

Prekkha: A Blockchain Based Platform to Track and Provide Financial Aid

by

**Mir Nushrat Zahan Tirumony
181014074**

**Md. Arifur Rahman Md Siam Reza Akash
183014017 183014056**

*Capstone project report submitted in partial fulfillment of the
requirements for the degree of*

Bachelor of Science in Computer Science and Engineering

Under the supervision of

Nafees Mansoor, PhD



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
UNIVERSITY OF LIBERAL ARTS BANGLADESH**

SUMMER 2022

© *Mir Nushrat Zahan Tirumony, Md. Arifur Rahman and Md Siam Reza Akash*
All rights reserved

DECLARATION

Project Title: Prekkha: A Blockchain Based Platform to Track and Provide Financial Aid

Authors: *Mir Nushrat Zahan Tirumony, Md. Arifur Rahman, and Md Siam Reza Akash*

Student IDs: 181014074, 183014017 and 183014056

Supervisor: Nafees Mansoor, PhD

We state that this capstone project report titled *Prekkha: A Blockchain Based Platform to Track and Provide Financial Aid* is the outcome of our own effort excluding the work cited in the references. The capstone project report has yet to be received for any degree and is not simultaneously presented in candidature for any other degree.

Mir Nushrat Zahan Tirumony (181014074)

Department of Computer Science and Engineering
University of Liberal Arts Bangladesh

Md. Arifur Rahman (183014017)

Department of Computer Science and Engineering
University of Liberal Arts Bangladesh

Md Siam Reza Akash (183014056)

Department of Computer Science and Engineering
University of Liberal Arts Bangladesh
Date: November 10, 2022



Department of Computer Science and Engineering
University of Liberal Arts Bangladesh
Mohammadpur, Dhaka - 1207

CERTIFICATE

This is to testify that the capstone project report titled **Prekkha: A Blockchain Based Platform to Track and Provide Financial Aid**, submitted by **Mir Nushrat Zahan Tirumony** (Student ID: 181014074), **Md. Arifur Rahman** (Student ID: 183014017) and **Md Siam Reza Akash** (Student ID: 183014056) are undergraduate students of the **Department of Computer Science and Engineering** has been evaluated. Upon recommendation by the examination committee, we herewith grant our endorsement of it as the demonstrated work and submitted report delivers the requirements for its acceptance in the partial fulfillment of the degree of *Bachelor of Science in Computer Science and Engineering*.

Nafees Mansoor, PhD
Associate Professor

Department of Computer Science and Engineering
University of Liberal Arts Bangladesh

Dr. Muhammad Golam Kibria, SMIEEE
Professor & Head (Acting)

Department of Computer Science and Engineering
University of Liberal Arts Bangladesh

Place: Dhaka

Date: November 10, 2022

ACKNOWLEDGEMENTS

We would desire to convey our genuine and unfeigned appreciation to our research supervisor, *Nafees Mansoor, PhD*, for providing us the opportunity to carry out this research and provide irreplaceable guidance for the duration of the work. His go-getting attitude, vision, sincerity, determination, and motivation have deeply encouraged us. He instructed us on the procedure to conduct the work and to demonstrate the work as clearly as possible. It was a great privilege and honor to work and study under his council.

We are immensely appreciative of our distinguished teacher at the Department of Computer Science and Engineering at the University of Liberal Arts Bangladesh who taught us throughout the course of our study. Unequivocally, their teaching and supervision have altogether transformed us into the persons we are today.

We are tremendously thankful to our parents for their unrestricted love, support, never-ending prayers and caring, and immense support and sacrifices for educating and equipping us with knowledge of the future. We also wish to express our gratuitous gratitude to our friends and our next of kin for their kind encouragement.

In conclusion, we would like to appreciate all the people who have encouraged us to finish the project work in person or otherwise

Mir Nushrat Zahan Tirumony, Md. Arifur Rahman and Md Siam Reza Akash

University of Liberal Arts Bangladesh

Date: November 10, 2022

Dedicated to
my loving Parents

– *Mir Nushrat Zahan Tirumony*

Dedicated to
my loving Parents

– *Md. Arifur Rahman*

Dedicated to
my loving Parents

– *Md Siam Reza Akash*

ABSTRACT

The continuous digitization of financial amenities and money exposes prospects for more comprehensive and systematized financial amenities and economic growth. The five basic needs of modern humans include food, clothing, shelter, education, and healthcare. The modernization of technology over the past few decades has granted engineers and problem solvers the ability to use this technology to fulfill people's demands almost instantaneously. There are plenty of privileged people who are capable of affording good education, healthcare, and all the other necessities that are an integral part of modern humans, but not all individuals are so fortunate. One of the ways of helping underprivileged individuals is through financial aid. And to carry out the whole financial aid process or donation there are plenty of charity organizations in the world. Many people around the world do donate to these nonprofit charity organizations so that they can help people in need. But scandals and corruption regarding charity funds have made donors a bit skeptical about these organizations. Since they really do not know what is happening to their donated money or are able to track them. The donors do not have a secure system that can help track and provide financial aid. This is where the system that we created comes in. Our project "Prekkha: A Blockchain Based Platform to Track and Provide Financial Aid", is an online platform that is specially designed to track donations and make sure that students, patients, and children from orphanages get the donation requested by them. The primary technology behind this system is blockchain and smart contracts. Through the use of blockchain, we are able to mitigate the number of middlemen and greatly reduce the risks of corruption or money mismanagement by an organization. Our system will give donors more control over what is happening to their donated money. And every record of any sort of transaction will be stored in the blockchain, so no one will be able to alter the records.

Keywords: blockchain, fintech, donation, smart contract

Contents

1	Introduction	1
1.1	Background	2
1.1.1	Blockchain	2
1.1.2	Mining	4
1.1.3	Smart Contract.....	4
1.1.4	Ethereum	5
1.1.5	Non-Profit Organizations	6
1.2	Motivation	7
1.3	Problem Statement.....	8
1.4	Aims of the Projects	8
1.5	Outline of the Report.....	8
2	Literature review	9
2.1	Introduction	9
2.2	Existing Systems without Blockchain.....	9
2.2.1	Summary of the Existing Systems without Blockchain.....	9
2.2.2	Metrics Definition for Existing Systems without Blockchain .	11
2.2.3	Analysis of the Systems without Blockchain	12
2.3	Existing Systems with Blockchain	14
2.3.1	Summary of the Existing Systems with Blockchain	14
2.3.2	Metrics Definition for Existing Systems with Blockchain.....	23
2.3.3	Analysis of the Systems with Blockchain.....	25
2.4	Conclusion	31
3	Methodology	32
3.1	Introduction	32

3.2	Software Process Model	32
3.3	Required Tools	35
3.3.1	Web Tools.....	35
3.3.2	Blockchain Tools	36
3.3.3	API Tools.....	38
3.4	Conclusion	38
4	The Proposed System	39
4.1	Introduction	39
4.2	Block Diagram	39
4.3	Activity Diagram.....	40
4.3.1	Admin Activity Diagram.....	40
4.3.2	Donor Activity Diagram	41
4.3.3	Acceptor Activity Diagram.....	43
4.4	Use Case Diagram	44
4.5	Data Flow Diagram (DFD)	45
4.6	Conclusion	47
5	Implementation & Analysis	48
5.1	Introduction	48
5.2	Workflow of Prekkha.....	48
5.3	UI Design & Analysis.....	49
5.4	Smart Contract.....	59
5.5	Exception Handling	59
5.6	Analysis	59
5.7	Security.....	60
5.8	Cost Analysis	61
5.9	Conclusion	62
6	Conclusion	63
6.1	End Words	63
6.2	Social, Legal, Ethical & Environmental Issues.....	63
6.3	Future Works.....	64
	References	66

List of Figures

1.1	Blockchain Working Process.	3
1.2	Ethereum Network.....	6
3.1	Agile Scrum Process.....	33
3.2	Agile Model Iteration Process Flow	34
4.1	Block Diagram of Prekkha.	40
4.2	Admin Activity Diagram of Prekkha.	41
4.3	Donor Activity Diagram of Prekkha.	42
4.4	Acceptor Activity Diagram of Prekkha.....	43
4.5	Use Case Diagram of Prekkha.	44
4.6	Level-1 Data Flow Diagram of Prekkha.....	45
5.1	Workflow of Prekkha.	49
5.2	User Login Registration Page.....	51
5.3	Aid Request Page.....	52
5.4	Donors Dashboard.	53
5.5	Donors Dashboard.	54
5.6	Transaction Completion.....	55
5.7	Admin Dashboard.....	55
5.8	Admin Dashboard.....	56
5.9	Admin Dashboard.....	56
5.10	User Creation in Blockchain.	57
5.11	Transaction of a Donation.	57
5.12	Amount Update.....	58
5.13	Acceptors Getting Their Aids.....	58
5.14	Blockchain Transaction of Prekkha.....	60

List of Tables

2.1	Analysis Table of the Existing Systems without Blockchain	12
2.2	Analysis Table of the Systems with Blockchain	26
5.1	Tentative Budget of Prekkha	61

Chapter 1

Introduction

Education and healthcare are some of the basic human requirements that need to be fulfilled to become a functioning part of society. These two requirements constitute the lower part of Maslow's Hierarchy of Needs pyramid (54). But most people in our community are not lucky or privileged enough to achieve these two basic needs. Recently, technology has been rapidly evolving. We can observe how far technology has come when we look back ten years and contrast it with the present. Numerous changes have been brought about by the advancement of technology in several fields. Additionally, in order to adapt to modern living, people constantly change their lives. Our daily lives have undergone tremendous change as a result of the internet's rapid development. Everywhere, from sharing a moment with a buddy to ordering pizza to begin a relationship, the internet has an impact, so it will be effective if we use online platform to help someone instant. The globe has undergone a significant change since being born online. This is where our system comes in to help. It is a blockchain-based financial aid system. This system will allow its users to give and receive donations, which the system will track to mitigate corruption and irregularities in the distribution of donated money.

Blockchain is an emerging technology that has been around since 1991, which was introduced by Stuart Haber and W. Scott Stornetta (2). But gained a massive boost in popularity after publishing a white paper on Bitcoin by someone or a group of people by the pseudo name Satoshi Nakamoto (2). A blockchain is kind of a shared database where the pledged block is immutable and is organized in the list in sequential order. The blockchain is mostly replicated by nodes that distrust one another and is sequentially chained by a hash. Early decentralized payment

systems, such as Bitcoin (3), Ethereum (4), and Mixcoin (5), made transaction data, including sender and receiver addresses and transferred value, public in order to guarantee the stability of the blockchain ledger. An electronic coin can be defined by a series of digital signatures. The proceeding transaction which has a hash that has been digitally signed and the public key of the following owner are incorporated into each transaction. While the public key is used to verify the transaction, the private key is utilized to sign the transaction (39). This will be perfect if utilized for the banking industry, as banks might cooperate on the same blockchain and push customer transactions (1). Many organizations work with donations but all the donations in those specific organizations go through multiple middlemen. But this system excludes all intermediaries and allows users to directly donate to the beneficiary, thus reducing the possibility of corruption. The use of decentralized blockchain technology, which doesn't put a middleman between the donor and beneficiary and encourages transparency and confidence, in donation systems. Therefore, without messing with the previously saved data, this technology generates and stores contracts and monitors the flow of funds inside the network.

1.1 Background

1.1.1 Blockchain

Software systems can have two primary architectural approaches, they are centralized and distributed (40). The advantages of a distributed system are many, for example, the computing extent of all the connected nodes can be used to enhance computing power by pooling them, increasing the dependability of the system by not having a single point of failure, and many more. And like every other technology it has disadvantages too, such as security issues created by untrustworthy nodes misusing the network and communication cost (41).

Blockchain can be regarded as an element of a decentralized and distributed software system's application layer. Blockchain technology (Figure 1.1) can be utilized to attain and preserve the integrity of data in distributed networks (7). Additionally, blockchain might be viewed as a wholly peer-to-peer network made

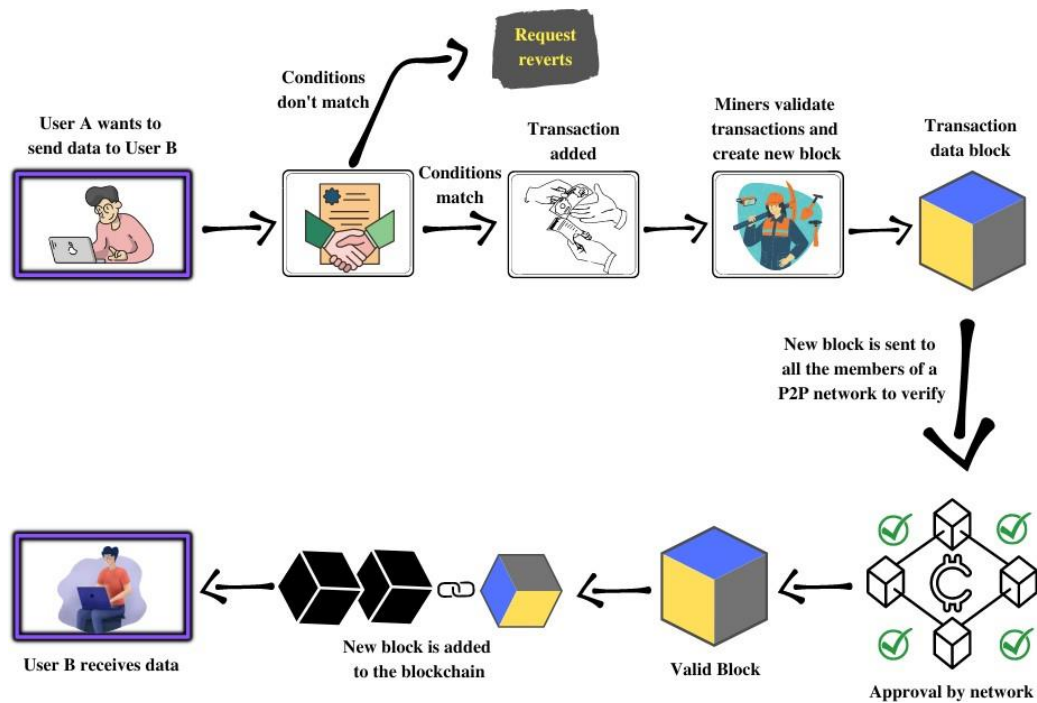


Figure 1.1: Blockchain Working Process.

up of individual nodes. In peer-to-peer systems, the main threat to the integrity of the system is via dishonest and malevolent nodes. Blockchain is a collection of connected blocks that operate on a peer-to-peer network with no single point of failure since the blocks are linked together using cryptographic hash codes. Due to the fact that other nodes in the peer-to-peer network will continue to function even if a few nodes fail, blockchain is more dependable to run and maintain. With public-key cryptography, in which each agent is provided with a private key (kept secret like a password) and a public key distributed with all other agents, blockchain technology ensures the eradication of the double-spend problem (2). When the next owner of the coins (or digital tokens) delivers the first owner their public key, a transaction is started. The digital hash signature is used to transmit the money. Public keys are generated via cryptography and saved as addresses in a blockchain. Each coin has a transaction and a corresponding address, in a simple exchange of

coins from one address to another constitutes the crypto-economy. The blockchain's distinguishing characteristic is the lack of connection between public keys and actual identities. Although users do not trust one another or there are unreliable users in the network, it allows for trustless and reliable transactions without the need for centralized management. Since then, blockchain has garnered a lot of interest for its decentralized transaction ledger capabilities, which may be used to transfer payments or contracts or to register, confirm, and send transactions (41). Beyond financial transactions, blockchain technology has been used in a variety of industries and applications, including real estate, utilities, healthcare, and government (42). Blockchain technology has the potential to significantly improve a number of financial industry operations, including trade finance, payments, the settlement of securities, and regulatory compliance (5). Blockchain's first focus was on integrating cryptocurrencies with traditional banking and financial institutions. Financial institutions can conduct their financial operations directly between themselves without the use of centralized authorities or middlemen thanks to the innovative banking ecosystem that blockchain technology enables. Every transaction needs to be verified with the consent of at least 50% of network participants (43).

1.1.2 Mining

Adding a new block to the blockchain is done through mining. Each node utilizes blockchain to check to see if the coin is valid and has not already been spent. A larger group of parties come to an agreement before the transaction records are added to the blockchain. Since mining requires a lot of resources, it is difficult for an attacker to validate a bad transaction. Each mined block is examined to determine whether it possesses a legitimate proof of stake (45) or proof of work (44).

1.1.3 Smart Contract

Smart contracts are self-regulating and self-driven programs that trigger the terms and conditions of a specific consensus or contract using Turing complete codes and computational framework. Smart contracts are a part of the use of distributed ledger. It works as a decentralized program of the blockchain network. The essential characteristics of the smart contract are implementation in a peer-to-peer manner without the involvement of a centralized mediator and service accessibility without

any centralized dependencies. The self-governing implementation in line with the predetermined conditions makes the contract smart. Smart contracts can amplify flexibility and ease the exchange of property, money, shares, service, or anything of value in mathematically computerized and ways that avoid conflict (51).

1.1.4 Ethereum

A group of nodes running Ethereum clients makes up an Ethereum network (Figure 1.2). These nodes each have a copy of the blockchain, which documents all transactions made on the network. Ethereum aims to equip developers with a platform that can be of service as the starting point for all transaction-based state machine ideas. Any developer can deploy Ethereum, a peer- to-peer system of virtual machines, to run distributed applications (DApps). To store, run, and secure contracts cryptographically, Ethereum employs its own decentralized public blockchain. Ethereum aims to develop an alternative protocol for developing decentralized applications. With a distinct set of tradeoffs that we think will be particularly beneficial for a wide range of decentralized apps. Ethereum makes sure of swift development time, security for small-scale and seldom-used applications, and the capability of different applications to be exceedingly efficient by establishing a blockchain with a programming language that is already integrated. In Ethereum, the state is composed of things referred to as "accounts," each of which has a 20-byte address, state transfer value, and information between accounts. The accounts contain four fields (i.e. nonce, ether balance, contact code, and storage (52)). The Ethereum "contract" are more similar to "autonomous agents" that exists inside the Ethereum execution environment, always perpetrating a particular piece of code when prompted by message or transaction, having total authority over their own ether as well as their own key/value store to monitor the persistent variables. They should not be considered something that needs to be "achieved" or "complied with."

Transaction in Ethereum: In Ethereum, the transaction means the signed data package node to be transmitted from an extrinsic controlled account. It contains a signature that recognises the sender, the receiver, amount of ether, it has STARTGAS and GASPRICE. A STARTGAS value, which denotes the highest number of computing phases the transaction completion is permitted to take. GASPRICE value denotes the charge the sender pays per computational step. An incentive for

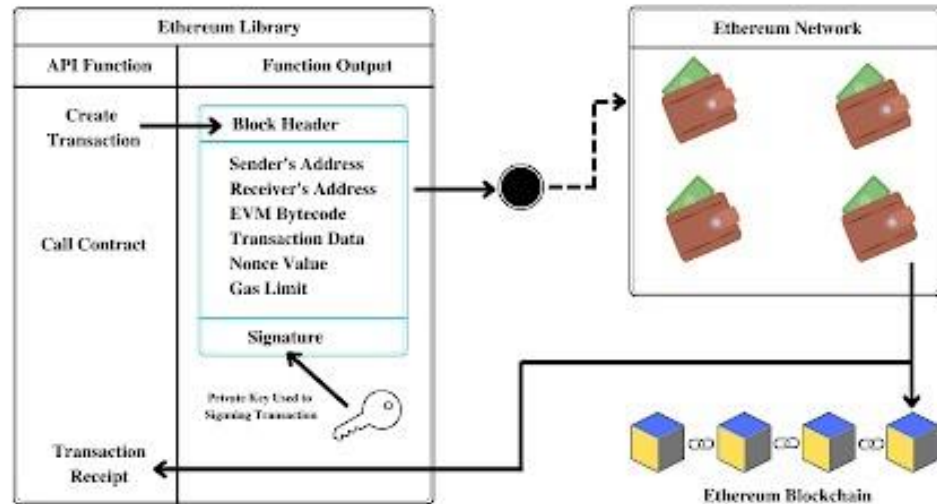
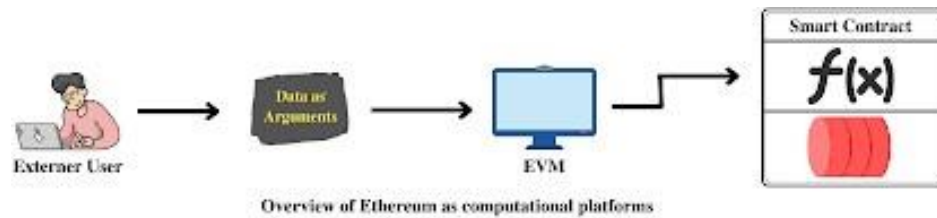


Figure 1.2: Ethereum Network.

a transaction to be completed is gas, a predetermined quantity of ether delivered to the node processing the transaction that is proportionate to the computational difficulty of the transaction. Due to this incentive scheme, contract creation time is influenced by system load and contract complexity.

1.1.5 Non-Profit Organizations

A regulated, non-commercial, non-profit legal entity is referred to as a non-profit organization (55). Unlike an entity that is publicly owned, it is privately owned, serves the public good, and it is tax-free. It is a business that runs for profit for its owners. Typically, these groups work in the fields of education, science, charity, literature, religion, or organizations for professionals. Donations from its founders and members are frequently possible, the majority of which are tax-free. Additionally, non-profit organizations represent a collection of private, philanthropic, and

nonprofit organizations and associations. Because of their significant influence, they are seen as the third branch of government and are compared to community institutions (whether in the public or private sector). Numerous instances from all across the world demonstrate how non-profit organizations have developed into significant social sectors in addition to becoming important economic sectors as a result of the economic significance of their activity. These organizations focus on a variety of things, including the prevention and alleviation of poverty, the advancement of education, the enhancement of health services (including the prevention and mitigation of sickness or human suffering), and social and communal advancement (including care). The constituent database and the merchant account make up the three parts of the non-profit organizations' online donation system. Donor and donation information is kept in the constituent database, sometimes called the Constituent Relationship Management Database (CRM) (56). A merchant account is a type of bank account designed specifically for nonprofit organizations (or businesses in general) that manages funds from the credit card company of the donor and deposits them into the nonprofit's bank account. Transaction fees (a percentage plus a certain amount) make up merchant account fees (13).

1.2 Motivation

There were lots of things behind for motivating us to work on this project, but firstly to fulfill the requirements which were needed for completion of graduation. The main reason we work on this project is that not a single platform across the country can offer to the donors that helps them to track and provide donations ensuring their money will be utilized properly. Moreover, beneficiaries do not get their actual donation amount. We were tried to solve the regular but major problems of the donors as well as beneficiaries. As a donor, the idea is simple to solve their problem but there was lots of complexity in this project as a developer, which is actually challenging us & at the same time motivates us to work on this project. By working on this project, we are trying to make a significant change in current donation methodology. We are trying to make trustworthy traceable donation platform. We are trying to ensure donations provided and utilized properly from donors to beneficiaries.

1.3 Problem Statement

The corruption related to the proper usage and distribution of funds in charity organizations has made donors around the world more hesitant and skeptical towards donating to these organizations. One of the leading causes of this sort of corruption is the middlemen involved in the donation process.

1.4 Aims of the Projects

- * Create a blockchain and smart contract-based web application for donation.
- * Give donors the ability to choose the individual to whom their donated money will be given.
- * Significantly mitigate the number of middlemen in the donation process.
- * Help beneficiaries with financial aid, so that students do not drop out, patients have to delay their medication, or orphans get to lead a comfortable life.

1.5 Outline of the Report

The following portion of our report covers the literature review of the existing works with and without blockchain. This section has a subsection that has an analysis of the available related systems and the metrics through which we analyzed them. The latter subsection has the same structure as before but these are systems with blockchain. Next is chapter 3, which is the methodology, which includes the software process model used in our system, next section is the required tools. Next is chapter 4, which consists of a block diagram, activity diagram, use case diagram, and DFD, that will help explain our system. Chapter 5 is the implementation of our proposed system. This includes workflow and UI design, smart contracts, exception handling, analysis, security, and cost analysis. Finally, chapter 6 includes a summary of social, legal, ethical, and environmental issues, and finally the future work.

Chapter 2

Literature review

2.1 Introduction

During the research period for our project, we had to go through plenty of systems and papers which were related or similar to our proposed system. This was done so that we could figure out the flaws of other systems and avoid those and learn how other people avoided such mistakes. This greatly improved and helped optimize our system. The technology that we use to develop the system was blockchain and smart contract. Hence, we had to study systems that were both blockchain-based and non-blockchain based. In this section, we put forward all our findings that include performance metrics, and then the analysis of those metrics in their respective systems.

2.2 Existing Systems without Blockchain

In this section, few existing systems without blockchain are studied and analyzed through metrics which are defined below:

2.2.1 Summary of the Existing Systems without Blockchain

Feeding America (58) is one of the biggest hunger-relief charities working in America that is fighting to end hunger. Their mission is to advance the change in America by safeguarding unbiased access to healthy food for all. They associate themselves with food banks, food pantries, and local food drives to secure food for people facing hunger. They do this by raising funds, hosting food service, partner with

companies, which is then distributed through the help of volunteers.

Habitat for Humanity (59) is an international Christian mission-based organization that helps everyone in need regardless of their race, religion, or background. They are active in 70 different countries. They mainly take donations from different campaigns and use that money to build infrastructure for impoverished communities, most of this infrastructure is home to locals. Their advocacy endeavour focus on policy improvement to eliminate systemic barrier that blocks low-income families from getting access to adequate housing.

Saving the Children (60) is an international organization that mainly focuses on underprivileged children from poverty-stricken, underdeveloped, or developing countries. It was founded by Eglantyne Jebb in 1919. The organization is now working over in 100 countries every day and in times of crisis and distress to give the children a safe and healthy life.

Jaago Foundation (61) is a charitable organization that is based in Bangladesh. They work in different fields education, youth, women, and climate change. It has been providing free of cost, quality education for the underprivileged children. They have dramatically transformed the quality of education in the remote areas. They work with youth groups to increase meaningful participation of youth within their communities, enhancing their skills, providing opportunities, and promote healthy relationship so they may raise on their collective leadership.

Bidyanondo (62) is a Bangladesh-based charity organization which was founded by Kishor Kumar Das in 2013, that focuses on helping pregnant women, orphan-ages, winter care, and their most popular campaign “One Taka Meal”. They do this work by taking donations from donors and distributing them via volunteer that work for them. They also allow a donor to specifically sponsor an underprivileged child.

BRAC (63) is an international charity organization, that focuses on different sectors of helping people in need. They take donations from donors, partner with other companies, and campaign to raise money and awareness for underprivileged

people.

Work for Humanity (WFH) (64) is a non-profit organization that originated in Bangladesh. They focus on education, health, emergency response, and awareness. They like other charity organizations take money from donors and distribute it through volunteers. They are working to remove illiteracy from Bangladesh. They want to make sure that they everyone is aware of their right and increase awareness about child marriage. They also want to make sure that people learn and know about easily avoidable disease.

Dhaka Ahsania Mission (65) is a non-profit organization established by Khan Bahadur Ahsanullah in 1958. It envisions a society that encourages humanity, equality, spirituality, humility, and caring nature. Their mission is to provide high quality amenities towards peace, unity, and development of spiritual and social life for both human community and the underprivileged and suffering humanity in particular.

2.2.2 Metrics Definition for Existing Systems without Blockchain

- a. **Update:** User can update their personal information and get notification regularly.
- b. **Tracking:** Donors are able to track their own donation.
- c. **Details:** Details about the person who is getting the support of donors.
- d. **Overview:** Users can see live overview of the particular organization/charity. For instance, number of donors, number of beneficiaries, area coverage, current charity projects etc.
- e. **Cause:** Donors are notified about the specific reason of donation.
- f. **Utilization:** Donors are ensured that their donation is utilized properly and acceptors got the full of it.
- g. **Middlemen:** If there are middlemen in that particular organization/charity to distribute the donation among the beneficiaries or not.

2.2.3 Analysis of the Systems without Blockchain

Not all systems or organizations use blockchain and smart contract technology to donate or distribute money. Most of them use Web 2.0 for their system. We also studied the system used by these organizations and put forward a performance metric to compare our system with. In this section, we discuss these systems and put forward an analysis.

Table 2.1: Analysis Table of the Existing Systems without Blockchain

Organizations	Update	Tracking	Details	Overview	Cause	Utilization	Middlemen
Feeding America	N	N	N	N	Y	N	Y
Habitat for Humanity	N	N	N	N	Y	N	Y
Save The Children	N	N	N	Y	Y	N	Y
Jaago Foundation	N	—	Y	Y	Y	N	Y
Biddyanando	N	Y	Y	Y	Y	N	Y
BRAC	N	N	N	Y	N	N	Y
WFH Foundation	N	N	N	Y	N	N	Y
Dhaka Ahsania Mission	N	N	N	Y	N	N	Y

Feeding America (58) is one of the biggest charities working in America that is fighting to end hunger. They associate themselves with food banks, food pantries, and local food drives to secure food for people facing hunger. They do this by raising funds, hosting food service, partner with companies, which is then distributed through the help of volunteers. The first issue with feeding America is that there are plenty of middlemen in the process which will definitely lead to mismanagement of the donated food or money. There is no way to update once you have donated. There is no way to know to whom the donated food or money is going; the donation cannot be tracked. There is visual photo evidence but these photos can be easily faked. This organization is only limited to America.

Habitat For Humanity (59) is an international Christian mission-based organization that helps everyone in need regardless of their race, religion, or background. They are active in 70 different countries. They mainly take donations from different

campaigns and use that money to build infrastructure for impoverished communities, most of this infrastructure is home to locals. But they have some flaws in their system. You cannot track the money you have donated. You do not know the details of where the money is going. There is no guarantee that the money is utilized properly as it goes through multiple middlemen before it reaches its destination.

Saving the Children (60) is an international organization that mainly focuses on underprivileged children from poverty-stricken, underdeveloped, or developing countries. But this organization like others suffers from the same flaws. There are many middlemen that might lead to mismanagement of the donation. The donor has no idea how their money is being utilized or to whom they are going. There is no way to track the donation.

Jaago Foundation (61) is a charitable organization that is based in Bangladesh. They work in different fields education, youth, women, and climate change. Here a donor can donate but cannot track where the money is being utilized. They have a blog that gives updates about how the donation is utilized via photos or videos but there is no other way to verify it. They also distribute donations through volunteers so the mishandling of donations might be in question.

Bidyanondo (62) is another Bangladesh-based charity organization that focuses on helping pregnant women, orphanages, winter care, and their most popular campaign “One Taka Meal”. They take donations from donors and distribute them through their volunteers. And many organizations that were explored previously, have no way to track the donations or where the money is being utilized.

BRAC (63) is an international charity organization, that focuses on different sectors of helping people in need. They also take donations from donors, partner with other companies, and campaign to raise money and awareness for underprivileged people. They too distribute most of their donations through volunteers, thus adding middlemen to the mixture. There is no tracking of the donation or where the donation is being utilized.

Work For Humanity (WFH) Foundation (64) is an organization that originated in Bangladesh. They focus on education, health, emergency response, and awareness. They like other charity organizations take money from donors and distribute it through volunteers. This raises the same problem, with too many middlemen there is a high chance that there will be mismanagement of donations and there is no way to track donations. Donors do not know whether their donation is being used properly.

Dhaka Ahsania Mission (65) is a charity institute that focuses on helping people in need. Similar to other organizations they also distribute their donations through volunteers, which might lead to mismanagement. There is no way for the donations to be tracked. There is no way to update information. No details about how the donation is being utilized.

2.3 Existing Systems with Blockchain

In this section, few existing systems with blockchain are studied and analysed through metrics which are defined below.

2.3.1 Summary of the Existing Systems with Blockchain

This sub-section discusses the summary of the paper we have reviewed till now. We have discussed how the system works, the underlining technologies used, and how it benefitted their systems.

This system (13) functions similarly to paper money in that there are platforms that oversee and control investor communications and private fundraising activities in an effort to promote trust and security in financial transactions. The donor goes to the non-profit organization's website, peruses the projects, and selects the project for which he wishes to make a donation. The payment gateway transfers the credit card details after the donor enters their information on the website. Some entities must keep track of the credit card billing time for recurring information in each time period. A transaction is authorized almost immediately, informing all parties

whether or not it will be completed within the allotted time frame which could be hours or even a whole day before the transaction is formally completed. Using decentralized blockchain technology, which mitigates the need for a middleman between the donor and beneficiary and encourages transparency and confidence, has been essential for these projects' donation systems. The donor can monitor the transfer of cash to their beneficiaries, enhancing transparency and building trust to guarantee the process's overall success. Using data on student aid from a typical institution in northern Jiangsu Province in 2018, this study looked at the attributes of student aid work in local colleges. Due to the fact that student loans must be returned, college students are less likely to apply for them than they might be for other types of help that have no payback obligations and no academic performance criteria.

This study (14) suggests a blockchain-based monitoring procedure for the forms in banks and the accountability of people involved in the banking process of Islamic banks. But in most countries where Islamic Banking is offered as an alternative to traditional banking, blockchain and smart contract technology are not legally recognized or are being scrutinized by government regulatory boards. This study puts forward the utilization of blockchain and smart contracts in supervising the personnel involved in the dealings of all the important processes to ensure transparency in Islamic banking. The personnel to be supervised includes Sharia supervisor boards, contributors, governmental regulators, and beneficiaries (14). This study claims that the addition of blockchain technology to Islamic finance can be beneficial. The benefits are no single point of failure, identify fraud quickly, the users of the blockchain network can oversee, and track transactions, altering the chain or the transactions in it is also computationally infeasible. The regulatory process can be simplified by the use of smart contracts. The service cost associated with the financial contracts and other services can be reduced by 95%. It uses the Blockchain Management System (BMS) as an accounting system. In the domain of crowd-funding, identifying whether the agent is acting in the interests of the stakeholders is a major concern. The next phase of the paper talks about how blockchain and smart contracts are used in payment systems to increase the speed of transactions, make the process more efficient, solve the double spending problem, reduce fraud, and allow auditing of the completed transactions. It also discusses how different

hashing algorithms are utilized to secure user data.

In this research (15), the local blockchain networks, like Ethereum, are made up of miners, retailers, and normal users in the proposed system, thus payment operators build many substitute nodes that are sporadically attached to remote communities in this study, distributed verification guarantees provided by blockchain technology were utilized to develop a unique digital payment methodology that can be installed on top of a network. The Utilization of smart contracts for payment amenities management, such as user account initiation, interactions with the credit operator, and management of rewards for blockchain miners. The objective is the construction of a low-cost and secure digital payment system based on a private Ethereum blockchain. Furthermore, it is demonstrated that block creation and transaction processing are closely coupled, and with a big enough block size, the transaction processing time is not affected by the transaction arrival rate. This paper demonstrates that the Proof-of-Work (PoW) (2) difficulty adjustment does not slow down transaction processing and that even with unpredictable miner availability, the average block generation time is largely stable. Session time-outs could impact USSD and SMS messages could be easily spoofable, hence, for security additional user verification is required. Early-generation token payment platforms protected by time-lock puzzles are another type of micro-banking system. IBM also suggested the Micro-iKP protocol, which uses "coupons" that are transferred between participants and confirmed by the bank, to handle frequent micropayments. However, this plan raises the expense of communication (3). For proxy node synchronization, currency exchange transactions only happen when the proxies are disconnected. In contrast, regular transactions arrive both when the proxies are linked via the back-haul link and when they are disconnected. Here, we anticipate that the times between connections and disconnections will be substantially longer than the block time. They have used (Equation 1),

$$PVC = nU(\sum_{i=1}^{nU} Ti = Tu) \quad \text{and} \quad nC(\sum_{i=1}^{nC} Ti = Tu) \quad (1)$$

according to the number of blocks produced when joined and separated. A single disconnected period's worth of transactions can tally up to sU. They have

proposed a solution in this paper that is intended to address the issue of latency in

Blockchain networks with respect to providing real-time services that are paid for cryptocurrency. They have proposed a remedy that runs off-chain, which makes agreements easier between the suppliers and the clients. It controls slack payments. a business deal signifies a transfer of cryptocurrency among multiple nodes that run within the primary network. This publication introduces the Latent Algorithm for Transactions. It completes all the hidden transactions that are logged on the ledger up until then. Another system offers a peer-to-peer electronic cash system by which Online payments can be made directly between clients, doing away with the need for a reliable middleman. Using a peer-to-peer network, the double spending issue can be resolved. Transactions that have the opposite impact of their intended purpose would protect sellers from fraud. An electronic coin can be defined by a series of digital signatures. By signing a hash of the prior transaction with the subsequent owner's public key, each owner transfers proprietorship of the coin to the next. A payee can check the signature to confirm the ownership chain.

In this system, "FastPay (16)" blockchain's distributed ledger acts as the backend for the system to guarantee the accuracy of the payments through the system on frontend IoT devices. However, quick payments are frequently required in such a scenario, there is still no consensus on how to do so. In the context of quick payments, blockchain-based systems protect against double-spending attacks. They suggest FastPay as a solution for establishing safe quick payments in edge-IoT systems supported by blockchains in order to convey this issue. The effectiveness of FastPay is demonstrated by preliminary testing on the prototype (16).

A blockchain-based multi-keyword ranked search with a fair payment (BMFP) system that utilizes a smart contract to automatically carry out fair payment activities. The system also checks the accuracy and completeness of the search results, and multi-keyword ranked search results that are checkable by the public. The smart contract's verification algorithm is economical and the BMFP is compatible with Ethereum (17). The cloud platform provides rapid services for distant computing and storage, making it easier to access and use data whenever and wherever. Traditional payment methods have a number of drawbacks, including the need for a completely reliable party, and the possibility of data owners or users' privacy being compromised. The smart contract of the system for BMFP ensures that the

data user receives an accurate and comprehensive search result, and the service and the result will be conveyed to the data owner and the cloud respectively. And in the event, that they are not, the data users' fees will be refunded to their account. They used the weighted zone scoring method (17) to calculate the importance of the relevance score. Here, they define zones, as t , and defined weight, such that (Equation 2),

$$\sum_{j=1}^t g_i = 1; \text{ For } 1 \leq i \leq t \quad (2)$$

Then, s_i - is the score of the presence or absence of keyword w . Weighted zone score, defined as (Equation 3),

$$S_{w,F} = \sum_{j=1}^m S_{wj}, F \quad (3)$$

In their system, DU(data user) asks for search authorization, and DO (data owner) uses the user management smart contract to grant DU the right to conduct searches. Then, DO provides DU with the key for the allowed search. The BMFP system has seven algorithms. They use Java to create the searchable encryption algorithms in BMFP and Solidity to build Ethereum smart contracts. The message authentication code function is instantiated by HMAC-SHA256, and the pseudo-random function is instantiated by HMAC-MD5. Since BMFP uses searchable encryption and blockchain.

DAP (fully decentralized anonymous payment) systems (18) can be misused for ill motives, such as internet extortion and money laundering. The study provides a novel definition of Decentralized Conditional Anonymous Payment (DCAP) and outlines the relevant security requirements in order to acknowledge the significance of regulation. First, a Condition Anonymous Payment (CAP) scheme is created (based on the signature of knowledge) whose security can be proven using the described formal semantic and security models in order to build a concrete DCAP system. They contrast the performance of their proposal with that of Zerocash in identical testing conditions to show their approach's benefit (18).

The paper (19) reviewed suggests a paradigm that focuses entirely on blockchain related tasks. Their primary goal is to create a safe payment system that will allow

users to conduct regular transactions with ease. The miners who validate the transactions will totally manage the system. The task of the Certificate Authority (CA) has been separated from the miner in the suggested system so that it can handle more requests than the prior system. The outdated approach takes substantially longer to process requests than the suggested system because the Certificate Authority (CA) does all of the work (19).

The suggested scholarship administration architecture involves numerous parties and procedures, ensures document integrity and openness, and, most crucially, allows eligible people to receive a scholarship to be approved by automated rules (20). This system uses two smart contracts for evaluating the student information and the other one for tracking and reissuing the scholarship. The proposed solutions employ Oracle services of those parties, so that automated verification may be done. Turkish government agencies "Mernis", "Minister of Youth and Sports", "Ministry of Health", "Ministry of Family, Labor and Social Services", "SYM", and "YK Student Information System (YKSS)" must provide the necessary data flow.

The mechanism to handle Indian college students' scholarship applications was suggested in this system. The state education board checks the applicant information using the proposed mechanism, which uses a smart contract to collect student applications. The system then uses blockchain to record payments. The proposed work varies from existing work in that it employs smart contracts for payments instead of traditional currency. In contrast, their solution exclusively uses blockchain to log payments (21).

This paper (22) talks about how blockchain is utilized to keep track of the donations provided by donors. In this work, they present a system for donating rice to an IoT-based orphanage that involves installing a large sensor in each orphanage and using Raspberry Pi devices to connect them to one another. When an orphanage is short on rice supplies, donors might use an application to keep track of the foster care situation. After the transaction, suppliers can send the rice to the destination. Blockchain technology and smart contract platforms allow all transactions among providers and contributors to be monitored and made public for increased security. The outcomes of using the suggested technique in 4 orphanages may be established,

which will help the donors (22). Every location has a unique IoT device with an indicator that alerts users when there is a rice scarcity situation. When the proposed rice has arrived at the target and collided with the rice compartment, the IoT device will alert the donor. After the rice has been delivered, the supplier will continue to switch sides with the provider and respond to the donor. This network was created utilizing Ethereum and additional transactions, enabling all parties to record and maintain IoT data and user transaction data on both sides. This method is used to lessen data manipulation by suppliers, donors, and providers. They create an Android-based mobile programming tool that enables users to create IoT projects with GUIs without using the Raspberry software Pi's and middle-ware, which manages data streams, device drivers, and connections between software and hardware. In a peer-to-peer network where each device will use blockchain technology in its transaction process, each IoT device should be installed in an orphanage, according to the research (22).

This paper (23) discusses how blockchain and smart contracts are utilized to provide a better mechanism for the banking system to provide services to the people. By acquiring more fruitful mechanisms than are now in place, blockchain technology can optimize the world's financial infrastructure and recommend sustainable development. In fact, to encourage economic growth and speed up the development of green technologies, many organizations are currently concentrating on blockchain technology (23). They examined the real performance of the Bitcoin system while also emphasizing some of its key shortcomings in order to comprehend the potential of blockchain technology to support the financial system (23). In this work, they look into the possibilities of blockchain technology and the pioneering role it might play in tackling sustainability and environmental concerns. They believe that the development and application of this technology in the future could completely alter the financial industry. A recent report predicts that blockchain based systems could bring significant future cost savings. It gives us a serious point to ponder about the potentialities of blockchain technology that, if exploited and developed in an adequate manner, could bring legitimate support to the actual financial system. This paper identifies numerous errors that call into question its viability. The most significant issues that could jeopardize the viability of the Bitcoin system are the threat of 51 percent assaults, the dominance of ASICs (Application

Specific Integrated Circuits), and excessive energy inefficiency. Although transactions in blockchain technology are nearly instantaneous, miners must confirm them. The amount of time it takes to confirm a block on average depends on the consensus method. One block is validated for Bitcoin every 10 minutes, one for Nxt every few seconds, and one for Ethereum each minute. The highest number of transactions per second (tps) that may be processed is impacted by this. There are currently 7 tps in the Bitcoin system on average (23).

The EduCTX (24) platform serves as the foundation for the EduCTX effort, which anticipates that diverse HEIs will collaborate to establish a universally efficient system. This study built and executed a smart contract for the Central Sector Scholarship Program for College and University Students. There were a number of issues with the CSS Scheme's current application process, including the inability to track application forms, the loss of application forms during Indian Postal Service delivery, a lack of communication between students and the Education Boards, and the absence of bank account verification. They were able to achieve transparency between the student entity and the Education Board entity. The CSS Scheme has been automated, so students are no longer faced with the problem of application forms getting lost in the mail. The automated system has several checkpoints in place to monitor application forms. Therefore, the suggested solution was successful in overcoming the aforementioned challenges. The four components of the CSS Scheme are the Education Board, Students, Colleges, and Banks. The CSS Scheme's blockchain-based Smart Contract offers students a user-friendly environment and upholds a transparent link with their individual Education Boards (24).

This paper (25) proposed a CSS scheme using a blockchain-based smart contract. Blockchain technology, which offers decentralization and tamper-proof records, powers a smart contract. The CSS Scheme's Smart Contract will automate the current system and lessen the demand. Consequently, the time required by physical work is reduced. For implementing this system, they used Solidity and Java Server Pages (JSP) with the help of NetBeans IDE 8.2, Remix Ethereum IDE, and Web3js. An integrated development environment for JSP is NetBeans. JavaScript is used to create Remix, an amalgamated development environment. It is utilized to create, test, and debug Solidity Smart Contracts. Application Programming Interface (API)

for Java and Android that is lightweight and highly modular is called Web3js. The Ganache framework from Truffle is used to test the performance of Smart Contracts using Web3js. It is accessible as a desktop program as well as a command line tool (25). Due to Ganache, the application is also protected from attacks by Sybil, Race, and Eclipse. Ganache simulates the Ethereum private blockchain and has built-in protection against attacks like Sybil, Race, and Eclipse. The Casper algorithm (25) is used by Ganache to defend against Sybil. By restricting the incoming and outgoing connections in Ganache, the eclipse attack is stopped (25).

A smart cable that connects to a smart socket and automatically pays for electricity is demonstrated in a study as a proof-of-concept (26). They introduce a single-fee micropayment protocol that combines numerous smaller contributions progressively into one larger transaction costing only one transaction charge to address the issue of high transaction costs in the Bitcoin network for micro-transactions (57). The objective of their proof-of-concept design is to compensate for one activity by another activity for the electricity both activities use. The concept behind this project is a smart cable that, when put into a smart socket, will reimburse the socket for the electricity it delivers. Anything can be connected to the cable's opposite end. Although they tested the functionality using a standard toaster, it could theoretically be a vehicle, a phone, or anything else that is energized by electricity (26).

The main objective was to reduce paper waste, reduce the step involved in the VAT calculation process, and remove third parties that are required to validate the transaction by creating a new digital invoice and VAT payment management system utilizing blockchain and smart contract. The new system has four entities VAT administrator (VAD), sellers, buyers, and the bank. The previous system required eight steps to get the invoice and VAT calculation but the new system will only take four, thus saving time and money. In the new system, invoices are encrypted and reserved in a Decentralized Storage Network (DSN) using InterPlanetary File System (IPFS) protocol, to reduce repository space in the blockchain network. The operation starts when VAD deploys the smart contract into the blockchain. Next step, the VAD adds the list of registered VAT payers to the smart contract. The seller then stores the encrypted invoices in the blockchain and records the hash code. The buyer later retrieves the blockchain's hash code and decrypts the encrypted invoices

with the corresponding hash codes from the blockchain. Then it is verified into the smart contract by the buyer. After that, the seller confirms the invoice following the buyer's validation then the legal invoice is generated and the smart contract calculates the VAT. For the purpose of validating the transaction, calculating the value-added tax, and approving the payment of the VAT. The periodic VAT payment (PVP) is calculated as a formula (Equation 4),

$$PVC = (\sum_{i=1}^n Vi - \sum_{j=1}^k Ej) * r \quad (4)$$

they have suggested a new model based on Blockchain technology. The Standard Audit File for tax is the typical VAT administration model (SAF-T). The Organization for Economic Co-operation and Development (OECD) member nations have used this concept (27). After that, the invoice will be saved in .xml format, the taxpayers then provide the administrators with XML files. A novel approach is provided to invoice authentication that makes use of blockchain smart contracts. Instead of the eight stages required by the DICE paradigm, the proposed model operated in three phases to obtain the legal invoice. This model makes use of the Rivest-Shamir-Adleman (RSA) asymmetric cryptography method (27).

This paper proposed a system that significantly (28) reduces the burden on the restaurant's dine-in because the entire process of taking orders is automated. In today's market, labor costs are rising daily making it difficult to find personnel when desired, and physically going to an ordering window is time-consuming. The EIP20 coin smart contract was solidly developed and deployed on a private Ethereum blockchain. The application's token name, Foody, is indicated by the letter "F". This token contract essentially consists of an interface with several functions, including Transfer() and totalSupply(), which provide information on the total supply of tokens, among others.

2.3.2 Metrics Definition for Existing Systems with Blockchain

- a. **Cryptocurrency:** An electronic coin can be defined by a series of digital signatures. The proceeding transaction which has a hash that has been digitally signed and the public key of the following owner are incorporated into each transaction (31).

- b. **Smart Contract:** Smart contract means generating a set of rules that are agreed upon by all parties involved in the contract. The payments and milestones of a contract must be documented on the blockchain so neither party may fudge the contract's legitimacy or registration (32).
- c. **Off-Chain:** Those values transmit outside of the blockchain.
- d. **Cloud-Based:** This is something that involves the internet-based delivery of hosted services.
- e. **Lightweight:** A computer software that is intended to utilize the system's resources sparingly overall, using little RAM and little CPU (34).
- f. **Smart Payment:** It is a payment system that supports a number of other applications to help manage business transactions and reduce friction during checkout.
- g. **Blockchain:** A dispersed digital ledger that contains a chunk of transaction which is signed by digital signature. Following validation and agreement, each chunk of transaction is cryptographically connected to the earlier one (making mature it tamper obvious). Older blocks become increasingly rough to change as new blocks are added (5).
- h. **User Centric:** Flexible for the user.
- i. **Availability:** The likelihood that the system will be in good working order when used is known as availability (35).
- j. **Authenticity:** Determining the legitimacy of a user.
- k. **Privacy or No Middlemen:** The right to privacy is the freedom from interference and intrusion. No third-party involvement.
- l. **IoT Based:** The grouping of physical objects that can link to and exchange data with other objects and systems over the internet thanks to sensors, software, and other technologies inherent in them (33)
- m. **TCP/IP** It refers to Transmission Control Protocol/Internet Protocol. It is the collection of protocols for communication employed by the Internet and comparable computer networks (36)

- n. **Confidentiality:** Confidentiality points to the proposal and practice of holding a secret until data custodian specifically consents to share it with another party.
- o. **Immutability:** A blockchain ledger's capacity to maintain a permanent, irrevocable, and unchangeable history of transactions.
- p. **Transparency:** In the blockchain, it means a complete, valid, auditable ledger of transactions.
- q. **Accountability:** It refers to successfully implementing and carrying out a service or piece of software from start to finish.
- r. **Trustworthiness:** Safe from misuse.
- s. **Access control:** Permission to access and use information and resources which are determined by access control.
- t. **Data Auditing:** Carrying out a data audit to evaluate how organization's data is apt for given scheme.
- u. **Cost Efficiency:** Whether the cost of the project is feasible or not.
- v. **Ethereum:** Ethereum is a blockchain that has a built-in programming language that gives users the ability to develop apps and businesses, store assets, carry out transactions, and communicate all without depending on a single entity (31).
- w. **Remove Node Attack:** There are several node attacks such as Sybil attack, Race attack, Eclipse attack, and Protection from these (25)

2.3.3 Analysis of the Systems with Blockchain

This paper (13) includes blockchain technology in donation systems that has been vital for these projects since it encourages transparency and boosts confidence because it is a decentralized technology and there is no middleman between the giver and beneficiary. Therefore, without messing with the previously saved data, this technology generates and stores contracts and monitors the flow of funds inside the network.

Table 2.2: Analysis Table of the Systems with Blockchain

Systems with Blockchain	Cryptocurrency	Smart Contract	Off-Chain	Cloud-Based	Lightweight	Smart Payment	User Centric	Availability	Authenticity	Privacy/no Middlemen	IoT Based	TCP/IP	Confidentiality	Immutability	Transparency	Accountability	Trustworthiness	Access Control	Data Auditing	Cost Efficiency	Non-Repudiation	Casper Algorithm	Remove Node Attack
(13)	Y	Y	N	N	Y	Y	Y	N	Y	Y	N	-	Y	Y	Y	-	Y	Y	N	Y	Y	Y	Y
(14)	Y	Y	-	-	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y	Y	Y	-	-	Y	Y	-	-
(15)	Y	Y	N	Y	Y	Y	Y	N	Y	Y	-	Y	-	-	-	-	-	-	Y	-	-	-	-
(16)	Y	-	-	-	-	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	N	Y	-	-	-	-	-	-
(17)	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	N	N	-	Y	Y	Y	Y	Y	-	-	-	-	-
(18)	Y	Y	Y	N	N	Y	Y	Y	Y	N	N	-	Y	Y	Y	Y	Y	Y	-	-	-	-	-
(19)	Y	Y	-	-	Y	Y	-	Y	Y	-	N	N	Y	Y	Y	Y	Y	-	Y	Y	Y	N	Y
(20)	Y	-	-	-	Y	Y	Y	Y	Y	Y	-	-	-	-	-	-	-	-	-	-	-	-	-
(21)	Y	Y	-	N	Y	Y	Y	Y	Y	-	N	N	Y	Y	Y	Y	Y	-	Y	Y	Y	N	-
(22)	Y	Y	Y	N	N	Y	N	N	N	N	Y	-	-	Y	Y	-	Y	-	-	N	-	-	-
(23)	Y	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
(24)	Y	Y	N	N	Y	-	Y	Y	Y	N	N	-	Y	Y	Y	Y	Y	-	-	Y	-	-	-
(25)	Y	Y	Y	N	N	Y	Y	Y	Y	Y	N	-	N	Y	Y	N	Y	N	N	Y	N	Y	Y
(26)	Y	-	-	-	-	-	-	-	-	N	Y	Y	-	-	-	-	-	-	-	-	-	-	-
(27)	Y	Y	Y	-	N	Y	Y	Y	-	-	-	-	-	-	-	-	Y	Y	-	Y	-	-	-
(28)	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	-	N	Y	Y	N	Y	Y	N	N	Y	N	-

This particular project (14) is a lightweight, user centric system. It utilizes blockchain and smart contract technology to monitor all the agents involved to increase transparency in Islamic banking. This emerging technology is used to supervise all personnel involved in the banking process, including Sharia supervisor boards, contributors, governmental regulators, and beneficiaries. The use of this technology benefits the users in several ways, there are no single point failures, fraud identification is easier, tracking and auditing of transactions is possible. The altering of data is also not computationally possible as it uses blockchain technology to store transactions. It helps reduce the service costs associated with the financial transactions and other services. It assists in increasing trustworthiness, accountabil-

ity, and confidentiality in the banking process as almost every aspect of the process is monitored.

This system (15) utilizes blockchain and smart contract technology to ensure inexpensive, cashless payment for remote villages that have poor internet connectivity. Here, smart contracts are utilized to manage and track all system operations. The payment operator creates a smart contract that keeps track of use balances in both fiat currency, token currency, and distributing the rewards to the miners. Availability and authenticity are ensured through the use of blockchain. It uses Ethereum blockchain technology to since allows developers to create second layer applications.

In a double spending problem, someone may lose their money. It is a huge trouble. The Fastpay (blockchain base IoT device) service solves this problem by taking payment proof to prevent double-spending which is more effective than Lightning Network (53) and Raiden Network. Much quicker than several widely used blockchain-based cryptocurrency systems, including Bitcoin, Fastpay (16) confirms a payment in under 9 seconds. In bitcoin, there is a proposed solution for blockchain fork, which is 6-confirmations but it is time-consuming since it will almost take one hour for the whole process to execute. So, FastPay overcome this problem as well.

This system (17) ensures accountability as it works from searching with a keyword to having an accurate result. They use Java for implementing the searchable encryption algorithms in BMFP and Solidity to build Ethereum smart contracts. The message authentication code function is instantiated by HMAC-SHA256, and the pseudo-random function is instantiated by HMAC-MD5. HMAC Hashing to Authenticate Messages It is a MAC that was created using a shared secret key and a hash function on the data. It makes faster calculation and verification which makes the system more efficient.

This entire system (18) is built upon permissioned blockchain. It is not fully decentralized; this was done as a compromise between regulation and privacy protection. For this system, initially, a Centralized Anonymous Payment (CAP) System

was built and on top of that, the DCAP system was constructed. The proposed DCAP has four entities certificate authority, user, manager, and blockchain network. Here the manager as a third party holds a lot of power as they are responsible for monitoring the authentic identity of a distrustful transaction and only they can transform an unidentified address into the original one. The smart contract is utilized to fetch certificates and mapping the user's public key to the transaction. It is used to recognize the certificate in the blockchain to verify to the authority and blacklist revoked users. In this DCAP, the Practical Byzantine Fault Tolerance consensus model was used as a consensus model, which will allow hundreds of transactions per second.

In their work (19), the verification in the suggested system is quite robust. In the current setup, CA manages the task. To manage the tasks in the suggested system, CA has been categorized with the miner. The illegal access is blocked. The proposed system logs all unwanted access and keeps a copy for later analysis. The current system takes longer. The suggested system requires less time.

In ScholarChain (20), Oracle has used to services of those parties in order to do automated verifications. Oracle can utilize the data kept in a database to verify the identity of anyone trying to connect to it, for this, must create each user with a password that is required when the user tries to establish a connection in order to configure Oracle to use database authentication.

In TEduChain (21), the CSS Scheme's Smart Contract will automate the current system the time required is reduced by physical work Which makes it better than other systems. This system achieves reliability, and availability by using smart contract. They use solidity in it helps to multiple-level inheritance properties. Multiple members of variables are maintained by the Solidity created for Contracts to express and organize data. Web3 helps to achieve lightweight features. Protecting the system from race attacks makes it more reliable. but failed to defend against the Man in the Middle and Denial-of-Service attacks. So, it is a drawback for them.

In this system (22) they combined IoT with blockchain and this initiative gives them so many benefits, such as it will enhance privacy, smart contract allows all

transactions between providers and contributors to be monitored and made public for increased security. They can track every rice donation. But for this project they need to set up IoT devices in every orphanage, this will cost more than usual. They have a middleman for managing the donation. This is the reason behind less trustworthiness. It will discourage people from donating rice through this system.

This system (23) used blockchain and smart contract technology as a primary technology to cut the cost related to banking. Here, the two consensus mechanisms analyzed are proof of work and proof of stake. The author discusses how proof of stake is significantly better than proof of work. It is much more environmentally friendly as mining for bitcoin is computationally expensive and requires a lot of electricity. There is no centralization as blockchain is a distributed ledger.

EduCTX (24) is a blockchain-based higher education credit and grading platform whose goal is to keep track of students' completed credits and transfer it when required. It uses all of blockchain's technological benefits as a decentralized architecture. An ECTX token is equivalent to an academic credit that is managed, prepared, and controlled by the EduCTX blockchain platform, which is on a globally peer-to-peer network. The user of this platform is higher education institutions (HEI), students, and organizations. For security purposes, each student will be allocated a 2-2 multi-signature by their native HEI. For any authorized HEI to join the network they must construct a network node for the purpose of maintaining a global and secure network. ARK Blockchain was used to build the platform. ARK was used because of its utilization of Delegated Proof of Stake consensus, where a delegate or in this case HEIs are chosen via voting by individual users. The platform uses both off-chain and on-chain technologies to give the user a proper user experience. It was built with the users in mind, it is a trustworthy platform that provides transparency, and confidentiality.

The objective of the work of (25) was to encourage meritorious students to aim for higher education by providing them with financial assistance given by the Center Sector Scheme of Scholarship for College and University Students. It was developed to mitigate the lack of transparency and traceability of the application

form for the scholarship. There are four entities on this platform Students, Education Boards, Colleges, and Banks. Smart contracts are used by the Education Boards to automate the verification process to see if the students are eligible or not. If the students are eligible, they will gain the scholarship in their respective bank accounts. The platform was tested for several attacks and finally concluded that it is secure against Phishing attacks, Sybil, Race, and Eclipse attacks.

The aim of the device used in (26) is to automate the payment of money for the energy used. A smart cable was made to plug into a smart socket, where the smart cable will pay the smart socket for the energy used. Bitcoin is used as a currency for transactions. For the transaction to take place the cable is initiated with a Bitcoin account containing Bitcoin. The electricity supply is controlled by a relay and a current sensor is used to calculate the transferred energy. PLC (Power-line Communication) communication is utilized by the payment protocol to handle the bitcoin transaction process and negotiate power payment. Initially, a certain amount of satoshi is paid by the smart cable, which is broadcasted to the bitcoin network and the socket enters the paid mode so that the electrical device can get the electrical power required to operate. One of the major drawbacks of this device is that it is extremely slow as it takes a long period to boot up the Linux system in Raspberry Pi. It is also less user-friendly as it is not compact.

The objective of (27) was to minimize the steps that are involved in the VAT payment system and automate some of the key steps involving the VAT calculation and invoice. Thus, making it easier for the user to pay or manage their VAT. The system has four entities VAT administrator (VAD), buyer, seller, and bank. Invoices are encrypted and stored in a Decentralized Storage Network (DSN) via IPFS protocol. This was done to reduce the storage space in the blockchain network (BCN). The system is initiated by the VAD when they deploy the smart contract into the BCN and attaches the list of registered VAT payers. Encryption was used because it is necessary to protect invoice data. Rivest-Shamir-Adleman asymmetric cryptography algorithm was used in this case. RSA allows the user to certify the invoice so that the receiver knows it was not tampered with.

This system (28) helps to reduce the burden of orders in restaurants. They have used private Ethereum, Since the number of nodes in private blockchain is lower, it is significantly faster compared to the public blockchain. So, it will faster the system. By using this private blockchain, they ensure minimized downtime which reduces unavailability, uptimes are increased, and scaling is facilitated which means a large number of users can be handled easily. It is improbable that numerous participants will be added at once.

2.4 Conclusion

This concludes the literature review chapter. Here, we have discussed about few familiar organizations without the use of Blockchain technology which works for people and similar to our project. Also, we have discussed about few systems that uses blockchain technology. For comparison, we have provided necessary tables as well. In the next chapter, we have discussed about the methodology we have used for the development and how we have planned and worker throughout the development period.

Chapter 3

Methodology

3.1 Introduction

In the previous chapter, we have discussed some similar types of systems that are already available. We also discussed about "Prekkha" and how this stands out from those systems. In this chapter, we have discussed the methodology that we have followed for developing our project.

3.2 Software Process Model

A software process is a group of associated activities that lead to the making of the software. These exercises may incorporate the development of the software from the beginning or modifying an existing system (8). The software process model we are choosing for this project is the "Agile Model". This model breaks tasks of the project into small incremental builds and these parts/builds are provided in iterations. Which gives flexibility, easy to manage & use. We chose this model because of its all advantages & mainly it allows us to regularly adapt to changing requirements even late changes in requirements are welcomed, which is suitable for our project. Every iteration involves core functionality. The "Agile" (Figure 3.1) model is our best choice for the short time of project implementation and for maintaining everything. For managing tasks in our project, we use the Scrum agile development process. We use it because of its celerity, where development work is partitioned into packets.

In this development process, the role of members and events are well-defined.

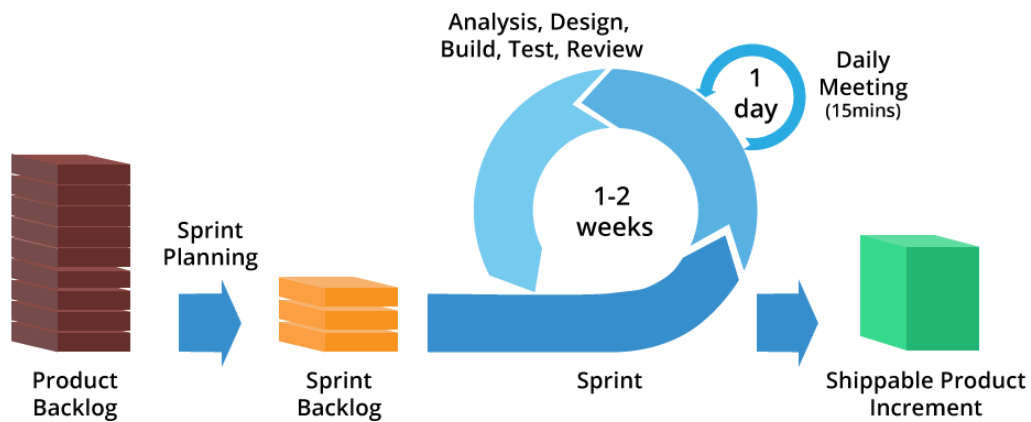


Figure 3.1: Agile Scrum Process.

The product backlog is where all the requirements needed to develop software are listed in order of priority. The sprint backlog is the list of the tasks and elements that need to be finished during the next Sprint. In the scrum development process, work flow of each event are given below:

- **Sprint planning:** This is the first phase or event of each iteration. Before starting an iteration (sprint time frame) we conduct an online meeting where we decide what we should implement in the upcoming sprint. Planning how we work for the upcoming sprint.
- **Daily Scrum:** This is the event where we conduct an everyday small meeting. In this meeting, we discussed with the team members what we have done on this.
- **Sprint Review & Retrospective:** In this event, we conduct an informal meeting with the team members at the end of each sprint/iteration. Where we review our work which we did during the sprint. After that, we conduct meetings with our supervisor about our progress.
- **Planning & Requirement Analysis:** This is the first phase of starting the project and also this is the most crucial part of any project. Most of the possible elements, data and other additional information on the system to be developed are collected in this phase. In this first phase, we are working

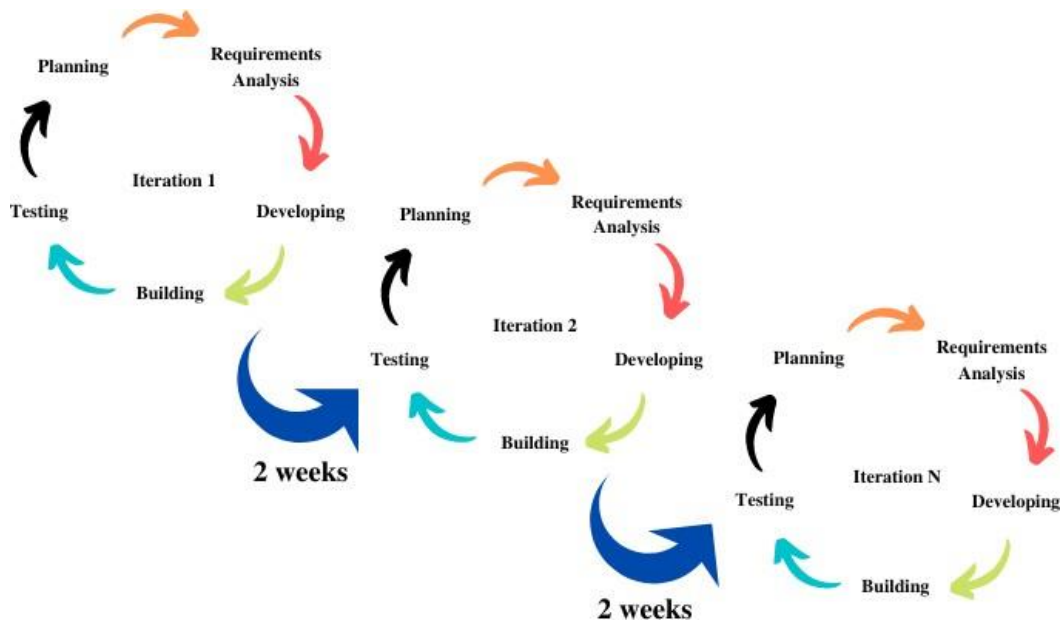


Figure 3.2: Agile Model Iteration Process Flow.

on which type of data is needed in our system. We scrutinize its function, specifications, purpose, etc. We also study other things about the project such as business opportunities, demand, market conditions, etc. This is one of the lengthy periods of the project.

- **System Design:** Now comes with the system design, it helps in defining the overall system architecture. In the phase of system design, according to Agile model iteration process flow (Figure 3.2), we work on many types of design methods. We design system architecture such as block diagram, activity diagram, use case diagram, data flow diagrams, and class diagram. We also design how our database will work, how our blockchain will be connected to our system based on our project requirements and other high-level technical details of the project.
- **Implementation:** This is the phase where the concept is transforming into an actual product. In this stage, we use various types of tools to implement the project. As we developed a cross-platform system firstly we break our project

into multiple separate units. We mainly divide our system into 3 sections as a smartphone section, web section, and data handling. In these 3 categories, we also divided our system into multiple units and developed as per unit.

- **Testing:** After implementing all units, in this section, we conduct unit testing. After successfully testing all the units we integrated all the units into a system. Then we also ran some level of full system tests to make sure that the systems are working properly as we were expected.
- **Deployment & Feedback:** Since we are working on the prototyping of the project, that's why we did not deploy our project in the production environment and there is no need for maintenance.

3.3 Required Tools

There were lots of tools required for implementing this project. As we developed a cross-platform online service, therefore, we are dividing our required tools section. The required tools for implementing this project are given below:

3.3.1 Web Tools

WebStrom & VS Code: WebStrom (66) & Visual Studio Code are integrated development environment (IDE) for JavaScript and affiliated technologies. The IDE offers numerous built-in developer tools that help developers streamline their work and make it more efficient. It detects and suggests fixes for errors and redundancies, and helps refactor codes. It is also easier and faster to search and navigate for specific things when required.

HTML: HTML (Hyper Text Markup Language) (67) is the code that is deployed to structure a webpage and the contents inside it. It contains series elements, which can be used to encircle or wrap distinct parts of the content to make it viewable a particular way or act in a specific way.

CSS: CSS (Cascading Style Sheets) (67) is the code that is used to style web content. It is used to selectively style the content of HTML elements.

JavaScript: JavaScript (68) is a programming language that adds functionality to a website. It is relatively compact and flexible. It was invented by Brendan Eich. It allows browser Application Programming Interfaces innated into web browsers, bestowing functionality like interactively creating HTML and mounting CSS styles. It allows third-party APIs that supports developers to include functionality in their sites from other content providers.

Node.js Node.js (69) is a server-side JavaScript environment built upon V8 engine. It was implemented using C and C++ which focused on reduced memory expenditure and better performance. V8 mostly supports JavaScript in the browser. The aim of Node.js is to provide a long-term server process. It is built upon asynchronous I/O events and does not rely on multithreading. It is better because event-driven programming supplies a more streamlined, scalable substitute that imparts developers with more sovereignty over changing between application activities. Every operation in the Node.js programming model is handled by means of a higher-order function.

Node Package Manager (NPM): Node Package Manager (NPM) (70) is the standard package manager. It is the world's most comprehensive software registry. It is open-source and used by millions of developers worldwide. It is used to download packages and dependencies used by developers.

Composer Dependency Manager: Composer Dependency Manager (71) is a tool that is used for dependency management. It allows developers to declare libraries that a project might depend on and it will install/update them for developers.

3.3.2 Blockchain Tools

Ethereum: Ethereum (72) makes it possible for nodes to stop fraudulent practices like cryptocurrency forgery and copycat production, having a traceable record of every transaction carried out over a network owing to the decentralization of the network's structure, the Ethereum foundation maintains user pseudonymity (a less reliable method of anonymity), since each user's identity is disclosed to the public key. This makes it possible for users of the platform to do activities like money

transfers, buying, and selling, plus a lot more. Ethereum has used an algorithm called keccak-256, Keccak is a family of cryptographic hash functions built upon the sponge construction and is utilized as an elementary unit of a permutation from a set of seven permutations. The rudimentary element is the Keccak-f permutation, which includes the permutation of bits and several simple rounds with logical operators. Keccak-256 is efficient as it allows high-level 8 parallelisms. The bit-interleaving permits Keccak-256 to be flexible and it is better suited for protection against side-channel attacks.

Solidity: Solidity (73) is an object-oriented programming language for executing smart contracts. It is a language developed to aim at the Ethereum Virtual Machine (EVM). It was induced by C++, Python, and JavaScript. It has features like inheritance, it is statically typed, and allows user-defined functions.

Truffle: Truffle (74) is an environment for developing, testing, debugging framework and asset pipeline for Ethereum. It has integrated smart contract compilation, linking, deployment, and binary management. It has automatic contract testing. It allows developers to write scripts that is used for deployment and migration framework. Moreover, it has management system for deploying to many public and private networks. It also has an external script runner that executes a script within the Truffle network.

Web.js: Developers using the web3.js (75), can have access to the Ethereum network through this platform. This makes it possible for web applications to decipher messages provided by the Ethereum network and send transactions to the network. Through blockchain-enabled browsers like Metamask for Chrome and the Mist browser, Ethereum also offers a user interface to customers. These interfaces give users access to their ether wallets, allowing them to conduct transactions using Ethereum. For local machine tests, it can use ganache for the testing wallet. The program also leverages IPFS to store item data securely and decentralized, as well as MongoDB for efficiency.

Ganache: Ganache (78) is a personal/private blockchain that is implemented for rapid Ethereum-distributed application development. It allows zero-configure

the mainnet, that is it automatically creates a network without having to manually configure the network. It allows the development, deployment, and testing of decentralized applications in a secure and deterministic environment. Ganache allows Ethereum JSON-RPC support. It has a feature that listens for JSON-RPC 2.0 requests over HTTP/WebSockets. It allows a revert state and blocks can be mined instantaneously when required, or after a certain period of time.

3.3.3 API Tools

- NodeJS
- Node Package Manager (NPM)
- Web3 Module for Blockchain interaction

3.4 Conclusion

With that being discussed, methodology chapter ends here. We have discussed what approach is taken to develop this project and what type of different tools we have used. In the next chapter, we have discussed our system through diagrams which helps to understand Prekkha better.

Chapter 4

The Proposed System

4.1 Introduction

In the previous chapter, we have discussed the methodology which we have followed for the development of "Prekkha: A Blockchain Based System to Track and Provide Financial Aid". We also have discussed the full specification of the project and tools that we are used to develop this project. In this chapter, we have described our proposed system through diagrams.

4.2 Block Diagram

A Block diagram is a diagram of a system that shows a graphical representation of a system. In a block diagram, the core parts or functions are illustrated by blocks. It provides us a better understanding of a systems function. Prekkha's block diagram Figure 4.1 shows the whole system's core functionalities and how they are connected. Non-registered users are be able to explore the system and by exploring the system it is meant that they can know what Prekkha is and what its aims are. Also, they can view live counts of donations, donors, total contributions etc. Registered beneficiaries or donors can also explore the system after login to the system. It is the crucial part of the system; it validates the user firstly then provides user information according to the credentials. After that users can access different types of functionalities according to the user types. Beneficiaries can update their information. But the most importantly, they can apply for aid according to their need which are uploaded to the system and visible to donors end after storing that information in a database. They can logout whenever they think they are done for

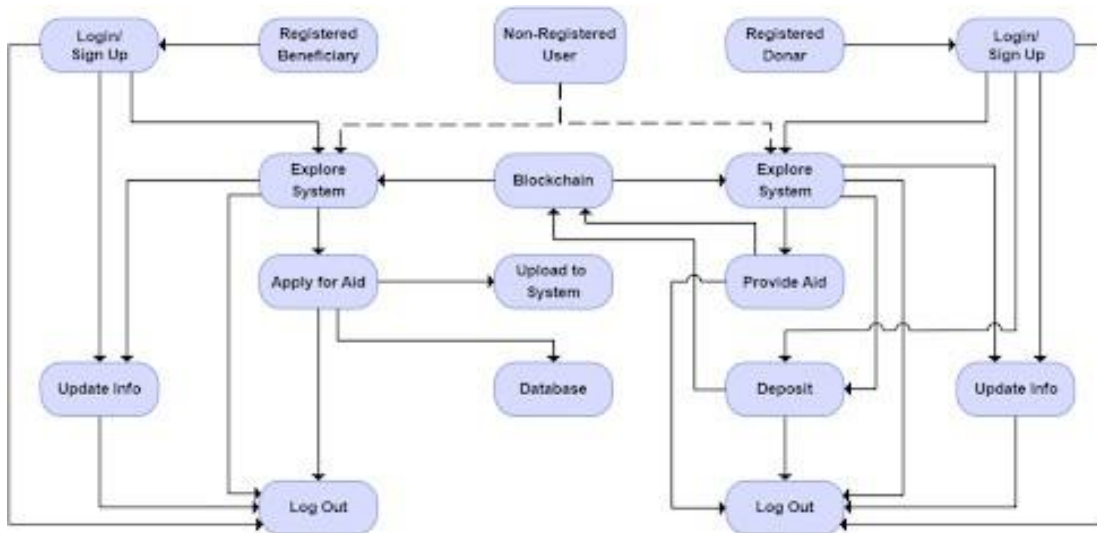


Figure 4.1: Block Diagram of Prekha.

that time being. Similarly, donors can update their information and deposit money (in BDT) which is stored in Prekha’s blockchain network after the confirmation. Donor can provide financial aid by choosing someone from the aid list. Whenever the donation is done, transaction details about the donation are stored in blockchain and logout from the system if they wish to.

4.3 Activity Diagram

An activity diagram describes the workflows of step wise exercises and operations with support for alteration and iteration. In activity diagrams, we have described the whole system’s workflow and the steps involved in the execution to use case, which is shown in Figure 4.5. We have divided activity diagrams into 3 steps, where admin, donors and acceptors, and their diagram independently as shown in Figure 4.2, Figure 4.3 & Figure 4.4.

4.3.1 Admin Activity Diagram

An admin account can be created by a super admin. Admin can login to the system using their credentials and after they are allowed to update necessary information

of the system, donors and acceptors. They can logout when they are done with their assigned task.

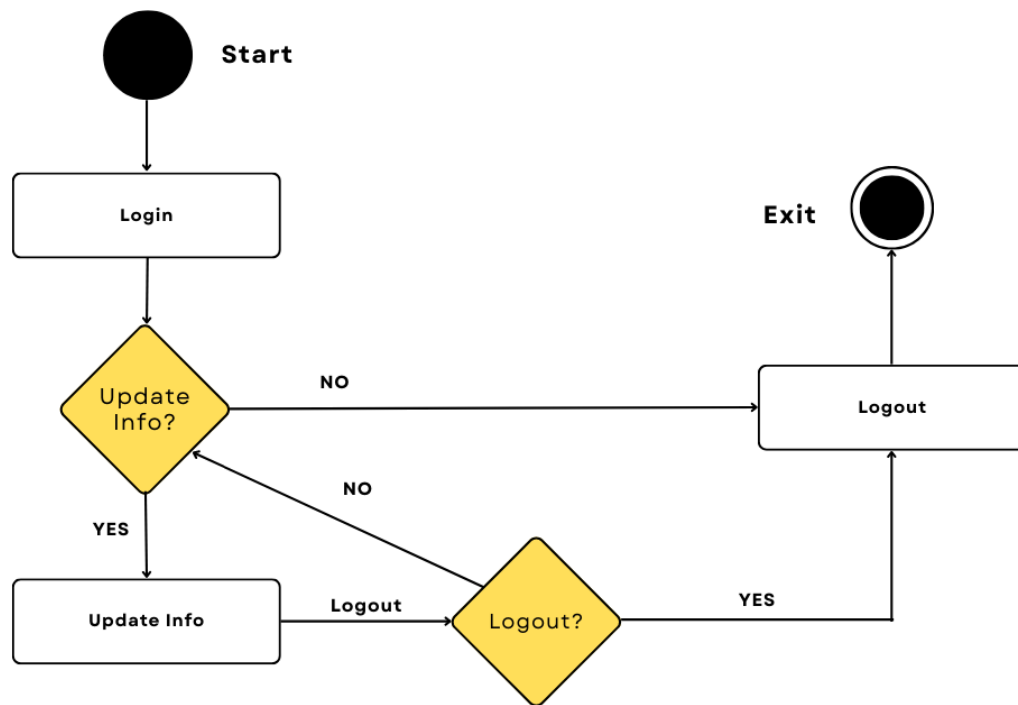


Figure 4.2: Admin Activity Diagram of Prekkha.

4.3.2 Donor Activity Diagram

Donors have to go through a registration process in order to login in to the system if it's their first time in the system. After that, they are able to explore the system which shows them necessary details to choose his next step. A donor can deposit money to a dedicated account as well as they can provide someone financial aid from the list. Also, they are allowed to update his account information if necessary.

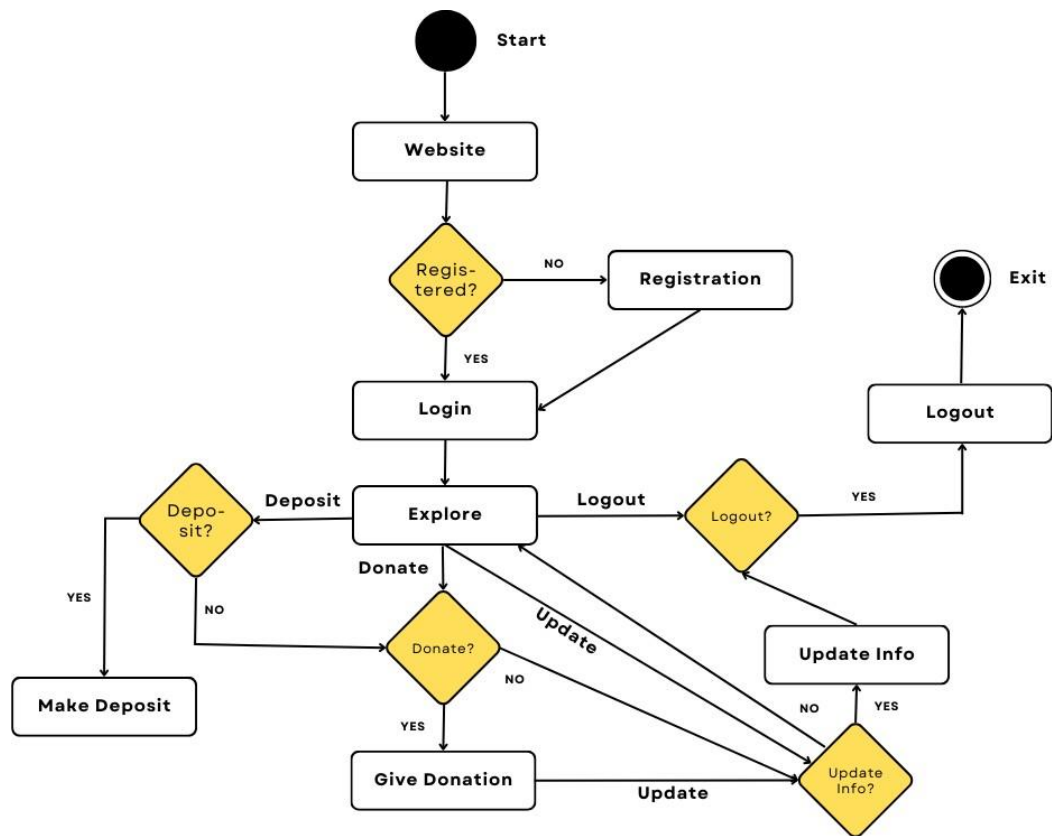


Figure 4.3: Donor Activity Diagram of Prekha.

4.3.3 Acceptor Activity Diagram

Acceptors activity are almost similar to donors. They can login and update their information if they are registered to the system. Mainly, they can request for a financial aid according to their need and logout from the system when they decide to.

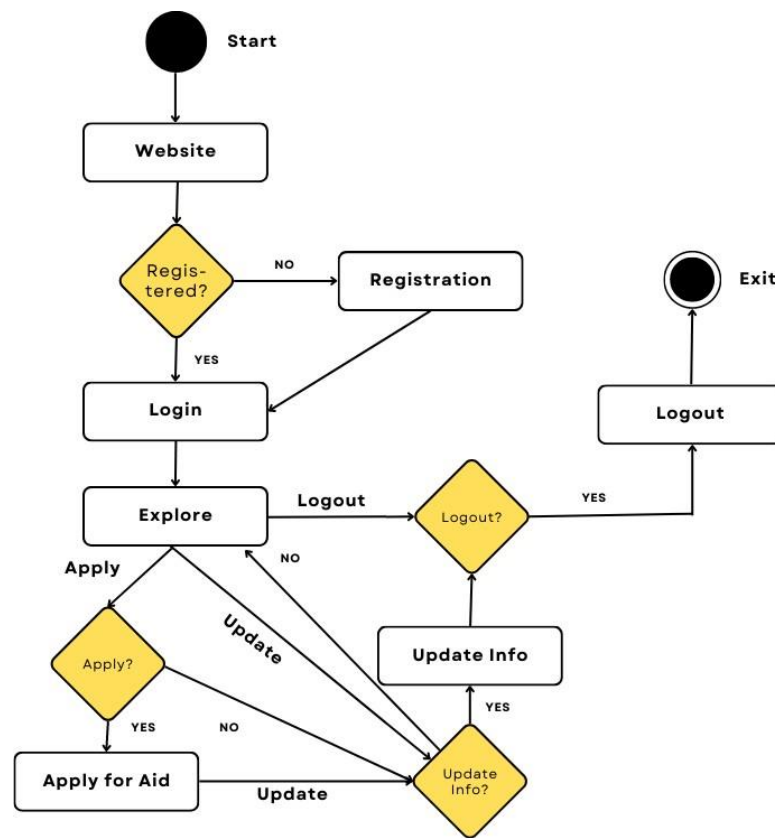


Figure 4.4: Acceptor Activity Diagram of Prekha.

In all above three diagrams we have tried to show the various process of our system and how each activity are related to the other activity. In those diagrams shown how each process acts logically according to the user's input and also shows where validation is needed and where not.

4.4 Use Case Diagram

A use case diagram demonstrates all the functionalities user can perform. In this use case diagram, Figure 4.5, we can see which user can perform which type of functionalities. In Prekkha, there are 3 types of users and those are Admin, Donor and Acceptor. All 3 types of users can login and log out of the system but other functionalities are defined separately. As shown in (Figure 4.5) except for admin donors and acceptors both can create their profile in this system, where the admin profile can only be created by the super admin. Admin can log in to the system and after that, an admin is responsible for managing the whole system and also admin can manage their profile. Donors can access all the functionalities except for aid application. At last, acceptors can access most of the functionalities similar to the donors as well as aid application except for providing donation and deposit money to Prekkha's dedicated bank account.

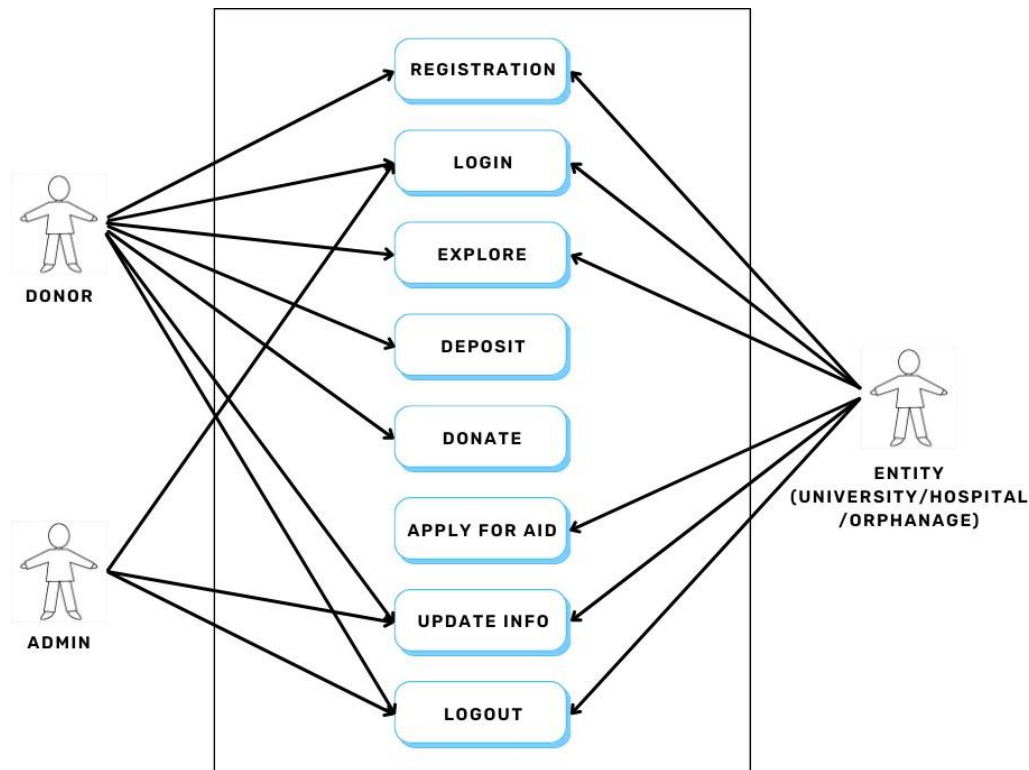


Figure 4.5: Use Case Diagram of Prekkha.

4.5 Data Flow Diagram (DFD)

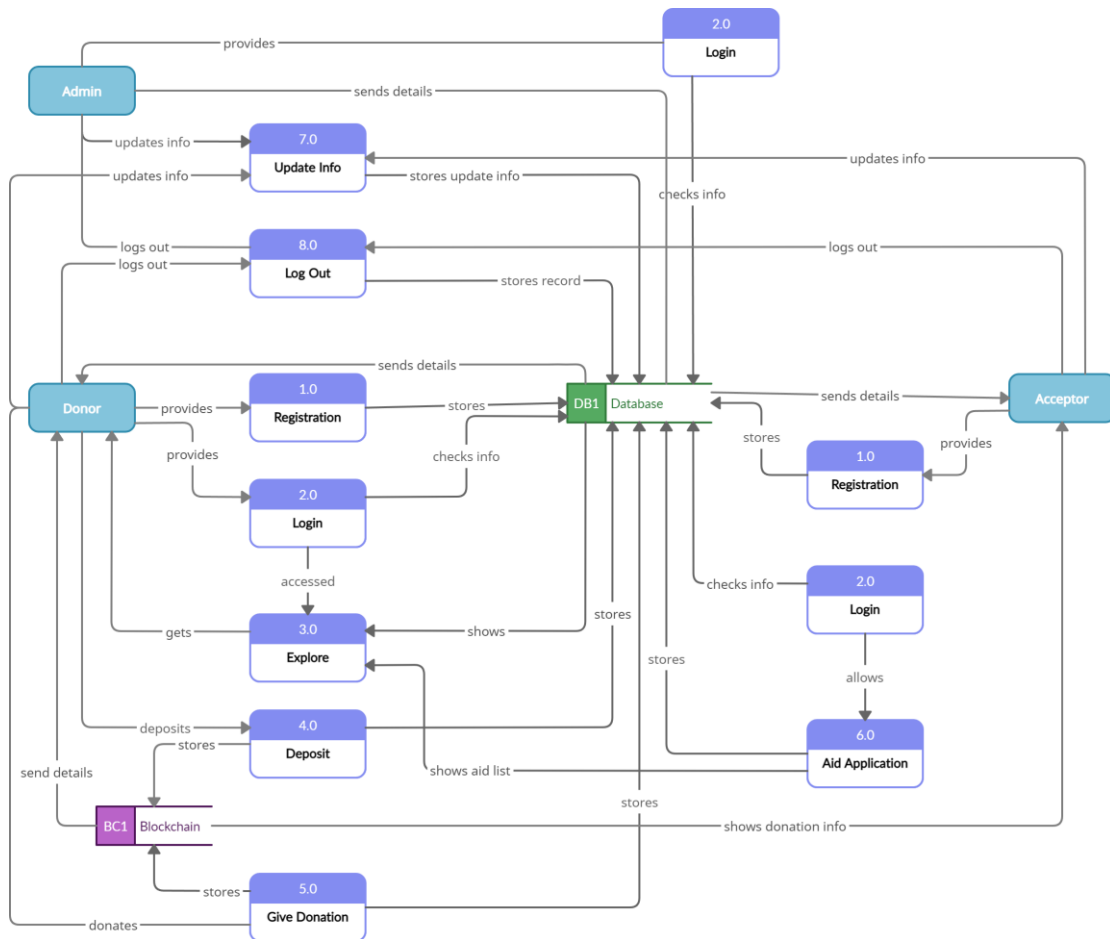


Figure 4.6: Level-1 Data Flow Diagram of Prekkha.

The data flow diagram is one of the most important parts to understand the system. It is the graphical representation of data flow in any system. Figure 4.6 is the level-1 data flow diagram of Prekkha. It is the diagram to show how data is flowing in the system from one process to another process, how those data are stored and accessed. As shown in this diagram there are 8 processes, and a total of 2 data stores in the system. How the system is working that previously discussed with other diagrams. The description of the process data flow is given below:

1. Registration: This is the first process for accessing the system. This is the

registration process where the user must provide some information like user name, phone number, password etc. to access the system and those data is first saved in the database.

2. Login: If a user already has an account on our system in this process users have to provide their credentials such as phone number, password, and user type. After that system checks that user information is valid or not. If the user credentials are valid then the system generates a session corresponding to the user and provides information according to the user type.

3. Explore: In this process, donors can explore all information such as, number of donors, total contribution till date, what Prekkha is and what are their objectives, aid list available right on that time, their personal information etc., that are in the platform.

4. Deposit: In this process, donors can deposit money (in BDT) to Prekkha's dedicated account which will be used for donation later. After validating the transaction this data is permanently stored in Blockchain as well as in the database and donors can see their deposit details whenever they want.

5. Give Donation: When a donor chooses a person from the aid list in order support him, this process is executed. An API call is generated by the system to Bank's server and allow it to send money to that particular acceptor dedicated account. Later on, this transaction will be stored in to blockchain and database. A notification about this transaction will also be sent to both the donor and acceptor.

6. Aid Application: This process is only for acceptors. After entering to the system they can apply for a financial aid specially mentioning about required amount, reason and bank account. When they are done applying, their request information will be stored in database and uploaded to the system so that donors can support them.

7. Update Info: This particular process is available for everyone. Donors and acceptors can update their personal information if they need. On the other hand,

admin can use this process in order to update information about the system, donors and acceptors.

8. Logout: The session which was started after logged in to the system will be terminated as soon as user logout from the system after doing their work.

4.6 Conclusion

This concludes the diagram analysis chapter of our system. In the next chapter we have discussed the workflow and user interface for better understanding of the project. Also, it gives an overview of how data are flowing throughout the entire system which are discussed in this chapter as well as which user can use which features.

Chapter 5

Implementation & Analysis

5.1 Introduction

In the previous chapter, we have discussed about the system through different types of diagram diagrams and here we have discussed about the system's workflow through the user interface.

5.2 Workflow of Prekkha

Figure 5.1 shows how actually Prekkha works. Initially, the donor and beneficiaries both registers to our system. Here the donor could be anyone who wants to help the people in need. The beneficiaries can only be students, patients, and orphanage directors. After registration is complete the beneficiaries will apply for donation. For the verification part of the legitimacy of the beneficiaries their respective institutes must be registered to our system, so that someone from the inside of the institution can verify and greenlit the whole process. Then after verification the application will be uploaded to our system. The donors will be to see the application that were verified. And the money would be transferred to Prekkha's bank account to temporary hold it. Then it will be directly transferred to the beneficiaries' respective institutions bank account. The transaction to the account will be verified by our admin. And all the information related to the transaction will be stored in the blockchain.

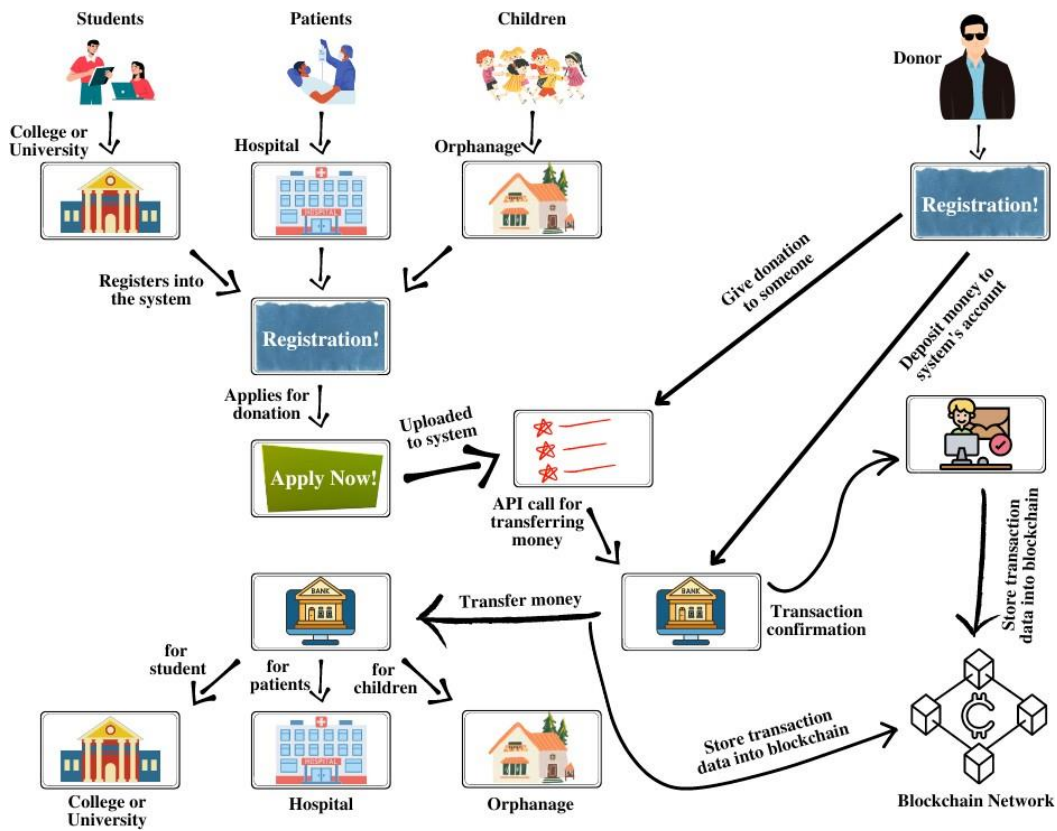


Figure 5.1: Workflow of Prekkha.

5.3 UI Design & Analysis

We have developed a system that works on web browsers and for that we have used different frameworks and languages. We have used Noje.js, a free and open-source JavaScript framework which follows MVC architecture for backend development. It is very robust and adaptive to modern technology and comes in various packages. For developing the fronted, we have used Bootstrap and Express.js. Moreover, we have used Web3 which is a collection of libraries that works as a communicator. It allows a developer to work with local and remote Ethereum node using HTTP, IPC, or WebSocket. For local Blockchain, we have used Truffle Suite's Ganache.

The decentralized application's implementation involves the following steps:

- As we develop a system that works on web browsers, for that we use different

frameworks and different languages. In the development of web applications, we use Node.js. It follows MVC architecture. We use Node.js, a free and open-source JavaScript framework. It is very robust and adaptive to modern technology. As for programming languages, node.js uses JavaScript. It comes in various packages. For developing the fronted we use Bootstrap. For, making an API of Prekkha Node.js has been used. Mainly the whole system data flow is controlled by this API. Node.js backend server is responsible for communicating with the fronted web and Blockchain as well as MongoDB to store data. It is more stable and more secure compared to others. For storing the general data in MongoDB this system has used NoSQL. We are using NoSQL because of its low latency, large data volume, and flexible data models.

- The system's smart is written in solidity. Use the Truffle framework to implement the contracts in Solidity, deploy them to Ganache, and communicate with them via the Truffle console.
- Frontend is constructed so that they can interact with the contract and the frontend's functionality after the backend has been implemented. The server.js is for implementing the server functionally. It contains the `app.get( )` function for communicating with the frontend folder by API calls.
- Execution of the Node.JS server-side code that waits for the contract events and saves the request to the console once the database is active and running. then put the code into action to add products to the database.

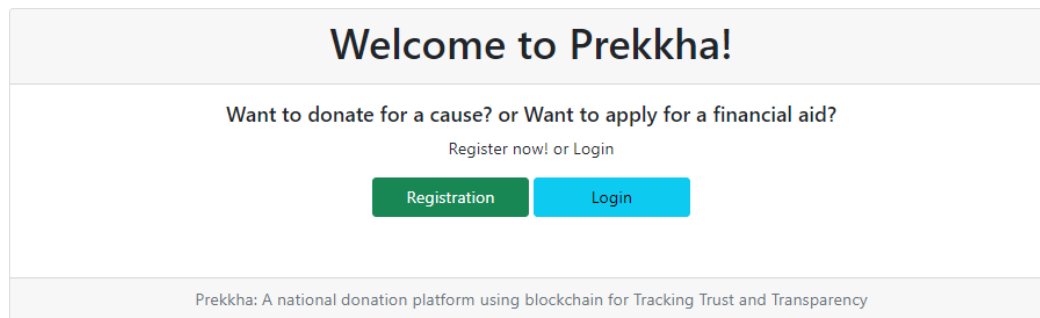


Figure 5.2: User Login Registration Page.

Figure 5.2 shows the login and registration page of prekkha. A non-registered user can create an account and registered user can login in to the system using this page. Provided data are stored in database in case of registration and a session is created for a user against his credentials. After that, each user can use Prekkha according to his or her account type.

After logged in to the system, a beneficiary can apply for financial aid according to his cause. Figure 5.3 shows the aid request page where three different types of purpose can be seen for students, patients and orphanage. A beneficiary can apply by choosing any of the purposes and providing necessary information, such as name, purpose, aid amount, bank account number, NID or Student ID etc. mentioning his or her authoriser's name who will validate that particular request. After that, the request will be updated to the system and visible to donors' end.

Whenever a beneficiary applies for financial aid, Prekkha takes the user to which shows that aid request is successful. After that, user can go back to his or her initial dashboard and logout according to his or her will.

Aid Request

Choose your Purpose

☐ Education Aid

☒ Medical Aid

☐ Orphanage

Bank Name	Bank Account Number
UCB	0971567
Amount	Authorizer Name
1000	inb sina
Authorizer Phone	
0170000000	
Write a details about your need need for operation.	

Request

Figure 5.3: Aid Request Page.

When a registered donor logs in to the system, the system takes that user to his dashboard as shown in Figure 5.4 & 5.5. From there, a donor can view his or her personal details and all available request for financial aid. A donor is able to deposit money from his account to Prekkha's dedicated bank account in order to temporary hold and provide financial supports to the beneficiaries. After deposit money to Prekkha's bank account, donor must provide the transaction ID to confirm his or her deposit against his or her name. A transaction ID can be used only once and after confirmation data is stored in both database and Blockchain. If a donor has money in Prekkha's account against his or her name, then can make a donation by choosing anyone from the list. Also, a donation cannot be made if a donors' deposited amount is less than the amount he or she wants to provide to someone. This particular action is performed through Prekkha's smart contract.

Since we are in the development and testing phase of the project, integration of a real bank is not possible for time being. Therefore, we have created a dummy bank and its API. This dummy bank's API can be used for depositing money to Prekkha's

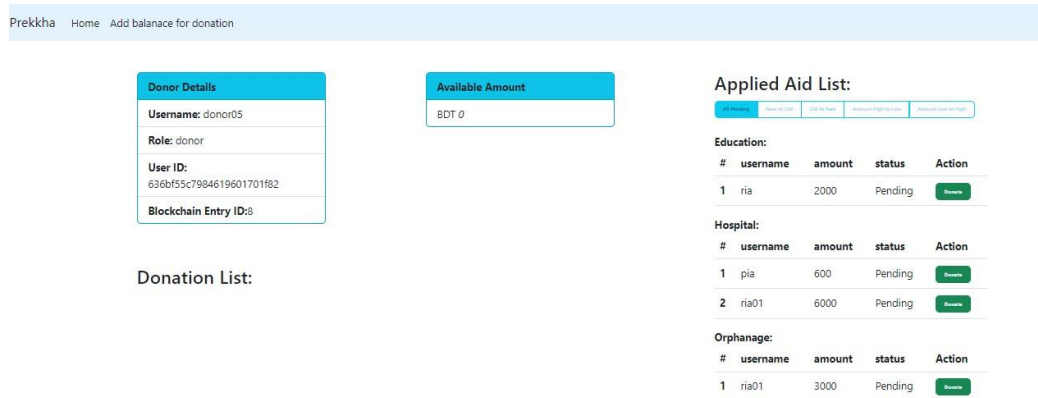


Figure 5.4: Donors Dashboard.

account and later that money can be transferred to the beneficiaries. When a donor deposits money against his or her name, a confirmation like Figure 5.6 is shown to the donor.

An admin can view details about donors, such as, number of donors are currently active in the system, total donated amount, beneficiary details etc. as well as all the request list which are shown in Figure 5.7 & 5.8. After a beneficiary has applied for financial aid, the first task of the admin is to verify whether the beneficiary, for example, university student is in actual need of that aid. After the verification, the admin will approve the application and it will automatically be uploaded to the system which can be visible to donor's end. Second task of the admin is to approve the transaction from donors to the beneficiary as shown in Figure 5.9. Later on, that transaction details are stored in the blockchain for future purpose.

Figure 5.10, 5.11, 5.12 & 5.13 shows interaction between users and the blockchain. Ganache is a local blockchain simulator. It is used to develop, deploy and test decentralized applications or smart contracts. We used ganache as our local blockchain for our project. After the user initially registers, the information generates into hashed that the users provide and passes to our local blockchain. From there, we get multiple type return values, one is a block ID, and another is a user ID for

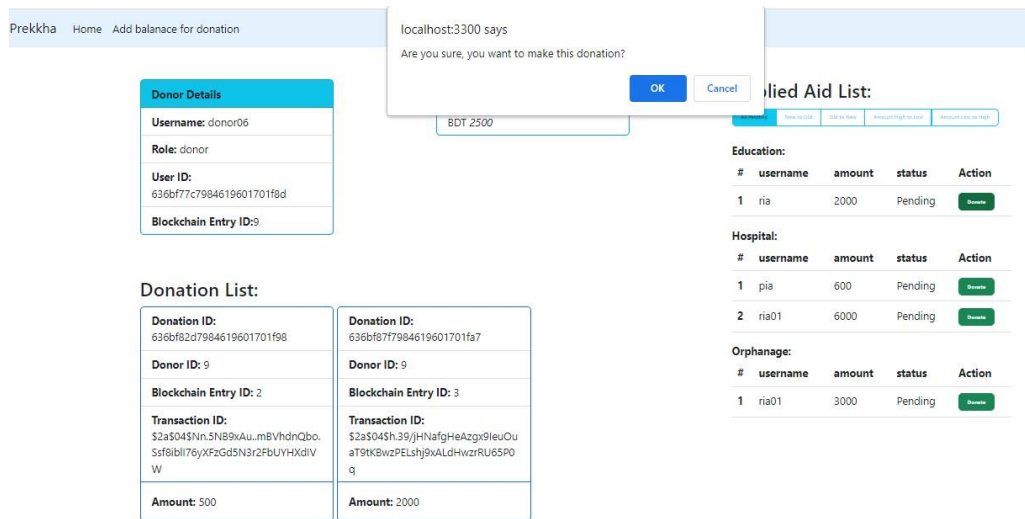


Figure 5.5: Donors Dashboard.

the local database (MongoDB). Another is user type (User beneficiary or donor), and finally, the user details, which returns upon call a message donation ID, user ID, Blockchain user ID, Bank name, Bank account number, donation amount, and transaction ID.

The Figure 5.10 shows the Blockchain entry when a user is created. With 4 key information, user's Blockchain ID, corresponding user ID from mongodb, roll of the user and user details are stored in the Blockchain.

Figure 5.11 shows, information when a donor deposits money to Prekkha's dedicated account in order to provide donation. We temporary hold this amount before he or she chooses a beneficiary from the aid list.

Figure 5.12 show the current and previous balance of a donor which is stored in the Blockchain. This amount automatically updates whenever a donor deposits money to Prekkha's account or provides aid to someone.

Figure 5.13 shows the details when a beneficiary applies for a donation. All the information regarding that particular application, such as beneficiary name, Id, reason of donation, authorizer etc. are stored in the Blockchain.

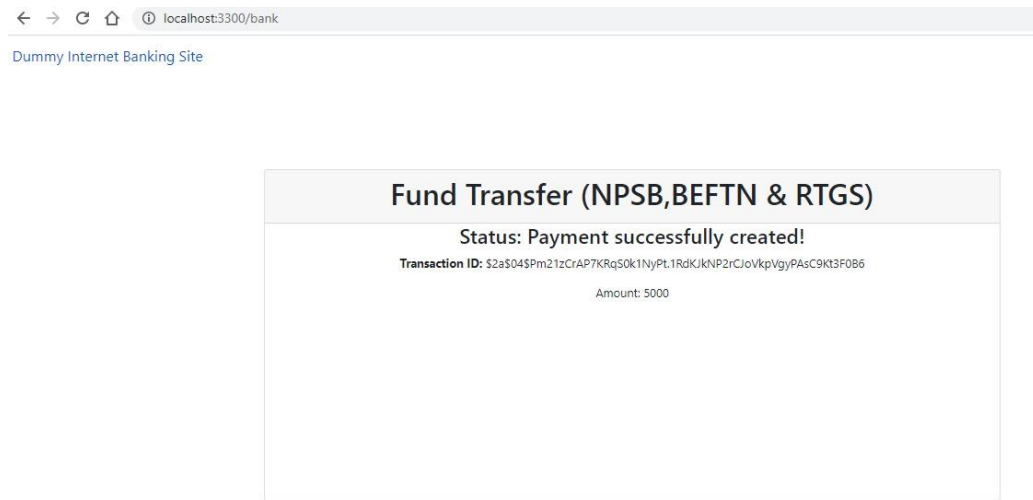


Figure 5.6: Transaction Completion.

All Donors

Donor ID: 635983a30725ca6bde7983ab
Donor Blockchain ID: 6
Donated Amount: 600
Bank Name: Dummy Bank Name Limited
Bank Account Number: 15682526282636
Donation ID: 635983a30725ca6bde7983ab
Donation Entry ID in Blockchain: 1
Beneficiary Blockchain ID: undefined
Transaction ID: \$2a\$04\$UyJyFP6NtGzgcLuOqxXgmOt.X.v7FGd Z.yF7Uflo9bPcsiKhHVk/q

Figure 5.7: Admin Dashboard.

Prekkha Home Logout		
All Financial Aid Requests		
Purpose: Education Aid ID: 636be84c7984619601701ef6 Amount: 2000 Bank Name: city bank Bank Account: 090876543 Authorizer Name: ULAB Authorizer Details: 01913000000 Beneficiary ID: 636be8037984619601701eef Beneficiary Blockchain ID: 2 Aid Entry ID in Blockchain: 1 Aid Description: aid for tuition fees. Status: Donated Applied at: Thu Nov 10 2022 01:03:05 GMT+0600 (Bangladesh Standard Time) Verification status: Verified	Purpose: Education Aid ID: 636be90d7984619601701f02 Amount: 2000 Bank Name: city bank Bank Account: 098764000 Authorizer Name: ULAB Authorizer Details: 018000009 Beneficiary ID: 636be8cd7984619601701efb Beneficiary Blockchain ID: 3 Aid Entry ID in Blockchain: 2 Aid Description: aid request for tuition fees Status: Donated Applied at: Thu Nov 10 2022 01:03:05 GMT+0600 (Bangladesh Standard Time) Verification status: Verified	Purpose: Medical Aid ID: 636be9c27984619601701f18 Amount: 6000 Bank Name: city bank Bank Account: 987654000 Authorizer Name: DMC Authorizer Details: 01709090 Beneficiary ID: 636be98d7984619601701f11 Beneficiary Blockchain ID: 5 Aid Entry ID in Blockchain: 3 Aid Description: aid request for medical issue Status: Pending Applied at: Thu Nov 10 2022 01:03:05 GMT+0600 (Bangladesh Standard Time) Verification status: Verified

Figure 5.8: Admin Dashboard.

All Financial Aid Requests

Purpose: Education
Aid ID: 6356965e4860eb3ae0a48127
Amount: 300
Bank Name: city bank
Bank Account: 097675478
Authorizer Name: ulab
Authorizer Name: ulab
Authorizer Details: 01000000
Beneficiary ID: 635695ec4860eb3ae0a48120
Beneficiary Blockchain ID: 1
Aid Entry ID in Blockchain: 1
Aid Description: want aid for education purpose
Status: Approved

localhost:3300 says
Insufficient Balance available in Blockchain Ledger.

OK

Amount: 5000
Bank Name: testBank
Bank Account: 12345678
Authorizer Name: mdSiam
Authorizer Name: mdSiam
Authorizer Details: 01832000000
Beneficiary ID: 63597ec53318bbd9e053321b
Beneficiary Blockchain ID: 3
Aid Entry ID in Blockchain: 2
Aid Description: xydru
Status: Pending
Approve

Amount: 5000
Bank Name: testBank
Bank Account: 12345678
Authorizer Name: mdSiam
Authorizer Name: mdSiam
Authorizer Details: 01832000000
Beneficiary ID: 63597ec53318bbd9e053321b
Beneficiary Blockchain ID: 3
Aid Entry ID in Blockchain: 3
Aid Description: https://github.com/Siam9717
Status: Pending
Approve

Figure 5.9: Admin Dashboard.

ACCOUNTS

BLOCKS

TRANSACTIONS

CONTRACTS

EVENTS

LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK
33

GAS PRICE
20000000000

GAS LIMIT
6721975

HARDFORK
MUIRGLACIER

NETWORK ID
1337

RPC SERVER
HTTP://127.0.0.1:8545

MINING STATUS
AUTOMINING

WORKSPACE
PREKKHA

SWITCH

← BACK

0x0b5b29fd1508246ff32e6caf0ee1c3a709d0125eb65d7603de9a61aebf9ec90a (0)

CONTRACT NAME
Prekkha

CONTRACT ADDRESS
0x28459992C638e7C85e86aBBEDCcFdC43a68449EF

SIGNATURE (DECODED)
UserCreated(id: uint256, user_id: string, user_type: string, user_details: string)

TX HASH
0x0b5b29fd1508246ff32e6caf0ee1c3a709d0125eb65d7603de9a61aebf9ec90a

LOG INDEX
0

BLOCK TIME
2022-11-10 00:54:53

RETURN VALUES

ID
9

USER_ID
636bf77c7984619601701f8d

USER_TYPE
donor

Figure 5.10: User Creation in Blockchain.

ACCOUNTS

BLOCKS

TRANSACTIONS

CONTRACTS

EVENTS

LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK

33

GAS PRICE

20000000000

GAS LIMIT

6721975

HARDFORK

MUIRGLACIER

NETWORK ID

1337

RPC SERVER

HTTP://127.0.0.1:8545

MINING STATUS

AUTOMINING

WORKSPACE

PREKKHA

SWITCH

CONTRACT NAME

Prekkha

CONTRACT ADDRESS

0x28459992C638e7C85e86aBBEDcFdC43a68449EF

SIGNATURE (DECODED)

DonationCreated(id: uint256, donor_id: uint256, amount: uint256, donation_details: string)

TX HASH

0x107750e040e0ad7ebee73d5efa08a26442c3d38ab2934a23d7dc1da16fa8070

LOG INDEX

0

BLOCK TIME

2022-11-10 00:59:14

RETURN VALUES

ID

3

DONOR_ID

9

AMOUNT

2000

Figure 5.11: Transaction of a Donation.

ACCOUNTS

BLOCKS

TRANSACTIONS

CONTRACTS

EVENTS

LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK

GAS PRICE

GAS LIMIT

HARDFORK

NETWORK ID

RPC SERVER

MINING STATUS

WORKSPACE

SWITCH

33

20000000000

6721975

MUIRGLACIER

1337

HTTP://127.0.0.1:8545

AUTOMINING

PREKKHA

BACK

0xb803efcc8241fed8b8044639981694f5321757bf9ddc58d2ef6280a84c6b84f3 (1)

CONTRACT NAME

CONTRACT ADDRESS

Prekkha

0x28459992C638e7C85e86aBBEDCcFdC43a68449EF

SIGNATURE (DECODED)

WalletUpdated(user_id: uint256, previous_amount: uint256, current_amount: uint256)

TX HASH

LOG INDEX

BLOCK TIME

0xb803efcc8241fed8b8044639981694f5321757bf9ddc58d2ef6280a84c6b84f3

1

2022-11-10 01:00:58

RETURN VALUES

USER_ID

9

PREVIOUS_AMOUNT

2500

CURRENT_AMOUNT

500

Figure 5.12: Amount Update.

ACCOUNTS

BLOCKS

TRANSACTIONS

CONTRACTS

EVENTS

LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK

GAS PRICE

GAS LIMIT

HARDFORK

NETWORK ID

RPC SERVER

MINING STATUS

WORKSPACE

SWITCH

33

20000000000

6721975

MUIRGLACIER

1337

HTTP://127.0.0.1:8545

AUTOMINING

PREKKHA

SIGNATURE (DECODED)

BeneficiaryUpdated(id: uint256, beneficiary_id: string, amount: uint256, beneficiary_details: string, status: bool, verified: bool)

TX HASH

LOG INDEX

BLOCK TIME

0xb803efcc8241fed8b8044639981694f5321757bf9ddc58d2ef6280a84c6b84f3

0

2022-11-10 01:00:58

RETURN VALUES

ID

1

BENEFICIARY_ID

636be84c7984619601701ef6

AMOUNT

2000

BENEFICIARY_DETAILS

{ "user_id": "636be8037984619601701eef", "user_name": "ria", "bc_user_id": "2", "bank_name": "city bank", "bank_account": "090876543", "amount": 2000, "authorizer_name": "ULAB", "authorizer_phone": "01913000000", "purpose": "education", "details": "aid for tuition fees.", "bc_entry_id": null, "id": "636be84c7984619601701ef6", "timestamp": "2022-11-09T17:50:04.645Z", "__v": 0 }

Figure 5.13: Acceptors Getting Their Aids.

5.4 Smart Contract

A smart contract named "prekkha.sol" has been created according to necessary requirements of the system. Firstly, few public variables, such as, mainBalance, userCount, donationCount, aidRequestAmount etc., multiple struct (user structure for data collection) has been initialized at the beginning of the smart contract. These struct is mapped with users, donations and beneficiaries for transaction. Few events have also been created for new user, donation, beneficiary and aid application entry so that data can be fetched at the time of necessity. For creating and starting users and transaction, multiple public functions, such as, userRegistration, makeDonation, aidRequest, approveRequest, has been used. Necessary data can be stored and fetched using these functions into and from the Blockchain.

5.5 Exception Handling

If a donor does not have sufficient amount or more amount than the donated amount in his name at Prekkha's dedicated bank amount then the transaction will revert and go back to its initial phase. This exception will be handled by Prekkha's smart contract.

Whenever a donor deposits certain amount in the Prekkha's bank account, that transaction is cross checked by transaction id and amount. This will ensure that that particular transaction is actually made by a donor. Moreover, we kept uniqueness while checking the transaction id which ensures a transaction id is not used twice or more.

5.6 Analysis

This project has some limitations with the features as this is a prototype and we had time constraints. So very few features have been implemented. Although, after the analysis of the results of the system, Prekkha is the only local donation system that does not use any middleman, the donation is fully automated and functional

without any third-party involvement. At the same time, it could be the reason for the disruption if the bank API stops working for a reason. It will halt the donation process and the whole system.

```
Deploying 'Prekkha'
-----
> transaction hash: 0xb3a95d011174d73ec8442513f6e2bc3b76ff5a0a0acf67b70fcc48782210cce3
> Blocks: 0          Seconds: 0
> contract address: 0x666E7eE11840E97b6cEDA33a0954131dFE6672E4
> account:          0xAe824D538cd58BB317345fE6b80CBfA72FD27F2d
> balance:          99.97039746
> gas used:         1300408
> gas price:        20 gwei
> value sent:       0 ETH
> total cost:       0.02600816 ETH

> Saving artifacts
-----
> Total cost:       0.02600816 ETH
```

Figure 5.14: Blockchain Transaction of Prekkha.

Figure 5.14 represents our system's contract deployment. It shows transaction hash which refers to, sometimes as a transaction ID, given to each and every transaction on the blockchain. The term "transaction" is sometimes replaced with the acronyms "tx" or "txn". The contract address of the smart contract controls the balances of all token holders and it is the location of the given address. Total gas used 1300408 for deployment the contract. Total cost 0.02600816 ETH and remaining balance 99.97039746 ETH.

5.7 Security

Due to Ganache, our application is also protected from attacks by Sybil, Race, and Eclipse. Ganache simulates the Ethereum private blockchain and has built-in protection against attacks like Sybil, Race, and Eclipse (25). The Casper algorithm (24) is used by Ganache to defend against Sybil. By restricting the amount of incoming and outgoing links that leave Ganache. When a transaction is sent on the

blockchain, Ganache automatically mines it and adds it to a block. Race attack is not relevant to the application due to the Ethereum network. Replay assault may be used against them because it was created on a non-fork blockchain.

5.8 Cost Analysis

This is the part where the total development cost of any project is discussed. In Prekkha, the total development stage is about 20 weeks, which is equal to 5 months. So, the cost analysis of Prekkha is given below:

Table 5.1: Tentative Budget of Prekkha

Cost Type	Description	Cost
Hardware Cost	1 Router 3 Computers Computer 1: Tk. 1,20,000/=	Tk. 1500/=
	Computer 2: Tk. 90,000/=	Tk. 2,60,000/=
	Computer 3: Tk. 70,000/=	
Software Cost	We have used all the working tools for free	Tk. 0/=
Developer Cost (Salary)	2 Senior Developer	Tk. 4,50,000/=
	Period: 5 months (20 weeks)	
	Tk. 50,000/= per month	
	1 Senior Developer	Tk. 1,50,000/=
	Period: 5 months (20 weeks)	
	Tk. 30,000/= per month	
Maintenance Cost	Period: 5 months (20 weeks)	
	Monthly maintenance cost = Tk. 3,000/=	Tk. 15,000/=
	Monthly internet bill = Tk. 1,000/=	Tk. 5,000/=
Other Cost	Operational cost, chair, table, rent etc.	Tk. 80,000/=
	Total Cost	Tk. 8,81,500/=

Table 5.1 shows the whole cost of the project that is required to complete this project. There are mainly 4 core costs during the development of Prekkha, which are hardware cost, software cost, developer cost, maintenance cost, and other extra costs. During the development of the project, we didn't need that much hardware; we

only required a Router that provides the internet and 3 computers for 3 developers to develop the system.

3 Computer Cost: $1,20,000 + 90,000 + 70,000 = 2,60,000$ Taka.

Total Hardware Cost is $2,60,000 + 1,500 = 2,61,500$ Taka. including a router which costs 1500 taka.

During the development stage, we didn't use any paid version of the software. All software that is required for the development of this prototype is available online free of cost. So, there is no software cost right now but in the future production level, we require multiple software and services that need to be bought and which will add software cost. A big chunk of the cost goes to the developer's salary. This is the maximum cost during the development. There are a total of 3 developers which include 2 senior and 1 junior developer and the total development period is 20 weeks which is equivalent to 5 months.

Senior Developer salary (5 months): $45,000 * 5 * 2 = 4,50,000$ Taka Junior Developer salary (5 months): $30,000 * 5 = 1,50,000$ Taka Total Developer Salary (5 months): $4,50,000 + 1,50,000 = 6,00,000$ Taka

Monthly (5 months) maintenance cost is 3000 Taka and the monthly (6 months) internet cost is 1000 Taka. Total Maintenance Cost: $(3000*5) + (900*6) = 20,400$ Taka

There are some other costs which include rent, chair, table, operational, etc. Cost is: 80,000 Taka. So, the total cost of developing this project is: $= 1400 + 2,60,000 + 6,00,000 + 20,400 = 8,81,500$ Taka

5.9 Conclusion

This concludes the cost analysis section of our system. In the next chapter we have summarized our entire project and also discussed its social, ethical, legal and environmental issues. Since we are in the development period, we have plenty of scopes of future development which is also discussed in the next chapter.

Chapter 6

Conclusion

6.1 End Words

In this report, we have putted forward blockchain based donation system that allows donors to donate for the causes presented to them through our system. We have made use of blockchain technology to mitigate corruption and fraud involved in the donation process, so that the donors feel comfortable using our system. We have also made sure that there are no irregularities in the distribution of the donated money. We have utilized smart contract that acts as a mediator between the donors and beneficiaries, removing the middlemen. Our project also stores each transaction data in the blockchain so that if anyone wants to audit the system for irregularities, they always get the authentic data, since the data stored in the blockcain is immutable.

6.2 Social, Legal, Ethical & Environmental Issues

Prekkha is a large-scale non-profit project. As we are trying to solve a problem that exists in our society for a long time, it has a huge impact on society. We have tried to remove the middleman from the donation process, who has previously played a huge role in distribution of donation and management for their respective organization or charity. But in many cases, they are responsible for various damages to the sector by losing trust on this kind of organization which have a great impact on our society. Now no students have to delay their education as they could use our system to ask for the financial support they require, in the same manner, patients will no longer have to delay or halt their lifesaving medication as they also ask for

financial support.

As for legal & ethical issues we have faced and addressed many problems. For example, now the beneficiary is able to get a fair donation and as we keep the donation transparent. Also, donors get satisfied by seeing their donations are utilised properly and reached to the right person. In the past, some corrupt organization raised the fund & did not give the fund to people who seeks supports. Our system solves this problem.

As for the environmental perspective, our system will play an important role. Beneficiaries will observe environmental effects after they stop engaging in any risky everyday activities and start receiving donations. When they pause, the environment supports the shift in perspective and greatly reduces waste. Prekkha runs on Ethereum blockchain, and it requires miner to solve computationally extensive puzzles to add data to the block. This solving of the puzzle requires a lot of power, that is electricity. As electricity is produced by burning coal or crude oils this adds to the pollution. But Ethereum finally moved on to the Proof of Stake consensus, this requires a different method to validate blocks that requires significantly less electricity so it is better for the environment.

6.3 Future Works

As we are working on the Development level, we haven't deployed our system in the production environment. But in the future, we have a lot of planning for this project. Now we are working on a single machine block-chain server but in the future, we are going to deploy this block-chain server in the public Ethereum network. We have a plan to make our system more robust and include features by adding some high-level algorithms & security protocols, which are currently required licenses for using. For the general data store, we have used a regular free version of MongoDB, which has a data limitation cap because it is neither local nor paid, but in the future, we are going to use an unlimited storage plan. As of now, our system supports only one language which is English, in the future we will also make our system support multiple languages. Currently, we have only web application, but we have a plan to develop cross-platform. We are also determined to reach out to as many people

as possible to do this we will add some features, which will attract more people to join our platform. One of the features that we will add is rewarding options, where donors can get a reward point based on their service, which they can use to get some discount on products.

References

- [1] Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, 36, 55–81
- [2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Consulted, 2008.
- [3] G. Wood, "Ethereum: A secure decentralized generalized transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, 2014.
- [4] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, "Mixcoin: Anonymity for bitcoin with accountable mixes," in *Proc. Financial Cryptogr. Data Secur.-18th Int. Conf. (FC) in Lecture Notes in Computer Science*, vol. 8437, N. Christin and R. Safavi-Naini, Eds. Christ Church, Barbados: Springer Mar. 2014, pp. 486–504
- [5] Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview.
- [6] A. S. Tanenbaum and M. Van Steen, *Distributed systems: principles and paradigms*. Prentice-Hall, 2007
- [7] D. Drescher, "Blockchain basics," Springer, Tech. Rep. Rigoberto, J. and Daza, P., "Economy of Non-Profit Organizations Charities and Donations", p6-8, (2010).
- [8] Rigoberto, J. and Daza, P., "Economy of Non-Profit Organizations Charities and Donations", (2010).
- [9] Choo, K.-K. R. (2013). New payment methods: A review of 2010–2012 FATF mutual evaluation reports. *Computers & Security*, 36, 12–26.
- [10] Sirisha, N. S., "Blockchain", Proposed Solution For Trackable Donations Using Blockchain, (Icнте): 3–7 (2019).
- [11] Pollach, I., Treiblmaier, H., and Floh, A., "Online Fundraising for Environmental Nonprofit Organizations", (2005).

- [12] Bellini, E., Iraqi, Y., & Damiani, E. (2020). Blockchain-based distributed trust and Reputation Management Systems: A survey. *IEEE Access*, 8, 21127–21151
- [13] FERWANA, E. A. (2021). A BLOCKCHAIN BASED TRACKING SYSTEM FOR UNIVER SITY DONATION.
- [14] Rabbani, M. R., Khan, S., & Thalassinos, E. I. (2020). Fintech, Blockchain and Islamic Finance: an extensive literature review. *International Journal of Economics and Business Administration*, VIII(Issue 2), 65–86.
- [15] Hu, Y., Manzoor, A., Ekparinya, P., Liyanage, M., Thilakarathna, K., Jourjon, G., & Seneviratne, A. (2019). A delay-tolerant payment scheme based on the Ethereum blockchain. *IEEE Access*, 7, 33159–33172.
- [16] Hao, Z., Ji, R., & Li, Q. (2018). FastPay: A secure fast payment method for edge-IOT platforms using blockchain. 2018 IEEE/ACM Symposium on Edge Computing (SEC).
- [17] Yang, Y., Lin, H., Liu, X., Guo, W., Zheng, X., & Liu, Z. (2019). Blockchain-based verifiable multi-keyword ranked search on encrypted cloud with fair payment. *IEEE Access*, 7, 140818–140832
- [18] Lin, C., He, D., Huang, X., Khan, M. K., & Choo, K.-K. R. (2020). DCAP: A secure and efficient decentralized conditional anonymous payment system based on Blockchain. *IEEE Transactions on Information Forensics and Security*, 15, 2440–2452.
- [19] Ahamed, S., Siddika, M., Islam, S., Anika, S. S., Anjum, A., & Biswas, M. (2021). BPS: Blockchain based decentralized secure and versatile light payment system. *Asian Journal of Research in Computer Science*, 12–20.
- [20] TEKGUC, U., ADALIER, A., & YURTKAN, K. (2020). ScholarChain: The Scholarship Management Platform with Blockchain and Smart Contracts Technology. *The Eurasia Proceedings of Educational & Social Sciences (EPESS)*, 2020, Volume 18, 86–91.
- [21] Rashid, M. A., Deo, K., Prasad, D., Singh, K., Chand, S., & Assaf, M. (2020). TEduChain: A blockchain-based platform for crowdfunding tertiary education. *The Knowledge Engineering Review*, 35.
- [22] Junfithrana, A. P., Liani, E., Suwono, M. Z., Meldiana, D., & Suryana, A. (2018). Rice donation system in orphanage based on internet of things, raspberry-pi, and Blockchain. 2018 International Conference on Computing, Engineering, and Design (ICCED).

- [23] Cocco, L., Pinna, A., & Marchesi, M. (2017). Banking on blockchain: Costs savings thanks to the blockchain technology. *Future Internet*, 9(3), 25.
- [24] Turkanovic, M., Holbl, M., Kasic, K., Hericko, M., & Kamisalic, A. (2018). EduCTX: A blockchain-based higher education credit platform. *IEEE Access*, 6, 5112–5127.
- [25] Bedi, P., Gole, P., Dhiman, S., & Gupta, N. (2020). Smart contract-based Central Sector Scheme of scholarship for college and University Students. *Procedia Computer Science*, 171, 790–799.
- [26] Lundqvist, T., de Blanche, A., & Andersson, H. R. (2017). Thing-to-thing electricity micro payments using blockchain technology. 2017 Global Internet of Things Summit (GloTS).
- [27] NGUYEN, V.-C., PHAM, H.-L., TRAN, T.-H., HUYNH, H.-T., & NAKASHIMA, Y. (2019). Digitizing invoice and managing VAT payment using blockchain smart contract. 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC).
- [28] Yadav, A., Yadav, D., Gupta, S., Kumar, D., & Kumar, P. (2018). Online food court payment system using blockchain technology. 2018 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON).
- [29] Ainsworth, R. T., & Alwohaibi, M. (2017). Blockchain, Bitcoin, and VAT in the GCC: The missing trader example. *SSRN Electronic Journal*.
- [30] Si, H., Cai, Y., & Cheng, Z. (2010). An improved RSA signature algorithm based on complex numeric operation function. 2010 International Conference on Challenges in Environmental Science and Computer Engineering.
- [31] Vujicic, D., Jagodic, D., & Randic, S. (2018). Blockchain technology, Bitcoin, and Ethereum: A brief overview. 2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH).
- [32] Zheng, Z., Xie, S., Dai, H.-N., Chen, W., Chen, X., Weng, J., & Imran, M. (2020). An overview on smart contracts: Challenges, advances, and platforms. *Future Generation Computer Systems*, 105, 475–491.
- [33] Papadodimas, G., Palaiokrasas, G., Litke, A., & Varvarigou, T. (2018). Implementation of smart contracts for blockchain based IOT Applications. 2018 9th International Conference on the Network of the Future (NOF).
- [34] Khalid, U., Asim, M., Baker, T., Hung, P. C., Tariq, M. A., & Rafferty, L. (2020). A decentralized lightweight blockchain-based authentication mechanism for IoT systems. *Cluster Computing*, 23(3), 2067–2087.

- [35] Boudguiga, A., Bouzerna, N., Granboulan, L., Olivereau, A., Quesnel, F., Roger, A., & Sirdey, R. (2017, April). Towards better availability and accountability for iot updates by means of a blockchain. In 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 50-58). IEEE.
- [36] Ortega, V., Bouchmal, F., & Monserrat, J. F. (2018). Trusted 5G vehicular networks: Blockchains and content-centric networking. *IEEE Vehicular Technology Magazine*, 13(2), 121-127.
- [37] Popa, A. B., Stan, I. M., & Rughinis, R. (2018). Instant payment and latent transactions on the Ethereum blockchain. 2018 17th RoEduNet Conference: Networking in Education and Research (RoEduNet).
- [38] Wright, C. S. (2008). Bitcoin: A peer-to-peer electronic cash system. *SSRN Electronic Journal*.
- [37] Poon, J., & Dryja, T. (2016). The bitcoin lightning network: Scalable off-chain instant payments.
- [38] Hao, Z., Ji, R., & Li, Q. (2018, October). FastPay: a secure fast payment method for edge-IoT platforms using blockchain. In 2018 IEEE/ACM Symposium on Edge Computing (SEC) (pp. 410-415). IEEE.
- [39] Vujicic, D., Jagodic, D., & Randic, S. (2018). Blockchain technology, Bitcoin, and Ethereum: A brief overview. 2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH).
- [40] Van Steen, M., & Tanenbaum, A. (2002). Distributed systems principles and paradigms. *Network*, 2, 28.
- [41] Tama, B. A., Kweka, B. J., Park, Y., & Rhee, K.-H. (2017). A critical review of Blockchain and its current applications. 2017 International Conference on Electrical Engineering and Computer Science (ICECOS).
- [42] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access*, 4, 2292–2303.
- [43] Shah, J., & Parveen, S. (2021). Understanding the blockchain technology beyond bitcoin. *Lecture Notes in Mechanical Engineering*, 499–516.
- [44] King, S. (2013). Primecoin: Cryptocurrency with prime number proof-of-work. July 7th, 1(6).
- [45] King, S., & Nadal, S. (2012). Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. selfpublished paper, August, 19(1).

- [46] Ranganathan, V. P., Dantu, R., Paul, A., Mears, P., & Morozov, K. (2018). A decentralized marketplace application on the ethereum blockchain. 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC).
- [47] Kavun, E. B., & Yalcin, T. (2010). A lightweight implementation of Keccak hash function for radiofrequency identification applications. *Radio Frequency Identification: Security and Privacy Issues*, 258–269.
- [48] Lin, C., He, D., Huang, X., Khan, M. K., & Choo, K.-K. R. (2020). DCAP: A secure and efficient decentralized conditional anonymous payment system based on Blockchain. *IEEE Transactions on Information Forensics and Security*, 15, 2440–2452.
- [49] Moubarak, J., Filiol, E., & Chamoun, M. (2018). On blockchain security and relevant attacks. 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM).
- [50] Aggarwal, S., & Kumar, N. (2021). Attacks on Blockchain. *Advances in Computers*, 399–410.
- [51] Zou, W., Lo, D., Kochhar, P. S., Le, X. B. D., Xia, X., Feng, Y., ... & Xu, B. (2019). Smart contract development: Challenges and opportunities. *IEEE Transactions on Software Engineering*, 47(10), 2084–2106.
- [52] Vujicic, D., Jagodic, D., & Randic, S. (2018). Blockchain technology, Bitcoin, and Ethereum: A brief overview. 2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH).
- [53] Poon, J., & Dryja, T. (2016). The bitcoin lightning network: Scalable off-chain instant payments.
- [54] McLeod, S. (2007). Maslow's hierarchy of needs. *Simply psychology*, 1(1-18).
- [55] Netzer, D. (2020). Non-profit organizations. In *Handbook of Cultural Economics*, Third Edition. Edward Elgar Publishing.
- [56] Marcinkevage, C. H. (2020). Critical Success Factors of Constituent Relationship Management (CRM) Strategy in a Higher Education Institution.
- [57] Mainetti, L., Patrono, L., & Vergallo, R. (2012, September). IDA-Pay: an innovative micro-payment system based on NFC technology for Android mobile devices. In *SoftCOM 2012, 20th International Conference on Software, Telecommunications and Computer Networks* (pp. 1-6).
- [58] Handforth, B., Hennink, M., & Schwartz, M. B. (2013). A qualitative study of nutrition-based initiatives at selected food banks in the Feeding America Network. *Journal of the Academy of Nutrition and Dietetics*, 113(3), 411–415.

- [59] Baggett, J. P. (2001). Habitat for humanity: Building private homes, building public religion. Temple University Press.
- [60] Humanitarian Aid Organization for Children. (1998). Save the Children.
- [61] Huda, S. S., Akhtar, A., & Maliha, S. R. (2021). Initiatives taken by NGOs and private companies to fight the COVID-19 pandemic. *International Journal of Work Organisation and Emotion*, 12(1), 86-92.
- [62] Kumar, B., Kamal, R. S., Parvin, R. A., & Wares, N. M. (2021). Assessing the impact of COVID-19 pandemic on vulnerable populations in Bangladesh.
- [63] Chowdhury, A. M. R., & Bhuiya, A. (2004). The wider impacts of BRAC poverty alleviation programme in Bangladesh. *Journal of international development*, 16(3), 369-386.
- [64] WFH Foundation - non-profit organization in Bangladesh. WFH Foundation - Non-Profit Organization in Bangladesh. (2022, May 7).
- [65] Karim, M. R. (2015). Dhaka Ahsania Mission.
- [66] Talekar, S. (2008). WebStorm: Web based support tool for organization of requirements modeling.
- [67] Duckett, J. (2011). HTML & CSS: design and build websites (Vol. 15).
- [68] Crockford, D. (2008). JavaScript: The Good Parts: The Good Parts.
- [69] Tilkov, S., & Vinoski, S. (2010). Node. js: Using JavaScript to build high-performance network programs. *IEEE Internet Computing*, 14(6), 80-83.
- [70] Ali, J. (2013). Instant Node Package Manager.
- [71] Laaziri, M., Benmoussa, K., Khouilji, S., Larbi, K. M., & El Yamami, A. (2019). A comparative study of laravel and symfony PHP frameworks. *International Journal of Electrical and Computer Engineering*, 9(1), 704.
- [72] Dhillon, V., Metcalf, D., & Hooper, M. (2017). Blockchain enabled applications.
- [73] Dannen, C. (2017). Introducing Ethereum and solidity (Vol. 1, pp. 159-160).
- [74] Mohanty, D. (2018). Deploying smart contracts. In *Ethereum for Architects and Developers* (pp. 105-138).
- [75] Lee, W. M. (2019). Using the web3. js APIs. In *Beginning ethereum smart contracts programming* (pp. 169-198).
- [76] Taş, R., & Tanrıö ver, Ö . Ö . (2019, October). Building a decentralized application on the Ethereum blockchain. In *2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)* (pp. 1-4).

Please use the following page format for the cover of your report.

Prekkha: A Blockchain Based Platform to Track and Provide Financial Aid

by

**Mir Nushrat Zahan Tirumony
181014074**

**Md. Arifur Rahman
183014017**

**Md Siam Reza Akash
183014056**

Capstone project report for the degree of

Bachelor of Science in Computer Science and Engineering



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
UNIVERSITY OF LIBERAL ARTS BANGLADESH**

SUMMER 2022