public procurement sector works currently and some new procedures to deal with existing problems. All of our work on this project, our proposed model, results of our work, and cost analysis are mentioned in chapter 4. And then chapter 5 contains the conclusion and future work. Lastly, there is a bibliography that contains all the references. That's how this paper is organized.

Chapter 2

Literature Review

2.1 Delianiting Blockchain

A blockchain network is an immutable, decentralized ledger for all the transactions and exchange of information in peer-to-peer networks. In this blockchain network, no central authority is needed to confirm all the transactions [1]. A blockchain is a collection of chains of blocks where each block contains information about the transactions. Informations can not be changed which are stored inside the blockchain. For example, no new information can be added or deleted once the information has been recorded in the block.

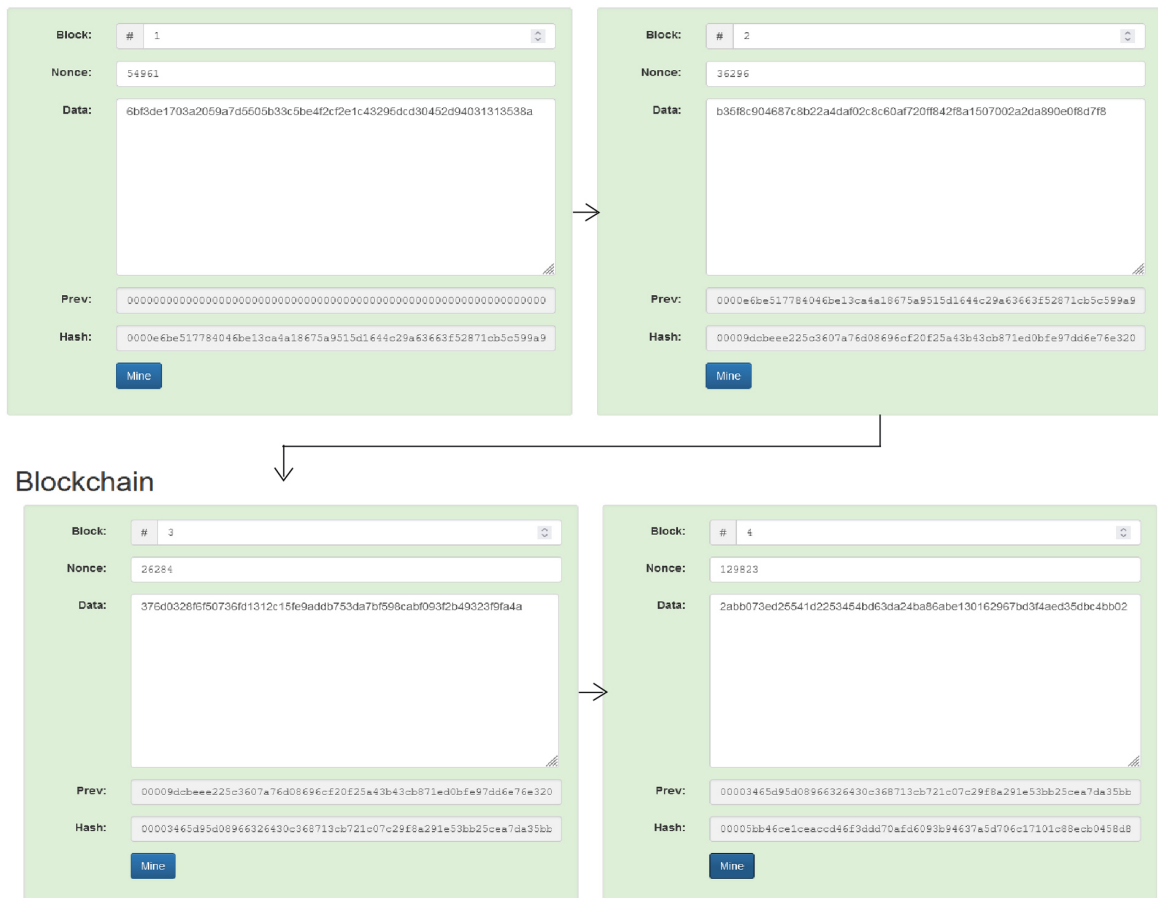


Figure 2.1: Blockchain networks of 4 blocks

2.1.1 Block

Each block is divided into some segments where data, the hash of the block and previous hash values, nonce, and timestamps are stored. Data or information can contain sender's and receiver's information along with the transactional information.[2] The hash of the block is a unique identifier which represents the block and all the information inside the block. The hash is set when a block is created, and if any change occurs in the block, the hash will change accordingly. By inspecting the hash, any change in blocks can be easily determined.

Block: # 1

Nonce: 72608

Data: 6bf3de1703a2059a7d5505b33c5be4f2cf2e1c43295dcd30452d94031313538a|

Hash: 63d5d288792c3f4fc804be03a6b1dd838afe575aa6ccf1897521115ff700c306

Mine

Block

Block: # 1

Nonce: 27488

Data: 6bf3de1703a2059a7d5505b33c5be4f2cf2e1c43295dcd30452d94031313538a

Hash: 0000628fe2ccfb3be9d631ac6c222e7e182ed26a3622bdfacf8edcbfffd033e15

Mine

Figure 2.2: Block creation and Mining

The blocks contain hashes as the form of encrypted data. The hash value of the transactions in each block represents the main information in encrypted form. After putting the hash information as data in the block, it will be mined. Therefore, each block will generate a new nonce and new hash value, which will be then used for creating a blockchain. Here are a few examples of the blocks shown in the figure.

Block

Block: # 2

Nonce: 66738

Data: b35f8c904687c8b22a4daf02c8c60af720ff842f8a1507002a2da890e0f8d7f8

Hash: 00009e14b6a6044c908436a0d5adca81d825823b5d9570252c6f248bda9baef2f

Mine

Block

Block: # 3

Nonce: 67161

Data: 376d0328f6f50736fd1312c15fe9addb753da7bf598cabf093f2b49323f9fa4a

Hash: 0000a6461660d01bcd9f15780fe4fd5fe488bc27ca929e2da9089a0e4654241

Mine

Block

Block: # 4

Nonce: 94740

Data: 2abb073ed25541d2253454b63da24ba86abe130162967bd3f4aed35dbc4bb02

Hash: 0000a53f20891a53d1d35a1codd148f8524e4c0ee270d257346c69d3ea34c326

Mine

Figure 2.3: Block creation

2.1.2 Types of Blockchain

The blockchain types can be categorized into three sections, which are permissioned, permissionless, or both [3]. Permissionless blockchain networks are open networks that are not controlled by a central authority. Hence, it gives full transparency to the users, and transactions take place without the permission of anyone. Users can join anonymously on the network. Permissionless blockchains are considered more

secure than permissioned ones because in this network, all the transactions are validated by many nodes. Moreover, permissionless blockchains take more time for the transaction process owing to their larger nodes. On the other hand, a permissioned blockchain network is a closed network opposite to the permissionless one. In the case of a permissioned blockchain, the identities of the users are not anonymous; rather, all the users of the network are known to each other. Permissioned blockchain access is restricted, so there are fewer users and fewer blocks. Therefore, all the transactions in this network take less time to occur. The transparency in the permissioned blockchain is not full, but the transparency is controlled in the permissioned network. Furthermore, users need permission for any kind of transaction in the permissioned blockchain.

Under permissioned blockchain and permissionless blockchain, there are four sub-sectors which are: public blockchain, private blockchain, hybrid blockchain, and consortium blockchain. As the public blockchain has no central authority, it falls under the permissionless blockchain, which also has no central authority. Private blockchains and consortium blockchains are under permissioned blockchain networks because both of them are controlled either by a single authority or by a group of authorities. However, hybrid blockchains are in the middle position, as these types of blockchains are controlled by a single authority but have some permissionless procedure.

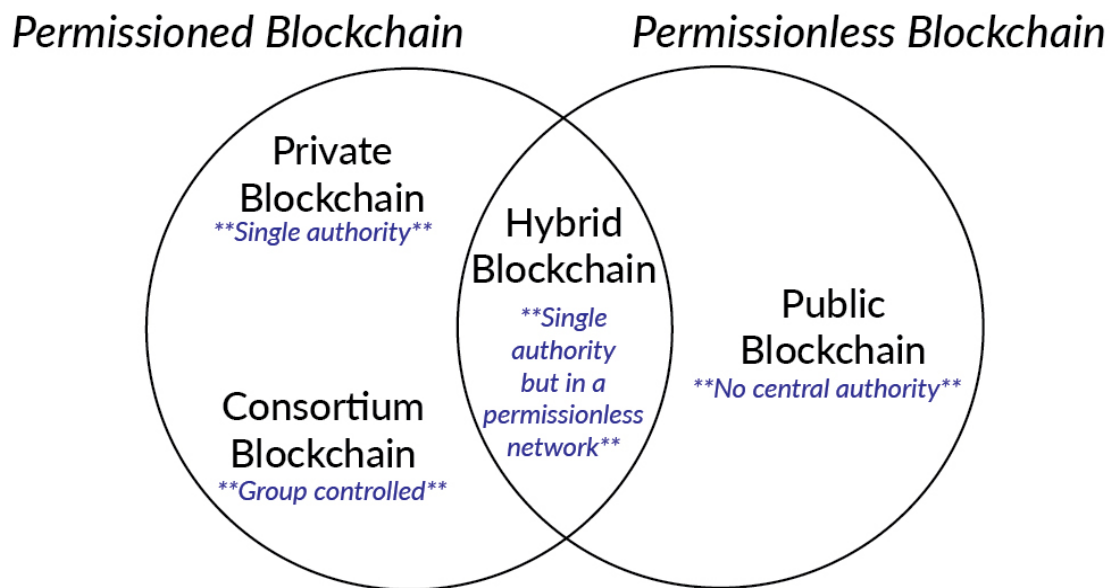


Figure 2.4: Types of Blockchain

2.2 Related Works

A blockchain is a method of storing data that makes it nearly impossible to alter, hack, or defraud the system. A blockchain is essentially a digital log of transactions that is copied and distributed across the network of computer systems that make up the blockchain. Every block in the chain contains a number of transactions, and whenever a new transaction occurs on the blockchain, a record of it is automatically added to the ledger of all participants. A decentralized database administered by several members is referred to as Distributed Ledger Technology. Smart contracts, which may be created using blockchain, can improve the transparency and efficiency of any task.

In this paper [4], the authors modernize the land registry system by adapting the blockchain system using the Proof-of-Work (PoW) algorithm. The core purpose is to make the land registry system more secure and more reliable. They came up with a system where every transaction will be recorded within a block, and all blocks will be connected to each other using hash values. The authors use the SHA256 hashing algorithm to generate hash code with the help of the Elliptic Curve Digital Signature Algorithm. In their proposed idea, there is an option to purchase land directly, which ensures no third-party transaction. After fulfilling the requirements, transactions are enlisted and new chains are distributed among the nodes. If a chain of nodes' computerized signature matches that of more than 50 percent of other chains of hubs, it is acknowledged and protected by the framework; if something else, it is erased. This paper [4] aims to remove fraudulent activities and unauthorized entities by using blockchain to secure land registry systems.

According to the author [5], one of the most challenging tasks in developing nations' land governance is maintaining up-to-date and accurate land registry documentation that is secure from attackers or corruption. Their proposed solution takes an approach to digitizing Bangladesh's land registry documentation process while also making the documentation secure. The proposed system integrates with the government of Bangladesh's existing land registry services. All the information related to land properties included in land registry documentations is kept in a private ledger and is kept connected to each other using cryptographic hashes when Blockchain technologies are used in land registry. One of the key features that the author implemented is DPOS (Delegated Proof of Stake system) based blockchain integration. Although DPOS is faster and more efficient. However, by concentrating validation in a few hands, delegates might form cartels, reducing the blockchain's decentralization and vulnerability to attacks.

We can see that the authors [6] describe the core function of government activities, which is public procurement. Despite these advantages, developing countries such as Nigeria face difficulties such as a lack of confidence and openness among key actors in the public procurement process. Corrupt money transactions among companies and other government officials are on the rise. Therefore, they have created a system that takes an innovative approach to keeping track of all aspects of public procurement with confidence and transparency. In this paper, they showed a blockchain based e procurement framework where they proposed additional chain actions for citizens to vote on project requirements that are prioritized at the bidding stage. In this article, the authors did not take into account the financial implications of the proposed blockchain system. Again, they haven't even given enough thought to blockchain,

security, and privacy.

In the research paper [7], the author emphasizes the importance of implementing blockchain in the healthcare domain. The review presented the most up-to-date information on the current implications and gaps surrounding the usage of blockchain technology to improve healthcare operations. The blockchain is being used to produce unique and advanced solutions to improve the current standards of medical data handling, sharing, and processing. This technology has provided significant value to data management procedures by improving efficiency, access control, technical progress, privacy protection, and security. Essentially, a blockchain is a decentralized public ledger database that operates in a manner controlled by a network of verified members or nodes and supports arbitrary data blocks. Variables can be safely passed without the intervention of a third party. Where cryptographic signatures and consensus techniques are used to preserve and record data, which act as crucial enablers for its implementation, Despite this well-sorted technology, there is a limitation: the public and individual users, such as patients or doctors, are unfamiliar with how blockchain works, its technological characteristics, or its benefits for data management.

The author, [8] , proposes a complete and non-renewable anti-counterfeiting system that works on Blockchain. In the diagram, constructors use this procedure to store admissible information about product sales in the blockchain that is accessible to everyone. The merchant's total salable sales and the merchant's available product balance are transparent to the user. Users can use the functions provided by our system to perform instant verification of the provider's website but cannot do this verification.

In [9] , we can see it's work from India. Land-related fraud is a big problem in countries like India, so the authors proposed the use of blockchain and smart contract technologies to counter some major problems. In their work, they will try to make some changes, like using smart contracts for ownership transfer, selling land digitally through smart contracts, capturing the terms of sale, etc. This idea will enhance data security, ensure authenticity of land records, and also make customers' experience less cumbersome. Here, the authors could not find a way to solve the problems if they took place during the time of download. Finally, they suggest that if by using AI we could recognize fraud, then the idea would work fully.

Blockchain was employed by the authors [10] to combat corruption. Because blockchain is used to construct a tamper-proof digital ledger of any transactions and share them, transparency is preserved. They also referenced a situation in China where the use of fraudulent export invoices to cover up cross-border capital problems is widespread. 10 billion in illegal trade transactions were uncovered between April and September of this year. To address these issues, Chinese banks charge higher interest rates in order to bring the economy back into balance. Blockchain can help to prevent this type of corruption and so aid in the growth of a country's economy as well as minimize or eliminate integrity issues.

In this paper [11], the author used blockchain technology on public procurements in Nigeria to enhance the effectiveness, ease and transparency to eradicate corruption in public sectors. The author wants to erase massive corruption involved in the procurement process by using blockchain-based e-procurement systems. He used

case study-based qualitative analysis as the main research methodology. Case study: data was collected through interviews and reviews of related documents. The main limitation of this paper [4] is that the case study only deals with one particular group of people. The author aims to do in-depth analysis and research in the future with a broader population. To sum up, adapting blockchain technology to the e-procurement system elevates the management system in the procurement process as well as makes it more transparent for the growth and development of the country, Nigeria.

The writers of this study report [12] looked at how blockchain technology can help reduce corruption in the context of Brazil. Because of its unique encryption and security features, this system is almost fraud-proof. In addition, a blockchain is a decentralized ledger that is often controlled via a peer-to-peer network. These distributed registers store information such as ownership and transfer records, financial transaction records, digital currency records, and more. Their findings demonstrate that corruption in Brazil has risen at an alarming rate; for example, 141 articles dealing with corruption issues have been published in the last five years, out of a total of 227.

Here in the research paper [13], the author particularly emphasized the fact that blockchain technology has become increasingly popular due to the popularity of cryptocurrencies, and its multi-domain implementation has become a viable concept. According to the results, the research of blockchain technology in healthcare is growing and it is mainly used for data exchange, patient record management, and access control. The blockchain serves as a distributed ledger in the cryptocurrency market and stores all completed coin transactions. Finally, the author believes that blockchain research in healthcare appears to be a promising field as it consists of data sharing, health records, and access control, but it is rarely used for other situations, such as supply chain management or prescription drug management, according to current developments. Most of the research in health uses blockchain technology to propose a new framework, design, or paradigm. This reflects the author's ideology of designing a transparent healthcare system using blockchain technology.

Chapter 3

Methodology and Case Study

The main objective of our project is to ensure transparency and the rightful distribution of money in the public procurement sector. Keeping this in mind, we tried building such a system where all the transactions would be secured as well as monitored. Therefore, we must ensure that mismanagement is eradicated from the public procurement system and make it fulfill its actual purpose.

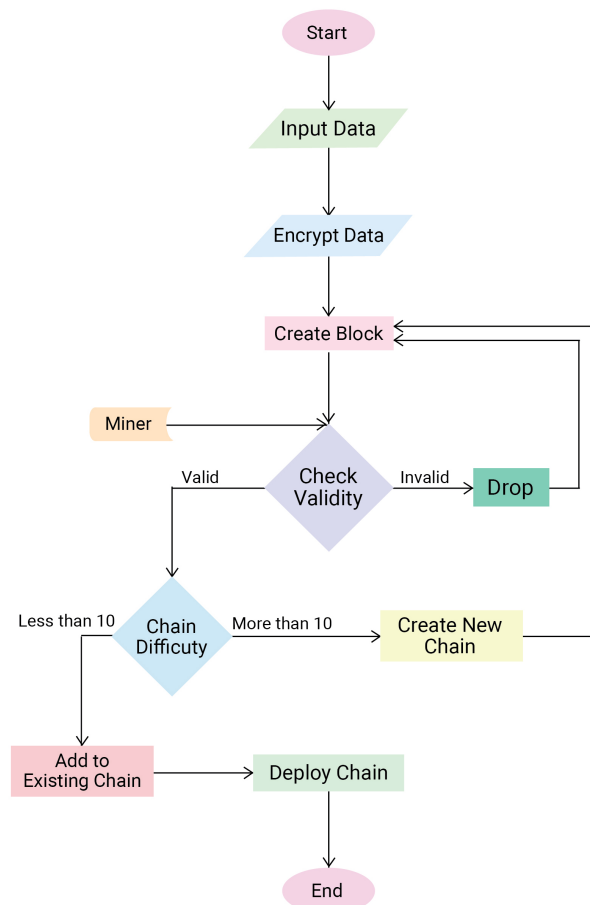


Figure 3.1: Flow chart of blockchain based e-procurement system (User Side)

3.1 Case Study

For the economic growth of any country, the necessity of health is shown in the Millennium. In the Millennium Development Goal (MDG) [14]. There are eight goals in the MDG and three of them directly indicate health. One of the additional goals is to ensure affordable drug access in developing countries. To make sure people are getting an equal amount of quality health services, the government allocates a huge share of public revenues to the health sector. But the question arises here, if we have all these budgets, why are so many people still ill treated today? Why are so many of them facing death due to a lack of proper treatment? Why are the majority of people not getting the medicines that were supposed to be free and government funded? What actually happens is that allocated resources for health for the health sector flow through different layers of national and local government institutions on their way to health facilities. And they are not even utilized for the purpose they were supposed to do.

A research [15] show that the Anti-Corruption Commission found that five people, along with former and current directors of the 250-bed TB hospital in Dhaka, collaborated with each other to steal the government's fund to propose an additional price of around Tk 4.46 crore in the name of buying necessity goods for the hospital. In this deteriorating pandemic, our government declared 19 incentive packages totaling USD 12.13 billion to mitigate people's sufferings from the pandemic. [16] Even in this situation, the media reported 218 relief-related corruption cases from March 10, 2020, to June 15, 2020. And in almost every case, the lawbreakers are government service holders, public employees, and activists. The proposed expenditure for equipment for Tajuddin Medical Hospital was USD 20.70 million, which was almost 10 times larger than the actual cost. The food and living costs of 500 physicians for one month were proposed to be 23.60 billion, which is really absurd and obviously the actual was way less than this. Inadequate information flow, lack of transparency, insufficient accountability are all pulling our health care sectors as well as our economic growth behind.

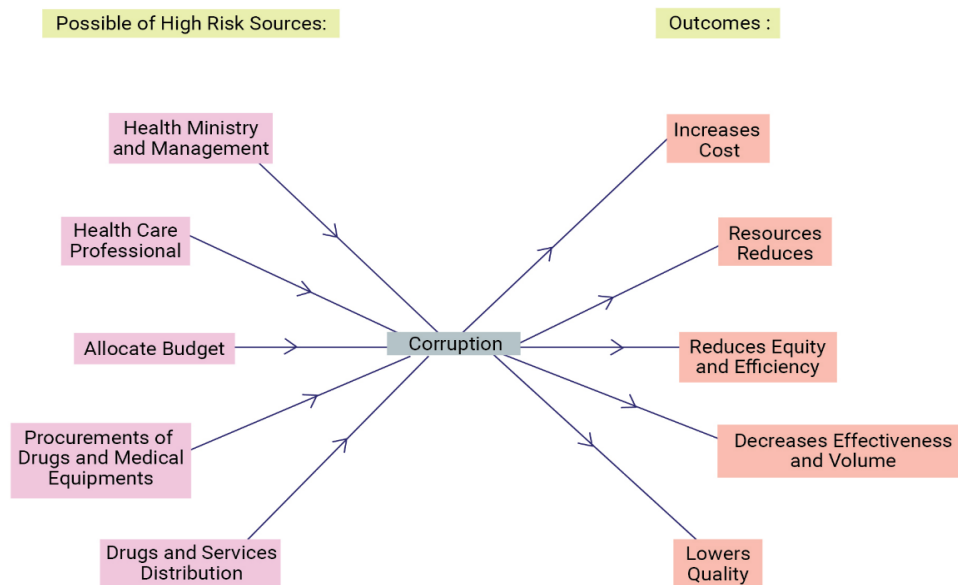


Figure 3.2: Threatening areas of corruption and its end result.

3.1.1 Case In Point

Imagine utilizing all the facilities given by our government. What would our country look like if we could have proper and rightful utilization of public procurement? This is like a dream, right? If this dream comes true, our citizens will benefit. People's lives will become easier, and most importantly, our country's standards will rise. So, to make this dream come true, we are thinking of building a system that will ensure proper utilization of government fund allocation.

Let's take Dhaka Medical as an example, as it renders the best yet cheapest service to the people. Any sort of treatment is cheap here, but the question is how DMC gives service at this very low rate. It's simply because the government is providing them with a huge amount of funding. The health ministry of the government allocates funds for this medical and, after proper investigation, the money is transferred to the hospital's account from the national treasury. And from the hospital's account, the money is used whenever needed. And in the middle of the process, corruption takes place because of a lack of accountability and proper monitoring. Thus, government funds cannot fulfill their intended purpose. So, we need to monitor and secure this transaction to have a transparent and proper utilization of funds.

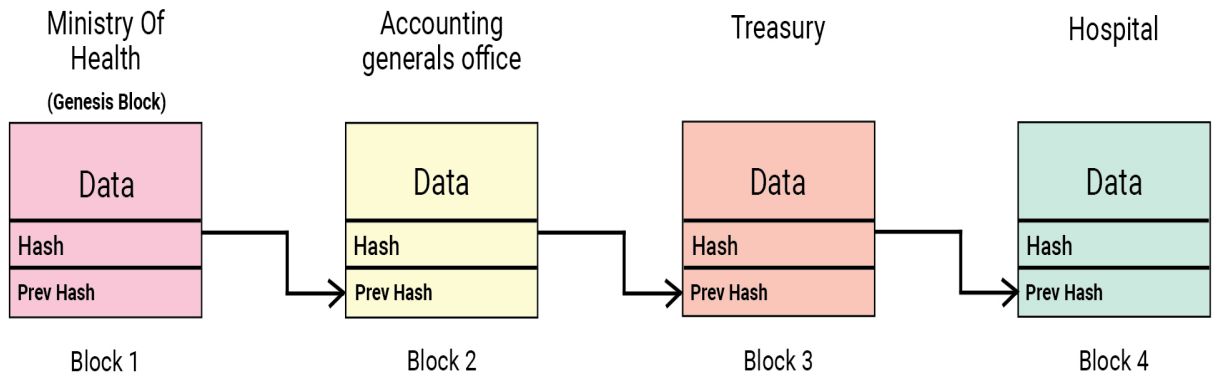


Figure 3.3: Blockchain based E-procurement System (health sector) [17]

3.2 Proposed Model

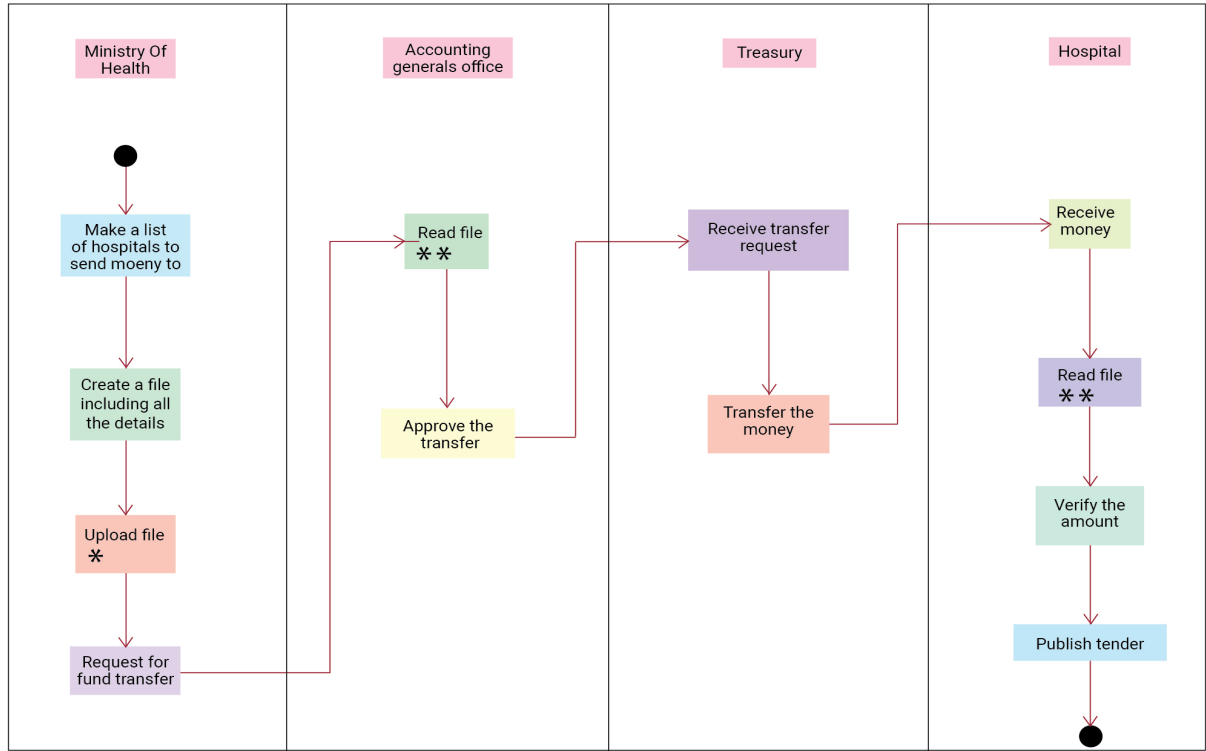


Figure 3.4: Activity diagram of Proposed Model (Government Side)

3.2.1 Genesis Block

The Genesis block is the name given to the blockchain network's very first block. The network consists of a series of blocks where each block has its own unique header, which is recognized by its block header hash. The blocks are used for storing information about the transactions made in accomplishing the project with the help of a blockchain network system, which ensures more transparency and improved security. The layers and extensive history of each sequence are one of the essential qualities that make a block chain based network so reliable. Among the other blocks on top, there is a collection of some blocks where all the most recent transactions are stored, that haven't been recorded in any prior blocks. As a result, the block chain network system mimics the functionality of a ledger page or a record. These blocks are piled one on top of the other, with the Genesis Block serving as the foundation, and they continue to rise in height until the maximum limit for the blockchain network has been reached. The Genesis Block, or Block 0, is the very first block in a blockchain, upon which subsequent blocks are placed. Because, every block refers to the one before it, every block will have the header hash of the block next to it. Thus, all the transactions are saved and the user's actions can always be monitored, making it difficult or almost impossible to tamper with any kind of information.

3.2.2 Data Block

Data blocks are data storage units that are similar to files in a traditional system, where permanent records of network data can be found. When a block in the blockchain is finished, it makes room for the next block in the chain. Here, as we go down the series, each block is linked to the hashes that came before it, which forms a chain of blocks connected to its preceding one, which is the reason why it is called a block chain. Among all the aspects, the most significant one for storing information is the data blocks or nodes where the records are permanently stored and can't be changed or erased once recorded. The blocks are uploaded to the block-chain network and contain all transactional data and other information. Like in a linked list, the blocks in our design are appended linearly across a chain to the preceding hash.

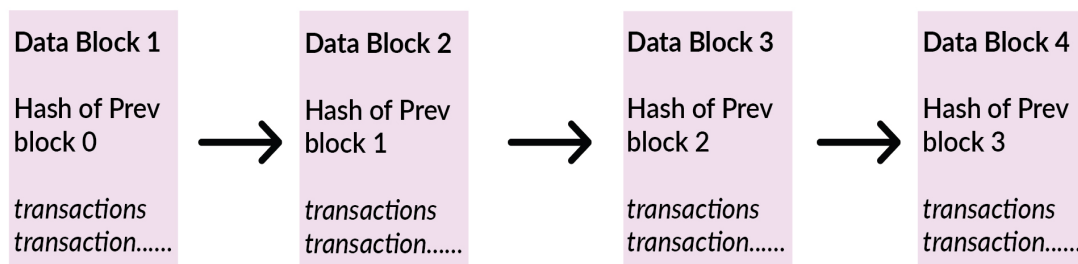


Figure 3.5: Data block

3.2.3 Previous Hash

A hash function is a mathematical operation used to convert an arbitrary-length input into a fixed-length encrypted output. Keeping the unique hash for each block of the same length. A hash cannot be used for reverse engineering; it is only applicable for one-way traversal across the block chain network. The preceding hash (SHA256, used in coding) links all of the blocks in our blockchain, ensuring the originality of the block chain's one-way traversal. This system uses a 64-bit (SHA256, used in coding) hash that cannot be overwritten. Our system's blocks all point to the preceding block and finally towards the genesis block. However, because the blocks are dynamically generated and altered on a regular basis, traveling through them will never take you to the genesis block. As a consequence, the block-chain is immutable and maintains its integrity. Traversing through the blocks, however, will never lead to the genesis block because they are dynamically formed and updated on a regular basis. The result is that the block-chain is immutable and consistent.

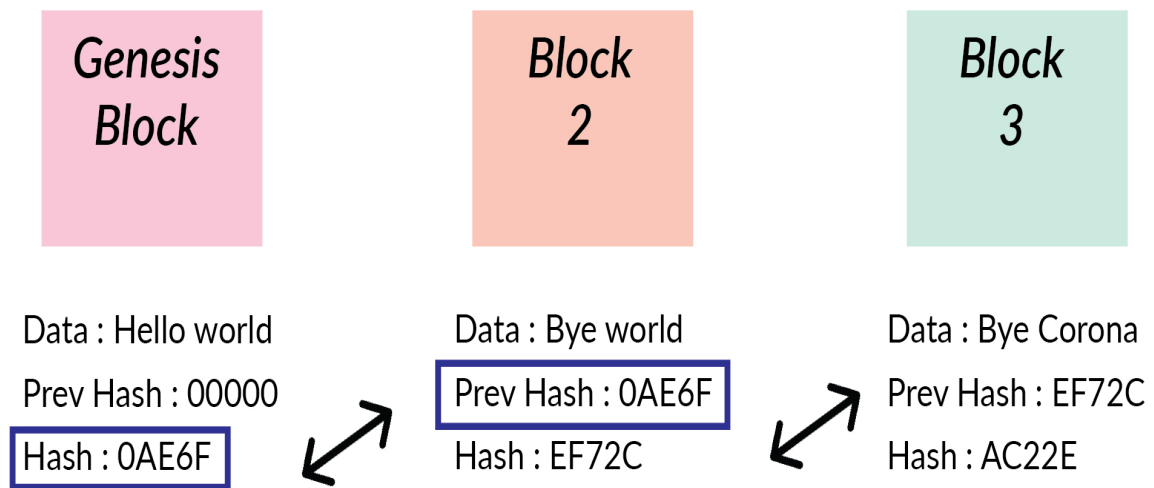


Figure 3.6: Hash and Previous hash

3.2.4 Current Hash

In the blockchain network, every block contains a hash that is unique to it. These hashes cannot be overwritten and serve as the basis of the network by connecting all the individual blocks with the block chain network system, where each block contains its preceding block hash. Our main concern is how to create those hashes so that they represent each block by giving them a unique identity. In doing so, we need to take into account three things: timestamp, nonce, and flags. After that, large hash keys are converted into small ones using the hash function. When hashing is done, the data will be stored in the hash table for convenient retrieval.

3.2.5 Timestamp

The timestamp within the block is a section of data where the time of creation for the block can be found, which has been mined and validated using the network. This recorded data is unique to each block, which further contributes to generating a unique hash for each block, making the block chain network immutable. Timestamps keep the record of the transactions. For example, when blocks are being created, deleted, or exchanged information, timestamps are essential.

3.2.6 Nonce

The term "Nonce" stands for "Number Only Used Once." In any cryptographic network, in our case, a block chain nonce is a random number of one-time use only. It ensures the block delivery on time using the timestamp data. The whole network should be synchronized, which makes it suitable for two-factor authentication. We need to keep in mind that a nonce should have a timestamp in its value or be created with enough random bits to ensure that a previously built value has a lower probability of being duplicated.

Client-server communication during nonce based process

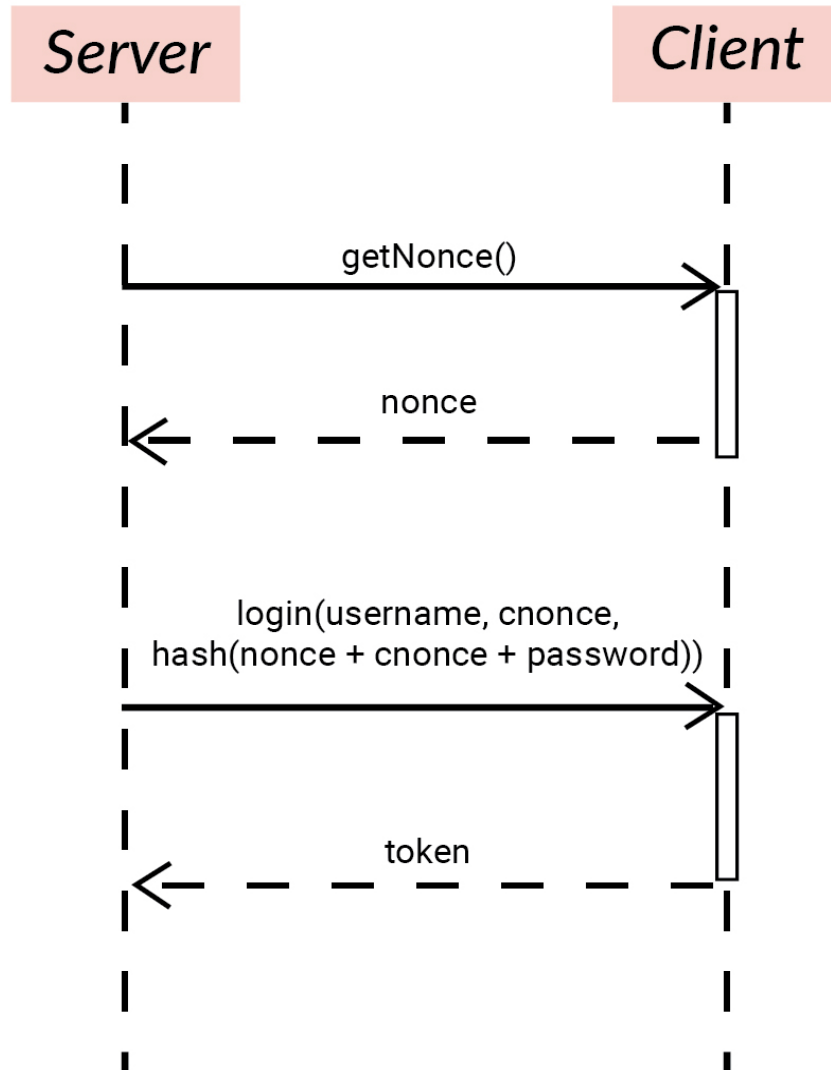


Figure 3.7: Nonce [18]

3.2.7 Consensus

Consensus is one of the pillars of our block chain network and it is considered as an agreement for eradicating non-viable transactions. The involvement of third parties and corrupted systems results in the wastage of resources, which is common in our traditional transaction systems. The whole block chain network is developed using appropriate algorithms in order to track the whole transactional activity from time to time. The most crucial part of the consensus protocol in our system is the Proof-of-Work algorithm, which allows a digitalized and decentralized system to monitor if a transaction is authentic or not.

3.2.8 Proof of Work (PoW)

Proof of work (PoW) is a decentralized consensus technique that encourages network users to spend time completing arbitrary tasks in order to prevent the system from being monopolized.[19] PoW is widely used in cryptographic networks like Block Chain for validating transactions and mining them. It takes a lot of energy to mine, and the amount of energy required grows as more miners join the network. Without the use of a trusted third party, transactions can be completed peer-to-peer in a secured and more transparent way. Because altering any aspect of the blockchain would require re-mining all subsequent blocks, the Proof of Work makes it very difficult to crack. It also makes it impossible for a single user or a group of users to monopolize the network's computing capability, because the hash functions demand a lot of machinery and resources in order to crack the function and manipulate.

3.2.9 Distributed Ledger

A distributed ledger is a database that can be synced and accessed by different users.[20] Each network node's participant has access to the network's shared information and may retrieve a copy of it. Any manipulations or additions to the ledger will be notified to all participants instantaneously in an automated manner. The deployment of a distributed ledger eliminates the need for a central authority to maintain a check on the manipulation of data. The technology is the same as that implemented by bitcoins, which serves as the distributed ledger for our blockchain system.

Distributed ledgers also eliminate discrepancies, reduce the time it takes to execute a transaction, and are automated, allowing them to operate 365 days a year and at any given time, all of which lower total costs for the institutions that utilize them. In effect, the implementation of this technology helps to prevent cyber threats and financial fraud by adding an extra layer of protection. A further benefit of distributed ledgers is that they facilitate the uniform flow of information, which makes it easier for accountants to follow an audit trail while conducting financial statement reviews. It is also an eco-friendly approach since people will reduce their consumption of printed materials.

3.2.10 Decentralized System

Mostly, blockchain technology and its applications rely on decentralization. Decentralized applications' (dApp) aid may be improved by decentralizing their management and access to their dedicated database. As a result, more prominent and pleasant support can be provided to all the users and stakeholders within the system. Although decentralization has one major drawback regarding lower rate of data exchange. However, our goal is to build a secure and transparent flow of information, which is what a decentralized system is ideal for. One of the key benefits is In a decentralized blockchain system, there is no need to have blind faith among members. This is due to the fact that every member of the network possesses a duplicate or exact copy of the information contained in a distributed record. Whenever a member's record is altered or polluted in any manner, the majority of the people in the network and the members themselves will be notified regarding all tampering, which will be enough to take legal action against the manipulators. Through the

system, it is possible to regularly update information and save each party's information in their respective storehouses, which can be retrieved when it is necessary to be transferred downstream. Thus, making the system reliable, secured and convenient to interact with.

3.2.11 Smart Contract

Smart contracts are basically programs which operate in such a way that when the predetermined criteria of the program are fulfilled and are maintained on a blockchain, only then are the contracts allowed to be executed. They are actually used to create a systematic platform for the execution so that all parties can feel secure about the end results from the very first day of starting the contract, without the need for any intermediary parties or brokers. Smart contracts also retain the characteristics of each block within the blockchain, as well as an existing data document where all the failures and limitations are preserved. Smart contracts oppose traditional paper contracts that rely on middlemen and other third-party intermediaries for implementing contractual activities and lowering administration expenses. Permissioned smart contracts on block-chains are becoming more and more widespread in joint corporate operations as they serve accountability and privacy in an efficient way. Here, our choice of approach is the Private Smart Contract, which serves our concerns for privacy and reliability to a greater extent compared to that of the Public Smart Contracts.

Private Smart Contracts

Private smart contracts are different when compared to public ones because the data handled by smart contracts is much more complex. Private smart contracts are able to work with documents and data held outside of the blockchain, which is not achievable on public blockchain systems. There are pools of data on a public network that are either trustworthy or have the ability to store extremely restricted data items instantly on the blockchain.[21] In all circumstances, there are significant restrictions on personal usage. And this is when the role of private smart contracts comes into the spotlight. When engaging with private smart contracts, transactions that activate smart contracts should be encrypted since only authorized personnel may decode and operate the contract. Thus, private smart contracts are proven to be more efficient, since they can handle contracts held by the network without compromising the privacy and reliability.

3.2.12 On Chain and Off Chain

Organizations and different institutions have adopted a way of managing data in blockchain systems by making use of on-chain or off-chain techniques for data storage over the past few years.

On Chain

When conducted on the public ledger, on-chain transactions are legitimate. They include a large number of people validating transactions, and all of the validation signatures must match exactly for the transaction to be regarded as genuine. While

each transaction's specifics are broadcast on the publicly accessible blockchain for verification, as a result, they cannot be manipulated or tampered with, it may take even longer than off-chain transactions. Furthermore, there is a strong possibility that transaction costs will be high, causing members to adopt the off-chain arrangement.

Off Chain

In contrast to that, off-chain transactions are not made available to the general public. Off-chain systems for storage imply that the data will not be visible to the public, much less the corporation itself. It is very obvious that any institution would not reveal its data within a publicly available database or directory. When these notions are applied to a traditional cloud system, it's quite similar to the difference between a public and private cloud.[22] "Values that are outside the blockchain and may be completed via a variety of techniques" are the focus of off-chain transactions. The transfer must be agreed upon by both parties, and then the transaction must be approved by a third party. Off-chain transactions are rapid and instant, with none of the additional costs associated with transactions through on-chain mechanisms. There are some key reasons for implementing an off-chain based storage mechanism that should be considered when designing a blockchain system over an on-chain. Off-chain storage is often used to provide a cache for the current values of the state from the on-chain data, as well as to back up directly for enhanced analytical help. Another significant feature of the off-chain system is its ability to store any form of real-time critical data. This difficulty does not occur with the data management mechanisms adopted for off-chain data, whereas on-chain data is non-negotiable in terms of updating manually and requires a set of validations. Overall, the key advantage of Off-chain transactions are:

- More private, since only visible to the members within the organization and not publicly accessible.
- Transactions are cost effective; in most cases it is free of cost.
- Faster, as it does not require validation for updating the information from all the members within the system.

In our suggested design, we have implemented hashed-based content-addressable storage to keep data off-chain. When a huge quantity of data connected to a smart contract is kept on-chain, it is extremely costly. Only the hash value is saved in the hashed based content addressable off-chain storage inside the smart contract. The hash value may be retrieved from on-chain storage using the smart contract, and the primary data can be retrieved from off-chain storage using this hash value. By calculating the hashed value of the data they've acquired and comparing it to the hashed value stored in the smart contract, they can verify its legitimacy. because any update to the records might alter their scope and invalidate their references or hash value right away. The storage costs of a utility may be drastically reduced in this manner, and data that could not previously be kept on-chain can now be referenced without establishing trust by adopting an off-chain architecture.

3.2.13 Mining

A block chain is identical to a computer server. Mining is a method of verifying new transactions. Different block chain executions use different approval processes. All excavators involved in mining are given a numerical problem to solve before new block-chain exchanges are added to the block. This is a difficult numerical problem that must be solved since it is based on the hash algorithm. There are no other options for dealing with this problem; one must examine every possible solution to ensure that it is correct. Finding the arrangement does not require intelligence; nevertheless, it does require speed. The numerical arrangement is known as Proof of Work (PoW) . The proof-of-work is that the excavator has put in the effort and resources required to get the desired result. Block-chain mining, as previously said, requires a large number of assets. For giving their time and assets, the digger receives a mining reward.

How mining works

Mining is practically impossible to do on a conventional desktop computer, requiring the use of specialist equipment with faster computing speed. To set up a mining setup, we'll need an ASIC (application-specific integrated circuit) or a GPU (graphics processing unit). Individual mining and mining pools are the two types of mining.

Individual Mining

Individuals must first register as miners before they can begin mining. Every individual member of the blockchain network is given a mathematical problem to solve as soon as a transaction is finished. The first person to solve it gets rewarded. When the solution is found, all the other miners in the blockchain system must confirm the decrypted value before it can be added to the blockchain. As a consequence, the transaction is completed and validated.

Mining Pool

A mining pool is a group of cryptocurrency miners that pool their computing resources in order to improve their chances of finding a block or mining bitcoin more effectively in general. A single miner might not have all the sufficient resources to mine the Block-chain. A mining pool is created in this situation by a group of miners. These miners combine their resources to speed up the mining of the block chain. Individual mining, like the MiningPool, gets the task and is paid after successfully completing it. The miners divide this award depending on how much resource they have contributed.

3.2.14 Cryptography

"Crypto" basically translates as "hidden" or "secret." "Cryptography" implies "secret writing," or the capacity to send messages that only the intended receiver can read. [23]Cryptography technology may provide pseudo- or true anonymity depending on the settings. Cryptography ensures the security of transactions and participants, as well as the freedom of operations from the decentralized authority and protection against cyber attacks. Our block chain system is designed in such

a way that no one knows the true data of someone without its key. For example, suppose someone has to communicate data within the network with someone else. This data will be transferred using the sender's public key, ensuring that it will not be attacked aggressively. Every person who has to process data or monitor that individual will be aware of their public key. In our system, the private key, on the other hand, is a key that only the client knows and may use for their own objectives. In depth concepts of both private and public keys are discussed below.

Public Key

A public key is being used to showcase an individual's information publicly so that everybody on the block-chain knows who that person is or what information he holds. Furthermore, the public key is utilized to exchange information among people on the block chain. This public key would be used to transmit and receive data and information. In our system, the public key is hashed using the person's email ID, their National Identification Number (NID), and the unique security number (SSN) that we will be providing. We adopted the SHA256 hash, which has been proven to be hard and almost impossible to crack. Making the hash highly unpredictable.

Private Key

This key has access to all of a person's information, including the public key in our system. The private key is being used to connect directly to that person's whole profile as well as to make modifications and transactional operations on their account. Any user in our hashing algorithm must log in using their private key, which they can only use to transact and update their account. The disclosure of a person's private key presents a significant risk to that person's information. By analyzing the public and private keys, anybody may figure out which key was used to hash the keys and acquire access to that person's account. We developed this private key using an email ID, the person's national identification number, security number, and a password issued by that person, keeping in mind the security measures by eliminating the loopholes within the system.

3.2.15 Revocation

A way of deleting or altering a credential is revocation. The ability for a provider corporation to revoke a credential is critical from the perspective of architecture security and therefore ensuring that identities are unique is an important aspect. Other credentials, such as a passport or a driving license, have an expiration date and some attributes. The fact is that in order to secure the tool's integrity and eliminate the risk of fraud, the credentials must be unchangeable. [24]After it is issued, no one (even the corporation) may be able to change the credential's records. As a result, a new credential is given every time the property changes, and the old one is marked as invalid. In effect, whenever the user wishes to demonstrate that the credentials used are still valid, the revocation register will allow them to find out without having to contact the issuing authority. The Revocation Registry policy need to have 4 properties which are given below:

- The provider must be able to revoke credentials.

- Privacy must be ensured during revocation testing.
- The revocation must be concise and fast.
- Verification and validation need to be made possible even without the approval of the provider corporation.

To conclude, with the help of an accumulator, our main objective is to present only legitimate information. Therefore, the owner's identity may now be established to validate his or her credential by using that information, and this is the basic principle of the revocation register that is being used in our blockchain network.

3.3 Store and Retrieve Files

We did adopt a different scheme as we could not fully store private files of the government on the blockchain. On the other hand, the amount of data that can be stored is limited by protocols or by the massive transaction fees that must be paid along with the access latency. We'll keep files on government systems already in place. The file will first be encrypted with the SHA256 hashing technique, followed by the generation of a secret key. The encrypted file will then be transferred to a central file server. The file will be saved with the structure of an ethereum block and a pointer to the SHA256 hash. We'll need to use the SHA256 algorithm to find the file.

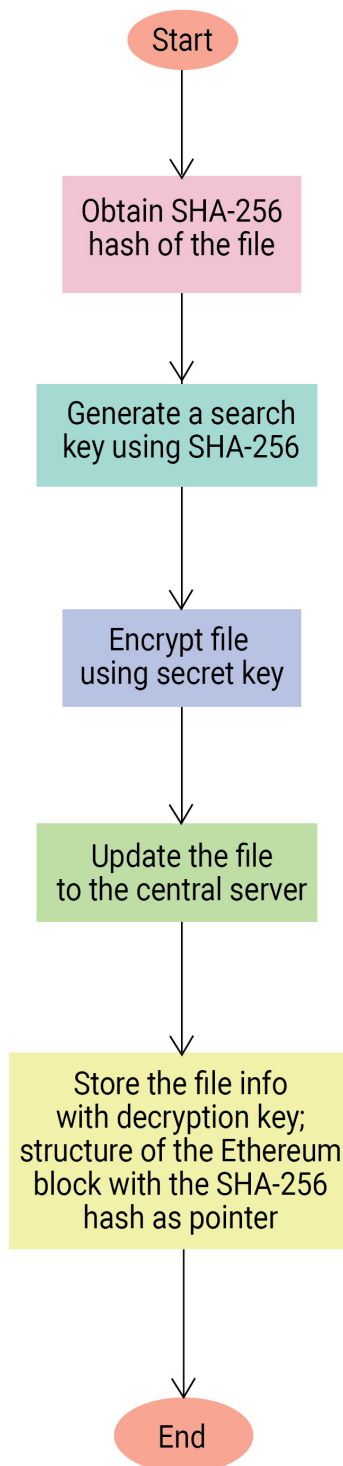


Figure 3.8: Storing file in the server

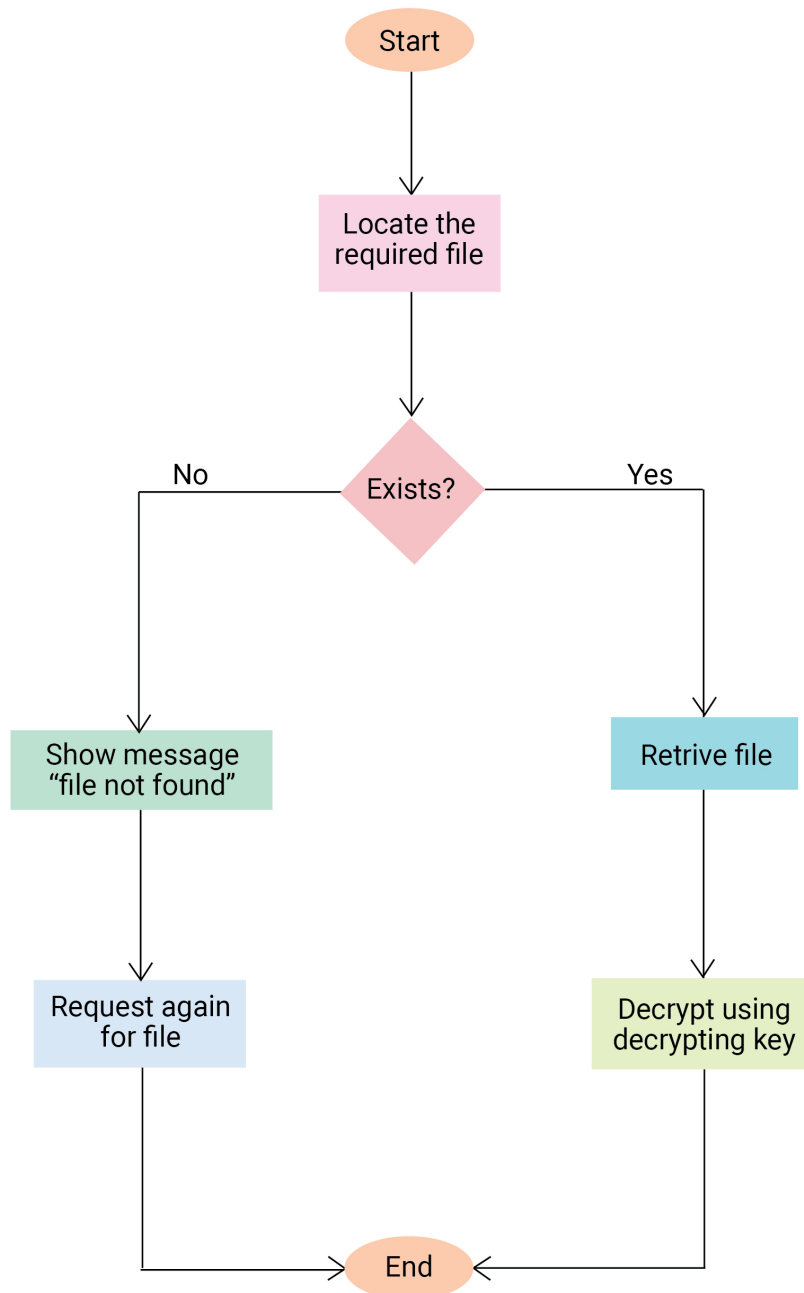


Figure 3.9: Retrieving file from the server

3.4 Reasons behind choosing DPoS over PoS.

Proof-of-Stake (PoS) consensus algorithms increase the efficiency of blockchain networks by eliminating the energy-intensive computational mining procedures required by Proof-of-Work protocols. PoS algorithms motivate users to authenticate network data and ensure security through a collateral staking process. However, Delegated

Proof of Stake (DPoS), a variant of the concept, takes the procedure to a whole new level by adding a voting and delegation mechanism to make the process more democratic. Users in the DPoS network can vote for the delegates to authenticate the upcoming block. Witnesses and block producers are two terms for delegates. By staking your tokens in a staking pool and tying them to a specific delegate, you can vote on delegates using DPoS. You stake your tokens in a staking pool using a staking service provider instead of physically moving them to another wallet. Hence, the DPoS framework is considered to be a more transparent and effective alternative to PoS.

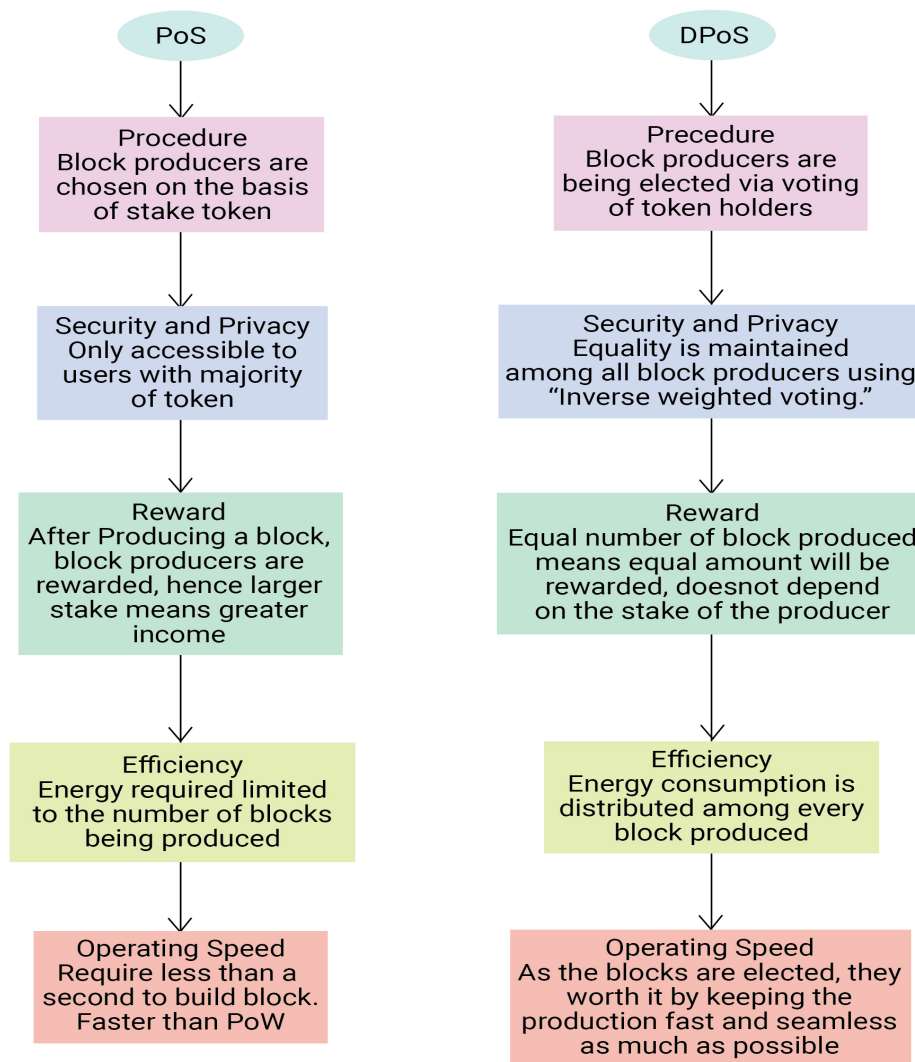


Figure 3.10: Working process of PoS and DPoS

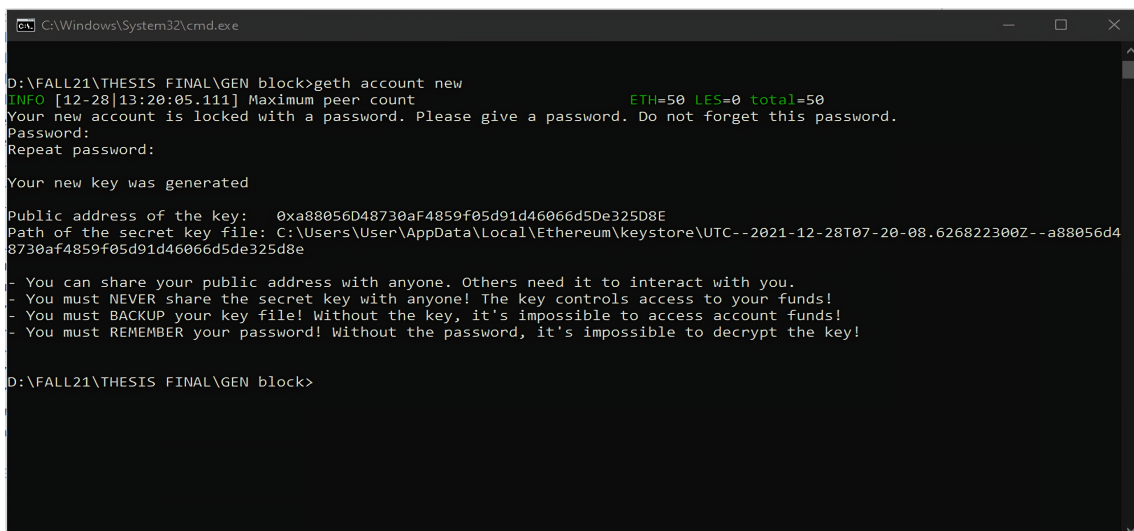
Chapter 4

Implementation and Analysis

In this paper, we worked with GETH and Remix IDE. Geth (Go Ethereum) [25] is a command line interface for running Ethereum nodes written in the Go programming language, and Remix IDE is an open source web and desktop application. It promotes a quick development cycle and includes a large number of plugins with user-friendly interfaces. Remix is used throughout the contract development process, as well as a playground for learning and teaching Ethereum [26]. We used GETH to create our own private network to deploy the smart contracts written with the Remix IDE.

4.1 Configuration

Before we can deploy the smart contracts, the system needs to be prepared. First, a network must be created to deploy the contracts. In our research, we are using a permissioned blockchain, so our network is private.[27] At first, we need to initialize Geth and create an account. When we create an account in Geth, we get a public address which is used to deploy and receive contracts. We will use our public address to create our genesis block.



```
C:\Windows\System32\cmd.exe
D:\FALL21\THESIS FINAL\GEN block>geth account new
INFO [12-28|13:20:05.111] Maximum peer count          ETH=50 LES=0 total=50
Your new account is locked with a password. Please give a password. Do not forget this password.
Password:
Repeat password:

Your new key was generated

Public address of the key: 0xa88056d48730af4859f05d91d46066d5de325d8e
Path of the secret key file: C:\Users\User\AppData\Local\Ethereum\keystore\UTC--2021-12-28T07-20-08.626822300Z--a88056d48730af4859f05d91d46066d5de325d8e

- You can share your public address with anyone. Others need it to interact with you.
- You must NEVER share the secret key with anyone! The key controls access to your funds!
- You must BACKUP your key file! Without the key, it's impossible to access account funds!
- You must REMEMBER your password! Without the password, it's impossible to decrypt the key!

D:\FALL21\THESIS FINAL\GEN block>
```

Figure 4.1: Account Creation

After creating an account, we have created the genesis block. The code for the

genesis block is written in JavaScript. We have configured our genesis block to our needs. We are using a developer test network to deploy our contracts. We used chain id 15, which is the Diode Pre-net [28]. The configuration for our genesis block includes specifying the gas limit, chain ID, and mining difficulty. "Gas is the unit of measurement for the amount of computational effort required to carry out specific operations on the Ethereum network. Because each Ethereum transaction necessitates the use of computational resources, each transaction necessitates a fee. The term "gas" [29] refers to the fee required to successfully complete an Ethereum transaction. The chain ID is a property of the chain that the node manages. It is used to protect transactions from being replayed. Setting the chain ID has the effect of changing one of the transaction's parameters, specifically the V parameter. $(2 * \text{ChainID} + 35/36)$ is the value for the v parameter. This means that all transactions on the Ethereum main net, which has a chain ID of 15, have a value of 65 or 36 [30]. The mining difficulty is a measure of how difficult it is to mine a Bitcoin block, or, in more technical terms, to find a hash that is less than a certain value. A high difficulty means that mining the same number of blocks will require more computational power, making the network more secure against attacks. In our test scenario, we have set the difficulty to 1 and set the gas limit to 8000000.

config <i>//configuration of the genesis block</i>
chainID: <i>//value of chainID</i>
homesteadBlock: <i>//set the value</i>
eip150Block: <i>//set the value of eip150 block</i>
eip155Block: <i>//set the value of eip155 block</i>
eip158Block: <i>//set the value of eip158 block</i>
byzantiumBlock: <i>//set the value</i>
petersburgBlock: <i>//set the value</i>
clique: {
period: <i>//set the period value</i>
epoch: <i>//set the epoch value</i>
}
}
difficulty: <i>//the difficulty value</i>
gaslimit: <i>//gaslimit</i>
extradata
alloc: {
balance: <i>//set balance</i>
balance: <i>//set balance</i>
}

Figure 4.2: Genesis block pseudo code

```

C:\Windows\System32\cmd.exe
Your new key was generated
Public address of the key: 0xc29436C3E8ff33251F6c0a09ea10757de3649292
Path of the secret key file: data\keystore\UTC--2021-12-28T07-21-36.981400500Z--c29436c3e8ff33251f6c0a09ea10757de3649292

- You can share your public address with anyone. Others need it to interact with you.
- You must NEVER share the secret key with anyone! The key controls access to your funds!
- You must BACKUP your key file! Without the key, it's impossible to access account funds!
- You must REMEMBER your password! Without the password, it's impossible to decrypt the key!

D:\FALL21\THEESIS FINAL\GEN block>
D:\FALL21\THEESIS FINAL\GEN block>geth init --datadir data genesis.json
INFO [12-28|13:21:59.208] Maximum peer count          ETH=50 LFS=0 total=50
INFO [12-28|13:21:59.212] Set global gas cap          cap=50,000,000
INFO [12-28|13:21:59.214] Allocated cache and file handles database="D:\FALL21\THEESIS FINAL\GEN block\data\geth\chaindata" cache=16.00MiB handles=16
INFO [12-28|13:21:59.465] Writing custom genesis block
INFO [12-28|13:21:59.467] Persisted trie from memory database nodes=3 size=397.00B time=0s gcnodes=0 gcsiz=0.00B gctime=0s livenodes=1 livesize=0.00B
INFO [12-28|13:21:59.471] Successfully wrote genesis state database=chaindata hash=8e1f4a..11c5a5
INFO [12-28|13:21:59.474] Allocated cache and file handles database="D:\FALL21\THEESIS FINAL\GEN block\data\geth\lightchaindata" cache=16.00MiB handles=16
INFO [12-28|13:21:59.765] Writing custom genesis block
INFO [12-28|13:21:59.767] Persisted trie from memory database nodes=3 size=397.00B time="500.2µs" gcnodes=0 gcsiz=0.00B gctime=0s livenodes=1 livesize=0.00B
INFO [12-28|13:21:59.771] Successfully wrote genesis state database=lightchaindata hash=8e1f4a..11c5a5
D:\FALL21\THEESIS FINAL\GEN block>

```

Figure 4.3: Creating the genesis block

Next, we have to specify the IP address of our network. For our test case, we have used a typical residential IP address and set the network ID to 15. Which will use Diode prenet credentials to validate and mine our blocks. As the mining difficulty is set to 1, it will take less computational power to validate the blocks.

```

C:\Windows\System32\cmd.exe - geth --datadir data --networkid 15 --nat extip:103.198.138.131
Microsoft Windows [Version 10.0.19044.1415]
(c) Microsoft Corporation. All rights reserved.

D:\FALL21\THEESIS FINAL\GEN block>geth --datadir data --networkid 15 --nat extip:103.198.138.131
INFO [12-28|13:28:03.553] Maximum peer count          ETH=50 LFS=0 total=50
INFO [12-28|13:28:03.556] Set global gas cap          cap=50,000,000
INFO [12-28|13:28:03.558] Allocated trie memory caches clean=154.00MiB dirty=256.00MiB
INFO [12-28|13:28:03.560] Allocated cache and file handles database="D:\FALL21\THEESIS FINAL\GEN block\data\geth\chaindata" cache=512.00MiB handles=8192
INFO [12-28|13:28:03.994] Opened ancient database      database="D:\FALL21\THEESIS FINAL\GEN block\data\geth\chaindata\ancient" readonly=false
INFO [12-28|13:28:03.998] Initialised chain configuration config="{\"ChainID\": 15 Homestead: 0 DAO: <nil> DAOSupport: false EIP150: 0 EIP155: 0 EIP158: 0 Byzantium: 0, Berlin: <nil>, London: <nil>, Arrow Glacier: <nil>, MergeFork: <nil>, Engine: clique}"
INFO [12-28|13:28:04.006] Initialising Ethereum protocol network=15 dbversion=8
INFO [12-28|13:28:04.010] Loaded most recent local header number=0 hash=8e1f4a..11c5a5 td=1 age=52y8mo4w
INFO [12-28|13:28:04.013] Loaded most recent local full block number=0 hash=8e1f4a..11c5a5 td=1 age=52y8mo4w
INFO [12-28|13:28:04.015] Loaded most recent local fast block number=0 hash=8e1f4a..11c5a5 td=1 age=52y8mo4w
INFO [12-28|13:28:04.018] Loaded local transaction journal transactions=0 dropped=0
INFO [12-28|13:28:04.019] Regenerated local transaction journal transactions=0 accounts=0
INFO [12-28|13:28:04.024] Gasprice oracle is ignoring threshold set threshold=2
INFO [12-28|13:28:04.026] Starting peer-to-peer node instance=Geth/v1.10.14-stable-11a3a350/windows-amd64/go1.17.5
INFO [12-28|13:28:04.461] Mapped network port proto=tcp extport=30303 intport=30303 interface=ExtIP(103.198.138.131)
INFO [12-28|13:28:04.461] Mapped network port proto=udp extport=30303 intport=30303 interface=ExtIP(103.198.138.131)
INFO [12-28|13:28:04.470] New local node record seq=1,640,676,242,954 id=6aa1a8e75f7afe7a6 ip=103.198.138.131 udp=30303 tcp=30303
INFO [12-28|13:28:04.474] Started P2P networking self=enode://07450e3175632cd2eccf96a39267ca686eaa5c594767ec01499795037bdc52ce9d25ad41fcdcf922f79fcd9686b
INFO [12-28|13:28:04.474] IPC endpoint opened url=\\.\pipe\geth.ipc

```

Figure 4.4: Creation of private blockchain network

After we create our private network and deploy our genesis block, it is time for us to validate the authenticity of the block by mining it. After mining the block, it will be added to the chain automatically[Etherbase automatically configured].

```
D:\FALL21\THEISIS FINAL\GEN block>geth --mine
INFO [12-30]20:41:15.798] Starting Geth on Ethereum mainnet...
INFO [12-30]20:41:15.800] Bumping default cache on mainnet
INFO [12-30]20:41:15.804] Maximum peer count
INFO [12-30]20:41:15.807] Set global gas cap
INFO [12-30]20:41:15.808] Allocated trie memory caches
INFO [12-30]20:41:15.812] Allocated cache and file handles
INFO [12-30]20:41:15.840] Opened ancient database
INFO [12-30]20:41:15.844] Writing default main-net genesis block
INFO [12-30]20:41:15.862] Persisted trie from memory database
INFO [12-30]20:41:15.866] Initialised chain configuration
INFO [12-30]20:41:15.878] Disk storage enabled for ethash caches
INFO [12-30]20:41:15.881] Disk storage enabled for ethash DAGs
INFO [12-30]20:41:15.884] Initialising Ethereum protocol
INFO [12-30]20:41:15.995] Loaded most recent local header
INFO [12-30]20:41:15.999] Loaded most recent local full block
INFO [12-30]20:41:16.002] Loaded most recent local fast block
WARN [12-30]20:41:16.005] Failed to load snapshot, regenerating
INFO [12-30]20:41:16.008] Rebuilding state snapshot
INFO [12-30]20:41:16.010] Resuming state snapshot generation
INFO [12-30]20:41:16.010] Loaded local transaction journal
INFO [12-30]20:41:16.016] Regenerated local transaction journal
INFO [12-30]20:41:16.020] Gasprice oracle is ignoring threshold set
WARN [12-30]20:41:16.023] Error reading unclean shutdown markers
INFO [12-30]20:41:16.026] Starting peer-to-peer node
INFO [12-30]20:41:16.062] Mapped network port
INFO [12-30]20:41:16.063] Generated state snapshot
INFO [12-30]20:41:16.066] Mapped network port
INFO [12-30]20:41:16.075] New local node record
INFO [12-30]20:41:16.079] Started P2P networking
INFO [12-30]20:41:16.081] IPC endpoint opened
INFO [12-30]20:41:16.087] Transaction pool price threshold updated
INFO [12-30]20:41:16.089] Updated mining threads
INFO [12-30]20:41:16.091] Transaction pool price threshold updated
INFO [12-30]20:41:16.093] Etherbase automatically configured
INFO [12-30]20:41:16.096] Commit new mining work
INFO [12-30]20:41:26.103] Looking for peers

provider=1024 updated=4096
ETH=50 LES=0 total=50
cap=50,000,000
clean=614.00MiB dirty=1024.00MiB
database=C:\Users\User\AppData\Local\Ethereum\geth\chaindata cache=2.00GiB handles=8192
database=C:\Users\User\AppData\Local\Ethereum\geth\chaindata\ancient readonly=false
config={ChainID: 1 Homestead: 1150000 DAO: 1920000 DAOsupport: true EIP150: 2463000 EIP155: 2675000 Byzantium: 4370000 Constantinople: 7280000 Petersburg: 7280000 Istanbul: 9060000 Muir Glacier: 9200000 Berlin: 12244000 London: 12965000 Arrow Glacier: 13773000 MergeFork: <nil>, Engine: ethash}
dir=C:\Users\User\AppData\Local\Ethereum\geth\ethash count=2
dir=C:\Users\User\AppData\Local\Ethereum\geth\ethash count=2
network=1 dbversion=<nil>
number=0 hash=d4e567...cbfa3 td=17,179,869,184 age=52y9m0d
number=0 hash=d4e567...cbfa3 td=17,179,869,184 age=52y9m0d
number=0 hash=d4e567...cbfa3 td=17,179,869,184 age=52y9m0d
err="missing or corrupted snapshot"
root=d7f097..0f0544 accounts=0 slots=0 storage=0.000 elapsed=0s
transactions=0 dropped=0
transaction=0 accounts=0
threshold=2
error="leveldb: not found"
instance=Geth/v1.10.14-stable-11a3a350/windows-amd64/go1.17.5
proto=udp extport=30303 intport=30303 interface=NAT-PMP(192.168.0.1)
accounts=8893 slots=0 storage=400.64KiB elapsed=53.045ms
proto=tcp extport=30303 intport=30303 interface=NAT-PMP(192.168.0.1)
seq=1,640,620,144,238 id=650b9a542cf6eb9 ip=103.198.138.131 udr=30303 tcr=30303
self=enode://2859cdec195f59efa8bc2f8a4ac16d6ed4f0f9b77254e5497266739541af039bc07f3337cce722ae0f9a115d47a3a39378dcfbaf9570fcaecce461e989448bb0@103.198.138.131:30303
url=\.\pipe\geth.ipc
price=1,000,000,000
threads=0
price=1,000,000,000
address=0x8c928e3f13e08b42560628094a672c2279c57ff
number=1 sealhash=a5e93e..242f72 uncles=0 txs=0 gas=0 fees=0 elapsed="500.3µs"
peercount=0 tried=11 stat=0
```

Figure 4.5: Mining to validate block

```
D:\FALL21\THEISIS FINAL\GEN block>geth --http --http.corsdomain https://remix.ethereum.org
INFO [12-30]20:46:05.003] Starting Geth on Ethereum mainnet...
INFO [12-30]20:46:05.005] Bumping default cache on mainnet
INFO [12-30]20:46:05.008] Maximum peer count
INFO [12-30]20:46:05.011] Set global gas cap
INFO [12-30]20:46:05.013] Allocated trie memory caches
INFO [12-30]20:46:05.015] Allocated cache and file handles
INFO [12-30]20:46:10.658] Opened ancient database
INFO [12-30]20:46:10.676] Initialised chain configuration
INFO [12-30]20:46:10.685] Disk storage enabled for ethash caches
INFO [12-30]20:46:10.690] Disk storage enabled for ethash DAGs
INFO [12-30]20:46:10.690] Initialising Ethereum protocol
INFO [12-30]20:46:10.697] Loaded most recent local header
INFO [12-30]20:46:10.700] Loaded most recent local full block
INFO [12-30]20:46:10.704] Loaded most recent local fast block
INFO [12-30]20:46:10.707] Loaded last fast-sync pivot marker
WARN [12-30]20:46:10.709] Snapshot maintenance disabled (syncing)
INFO [12-30]20:46:10.710] Upgrading chain index
INFO [12-30]20:46:10.710] Loaded local transaction journal
INFO [12-30]20:46:10.715] Regenerated local transaction journal
INFO [12-30]20:46:10.717] Gasprice oracle is ignoring threshold set
INFO [12-30]20:46:10.720] Starting peer-to-peer node
INFO [12-30]20:46:10.748] Mapped network port
INFO [12-30]20:46:10.759] New local node record
INFO [12-30]20:46:10.761] Mapped network port
INFO [12-30]20:46:10.763] Started P2P networking
INFO [12-30]20:46:10.763] IPC endpoint opened
INFO [12-30]20:46:10.773] HTTP server started
INFO [12-30]20:46:10.900] Upgrading chain index
INFO [12-30]20:46:20.700] Looking for peers
INFO [12-30]20:46:26.911] Upgrading chain index

provider=1024 updated=4096
ETH=50 LES=0 total=50
cap=50,000,000
clean=614.00MiB dirty=1024.00MiB
database=C:\Users\User\AppData\Local\Ethereum\geth\chaindata cache=2.00GiB handles=8192
database=C:\Users\User\AppData\Local\Ethereum\geth\chaindata\ancient readonly=false
config={ChainID: 1 Homestead: 1150000 DAO: 1920000 DAOsupport: true EIP150: 2463000 EIP155: 2675000 Byzantium: 4370000 Constantinople: 7280000 Petersburg: 7280000 Istanbul: 9060000 Muir Glacier: 9200000 Berlin: 12244000 London: 12965000 Arrow Glacier: 13773000 MergeFork: <nil>, Engine: ethash}
dir=C:\Users\User\AppData\Local\Ethereum\geth\ethash count=3
dir=C:\Users\User\AppData\Local\Ethereum\geth\ethash count=2
network=1 dbversion=8
number=420,927 hash=6f92a0..1d08bd td=2,137,603,220,920,331,184 age=6y2m0w
number=0 hash=d4e567...cbfa3 td=17,179,869,184 age=52y9m0d
number=420,927 hash=6f92a0..1d08bd td=2,137,603,220,920,331,184 age=6y2m0w
number=13,705,939
type=bloombits percentage=0
transactions=0 dropped=0
transactions=0 accounts=0
threshold=2
instance=Geth/v1.10.14-stable-11a3a350/windows-amd64/go1.17.5
proto=tcp extport=30303 intport=30303 interface=NAT-PMP(192.168.0.1)
seq=1,640,620,144,239 id=650b9a542cf6eb9 ip=103.198.138.131 udr=30303 tcr=30303
proto=udp extport=30303 intport=30303 interface=NAT-PMP(192.168.0.1)
self=enode://2859cdec195f59efa8bc2f8a4ac16d6ed4f0f9b77254e5497266739541af039bc07f3337cce722ae0f9a115d47a3a39378dcfbaf9570fcaecce461e989448bb0@103.198.138.131:30303
url=\.\pipe\geth.ipc
endpoint=127.0.0.1:8545 prefix= cors=https://remix.ethereum.org whois=localhost
type=bloombits percentage=40
peercount=0 (trie)=17 stat=0
type=bloombits percentage=79
```

Figure 4.6: Connecting remix ide to geth private network to deploy smart contract

After completing all the configuration, we can now finally deploy our contract. We need to deploy our code via the WEB3 [21] environment. We connected remix IDE to Geth and deployed the contracts on our private blockchain network.

DEPLOY & RUN TRANSACTIONS

ENVIRONMENT

Web3 Provider

ACCOUNT 

0x5B3...eddC4 (100 ether)  

GAS LIMIT

3000000

VALUE

0 Wei

CONTRACT

Types - 2ndcontract.sol

Deploy

☐ Publish to IPFS

OR

At Address Load contract from Address

Transactions recorded **0**

Deployed Contracts 

Figure 4.7: Contract Deployment using web3 injection

contract transfermoney
amounttotal; <i>// total amount of transactions</i>
sendername; <i>// name of the sender who takes participate in the transaction</i>
senderdob; <i>// date of birth of the sender</i>
nidno; <i>// NID number of the sender</i>
bankid; <i>// Bank identification number</i>
accountnumber; <i>//account number of that account where transactions are to be done</i>
constructor() public { <i>// creating constructors for amount, sender's name, sender's date of Birth, bank account number</i>
amounttotal , sendername, senderdob, nidno, bankid ; <i>// call function for each of these to get and set the values</i>
function getmoney() {
<i>// return the total amount of transaction</i>
}
function setmoney() {
<i>// set the total amount after each transaction</i>
}
function getnid() {
<i>// return the NID number</i>
}
function setnid() {
<i>// set the NID number</i>
}

function getname() {
<i>// return the string value of the sender's name</i>
}
function setname() {
<i>// set the sender's name for each transaction</i>
}
function getdob() {
<i>// return sender's date of birth set for the transaction</i>
}
function setdob() {
<i>// set the date of birth for the transaction</i>
}

Figure 4.8: Pseudo code for smart contract 1

contract Types
receivername; <i>// receiver's name</i>
receiverid; <i>// receiver's id</i>
receiverdob; <i>// date of birth of the receiver</i>
moneyreceived; <i>// the total amount of money received</i>
moneyspent; <i>// the total amount of money spent</i>
constructor () public { <i>//creating constructor for the receiver's name, receiver's id,</i>
<i>Receiver's date of birth, money received, money spent</i>
data [] <i>// array of data</i>
function dynamic_array() <i>//function call and return the value of data to the array</i>
function array_push() <i>//return the data of money spent</i>
function setmoney() <i>// set the value of spent money</i>
function getname() <i>// return the receiver's name</i>
function setname() <i>// set the receiver's name</i>
function getnid() <i>// return the value of receiver's nid</i>
function setnid() <i>// set the receiver's nid</i>

Figure 4.9: Pseudo code for smart contract 2

We have issued two contracts in our research work. One contracts ensure the safe and secure transaction of money. The second contract is for keeping track of the money that is being spent. Some of the functions that we used in the the smart contracts are listed below:

- Setaccount- The bank account number of the organization to send the money to. This function stores integers
- Getaccount- This function allows the user to view the account number of the receiver stored in the smart contract.
- Getbankid- A function that stores string value. Used to store the bank identification number of the receiver.
- Setbankid- Retrieve the bankID of the receiver.
- Setmoney- Stores integer value. Used to keep record of the amount of money being sent
- Getmoney- Read the amount of money stored in the contract.
- Setname-Sets the name of the sender in string value
- Getname- Read the name value.
- Setnid- NID(National Identity Card) number to ensure that all the transactions are by real people. NID number is stored as integer.
- Getnid- retrieve the NID number of the sender.

- pushvaluearray- Add a new value to the already created dynamic array
- Readvaluearray- Fetch the information stored in the array.

4.2 Result

After we successfully deploy our smart contract remix, the IDE will show the transaction hash, gas cost, current hash and log of the contract. In our test case we have successfully deployed both of our contracts.

```
creation of transfermoney pending...

[vm] from: 0x5B3...eddC4 to: transfermoney.(constructor) value: 0 wei data: 0x608...a0029 logs: 0 hash: 0x2a8...0d52b

status true Transaction mined and execution succeed
transaction hash 0x2a80626348a6e097213bae9a171725907b32909cbe37ed1fd7e350192370d52b
from 0x5B38Da6a701c568545dCfc803Fc8875f56beddC4
to transfermoney.(constructor)
gas 80000000 gas
transaction cost 751815 gas
execution cost 751815 gas
hash 0x2a80626348a6e097213bae9a171725907b32909cbe37ed1fd7e350192370d52b
input 0x608...a0029
decoded input {}
decoded output -
logs []
val 0 wei
```

Figure 4.10: Contract 1

```
[vm] from: 0x5B3...eddC4 to: test.(constructor) value: 0 wei data: 0x608...d0032 logs: 0 hash: 0x4bb...28321

status true Transaction mined and execution succeed
transaction hash 0x4bb754728015e106cdd432890c5471cd11d65270117890ab9da4a7b6b5028321
from 0x5B38Da6a701c568545dCfc803Fc8875f56beddC4
to test.(constructor)
gas 80000000 gas
transaction cost 112165 gas
execution cost 112165 gas
hash 0x4bb754728015e106cdd432890c5471cd11d65270117890ab9da4a7b6b5028321
input 0x608...d0032
decoded input {}
decoded output -
logs []
val 0 wei
```

Figure 4.11: Contract 2

The smart contracts enable transparency that conventional methods cannot deliver. In our test case, we can see all the details of the transactions that were made. As blockchain is immutable therefore, all the previous records of the transaction that



Figure 4.12: Successful transaction confirmation

occur in the chain can be viewed anytime. So this method of sending money will cut down the middle man and will allow proper cash flow, create transparency and lower the scope of corruption.

4.3 Cost Analysis

Using complex algorithms and computers requires a lot of power and energy. In the case of ethereum based blockchain the unit to measure the cost of running the blockchain operation is known as Gas cost. In our test case, we have used two different contracts for transactions and to keep a record of the money that is being spent. We need a large amount of gas to deploy and validate both of our smart contracts.



Figure 4.13: Comparison Between Contracts

As we can see in the figure above, contract 1, which is used for sending the money, has a cost of 751815 and the second contract, which is used to store the amount of money spent, has a gas cost of 112165. Contract 1 stores information such as the sender's name, NID number, date of birth, receiver's bank account number, bank ID number, and the amount of money to be sent. All of these functions require additional gas to complete their transactions and execution. Therefore, the gas cost of contract 1 is 6.7 times greater than the gas cost of contract 2 .

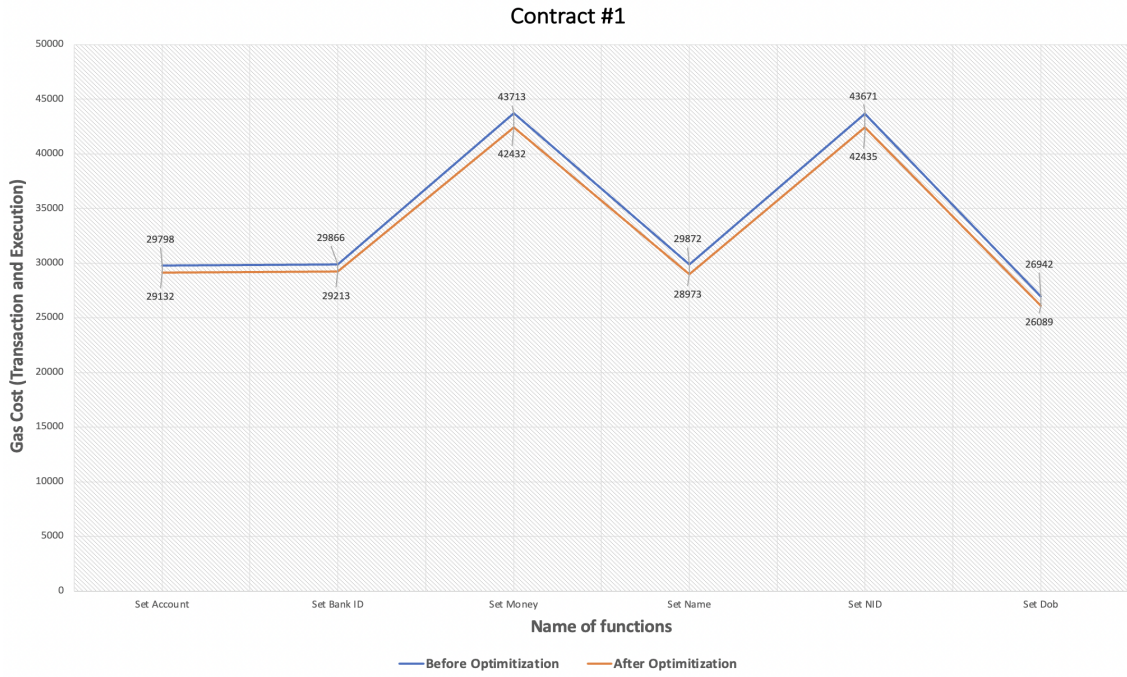


Figure 4.14: Graph of Contract 1

In order to lower the gas cost of our contract 1, we optimized the code a little bit. As we can see on the line chart above, the blue line represents the initial cost before any optimization and the orange line represents the gas cost after optimization. By looking at the graph, we can see the gap between the blue and the orange line is not that wide. This is due to the failings of the Solidity programming language. We can also see the same sort of behavior in the graph of contract 2 also.

To conclude, the system that we have created requires a little bit of effort to set up compared to the current conventional system. But it offers additional security and requires less human interaction.

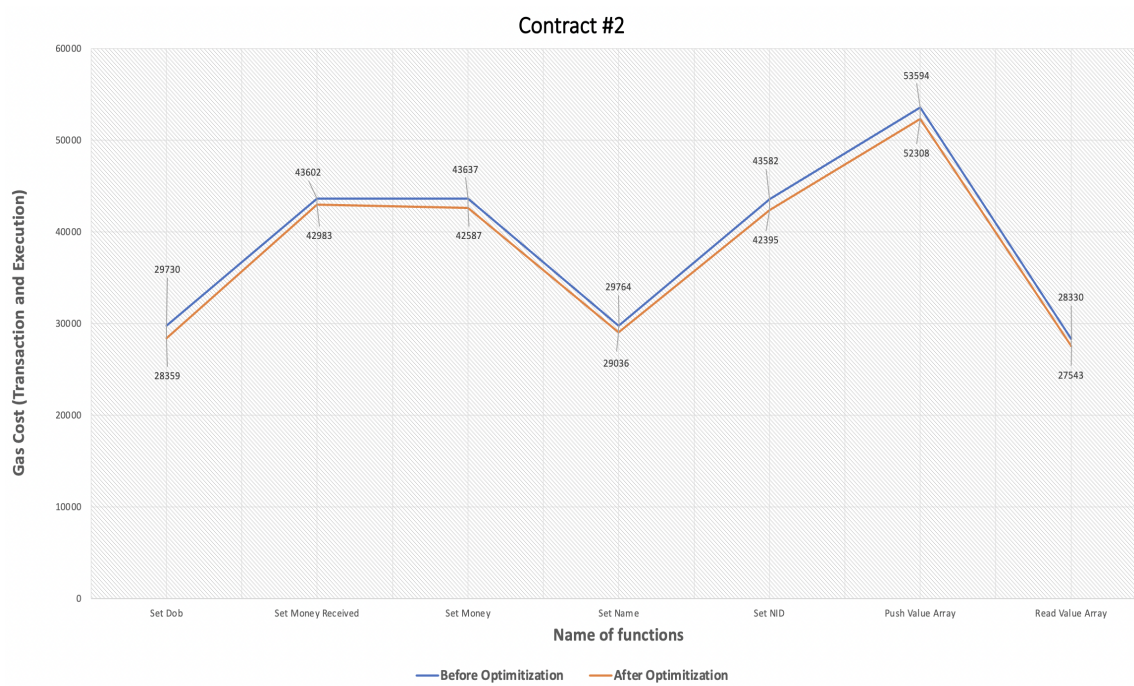


Figure 4.15: Graph of Contract 2

Chapter 5

Conclusion

Future Work and Conclusion

We started our research by thinking about building a system where public procurement would be distributed rightfully to fulfill its intended purpose. Then, we started working in the health sector. We tried building a blockchain-based security system where all the transactions of the health sectors would be monitored strictly to avoid any sort of mismanagement. We can apply the same system in different sectors. For example, if we want to supervise any other public procurement sector, like the construction sector, we can also do that using our same model. Suppose the government is allocating funds for the construction of a bridge. From tenders, getting the tender to billing of all the raw materials, until the construction is finished, the construction will be monitored. By this, we can assure proper management without any corruption.

Again, let's think about any sort of pension. As we know most of the needy people are not getting pension whereas the government is providing it regularly. So, we can also implement our proposed model in this regard. All the candidates of pension will be under the same ledger. When the money is given, we can check if the values of all the blocks are changing or not. If any sort of mismanagement occurs, we will be able to figure it out and sort it out. Like this, our proposed model can be used in all the public procurement sectors and thus can maintain proper balance and transparency.

We firmly believe that the newly presented blockchain technology has the potential to support anti-corruption in various different aspects. This technology promotes transparency, accountability, and citizen participation. In this research, our aim is to implement blockchain and establish e-procurements, which will in effect play an important role in eliminating corruption. Implementation of this technology also helps in efficiency when compared to the traditional way of working and adds a layer of transparency among the stakeholders and government authorities.

In our proposed e-procurement system for health sector management, we have adopted consensus algorithms, Delegated Proof of Stake (DPoS) over Proof of Work (PoW) to ensure a higher success rate in health sector allocation. In doing so, our goal was to design a more efficient and, at the same time, reliable system that focuses on the proper and rightful distribution of allocated money for the health sector.

To conclude, blockchain technologies can encourage greater citizen participation and awareness by elevating transparency, which will eventually contribute to the development of our country, Bangladesh. And, if that happens, it will give the government integrity in its anti-corruption efforts.

Bibliography

- [1] “Cargosmart and maritime industry operators commit to transforming the shipping industry, cargosmart,” 2021. DOI: <https://www.cargosmart.com/en/news/cargosmart-and-maritime-industry-operators-commit-to-transforming-the-shipping-industry.htm>;
- [2] “Smart contract,” 2021. DOI: <https://builtin.com/blockchain>.
- [3] “The worldwide blockchain supply chain industry is expected to reach 3 + Billionby2026–ResearchAndMarkets.com.Businesswire,” 2021. DOI: <https://www.businesswire.com/news/home/20210316005759/en/The-Worldwide-Blockchain-Supply-Chain-Industry-is-Expected-to-Reach-3-Billion-by-2026---ResearchAndMarkets.com..>
- [4] S. . I. Mostofa, “Modernization of land registry by adapting blockchain with proof-of-work (pow).,” Jan. 2019, pp. 1254–809. DOI: <http://dspace.bracu.ac.bd/xmlui/handle/10361/14063>.
- [5] M. . Shahriyer M.M. Monim, “Blockchain based land registry with delegated proof of stake (dpos) consensus in bangladesh.,” Aug. 2019, pp. 973–979. DOI: <http://dspace.bracu.ac.bd/xmlui/handle/10361/14049>.
- [6] N. Akaba T.I, “A framework for the adoption of blockchain-based e-procurement systems in the public sector: A case study of nigeria.,” Aug. 2020, pp. 973–979. DOI: https://www.researchgate.net/publication/338552921_A_Framework_for_the_Adoption_of_Blockchain-Based_e-Procurement_Systems_in_the_Public_Sector_A_Case_Study_of_Nigeria.
- [7] A. Anushree Tandon Amandeep Dhir, “Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda, computers in industry.,” Aug. 2020. DOI: https://reader.elsevier.com/reader/sd/pii/S0166361520305248?token=4DE7A544C9D297BA419E4B03D6684B10743B3BB69D219D30D6originRegion=eu-west-1&originCreation=20210924032158&fbclid=IwAR0k5uHh3IniHUb7UZ91XajRhHlgL6Uav_xd4031N5MoP4.
- [8] P. Aarvik, “Blockchain as an anti-corruption tool, u4 anti-corruption resource centre, chr. michelsen institute (u4 issue 2020:7).,” 2020. DOI: <https://www.u4.no/publications/are-blockchain-technologies-efficient-in-combatting-corruption>.
- [9] N. Kshetri, ““blockchain in developing countries,”.,” 2018. DOI: 10.1109/MITP.2018.021921645..
- [10] S. S. Dr Ahila, “International journal of future generation communication and networking vol. 13, no. 1, pp. 1136-1149.,” 2020. DOI: <https://serisc.org/journals/index.php/IJFGCN/article/view/8109>.

- [11] T. Akaba, "A framework for the adoption of a blockchain-based e-procurement system: A case study of nigeria.," 2019. DOI: [// www.researchgate.net / publication/333982004_A_FRAMEWORK_FOR_THE_ADOPTION_OF_A_BLOCKCHAIN-BASED_E-PROCUREMENT_SYSTEM_A_CASE_STUDY_OF_NIGERIA](https://www.researchgate.net/publication/333982004_A_FRAMEWORK_FOR_THE_ADOPTION_OF_A_BLOCKCHAIN-BASED_E-PROCUREMENT_SYSTEM_A_CASE_STUDY_OF_NIGERIA).
- [12] E. Luciano, "“blockchain potential contribution to reducing corruption vulnerabilities in the brazilian context,”," 2020. DOI: 10.1109/ICEDEG48599.2020.9096749..
- [13] M. Hölbl, "“a systematic review of the use of blockchain in healthcare. symmetry,”," 2018. DOI: <https://www.mdpi.com/2073-8994/10/10/470/htm>.
- [14] "Bangladeshi health sector corruption hits poor hardest," 2013. DOI: <https://reliefweb.int/report/bangladesh/bangladeshi-health-sector-corruption-hits-poor-hardest?gclid=CjwKCAjw7rWKBhAtEiwAJ3CWLFFT15O1P1Knh-ZEFowYE3Lhu873VDdhg0nWygZgn2k6F-9nDF1O3xoCwykQAvD.BwE>.
- [15] A.-Z. .M.S., "Healthcare crisis in bangladesh during the covid-19 pandemic.,"," 2020. DOI: <https://doi.org/10.4269/ajtmh.20-0826>. Retrieved from: <https://www.ajtmh.org/view/journals/tpmd/103/4/article-p1357.xml>.
- [16] "Corruption in the health sector:," 2021. DOI: <https://www.dhakatribune.com/bangladesh/corruption/2021/06/01/corruption-in-health-sector-acc-approves-3-cases-against-5>.
- [17] "Blockchain," 2021. DOI: https://www.researchgate.net/figure/Blockchain-data-structure_fig2_331639364.
- [18] "Cryptographic nonce," 2021. DOI: https://en.wikipedia.org/wiki/Cryptographic_nonce;
- [19] "Pow," 2021. DOI: [https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-stocks/proof-of-work/#:~:text=Proof%20of%20work%20\(PoW\)%20is,hash%20for%20the%20current%20block..](https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-stocks/proof-of-work/#:~:text=Proof%20of%20work%20(PoW)%20is,hash%20for%20the%20current%20block..)
- [20] "Distributed ledger," 2021. DOI: https://scholar.google.com/scholar?q=distributed+ledger+technology&hl=en&as_sdt=0&as_vis=1&oi=scholar.
- [21] "Smart contract," 2021. DOI: <https://www.ibm.com/topics/smart-contracts>.
- [22] "Off chain," 2021. DOI: https://ctl.mit.edu/sites/default/files/SCB_Security_9.09.pdf.
- [23] "Cryptography," 2021. DOI: https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&as_vis=1&q=cryptography+in+blockchain+technology&btnG=.
- [24] "Revocation," 2021. DOI: https://scholar.google.com/scholar?q=revocation+in+blockchain&hl=en&as_sdt=0&as_vis=1&oi=scholar.
- [25] "Geth in depth. [online] available at:," 2022. DOI: [https://medium.com/@kacharlabhargav21/geth-in-depth-d627e85b5a44#:~:text=Geth\(Go%20Ethereum\)%20is%20a%20command%20line%20interface%20for%20running,directly%20from%20Download%20Geth%20page](https://medium.com/@kacharlabhargav21/geth-in-depth-d627e85b5a44#:~:text=Geth(Go%20Ethereum)%20is%20a%20command%20line%20interface%20for%20running,directly%20from%20Download%20Geth%20page).
- [26] "Welcome to remix's documentation! — remix - ethereum ide 1 documentation.," 2022. DOI: <https://remix-ide.readthedocs.io/#:~:text=Remix%20IDE%20is%20an%20open,for%20learning%20and%20teaching%20Ethereum..>

- [27] “Solidity,” 2021. DOI: <https://docs.soliditylang.org/en/v0.8.11/>.
- [28] “Ethereum.org. 2022. gas and fees — ethereum.org.,” 2022. DOI: <https://ethereum.org/en/developers/docs/gas/>.
- [29] “Community, g., 2022. network and chain id - goquorum.,” 2022. DOI: <https://consensys.net/docs/goquorum/en/latest/concepts/network-and-chain-id/#:text=The%20chain%20ID%20is%20a,transaction%2C%20namely%20the%20V%20parameter..>
- [30] “En.wikipedia.org. 2022. web3 - wikipedia.,” 2022. DOI: <https://en.wikipedia.org/wiki/Web3>.