

Report On
Electronic Voting System Based on Blockchain

By

Tanvir Ahmed
21373001

A project report submitted to the Computer Science and Engineering in partial fulfillment of the requirements for the degree of M.Engg. in Computer Science and Engineering

Computer Science and Engineering
BRAC University
September 2022

© 2022. Brac University
All rights reserved.

Declaration

It is hereby declared that

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

Student's Full Name & Signature:

Tanvir

Tanvir Ahmed
20166021

Approval

The Project titled “Electronic Voting System Based on Blockchain” submitted by,

Tanvir Ahmed (21373001)

Of spring, 2022 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of M.Engg in Computer Science and Engineering on May 26, 2022.

Examining Committee:

Supervisor:



Moin Mostakim

Lecturer

Department of Computer Science and Engineering, BRAC University

Program Coordinator:

Amitabha Chakrabarty, PhD

Associate Professor

Department of Computer Science and Engineering, BRAC University

Head of Department:

Sadia Hamid Kazi

Chairperson and Associate Professor

Department of Computer Science and Engineering, BRAC University

Letter of Transmittal

Moin Mostakim

Lecturer,

Department

BRAC University

66 Mohakhali, Dhaka-1212

Subject: Master's project report on electronic voting system based on Blockchain.

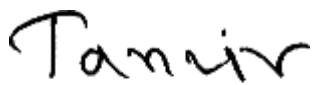
Dear Sir,

This is my pleasure to display my Master's project report on electronic voting system based on blockchain.

I have attempted my best to finish the report with the essential data and recommended proposition in a significant compact and comprehensive manner as possible.

I trust that the report will meet the desires.

Sincerely yours,



Tanvir Ahmed

21373001

Computer Science and Engineering

BRAC University

Date: September 08, 2022

Abstract

The primary goal of this application is to create a voting app which is safe and the result is unchangeable. By using blockchain technology these goals can be achieved. Data in blockchain is not stored in only one location and the administration responsibility do not belong to any person. All the data of a blockchain is stored in different locations. The blockchain is instead duplicated and dispersed among many computers in a network. Every computer on the network updates its blockchain each time a new block is added to the blockchain to reflect the change. In this application anyone can create a voting poll and the poll will be added to a block. People visiting the app will be able to see the polls and can cast a vote to the favorite candidate. And people will get to choose a winner based on the amount of vote on candidate got. Because this application is created using blockchain technology, everyone can trust this application and will be satisfied with the result they get as the result will be unbiased. This application will be useful to anyone who is willing to share their opinion and is willing to compare popularity of different persons.

Dedication

This work is dedicated to my beloved parents, loving wife and Moin Mostakim sir for guiding and bearing with me during this period with love and patience.

Acknowledgement

I have taken efforts in this project. However, it would not have been possible without the kind support and help of many individuals and organizations. I would like to extend my sincere thanks to all of them. I am highly indebted to Moin Mostakim Sir for his guidance and constant supervision as well as for providing necessary information regarding the project & also for his support in completing the project. I would like to express my gratitude towards my parents & BRAC University for their kind co-operation and encouragement which help me in completion of this project. My thanks and appreciations also go to my classmates in developing the project and people who have willingly helped me out with their abilities.

Table of Contents

Declaration.....	ii
Approval	iii
Letter of Transmittal	iv
Abstract.....	v
Dedication	vi
Acknowledgement.....	vii
List of Figures	x
List of Tables	x
List of Acronyms	xi
Glossary... ..	xii
Chapter 1 Introduction.....	1
1.1 Motivation.....	1
1.2 Project Problem	3
1.3 Aim and Objectives	4
1.4 Organization of the Report	5
Chapter 2 Background Study... ..	6
2.1 Blockchain Overview.....	6
2.2 Blockchain Current Applications	11
2.2.1 Financial Service.....	13

2.2.2 Healthcare	14
2.2.3 Business and Industry	16
2.2.4 Social Applications	17
2.2.5 Other Applications	18
2.3 Block.....	19
2.4 Blockchain Formation	20
2.5 Smart Contract	21
Chapter 3 Requirement Analysis	23
3.1 User Requirement	23
3.2 System Requirement	23
3.3 Used Platform/Tools	24
Chapter 4 Project Analysis	25
4.1 The Smart Contract.....	25
4.2 The Home Page.....	26
4.3 The Polling Station	27
4.4 The New Poll Form	28
Chapter 5 Implementing Blockchain	29
5.1 The Smart Contract.....	29
Chapter 6 Conclution and Future Work	32
6.1 Conclusion	32

6.2 Future Work	33
References	34
Appendix A	40

List of Figures

Figure 1: Concepts of Blockchain... ..	1
Figure 2: A Block... ..	3
Figure 3: Architecture of Blockchain	4
Figure 4: Application of Smart Contract	5
Figure 5: The Home Page	9
Figure 6: The Polling Station	10
Figure 7: Poll Form	11
Figure 8: Example of Change Method... ..	13
Figure 9: Example of View Methods	15

List of Tables

Figure 1: The Current Existing Cryptocurrency System	13
Figure 2: Blockchain for Healthcare	15

List of Acronyms

URL	Uniform Resource Locator
TS	Type Script
JS	Java Script
CHF	Cryptographic Hash Function
P2P	Peer-to-Peer
IDE	Integrated Development Environment
B2B	Business-to-Business
IoT	Internet of Things
HDG	Healthcare Data Gateway
EHR	Electronic Health Records

Glossary

Block	Think of a blockchain as consisting of a ledger that is being constantly updated, and those changes synced between any number of different nodes.
Blockchain	A digital ledger comprised of unchangeable, digitally recorded data in packages called blocks. Each block is ‘chained’ to the next block using a cryptographic signature. Ethereum is a public blockchain, open to the world; its digital ledger is distributed, or synced, between many nodes; these nodes arrive at consensus regarding whether a transaction is valid before encrypting a number of transactions into a block.
Decentralization	The transfer of authority and responsibility from a centralized organization, government, or party to a distributed network.

Chapter 1

Introduction

1.1 Motivation

Voting is the process of making a choice by a particular person or a group of people in order to elect. Voting is a general right for people of many countries. People generally goes to a voting poll to cast a vote for their favorite politician. Without proper voting process, there may be chaos all over the country. So, the voting process must be as honest as possible. If a government is willing to adopt to a voting app, the government must insure the protection of data. If the data is stored centrally in a server the data can be altered easily which cannot be trusted by the people of the country. But if blockchain is used to stored data, people can easily trust the system because data in blockchain cannot be manipulated. Here, I have created a sample voting application using blockchain which can be improved farther by releasing future version of the application and new features can be added in the future. At present it is a simple project where people will be able to create a voting poll and other user will be able to cast a vote to decide the winner of the poll. In this process the voters can be ensured cleanliness of the voting process and can cast vote peacefully and will be able to accept the outcome without any question.

Election integrity is not only necessary for democracies to function, but it also has a significant impact on public voters' trust and sense of accountability. Political voting procedures are crucial in this regard. From a governmental perspective, electronic voting technologies may boost voter participation, boost voter trust, and rekindle interest in the electoral process. Research has shown that using electronic voting systems can improve security. When deciding whether to implement voting system based on blockchain, one must analyze why it is thought to be preferable than a regular manual voting process.

Although it increases democracy's value and potency, but it is also anticipated to be a answer to various critical issues, such as increasing election turnout, making voting easier for the elderly and disabled, and improving accessibility to the polls. It is common knowledge that operating electronic voting systems under rigorous security measures is important, particularly when relying on the use of cutting-edge encryption technology.

A current solution to increase the propulsion of systems employed in several domains is blockchain. Most important use of blockchain at first was to keep track of cryptocurrency affairs. In contrast, new uses and applications have advanced in recent years. Recently, electronic voting system based on blockchain has grown in importance as a solution to some issues that might be related to e-voting. Due to the blockchain's immutability, which makes it a distributed, decentralized, and decentralized ballot box, voting systems based on blockchain have been proposed as the next initiation of contemporary electronic voting systems.

Electronic voting was initially suggested as a possibility to overcome the problems with manual voting and guarantee accurate and impartial elections. The security of electronic voting systems has been one of the areas that has been thoroughly addressed in the literature. Consequences of malfunction, ballot secrecy, data integrity, transparency, reliability, voters without formal education, requirement for professional security, IT skills, fraud-related issues, equipment storage, and cost are some of the challenges that using electronic voting may bring up.

A current solution to increase the propulsion of systems employed in several domains is blockchain. Most important use of blockchain at first was to keep track of cryptocurrency affairs. In contrast, new uses and applications have evolved in recent years. Recently, electronic voting system based on blockchain has grown in importance as a solution to some issues that might be related to e-voting. Due to the blockchain's immutability, which makes it a distributed, decentralized, and decentralized ballot box, voting system based on blockchain have been proposed as the next evolution of voting systems based on electronic. Governments are encouraged to embrace intelligent feasible voting systems and to incorporate continuity of information into voting systems through blockchain technology. It makes certain that everyone has accurate knowledge on sustainable assets. It's critical to note that while the electronic voting system is increasingly using blockchain to increase security, a number of problems still exist.

1.2 Project Problem

To implement blockchain as the data storage system and as the backend feature of the project is the most crucial aspect of the project. Without properly implementing blockchain the project cannot be successful because it is the main feature of the application.

1.3 Aim and Objectives

There are many application out there which allows user to participate in a voting poll. However those applications does not uses blockchain as the data storage system rather those applications uses traditional database system which stores all the user data in a single place which can be easily manipulated by the system admins. But in this application there will be use of the latest blockchain technology and the data will be distributed in a network and no one will be able to manipulate the data in this system. So, in summary the propositions are:

- The information should be stored in a blockchain database system and data should be secured.
- Users should be able to create voting polls, choose a topic and add candidates according to their choice.
- Users should be able to cast only one single vote for a particular voting poll.

1.4 Organization of the Report

The report is structured in the following manner:

- Chapter 1: Describes the motivation, organization of the report structured, aims and objective of my project work.
- Chapter 2: Explains the functionalities of blockchain and process of how the blockchain stores informations.
- Chapter 3: This chapter explains the requirements of the project. Such as, User requirements, System requirements and used platform and tools.
- Chapter 4: In this chapter the analysis of the complete project is explained. The topics include the front-end, the home page, the polling station and the new poll form.
- Chapter 5: This chapter contains the details of implementing blockchain. How the smart contract is created is explained in this chapter.
- Chapter 6: The conclusion and future work possibilities is included in this chapter.

Chapter 2

Background Study

2.1 Blockchain Overview

Haber and Stornetta first put forth the idea of the blockchain in 1991. Designing a timestamp to prevent tampering with digital documents was the major goal. First blockchain based system is known to be developed by Satoshi Nakamoto in 2008. The idea of a blockchain can be compared to an open, secure data book and distributed. So, the idea can be used not only to the financial and cryptocurrency industries but also to a wide range of other fields where transactions are involved. So, the idea is primarily regarded as a crucial part of industry applications for the times to come. Although blockchain is well recognized in the cryptocurrency industry, one could legitimately argue that its potential goes much beyond virtual currency. Government agencies as well as private businesses have started experimenting with blockchain.

Blockchain technology and distributed ledger development have sparked a number of projects in a variety of industries. A blockchain is an increasing collection of records known as blocks that are connected and secured by cryptography. Blockchains store data in blocks that are then chained together, which sets them apart from traditional databases in this regard. As each new piece of data arrives, a new block is created. The data is tied together in sequential order once the block has been packed with data and is chained onto the block previous to it.

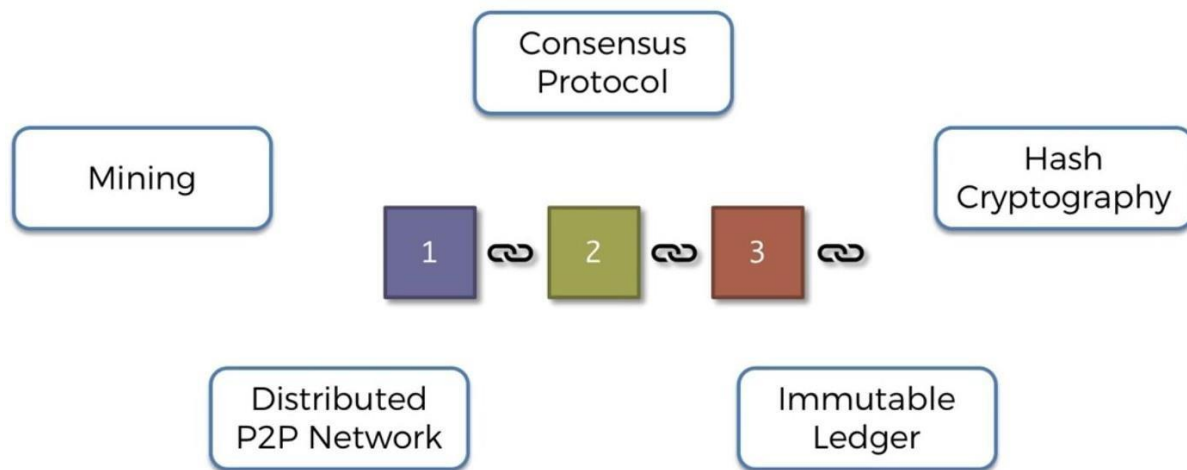


Figure 1: Concepts of Blockchain

Blockchains are distributed, usually decentralized digital ledgers that are both tamper-resistant and tamper-evident. At the most fundamental level, they allow a few users to keep track of transactions in a shared ledger so that, as long as the blockchain is performing normally, no agreement can be changed after it has been published.

Figure 2 depicts a typical example of a blockchain. Data sets consists of a chain of data packages, each of which includes some transactions, make up a blockchain. Each new block joins to the blockchain, which handles as a broad record of all transactions.

The blockchain can justify blocks by using cryptographic techniques. Along with the transactions, every block also contains a time-stamp, the cryptographic value of the block that came before it (referred to as the "parent"), a random number used to verify the cryptographic hash. This concept ensures the uprightness of the whole blockchain through the "genesis

block." Cryptographic hash values are unique and can be used to successfully identify fraud because changes to a block in the chain would instantly affect the relative hash value. If the most of nodes in the network agree via an agreement procedure that both the transactions in a block and the block itself are authentic, the block can only be then added to the blockchain.

The distributed system mentioned above provides a lot of benefits. Unlike concentrated systems, the blockchain network can still function although some nodes go down. Users have more confidence because they don't have to assess any other network participants' dependability. It is enough for users to have more faith in the system as a whole. The lack of mediators also makes security easier.

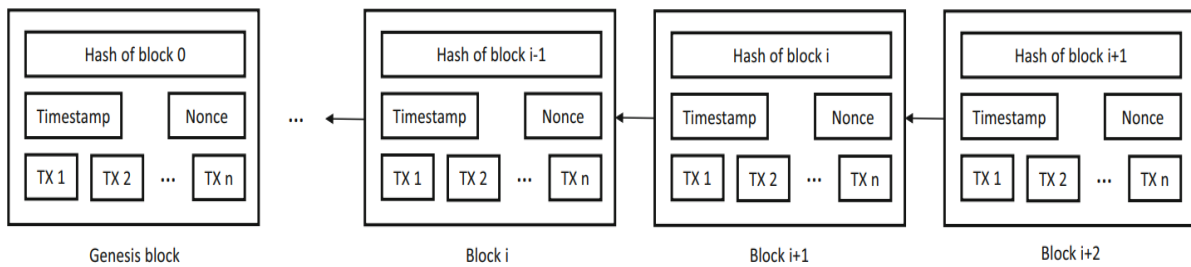


Figure 2: Example of a Blockchain

There are five main concepts of blockchain. Main concepts of blockchain are 1. Mining 2. Consensus Protocol 3. Hash Cryptography 4. Immutable Ledger 5. Distributed P2P Network.

- **Mining:** The process of attaching new transactions to the chain, a sizable distributed public ledger of past transactions, is called mining. Although other blockchain-based technologies also use mining, the term is most commonly associated with bitcoin.
- **Hash Cryptography:** Any key or string of characters can be transformed into another value by hashing. An arithmetical algorithm known as a cryptographic hash function (CHF) changes data of any size into a bit array of a particular size.
- **Consensus Protocol:** The consensus protocol has some certain aims, including outreach a consensus, collaborating, giving every node same privileges, and mandating that every node participates in the consensus process.
- **Immutable Ledger:** A record that cannot be changed is called an immutable ledger. Data security and evidence that the data has not been altered are necessities in the digital age.
- **Distributed P2P Network:** P2P is a technology built on a fundamental idea. Decentralization is another fundamental plan. Blockchain's P2P architecture enables global cryptocurrency transfers without the use of intermediary, intermediaries, or concentrated servers.

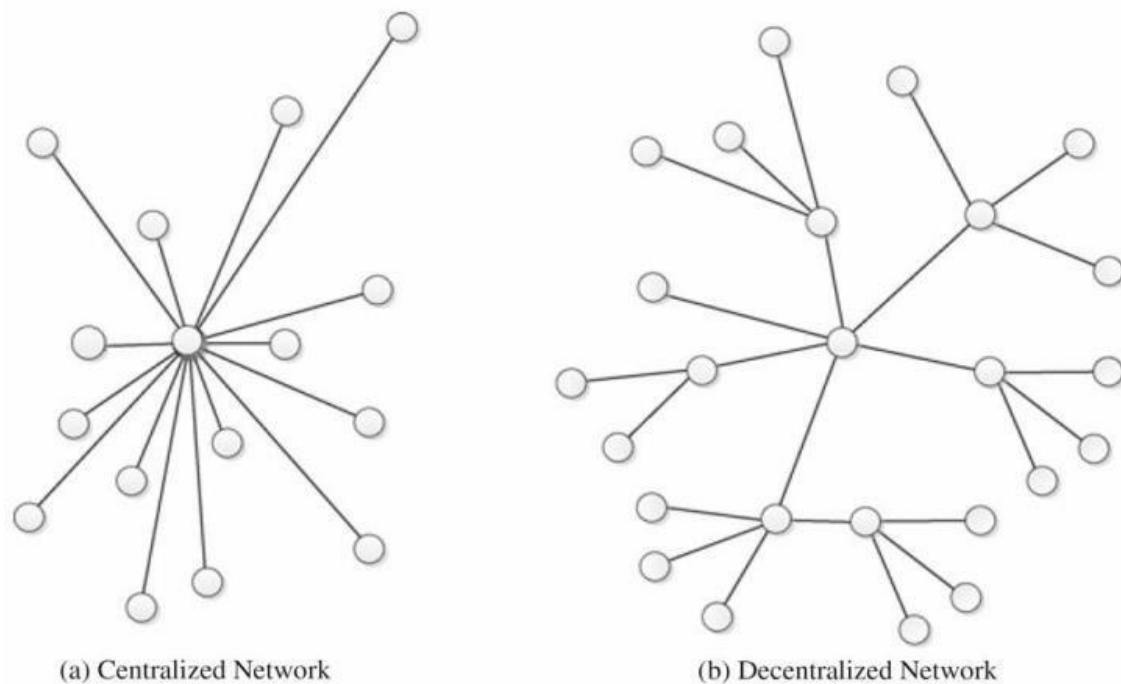


Figure 3: Centralized and Distributed network architecture

Blockchain technology is built using distributed network architecture. The main differences between distributed and centralized network system is described below:

Centralized Network: Systems with client/server based architecture that are concentrated are those in which one or multiple customer nodes are associated to a concentrated server. This kind of system, in which a client sends a request to a business server and then receives the response, is commonly used in many organizations.

Decentralized Network: These other kinds of systems have been very popular lately, largely as a result of the enormous hype surrounding Bitcoin. Numerous organizations are currently looking for applications for these systems.

Each node can make its own decision in a decentralized network system. The concluding action of the system is fixated by the sum of the conclusion taken by the single nodes. It should be noted that more than one companies deal with the appeal.

2.2 Blockchain Current Applications

Blockchain applications have started to be incorporated into several sectors' businesses. Enterprises try to increase the transparency of their management and business processes in this way. Blockchain is regarded as an enabler that can help with a number of security difficulties, such as managing fraud and identity concerns. Financial firms can investigate their clients and stop fraud using blockchain-based solutions. Although the majority of payment and banking systems are suitable for blockchain use cases, there are other industries for which distributed ledger technology can be put to use.

The reliable operations of logistics management and B2B commerce are the second field of blockchain that is very useful. By encouraging consumer-manufacturer engagement, assisting individuals in adopting more sustainable lifestyles, and assisting businesses in streamlining resource and resource reutilization processes, blockchain is playing an increasingly important role in sustainability. Supply chain management can benefit greatly from blockchain by reducing challenges by assuring traceability, transparency, and security. Each transaction in supply chain system is carried out on a common blockchain, and it does not require the endorsement of a trustworthy center. Following the completion of the delivery phase, the payments are made automatically. The blockchain may significantly contribute to improving end-to-end tracking and product safety because the transactions are observed by the parties. As a result, before the consumer buys the product, reliable information on process transitions can be provided. Process visibility, integrity, quicker transactions, and disintermediation are major advantages.

Blockchain can be used in different kinds of internet-based applications and smart services, in addition to the possible advantages in the supply chain management and financial industries. In addition to other industries, the energy sector has used blockchain technology. Projects for organizing efficient charging schedules for electric vehicles and local energy trade are suggested. The machines are capable of trading energy in accordance with the predefined Internet of Things (IoT) devices. The real-time data collected by IoT devices can be stored in the blockchain chain. Big data analysis using it in real-time has begun.

Another industry that makes use of the blockchain is insurance. The current insurance industry relies on relationships of trust, and it is assumed that in the future, blockchain will be able to address the rare error or delay. Another industry that has the potential to benefit from blockchain technology is the healthcare sector. In this industry, the blockchain serves as a useful tool for enabling key collaborators like clinical researchers, healthcare providers, patients, pharmacists and to gain secure, quick, and dependable access to electronic medical records.

In the near future, it's feasible that blockchain integration can assist any industry that needs strict security, dependability, and transparency standards, including cybersecurity, transportation systems, cloud storage, real estate, agriculture traceability, and identity management generally. Among other domains, e-voting systems stand out as a potential but difficult field that could benefit from the incorporation of blockchain.

2.2.1 Financial Service

Blockchain is used extensively for so-called cryptocurrency, or financial transactions. Cryptocurrencies are now widely used as software systems. The currency of cryptocurrency is distinct (coin). Mining is used for adding new block to the blockchain. Every node uses blockchain to check to see if the coin is valid and has not already been consumed. More participants come to an agreement before the agreement records are added to the blockchain. Since mining requires a lot of resources, it is almost impossible for an striker to validate a bad transaction. Each mined block is examined to determine whether it possesses a legitimate proof of stake or proof of work.

Cryptocurrency	Year	Hash Function	Mining Method
Bitcoin	2008	SHA-256	Find all possible nonce values by computing proof of work and other users agree and verify the proof.
Litecoin	2011	Scrypt	Similar to Bitcoin (proof of work)
Peercoin	2012	SHA-256d	proof of work and proof of stake
Primecoin	2013	Cunningham chain	proof of work
Ripple	2014	EC digital signature	consensus system
Ethereum	2014	Ethash	proof of work
Permacoin	2014	Floating digital signature	proof of retrievability
Blackcoin	2014	Scrypt	proof of stake
Auroracoin	2014	Scrypt	proof of work
Darkcoin	2014	X11	proof of work
Namecoin	2015	SHA-256d	proof of work

Table 1: The Current Existing Cryptocurrency System

The typical steps in cryptocurrency are as follows: For a user who has a wallet, (i) a generated address is accessible, and (ii) a private key is assigned to the wallet. It is employed to sign transactions and demonstrate ownership, (iii) the payer uses the provided address to send coins to the payee while signing them with the remunerator's private key, and (iv) the transaction is validated through the mining process. Eleven cryptocurrency systems, including Peercoin, Litecoin, Bitcoin, Primecoin, Ripple, Auroracoin, Permacoin, Ethereum, Blackcoin, Namecoin and Darkcoin are covered. The previously mentioned cryptocurrency systems are summarized in Table 1 which is displayed in the order in which events occurred.

2.2.2 Healthcare

There are significant interoperability problems in the current healthcare systems, which can be solved by blockchain. It can be applied as a standard that enables stakeholders, such as healthcare organizations, researchers in the field of medicine, etc., to securely share electronic health records (EHR). The ability to share EHR allows us to enhance recommendations for doctors, for example, which are displayed in chronological order of occurrence.

Nevertheless, managing healthcare data—such as, collecting, storing, and inspecting it—is a difficult task, mainly when privacy matters are involved. We shouldn't share healthcare issues with others because they could misuse it fraudulently by hackers or other bad actors.

A blockchain based healthcare data gateway (HDG) platform is suggested by as a solution to these problems. It is a smartphone app that makes it simple to manage and regulate data sharing. Users of the proposed system can process patient data without jeopardizing patient privacy. Additionally, the data is stored in a private blockchain cloud, guaranteeing that no one, including doctors and patients, will be able to change it.

The focus of the work is on designing MedRec, a new system to prioritize patient agency. Blockchain is a distributed ledger protocol that makes use of public key cryptography. On each node in the network, there is a distribution of the blockchain replicas. Similar to earlier work, the use of blockchain technology as an access control enables the automation and tracking of specific tasks, such as the addition of new records and the modification of viewership rights. Furthermore, intelligent representations of EHR are created and stored in each individual node.

Study	Year	Hash Function	Mining Method
HDG [29]	2016	NA	NA
MedRec [30]	2016	Ethash	proof of work
PSN [31]	2016	NA	NA
BBDS [32]	2017	SHA-256	proof of work

Table 2: Blockchains for Healthcare

Subsequently, we are able to share medical data obtained by medical sensors thanks to the application of pervasive social network (PSN). The authentication protocol between mobile devices and medical sensors in wireless body area networks (WBAN) and the EHR data sharing using blockchain in PSN area are the two main security protocols that make up PSN-based healthcare systems. Each PSN node is in charge of producing and broadcasting medical data transactions, including node addresses and data from medical sensors. On the other hand, the miners are in charge of transaction validation and new block creation.

Finally, an access control mechanism based on a blockchain includes processes for identification, authentication, and authorization. It confirms a condition of responsibility where user entry can be followed for a specific action. After authenticating their identification and cryptographic keys, the system enables users to access EHR from shared data pools using blockchain. Identity-built authentication is used to achieve user authentication. Additionally, a powerful lightweight block format is suggested to improve the way blockchain is being used right now. Table II contrasts the relevant research on using blockchain technology in the healthcare industry.

2.2.3 Business and Industry

The development of the Internet of Things (IoT) has many facilities, including enabling a connection between physical objects and people. This inspires authors to suggest an e-business architecture designed specifically for an IoT environment. Distributed autonomous corporation (DAC), a company that provides transaction services without human involvement, is used for this purpose. The main component of the proposed system is a transaction mode in which peer-to-peer transactions are carried out automatically. IoTcoin and Bitcoin are used as the system's exchange certificate and currency, respectively.

Authors have been drawn to create a trustworthy payment system based on Bitcoin by the so-called edge computing or fog computing extension of the cloud. Fog computing can be thought of as a vast, all-encompassing, and distributed system that handles any computing tasks. The system was developed to be better than the current electronic cash system, which requires a bank or another reputable institution to create payment tokens. By using Bitcoin-based payments, fog users can send money directly to fog nodes without a middleman. The authors contend that regardless of whether the outsourcers are malicious or not, the proposed system can assure payment for any tasks completed by truthful workers.

2.2.4 Society Applications

Lending unconventionally: The next generation network system known as Smart Contract is meant to address credit issues, have the power to dismantle conventional borrowing arrangements. In a traditional lending arrangement, the lender lends money and also takes risks, which also results in the mortgage of goods and high loan interest, the value of which is frequently greater than the loan quantity. Borrowers can use virtual assets as collateral with smart contracts to avoid discounts on tangible goods as well as to lower the cost of credit. No need to provide the lender with extensive documentation, a work history, or your credit history. For everyone to use, the property is encoded on the blockchain.

Car/Smartphone: For instance, a car with an anti-theft device can be activated by clicking the right button on the key. You must enter the right password in order for the smartphone to function. To protect ownership, they are all ready to carry out using encryption technology. The drawback of the original form of intelligent property is that it cannot be easily copied or transferred because the key is kept in a physical container. By enabling blockchain miners to replace and copy lost protocols, the blockchain ledger finds a solution to this issue.

Blockchain Music: Music publishers have struggled with copyright issues throughout the record and digital music eras. By using a blockchain and smart contract to build a traceable music copyright database, this issue can be resolved. Additionally, you can even transfer money in real time as user behavior changes to both the copyright holder and the musician. Music lovers can make payments with digital currency.

Blockchain Government: Democrats and Republicans questioned the integrity of the 2016 U.S. election's voting process. Each person can view their vote as well as the overall statistical process thanks to the blockchain and smart contracts. The process of verifying the flow of funds also consumes a sizeable portion of the annual government budget, but blockchain technology

can greatly streamline it. By offering a platform for businesses, foundations, governmental organizations, and private citizens, blockchain can be self-managed. Through blockchain, individuals can make sure their wishes are carried out.

2.2.5 Other Implementations

This section discusses how blockchain technology is currently being used in a variety of fields, including WiFi authentication, IoT security, right management systems, reputation systems, and systems for distributing digital content.

BRIGHT is a decentralized right management system that uses blockchain technology to completely depart from the conventional method, which frequently takes into account a central third party. The proposed system enables us to reduce user service fees and is anticipated to have a robust mechanism against attack. A reputation system also has a lot of potential for measuring how much the community values our trust. Our previous interactions and transactions in this network, or e-commerce website, are used to calculate it. The main problems with the current reputation system, namely freeloaders, can be resolved by incorporating blockchain into it.

An alternative payment system derived from Bitcoin, Bitcoin 2.0, is the foundation of a new WiFi authentication protocol. Prior to receiving their Auth-Coins, users must first install the Auth-Wallet application. Tokens are interchanged for authentication between access points and users. Finally, describes the use of blockchain for home security. A local and private blockchain is used to provide secure access control to the IoT devices. The blockchain generates an unchangeable time-ordered of transactions in addition to enabling a simple security mechanism for smart home devices. Additionally, a device that centrally manages smart home transactions is referred to as a "smart home miner."

2.3 Block

There are multiple blocks in each blockchain and it has three basic elements. The three elements are, Data, the block hash value and the hash of the previous block. Hash value is always a unique value which identifies one block. The previous hash indicates the previous block and the hash of the block is the identification of that block.

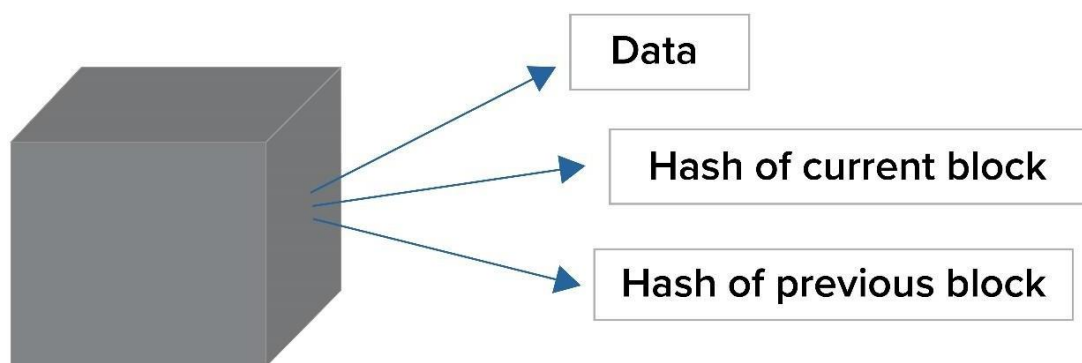


Figure 3: A Block

Transactions and a transaction counter make up the block body. The transaction counter denotes the number of transactions that came before, and transactions is a list of all the block's recorded transactions. Depending on the size of each transaction and the block size, a block can contain a maximum number of transactions. The authenticity of transactions are verified by blockchain using an asymmetric cryptography mechanism. Digital signatures based on asymmetric cryptography are used in unreliable environments, like the blockchain network.

2.4 Blockchain Formation

Each block can point to the block before, which means the third block is taking a reference to the second one and second block is taking a reference to the first one. And this is how a blockchain is created. The key element that makes blockchain immutable is cryptographic hashes, which is why blockchain is immutable.

A series of blocks makes up the blockchain that act as a public ledger-like database for all transactions. These blocks are connected to one another by a reference hash that is a part of the parent block, the block that came before. The genesis block, which has no parent blocks, is referred to as the initial block. The block header and block body make up a block.

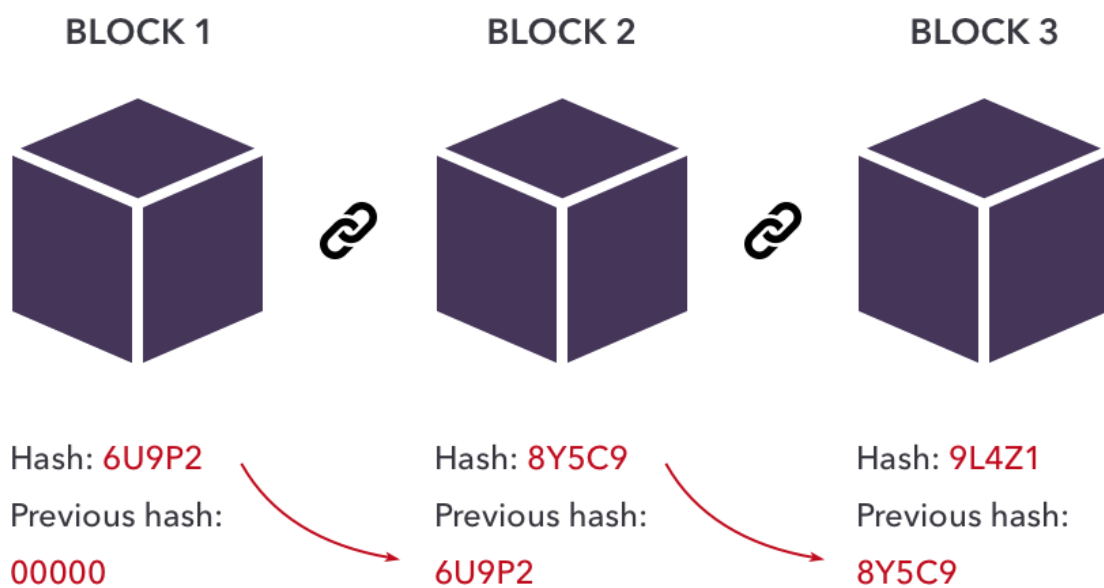


Figure 4: Architecture of Blockchain

2.5 Smart Contract

The development of blockchain technology in recent years is also consistent with other ideas put out in literature. One of such ideas is the smart contract, which combines human interfaces and computer protocols to carry out a contract's terms. Since Smart Contracts can be used more readily by utilizing blockchains compared to the technology available at the time of their invention, they are growing in popularity as a result of the blockchain. Depending on predetermined factors, this novel approach might, for instance, replace banks and lawyers who have been involved in asset deal contracts (Fairfield 2014). The ownership of properties can also be managed with the help of smart contracts. These assets may be tangible (like homes or cars) or intangible (like shares or access rights).

Even now, the financial sector is speculating about how much of their current business the blockchain might displace. The payment procedure serves as an example of this. When consumers purchase items today using a credit card, the settlement takes place after a few days. With the use of the blockchain, this postponed settlement would be unnecessary because payments could be made instantly by updating the ledger.

Smart contracts are self-executing agreements between peers that include the terms and conditions of the agreement. They are merely programs based on blockchain that are set to execute when certain conditions are met. They are frequently used to automate the implementation of an arrangement so that all groups can be sure of the result at that moment.

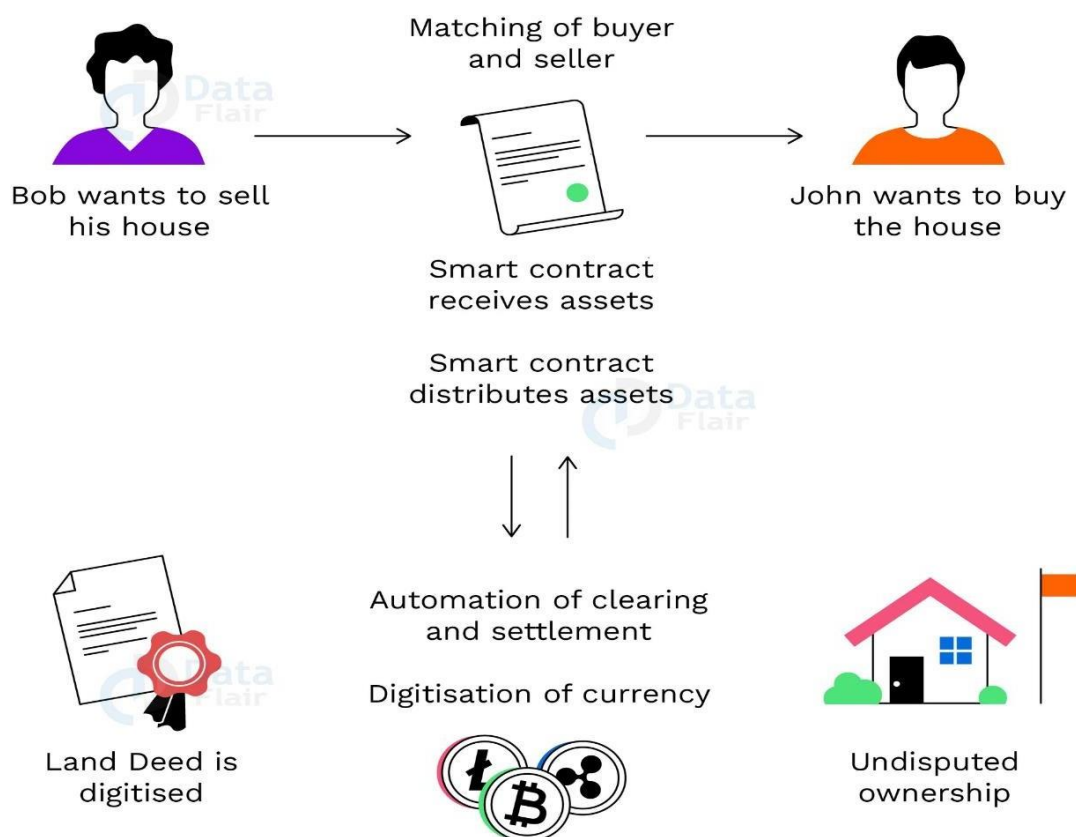


Figure 5: Application of Smart Contract

Chapter 3

Requirement Analysis

This is a user friendly application and this application can be used by users with minimum technical knowledge. There are certain requirements to use this application and to create an account, creating a voting poll and casting a vote.

3.1 User Requirement

To use this application, the user needs to do the following:

- ❖ User needs to create an account to register in this application. Unauthorized access is not allowed in this application.
- ❖ After creating an account user will have to login to this application by providing valid information such as: User Name or Email Address and Password.
- ❖ In the home page the user will be able to find existing voting polls where the user can cast a vote or the user will have to create his own voting poll.

3.2 System Requirement

To use this application, the system needs to do the following:

- ❖ User should have a working laptop or desktop computer.
- ❖ There should be any type of browser installed in the computer.
- ❖ There should be stable internet connection.

3.3 Used Platform/Tools

Programming Language: Typescript

IDE: Visual Studio Code

Libraries: React, Near Blockchain

- ❖ **Front-End:** For the user interface of the application latest version of React library with typescript is used. React is a popular JavaScript library which is library for creating user interfaces. Typescript in built on JavaScript which is a strongly typed programming language. The user interface is user friendly and well responsive.
- ❖ **Back-End:** The back-end is built with a blockchain protocol called NEAR blockchain. The NEAR protocol serves as the secure, scalable foundation for a new kind of decentralized applications. It is also built to be especially easy for developers to use. Hundreds of projects are already built on NEAR blockchain.

Chapter 4

Project Analysis

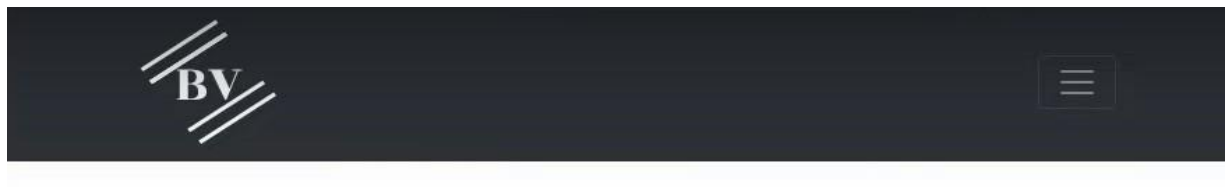
Voting is a sensitive matter and it must be secured system otherwise people may change data and it will cause problems and will provide biased result of voting. But blockchain is secured and people will trust the voting system if it is built using blockchain. Once a block is added to a blockchain, it is almost impossible to change the data of the block. So, blockchain can be a solution to the secured voting system.

4.1 The Front-End

With react, react router is also used in this application. There are three main routes/pages in this application. The pages are home page, create new poll and polling station. In react, these pages are called components. These components are stored in components folder of the application. The routes of these components are added with the navigation buttons so that the users can navigate through the application.

4.2 The Home Page

Main part of the home page of the application is the table of content. In the table there are three main columns. The first column is for the serial number. The second column displays the list of polls and the third column contains a button which leads to the details page of the voting poll. There can be multiple voting polls listed on the home page.



#	List of Polls	Go to Poll
1	Who would win in Smash bros?	Go to Poll
2	Who is the better actor?	Go to Poll

Figure 6: The Home Page

4.3 The Polling Station

In the polling station there is one row with three columns. On the first column there is a picture of the first candidate, there is a button for voting the first candidate and there is a field containing the amount of vote the first candidate got. In the second column there is the text which explains in which basis the candidates are being compared. The third column is similar to the first column. There is a picture of the second candidate, a voting button for the second candidate and there is a text field which displays the amount of vote the second candidate got.

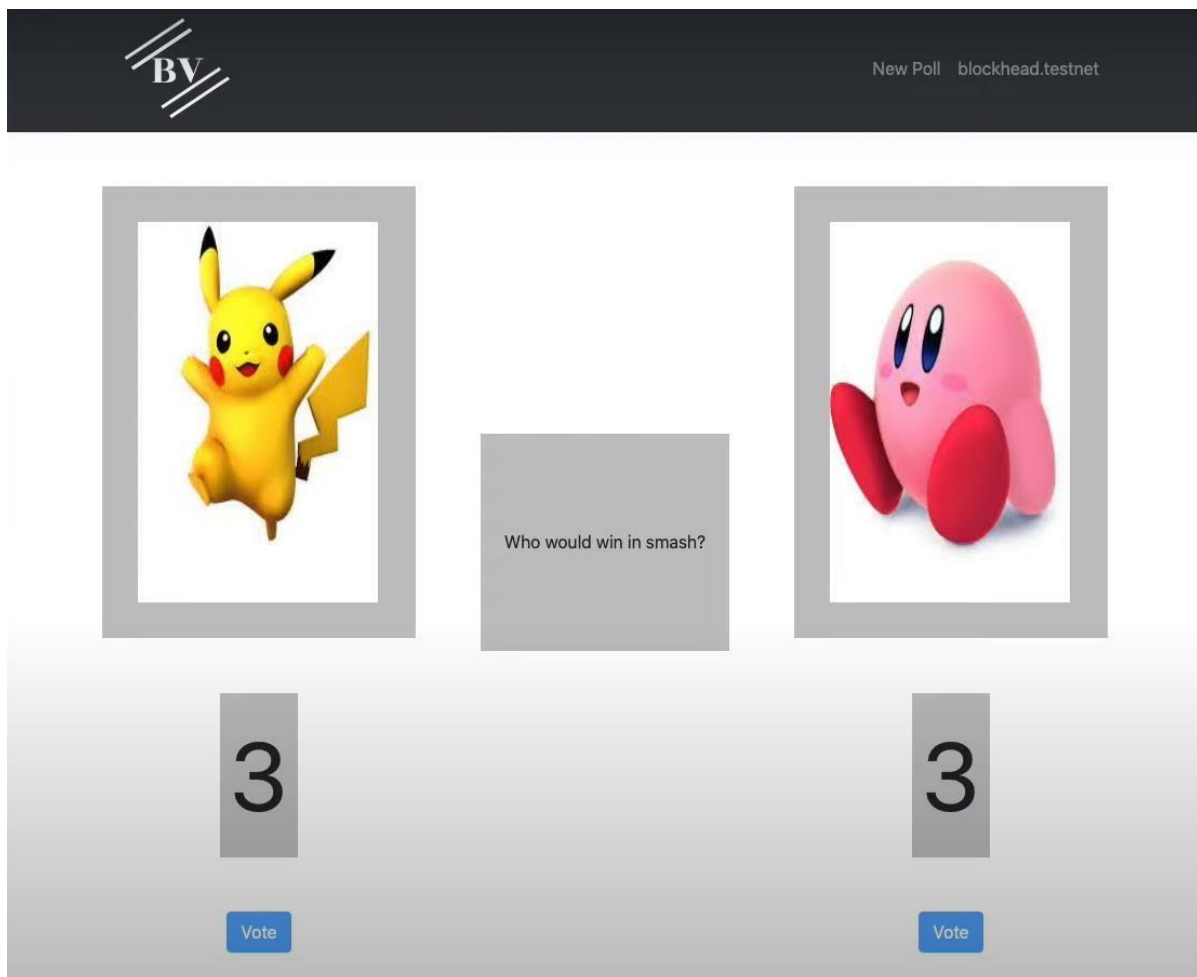
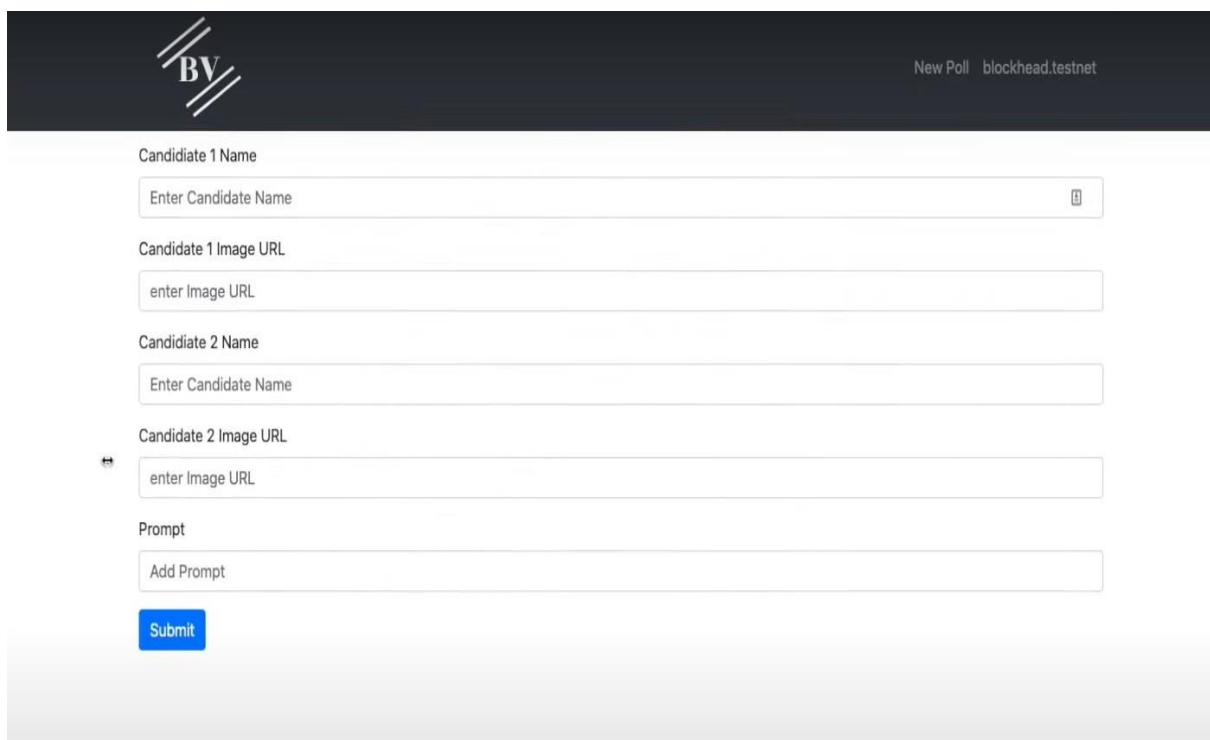


Figure 7: The Polling Station

4.4 The New Poll Form

There are multiple fields in the new poll form. The first field is for declaring the candidates name, the second field is for adding the first candidate image URL. The third field is for declaring the second candidates name and the fourth field is for the image URL of the second candidate. The last field is the most important field which declares the topic based on which the candidates are being compared.



The screenshot shows a web interface for creating a new poll. At the top left is a logo with the letters 'BV' and three diagonal lines. At the top right, it says 'New Poll' and 'blockhead.testnet'. The form consists of the following fields:

- Candidate 1 Name:** A text input field with the placeholder text 'Enter Candidate Name' and a small icon on the right.
- Candidate 1 Image URL:** A text input field with the placeholder text 'enter Image URL'.
- Candidate 2 Name:** A text input field with the placeholder text 'Enter Candidate Name'.
- Candidate 2 Image URL:** A text input field with the placeholder text 'enter Image URL'.
- Prompt:** A text input field with the placeholder text 'Add Prompt'.

At the bottom left of the form area is a blue button labeled 'Submit'.

Figure 8: Poll Form

Chapter 5

Implementing Blockchain

After completing the user interfaces the back-end is being created which is the most important aspect of the application. In this project the back-end and the database is in blockchain. This was the most challenging part of the application.

5.1 The Smart Contract

Simply put, blockchain based smart contracts are programs that are used when definite formulas are met. They are typically used to automate the execution of an agreement so that all groups can be sure of the outcome at that moment, without any additional or intermediary time. In the application the smart contract is written inside the assembly folder inside the index.ts file. There are two different types of methods in the smart contract. They are the view methods and change methods. The view methods does not change the state of the blockchain. It pulls and reads information from blockchain. And the change methods changes the state of the blockchain. The change methods adds or modifies the blockchain.

The first change method is addUrl method which adds the URL of pictures of the candidates to the blockchain. The addCandidatePair method binds both the candidates together. The addVote method adds vote to the selected candidate. The recordUser method will record the user credentials to the blockchain. The addToPromptArray will add a new comparison text to the blockchain.

```
71 // Change Methods
72 // Changes state of Blockchain
73 // Costs a transaction fee to do so
74 // Adds or modifies information to blockchain
75
76 export function addUrl(name:string, url:string):void{
77     CandidateURL.set(name,url);
78     logging.log('added url for '+ name);
79 }
80
81 export function addCandidatePair(prompt:string,name1:string,name2:string):void{
82     CandidatePair.set(prompt,[name1,name2])
83 }
84
85 export function addToPromptArray(prompt:string):void{
86     logging.log('added to prompt array')
87     if(PromptArray.contains("AllArrays")){
88         logging.log('add addition to prompt array')
89         let tempArray=PromptArray.getSome("AllArrays")
90         tempArray.push(prompt)
91         PromptArray.set("AllArrays",tempArray);
92     }else{
93         PromptArray.set("AllArrays",[prompt])
94     }
95 }
96
97 export function clearPromptArray():void{
98     logging.log('clearing prompt array');
99     PromptArray.delete("AllArrays")
100 }
101
102
```

Figure 9: Example of Change Method

```

17 // View Methods
18 // Does not change state of the blockchain
19 // Does not incur a fee
20 // Pulls and reads information from blockchain
21
22 export function getUrl(name:string):string{
23     if(CandidateURL.contains(name)){
24         return CandidateURL.getSome(name)
25     }else{
26         logging.log(`can't find that user`)
27         return ''
28     }
29 }
30
31 export function didParticipate(prompt:string, user:string):bool{
32     if(userParticipation.contains(prompt)){
33         let getArray=userParticipation.getSome(prompt);
34         return getArray.includes(user)
35     }else{
36         logging.log('prompt not found')
37         return false
38     }
39 }
40
41 export function getAllPrompts():string[]{
42     if(PromptArray.contains('AllArrays')){
43         return PromptArray.getSome("AllArrays")
44     }else{
45         logging.log('no prompts found');
46         return []
47     }
48 }

```

Figure 10: Example of View Methods

The getUrl get method will get the pictures of the candidates from the blockchain. The didParticipate get method will get the information of the user participation to the voting poll. If the user has casted a vote already this method will not allow the user to caste a vote again. The getAllPrompt method will get all the voting polls as a list to display it on the home page. The get vote method will display the amount of vote each candidate got.

Chapter 6

Conclusion and Future Work

6.1 Conclusion

In this project I have implemented blockchain for voting system. The project offers users some interesting functions. Such as, creating a voting poll according to that persons will. The user can create a poll on any subject, comparing two different persons or two different topics or ideas. The user can trust fully on the result of the poll as this application uses blockchain and it is impossible to corrupt the data.

In this work, I presented an electronic voting system based on blockchain that protects voters' privacy while enabling secure and affordable elections. I have demonstrated how using blockchain technology opens up new ways to get over electronic voting systems' disadvantages and assumption difficulties, ensuring election integrity and security and laying the preliminaries for transparency. Utilizing every feature of the smart contract to lighten the strain on the blockchain, it is possible to transfer hundreds of transactions onto it per second. Greater throughput of transactions per second might require some additional steps for larger countries.

6.2 Future Work

Although this application provides basic functionalities of voting system but the system can be improved. There are many additional features can be added to this application. One such feature can be, comparing between more than two competitors. There can be many contenders for a single position. And also many more features can be added based on user preferences. Also some more changes may be required after the system goes through testing process. Also some optimizations may be required in order to adjust pressure of many user casting votes at the same time.

References

- [1] Zibin Zheng, Hong-Ning Dai, Shaoan Xie, "Blockchain challenges and opportunities: a survey," Article in International Journal of Web and Grid Services · October 2018 .
- [2] A. A. Monrat, O. Schelén and K. Andersson, "A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities," in IEEE Access, vol. 7, pp. 117134-117151, 2019, doi: 10.1109/ACCESS.2019.2936094.
- [3] M. Belotti, N. Božić, G. Pujolle and S. Secci, "A Vademecum on Blockchain Technologies: When, Which, and How," in IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3796-3838, Fourthquarter 2019, doi: 10.1109/COMST.2019.2928178.
- [4] Nofer, M., Gomber, P., Hinz, O. *et al.* "Blockchain,". *Bus Inf Syst Eng* **59**, 183–187 (2017). <https://doi.org/10.1007/s12599-017-0467-3>
- [5] Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, Qiaoyan Wen, "A survey on the security of blockchain systems, Future Generation Computer Systems," Volume 107, 2020.
- [6] Glaser F, Bezenberger L (2015) Beyond Cryptocurrencies-A Tax-onomy of Decentralized Consensus Systems. In: Proceedings of the 23rd European Conference on Information Systems (ECIS 2015), Muenster, Germany.
- [7] Glaser F, Zimmermann K, Haferkorn M, Weber M, Siering M (2014) Bitcoin-asset or currency? Revealing users' hidden intentions. In: Proceedings of the 22nd European Conference on Information Systems (ECIS 2014); Tel Aviv, Israel.

- [8] Kosba A, Miller A, Shi E, Wen Z, Papamanthou C (2016) Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In: IEEE Symposium on Security and Privacy (SP), pp 839–858
- [9] Lewenberg Y, Sompolinsky Y, Zohar A (2015) Inclusive block chain protocols. In: International Conference on Financial Cryptography and Data Security. Springer, Heidelberg, pp 528–547
- [10] Zheng Z, Xie S, Dai HN, Wang H (2016) Blockchain Challenges and Opportunities: A Survey. Work Pap
- [11] Zyskind G, Nathan O, Pentland A (2015) Decentralizing privacy: Using blockchain to protect personal data. In Security and Privacy Workshops (SPW), IEEE 180–184
- [12] Ali, S.T.; Murray, J. An Overview of End-to-End Verifiable Voting Systems. arXiv 2016, arXiv:160508554.
- [13] Daramola, O.; Thebus, D. Architecture-Centric Evaluation of Blockchain-Based Smart Contract E-Voting for National Elections. *Informatics* 2020, 7, 16.
- [14] Ryan, P.Y.A.; Schneider, S.; Teague, V. End-to-End Verifiability in Voting Systems, from Theory to Practice. *IEEE Secur. Priv.* 2015, 13, 59–62.
- [15] Zhang, S.; Wang, L.; Xiong, H. Chaintegrity: Blockchain-enabled large-scale e-voting system with robustness and universal verifiability. *Int. J. Inf. Secur.* 2020, 19, 323–341.
- [16] Haber, S.; Stornetta, W.S. How to time-stamp a digital document. *J. Cryptol.* 1991, 3, 99–111.

- [17] Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564.
- [18] Hanifatunnisa, R.; Rahardjo, B. Blockchain based e-voting recording system design. In Proceedings of the 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), Lombok, Indonesia, 26–27 October 2017; pp. 1–6.
- [19] Moura, T.; Gomes, A. Blockchain Voting and its effects on Election Transparency and Voter Confidence. In Proceedings of the 18th Annual International Conference on Digital Government Research, Staten Island, NY, USA, 7–9 June 2017; pp. 574–575.
- [20] A. S. Tanenbaum and M. Van Steen, Distributed systems: principles and paradigms. Prentice-Hall, 2007.
- [21] D. Drescher, “Blockchain basics,” Springer, Tech. Rep.
- [22] L. Lamport, R. Shostak, and M. Pease, “The byzantine generals problem,” ACM Transactions on Programming Languages and Systems (TOPLAS), vol. 4, no. 3, pp. 382–401, 1982.
- [23] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” URL: <http://www.bitcoin.org/bitcoin.pdf>, 2008.
- [24] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the internet of things,” IEEE Access, vol. 4, pp. 2292–2303, 2016

- [25] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Applied Innovation*, vol. 2, pp. 6–10, 2016.
- [26] U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, and R. Brooks, "A brief survey of cryptocurrency systems," in *2016 14th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2016, pp. 745–752.
- [27] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2084–2123, 2015.
- [28] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology? a systematic review," *PloS one*, vol. 11, no. 10, p. e0163477, 2016.
- [29] S. Seebacher and R. Schuritz, "Blockchain technology as an enabler " of service systems: A structured literature review," in *International Conference on Exploring Services Science*. Springer, 2017, pp. 12– 23.
- [30] H. Kalodner, M. Carlsten, P. Ellenbogen, J. Bonneau, and A. Narayanan, "An empirical study of namecoin and lessons for decentralized namespace design," in *Workshop on the Economics of Information Security (WEIS)*. Citeseer, 2015.
- [31] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2017 IEEE International Conference on. IEEE, 2017, pp. 618–623.

- [31] T. Sanda and H. Inaba, "Proposal of new authentication method in WiFi access using bitcoin 2.0," in Consumer Electronics, 2016 IEEE 5th Global Conference on. IEEE, 2016, pp. 1–5.
- [31] R. Dennis and G. Owen, "Rep on the block: A next generation reputation system based on the blockchain," in Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference for. IEEE, 2015, pp. 131–138.
- [31] J. Kishigami, S. Fujimura, H. Watanabe, A. Nakadaira, and A. Akutsu, "The blockchain-based digital content distribution system," in Big Data and Cloud Computing (BDCloud), 2015 IEEE Fifth International Conference on. IEEE, 2015, pp. 187–190.
- [31] S. Fujimura, H. Watanabe, A. Nakadaira, T. Yamada, A. Akutsu, and J. J. Kishigami, "BRIGHT: A concept for a decentralized rights management system based on blockchain," in Consumer Electronics-Berlin (ICCEBerlin), 2015 IEEE 5th International Conference on. IEEE, 2015, pp. 345–346.
- [31] J. J. Sikorski, J. Haughton, and M. Kraft, "Blockchain technology in the chemical industry: Machine-to-machine electricity market," Applied Energy, vol. 195, pp. 234–246, 2017.
- [31] F. Tian, "An agri-food supply chain traceability system for china based on RFID & blockchain technology," in Service Systems and Service Management (ICSSSM), 2016 13th International Conference on. IEEE, 2016, pp. 1–6.
- [31] Y. Zhang and J. Wen, "An IoT electric business model based on the protocol of bitcoin," in Intelligence in Next Generation Networks (ICIN), 2015 18th International Conference on. IEEE, 2015, pp. 184–191.

- [31] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments," *Information*, vol. 8, no. 2, p. 44, 2017.
- [31] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Open and Big Data (OBD), International Conference on*. IEEE, 2016, pp. 25–30.
- [31] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *e-Health Networking, Applications and Services (Healthcom), 2016 IEEE 18th International Conference on*. IEEE, 2016, pp. 1–3.
- [32] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," *Journal of medical systems*, vol. 40, no. 10, p. 218, 2016.
- [32] B. A. Tama, "Learning to prevent inactive student of Indonesia open university." *Journal of Information Processing Systems*, vol. 11, no. 2, pp. 165–172, 2015.
- [20] Tan, B.Q.; Wang, F.; Liu, J.; Kang, K.; Costa, F. A Blockchain-Based Framework for Green Logistics in Supply Chains. *Sustainability* 2020, 12, 4656.

Appendix A.

While developing this project I faced some problems with implementing blockchain. I needed to do some intensive research on how to implement blockchain. Also there are many IDEs available to write the application. After doing some research I chose to use Visual Studio Code as my IDE among many alternatives.