TRIBHUVAN UNIVERSITY

Institute of Science and Technology

GODAWARI COLLEGE

Itahari, Sunsari

A Project Report

On

"eChunab", an Online Voting System Using Blockchain

Submitted to:

Department of Computer Science and Information Technology

Godawari College

Itahari, Sunsari

In partial fulfillment of the requirement for the Bachelor Degree in Computer Science and Information Technology (B.Sc. CSIT)

Submitted by:

Arash Thapa (TU Exam Roll No: 16449/074)

Doleshor Khadka (TU Exam Roll No: 16458/074)

Prabesh Guragain (TU Exam Roll No: 16464/074)

January, 2022

Godawari College
Tribhuvan University

Supervisor's Recommendation

I hereby recommend that this project prepared under my supervision by **Arash Thapa, Doleshor Khadka and Prabesh Guragain** entitled **"eChunab", an Online Voting System Using Blockchain** in partial fulfillment of the requirements for the degree of B.Sc.in Computer Science and Information Technology be processed for the evaluation.

……...……...

Prakash Neupane

Project Supervisor

Department of Computer Science and Information Technology

Godawari College

Itahari, Sunsari

Godawari College
Tribhuvan University

LETTER OF APPROVAL

This is to certify that this project prepared by **Arash Thapa, Doleshor Khadka and Prabesh Guragain** entitled **"eChunab", an Online Voting System Using Blockchain** in partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Science and Information Technology has been well studied. In our opinion it is satisfactory in the scope and quality as a project for the required degree.

……...……...	……..
Prakash Neupane	Rabin Rimal
Project Supervisor	Coordinator
Godawari College	Godawari College
Itahari, Sunsari	Itahari, Sunsari
……...……...	……...…….
Tantra Nath Jha	Saroj Guragain
External Examiner	Internal Examiner
Tribhuvan University	Godawari College
Kathmandu, Nepal	Itahari, Sunsari

ACKNOWLEDGEMENT

We would like to express our heartfelt gratitude to our respected supervisor Mr. Prakash Neupane for his kind support, encouragement and constructive recommendation on doing this project. We thank him for showing us how to research and channel data needed for the report.

We are really thankful to Mr. Bodhraj Nepal, Principal, Godawari College and Mr. Rabin Rimal, Head of Department for making available facilities to carry out the best in this dissertation work.

We would also like to give our special thanks to Mr. Pratik Gautam for his precious time and suggestion during our dissertation work and timely suggestions offered to us by Teaching Mr. Sacar Pathak and Mr. Santosh Dahal are all worth remembering.

We cannot stay from thanking all our classmates for their help in preparing the final work. Special thanks must be bestowed to our friends for their support during the completion of this work. we salute all those whose perceptions, observation and inputs have helped us directly or indirectly.

We also express my sincere thanks to our teachers, staff of library and laboratory for their direct and indirect co-operation and suggestions.

No words in this world can ever express the love and encouragement given by the parents so thanks to them during our toughest days and providing moral and financial support in project work.

Sincerely,

1. Arash Thapa (16449)
2. Doleshor Khadka (16458)
3. Prabesh Guragain (16464)

ABSTRACT

e-chunab stands for electronic chunab (voting) which is an electronic means of casting and counting votes. It is an efficient and cost-effective way for conducting a voting procedure in real time with high safety. Since security of networking is a major concern, securing e-chunab is a major challenge. For this we present a technique to exploit blockchain in P2P network. First, we design a synchronized model of voting records based on distributed ledger technology (DLT) to avoid forgery of votes. Second, we design a user credential model to provide authentication and non-repudiation. Third, we design a user friendly website for users/voters to cast their vote, see the results and other elections information. Last, we design a admin panel for election officer from where they register the candidates and publishes the result to the voters. By integrating the above design, a blockchain-based e-voting system i.e. e-chunab is proposed for conducting the election in a transparent way. Its various merits such as security, easy access, portability etc. can replicate the traditional e-voting system or ballot-based system.

Keywords: e-chunab, blockchain, P2P, Distributed Ledger Technology, e-voting System, Ballot-based System

Table of Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Full Form
DLT	Distributed Ledger Technology
HTML	Hyper Text Markup Language
CSS	Cascading Style Sheets
P2P	Peer to Peer
ER	Entity Relation
SDLC	Software Development Life Cycle
DRE	Direct Recording Electronic
AUT	Application Under Test
DFD	Data Flow Diagram
RAD	Rapid Application Development

CHAPTER 1: INTRODUCTION

1.1 Introduction

“eChunab” is an online web based voting system which allows specific audience or mass public to cast their vote safely and easily without breaking the daily routine. The web app can be used for specific institutions to choose their position and also used for nationwide elections for choosing the best leaders. As there are numerous disadvantages and bugs in the electronic voting system, our system is designed using a blockchain technology which is a secure and robust system that ensures anonymity of the voter, transparency in the process, robust Functioning and the decentralized system.

The use of Ethereum on our web app enables the deployment of smart contracts and decentralized applications (dapps) to be built and ensure that the app will run without any interference from a third party. Also the transaction of the ethereum is fast which ensures the less time requirement for the voters to cast their vote and calculate the end result. The another purpose of using the transaction of ethereum is that it cannot be modified, hacked and controlled by intruder which makes the voting process transparent and legit.

The electoral framework will have a node in every region to ensure that the system decentralized. This system can be used for a small scale organization. The blockchain technology and Face Detection is executed in web3.js and Python using the Flask framework respectively. The web page to caste vote is developed using HTML, CSS, and javascript along with the nodejs.

User friendly web page ensure interactive site for casting votes and displaying outcomes and other essential information such as profile, candidate political background, the agenda of different political parties. The web page gives unquestionable visions for both nominees and voters. The two main module of our system are listed below:

i. **Registration**: The sign-up feature along with face recognition for voters is set before the voting procedure starts. This features gathers the personal information which at last use for verification process.

ii. **Cast Vote:** Validate users/voters can cast a vote. The voter logins to cryptowallet and uses ethereum on a metamask to cast vote.

1.2 Problem Statement

In the context of Nepal, Government uses traditional booth voting system which can be easily modified and changed. The research of the traditional booth voting system leads us to point out the following demerits:

- Expensive
- Insecure (as we heard booth capturing news)
- Time consuming
- Faults may rise in counting process

So, to overcome the mentioned problem the government should goes for alternative way i.e Electronic voting system. In centralized electronic voting system following problem might arise:

- Data can be changed
- Multiple entries can be registered
- Manipulation of the result
- Hacking of the entire system

At last government should adapt the E-voting system which contains decentralized database. For this purpose, our web app is suitable as it overcomes all the problems stated below and has the following features:

- User friendly website with the ongoing elections list.
- Clock counting Deadline time
- E-pamphlets of all political parties involved in elections.
- On screen result
- Confidential Personal Info keeping and viewing at any time.

1.3 Objectives

The main objective of the project is to develop a website for the general public and election commission officer to fulfill the mentioned objectives of the project which are as follows:

- To bring automation from registration process to casting vote.
- To develop highly secured voting system which can save money as well as time.

1.4 Scope and Limitations

eChunab have a lot of benefits and scope which can solve various problems and the scope are described below:

- **Accessibility:**
  As this system is a means of internet, people can access it from anywhere in anytime by the use of variety of portable devices.
- **Speed:**
  The voting and counting process imposed in this system reduce the time drastically. The election's result can be obtained instantly as soon as the voting time ends.
- **Accuracy:**
  The voting counting is done according to the algorithm set for the system so that vote counting will be way more accurate than calculated by humans.
- **Cost reduction:**
  Resources like papers, pen, voting booth and other many more wouldn't be used or lessen so that the cost is automatically reduced.
- **Validation:**
  The validation will be performed by the system itself according to the rule set of an algorithm. It will check and validate every small detail so only the legal voters can cast their vote. E-voting system can provide large number of features as compared to paper based system although E-voting system have some limitation on which we'll be working on in the future.

Besides scopes, there are some of the limitations of echunab. The limitations are listed and discussed below in details.

- **Language:**
  Language is the major barrier as most of the people are unfamiliar with English language. So, a language translator added in future, can translate the entire system accordance with their comfort language.
- **Threat to hash function:**
  Hash function generated for performing transaction, such as voting and counting, can be altered as soon as quantum computers developed. The development of quantum computers can be possible in near future.

- **Disable Voters:**
  The currently proposed system lacks technology that allows disabled people to easily vote, but features such as Text to Voice, Voice Command, Voice Assistance and many more can be added in near future.
- **Lack of Awareness:**
  Since this is a new technology majority of the people are unfamiliar with this e-voting system.
- **Unchangeable:**
  The entire process is unchangeable; the system is unable to make any necessary changes after it has been activated.

1.5 Development Methodology

Development Methodology refers to structured processes involved when working on a project. Its goal is to provide a systematic approach to develop a system. It also provides a platform for developers to work together more efficiently as a team. It formalizes communication and determines how information is shared within the team. Using a software development methodology allows the team to cut down on inefficiency and provide a more accurate delivery timeline. It prevents the team from reacting to every input, but instead, allows them to be more organized and structured when dealing with spontaneous changes.

Developers have high number of choices to select from various methodologies available. Most of the methodologies falls under waterfall, iterative or continuous model. Among these models, it was found that waterfall model is frequently used by different software companies.

Waterfall Development Model

It is a SDLC which is simple to understand and use. In waterfall model, each phase must be completed before the next phase i.e. phases cannot overlap. In this approach, the outcome of the one phases acts as an input for the next phase in a sequential way. Due to this linear sequential flow, it is sometimes called as Linear-Sequential Life Cycle Model. The following figure shows the different figure involved in waterfall model [1].

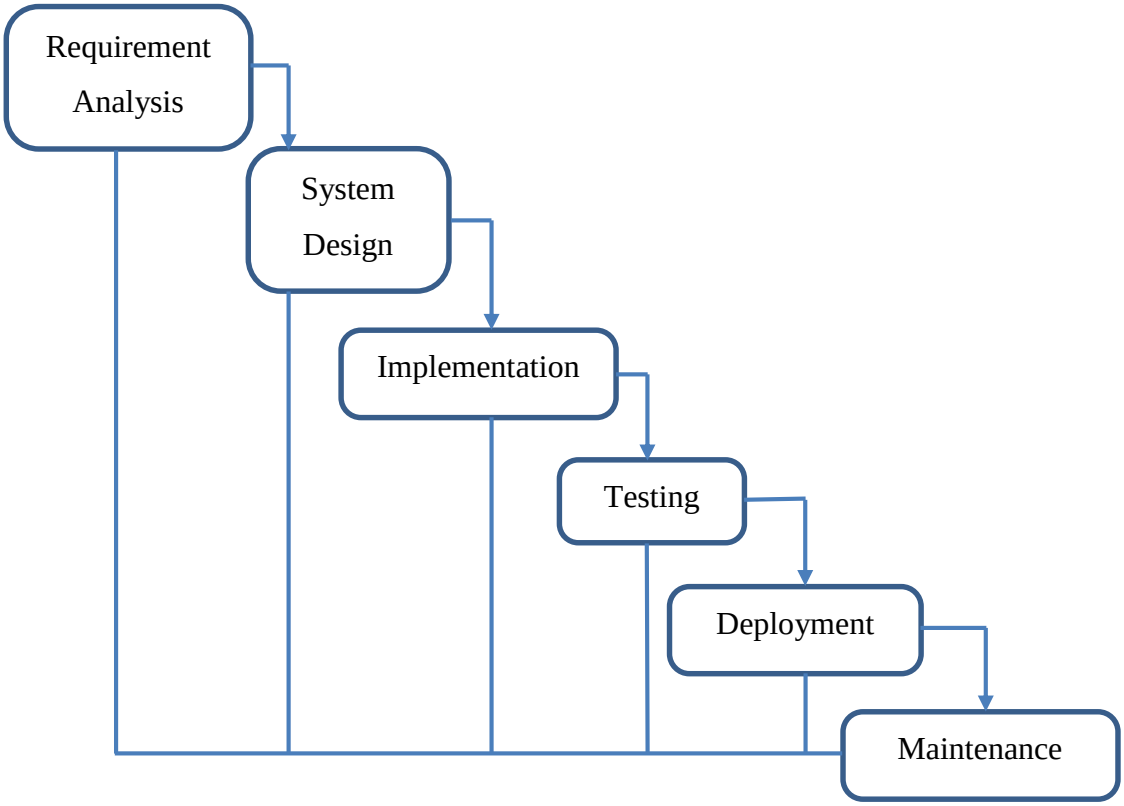


Figure 1: Different phases of waterfall model

The sequential phases of waterfall model are listed below.

- **Requirements**: The first phase involves understanding what needs to design and what is its function, purpose, etc. Here, the specifications of the input and output or the final product are studied and marked.
- **System Design**: The requirement specifications from the first phase are studied in this phase and system design is prepared. System Design helps in specifying hardware and system requirements and also helps in defining overall system architecture. The software code to be written in the next stage is created now.
- **Implementation**: With inputs from system design, the system is first developed in small programs called units, which are integrated into the next phase. Each unit is developed and tested for its functionality which is referred to as Unit Testing.
- **Integration and Testing**: All the units developed in the implementation phase are integrated into a system after testing of each unit. The software designed, needs to go through constant software testing to find out if there are any flaws or errors. Testing is done so that the client does not face any problem during the installation of the software.

- **Deployment of System**: Once the functional and non-functional testing is done, the product is deployed in the customer environment or released into the market.
- **Maintenance**: This step occurs after installation, and involves making modifications to the system or an individual component to alter attributes or improve performance. These modifications arise either due to change requests initiated by the customer, or defects uncovered during live use of the system. The client is provided with regular maintenance and support for the developed software.

1.6 Report Organization

The required content for the project is structured into six main chapters. **Chapter 1** is introductory part which explains about the overview of the system. **Chapter 2,** the Literature review part covers the background study, fundamental theories and the review of the relevant research presented by other researchers. The **Chapter 3,** System Analysis provides the outline, requirements along with the feasibility of the project. In **Chapter 4** System is designed based on the overall model building with the appropriate algorithms. Here, system is designed following structured approach. **Chapter 5** called Implementation and testing covers tools and technology used to build a system. It also deals with the testing and result analysis. In the end, **Chapter 6** is Conclusion in which we summarized the overall outputs along with the appropriate recommendation for the betterment in future.

CHAPTER 2: BACKGROUND STUDY AND LITERATURE REVIEW

2.1 Background Study

Electronic voting has been an area of research focus for many years by using computing machines and equipment for casting votes and producing high quality and precise results in accordance with the sentiments of the participating voters. Various attempts have been adopted in practice to support election process. Initially computer counting system allowed the voter to cast vote on papers. Later on, those cards went through the process of scanning and tallying at every polling cell on a central server (Kadam et al, 2015; Rockwell, 2017; Hao et al, 2010). Direct Recording Electronic (DRE) voting systems were put in place later on which were admired and acknowledged greatly by the voters in-spite of the resistance from computer scientists. If the voting system is well understood by the voters, the system's usability can be increased remarkably. DRE systems in particular have gathered a lot of successes in bringing the voters to use this technology. These systems work more or less in the same way as any conventional election system does. In the case of DRE, a voter begins his journey by going to their polling place and get their token to vote where he utilizes his token at the voting terminal to vote for his candidate. When the candidate selection procedure is completed, DRE systems present the final selection to the voter before actually casting it (in case if the voter wants to change his opinion) and after the final selection, the ballot casting is completed (Multichain, 2017; Dalia et al, 2012).

Blockchain refers to a distributed, encrypted database, which is a public depository of information that cannot be reversed and is incorruptible. In other words, a blockchain can be defined as distributed public ledger or database of records of every transaction that has been carried out and shared among those participating in the network.

Every transaction in the public ledger has to be authenticated via the agreement of more than half of those participating in the network. The blockchain technology is unique in the sense that it reduces the function of the middle man. The key features of Blockchain are listed below:

- Decentralized Database
- Eliminating Third Party
- Smart Contracts

- Self-Executing and Faster System
- Better Security

Ganache

Truffle Framework is utilized to check the smart contracts and dispatch them to the blockchain. Ganache is a piece of Truffle environment. It is a personal blockchain for rapid Ethereum and Corda distributed application development. The use of Ganache enables us to develop, and test our dApps in a safe and deterministic environment. Ganache comes in two flavours: UI (desktop app supporting both Ethereum and Corda technology) and CLI (command-line tool available for Ethereum development. All versions of Ganache are available for Windows, Mac, and Linux.

2.2 Literature Review

There are many paper published on the subject of electronic voting system and electronic voting system using blockchain technology. The major paper which help us investigate more on our project are listed below;

An Ethereum-based E-voting system: An Ethereum-based E-voting system, University of Information Technology Vietnam National University HCMC, Vietnam reviews the requirements and then propose Votereum, an Electronic voting system that utilizes the blockchain technology. The proposed system is empowered by Ethereum platform, including one server manages the entire system and the other handles all blockchain-related requests [2].

Decentralized Voting Platform Based on Ethereum Blockchain: Department of Computer Science American University of Science and Technology, propose a novel approach for a decentralized trustless voting platform that relies on Block-chain technology to solve the trust issues. The main features of this system include ensuring data integrity and transparency, and enforcing one vote per mobile phone number for every poll with ensured privacy. To accomplish this, the Ethereum Virtual Machine (EVM) is used as the Blockchain runtime environment [3].

Possibilities and Challenges of E-Voting in Context of Nepal: The research proposed the presentation which discusses the potential of evoting in the context of Nepalese society, both in and out of the country. It showcases the pros and cons of this state-of-art technology;

the core issues being security and scalability. Also presented are the the author's experience with the implementation of evoting software during the election in a Nepali organization. The presentation ends by highlighting some of the most prominent issues that need to be addressed in the Nepalese context- education, infrastructure-building, and policy-making [4].

Implementing Blockchain in Online Voting for Nepalese Voters: It provides a simple method to utilize the blockchain technology to overcome the problem of traditional online voting. A hypothetical model was designed referring to voting system in Nepal and is intended to operate on a consortium blockchain with voters, candidates and the election authority as a participating node [5].

CHAPTER 3: SYSTEM ANALYSIS

3.1 System Analysis

3.1.1 Requirement Analysis

i. **Functional Requirements:** These are the requirements that the end user requires as the basic features that the system should offer. It is a high-level statement of what the system should do. The followings are the some of the functional requirement that the user requires from our system:

- Users having citizenship should possess vote throughout the world.
- Secured and accurate so that correct result publishes.
- Avoid multiple votes.
- Authenticate the voter's nationality and age criteria.
- Confirm the respective voter votes in the system.
- Avoid Election officers or system administrator interception in counting vote.

ii. **Non-Functional Requirements:** These are the quality constraints that the system must satisfy according to the project requirement. It specifies how our system fulfill the above listed functional requirements. The basic non-functional requirements of our system are listed below:

- Simple UI/UX so that majority can access easily.
- Voting process should complete in a specific time constraint.
- Handle the huge traffic as we have mass audience.

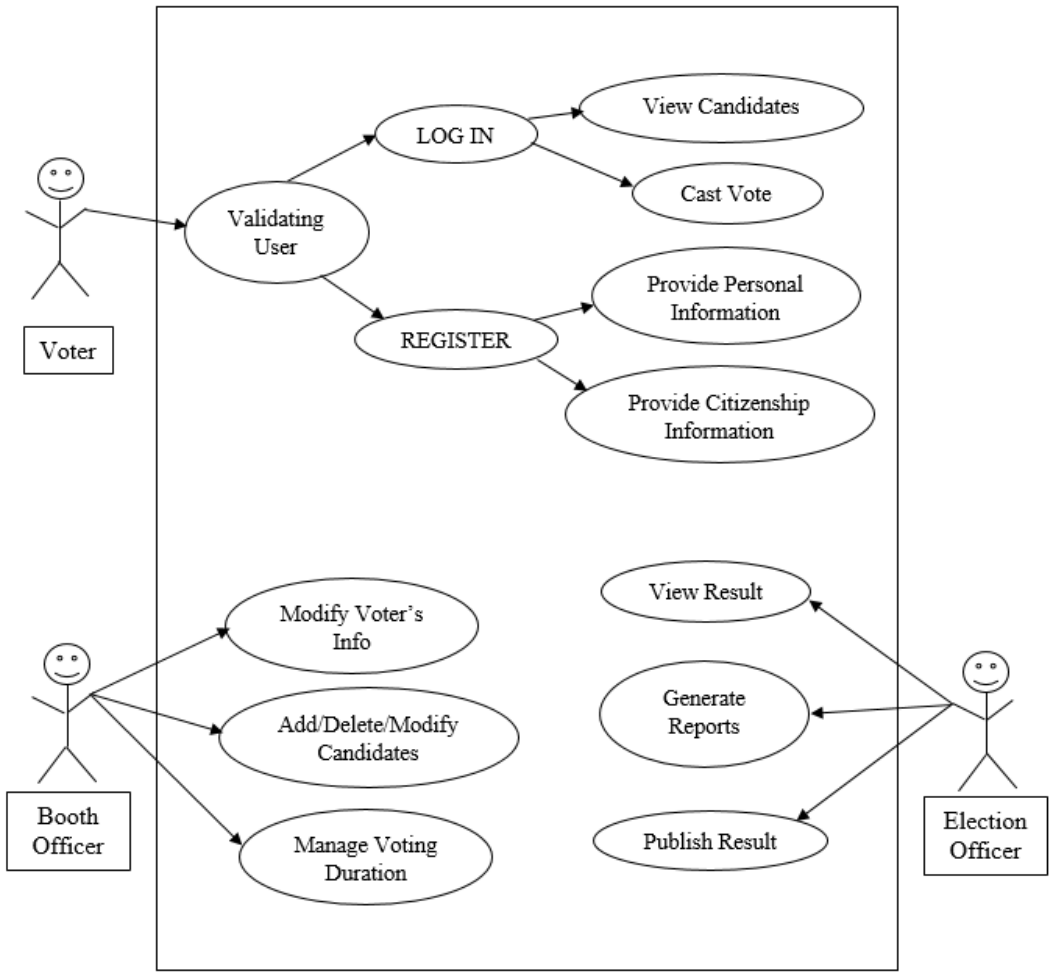


Figure 2: Use-case diagram of the web app

3.1.2 Feasibility Analysis

Feasibility study is a high-level capsule version of the entire system analysis and design process. The study begins by classifying the problem definition. The purpose of feasibility study is to uncover the failing and robustness of an existing or proposed system. It is a preliminary study conducted before the real development of the project ensuring project's success. A good research on feasibility study provides the historical background of the project [6]. The feasibility study concentrates on the following areas:

i. Technical feasibility

Evaluating the technical feasibility study is the trickiest part of a feasibility study. This is because, at this point in time, not too many detailed designs of the system, making it difficult to access issues like performance, costs on (on account of the kind of technology to be deployed) etc. The system we are designing is based on web, so it is portable i.e usable in various devices like laptop, desktop, mobiles, and many more. This system provides comprehensive function to make it user friendly. The data entry and result generations is also made easy. It also provides easy retrieval of data. So, this system is technically feasible.

ii. Operational feasibility

The operational feasibility study focuses on the degree to which the proposed system solves the problems, how it satisfies the requirements identified in the requirement analysis phase of development. It is also the measure of how well the proposed system will work after it is deployed. As we are dealing with Blockchain voting system, which indirectly targets the country's, state's or large scale organization's election process protocol, there will be a detailed comparison between the existing system and proposed system to check which one dominates the other. Since the system is being user friendly, the new users can master it within a few time. A same user can reconnect the system again and again but cannot perform major multiple operation i.e vote. Voting features is only for one time for the respective election. So, this system is operationally feasible.

iii. Economical feasibility

The economic feasibility study evaluates the cost of the software development against the ultimate income or benefits gets from the developed system. There must be scopes for profit after the successful Completion of the project. The major expenses are employment payroll, server charges, and equipment cost. The project that we are planning to make has the scope in the market and the cost for making it moderate. Since the cost for development is affordable, less than the traditional paper based voting system and demand of the market is very high so our project is economically feasible.

iv. Schedule Feasibility

It is the probability of a project to be completed within its scheduled time limits. The project completed on-time has high schedule feasibility. The project will be unsuccessful if it takes

longer timeframe than it was estimated. The following gantt chart shows eChunab is accomplished on the given time interval which proves that it is feasible in terms of the schedule.

Table 1: Gantt Chart

S. N	Phases	Start Date	End Date	Total Working Days	Week Ending												
					10/02/2021	10/09/2021	10/16/2021	10/23/2021	10/30/2021	11/06/2021	11/13/2021	11/20/2021	11/27/2021	12/04/2021	12/11/2021	12/18/2021	12/25/2021	01/01/2022
1	Requirement Analysis	10/02/2021	10/16/2021	14														
2	System Design	10/17/2021	11/07/2021	20														
3	Implementation	11/08/2021	12/04/2021	27														
4	Testing	12/05/2021	12/11/2021	7														
5	Deployment	12/13/2021	12/18/2021	6														
6	Maintenance	12/20/2021	12/25/2021	6														
7	Report Writing	10/02/2021	01/01/2022	till end														

3.1.3 Analysis

Data Modelling using ER diagram

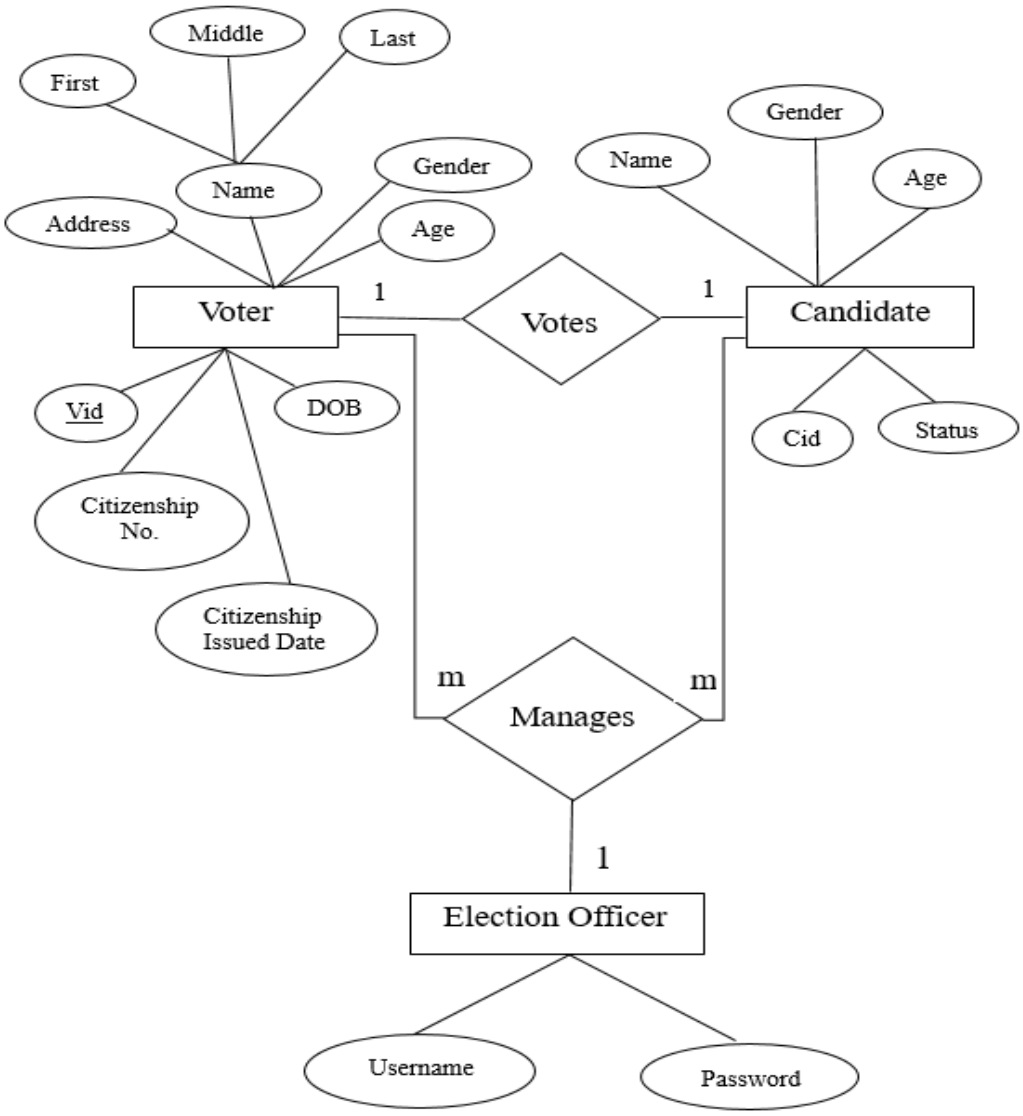


Figure 3: ER Diagram of eChunab

Process Modelling using DFD diagram

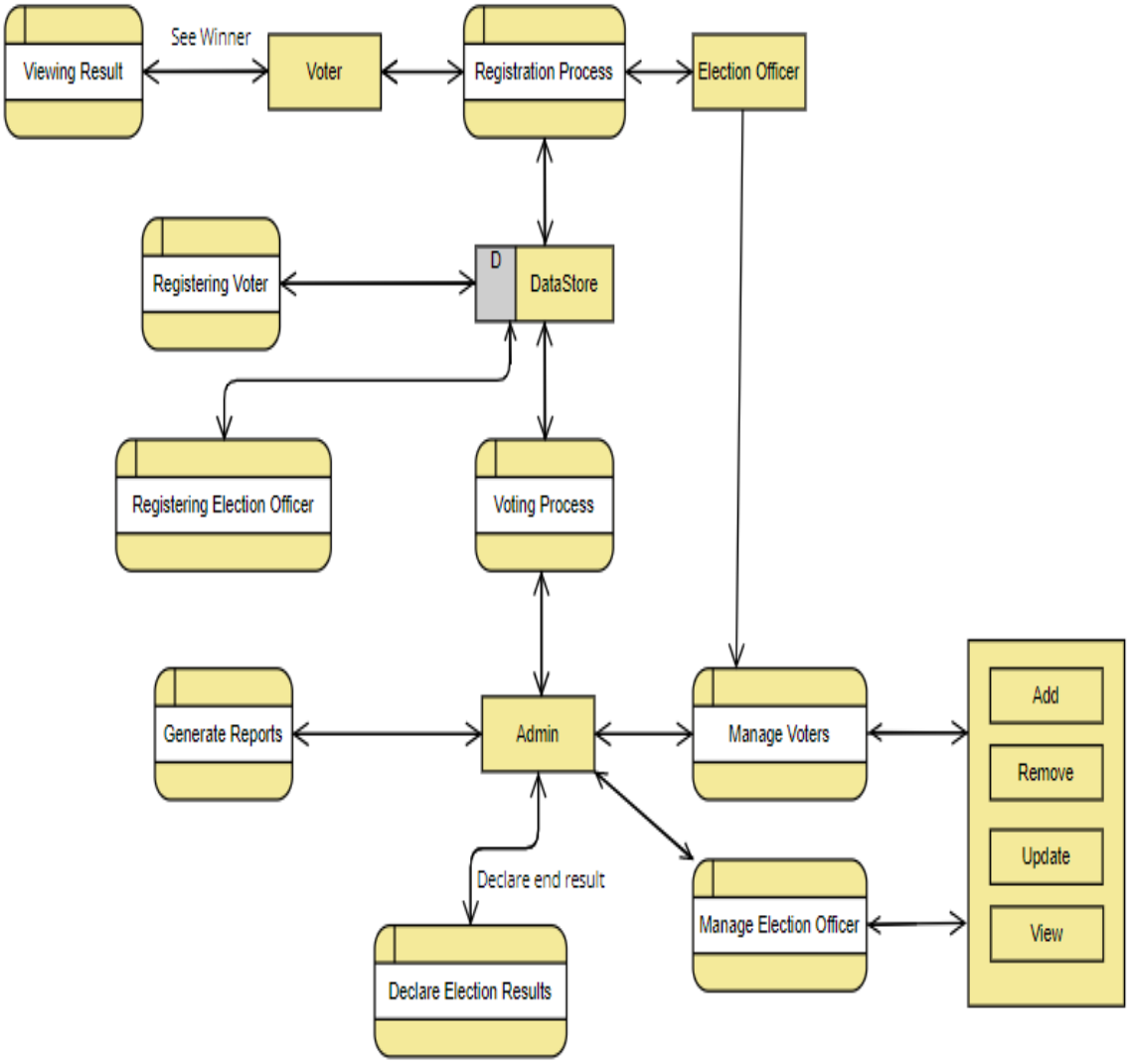


Figure 4: DFD Diagram of eChunab

CHAPTER 4: SYSTEM DESIGN

4.1 Design

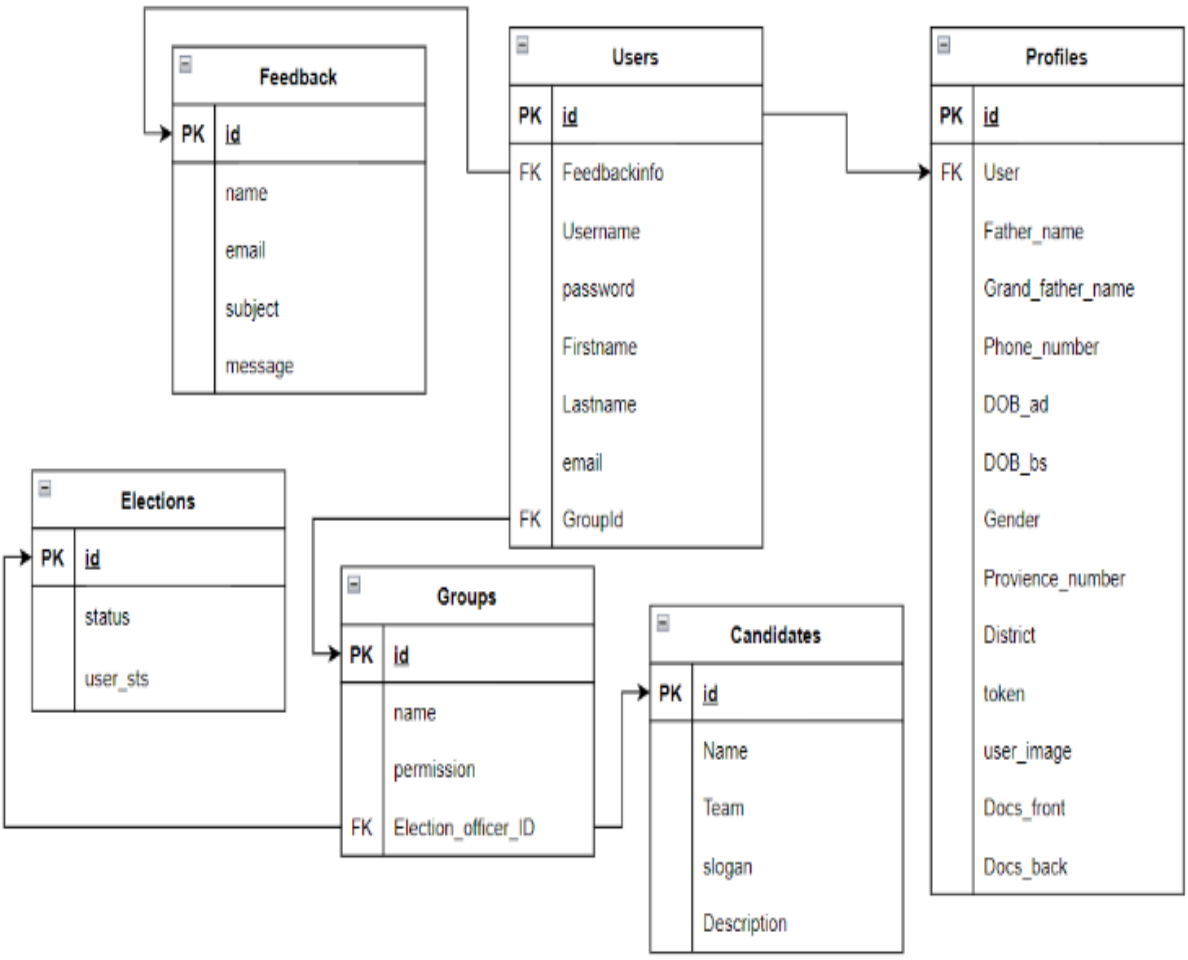


Figure 5: Database Design of eChunab

The different dabase tables designed are mentioned above. These tables have relations among each others. There are two types of users, one is user who cast vote to candidate and another is office who controls the elections. The ***user*** sends feedback. The ***feedback*** is resolve by officer. ***Election_officer*** is responsible to manage the candidate. The election table has two entities- ***status***, which is boolean, to start or end election and ***user_sts***, which is also boolean to make voting process visible and invisible.

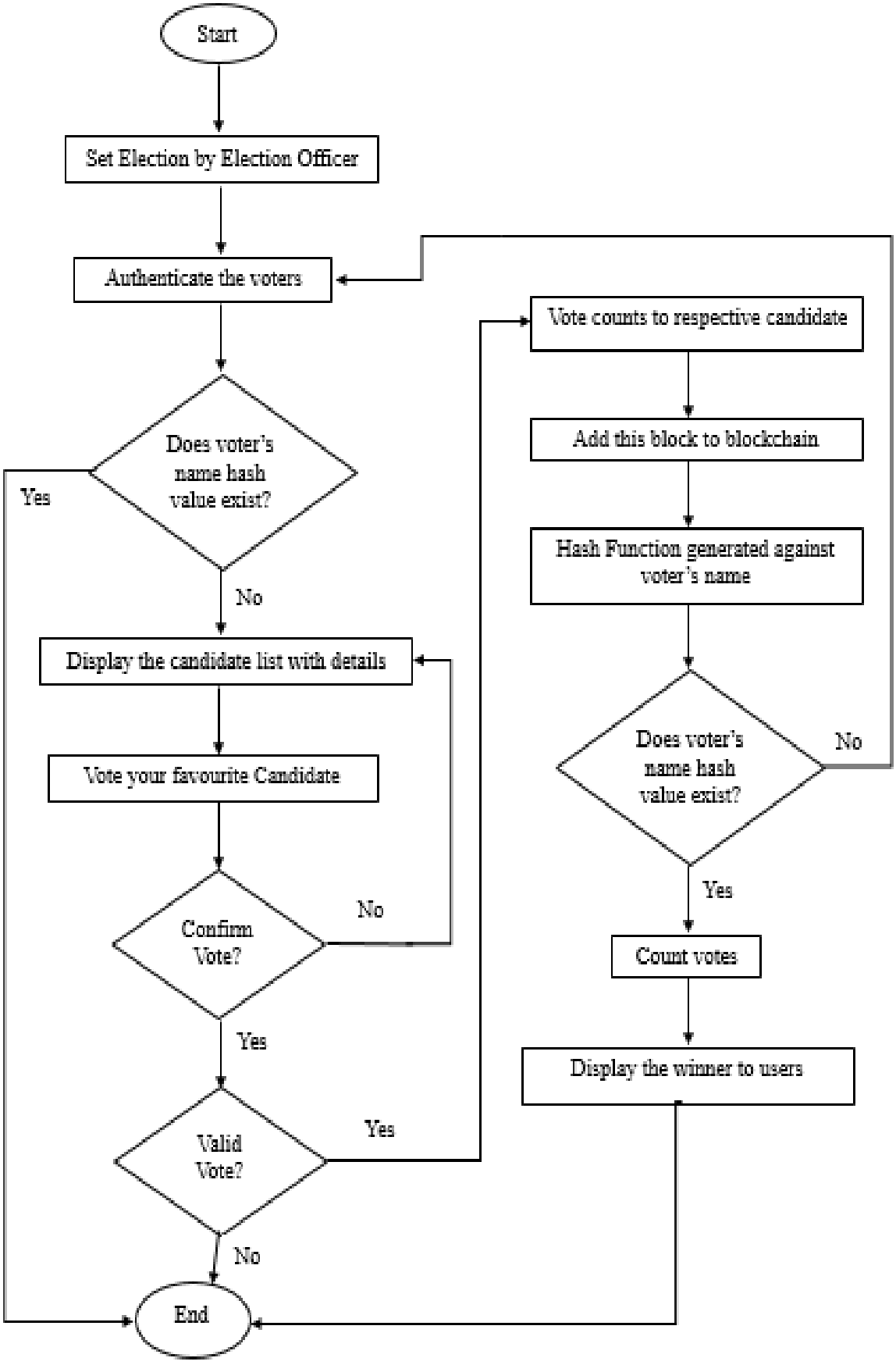


Figure 6: Flow chart of eChunab

4.2 Algorithm Details:

There are two general algorithms used in our project. The first algorithm is related with the implementation of blockchain technology where as other one, SHA-256 is for the security purpose.

i) Consensus Algorithm in Blockchain:

A consensus algorithm is a procedure through which all the peers of the Blockchain network reach a common agreement about the present state of the distributed ledger. In this way, consensus algorithms achieve reliability in the Blockchain network and establish trust between unknown peers in a distributed computing environment.

Proof of stake (Pos) is used to achieve distributed consensus in a Blockchain. The working mechanism of Pos are listed below;

- Nodes makes transactions. Pos algorithm put all these transactions in a pool.
- All the nodes contending to become validator for the next block raise a stake. This stake is combined with other factors like 'coin-age' or 'randomized block selection' to select the validator.
- The validator verifies all the transactions and publishes the block. His stake still remains locked and the forging reward is also not granted yet. This is so that the nodes on the network can 'OK' the new block.
- If the block is 'OK'-ed, the validator gets the stake back and the reward too. If the algorithm is using a coin-age based mechanism to select validators, the validator for the current blocks has its coin-age reset to 0. This puts him in a low-priority for the next validator election.
- If the block is not verified by other nodes on the network, the validator loses its stake and is marked as 'bad' by the algorithm. The process again starts from step 1 to forge the new block.

ii) SHA-256:

SHA-256 is used in this project for secure password hashing. Cryptocurrencies use SHA-256 for verifying transactions. Three properties make SHA-256 this secure. First, it is almost impossible to reconstruct the initial data from the hash value. A brute-force attack would need to make 2256 attempts to generate the initial data. Second, having two messages with the same hash value (called a collision) is extremely unlikely. With 2256

possible hash values (more than the number of atoms in the known universe), the likelihood of two being the same is infinitesimally, unimaginably small. Finally, a minor change to the original data alters the hash value so much that it's not apparent the new hash value is derived from similar data; this is known as the avalanche effect.

Voting Algorithm:

Step1: Start

Step2: Voter/User are supposed to authenticate their identity.

Step3: Checks the identity of the voter.

Step4: If identity verifies, list of candidates shown to the end users.

Step5: Checks if the verified voter has already voted or not, if already voted then throws an error message, "You have already voted.".

Step6: Else transaction is confirmed.

Step7: Voted successfully.

Step8: Display the result of election after the end of election time.

Step9: End

CHAPTER 5: IMPLEMENTATION AND TESTING

5.1 Implementation

5.1.2 Tools Used

Programming Language is a high level language used to write a computer programs, which allows programmers to write the source code in a natural fashion using logical words and symbols. The major three programming language used are:

a) **Solidity:** Solidity is an object-oriented, high-level language for implementing smart contracts. Smart contracts are programs which governs the behavior of account with in the Ethereum state. It is influenced by C++, Python, and Javascript and is designed to target the Ethereum Virtual Machine(EVM). It is statically typed, supports inheritance, libraries and complex user-defined types among other features. With solidity one can create a crontracts for different uses such as voting, crowfunding, blind auctions, and multi-signature wallets [7].

b) **Python:** Python is an interpreted, object-oriented, high-level programming language with dynamic semantics. Its high-level built in data structures, combined with dynamic typing and dynamic binding, make it very attractive for RAD as well as for use as a scripting components together. It's simple, easy to learn syntax emphasizes readability and therefore reduces the cost of program maintenance. It supports modules and packages, which encourages program modularity and code reuse. The standard library of python is free of cost and is available for all platforms [8].

c) **Java Script:** JavaScript (js) is a light-weight object-oriented programming language which is used by several websites for scripting the webpages. It is an interpreted, full-fledged programming language that enables dynamic interactivity on websites when applied to an HTML document. It was introduced in the year 1995 for adding programs to the webpages in the Netscape Navigator browser. Since then, it has been adopted by all other graphical web browsers. With JavaScript, users can build modern web applications to interact directly without reloading the page every time. The traditional website uses js to provide several forms of interactivity and simplicity. Although, JavaScript has no connectivity with Java programming language. The name was suggested and provided in the times when Java was gaining popularity in the market. In addition to web browsers, databases such as CouchDB and MongoDB uses JavaScript as their scripting and query language [9].

For storing and retrieving the data, the most commonly used database i.e SQL is integrated. SQLite databases are lightweight and easy to handle. In contrast to other database frameworks, there is no setup, establishment needed to begin chipping away at an SQLite Open database. We will kick off dealing with SQLite databases and tables straightforwardly. SQLite provides the create database functionality to users, in which that user can be able to create a database as per their requirement. SQLite gives you the alternative of making another database (or opening a current one) each time you start the order line utility. At the point when you use sqlite3 to begin the command line utility, you can alternatively affix a data set document name.

Besides these other most important tools and technologies implemented in the system are:

I. **Truffle:** A world class development environment, testing framework and asset pipeline for blockchains using the Ethereum Virtual Machine (EVM), aiming to make life as a developer easier.

II. **Etherium:** Ethereum smart contracts are programs executed within the context of transactions on the Ethereum blockchain. Ethereum Ganache forms part of the Truffle Suite, a set of developer tools that allows users to recreate blockchain environments locally and test smart contracts. Smart contract execution on the Ethereum blockchain is very different from other types of software.

   First of all, the on-chain context makes it hard to communicate with the outside world. Simple input and output operations, such as writing to a console, are not possible, as transactions are the only means of communicating with the blockchain. Secondly, the transactional nature of the blockchain means that all state changing interactions with a smart contract are asynchronous in nature. This means that when transactions are sent, the effects are not visible until the transaction has been confirmed by being included in a block. Finally, the blockchain environment places some specific restrictions on the code that can be executed, mostly related to the cost associated with each operation. Programmers have to consider factors such as the block gas limit, or how many operations can be executed safely within the gas allowance of certain functions. In short, smart contracts are hard to program. In addition, once deployed, smart contracts cannot be modified and each deployment has an associated cost. Getting things right the first time, therefore, has a criticality usually only associated with software in high-risk applications such as control software in critical infrastructures or aviation. In order to debug and test smart contracts before going into production, it is therefore essential to

allow developers to recreate blockchain environments locally, without the added inconvenience of deployment costs and transaction delays.Fortunately, the Truffle Suite, a set of developer tools for Ethereum, includes Ethereum Ganache, a tool designed for this purpose [10].

5.1.2 Implementation Details of Modules

We used smart contracts to govern the activities of the accounts which are used to sign the transaction to the ethereum virtual blockchain. The major functionalities used in our smart contracts are pointed below:

- addCandidate: It is the function which adds the list of candidates to the ethereum blockchain along with assigning the candidate a null vote and their respective id starting from one.
- Vote: We use this module to sign the transaction for votes using the user's respective tokens (which is unique 64 characters and is validated by the web3 API). Due to the use of tokens, a user can never cast a vote twice. Here, we used a modifier which checks that a user can vote only once.
- getName: We use this module to get the names of the candidates by passing their prospective IDs.
- We have five other modules which help while testing the systems.

Process:

Truffle is used to compile the smart contract and save the migrations and artifacts to the blockchain. The Web3.py API added in the project talks to the ethereum network chain for adding, updating, & modifying the candidate's name and their prospective vote count. Users are registered and a 256 bits token is provided to the user by the ganache, where virtual blockchain is hosted, with which users can sign transactions to vote for a candidate. The other main functions of the web3.py are listed below.

- Web3.eth.accounts: It provides the addresses of the blockchain to the user
- Web3.HTTPprovides: It connects the web3 API to the blockchain network.

5.2 Testing

Software testing is a method to check whether the actual software product matches expected requirements and to ensure that software product is Defect free. In short, software testing

means verification of AUT. Out of the various testing strategies the following table summarizes the unit testing and system testing of the proposed system.

Table 2: Test Case for Signup Page

Test ID	Test Description	Input Test Data	Expected Result	Actual Result	Status
1	Enter valid Details	Citizenship ID, First Name, Last Name, Email, Password, Password Confirmation, Gender, Father's Name, Grand Father's Name, Province No, District, Phone Number, DOB, Images	Redirect to Login Page	Redirect Successful	Pass
2	Enter Incomplete Details	Citizenship ID, First Name, Last Name, Email, Password, Password Confirmation, Gender, Father's Name, Grand Father's Name, Province No, District, Phone Number, DOB, Images	Error message appeared Redirect to Signup Page	Error message appeared Redirected to Signup Page	Pass

Table 3: Test Case for Vote now page

Test ID	Test Description	Input Test Data	Expected Result	Actual Result	Status
1	When User Clicked Vote Now Button	Null	Voted Successfully	Voted Successfully	Pass

Table 4: Test Case for login page

Test ID	Test Description	Input Test Data	Expected Result	Actual Result	Status
1	Enter valid login Details	Citizenship ID, Password	Redirect to Dashboard	Redirect Successful	Pass
2	Invalid login credentials	Wrong Citizenship ID, Password	Redirect to Login Page	Error message appeared	Pass
3	logout	null	Redirect to Landing Page	Redirect Successful	Pass

Table 5: Test Case for Dashboard page

Test ID	Test Description	Input Test Data	Expected Result	Actual Result	Status
1	When Voting Process started	null	Show the Candidates	Show the Candidates	Pass
2	When Voting Process isn't started	null	Redirect to Not Started	Redirect to Not Started	Pass
3	When Result isn't published	null	Redirect to No Result	Redirect to No Result	Pass
4	When Result is published	null	Show Result	Show Result	Pass
5	When user submit Query	Name, Email, Subject, Message	Query Submitted	Query Submitted	Pass
6	When user is Idle for 20 Minute	null	Logout User	Logout User	Pass

Table 6: Test Case for Officer page

Test ID	Test Description	Input Test Data	Expected Result	Actual Result	Status
1	Election is live	Token assigned to User	Show End Election option in officer dashboard and Run the election	Show End Election option in officer dashboard and Run the election	Pass
2	Election is not started	null	Show Start Election option in officer dashboard	Show Start Election option in officer dashboard	Pass
3	Officer clicked Candidates button	null	Officer CRUD candidates	Officer CRUD candidates	Pass
4	Officer Clicked User Button	null	Officer CRUD User	Officer CRUD User	Pass
5	Officer Clicked User Queries	null	User Query shown	User Query Shown	Pass

Table 7: Integration Test for eChunab

Test ID	Test Case Objective	Test Case Description	Expected Result	Actual Result	Status
1	Check the interface linked between Signup and login module	Enter Required details and click signup button	To be directed to the login page	To be directed to the login page	Pass
2	Check the interface linked between login module and Dashboard Module	Enter Required details and click Login button	To be directed to the Dashboard page	To be directed to the Dashboard page	Pass
3	Check the interface linked between Dashboard page and Vote now module	Click Vote now button	To be directed to the Voting page	To be directed to the Voting page	Pass
4	Check the interface linked between Dashboard page and Result module	Click Result button	To be directed to the result page	To be directed to the result page	Pass
5	Check the interface linked between Dashboard page and Query module	Click query button and fill the details	Details stored on DB and reflected to Officer module	Details stored on DB and reflected to Officer module	Pass
6	Check the interface linked between login module and Officer Module	Enter officer login details	To be directed to Officer page	To be directed to Officer page	Pass

CHAPTER 6: CONCLUSION AND FUTURE RECOMMENDATIONS

6.1 Conclusion:

This project simplifies the process of polling and counting votes and hence provide the exact number of vote count to the election officer. This whole process is decentralized using a Blockchain which makes it more secure, faster, distributed and better than the traditional system. The voters/users involved are highly authorized by the system so that no false users cast the votes. Finally, the election officer involved helps to publish the result to the public after the time limit ends.

With the robust growth of blockchain technology in recent years, there is no doubt that more disruption for the credit rating industry are yet to come. The application of the technology in the government will not only provide secured voting process in national level but will be beneficial for other private/public agencies. It becomes very easy for organizations to make better pooling system and accurate voting results. This project solves the problem of voting process and reach out to mass audience who are capable to vote.

6.2 Future Recommendation:

This project can be further continued with the following recommendations:

- Integrating the voice command for disabled voters.
- Biometric validation of the users can be used.
- Developing mobile, desktop app for simplicity of the project.

References

[1] "SDLC - Waterfall Model.," [Online]. Available: https://www.tutorialspoint.com/sdlc/sdlc_waterfall_model.htm. . [Accessed 15 october 2021].

[2] L. Vo-Cao-Thuy, K. Cao-Minh, C. Dang-Le-Bao and T. A. Nguyean, "Votereum: An Ethereum-based E-voting system," 2019.

[3] D. Khoury, E. F. Kfoury, A. Kassem and H. Harb, "Decentralized Voting Platform Based on Ethereum Blockchain," 2018.

[4] K. Simkhada, "E-Voting: Possibilities and Challenges in the Nepalese Context," (Accessed: 01-Nov-2021).

[5] R. Karmacharya and R. Shrestha, "Implementing Blockchain in online voting for out-of-country Nepalese Voters".

[6] R. T. Justis and B. Kreigsmann, "The feasibility study as a tool for venture analysis," *Business Journal of Small Business Management*, vol. 17, pp. 35-42, 1979.

[7] "Solidity Docs," [Online]. Available: https://docs.soliditylang.org/en/v0.8.12/. [Accessed 21 November 2021].

[8] "Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Python_(programming_language). [Accessed 21 November 2021].

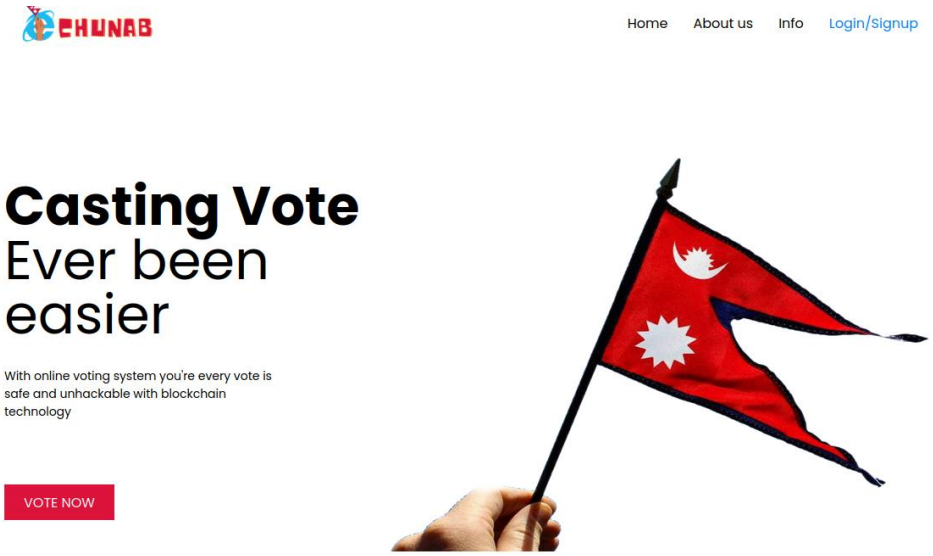
[9] "Java T Point," [Online]. Available: https://www.javatpoint.com/javascript-tutorial. [Accessed 21 November 2021].

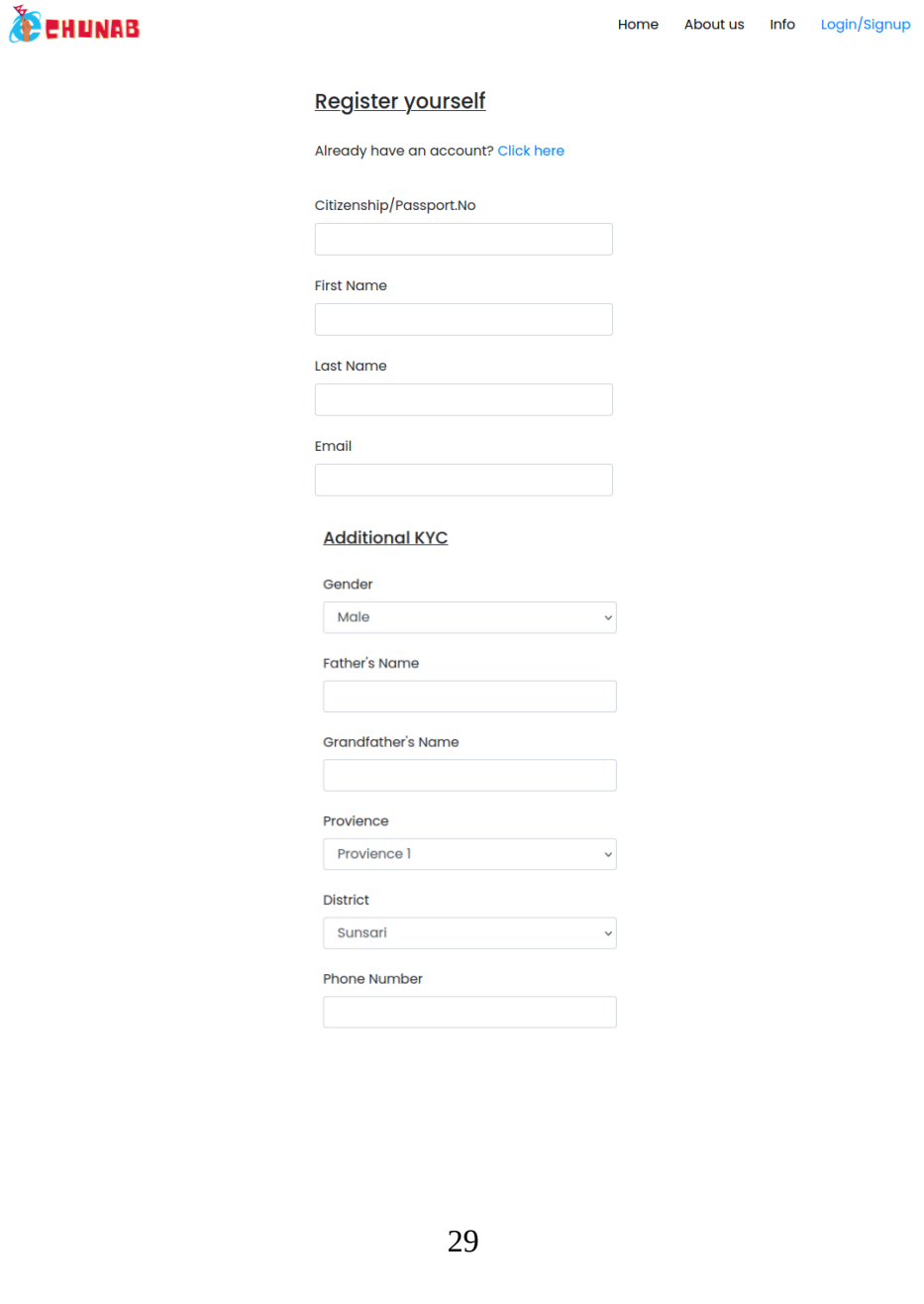
[10] "Coin Base," [Online]. Available: https://www.coinbase.com/price/ethereum#. [Accessed 22 November 2021].

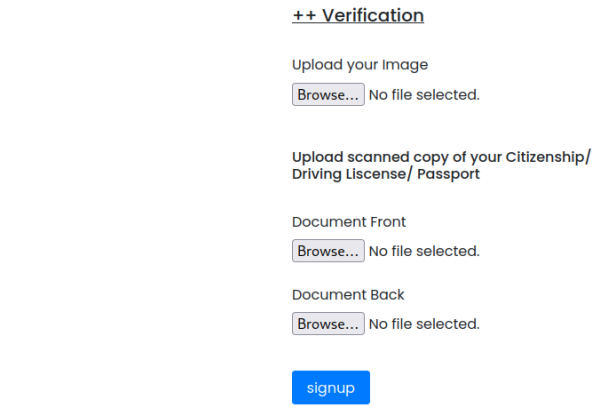
Bibliography

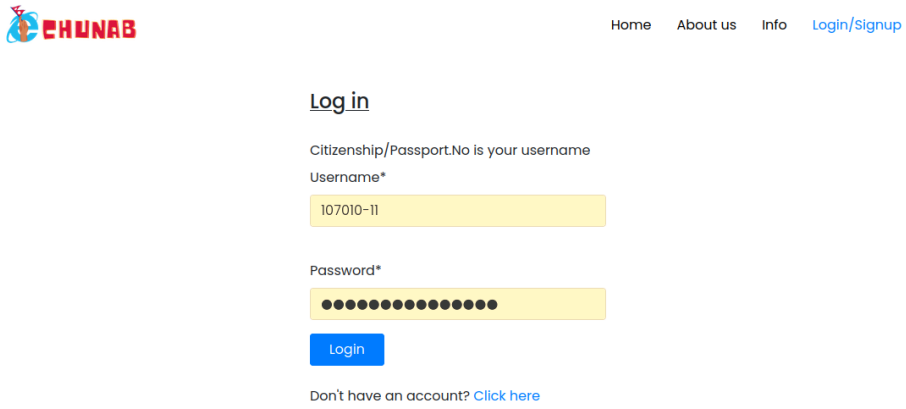
1. Ahmed Ben Ayed, “A Conceptual Secure Blockchain based Electronic Voting System”, IJNSA, Vol.9, No.3, May 2017.
2. D. Zhu, "Fraud detections for online businesses: a perspective from blockchain technology," December 2016.

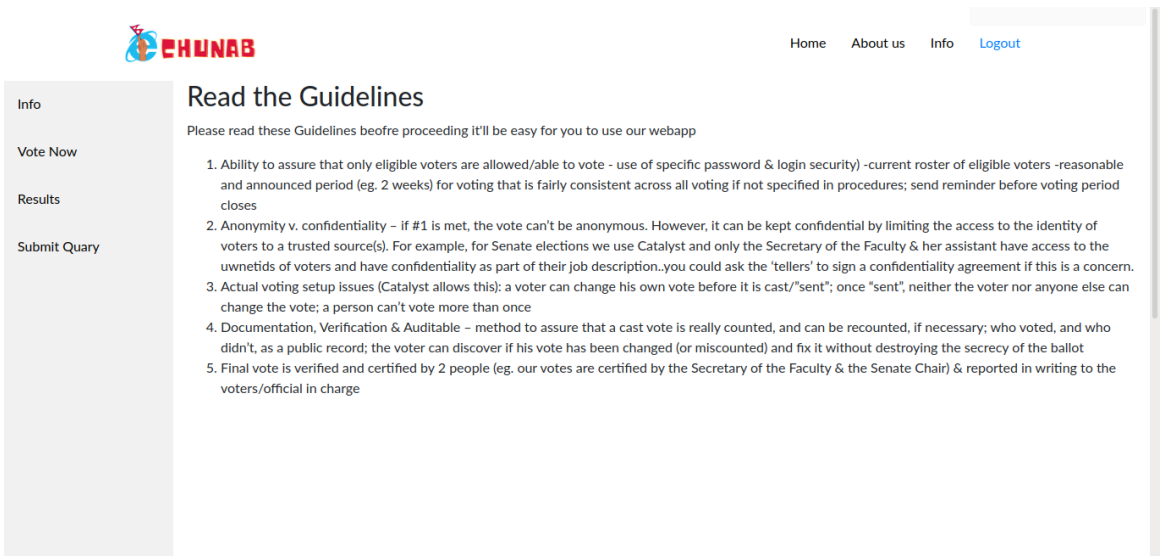
Appendices

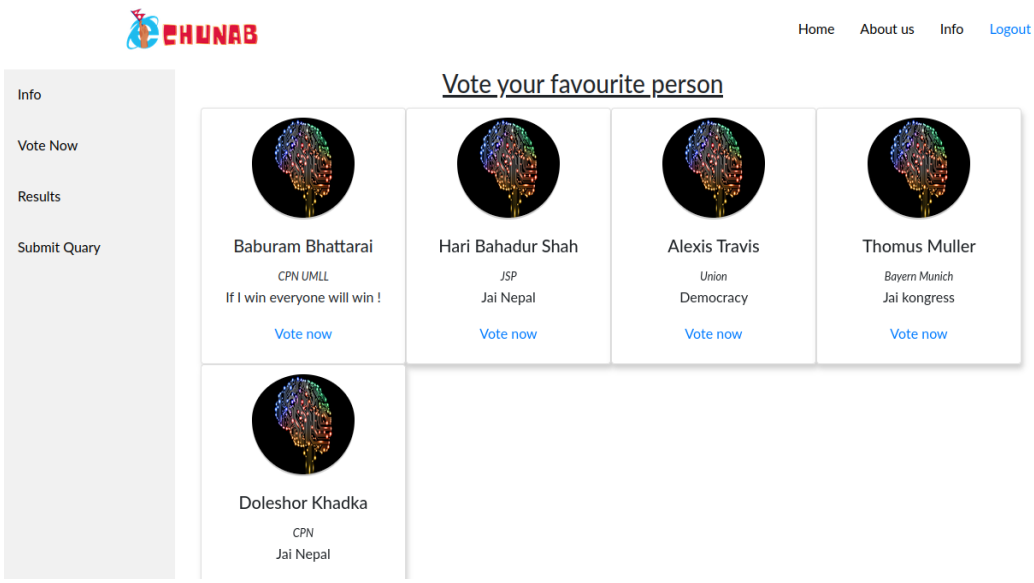

CHUNAB
Home
About us
Info
Login/Signup
Casting Vote
Ever been
easier
With online voting system you're every vote is safe and unhackable with blockchain technology
VOTE NOW

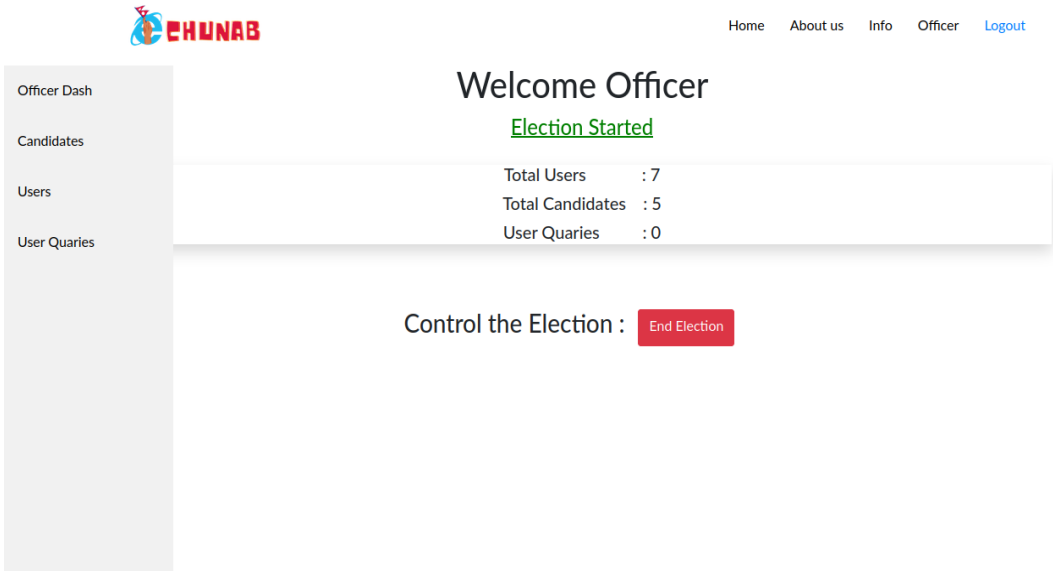

CHUNAB
Home
About us
Info
Login/Signup
Register yourself
Already have an account? Click here
Citizenship/Passport.No
First Name
Last Name
Email
Additional KYC
Gender
Male
Father's Name
Grandfather's Name
Provience
Provience 1
District
Sunsari
Phone Number

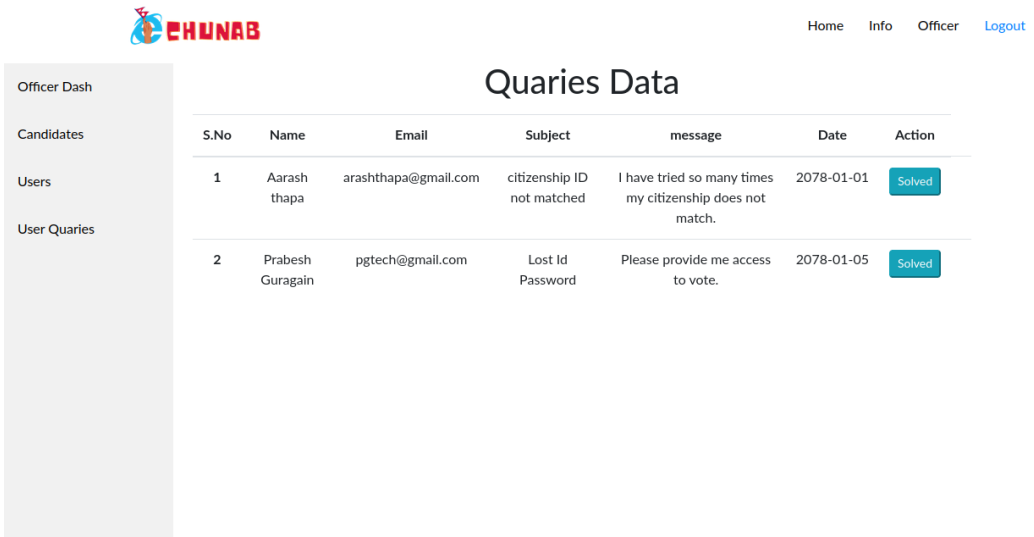

++ Verification
Upload your Image
Browse... No file selected.
Upload scanned copy of your Citizenship/ Driving Liscense/ Passport
Document Front
Browse... No file selected.
Document Back
Browse... No file selected.
signup

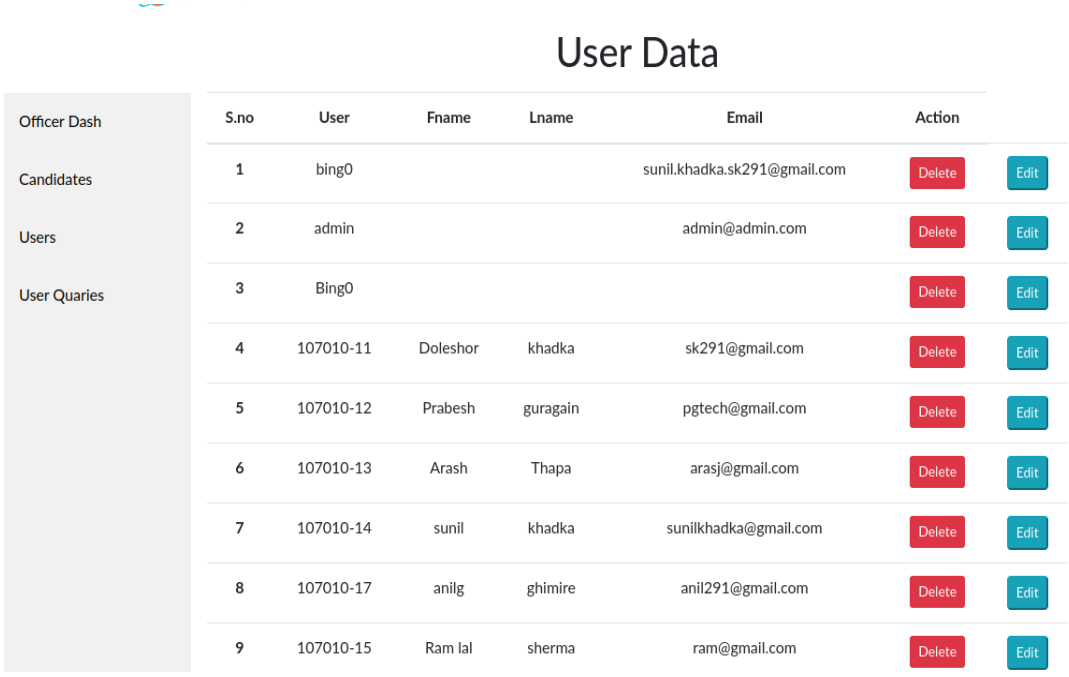

CHUNAB
Home
About us
Info
Login/Signup
Log in
Citizenship/Passport.No is your username
Username*
107010-11
Password*
Login
Don't have an account? Click here

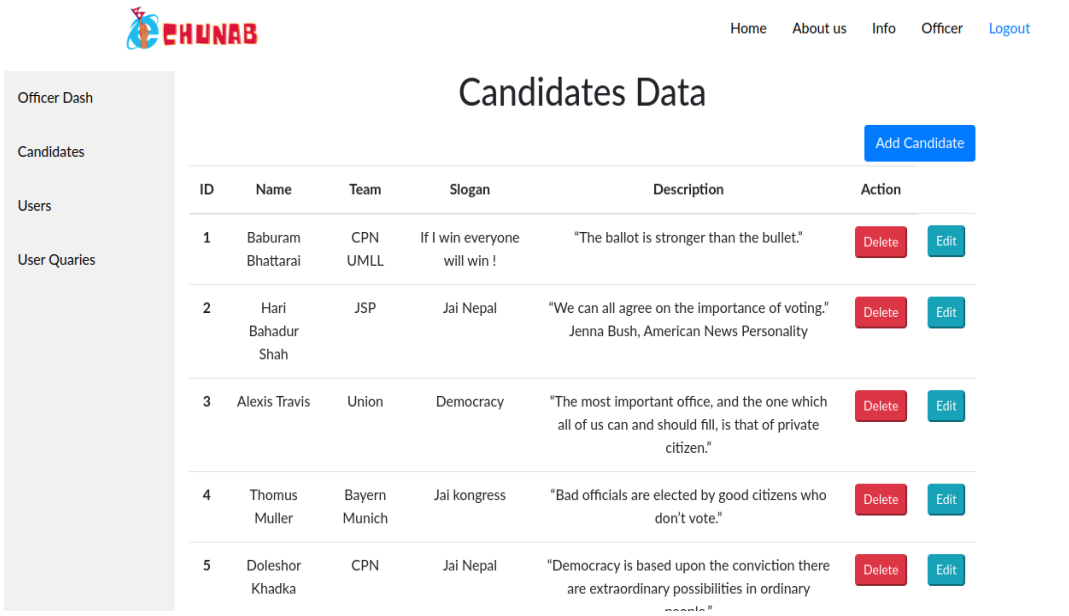

CHUNAB
Home
About us
Info
Logout
Info
Vote Now
Results
Submit Quary
Read the Guidelines
Please read these Guidelines beofre proceeding it'll be easy for you to use our webapp
1. Ability to assure that only eligible voters are allowed/able to vote - use of specific password & login security) -current roster of eligible voters -reasonable and announced period (eg. 2 weeks) for voting that is fairly consistent across all voting if not specified in procedures; send reminder before voting period closes
2. Anonymity v. confidentiality – if #1 is met, the vote can't be anonymous. However, it can be kept confidential by limiting the access to the identity of voters to a trusted source(s). For example, for Senate elections we use Catalyst and only the Secretary of the Faculty & her assistant have access to the uwnetids of voters and have confidentiality as part of their job description..you could ask the 'tellers' to sign a confidentiality agreement if this is a concern.
3. Actual voting setup issues (Catalyst allows this): a voter can change his own vote before it is cast/"sent"; once "sent", neither the voter nor anyone else can change the vote; a person can't vote more than once
4. Documentation, Verification & Auditable – method to assure that a cast vote is really counted, and can be recounted, if necessary; who voted, and who didn't, as a public record; the voter can discover if his vote has been changed (or miscounted) and fix it without destroying the secrecy of the ballot
5. Final vote is verified and certified by 2 people (eg. our votes are certified by the Secretary of the Faculty & the Senate Chair) & reported in writing to the voters/official in charge

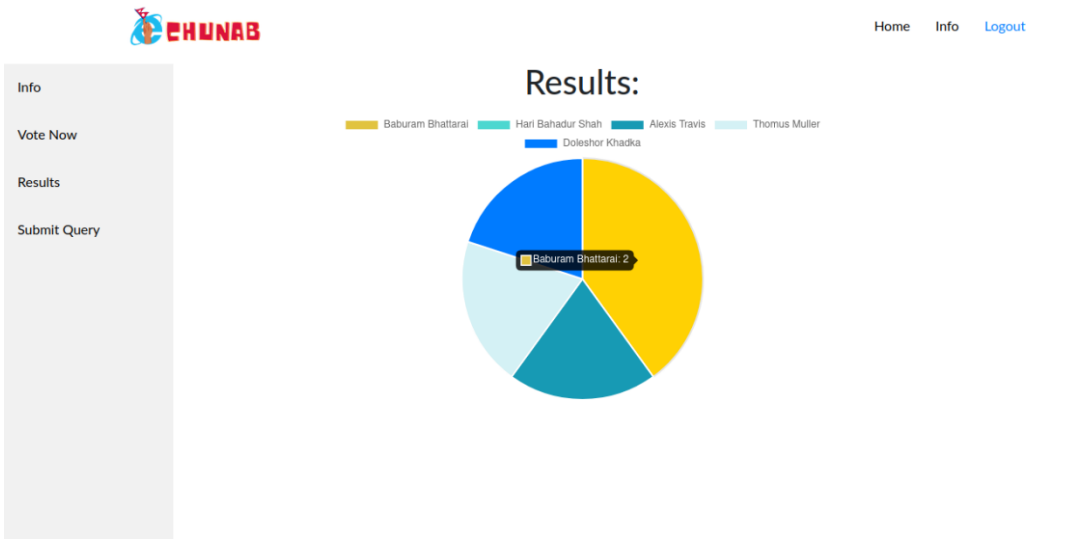

CHUNAB
Home
About us
Info
Logout
Info
Vote Now
Results
Submit Quary
Vote your favourite person
Baburam Bhattarai
CPN UMLL
If I win everyone will win !
Vote now
Hari Bahadur Shah
JSP
Jai Nepal
Vote now
Alexis Travis
Union
Democracy
Vote now
Thomus Muller
Bayern Munich
Jai kongress
Vote now
Doleshor Khadka
CPN
Jai Nepal


CHUNAB
Home
About us
Info
Officer
Logout
Officer Dash
Candidates
Users
User Quaries
Welcome Officer
Election Started
Total Users : 7
Total Candidates : 5
User Quaries : 0
Control the Election :
End Election


CHUNAB
Home
Info
Officer
Logout
Officer Dash
Candidates
Users
User Quaries
Quaries Data
S.No
Name
Email
Subject
message
Date
Action
1
Aarash thapa
arashthapa@gmail.com
citizenship ID not matched
I have tried so many times my citizenship does not match.
2078-01-01
Solved
2
Prabesh Guragain
pgtech@gmail.com
Lost Id Password
Please provide me access to vote.
2078-01-05
Solved


User Data
Officer Dash
Candidates
Users
User Quaries
S.no User Fname Lname Email Action
1 bing0 sunil.khadka.sk291@gmail.com Delete Edit
2 admin admin@admin.com Delete Edit
3 Bing0 Delete Edit
4 107010-11 Doleshor khadka sk291@gmail.com Delete Edit
5 107010-12 Prabesh guragain pgtech@gmail.com Delete Edit
6 107010-13 Arash Thapa arasj@gmail.com Delete Edit
7 107010-14 sunil khadka sunilkhadka@gmail.com Delete Edit
8 107010-17 anilg ghimire anil291@gmail.com Delete Edit
9 107010-15 Ram lal sherma ram@gmail.com Delete Edit


CHUNAB
Home About us Info Officer Logout
Candidates Data
Officer Dash
Candidates
Users
User Quaries
Add Candidate
ID Name Team Slogan Description Action
1 Baburam Bhattarai CPN UMLL If I win everyone will win ! "The ballot is stronger than the bullet." Delete Edit
2 Hari Bahadur Shah JSP Jai Nepal "We can all agree on the importance of voting." Jenna Bush, American News Personality Delete Edit
3 Alexis Travis Union Democracy "The most important office, and the one which all of us can and should fill, is that of private citizen." Delete Edit
4 Thomus Muller Bayern Munich Jai kongress "Bad officials are elected by good citizens who don't vote." Delete Edit
5 Doleshor Khadka CPN Jai Nepal "Democracy is based upon the conviction there are extraordinary possibilities in ordinary


CHUNAB
Home Info Logout
Info
Vote Now
Results
Submit Query
Results:
Baburam Bhattarai Hari Bahadur Shah Alexis Travis Thomus Muller
Doleshor Khadka
Baburam Bhattarai: 2

Meeting Report

MEETING REPORT – 1ST			
Project Name:	eChunab		
Date of meeting:	2078-07-10	Time:	10:30 am
Meeting Facilitator:	Prakash Neupane	Location:	Godawari College

1. Meeting Objective:

- Proposal Checking
- Discussion on Feature integration
- Algorithm Discussion

2. Attendance:

Name	E-mail
Arash Thapa	xettriaarash@gmail.com
Doleshor Khadka	Sunil.khadka.sk291@gmail.com
Prabesh Guragain	prbshguragain@gmail.com

3. Meeting Agenda:

- Way of Documentation
- System Requirements
- Features discussion

4. Preparation:

Description	Prepared By
Documentation, High level design	Arash Thapa
Requirement Identification	Doleshor Khadka
Expected outcome, layout design	Prabesh Guragain

5. Assign Work:

- Design Prototype
- Build Algorithm
- Design Structure of report

MEETING REPORT – 2ND			
Project Name:	eChunab		
Date of meeting:	2078-07-25	Time:	10:30 am
Meeting Facilitator:	Prakash Neupane	Location:	Godawari College

1. Meeting Objective:

- Prototype checking
- Algorithm checking
- Report format checking

2. Attendance:

Name	E-mail
Arash Thapa	xettriaarash@gmail.com
Doleshor Khadka	Sunil.khadka.sk291@gmail.com
Prabesh Guragain	prbshguragain@gmail.com

3. Meeting Agenda:

- Prototype Discussion
- Data Model Discussion
- Voting Process

4. Preparation:

Description	Prepared By
Design Data Model	Arash Thapa
Build Prototype	Doleshor Khadka
Build Prototype	Prabesh Guragain

5. Assign Work:

- Update Prototype
- Design Landing, signup/Login page
- Design database

MEETING REPORT – 3RD			
Project Name:	eChunab		
Date of meeting:	2078-07-25	Time:	10:30 am
Meeting Facilitator:	Prakash Neupane	Location:	Godawari College

1. Meeting Objective:

- Prototype Checking
- Home page, Login/Signup page Checking
- Database Design Checking

2. Attendance:

Name	E-mail
Arash Thapa	xettriaarash@gmail.com
Doleshor Khadka	Sunil.khadka.sk291@gmail.com
Prabesh Guragain	prbshguragain@gmail.com

3. Meeting Agenda:

- Database Design Discussion
- Design of home page and login/register page

4. Preparation:

Description	Prepared By
Documentation, System Design	Arash Thapa
Backend	Doleshor Khadka
Frontend	Prabesh Guragain

5. Assign Work:

- Validation in register and voting process
- System Design (Diagrams)
- Add KYC Features

MEETING REPORT – 4TH			
Project Name:	eChunab		
Date of meeting:	2078-08-29	Time:	7:30 pm
Meeting Facilitator:	Prakash Neupane	Location:	Google Meet

1. Meeting Objective:

- Validation Checking
- Diagrams Checking
- KYC checking

2. Attendance:

Name	E-mail
Arash Thapa	xettriaarash@gmail.com
Doleshor Khadka	Sunil.khadka.sk291@gmail.com
Prabesh Guragain	prbshguragain@gmail.com

3. Meeting Agenda:

- Final Documentation Discussion
- Adding additional front end features

4. Preparation:

Description	Prepared By
Necessary System design (Diagrams)	Arash Thapa
Backend	Doleshor Khadka
Validation, add KYC form	Prabesh Guragain

5. Assign Work:

- Final Document
- Testing Process
- Show election result in chart view

MEETING REPORT – 5TH			
Project Name:	eChunab		
Date of meeting:	2078-09-20	Time:	8:30 pm
Meeting Facilitator:	Prakash Neupane	Location:	Google Meet

1. Meeting Objective:

- Document Checking
- System demo
- Testing checking

2. Attendance:

Name	E-mail
Arash Thapa	xettriaarash@gmail.com
Doleshor Khadka	Sunil.khadka.sk291@gmail.com
Prabesh Guragain	prbshguragain@gmail.com

3. Meeting Agenda:

- Final Documentation Discussion
- Viewing overall system Demo

4. Preparation:

Description	Prepared By
Documentation	Arash Thapa
Backend	Doleshor Khadka
Frontend	Prabesh Guragain

5. Assign Work:

- Reference Formatting
- Managing Table of Content