Towards Devising a Fund Management System Using Blockchain

by

Nibula Bente Rashid
18101110
Joyeeta Saha
18101059
Raonak Islam Prova
18101117
Nowshin Tasfia
18301166
Md. Nazrul Huda Shanto
18301071

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 and Engineering

Department of Computer Science and Engineering
Brac University
May, 2022

Declaration

Upon the completion of the thesis with necessary requirements, it is declared that,

1. The thesis paper is completed as our own work for the purpose of completion of our degree at BRAC University.

2. The thesis paper does not contain full, partial or intentional contents from any existing or previously completed works and therefore, it is free of any kind of direct imputation of any information from published sources. The materials which were investigated for the purpose of completing the thesis were cited with appropriate referencing.

3. The thesis is completely genuine and a new creation and therefore, it is only submitted to the authority of our supervisor only. It was never proposed, submitted or contacted to be used as a publishing material to any other stakeholder party.

Student's Full Name & Signature:

Nibula Bente Rashid

Nibula Bente Rashid
18101110

Joyeeta Saha

Joyeeta Saha
18101059

Raonak Islam Prova

Raonak Islam Prova
18101117

Nowshin Tasfia

Nowshin Tasfia
18301166

MD Nazrul Huda Shanto

Md. Nazrul Huda Shanto
18301071

Approval

The thesis titled "Towards Devising a Fund Management System Using Blockchain" submitted by

1. Nibula Bente Rashid (18101110)
2. Joyeeta Saha (18101059)
3. Raonak Islam Prova (18101117)
4. Nowshin Tasfia (18301166)
5. Md. Nazrul Huda Shanto (18301071)

Of Spring, 2022 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science and Engineering on May, 2022.

Examining Committee:

Supervisor:
(Member)

Jannatun Noor
Lecturer
Department of Computer Science and Engineering
Brac University

Thesis Coordinator:
(Member)

Md. Golam Rabiul Alam, PhD
Associate Professor
Department of Computer Science and Engineering
Brac University

Head of Department:
(Chair)

Sadia Hamid Kazi
Chairperson and Associate Professor
Department of Computer Science and Engineering
Brac University

Ethics Statement

The thesis is written in strict accordance with BRAC University's research ethics, rules, guidelines, and regulations. In order to conduct the research, we gathered data from a variety of sources. To gather information, we read published articles, papers, and other materials from many sites. The resources we've utilized here have been presented in our own words and are appropriately cited as references. Every source that assisted us in continuing our work is appreciated and acknowledged. Finally, we proclaim that even if any violations of BRAC university standards are discovered, the five authors of this article will be found liable.

Abstract

Trustworthiness has become a matter of concern in today's world. Loyalty among people has been abolished as time passes due to corruption. Greediness to achieve material gains is winning over human ethics. In these circumstances, even if someone has a good intention to help other people; they do not find the guts as there are no guarantees that under-served people will receive the goods. This distrust among donors is a great threat in the development of poor and marginalized people. Hence, in this paper, we are focusing on the issue that occurs when funds are provided to finance projects, programs or needs. Most of the cases, it is seen that, there are no proper records of how the total allocated fund has been utilized. A big amount of funding remains hidden because of some dishonest people in charge. Hence, figuring this issue and to bring transparency in financial sectors, we have introduced a system that will be able to keep track of all the transactions of all the funds. We have used blockchain technology in our proposed system. As only blockchain technology can provide a system of databases that is quite impossible to cheat, delete, hack or change. It is also popular for storing each transaction in a digital ledger that is distributed as well as duplicated to all over the blockchain network. Furthermore, in our proposed system, we have used ethereum as a platform to build up the network. High secured characteristics of blockchain will ensure the immutable, accountable and transparent nature of the system regaining the trust of the donors.

Keywords: Blockchain, Polygon, Cryptocurrency, Etherium, Smart contract, Metamask, Solidity, DAPPS, Public Key, Private Key, Remix Testing framework,Funding.

Dedication

We'd really like to devote our thesis to our parents, who have helped us get this far by every means possible. Then to Jannatun Noor miss, our esteemed supervisor. We would not have been able to perform our research without her guidance and supervision. Finally, condolences to all those who are experiencing and continue to suffer due to fund theft and fund distribution difficulties.

Acknowledgement

With the blessing of almighty Allah, we finally finished our thesis on the topic named Towards Devising a Fund Management System Using Blockchain. It was a great learning experience for all of us. We would like to express our heartfelt gratitude and thanks to our honorable supervisor Ms. Jannatun Noor Mukta ma'am for his delightful guidance. Through this research, we have learned so many important things which will be beneficial for our country in future. Also, our family and friends who assisted us in remaining calm during the pandemic. Finally, to our university as well as its authorities, where we were offered the chance to take a step ahead in achieving our objectives.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Overview

World economic system is driven on the basis of faithfulness and loyalty. Basically, people deposit their earned money in a bank and invest in different economic activities. By using the existing trading system people participate in different important manufacturing and marketing and become financially benefited. In this case, people choose reliable and profitable institutions and media for investment. But in developing countries like Bangladesh, corruption has become a major issue and people have lost their trust in the country's financial system. It obstructs the development of the country and creates economic contortion in different public sectors. In many cases, it is common that government officials are the ones who are directly or indirectly connected with corruption. But grievously, the government is incapable of taking proper steps against those antiheroes of the country. As in most of the scenarios, the actual evidence is hidden from the project owner. Hence, no one knows where and how the funds were utilized.

In order to eradicate corruption and bring transparency, technology can be used in an efficient way. An important task to exterminate corruption is to keep track of all the financial transactions of an undergoing project. Technology offers us to ensure proper transparency in transactions and inside views of how the allocated budget has been utilized. In this automated universe, blockchain is being considered as the most rising technology that will have great impact in every system which needs high security. Usage of this technology is increasing rapidly in multiple sectors. Such as identity management, supply chains, healthcare, data security, voting, telecommunication, manufacturing, cryptocurrencies, digital payment, and so on [12]. All of its applications are based on its beneficial characteristics like transparency, security, decentralized nature, non-corruptibility, immutability, consistency, and speed. A fund tracking system also requires this sort of facility that blockchain can provide us. So, introducing this technology in money tracking can bring a significant change in management and administration.

Therefore, in our proposed system, we have adopted blockchain technology by building up the system on the Ethereum platform. Ethereum is basically a public blockchain platform that provides maximum security, full transparency, and true decentralization which facilities are missing in private blockchain platforms. In

Ethereum, all people work independently in a community and no strict regulations from the central server. This decentralized system of ethereum has been run by a computer which is named as the Ethereum Virtual Machine (EVM) [13]. This ensures that the system can be executed fully without any kind of human interaction. So, using ethereum as a platform will broaden up the scope for our proposed system. Moreover, Ethereum's layer 2 scaling technique, polygon, provides a faster transaction speed along with a cost effective fund management system [14].

1.2 Motivation

The idea of blockchain technology is constantly evolving in this era of technological advancement. Before, blockchain was utilized only as a cryptocurrency, but it has extended into a multitude of sectors, including finance, healthcare, IoT, security-based systems, and so on. The immense facilities of blockchain architecture motivate us to work with technology and extend its real-world applications. However, it is worth noting the absence of knowledge on extra-budgetary monies, which are not fully disclosed in the executive's fiscal plan (IBP 2012b). Furthermore, there are regulatory organizations that carry out government tasks; unfortunately, not all of their funding is adequately represented in the budgetary (PEFA 2010). It's also worth noting that undocumented extra-budgetary spending accounts for 1-5 percent of overall spending (Ibid). This complete absence of honesty in budget distribution raises the possibility of corruption and mismanagement of off-budget expenses. Off-budget expenditures, since they are not part of the usual budget review process, are sometimes utilized as a vehicle for theft, favoritism, or corruption [15]. Moreover, Bangladesh is one of the countries with the highest rates of informal payments in regard with public services (GCR 2015-2016). When getting operational licenses such as an electricity connection, almost 60% of companies intend to make informal payments (ES 2017) [16]. For this, keeping track of the payment system has become a challenging issue for Bangladesh. The anti-corruption commission also fails to carry its responsibilities. These varied facts inspire us to research on anything effective that can facilitate the society with zero tolerance to corruption and thus provide a useful money transaction system for its beneficiaries.

1.3 Problem Statement

Nowadays, fund mismanagement has become a serious problem. If we think about an organization, a fund when it comes to the organization, other people of the organization may not know about this and it may bring misconception about the fund or some people may misuse this fund. Moreover, if anyone misuse the money or use it in any work, other people may not know about this which can bring trust issues as well. The present tracking system's key flaws include real-time monitoring, slowness, and operational errors.

According to the experts, Bangladesh has made great progress in a variety of social sectors. On the other hand, corruption, nepotism, malinvestment, and misdirected funds have delayed the economic growth and stopped the country from progressing. According to a study conducted by the Stockholm University, corruption in

Bangladesh diverts public resources to unproductive sectors, obstructs the government's ability to apply good policies, and reduces public trust in the government [17]. Moreover, In many sectors, we rely on many organizations or many companies. Even our country takes funds from different foreign organizations and then it divides into many subsectors. That's why it could be difficult to keep track of every transaction. So, a fund tracking management system is needed for the authority to decrease the rate of corruption. it would be much easier to rely on these if we exactly get the updates and of course it would be more preferable. But in the current system, we don't have any other options but to trust these organizations blindly. Because we don't have any system to track all the updates inside the organization.

1.3.1 Corruption in Government Funds

Governments are responsible for a large variety of activities. State government operations comprise a large number of transactions for different processes that must be carried out across the state. This comprises new projects, maintenance and repairs, public employee compensation, and agricultural schemes, among other things. Low-level corruption, which is sometimes difficult to trace and hinders state growth, is a big challenge for the top administration. Researchers claim that 1% corruption reduces 0.72% growth rate and 2% productivity of a country [18]. As corruption occurs when the construction companies build a project with low materials and achieve maximum profits from the allocated money. That weakens the quality and value of public essences.

In Bangladesh, corruption mainly takes place in the form of bribery and embezzlement. High officials working in a government or non-government organization are mainly responsible for corruption. They start a chain of corruption which ultimately reaches the root level. Whenever the government or any other organization undertakes a complex project they create funds. Corrupted people target these funds to achieve their self-gain. In most cases, the actual cost to complete the project differs from the initially estimated cost and time period is prolonged. Often, it is seen that there are no proper records of how the allocated fund has been utilized. A big amount of funding remains hidden. In these circumstances, corrupt officials get a chance and embezzle a handsome amount from the fund. These kinds of grand corruption are causing great damage to the socio-economic structure of the society and the nation. It is necessary to take proper steps urgently. It is a matter of sorrow, in developing countries like us officials and politicians who are bestowed with the duty to eradicate corruption are also beneficiaries of this heinous crime.

There are lots of different cases where the corruption is well-marked. For example, in a report of TIB, it is shown that there is more than 61% misuse of total allocated funds for the implementation of a forest project [19]. Information was collected from 62 offices, but lack of cooperation and mismanagement has been shown among the officers of the forest department. In another report, it is shown that about 14.36% to 76.92% corruption and misinformation occurs in the climate projects of our country [20]. There were 4 different projects and the total fund was Tk 1,102 crore where the amount of corruption is Tk 191 Crore according to the deputy manager, Newazul Moula. Also in infrastructure development projects, there is no such evidence of using Tk 27.20-41.73 crore [21]. In addition, each year, a significant amount of money vanishes from the rural development projects. Furthermore, Transparency International, a Berlin-based non-governmental organization, placed Bangladesh 13th out of 183 nations assessed in 2021 for how corrupt their public sectors are judged to be. According to an NGO survey on everyday corruption, 66 percent of the populace paid bribes to authorities in order to get basic government welfare services [22]. These issues need to be addressed and come out to a proper solution. Participation of common people and an automated management system can deliver a positive result in this case.

1.3.2 Corruption in Foreign Donations

Donation systems in non-profit organizations lack transparency because donors feel inadequate that funds would reach people who deserve them due to dishonesty in fund administration. According to a study conducted by the National Research University's higher school of economics, 57 percent of people give donations, although some of the allegations that have been publicly known in the more encompassing charitable sector in recent years have ended up causing financial support to fall by 11 percent since early 2000s [23].

Bangladesh receives about 63% of the foreign aid as loan and the rest of the aid (37%) is received as grants. In the economic year of 2010-11, Bangladesh has received $1721.771 millions in terms of commitment and disbursement. OPEC, ADB, and IDA are the leading aid donor organizations [24]. Though Bangladesh has achieved substantial steps to improve assistance efficiency, doubts persist about who are the main beneficiaries of US$1.5 billion foreign aid that country gets each year. "Whether foreign assistance helps the nation or not is a tricky subject," said Piash Karim, a sociology and economics professor at BRAC University. "People get a relatively little portion of the entire sum, while a crooked clique of NGOs and government leaders profit. There is no way to provide proof, but there have been claims of wrongdoing in foreign-aid projects," he continued. Therefore, an anonymous foreign assistance worker told IRIN that the underlying restrictions are a lack of adequate collaboration of bilateral aid, weak governance, and the bloated bureaucracy that accompanies help; A comprehensive overhaul of the assistance system is required, as is more openness and a firm commitment to addressing aid objectives. However, according to Muhammad from the Jahangirnagar University, fighting with corruption is the only solution to the issue. "We should assess the whole aiding process and determine what value we really get, since we have been receiving foreign help for quite some time," he added. "The whole assistance system's approach is flawed. It's time to learn how to use our own resources". If the problem is not solved on an urgent basis, our country will soon be deprived of financial help from foreign organizations [25].

1.4 Research Questions

In the previous section, as we discuss the present situation of financial sectors and how the overall system is corrupted and lacking of transparency, there remains no choice but introducing digital currency in finance, specially in funding services. To handle these matters, blockchain technology is certainly providing an efficient way. In later sections, we will discuss several reasons why we prioritized blockchain over any other technologies for our research work as well as answer questions that come forward through this research. The research questions are:

RQ 1. How can a blockchain-based system be able to handle transparency of a funding system?

RQ 2. How can the proposed model be verified to guarantee the accountability of funding procedures?

1.5 Research Objectives

The basic purpose of our research is to track all the updates of fund management of any organization. For this, we would be using blockchain. By using the theory of blockchain we would make a chain or a gateway where all the updates of a fund like from where it's received, who received it, where the money will be used, and who withdraws the money everything would be updated and all the members of an organization would be able to know that. So, there will be no chance to misuse the information or change any information from the blockchain as it will be secured. Here, we are using Ethereum which is a smart contract and digital certification platform that also offers users access to the Ether cryptocurrency. Ether, like Bitcoin, is independent of government currency systems similar to the dollar and the Euro. The acquisition of computer-generated keys determines who has the right to acquire Ether. Here, payments are cryptographically validated and executed by a network of computers with equality and also eliminating any need for a bank. For administration, a decentralized and synchronized accounting system known as blockchain is being used for the administration here. In this paper, we will be exploring more about this. The objectives of the research are given below:

- To gain a better understanding of the potentiality of blockchain technology.
- To explore the implementation of the blockchain technology in financial sectors.
- To build a decentralized solution for the fund management system.
- To introduce the most efficient blockchain-based money tracking platform in comparison to existing applications.
- To use smart contracts for autonomous payment systems.
- To gain the vast idea about crypto-currency and its market.
- Learning to overcome errors by using hashing algorithms.

1.6 Contribution

Our suggested research uses blockchain technology to keep track of fund management systems and assure the transparency of any financial statement. The main contributions of the thesis are given below:

Currency conversion: Our technology allows a wide range of organizations from different countries to conduct fund transfers. Because our system can accept dollars and convert them to ether. Furthermore, if funds are received in taka, they will be converted to dollars, which will then be transferred to ether. As a result, our technology allows for dollar transactions with foreign countries.

Corruption detection: Using blockchain theory, we have created a gateway where all adjustments of a fund, such as where it was received and who received it, as well as all transaction records, are updated in the system and visible to all members of the organization. As a result, there will be no opportunity of misusing information or altering or changing any information in the chain which helps the authorities in eliminating corruption from the money management system.

Fast and Cost Effective: In comparison to existing systems, we present the most effective and reliable blockchain-based fund tracking solution. In our system, we use layer 2 scaling mechanism of ethereum, polygon. As polygon uses different side chains alongside the main chain, it boosts the transactional speed and lowers gas expenses while maintaining system's decentralization as well as security.

1.7 Outline of the Thesis

In our thesis work, we maintain the outline where each chapter contains different sections of our work. In chapter 2, we discuss the background of our study where we talk about a general overview of funding and blockchain and how the funding mechanism can be implemented via blockchain technology. In chapter 3, we focus on the related works that are present in the current system without blockchain as well as all the research works related to funding with blockchain. After that in chapter 4, we talk about our research methodology that contains our proposed model and framework architecture of the model. Also, the sequential activity model and the layered architecture are also discussed in this section. Additionally, in chapter 4, we show all the necessary steps of our implementation like setup environment, features implementation, our obtained output, and the evaluation with other related works. Lastly, in chapter 6, we discuss the future works on which we are still working and a brief conclusion of our thesis work.

Chapter 2

Background Of Study

2.1 Introduction

In this chapter, we give an overview of the general funding system, blockchain technology, and how this technology is relatable and can be implemented in financial sectors specially in funding procedures. Since the beginning till today, funding systems have been recognized in numerous ways and are often identified by a lack of traceability and transparency, which scholarly attempts have been tried to remedy using several technologies, among those the most notable one is the blockchain technology.

2.2 Funding in General

A fund refers to a collection of money that is set aside focusing on a certain goal. The formation of a fund may have different types of objectives, like a government may set a budget to construct a bridge for improving the country's economy, an educational institution may form a fund to grant student scholarships, an insurance agency may set money to compromise its clients' claims and so on. The money allocated as a fund is often professionally maintained and invested. Individuals, corporations, and governments all manage funds to utilize money. Individuals may create emergency funds to cover unexpected needs or trust funds to save money for particular events. Financial institutions may invest in various kinds of funds with the purpose of profiting. Governments employ funding to cover certain public costs, such as revenue funds, project funds, etc. Different non-profit organizations also collect funds as a donation to serve public interests. So, there is no certain point of view of funding. It has different types and purposes for different entities [26]. For our research, we have focused on government funds along with donations for non-profit firms.

Governmental funds are the government's monetary resources that are utilized to support budgetary programs and expenditures. The government, like any other company, has created accounts for certain expenditure classifications. Fund management is a mechanism for tracking resources that have been restricted by donor organizations, individual citizens, or governing bodies. The major objective of fund management is accountability for expenditure rather than profits. There are different types of governmental funds that are generally used to monitor and balance all operations' cash, data, and obligations. Such as general funds, debt interest, prominent revenue, infrastructure investments, and long-term funds; these are the typical fund services administered by the government. Each year the government has to go through budgeting procedures, where it is determined in which sector how much funds need to be distributed. But there are many cases where these governing agencies get manipulated and entangled with corruption and use the funds for their personal interests that serve a large negative impact on the country's progress.

Besides governmental funds, the non-governmental organizations are also concerned about funds or donations. These are basically the organizations that are voluntary, private, and non-profitable. As their activity has expanded, non-profit organizations are really a significant social sector, as seen by many instances throughout the world. These organizations work in a variety of areas, including poverty prevention and alleviation, development of education, improving health care services (including disease prevention and mitigation), community and social progress (including care, assistance, and security of the older population, disabled people, kids, and youth), endorsement of culture, music, and art, and heritage, progression of amateur sport, strengthening human rights, counseling and reconciliation, environmental preservation and enhancement, and a variety of activity that has societal benefits. Many non-profit organizations assist contributors in a variety of ways, including offering financial and in-kind assistance; nevertheless, these organizations have lately suffered from a lack of funding for the above-mentioned initiatives as a consequence of donor distrust owing to corruption and mismanagement of funds.

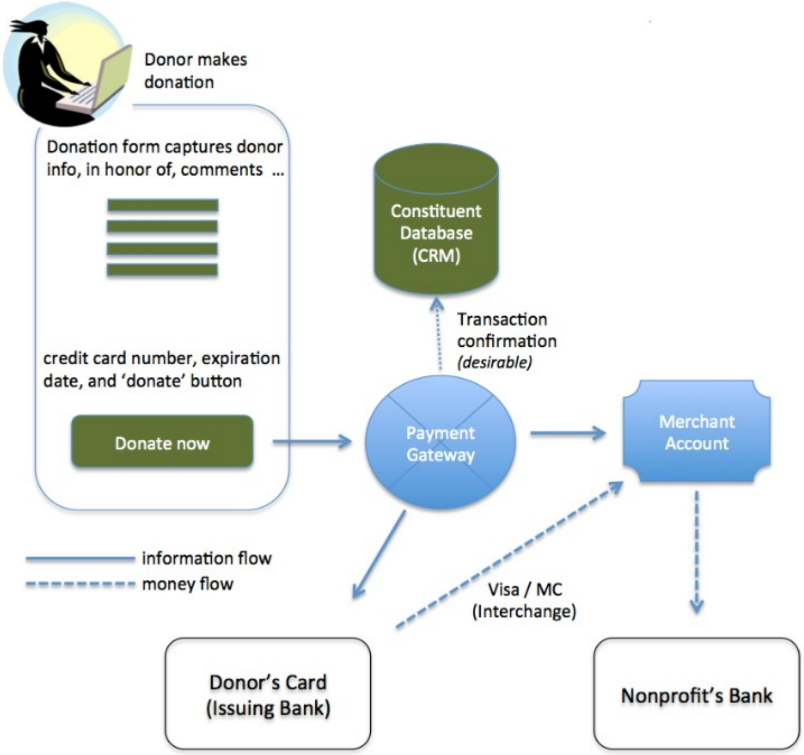

Donor makes donation
Donation form captures donor info, in honor of, comments ...
credit card number, expiration date, and 'donate' button
Donate now
Constituent Database (CRM)
Transaction confirmation (desirable)
Payment Gateway
Merchant Account
information flow
money flow
Visa / MC (Interchange)
Donor's Card (Issuing Bank)
Nonprofit's Bank

Figure 2.1: Funding system for non-profit organizations [1]

The online funding system for the non-profit organizations generally consists of three key elements that are a constituent database, a payment gateway, and a merchant account. The constituent database, also known as the Constituent Relationship Management Database (CRM), holds information of the contributors and contributions. The payment gateway is a virtualized credit gateway that handles information from the contribution button to the cardholder and bank account. Its duty also includes detecting fraud. Lastly, the merchant account refers to a customized account holder for organizations that accepts donations from donors' bank cards and transfers this into the organization's account [1].

2.3 Blockchain Technology

Blockchain technology represents a reliable, decentralized system where the ledger is copied across several identical repositories. Because disruption does not impact the whole system, blockchain-based services provide a higher reliability. Blockchain is derived on a high level of secured networks of tamper-resistant, high-efficiency nodes that adhere to predefined standards. This technology is becoming very popular for its different facilities. First it was outlined by Satoshi Nakamoto that the concept of digital currency is called the spine of bitcoin though that is not its only implementation. It is an encrypted ledger and a compilation of all recent transactions that have been validated. Once authenticated, the block becomes a permanent part of the chain.

It is built with 3 technologies –

1. Private Key Cryptography - Aside from the very advanced hashing algorithm, blockchain employs a mix of public and private keys. One key is used to encrypt, while another is used to decrypt. Encryption that is asymmetric.
2. P2P Network - Ensures total consistency. As verification is refused, no changes are allowed.
3. Blockchain Program - Based on the needs, it provides a wide range of protocols and security features. It is possible to implement it in any language.

In Figure 2.2, it is demonstrated the architecture of a widely specified blockchain system. All members in this peer-to-peer network must keep transaction records on their individual system simultaneously syncing with other peers through a consensus process. In reality, the consensus gets determined by the chain that is approved by the larger percent of the nodes.

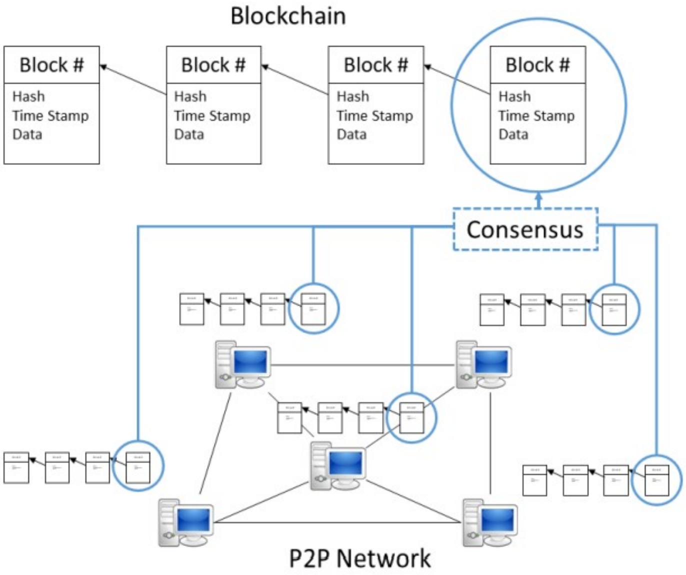


Figure 2.2: The Key elements of Blockchain system

2.3.1 Types of Blockchain

There are different types of blockchain and it is characterized by whether it is permissioned, permissionless, or both. Permissioned blockchains limit access to the blockchain network towards certain nodes as well as limit those nodes' privileges on that network. All user identities are known to each other. Permissionless blockchains enable any user to join the network pseudo-anonymously and do not limit the rights to enter nodes into the network. Permissionless blockchains are more trustworthy than permissioned blockchains since there are multiple nodes to confirm transactions and malicious people would find it impossible to collaborate on the network. However, owing to the high node density and large volume of transactions, processing times for all the transactions is much higher in permissionless blockchains. Whereas the permissioned blockchain works more proficiently. As connecting to the network is restricted, the blockchain has fewer nodes that results in a shorter process time per transaction [2]. The four types of blockchain are -

1. **Public Blockchain-** Public blockchains are based on permissionless networks that are entirely open and decentralized. All nodes in a public blockchain can equally access the network, by producing new blocks and verifying the old ones. Ethereum, Bitcoin, and Litecoin are some famous public blockchains [2]. In order to offer additional value to this blockchain industry, Ethereum is developed as a platform for the execution of decentralized smart contracts that has a currency of its own named Ether. The term 'smart contract' alludes to the notion that legal contracts may be certified and instantly performed. Ethereum developers may construct a system of smart contracts, that are basically executable programs inscribed into multiple blocks, via Solidity, that is a Turing-complete coding language. As a consequence of its eternal life, Ethereum extends blockchain implementation beyond the data domain to the

compute domain. In other words, no one will ever modify the program's logic once the developers have created and released their apps to the public. By establishing a smart contract, the public may have access to a set of trusted functionalities. These smart contracts will be performed in a decentralized manner by the distributed nodes when they are activated.

2. **Private Blockchain-** These are the permissioned blockchains, are often referred to as managed blockchain and administered by a particular entity. The central authority chooses who may be a node in a private blockchain. The central authority chooses whoever can enter into the blockchains. Additionally, each individual node may not be granted with same identical rights to deliver their duties. Because of this reason, the system is partially decentralized. This can be used to exchange virtual currencies from one business to another, but not suitable for security purposes as the system can easily be fooled if the majority of the nodes are fraudulent and untrustworthy [2].

3. **Consortium Blockchain-** According to some, consortium blockchains are a subclass of private blockchains. As a result, they are sometimes referred to as "partially private." It also has many of the same advantages of private blockchains, including high scalability, efficiency, and higher transaction privacy. The consortium blockchain, on the other hand, is a blockchain in which the consensus process is managed by a pre-selected collection of nodes rather than a single organization [2].

4. **Hybrid Blockchain-** Hybrid blockchains are made up of a permissioned blockchain that is managed by one or more parties and a permissionless blockchain that is not controlled by anybody but is agreed upon by most of the network's users. It can keep transactions private while still allowing them to be verified via an unchangeable ledger on permissionless blocks [2].

Therefore, blockchain technology can be classified into four generations: blockchain 1.0, 2.0, 3.0, and 4.0. The privileges of the blockchain technology in each generation contains transparency, security, decentralization, and immutability. Blockchain 1.0 was the first cryptocurrency that was extensively utilized for small money transfers, payment in foreign currency, and so on. Blockchain 2.0 is concerned with securities trading, smart contracts, banking tools, payment clearing, smart property, and a variety of other financial issues. Blockchain 3.0, on the other hand, concentrates on the blockchain based applications in healthcare, government, technology, research, art, and culture. Lastly, blockchain 4.0 relates to decentralization and enables IT systems to undertake business integration, focusing on business strategies using blockchain to facilitate supply chain management, workflow management, financial management system, and asset management.

There was a time when blockchain was only used for cryptocurrency and Bitcoin. However, with time blockchain is gaining popularity in a variety of sectors like identity management, supply chains, smart contract, healthcare, data security, voting, telecommunication, manufacturing, cryptocurrencies, digital payment, and so on. It is described as a worldwide database and a permanent ledger that enables transactions to be completely decentralized without the involvement of a third entity and is accessible to the public to read. However, once a transaction has been recorded,

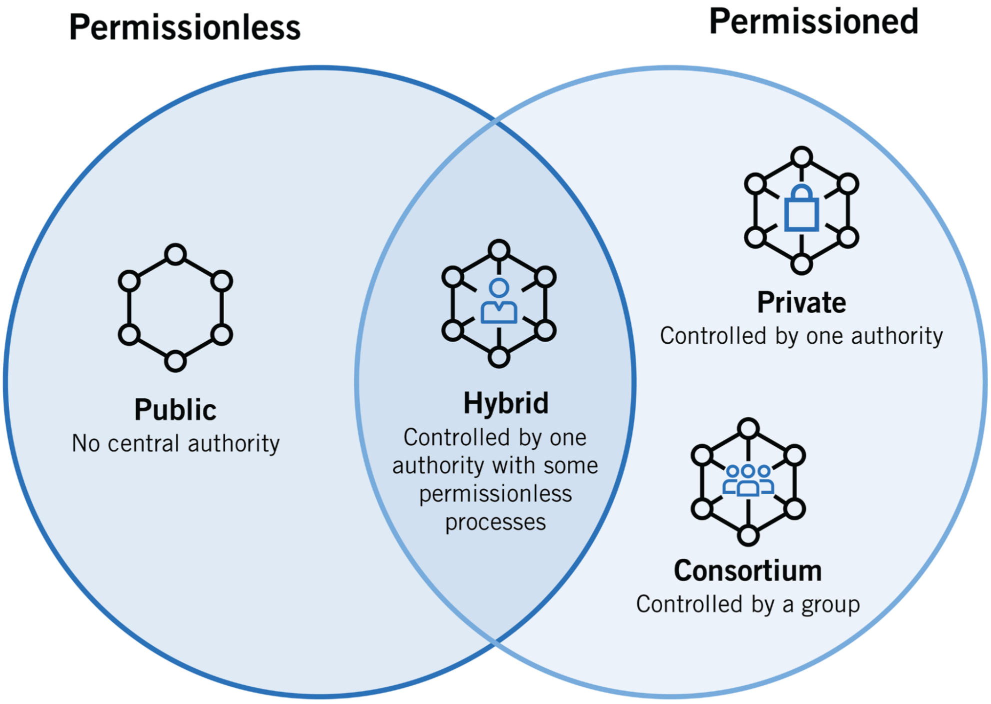


Figure 2.3: Types of Blockchain [2]

it cannot be amended. Its significance stems from the fact that it is anonymous, accurate, decentralized, and has a broad range of uses.

2.3.2 Blockchain Architecture

The essential components that encompass the fundamental structure of the blockchain technology are as follows:

Node: A node basically refers to a user or a computer inside the blockchain network that has a distinct copy of the entire database of the network. It is used by developers to create blockchain-based apps.

Transaction: A transaction is the tiniest building block of the blockchain system. In a transaction, the entire copy of distributed ledger remains stored. It also confirms the authenticity of the data that are stored in every blockchain node.

Block: A block in the blockchain network is defined as a data structure that holds a collection of transactions to distribute them among all the nodes. It comprises encrypted information from the previous blocks as well as new transaction data.

Chain: A chain is a set of blocks arranged in a particular sequence.

Miner: A miner is a node in the blockchain network that gathers and arranges transactions into blocks. When a transaction is made, it is deemed read by all nodes and if it is verified then the miners take those transactions from network's memory pool as well as begin generating those inside a block.

Consensus protocol: It is a collection of policies and procedures required to execute blockchain activities. It is designed to assure the stability of blockchain networks. Through the consensus mechanism, a contract commits to a specific transaction.

Any new transaction or data brings a new block in the blockchain system and gets validated by the majority of the nodes for the authenticity before signing into the main network. Figure 2.4 displays the layout of the blockchain structure and how it operates as a digital wallet.

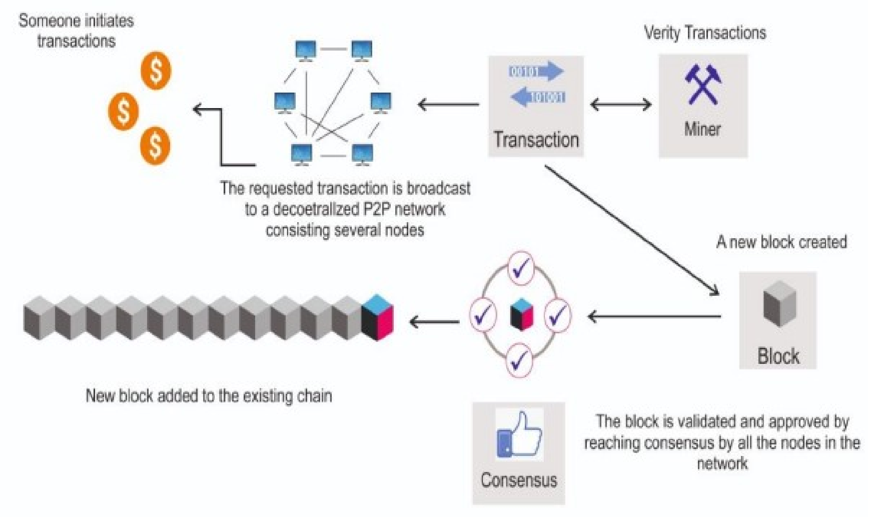

Someone initiates transactions
Verity Transactions
Transaction
Miner
The requested transaction is broadcast to a decoetralized P2P network consisting several nodes
A new block created
Block
New block added to the existing chain
Consensus
The block is validated and approved by reaching consensus by all the nodes in the network

Figure 2.4: Work mechanism of blockchain [3]

2.3.3 Blockchain Applications

Blockchain uses extend well beyond cryptocurrencies such as bitcoin, litecoin. Including its capacity of increasing openness and impartiality, while also utilizing organizations' money and time, this technology is influencing a broad range of fields, from contracting enforcement to running government more efficiently. There are lots of real-world applications of blockchain. For example:

Internet of Things (IoT): In an IoT scenario where Security is already an issue, it is evident that security must be prioritized even more. However, blockchain is considered as a solution to safeguard the Internet of Things. It has the potential to create the ideal system for monitoring the unique tales of thousands of smart gadgets that will start operating in the near future.

Financial Services: Financial facilities of blockchain technology are altering the traditional route of the current financial infrastructure. This highly functional area has several sections spanning from back-end trading and settlement to worldwide capital market architecture. Several financial organizations are aiming to build a private blockchain for their own by restricting to the complete decentralized nature of the distributed ledger.

Healthcare: The blockchain technology is utilized in healthcare sectors, to store as well as distribute patients' data amongst hospitals, diagnostic labs, pharmaceutical corporations, and physicians. In medical fields, blockchain applications may accurately detect serious as well as deadly errors. For this reason, it has the potency to boost the efficiency, security, and integrity of sharing of health information in the medicare system. This blockchain technology aids medical institutes in obtaining insight and delivering the evaluation of patient history.

Education: Blockchain regulates decentralized documentation in academic systems such as record student data, manage credentials, administration, learning activities, and so on. Blockchain provides students control over their academic identities by giving them control of their personal information. This makes it much simpler for alumni who are job looking, for example, to prove the veracity of the qualifications on their CV, and offers them full influence over what employers can access.

But, these are not the only fields blockchain works with. There are more blockchain applications in the real world that are shown in figure 2.5.

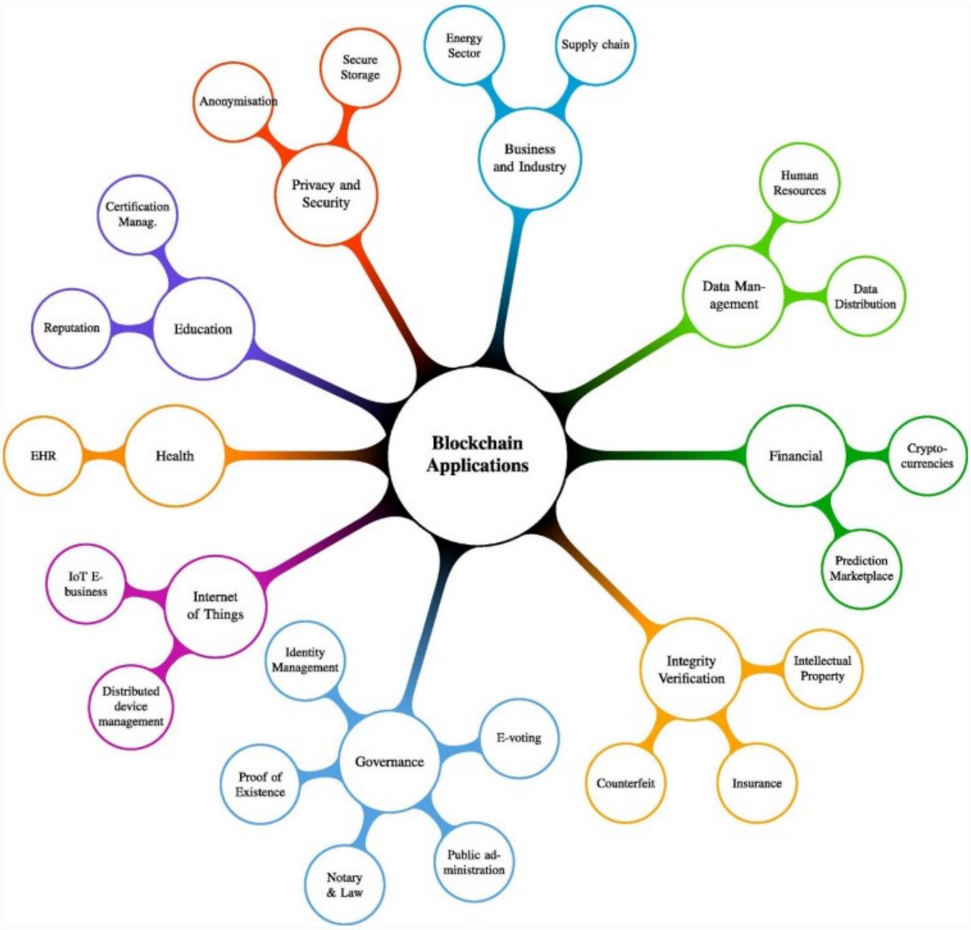


Figure 2.5: A mindmap representation of different blockchain applications [4]

2.4 Blockchain and Fund Collection

The achievement of the blockchain applications has not happened overnight. In fact, numerous visionaries with exciting and new ideas are required, as well as technical professionals with the necessary abilities to translate the concepts into reality. Here blockchain ecosystem concept has been recognized, since the usefulness of blockchain resides in its usage for the standardization of cross-enterprise activities. Blockchain ecosystems are defined as a collection of pieces designed to interact with one another and with the outside world to create a place with intended particular qualities. A blockchain ecosystem may alternatively be defined as the accepted governance framework for a certain use case. The system of governance defines acceptable participant conduct, funding, data ownership, exit and entry requirements, and rules for information exchange among participants. However, blockchain, just like every other modern technology has significant issues. Some of the major considerations in this scenario include controlling the selection of relevant information about the system and the identification of the writers of the pertinent material to the shared chains. All of these difficulties fall within the purview of growing blockchain ecosystem concepts, and appropriate planning for their maintenance assures the project's success.

The primary components of the fund collection ecosystem in blockchain are identification, privacy, monetary transactions, decentralized applications, wallets, exchanges, distributed ledgers, miners, distributed storage and the underlying infrastructure to construct the DApps. Because the charity collecting procedure includes monetary values, it needs high security and user data privacy. Meanwhile, one of the primary components of the blockchain ecosystem is secure identification and anonymity, which makes blockchain technology the perfect match for the charity collecting procedure.

The blockchain ecosystem comprises ICOs, wallets, and exchanges, which are essential parts of cryptocurrency transit and administration, while an unchangeable blockchain may be used to establish a safe money trail. On top of these fundamental qualities, blockchain offers infrastructure for the development of DApps that give a user interface to its clients, in this instance contributors and recipients. Furthermore, other blockchain ecosystem elements, such as distributed ledger and distributed storage, consider making blockchain appropriate for funds collection processes by giving organizations, beneficiaries, donors, and legal authorities more control over the information and promoting data transparency [5]. The blockchain ecosystem is shown in Figure 2.6 which includes all major characteristics.

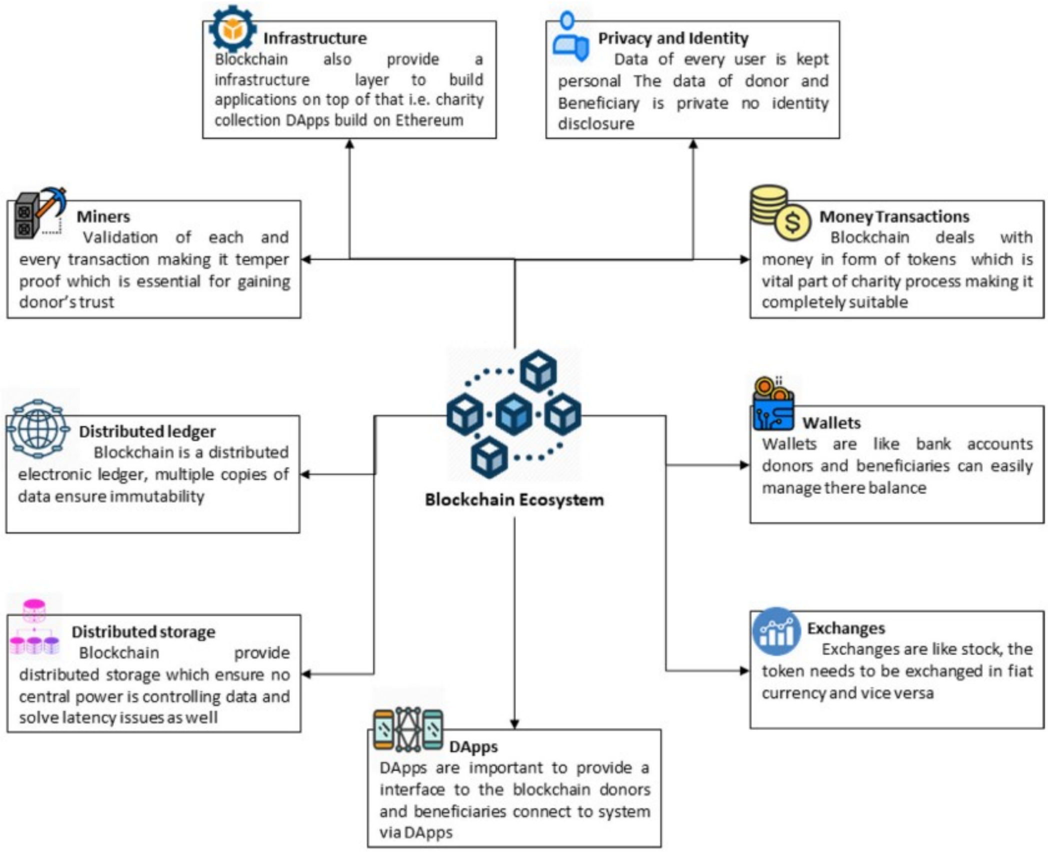

Infrastructure
Blockchain also provide a infrastructure layer to build applications on top of that i.e. charity collection DApps build on Ethereum
Privacy and Identity
Data of every user is kept personal The data of donor and Beneficiary is private no identity disclosure
Miners
Validation of each and every transaction making it temper proof which is essential for gaining donor's trust
Money Transactions
Blockchain deals with money in form of tokens which is vital part of charity process making it completely suitable
Distributed ledger
Blockchain is a distributed electronic ledger, multiple copies of data ensure immutability
Blockchain Ecosystem
Wallets
Wallets are like bank accounts donors and beneficiaries can easily manage there balance
Distributed storage
Blockchain provide distributed storage which ensure no central power is controlling data and solve latency issues as well
Exchanges
Exchanges are like stock, the token needs to be exchanged in fiat currency and vice versa
DApps
DApps are important to provide a interface to the blockchain donors and beneficiaries connect to system via DApps

Figure 2.6: Blockchain Ecosystem [5]

Different blockchain implementations with small changes in major technological sectors are continually developing to address various flaws in present frameworks. When selecting a blockchain technology, one may wish to have a sturdy implementation that is also prepared to be flexible when necessary. This may be determined by examining how often the network has “hard-forked” and how frequently derivative projects arise. It may also be necessary for the intended project to have an active developer community, which may be measured by the number of participants, code contributions, and branches. Any project may be subjected to a comparable comparison and analysis when selecting a suitable technology for execution. The usage of blockchain in funding has also been researched. The emphasis is on Blockchain technology application cases that increase the openness and dependability of information sharing procedures via distributed ledgers [6]. By utilizing the blockchain in funding, the fund provider is informed about the location through the blockchain tracking function and receives notice when it reaches the recipient. Once the transaction has been made, it is protected using smart contracts as well as proof of work, and the locked transaction cannot be modified in further. Whereas, the contributor transfers funds to the receiver without the involvement of any third party via smart contracts that include comprehensive data stored inside the blockchain network, shown in Figure 2.7.

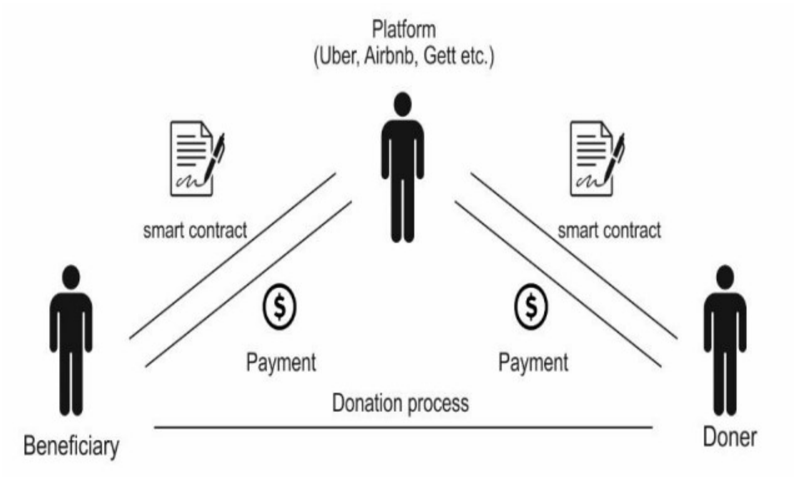


Figure 2.7: Online funding system using blockchain [6]

As a result of its excellent security qualities and decentralized design, blockchain technology is considered to be a particularly ideal technology for building and enhancing the charity systems.

The significance of this study is discovered through using blockchain technology in current funding procedures by utilizing its action based on the elimination of intermediary role, prevention of system manipulation, and digital validation of data. The study has also enlightened about how the overall funding system is corrupted and how the system can be converted to technology based approach rather than existing manual system. Where in current situation, the funding procedures are fully dependent on different institutions and organizations like central bank, government and NGOs for security purpose. Instead of relying on these, a blockchain based system itself can be enough for ensuring security, anti-counterfeiting measures, public safety, regulating money supply via using cryptocurrencies, encryption, and combinations of private and public keys. Blockchain is far more than a technological answer to the problem of double expenditure in digital currencies; it is shifting the balance of potential in markets, networks, all of the web's properties as well as the connection between the citizen and the state. In this analysis, based on foregoing, the significance about using this blockchain technology in fundraising systems by managing and tracking the financial contributions that reaches to the beneficiaries to preserve the confidentiality and privacy of the funding process, which makes a significant contribution to gain the trust and make the environment ideal for fundraising.

Chapter 3

Related Works

3.1 Introduction

In this part, the general funding system of different organizations and payment methods are analyzed and compared, then the payment methods using blockchain are also identified. Some challenges that organizations face using and without using blockchain technology is discussed as well as the work framework on which the study is focused is clarified in later part of this chapter.

3.2 Digital Fundraising Platform Without Blockchain

Today the world is getting digitalized in every aspect. Digitalization is the process of incorporation of digital technologies in social and business or monetary processes with a view to improving them. This ongoing process of digitalization has provided us huge potential benefits which opened the gateway for numerous possibilities in various fields. In modern times, financial companies and government and non-government organizations complete business transactions through the national and international banking system. International trading and payments are also done using the banking systems. Funds for high scale projects and various development work undertaken by the government or any other organizations are mostly transected using manual financial systems. Moreover, the government deposits foreign currencies and funds received for various ongoing processes in banks. Non-government organizations also deposit their funds and donations in these financial institutions.

Efficient settlement and payment systems are the mechanism through which funds are exchanged between financial institutions, corporations, or individuals and are regarded as a vital aspect in the effective operation of a state's overall financial system. In order to transfer the fund from donor to receiver, there are several payment services that transfer money in different currencies. Those are widely used for providing the fund securely nationally or internationally. Bangladesh Electronic Funds Transfer Network (BEFTN) is the first paperless digital inter-bank money transfer system, launched in February 2011 in Bangladesh. As a lean over checkbook clearing system, it supports both debit and credit transactions. Payroll, domestic and international remittances, welfare payments, bill payments, business dividends, security payments, corporate payments, federal tax payments, and individual payments, all types of credit transfer can be handled through this network. Similarly, it accepts debit transactions such as payments like utility bill, insurance premium, association, EMI, and so on [27].

In addition, there are many popular international payment methods that are widely used for donations and fundraising activities where the donation can be placed through the website of the service provider by payment gateway that facilitates the transactions among the fund providers and the beneficiaries using a variety of payment options. Some well-known payment mechanisms are given below-

Amazon: Amazon Payments imposes a fee of (2.9% + $0.30) per transaction for payments in excess of $10. The charge for payments below $10 is (5.0% + $0.05) each transaction, and 24hours is the maximum time it takes to process[11].

PayPal: It is the world's most popular payment organization, and for the money transfer, user must have a user account or credit card. The procedure takes 3-5 days and costs (0.30 + 2.9%) in every transaction[11].

Google Checkout: This service accepts payment using an account connected to the user's Google profile. Here, the transaction cost is $0.45 and a monthly service charge is $10.99. The whole transaction process takes almost 2-5 days[11].

Dwolla: This company can be assumed as a real competitor of PayPal which offers no transaction charges below $10. It costs $0.25 in each transaction, for transferring money over $10 and requires 3-4 days to process[11].

Stripe: A fantastic choice for a web development company who desires to connect a payment system via projects utilizing Stripe's strong API. Stripe charges ($0.30 + 2.9%) in every transaction along with no monthly or setup costs, and the whole procedure requires 7-14 days[11].

All online payments impose a rate of tax on variable or fixed transactions, restrict amount of funds transmitted, and what distinguishes them is the involvement of a typical third-party for settlement, which is essential for securing online payment systems. To realize the achievement of the digital payment platform, it is essential to consider the approaches of the participants involved in donation procedures as well as the disclaimer of commitment to preserve the confidentiality of private transactions.

Here, a comparison between different online payment platforms are shown in table 3.1.

Platform	Exchange	Payment accepted	Fees Per Transactions	Maximum Transfer per Transaction	Duration (Days)
PayPal	Yes	PayPal credit card	2.9% + $0.30	Limitation of $10,000 but upto $60,000 may consider	3-5
Google Checkout	In process	Credit cards	2.9% + $0.30	No upper limit	2-5
Dwolla	No	Dwolla credit card	$.25	Limit upto $10,000 but receive upto $5,000	3-4
Stripe	Yes	Credit cards	2.9% + $0.30	No regular limitation	7-14
Autho-rize.net	In process	Leading credit cards	$0.10	$100	1

Table 3.1: Comparison between different funding platforms without blockchain[11]

3.3 Relevent Funding System Using Blockchain

As the number of donors have been decreasing rapidly because of lacking trust and confidence among the receiving organizations, an increase in public inspection, accountability, and openness in donation procedures is the demand of time. Hence, there is a need to employ blockchain technology as a revolutionary approach to improve trust between contributors and beneficiaries by increasing transparency on the contribution process.

A methodology for making charitable activity public and auditable via blockchain technology is provided in a scholarly study [5] by authors Farouk, Abid and Khan. This article offers their own virtual currency named CharityCoin (CC) and a blockchain-based funding platform that promises to create a transparent, safe, auditable, and effective system that completely covers the operation of charity fundraising with cryptocurrency. In their proposed framework, the primer users are eligible to connect directly to the blockchain application- DApp, which represents a platform for charity management for all the users having their own private profile along with the public address as well as wallet. The donor also gets the opportunity to administer their donations using their profile via blockchain tracking system whether their donations have properly reached the beneficiaries or not. The smart contract regulates the locked transactions. Once a transaction is made, it is secured via two smart contracts which give a higher level of security containing proof of work along with restrictions to get tampered. As, these smart contracts specify the regulations for the total amount of CC, the trading of CC, and the Initial Coin Offering (ICO) system as a whole, while adhering to ERC20 protocols. Furthermore, few additional smart contracts have also been developed to categorize donors based on their contribution and potentials inconvenience to search for appropriate donors as well as a revocation option for the donors if they are dissatisfied with any offensive manner of fundraising organization. In this scientific research, the contribution procedure is carried out either by giving charities to the organizations that maintain digital wallets or directly to the beneficiaries if they own a digital wallet.

In another research paper [6], the authors discuss the basic mechanism to track charitable donations focusing on the blockchain technology and they demonstrate it by generating transparency records for any sort of financial transactions as well as allowing the users to monitor where, when and to whom his allocated funds have appeared. They have used the Ethereum test network Called Ropsten for this project and the Web3.js library to communicate with the blockchain server. The smart contracts are maintained using solidity language. The server (REST API) is built on the node.js platform and the Express framework on javascript language. MySQL is used as the central storage purpose and Python to create the Telegram bots which process the simulation of fundraising. Figure 3.1 depicts the platform for the proposed system where the servlet data is recorded in a centralized repository which is outside of the blockchain but master data is recorded inside the blockchain. All the entries are stored in a decentralized ledger via smart contracts also received and transmitted via blockchain network and centrally controlled storage using the rest orders.

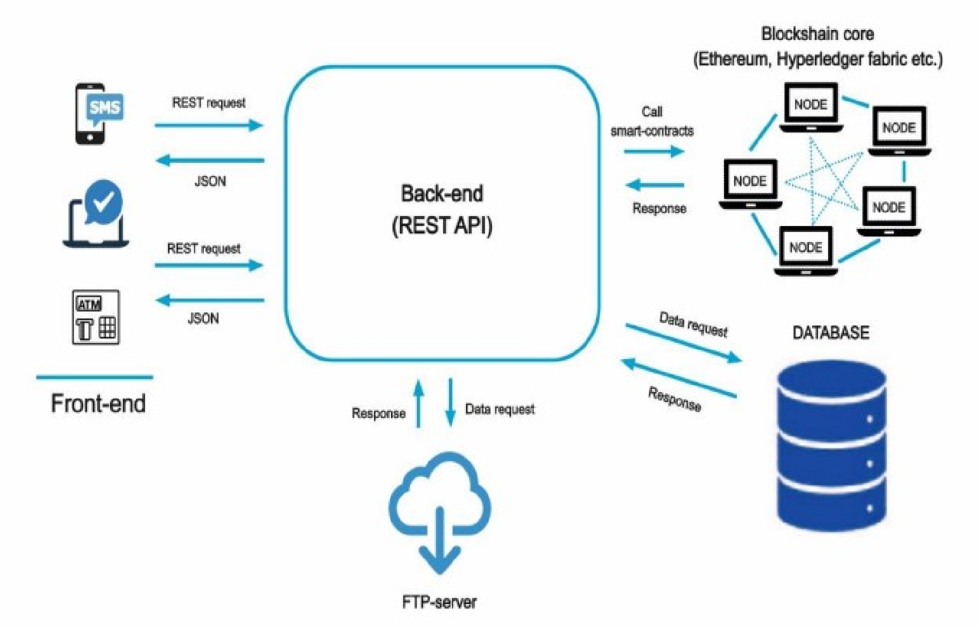


Figure 3.1: Architecture solution for donation tracking platform [6]

The research work [28], proposed a prototype of a blockchain application for Government Fund Tracking that will help to track the transactions and utilize Government allocated funds paving the way to reduce corruption. They have used the Hyperledger Composer from the Linux Foundation and CTO which is a modeling language used by Hyperledger Composer. It offers a playground user interface, which they utilize to create and test their prototype. As a transaction processor function, logics behind transactions have been developed in JavaScript. Their prototype model includes three components- participant, asset, and transaction. Here the asset refers to funds and the participants are people involved with financial management of the project. When a Fund Transaction is submitted, the transaction processing function is invoked. A transactional instance is supplied to the function, which identifies the relevant participant along with the transferred fund. If all of the restrictions are fulfilled by the transaction parameters, then it is logged in the database. This transaction record also includes a transaction ID and the timestamp of the transaction filed. It maintains a straightforward logic as when the transaction is placed, the assets register, and participants register to get updated to ensure the consistency of the data.

The paper [29] is about a tracking system where they used quarkchain to design the Blockchain based tracking System. The major goal of this article is to provide decentralized proof of product and delivery tracking in an e-commerce transaction with strict security, transparency and traceability. They presented a decentralized application that uses QuarkChain as its backbone to give the functionality of a monitoring system with delivery notes. Quarkchain is a distributed data blockchain protocol that is executed using two different layer architecture: one layer is for transaction processing, which consists of numerous shard chains widely recognized as the shard layer, and another one is for providing coordination and securing the network. The QuarkCoin proposal was established to solve Ethereum's poor TPS throughput. In this application, a SC Authority serves as the administrator. It is a third party which ensures that the processes run smoothly. When a transaction request is made, both the transporter and the seller must set aside. The SC authority pays the escrow funds to the transporter and seller after a successful transaction but takes measures to remedy any discrepancies or violations.

In research work [7], a blockchain-based solution for tracking charitable funds has been proposed by Sirisha, Agarwal, and Monde. They have made their own funding system named Charity-Chain using Ethereum that maintains a decentralized network. It enables a social business to operate openly by using smart contract-based incentives to guarantee that their effect is independently verifiable and visible to anyone. This makes it easy for funders to oversee transactions, enhancing trust on nonprofits. They have categorized four types of users based on their roles- organization, donor, retailer and government official, shows in figure 3.2. Their proposed Charity-Chain system maintains the Byzantine Agreement that locks decisions according to maximum agreement. There are also four modules in this system- Account registration and verification module, Tender generating module, Request verification and authorization module, Payments and monitoring module. All these have been built using the Ethereum platform on Embark framework and used React for GUI as well as Solidity for smart contracts. Using the Byzantine consensus technique brings computational ease and scalability to their proposed system.

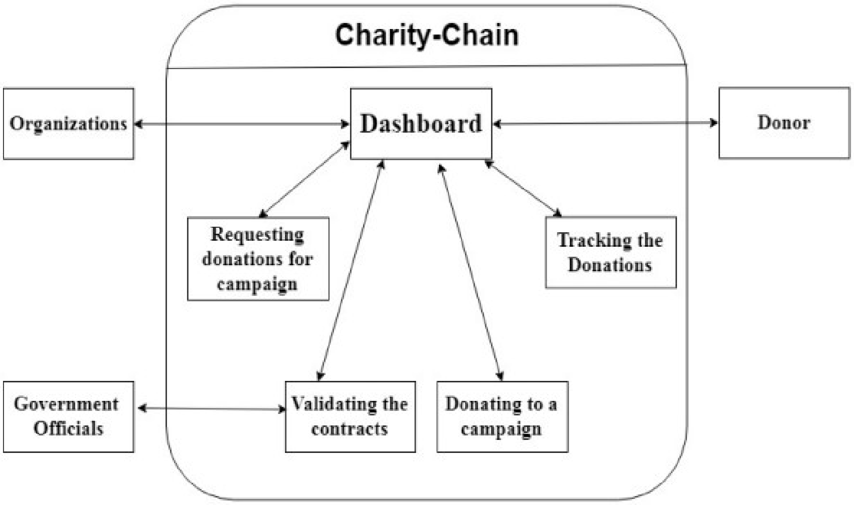


Figure 3.2: Charity-Chain Block Diagram [7]

Another research paper, Mehra et al. [30] suggested a transparent and safe framework for direct contributions. According to them, their platform would be linked to various non-profit organizations. For implanting the system, they have created a Hyperledger-based prototype that solely deals with the resources. Basically, charity collection deals with the dollars but anything in Hyperledger refers to an asset which restricts their approach. They did not use the consensus algorithm like proof-of-state or proof-of-work. Their system works when all the users of the network are predefined. But as their work is for charitable organizations and in charity, there is no specific donor for all the time, it changes over time, so it poses a barrier to their system's usability.

In paper [31] The author D.Fiergbor describes the blockchain technology of the fund management system in Ghana. Here, the author focuses on transparency, accuracy, and accountability among the fund managers. The main reason for that proposal is the security issues of data storage. This paper focuses on the mutual fund management system in Ghana.It also includes Ghana's fund management technology through blockchain.

In research paper [8], there has been proposed a transparent tendering system using blockchain where the citizens are able to participate in tendering directly. They have confessed that their system is more transparent, reliable, fair, and secure than the traditional tendering procedure. They have used a permissioned and private blockchain platform to build the system with the combination Hyperledger Fabric and Hyperledger Composer. They have used Hyperledger for its main 3 components-Membership Service Provider (MSP), Orderer, and Chaincode which together maintain a permissioned environment to protect the system for unwanted members. The system consists of 4 types of nodes like citizens, tenders, bidders and the final winner. At first, all the concerned entities register themselves to the blockchain network. When the government plans to introduce any project for welfare of the country, the citizens put their own suggestions regarding that to the system. After collecting all sorts of recommendations from the citizens, the tendering organizations observe those and publish the most prioritized one. After that, the bidding organization bids to get the project, and this bidding procedure is also organized in a decentralized way and only the eligible institution gets the opportunity and also all funds from the government. At last, they have also added a feature of tracking the fund of the winner account. Figure 3.3 shows the framework of their system. As all these steps are being handled by the automated blockchain system, there is no way to cheat the system and no trust issues can take place between the government and its citizens. But as they have used a private blockchain network, how the general citizens would be able to visualize the whole tendering and funding procedures still remain a concerning question.

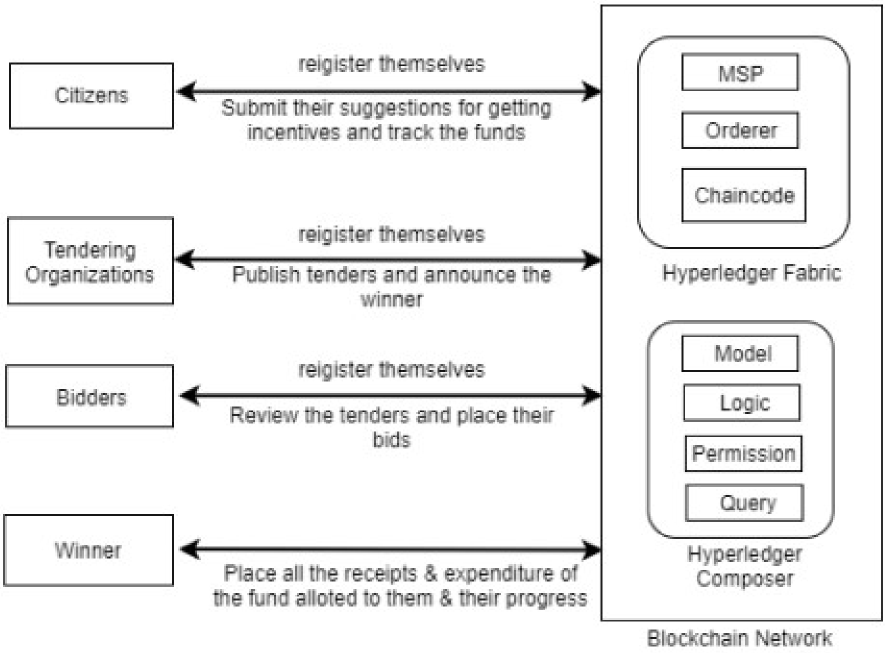

Citizens
reigister themselves
Submit their suggestions for getting incentives and track the funds
Tendering Organizations
reigister themselves
Publish tenders and announce the winner
Bidders
reigister themselves
Review the tenders and place their bids
Winner
Place all the receipts & expenditure of the fund alloted to them & their progress
MSP
Orderer
Chaincode
Hyperledger Fabric
Model
Logic
Permission
Query
Hyperledger Composer
Blockchain Network

Figure 3.3: E-governance framework via private blockchain [8]

In paper [3], a transparent donation system for university students has been approached. According to this paper, in their proposed system, the needy and financially unstable university students can get the facilities of funds without involvement of any other parties between the donor and students. The university authority updates information of each student to the system. When a donor provides help to any university, the system stores the transaction in a distributed ledger of the Ethereum network. The selected students can receive the help from their individual accounts using blockchain technology. A smart contract between the donor and the student is also possible if the donor wishes to provide help through study materials. They have used the SHA-256 algorithm for generating unique hash values which all together makes an unbreakable network. The Consensus protocol verifies transactions whether to approve or ignore the inputted transactions. To smart contract deploy they have used remix compiler and Rinkeby Test network which runs without the actual miners of blockchain rather than pre-defined trusted community. Also a mechanism from the Proof of Work algorithm has also been utilized to establish consensus of things such as account balances, sequence transactions, and guarantee about not to replace or attack the chain.

In paper [32], an authentic donation environment has been approached using blockchain technology. They have claimed that their proposed system can bring a solution to the traditional sponsorship system that fails to maintain trust among the sponsors and the recipients. Here, a peer-to-peer mixing technique is used so that the identity of the donors and the grantees can not get disclosed to other organizations. There are 3 types of nodes in this system which are donors, receivers, and voters. When a donor wants to give a donation to a receiver, the voters calculate a voting result by creating a renewed contract and then provide a changing address for both donor and receiver. Then the donors send donations using that changed address so that their identities remain unrecognized to other users of the system. They have built a test system using Metamask as a network, solidity as language, and also Remix IDE as platform. Though they have shown a secured identity management system to their donation system, there is no proper information about how the donors can trust the receivers if their provided donation is properly being utilized or not.

After looking at multiple research papers, a comparison among different funding mechanisms using blockchain technology is given in table 3.2.

Authors	**Platform**	**Algorithm**	**Use of Blockchain**	**Target Audience**
Abid, Farouk & Khan	Ethereum (Public)	Fault Tolerance	Charity collecting procedure via crypto wallet, ICO, an economic model & CharityCoin-digital currency	Charitable organizations
Saleh, Avdoshin & Dzhonov	Ethereum (Public)	Russian Certified	Employing distributed registry technologies, provide a platform for monitoring & hosting donations	Non-profit organizations
Apoorva & Acharya	Hyperledger Composer (Private)	Not mentioned	Tracking Government allocated funds in large projects	Government
Sirisha, Agarwal & Monde	Ethereum (Public)	Byzantine Consensus	Introducing CharityChain as a decentralized network, assists social groups transparently running their projects	Charitable organizations
Ferwana	Ethereum (Public)	Proof-Of-Work	Helping students providing money or study materials through a secured network	University students
Goswami, Agrawal & Bhatia	Hyperledger Fabric & Composer (Private)	Consensus	Voting, tendering, bidding & funding via maintaining one decentralized transparent system	Government and citizens

Table 3.2: Comparison among different funding mechanisms using blockchain technology

3.4 Open Challenges

Through all the research, it has turned out that a fund transferring mechanism without blockchain faces different types of challenges.

Lengthy procedures: First of all, the procedure becomes so lengthy as whenever one needs to transfer money from bank to bank, some bank or the money transfer firms demand customers to provide additional information before completing transactions. It might be stressful and time-consuming for someone who is utilizing this service for the first time.

Additional exchange rate: The most prominent problem during international money transfers is the currency exchange fees. Many payout companies and regional banks charge higher currency rates to their consumers, forcing them to spend more money. Furthermore, some platforms charge a greater service cost from their users.

Slow transfer system: In most of the cases, while transferring money internationally, the procedure takes more than a day or even more than a week too. This transfer time varies due to a variety of reasons such as different currencies, fraud protection, different time zones, and so on. Whoever needs the fund on an urgent basis like funds during natural calamities, it becomes very stressful for the people.

Limitation to transfer amount: Most of the payout companies or banks restrict the upper limit of the money transfer amount. When a larger amount needs to be transferred, the user might send the amount in multiple transactions, where each transaction takes a lot of time so the overall procedure becomes very complex for the user.

Overcoming all of these considerations and selecting the finest gateway is also a challenging task for anybody who needs to transfer money on a regular or infrequent basis. Therefore, the deployment of blockchain technology in secured money transfer systems can overcome these challenges. Hence, significant analysis of using blockchain in the funding system have been conducted in various scientific papers.

Implementation of Blockchain technology in the funding mechanism may bring a significant change in the overall current financial system. Analyzing different scientific papers on this system, it has been shown that there are still some remaining challenges that remain questionable. After analyzing multiple research papers, in table 3.3, some of the research gaps of these papers have been given.

Paper Title	Research Gap
A framework to make charity collection transparent and auditable	Not mentioned about tracking the government funds used in development projects.
Blockchain for government fund tracking using Hyperledger	As used a permissioned blockchain, when the system is managed by only the government officials and if most of the officials come out dishonest then the system can easily be fooled.
A blockchain based tracking system for university student	As per the claim there was no proper implementation on how the study materials are going to be tracked.
Blockchain-Based One-Off Address System to Guarantee Transparency and Privacy for a Sustainable Donation Environment	No proper information about how the donors can trust the receivers if their provided donation is properly being utilized or not.
Platform for Tracking Donations of Charitable Foundations based on Blockchain Technology	Lack of practical implementation, only talked about the tools but not any system prototype.
E-Governance, A Tendering Framework Using Blockchain	Because of using private network, a restriction came forward for the general citizens to visualize the tendering and funding procedures which creates confusion on the system's reliability.

Table 3.3: Gaps in different funding approaches using blockchain

Above discussions demonstrate that though blockchain technology can bring significant change in the funding system, still there remains controversy. Analyzing all these challenges, in our research work, we have tried to fulfill gaps in earlier models with all required features and execution. For this we have focused on both governmental and non-governmental organizations, as well as individual citizens all can be beneficiaries through our system. Also keeping in mind the reliability issue of private blockchain systems, we have decided to use public blockchain in our system. Moreover, the system is independent from any kind of third party and ensures the reliability and traceability of fundraising mechanisms.

Chapter 4

Research Methodology

4.1 Introduction

This chapter covers the research methodology used to answer the questions raised in part 1, and the proposed model as well as it's framework which provides a detailed logical explanation for the structure of the funding system given in this research. Then, the sequential activity model is also described to comprehend the model's activities in order to obtain a comprehensive overall picture of the model. After that, layered architecture is demonstrated. The framework given here is based on this layered architectural structure. Lastly, the cost analysis which depicts the estimated cost of our proposed model.

4.2 Phase Of Awareness Of The Problem

The methodology is initiated with a problem statement, which can be derived from a wide range of sources, including mismanagement of funds, flawed accounting records, lack of accountability, and transactional data loss. To resolve these constraints, we are using ethereum which is a smart contract blockchain technology to ensure transactional traceability and security at every stage.

There are countless cases in Bangladesh where corruption is clearly visible. Governments are in charge of a broad range of activities. Governmental agencies involve a significant number of transactions for multiple functions that must be completed throughout the state. Low-level corruption, which can be hard to detect and impedes state progress, is a major concern for the government. Following a focused evaluation of research journals that dealt with the issue of tracking donation and its mechanisms without using Blockchain technology, we found that maintaining transparency of all transactions is extremely difficult for the existing donation system whereas we choose blockchain technology to resolve this issue. Our system not only assures that important information is protected at all times but also prevents the possibility of data being corrupted without acknowledgment.

4.3 Proposed Model

In this research experiment, using the blockchain technology, we propose to generate a funding model that attains two sub-goals: designing a fund management methodology in which authorized individuals can receive and withdraw allocated funds in cryptocurrency, and evaluating a smart contract to incorporate the money and identify transparency and tracking. The system here is made up of the fund contributor, the approved receivers chosen by the contributor, and the general public.

Using blockchain technology, this study proposes a safe, accessible as well as efficient framework for managing funds. This technology improves system accountability by permitting contributors to monitor their money via blockchain traceability and get alerts when it reaches the desired receivers. Funding made by deployers is secured by the smart contract, which ensures an authentic transaction containing proof of full process. A smart contract transaction can't be distorted with, and the donors can track the donation by tracking down the distributor/institution and eventual recipients. The blockchain system notifies the contributor when the funds are received, and the blockchain nodes are adjusted to each entry. Meanwhile, smart contracts,which are nothing but programming software that enables blockchain to execute authentic transactions in the decentralized network without the intervention of any external parties. To guarantee that funds are not misappropriated, they are locked and cannot be used until they have been acknowledged by one of the authorized sources. Here, the entire system is transparent, and it records track of each transaction for examining bodies such as the government, who can intervene if they discover something suspicious. Figure 4.1 demonstrates how blockchain technology can be utilized to enhance the current funding processes.

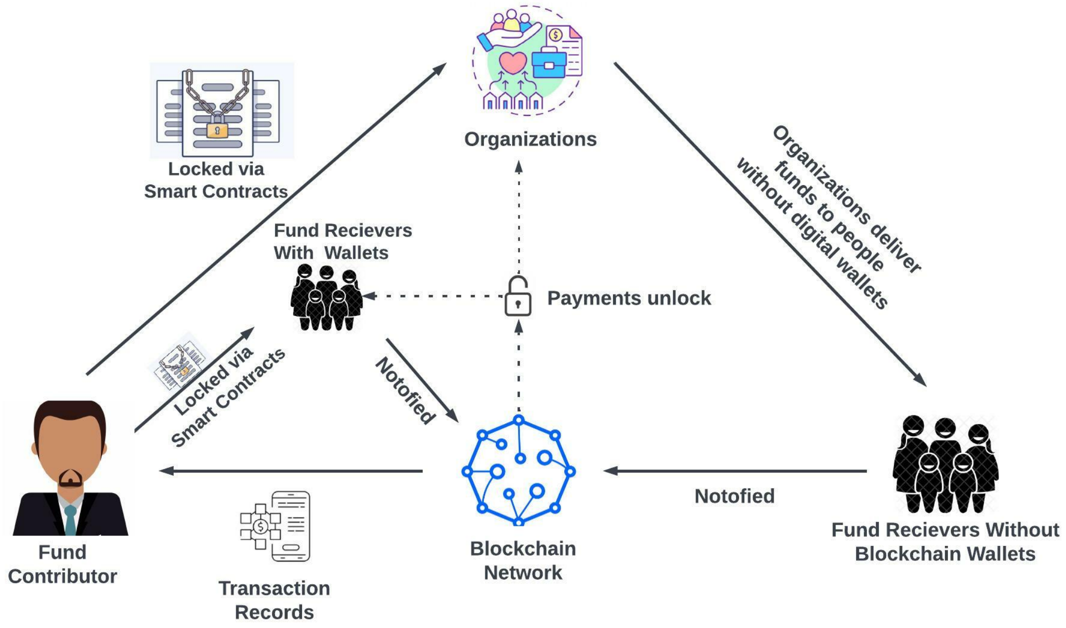

Organizations
Locked via Smart Contracts
Organizations deliver funds to people without digital wallets
Fund Recievers With Wallets
Payments unlock
Locked via Smart Contracts
Notofied
Fund Contributor
Transaction Records
Blockchain Network
Notofied
Fund Recievers Without Blockchain Wallets

Figure 4.1: Proposed Framework

4.4 Proposed Framework Architecture

The primary stakeholders in our approach are fund providers, receivers with wallets, and organizations. Its essential components of fund management systems such as DApps, smart contracts, the web, digital storage, and the blockchain network. The users register themselves on the platform by providing their personal details, and then the DApp answers them with a distinct public address. In this network, every user's public address is their primary identity. IPFS is a file system that allows data to be transformed between various components, such as DApps and data storage. The fund management system can be accessed by the system's three major users: contributors, organizations, and receivers via mobile and web based applications using blockchain technology.

Aside from that, the suggested system includes several administrators with varying extents authorization along with management control. DApps include digital currencies, external party payment interfaces, ICO exchanges, and numerous wallets integration as there are several wallets for several digital currencies. Users' information and statistics values are stored and shared using IPFS, which is secured by smart contracts. The IPFS is associated with storage devices and a diversified range of peers across public addresses made up of the system's primary users. A donor with a virtual wallet, or in simpler terms, a DApps account, can initiate a charitable donation. The deployer has the option of choosing who receives his funds. The owner will be notified when the beneficiary gets the donation, and the smart contract will track the complete transaction, which will be preserved in the contributor and receiver's records.

In our proposed model, the person who will fund in the system is the deployer and he will be also the owner for this transaction. The deployer has the full accessibility to track and control the whole transaction system. The funder can provide money in any currency through this system and later the currency will be converted into ether via the system. Here, only the deployer can withdraw the money and also decide whom he or she wants to give the access to withdraw the money along with keeping the records of the whole transaction process. The owner has the ability to delete the assigned owner if he or she wants to. If the owner sees any suspicious behavior among any assigned people or the selected work for them has done, then the deployer can delete the assigned owner from the system which basically protects the security of the system. Moreover, in our system, there is a feature where we can check the leftover balance of the funder's account. By the owner check feature, people can check and verify the actual owner of the current funding system. As it is a public blockchain based system, general people can also see the full transaction process though they can't edit or withdraw any currency from this. But, it's an advantage for them as they will be acknowledged about the funds which are allocated for them and they can complain to the owner if they find any difficulties in getting funds. So, the authorized people of the fund management system will withdraw the money through digital wallets and can transfer the monetary or non-monetary fundings to the beneficiaries who don't have digital wallets. In the latter scenario, organizations can also provide documentation by returning images of receipts to ensure that their money is properly distributed among the right persons. The suggested framework's high-level structure is shown below in 4.2.

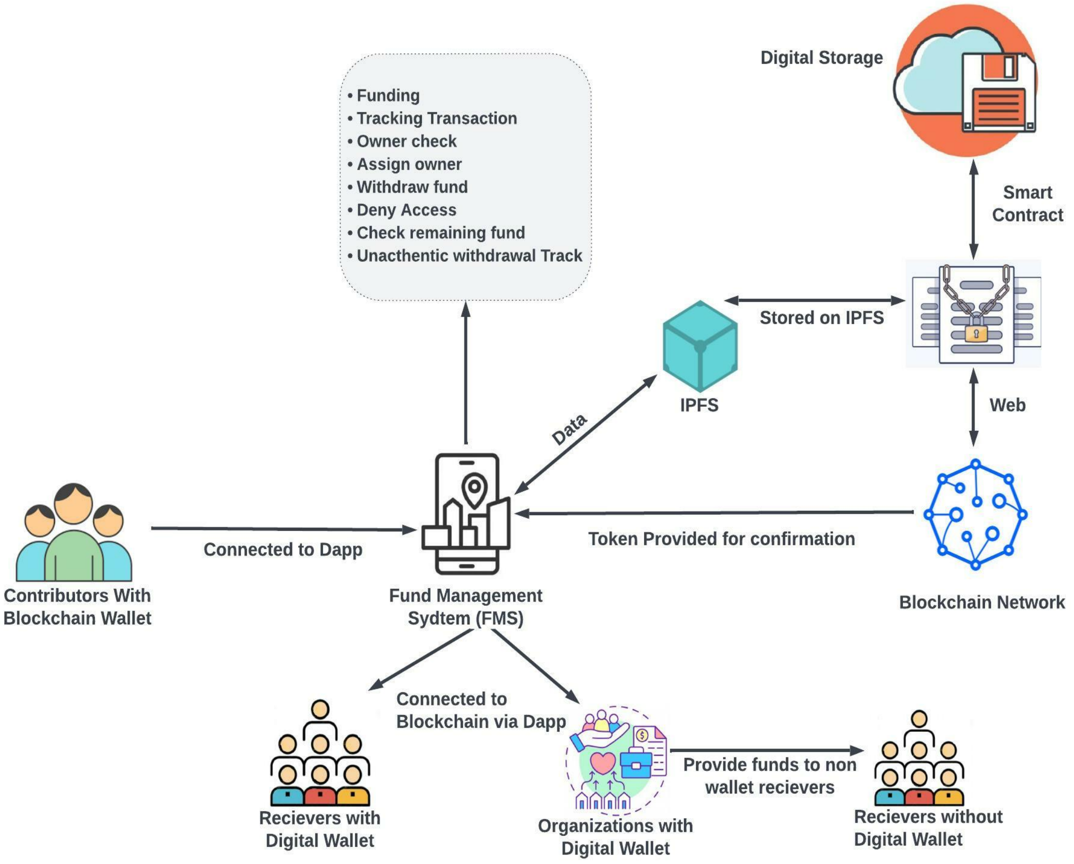

• Funding
• Tracking Transaction
• Owner check
• Assign owner
• Withdraw fund
• Deny Access
• Check remaining fund
• Unacthentic withdrawal Track
Digital Storage
Smart Contract
Stored on IPFS
IPFS
Web
Data
Contributors With Blockchain Wallet
Connected to Dapp
Fund Management Sydtem (FMS)
Token Provided for confirmation
Blockchain Network
Connected to Blockchain via Dapp
Recievers with Digital Wallet
Organizations with Digital Wallet
Provide funds to non wallet recievers
Recievers without Digital Wallet

Figure 4.2: Framework Architecture

4.5 Sequential Activity Model

It is essential to comprehend the model's activities in order to obtain a comprehensive overall picture of the model. This aids in the creation of an effective system model visualization.

Figure 4.3 depicts each system activity that must be completed and checked by everyone. Here, deployers and authorized people assigned by the owner must need to be registered to access the system. The deployer can provide access to the user. After gaining access, an authorized individual can enter into the system using their private key and withdraw funds. Unauthorized users will be denied access to the system and identified as inauthentic users. All other aspects will be handled by the system deployer, and only authorized people can withdraw funds from the system. After funding, the currency will be verified to see if it is taka or dollar using the model. If the currency is in taka, it will be converted to dollars and subsequently to ether. If it isn't taka, the dollar will be turned into ether straight. The whole transaction will be recorded and tracked by this blockchain based system to assure authenticity of the management.

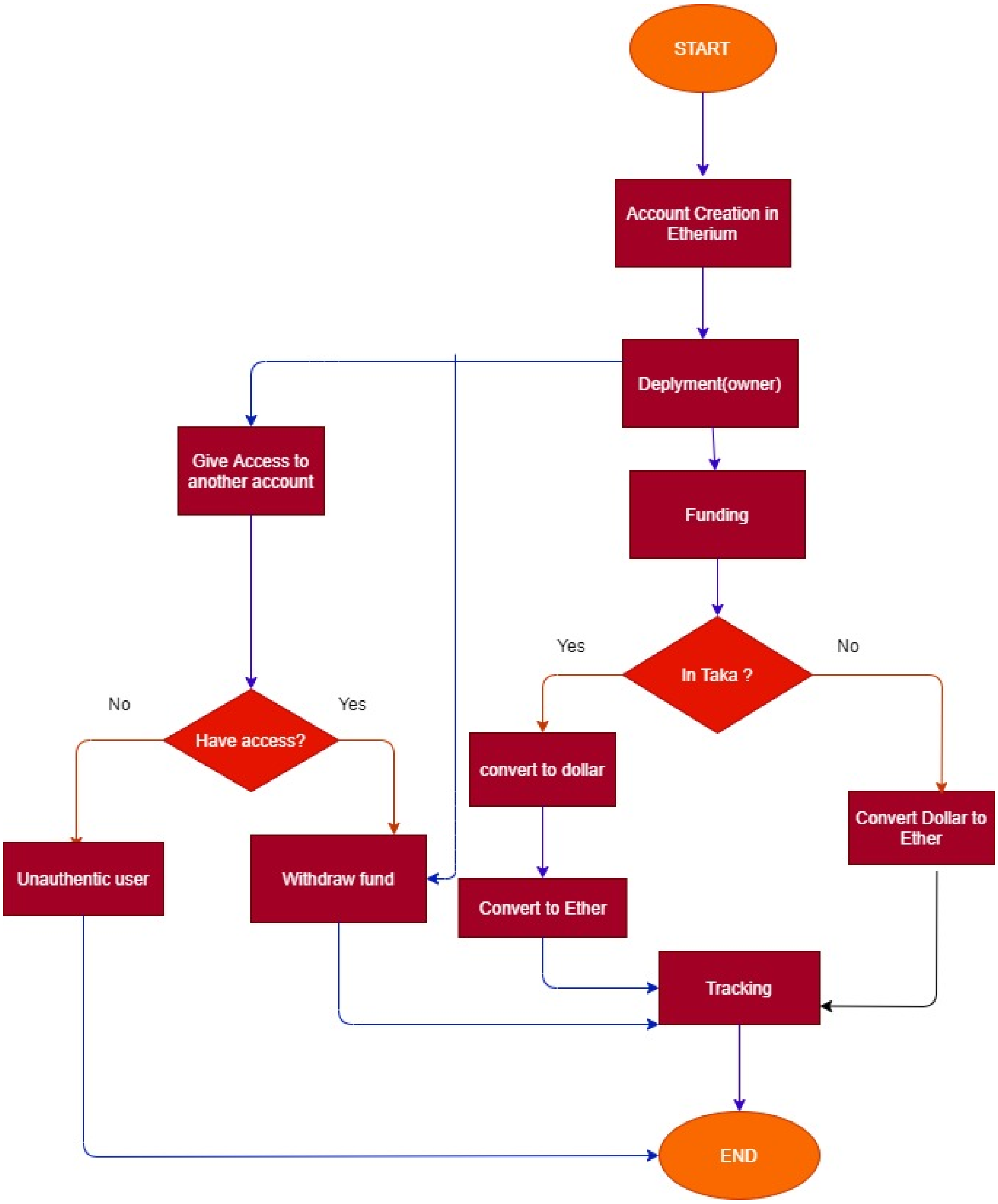


Figure 4.3: Activity Model

4.6 The Layer Structure Of Proposed Model

The presented framework is built on a layered architectural form, as seen in Figure 4.4. Interface layer, business logic layer, application layer, transaction layer, trust layer, blockchain layer, security and administrative layer, and infrastructure layer are the eight layers we've created here. The following is a breakdown of each layer:

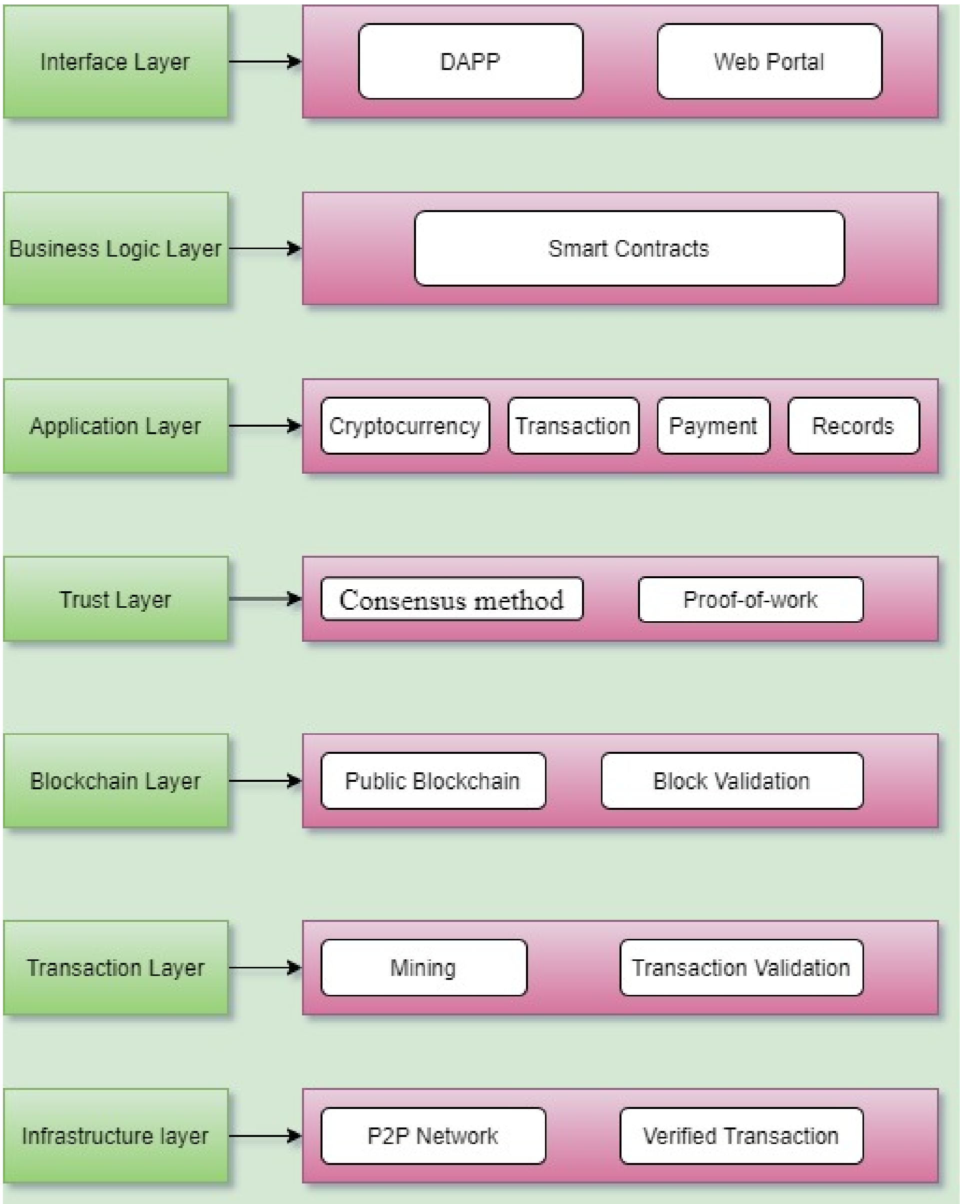


Figure 4.4: Layered Structure

Interface Layer: Internet based websites, DApps of the fund management system are encapsulated in the interface layer. The purpose of this layer is to offer an interface for funders, wallet beneficiaries, and organizations. This layer is used by these individuals to initiate the donation process.

Business logic layer: Smart contracts make up the business logic layer, which deals with terms, rules, and interaction requirements. As a result, this layer might be thought of as an operational database of smart contracts, equipped with all interaction, contract activation, and execution rules.

Application layer: Online records, donations records, identity verification, and transaction information are all part of the application layer. The application layer combines the interface layers with the business logic as in kind of a smart contract. The application layer combines the interface layers with the business logic as in kind of a smart contract.

Trust Layer: The trust layer contains the smart contract's security analysis, formal identity verification, and arbitration methods like Proof-of-Work. The trust layer also interacts with transaction consensus methods and recently introduced block verification, while the blockchain layer stores the results of execution.

The blockchain layer: This layer stores data about blocks' and nodes; it also holds the distributed ledger's basic information and hashes of each transaction executed by investors, organizations, and recipients with their secret and public keys addresses.

Security and administration layer: The system's security and maintenance is assured by this layer. Several security attacks aim at blockchain, with the 51 percent attack being the most common. This layer is interconnected to the system and works in tandem with it, containing several security algorithms and protocols as well as administrative responsibilities to ensure the system's integrity.

Transaction layer: The transaction layer is in charge of transactions, conducted by smart contracts or users of the fund management system.

Infrastructure Layer: It is made up of a peer-to-peer network that verifies, forwards and distributes the ethereum blockchain transactions. It also covers interaction, authentication, and distributed networking. When one transaction is completed, it is transmitted to all network nodes, and each node verifies the transaction using established parameters. The validated transaction is then saved in the database.

4.7 Cost Analysis

Depending on the aforementioned scenarios, we have estimated the cost of our proposed model:

- Procedure
- A Blockchain App's complexities
- Development Tools

Costs of deployment and third-party services :
Public Blockchain: $0.01 per transaction + $750 for third party
Costs of maintenance: Approximately 10% to 15% of the total project budget.

The following are some of the third-party tools which Blockchain Applications may require:
Amazon Web Services: Computation, Memory, Delivery. (Depends on the user's number, $100 - $1000).
Amazon SNS, Twilio: Provide notifications inside the interface. ($10 - $50).

Mixpanel/Flurry: Analysis of Data, channel, and monitoring. ($0 - $150).

The apps can be shifted to multiple platforms depending on their stability, adaptability, and confidentiality because blockchain technology is indeed new to the industry and new systems are arriving to the markets day after day. So, further additional costs for development is needed for this system. In our proposed model, we have made a medium complexity blockchain app which is dApps, built on the blockchain platforms like Ethereum. That's why we could work with multiple features at a minimal cost.

Chapter 5

Experimental Evaluation

5.1 Platforms For System Implementaion

i) **Smart Contract:**
Codes exist across decentralized, distributed blockchain networks. These codes can execute the transactions. The transactions are trackable and irreversible. These codes are automatically verified and these can be executed via a blockchain network. In 1998, an American computer scientist named Nick Szabo invented a virtual currency which is Bit Gold. IT defined smart contracts as computerized transaction protocol. It executes the terms of contract [33].

ii) **Solidity Programming Language:**
For implementing smart contracts, we can use solidity language which is an object-oriented program. It is a high-level language. Within the Ethereum state, the behavior of accounts can be handled by this language. For actions like voting, funding, multi-signature wallet we can create contracts by using solidity [34].

In this project, for the fund management system, we have used the last version of solidity which is v.8.11.

iii) **Brownie Development:**
For smart contract development, javascript-based libraries like truffle and Hardhat are basically used. But Python is also a highly based language and it can also be used in smart contracts as well. Web3.py is basically an entrancing python library that fulfills the needs of web3. The Brownie framework is built on the basis of web3.py [35].

We use brownie to test smart contracts. It is a python based framework and it supports smart contracts as well. In addition, contract testing through pytest can also be provided by brownie network.

iv)**Remix Testing framework:**
Remix is a solidity IDE which is a powerful source tool to write solidity programming language directly from the browser. We can write, compile and debug solidity codes through remix. It can be written locally as well. Remix is written in Javascript. We can use it both in browser and locally. Testing, Deploying, and debugging of smart

contracts are supported by remix [36].

v)**Proof Of Work:**
We use the Proof-of-work (Pow) algorithm in our system. The initial consensus algorithm in a blockchain system is the Proof of Work. This algorithm validates the transaction then adds a new block of transactions. Miners fight against one another to finish the network transaction in this algorithm. The production of proof of work occurs in a randomized and low-probability operation. A significant amount of trial and error is necessary in this case before a meaningful proof of work is created. The primary operating premise of proof-of-work is a mathematical problem that can be readily solved [37].

vi)**Blockchain Wallet:**
A wallet of blockchain is basically a digital wallet to store, manage and trade users' cryptocurrencies. To store the currency like bitcoin, ether, we use blockchain wallets. It is provided by a blockchain company which was founded by Nicolas Cary and Peter Smith. Through blockchain, we can transfer crypto-currencies and it also has the capability of converting these back into the local currency of the user. It also includes some security features as well [9].

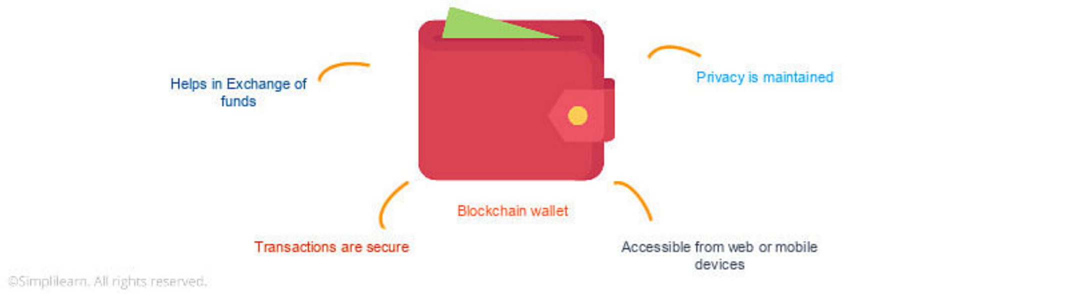
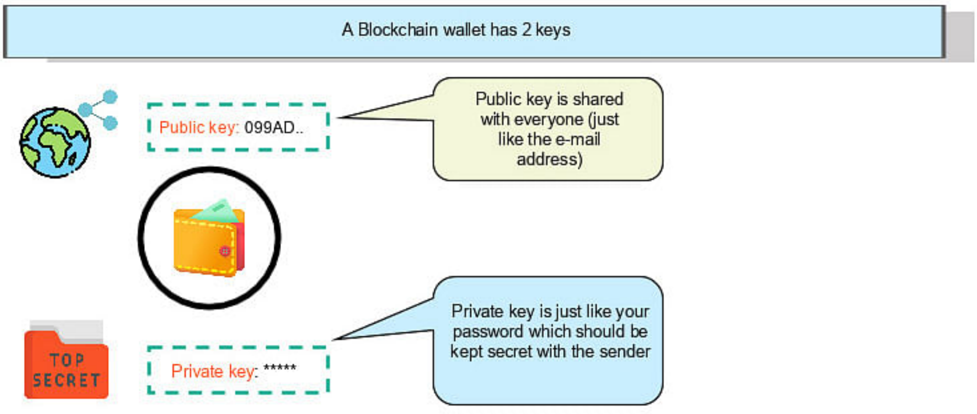

Helps in Exchange of funds
Privacy is maintained
Blockchain wallet
Transactions are secure
Accessible from web or mobile devices
©Simplilearn. All rights reserved.

Figure 5.1: Layered Structure [9]

How Blockchain Wallet Works:
To get access to a specific amount of crypto assets, users can request another party. A unique address can be generated by the system or also can be converted into a short Qr code as well. This code can store financial information and digital devices can read them. If anyone provides users any unique address they can also provide crypto assets. This process is almost similar to the sending and receiving fund process of PayPal but in that case, we can send and receive crypto-currencies [9].

Now, the interesting fact about blockchain wallet is, that it has private keys and public keys. When we create a blockchain wallet a public and private key will be associated with our wallet. We can share this public key with anyone if we want to receive funds.

But in the case of a private key, that is a secret key that should not be disclosed to anyone. Through this key, we can spend our funds from wallet and if anyone gets access to our private key we may face security issues and may lose our crypto-


A Blockchain wallet has 2 keys
Public key: 099AD..
Public key is shared with everyone (just like the e-mail address)
TOP SECRET
Private key: *****
Private key is just like your password which should be kept secret with the sender

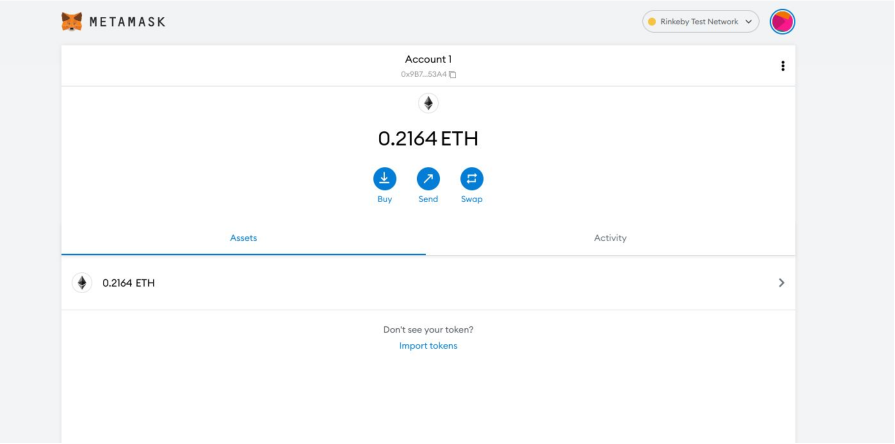
©Simplilearn. All rights reserved.

Figure 5.2: Blockchain Wallet [10]

currencies as well [10].

MetaMask: For this implementation, we used Metamask which is a blockchain wallet. It is a module for gaining access to distributed ethereum apps. Through the private keys, it enables users to set and administer their own identities. So, if a Dapp (decentralized application) wants to generate a transaction and also wants to write it to the blockchain, the user will get a secure interface. Users will get a chance to inspect the transactions before authorizing or rejecting it. Because in MetaMask it is required to get authorization for reading and writing any webpage.

In this metamask wallet, we have created two accounts for our project.


METAMASK

Rinkeby Test Network

Account 1
0x9B7...53A4

0.2164 ETH

Buy Send Swap

Assets Activity

0.2164 ETH

Don't see your token?
Import tokens

Figure 5.3: MetaMask wallet Account number 1

Figure 5.3 shows the blockchain wallet creation of metamask. Here in account 1, there are 0.2164 ether which is the amount of crypto-currency that this account has.

Figure 5.4 is another metamask wallet through which we can transfer currency to account 1 that we created before. This is account number 2 and it has 0.0656 ether which is the amount of currency of that account. If account 1 transfers any amount

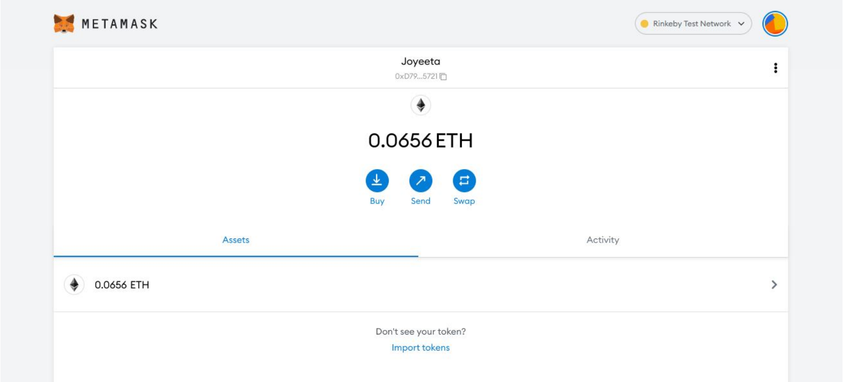


Figure 5.4: MetaMask wallet account number 2

to account 2, then the amount will be added to account 2. In this project, we will experiment our implementation with these accounts.

5.2 Experimental Settings

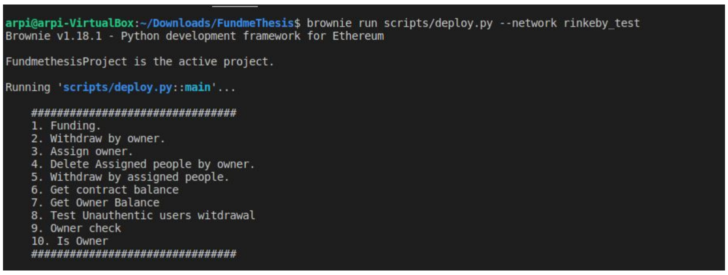
For implementation, we have to set up a few blockchain applications in our operating system which is Ubuntu. The steps for blockchain setup has given below-

1. Integrate metamask extension with browser.
2. Create a wallet account and set up a polygone network on that wallet.
3. Borrow some matic crypto for testing.
4. Install Remix IDE for writing smart contracts.
5. Brownie framework for testing smart contracts.

5.3 Experimental Results

After considering security issues there are some features for the fund management system where the deployer can fund and also has the right to ensure the security of the fund as well. The key features of blockchain-based fund management system are-

- Funding
- Withdraw by owner
- Assign Owner
- Delete Assigned people by owner
- Withdraw by assigned people
- Get owner Balance
- Test Unauthentic Users withdrawal



```
arpi@arpi-VirtualBox:~/Downloads/FundmeThesis$ brownie run scripts/deploy.py --network rinkeby_test
Brownie v1.18.1 - Python development framework for Ethereum

FundmethesisProject is the active project.

Running 'scripts/deploy.py::main'...

    ################################
    1. Funding.
    2. Withdraw by owner.
    3. Assign owner.
    4. Delete Assigned people by owner.
    5. Withdraw by assigned people.
    6. Get contract balance
    7. Get Owner Balance
    8. Test Unauthentic users witdrawal
    9. Owner check
    10. Is Owner
    ################################
```

Figure 5.5: Features of Blockchain based fund management system

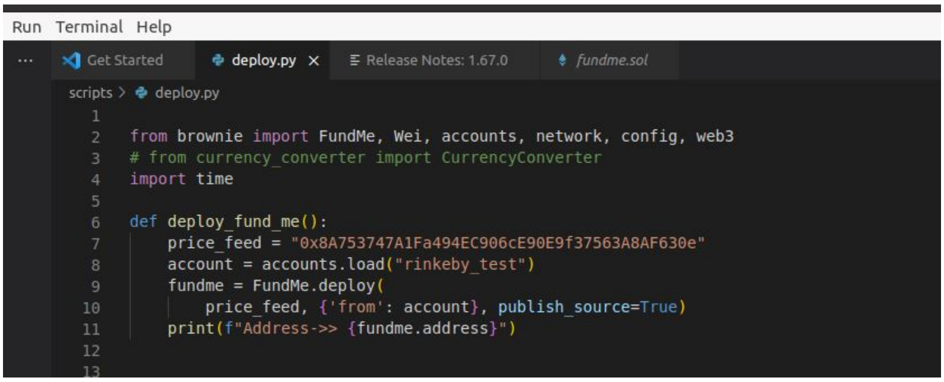
- Owner check

Here, figure 5.5 shows the features that we have used to ensure the security of our system.

Now, in the implementation part, both python and solidity have been used. Here, solidity is used to implement smart contracts. In EVM, smart contracts can only be used to run this system. But Python is basically for the client-side to call the smart contracts. But in that case, python and solidity are not alternatives. Each has an individual role to run the system.

5.3.1 Funding:

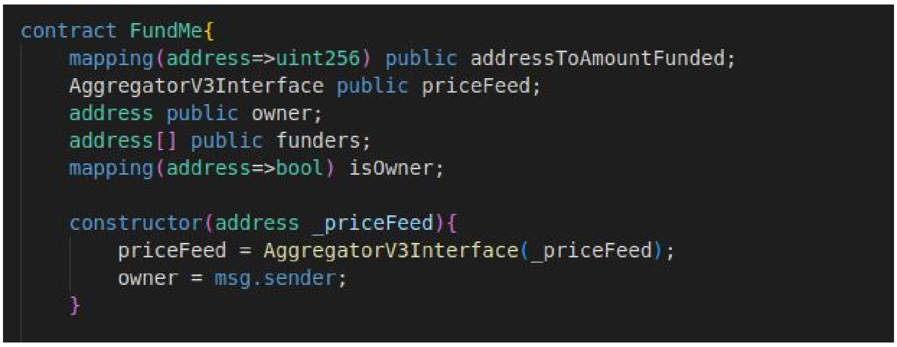
For this fund management system, one of the features is funding. The system of that feature is, that the person who will fund the system will be the deployer. At that time he or she is the owner and they will be able to track their transactions as well.



```python

from brownie import FundMe, Wei, accounts, network, config, web3
# from currency_converter import CurrencyConverter
import time

def deploy_fund_me():
    price_feed = "0x8A753747A1Fa494EC906cCE90E9f37563A8AF630e"
    account = accounts.load("rinkeby_test")
    fundme = FundMe.deploy(
        price_feed, {'from': account}, publish_source=True)
    print(f"Address->> {fundme.address}")


```

Figure 5.6: Funding by the deployer

Here, the fund_me() function is written for the funding. Now here price_feed is basically describing the real time value of etherium against the dollar. Now, here the “rinkeyby test” is basically the testing account that we created in metamask. Through this account we can test if the funding is successful or not.
Here the figure 5.6 and figure 5.7 is the representation of the fund me function in solidity programming language.

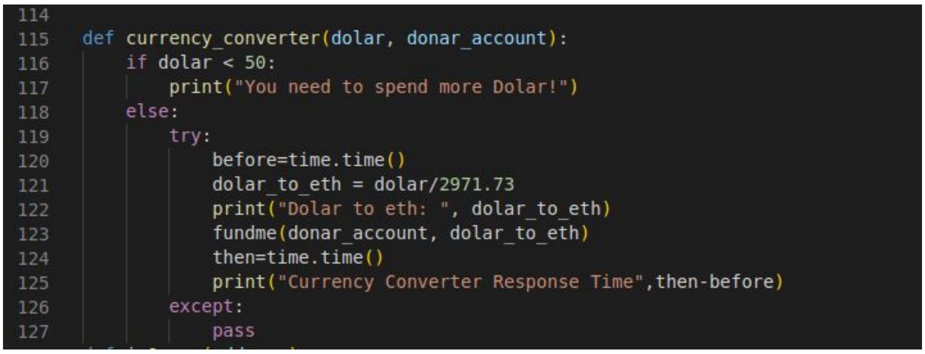


```
contract FundMe{
    mapping(address=>uint256) public addressToAmountFunded;
    AggregatorV3Interface public priceFeed;
    address public owner;
    address[] public funders;
    mapping(address=>bool) isOwner;

    constructor(address _priceFeed){
        priceFeed = AggregatorV3Interface(_priceFeed);
        owner = msg.sender;
    }
```

Figure 5.7: Backend solidity program of funding

5.3.2 Currency Conversion:

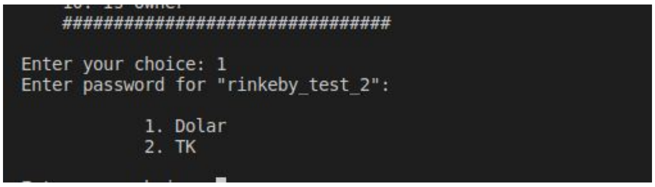
There are many organizations where we may need donations from other countries as well. For example, if anyone wants to donate in dollars or in taka then the system will maintain a gateway in that part. If anyone donates in taka then the taka will be converted to dollar and from dollar, it will convert to ether. On the other hand, if anyone wants to send dollars then the dollar will be converted to ether. In that way there is a way to take donations from other countries as well.



```
def currency_converter(dolar, donar_account):
    if dolar < 50:
        print("You need to spend more Dolar!")
    else:
        try:
            before=time.time()
            dolar_to_eth = dolar/2971.73
            print("Dolar to eth: ", dolar_to_eth)
            fundme(donar_account, dolar_to_eth)
            then=time.time()
            print("Currency Converter Response Time",then-before)
        except:
            pass
```

Figure 5.8: Conversion of the currency function

Here figure 5.8 is showing the conversion function of the currency. To convert the dollar or taka to ether, we have to divide the amount with actual ether price. For example, now the Ethereum price is 2971.73 ether. So, the dollar amount is going to be divided by the price so that we can convert the dollar or taka amount to ether.



```
    ################################

Enter your choice: 1
Enter password for "rinkeby_test_2":

            1. Dolar
            2. TK
```

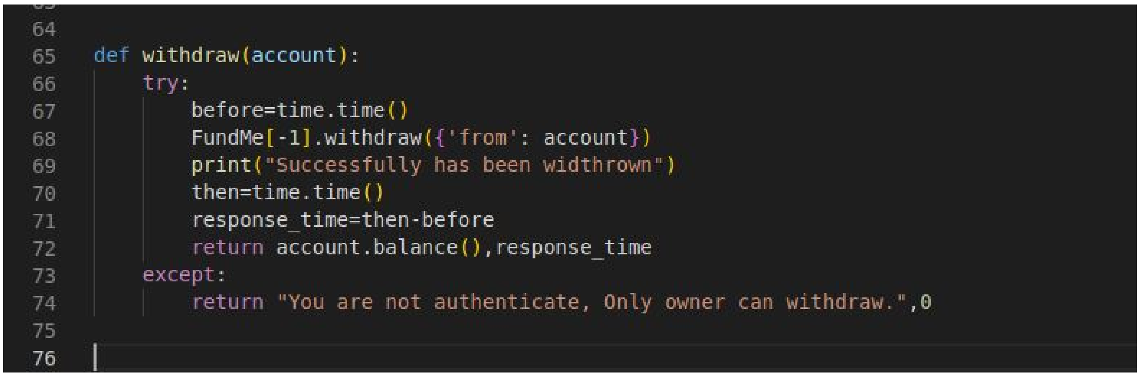
Figure 5.9: Conversion system

Figure 5.9 is basically showing the choice for the donor. If the donor wants to donate in taka or dollar on the basis of which the conversion will take place.

5.3.3 Withdraw By Owner

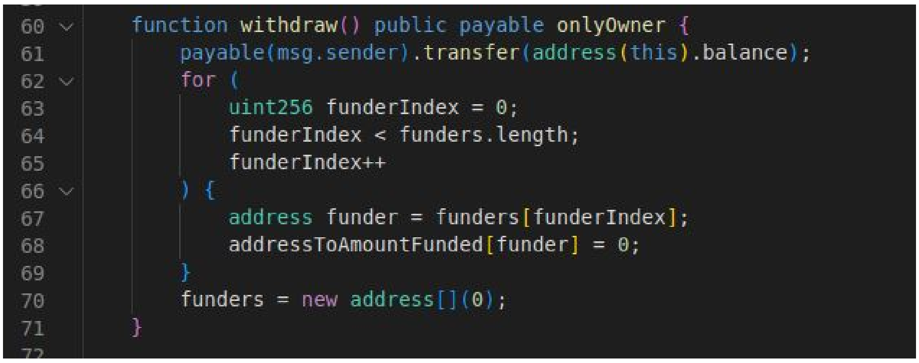
In that feature, only the owner of the system can withdraw the money. For example, if we consider any company or any industrial sector, there are many departments. For example, IT, HR, and event management. The deployer will decide to whom he or she wants to give the access to withdraw the money. So, if the owner gives access to the manager of the HR department, then the manager will be the owner at that time and will be able to withdraw the money. In that case, there will be the tracking of the transaction by whom the money has been withdrawn.

Figure 5.10 shows the withdrawal process of the system through the python programming language.



```python
def withdraw(account):
    try:
        before=time.time()
        FundMe[-1].withdraw({'from': account})
        print("Successfully has been widthrown")
        then=time.time()
        response_time=then-before
        return account.balance(),response_time
    except:
        return "You are not authenticate, Only owner can withdraw.",0
```

Figure 5.10: Python program of withdrawn of the transaction



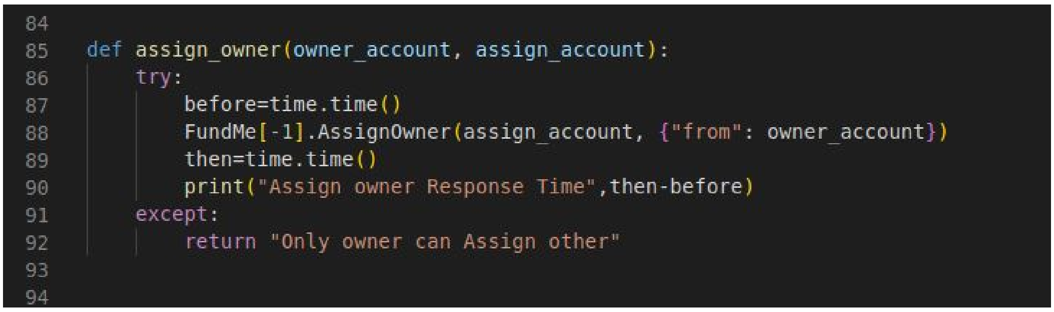
```solidity
    function withdraw() public payable onlyOwner {
        payable(msg.sender).transfer(address(this).balance);
        for (
            uint256 funderIndex = 0;
            funderIndex < funders.length;
            funderIndex++
        ) {
            address funder = funders[funderIndex];
            addressToAmountFunded[funder] = 0;
        }
        funders = new address[](0);
    }
```

Figure 5.11: Python program of withdrawn of the transaction

Figure 5.11 represents the withdrawal function process in solidity language.

5.3.4 Assign Owner:

In that feature, the deployer can assign the owner if he or she wants. It is because, if the deployer wants anyone to withdraw the money then the person needs to have the access to ownership. So, in that case, if the deployer gives the access of ownership to that person, only then he or she can withdraw the money.
Figure 5.12 shows the programs for assigning an owner to withdraw transactions or operate the system. Here owner_account basically describes the employer's account

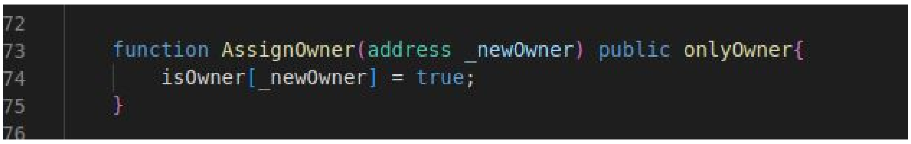


```python

def assign_owner(owner_account, assign_account):
    try:
        before=time.time()
        FundMe[-1].AssignOwner(assign_account, {"from": owner_account})
        then=time.time()
        print("Assign owner Response Time",then-before)
    except:
        return "Only owner can Assign other"

```

Figure 5.12: Assign owner feature in python programming language

who has the option to give access to any person to withdraw or operate the system.

Figure 5.13 shows the solidity program for the assigned owner feature of the system where the only owner, who is the deployer can assign a new owner for any specific purpose.

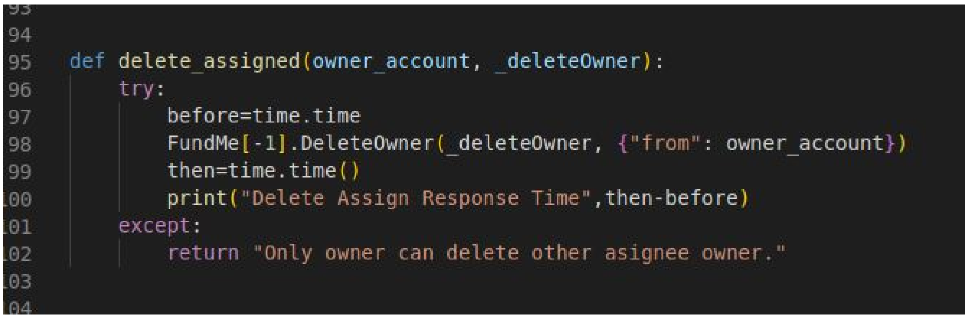


```solidity

    function AssignOwner(address _newOwner) public onlyOwner{
        isOwner[_newOwner] = true;
    }

```

Figure 5.13: Assign owner function in solidity

5.3.5 Delete Assigned people by owner:

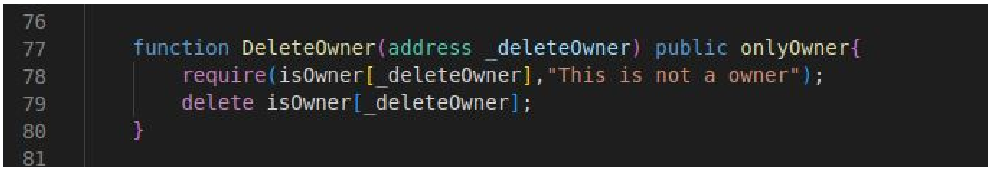
In that feature, the owner has the choice to delete the assigned owner if he or she wants to. That means, if an assigned owner is done with his/her work, then the owner can remove them as an owner as it's not needed anymore. It's also an important part for the security purpose as well. A deployer can assign ownership to a trusted person and if he/she feels any trust issues he/she can remove that person from the ownership as well. By this feature, it ensures the security of the system.



```python

def delete_assigned(owner_account, _deleteOwner):
    try:
        before=time.time
        FundMe[-1].DeleteOwner(_deleteOwner, {"from": owner_account})
        then=time.time()
        print("Delete Assign Response Time",then-before)
    except:
        return "Only owner can delete other asignee owner."

```

Figure 5.14: Delete assigned owner function in Python language

Here, figure 5.14 and figure 5.15 shows the function of delete_assigned owner where the deployer will be able to delete the ownership of the assigned person if it is needed.

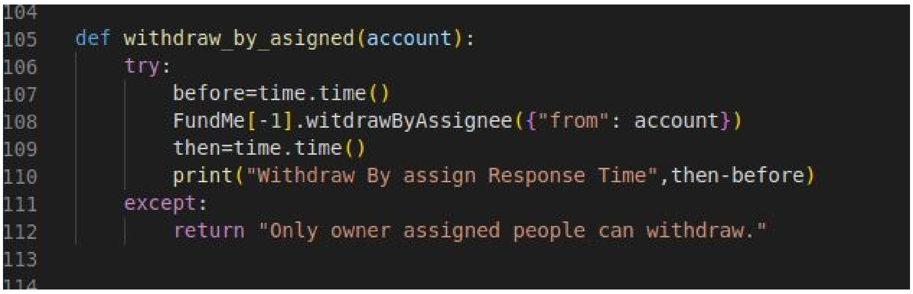


```
function DeleteOwner(address _deleteOwner) public onlyOwner{
    require(isOwner[_deleteOwner],"This is not a owner");
    delete isOwner[_deleteOwner];
}
```

Figure 5.15: Delete assigned owner function in solidity

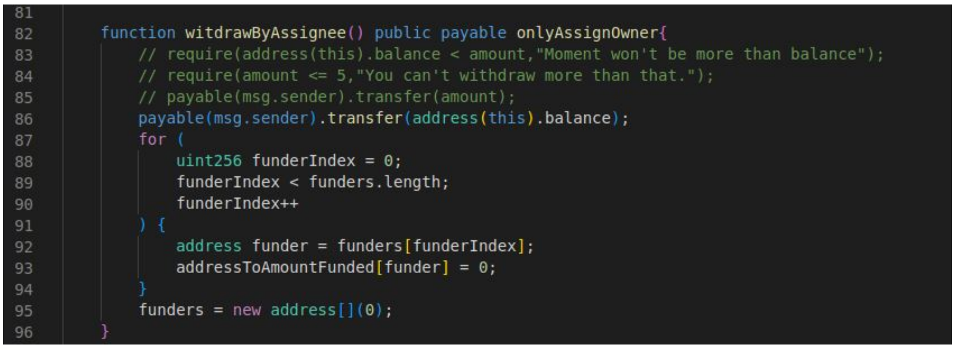
5.3.6 Withdraw By Assigned People:

This is the feature where the assigned people can withdraw money if they are given the access. If anyone outside of the department wants to access the transaction or wants to withdraw, then the account will be tracked and the system will refuse to give permission to that account as well.



```
def withdraw_by_asigned(account):
    try:
        before=time.time()
        FundMe[-1].witdrawByAssignee({"from": account})
        then=time.time()
        print("Withdraw By assign Response Time",then-before)
    except:
        return "Only owner assigned people can withdraw."
```

Figure 5.16: Withdrawal by assigned people function in python



```
function witdrawByAssignee() public payable onlyAssignOwner{
    // require(address(this).balance < amount,"Moment won't be more than balance");
    // require(amount <= 5,"You can't withdraw more than that.");
    // payable(msg.sender).transfer(amount);
    payable(msg.sender).transfer(address(this).balance);
    for (
        uint256 funderIndex = 0;
        funderIndex < funders.length;
        funderIndex++
    ) {
        address funder = funders[funderIndex];
        addressToAmountFunded[funder] = 0;
    }
    funders = new address[](0);
}
```

Figure 5.17: Withdrawal by assigned people function in solidity

Here figure 5.16 and figure 5.17 represent the function for assigned people's access to withdraw the transaction if they are assigned as the owner. If anyone who does not have the ownership tries to withdraw money, then the system will give the command which is "only assigned people can withdraw the money". So, in that case, there will be all the tracking of the accounts who withdrew the money or whoever tried to withdraw the money.

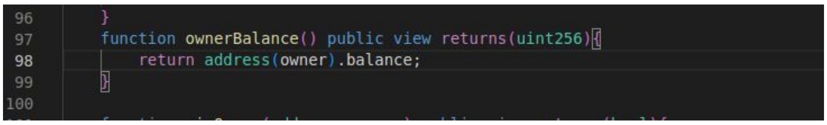
5.3.7 Inauthentic User Tracking:

In any organization or in any company, we may face some unauthentic users who are trying to access any account or access for any withdrawal. In that case, to track the account, we can get the account number of the account through this feature.

Here in figure 5.16, we can see that there is an exception which is basically indicating the tracking of inauthentic users.

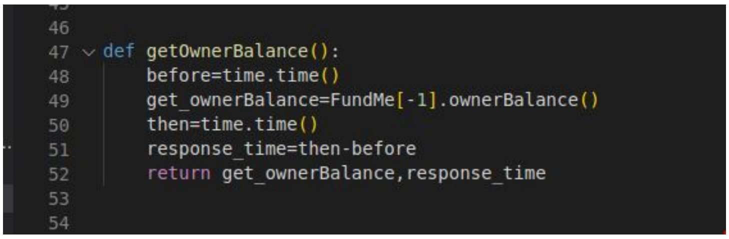
5.3.8 Check Owner Balance:

In this feature, we can check how much balance is left in the owner's account. If any confusion arises or if we need to verify anything, we can also check the owner's balance if it is needed. This feature is basically for security purposes or for verifying reasons.



```
    }
    function ownerBalance() public view returns(uint256){
        return address(owner).balance;
    }
```

Figure 5.18: Balance check function in solidity



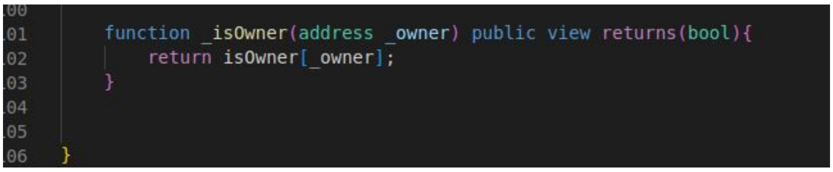
```
def getOwnerBalance():
    before=time.time()
    get_ownerBalance=FundMe[-1].ownerBalance()
    then=time.time()
    response_time=then-before
    return get_ownerBalance,response_time
```

Figure 5.19: Owner's balance check function in Python

Here, figure 5.18 and figure 5.19 shows the function for checking the owner's balance through which we can get an idea of the leftover balances in the owner's account.

5.3.9 Owner Check:

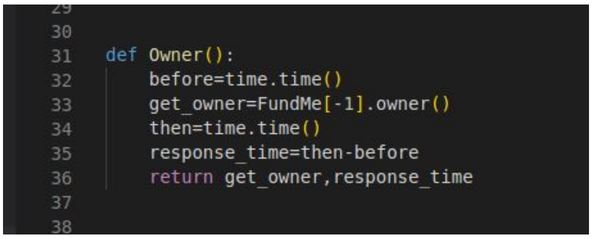
This is the feature to check who is the owner of the system. To know about the actual owner account or who is currently handling the system or if any inconvenience happens, then to find the actual owner, we can use that feature.



```
    function _isOwner(address _owner) public view returns(bool){
        return isOwner[_owner];
    }


}
```

Figure 5.20: Owner checking in solidity language

Here, Figure 5.20 and Figure 5.21 shows the owner function of our system through which we can find the current owner of the system.

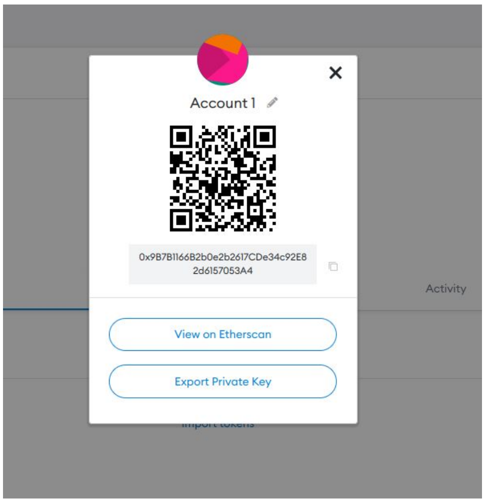


```python
def Owner():
    before=time.time()
    get_owner=FundMe[-1].owner()
    then=time.time()
    response_time=then-before
    return get_owner,response_time
```

Figure 5.21: Owner checking in python language

5.4 Experimental Findings

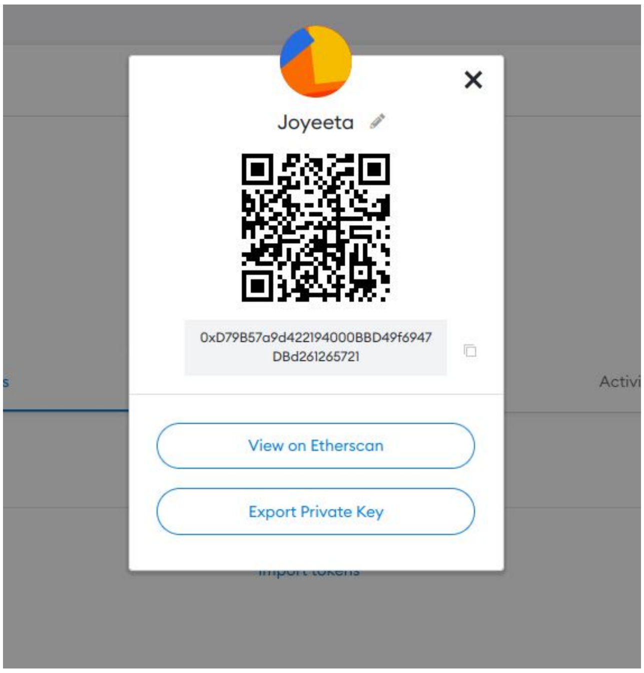
Here, let's first check who is the owner of the system. As we have two accounts. So, one of them will be the owner of that account.



0x9B7B1166B2b0e2b2617CDe34c92E8
2d6157053A4

Figure 5.22: Account 1 address

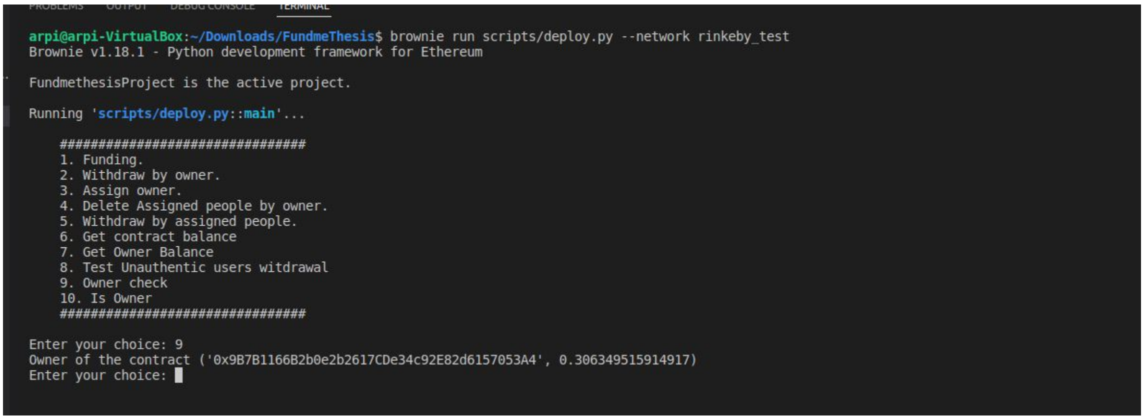
Here, we can see in figure 5.22, account number for account 1 is - 0x9B7B1166B2b0e2b2617CDe34c92E82d6157053A4



0xD79B57a9d422194000BBD49f6947DBd261265721

Figure 5.23: Account 2 address

Here in Figure 5.23, the account number of account number 2 is-0xD79B57a9d422194000BBD49f6947DBd261265721



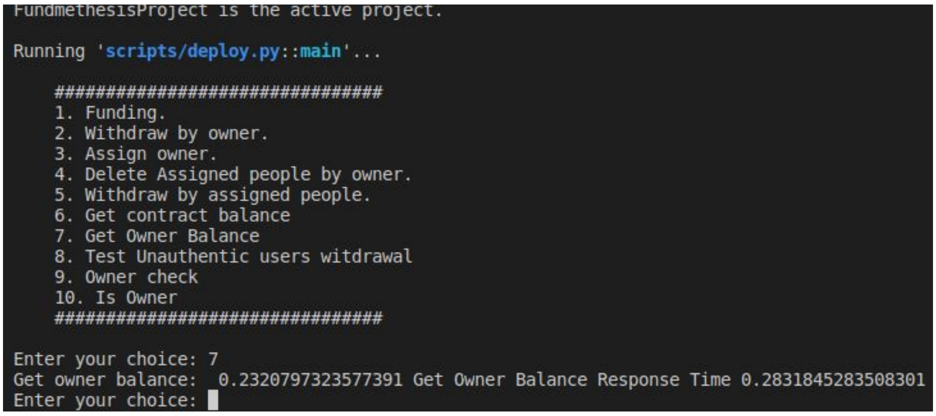
```
arpi@arpi-VirtualBox:~/Downloads/FundmeThesis$ brownie run scripts/deploy.py --network rinkeby_test
Brownie v1.18.1 - Python development framework for Ethereum

FundmethesisProject is the active project.

Running 'scripts/deploy.py::main'...

    ################################
    1. Funding.
    2. Withdraw by owner.
    3. Assign owner.
    4. Delete Assigned people by owner.
    5. Withdraw by assigned people.
    6. Get contract balance
    7. Get Owner Balance
    8. Test Unauthentic users witdrawal
    9. Owner check
    10. Is Owner
    ################################

Enter your choice: 9
Owner of the contract ('0x9B7B1166B2b0e2b2617CDe34c92E82d6157053A4', 0.306349515914917)
Enter your choice: █
```

Figure 5.24: Owner check

Here, in figure 5.24, we can see that the account number that owns the system right now is 0x9B7B1166B2b0e2b2617CDe34c92E82d6157053A4.

That means the owner of that contract is account 1. Because account 1 is the first deployer of that system. So, it is the current owner of that fund management system.

Now, if we want to check the balance of the owner for our security purpose, this can be possible through our system.

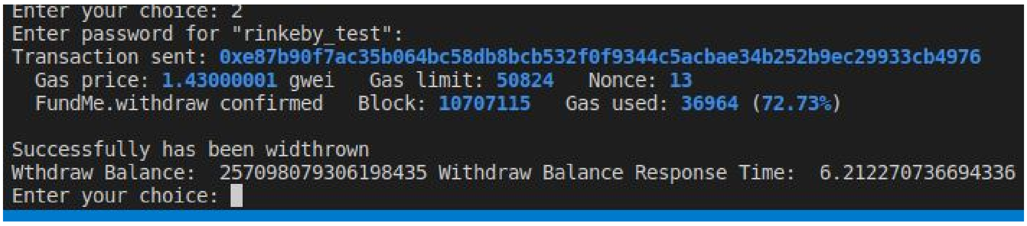


```
FundmethesisProject is the active project.

Running 'scripts/deploy.py::main'...

    ################################
    1. Funding.
    2. Withdraw by owner.
    3. Assign owner.
    4. Delete Assigned people by owner.
    5. Withdraw by assigned people.
    6. Get contract balance
    7. Get Owner Balance
    8. Test Unauthentic users witdrawal
    9. Owner check
    10. Is Owner
    ################################

Enter your choice: 7
Get owner balance:  0.2320797323577391 Get Owner Balance Response Time 0.2831845283508301
Enter your choice: █
```

Figure 5.25: Owner's balance check

Here, from the figure 5.25, we can match the owner's balance with our metamask balance. So, as the balance is matching, it means the system is working fine.

From the owner's account, we can withdraw money. Here, in figure 5.3, we can see, currently the owner has 0.2164 ether. So, let's check if the owner can withdraw the money or not.



```
Enter your choice: 2
Enter password for "rinkeby_test":
Transaction sent: 0xe87b90f7ac35b064bc58db8bcb532f0f9344c5acbae34b252b9ec29933cb4976
  Gas price: 1.43000001 gwei   Gas limit: 50824   Nonce: 13
  FundMe.withdraw confirmed   Block: 10707115   Gas used: 36964 (72.73%)

Successfully has been widthrown
Wthdraw Balance:  257098079306198435 Withdraw Balance Response Time:  6.212270736694336
Enter your choice: █
```

Figure 5.26: Account 1 withdrawal process

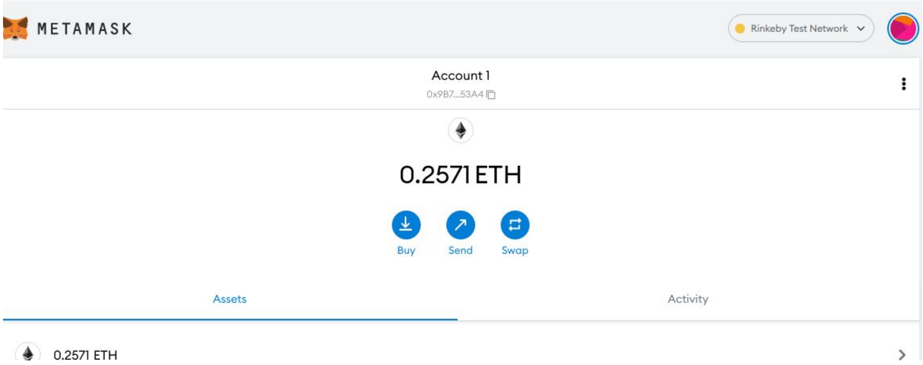
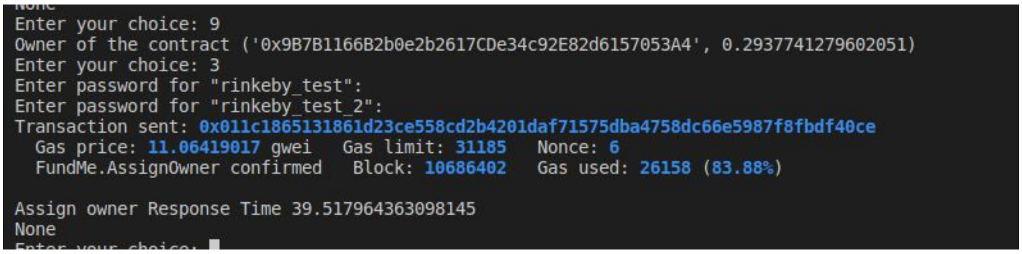


Figure 5.27: Account 1 withdrawal

Here, from the figure 5.27, we can see that the amount of the currency in account 1 is now 0.2571 ether which has been increased. That means the withdrawal process is successfully done.

In addition, we can assign a new owner as well through the current owner of the system.

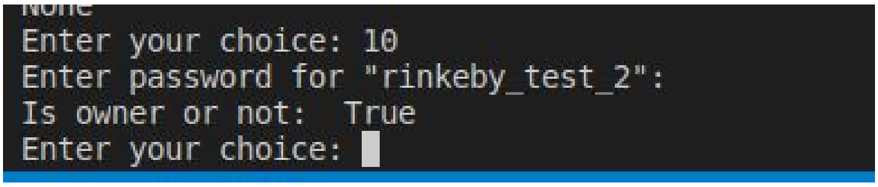


```
None
Enter your choice: 9
Owner of the contract ('0x9B7B1166B2b0e2b2617CDe34c92E82d6157053A4', 0.2937741279602051)
Enter your choice: 3
Enter password for "rinkeby_test":
Enter password for "rinkeby_test_2":
Transaction sent: 0x011c1865131861d23ce558cd2b4201daf71575dba4758dc66e5987f8fbdf40ce
  Gas price: 11.06419017 gwei   Gas limit: 31185   Nonce: 6
  FundMe.AssignOwner confirmed   Block: 10686402   Gas used: 26158 (83.88%)

Assign owner Response Time 39.517964363098145
None
Enter your choice:
```

Figure 5.28: Assign owner

Here, in figure 5.28, we have assigned another account which is account number 2. As for the test purpose we have created only two accounts. So, one is our deployer which is basically account 1. Now we have another account which can only be the other owner.

Now, to ensure if account 2 is the new owner or not, we can test it through another feature which is the owner's validity.

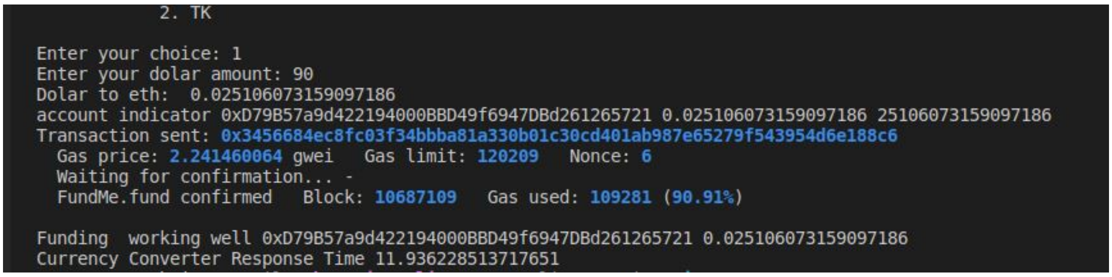


```
None
Enter your choice: 10
Enter password for "rinkeby_test_2":
Is owner or not:  True
Enter your choice:
```

Figure 5.29: Owner's validity

Here, from figure 5.29, we can ensure that account 2 is the assigned owner and is currently another owner of that system.

Now, let's test if the assigned owner(Account 2) can be able to do the funding process or not. Here, as we have already deployed account number 1 and it is the owner of that system, so here we are going to show the result of account number 2 for the funding process.



```
          2. TK

Enter your choice: 1
Enter your dolar amount: 90
Dolar to eth:  0.025106073159097186
account indicator 0xD79B57a9d422194000BBD49f6947DBd261265721 0.025106073159097186 25106073159097186
Transaction sent: 0x3456684ec8fc03f34bbba81a330b01c30cd401ab987e65279f543954d6e188c6
  Gas price: 2.241460064 gwei   Gas limit: 120209   Nonce: 6
  Waiting for confirmation... -
  FundMe.fund confirmed   Block: 10687109   Gas used: 109281 (90.91%)

Funding  working well 0xD79B57a9d422194000BBD49f6947DBd261265721 0.025106073159097186
Currency Converter Response Time 11.936228513717651
```

Figure 5.30: Funding process

Here in Figure 5.4, we can see that account 2 had 0.0656 ether initially. Then we in Figure 4.30, used 90 dollars for funding. This dollar will be converted to Ethereum. So, now, from our account 2, we have got 0.0402 ether after funding

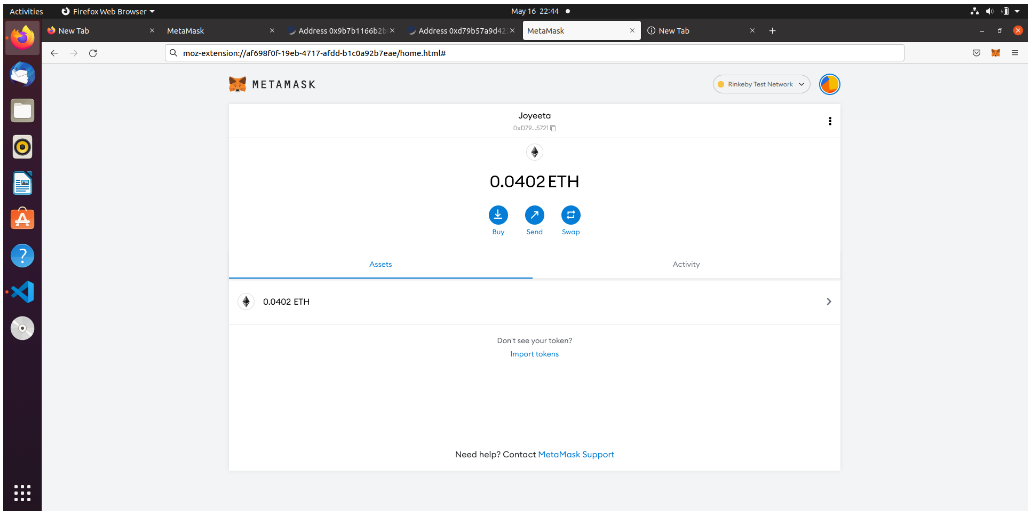
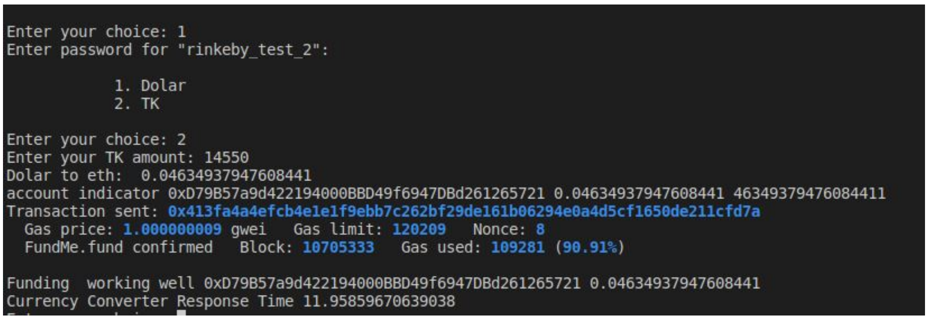


Figure 5.31: Result of funding process

which is represented in our Figure 5.31. So, we can see that our funding process is working correctly.



```
Enter your choice: 1
Enter password for "rinkeby_test_2":

            1. Dolar
            2. TK

Enter your choice: 2
Enter your TK amount: 14550
Dolar to eth:  0.04634937947608441
account indicator 0xD79B57a9d422194000BBD49f6947DBd261265721 0.04634937947608441 46349379476084411
Transaction sent: 0x413fa4a4efcb4e1e1f9ebb7c262bf29de161b06294e0a4d5cf1650de211cfd7a
  Gas price: 1.000000009 gwei   Gas limit: 120209   Nonce: 8
  FundMe.fund confirmed   Block: 10705333   Gas used: 109281 (90.91%)

Funding  working well 0xD79B57a9d422194000BBD49f6947DBd261265721 0.04634937947608441
Currency Converter Response Time 11.95859670639038
```

Figure 5.32: Funding process in Taka

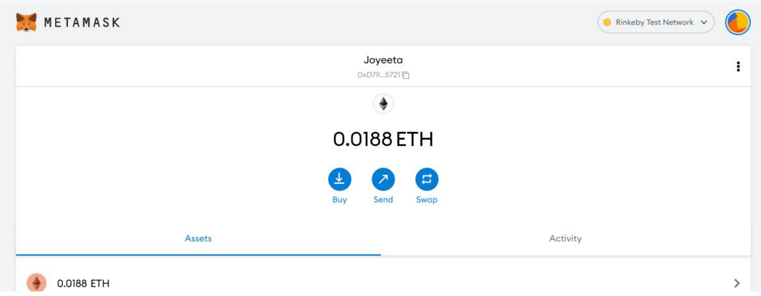
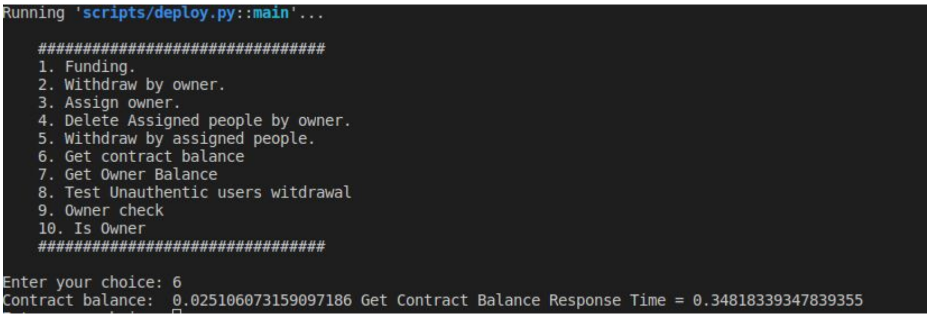


Figure 5.33: Result of funding process (2)

Here in figure 5.32, we have attempted for the funding in taka. Here the taka will be converted to dollars and from dollars, the currency will be converted to ether. So, after funding in taka, now, we have only 0.0188 ether which can be seen in figure 5.33.

So, from the figure 5.31 and figure 5.33, we can ensure that our funding process can work correctly in different currencies as well.

Now if we want to check the contract balance of our accounts, we can check it through the system. After deploying, each account creates a contract balance account where the money will be received and from here the money will be withdrawn.

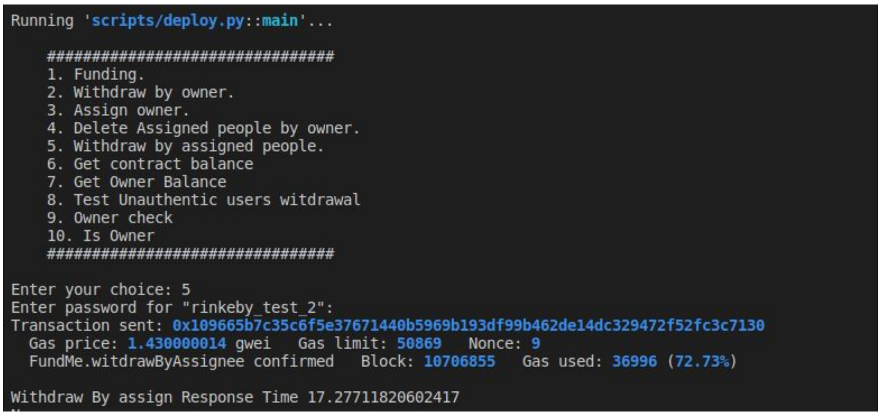


```
Running 'scripts/deploy.py::main'...

    ################################
    1. Funding.
    2. Withdraw by owner.
    3. Assign owner.
    4. Delete Assigned people by owner.
    5. Withdraw by assigned people.
    6. Get contract balance
    7. Get Owner Balance
    8. Test Unauthentic users witdrawal
    9. Owner check
    10. Is Owner
    ################################

Enter your choice: 6
Contract balance:  0.025106073159097186 Get Contract Balance Response Time = 0.34818339347839355
```

Figure 5.34: Result of funding process (2)

Figure 5.34 represents the contract balance of the account after deploying.

Now, if we want to withdraw our money from our assigned owner we have that access as well in our system.



```
Running 'scripts/deploy.py::main'...

    ################################
    1. Funding.
    2. Withdraw by owner.
    3. Assign owner.
    4. Delete Assigned people by owner.
    5. Withdraw by assigned people.
    6. Get contract balance
    7. Get Owner Balance
    8. Test Unauthentic users witdrawal
    9. Owner check
    10. Is Owner
    ################################

Enter your choice: 5
Enter password for "rinkeby_test_2":
Transaction sent: 0x109665b7c35c6f5e37671440b5969b193df99b462de14dc329472f52fc3c7130
  Gas price: 1.430000014 gwei   Gas limit: 50869   Nonce: 9
  FundMe.witdrawByAssignee confirmed   Block: 10706855   Gas used: 36996 (72.73%)

Withdraw By assign Response Time 17.27711820602417
```

Figure 5.35: Withdraw Processing

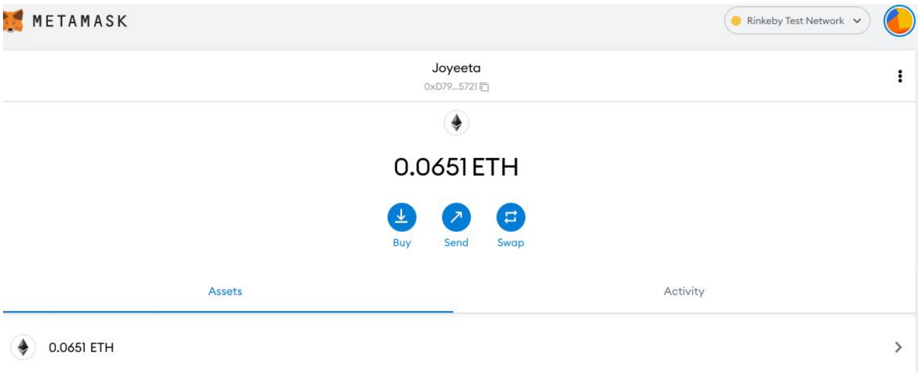
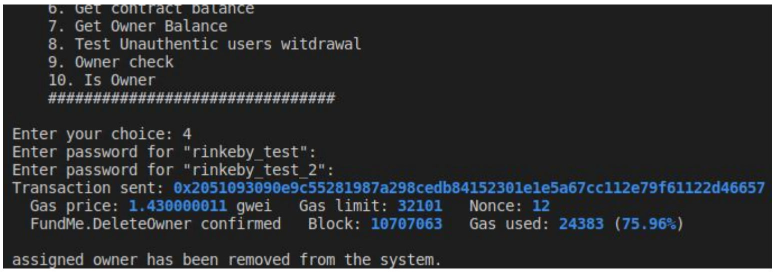


Figure 5.36: Result of withdrawal processing.

Here, in figure 5.35, we can see that from account 2 the withdrawal process has been done. Here we did not mention the amount of withdrawal activity but it is also possible to declare the amount for the betterment of the system. But for initial, the total amount that was in the contract balance, would be withdrawn by account 2. So, in figure 5.36, we can see that the total amount of account 2 has been increased because this account has withdrawn the money.

Now, we can also remove the assigned owner if the purpose of assigning him/her is done.

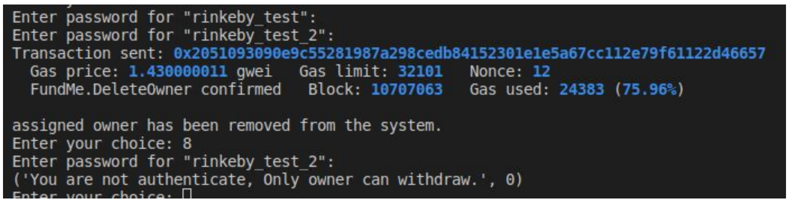
Here in figure 5.37, we can see that we have successfully removed the assigned owner which is our account number 2 and it will no longer be able to withdraw money from the system.



```
    6. Get contract balance
    7. Get Owner Balance
    8. Test Unauthentic users witdrawal
    9. Owner check
    10. Is Owner
    ################################

Enter your choice: 4
Enter password for "rinkeby_test":
Enter password for "rinkeby_test_2":
Transaction sent: 0x2051093090e9c55281987a298cedb84152301e1e5a67cc112e79f61122d46657
  Gas price: 1.430000011 gwei   Gas limit: 32101   Nonce: 12
  FundMe.DeleteOwner confirmed   Block: 10707063   Gas used: 24383 (75.96%)

assigned owner has been removed from the system.
```

Figure 5.37: Removed assigned owner

Now, we have to test if the removed account or anyone who doesn't have any access to withdraw money can withdraw money from the system or not.



```
Enter password for "rinkeby_test":
Enter password for "rinkeby_test_2":
Transaction sent: 0x2051093090e9c55281987a298cedb84152301e1e5a67cc112e79f61122d46657
  Gas price: 1.430000011 gwei   Gas limit: 32101   Nonce: 12
  FundMe.DeleteOwner confirmed   Block: 10707063   Gas used: 24383 (75.96%)

assigned owner has been removed from the system.
Enter your choice: 8
Enter password for "rinkeby_test_2":
('You are not authenticate, Only owner can withdraw.', 0)
Enter your choice: 
```

Figure 5.38: Unauthentic withdrawal detection

As we have removed the ownership of account 2 from the system (Figure 5.37), so it is not allowed to withdraw money. That's why in the figure 4.38, it is showing the unauthentic withdrawal access.

5.5 Theoretical and Experimental Comparison

Now, the paper that we are following to compare with our proposed model is “A framework to make charity collection transparent and auditable using blockchain technology” by Muhammad Shoaib Farooq, Misbah Khan, and Adnan Abid[5]. In that paper, they introduce a new cryptocurrency which is a charity coin based on ethereum. The paper also includes the authenticate donor, and audible charity for government authorities. But in our system, we have worked on a few features which include the system’s security while funding. It also includes the currency converter to make it possible to fund from other countries as well. In addition, our system basically focuses on security, and also the main purpose of our system is to reduce the corruption rate.

In Farooq and Abid’s proposed model, they showed the response time per experience in their paper which is shown below:

Latency per number of block increase in chain (Average of 10 experiments)

Number of Blocks	Latency(ms)
50	156
100	365
150	345
200	543
250	546
300	645
350	567
400	587
450	617
500	789

Table 5.1: Response time (ms) for scientific paper authors Abid, Farouk [5]

Here, table 5.1 is the response time for each experiment of the paper of the charity collection.

Now, in our proposed model, we can calculate response time on the basis of our features. That means the execution process in every account will remain the same. So, here we will differentiate the response time to execute every feature in our system.

Features	**Response time**
Owner check	0.3063 ms
Owner's balance check	0.2831 ms
Owner's withdrawal process	6.212270 ms
Assign new owner	39.51796 ms
Funding	0.046349 ms
Currency convert in Dollar	11.9362285 ms
Currency Convert in Taka	11.9585 ms
Get Contract Balance	0.34818 ms

Table 5.2: Response time for each feature of the proposed model

Here, in table 5.1, is the response time for each experiment in the scientific paper of authors Abid, Farouk. But in table 5.2, it is the response time for each feature of our proposed model. In table 1, per experiment, the response time can be 156 ms to 789 ms. But in our proposed model, to execute per feature it will take 0.304 ms to 40 ms. So, on average to execute the whole system, per account it will take on average 8.3786 ms including the currency converter in dollars. But on the basis of currency converter and also, withdrawal by the assigned owner, the average time may vary. Because the assigned owner may have to go through some process which may cause more time than the withdrawal by the owner itself. So, we can see that it will take less time in our proposed model than the scientific paper of the author Faruk and abid.

On the Other hand, the paper "Blockchain Technology in Fund Management" by D.Fiergbor basically focuses on the mutual fund management system in Ghana [31]. It also introduces the prospects of the technology of fund management in Ghana. But in our proposed model, we have worked on the basis of Bangladesh and other countries as well. Because of the currency converter feature, we can continue the funding process from other countries as well. In addition, we have worked on a few more features like transaction tracking, withdrawal, unauthentic withdrawal tracking, and assigning owner whereas, in D. Fiergbor's proposed model focuses on the mutual fund.

In addition, if we consider about the paper titled “Blockchain for government fund tracking using hyperledger”, here the authors focused on hyperledger playground for transaction testing purpose. They create blocks to represent transaction. In our case, we have used ethereum to maintain transactions by connecting to the polygon network. Because of polygon network it requires less cost and also reduce the transaction time as well. In our proposed model, we ensured the security factors. In addition, the currency conversion through oracle has been done in our proposed model which makes it unique than the fund tracking using hyperledger paper [28].

The paper titled “Proposed solution for trackable donations using blockchain” basically explains about the lack of transparency in the transaction [7]. The system of that paper represents a website where the user can check the whole transaction systems. They used Byzantine consensus algorithm for scalability. But in our proposed framework we used proof of work which is a consensus protocol and smart contract has been used to process whole system. But in their paper, the transaction will take place from dollar to ether. But in our proposed model, donors or users have the option to choose their currency type either in taka or in dollar. So that people from other countries can be encouraged to donate frequently.

Chapter 6

Future Work And Conclusion

6.1 Future Work

In the future, we can include more features in that system to ensure the security of that system. In our system, we only worked on currency converters of taka and dollar. But in the future, we can work on different currencies as well. So, it would be easier to transfer money or take donations from other countries in a very short period of time. In addition, in that system we have not mentioned anything specific about withdrawal amount. For example, how much money can an owner withdraw can depend on the owner as well. On the other hand, in our system, we have a limitation of funding. That means here we have to give at least 50 dollars to donate somewhere. But in the future, we can ignore that part as well. In our work, there is a chance to increase the value of ethereum in the future. So, in that case the system will work according to it. But that is a problem because some people may not make an effort. So, in future, we can use stable coins as a solution to this.

6.2 Conclusion

In this paper, a blockchain based fund management system has been introduced. The system is generic and can be used in a variety of business settings. The system has taken advantage of blockchain properties like irreversibility and security to create a trustworthy-decentralized system. It outperforms the existing standard methods by implementing a more reliable tracking system which would put an end to any wrongdoings or anomalies. And the smart contract authorities are in charge of making sure that practically all of the system's transactions can be tracked. Here we have worked on Ethereum which is very costly to handle. But we used it because Ethereum is a public network. Which means all the records can be visible and accessible by every peer. Here, by using blockchain, we make a structure for fund management where all the transactional data will be recorded. This data is undeletable and unchangeable. Hence, there is no way to corrupt this structure. By this structure, we can keep records of funds of different sectors so that it would be more trustable to rely on this and will help to reduce corruption as well. So, in the government sector or in any organization, this system can be utilized whenever it comes to any trustable fund issues. Moreover, in future development, we can work on safety and security issues of the system as the price of Ethereum value can face some up and down in future. Because, as we used proof of stake in that system which still has 51% attacks and it can be the reason for Ethereum to drop down in the future. In that case, we can include another way to handle this issue by decreasing the percentage of attacks in this system.

Bibliography

[1] "Do you know how to accept donations online?." https://www.littlegreenlight.com/blog/donation-processing-101/, Mar 2022.

[2] K. E. Wegrzyn and E. Wang, "Types of blockchain: Public, private, or something in between," *Foley & Lardner*, 2021.

[3] E. A. FERWANA, *A BLOCKCHAIN-BASED TRACKING SYSTEM FOR UNIVERSITY DONATION*. PhD thesis, 2021.

[4] https://www.researchgate.net/figure/Mindmap-abstraction-of-different-types-of/blockchain-applications-Source-Casino-F_fig1_356924906.

[5] M. S. Farooq, M. Khan, and A. Abid, "A framework to make charity collection transparent and auditable using blockchain technology," *Computers & Electrical Engineering*, vol. 83, p. 106588, 2020.

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

[7] N. S. Sirisha, T. Agarwal, R. Monde, R. Yadav, and R. Hande, "Proposed solution for trackable donations using blockchain," in *2019 International Conference on Nascent Technologies in Engineering (ICNTE)*, pp. 1–5, IEEE, 2019.

[8] Y. Goswami, A. Agrawal, and A. Bhatia, "E-governance: A tendering framework using blockchain with active participation of citizens," in *2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pp. 1–4, IEEE, 2020.

[9] J. Frankenfield, "What is a blockchain wallet?." https://www.investopedia.com/terms/b/blockchain-wallet.asp, Apr 2022.

[10] Simplilearn, "What is blockchain wallet and how does it work? [updated]." https://www.simplilearn.com/tutorials/blockchain-tutorial/blockchain-wallet#:~:text=conceptsView%20Course-,What%20is%20a%20Blockchain%20Wallet%3F,as%20they%20are%20cryptographically%20signed, Feb 2022.

[11] W. C. o. M. 2, "9+ best online payment systems for ecommerce payments." https://www.webfx.com/blog/web-design/online-payment-systems/, Mar 2022.

[12] A. Hayes, “Blockchain explained.” https://www.investopedia.com/terms/b/blockchain.asp, Apr 2022.

[13] T. E. Team, “What is ethereum? a beginner’s guide to ethereum and tips for investing in eth.” https://trading-education.com/what-is-ethereum-beginners-guide, Jan 2022.

[14] “What is polygon (matic)-’ethereum’s internet of blockchains’.” https://forkast.news/what-is-polygon-matic-ethereums-internet-blockchains/, Dec 2021.

[15] https://www.transparency.org/files/content/corruptionqas/Bangladesh_Corruption_Risks_in_PFM_2015.pdf.

[16] https://www.ganintegrity.com/portal/country-profiles/bangladesh/, Nov 2020.

[17] . b. A. Islam and A. A. I. a. Arif, “Contact.” https://lekhapora.org/corruption-in-bangladesh-composition/, May 2020.

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

[19] T. R. . December and T. Report, “61% fund embezzlement in forest projects: Tib.” https://www.tbsnews.net/bangladesh/corruption/61-fund-embezzlement-forest-projects-tib-178726, Dec 2020.

[20] “Tib study: 14% to 76% corruption found in climate change projects.” https://archive.dhakatribune.com/bangladesh/corruption/2020/12/24/tib-study-14-to-76-corruption-found-in-climate-change-projects, Dec 2020.

[21] “When corruption eats the infrastructure development.” https://www.thedailystar.net/editorial/news/when-corruption-eats-the-infrastructure-development-1944725, Aug 2020.

[22] B. Report, “Bangladesh ranks 13th most corrupt country in the world.” https://www.businessinsiderbd.com/national/news/16468/bangladesh-ranks-13th-most-corrupt-country-in-the-world, Jan 2022.

[23] K.-K. R. Choo, “New payment methods: A review of 2010–2012 fatf mutual evaluation reports,” *Computers & Security*, vol. 36, pp. 12–26, 2013.

[24] M. H. Ahamad, “Foreign grants and loans in bangladesh,” 2018.

[25] Bangkok, “What’s happening with aid to bangladesh?.” https://www.thenewhumanitarian.org/report/96902/analysis-what%E2%80%99s-happening-aid-bangladesh, Sep 2017.

[26] J. Kagan, “How funds work.” https://www.investopedia.com/terms/f/fund.asp, May 2022.

[27] “Payment and settlement systems.” https://www.bb.org.bd/en/index.php/financialactivity/paysystems.

[28] A. Mohite and A. Acharya, “Blockchain for government fund tracking using hyperledger,” in *2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS)*, pp. 231–234, IEEE, 2018.

[29] A. Chauhan, G. Savner, P. Venkatesh, V. Patil, and W. Wu, “A blockchain-based tracking system,” in *2020 IEEE International Conference on Service Oriented Systems Engineering (SOSE)*, pp. 111–115, IEEE, 2020.

[30] A. Mehra, S. Lokam, A. Jain, M. Sivathanu, S. Singanamalla, and J. ONeill, “Vishrambh: Trusted philanthropy with end-to-end transparency,” in *HCI for Blockchain: a CHI 2018 Workshop on Studying, Critiquing, Designing and Envisioning Distributed Ledger Technologies, Montreal, QC, Canada*, 2018.

[31] D. D. Fiergbor, “Blockchain technology in fund management,” in *International Conference on Application of Computing and Communication Technologies*, pp. 310–319, Springer, 2018.

[32] J. Lee, A. Seo, Y. Kim, and J. Jeong, “Blockchain-based one-off address system to guarantee transparency and privacy for a sustainable donation environment,” *Sustainability*, vol. 10, no. 12, p. 4422, 2018.

[33] J. Frankenfield, “Smart contracts: What you need to know.” https://www.investopedia.com/terms/s/smart-contracts.asp, Mar 2022.

[34] “Solidity.” https://docs.soliditylang.org/en/v0.8.13/.

[35] “How to deploy a smart contract with brownie.” https://www.quicknode.com/guides/web3-sdks/how-to-deploy-a-smart-contract-with-brownie.

[36] “Creating and deploying a contract.” https://remix-ide.readthedocs.io/en/latest/create_deploy.html.

[37] “Blockchain proof of work - javatpoint.” https://www.javatpoint.com/blockchain-proof-of-work#:~:text=Proof%20of%20Work(PoW)%20is,the%20transaction%20on%20the%20network.