Tribhuvan University

Institute of Science and Technology

GODAWARI COLLEGE

Proposal in "eChunab", an Online Voting System Using Blockchain

Submitted to

Department of Computer Science and Information Technology

Godawari College

Submitted by

ARASH THAPA (16449)

DOLESHOR KHADKA (16458)

PRABESH GURAGAIN (16464)

1st July 2021

In the partial fulfillment of the requirement for the degree of

Bachelor of Science in Computer Science and Information Technology

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.

Table of content

List of Figures

1. Introduction and Background

"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.

Blockchain is one technology which is said to be bringing in a revolution on par with the birth of internet. What started as a decentralizing currency and assests is now disrupting every mainstream industry. Wheather its fintech, healthcare, pharmaceuticals, insurance, digital security, enterprise etc. i.e blockchain is everywhere today.

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 Django framework. The web page to caste vote is developed using HTML, CSS, javascript, Python using Django Framework.

1.1 Web Portal

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.

1.1.1 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 atlast use for verification process.

1.1.2 Cast Vote: Validate users/voters can cast a vote. The voter login authenticated by Django and cast a vote while the voting process is represented by the ETH transaction.

1.2 Blockchain

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. [1]

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

1.3 Smart Contract

A smart contract is a self-employed contract that contains the terms of the agreement between the buyer and the seller written directly in the lines of code. The code and the agreements contained in it are available throughout the expanded, extended blockchain network. The code controls performance, and the action is trackable and irreversible.

Intelligent contracts allow trustworthy transactions and agreements to be made between different parties, anonymous without the need for a central authority, legal system, or external enforcement mechanism.

1.4 Etherium

Ethereum is a separate, open source blockchain that works with a smart contract. Ether (ETH) is a traditional cryptocurrency platform.

The forum allows anyone to install applications that are permanently divided and unmodified, with which users can interact.

1.2.1 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]
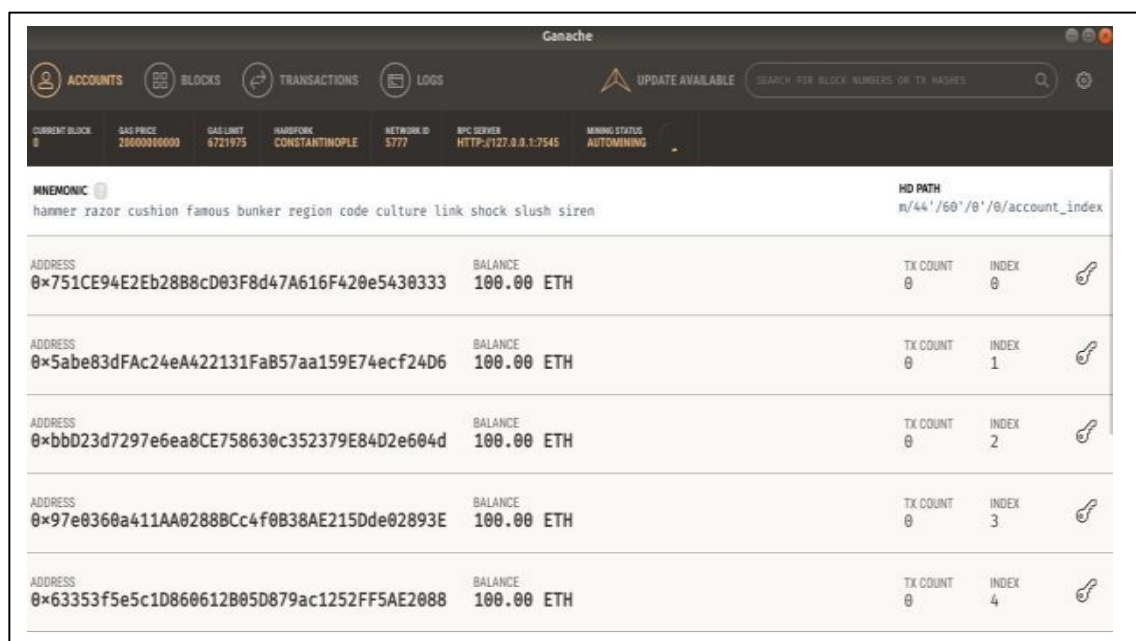
Fig-1 :- Sample view of Ganache

1.2.2 Truffle:

Truffle is a framework for creating, testing, and sending applications to the Ethereum network. The Truffle Framework contains three key components for

Ethereum smart contract development and application development (dApp) called Truffle, Ganache, and web3.

2.Problem Definition

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 anytime

3.Objectives

The major objectives of the proposed system are :-

1. To provide a safe and secure voting platform for any local bodies, nation and organization.
2. To speed the process of vote counting and result
3. To reduce the cost of paying staffs to count the vote manually
4. To decrease the expected expenses
5. To save time for voters as they can vote from their own location
6. To make the voting process and result transparent
7. To unauthorize the illegal and multiple votes
8. To increase the voter confidence and improve the voting experience
9. To improve the registration process

4. Scope & Limitation

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.

5. Methodology

5.1 Requirement Identification:

Among the two distinct phases of requirement identification process, the first phase is based on the study of existing system and then last phase is collecting the requirements by talking to some potential users and making our system with that findings.

5.1.1   Existing System

Since the establishment of voting system in Nepal, there has been paper based voting system. This is called as ballot Paper system. Voters had to go to polling booth and tick on paper to cast their vote. Manual counting of votes leads the declaration of winner. Due to over population, the ballot paper voting is not much reliable and time consuming. There are high chances of replacement of ballot paper boxes and performing multiples marking on vote. Hence these critical problem needs to be shutout. There is no implementation of Electronic voting system till now.

5.1.2   Requirement Collection

The study of different research papers [5][6] has lead us to gathered various features that are applicable to our system. We found that the major problem in voting security. The study of 2016 US Presidential Elections found that EVM's were likely to be intercepted and votes were tampered. At last we came to know that voting equipment is not the reason besides the failure, but alteration of votes count. The system is decentralized and does not rely on trust. The major requirements for our system are listed below:

- 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.

5.2 Feasibility Study:

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. [7] The feasibility study concentrates on the following areas:

5.2.1 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.

5.2.2 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.

5.2.3 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.

6. High level design of proposed system

Entity-Relationship Model:

ER model is well suited to data modelling for use with databases because it is fairly abstract and is easy to discuss and explain. ER models are readily translated to relations. ER models, also called an ER schema, are represented by ER diagrams.

ER modelling is based on two concepts:

- Entity :- It is defined as tables that hold specific information (data)
- Relationship :- It is defined as the associations or interactions between entities

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 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
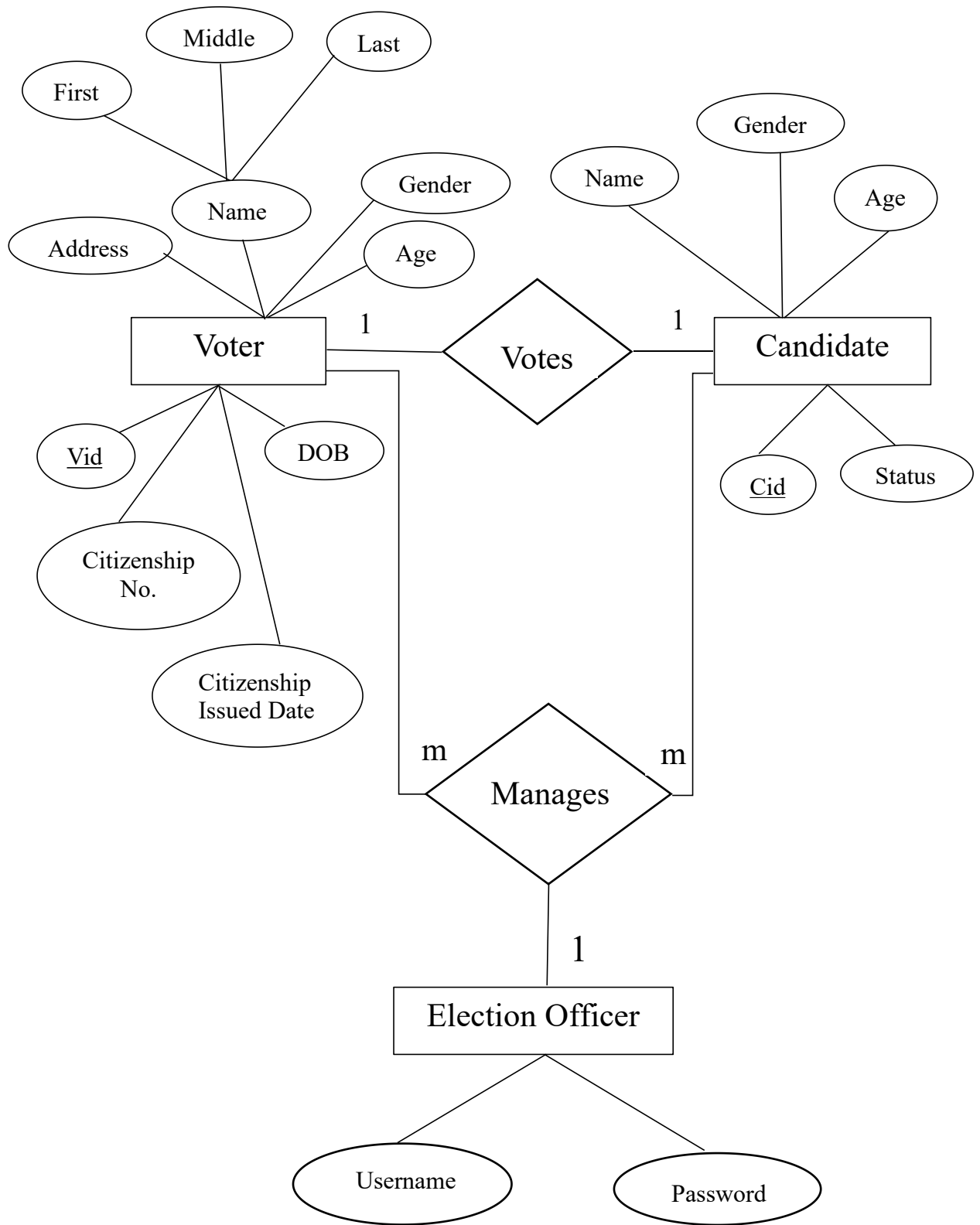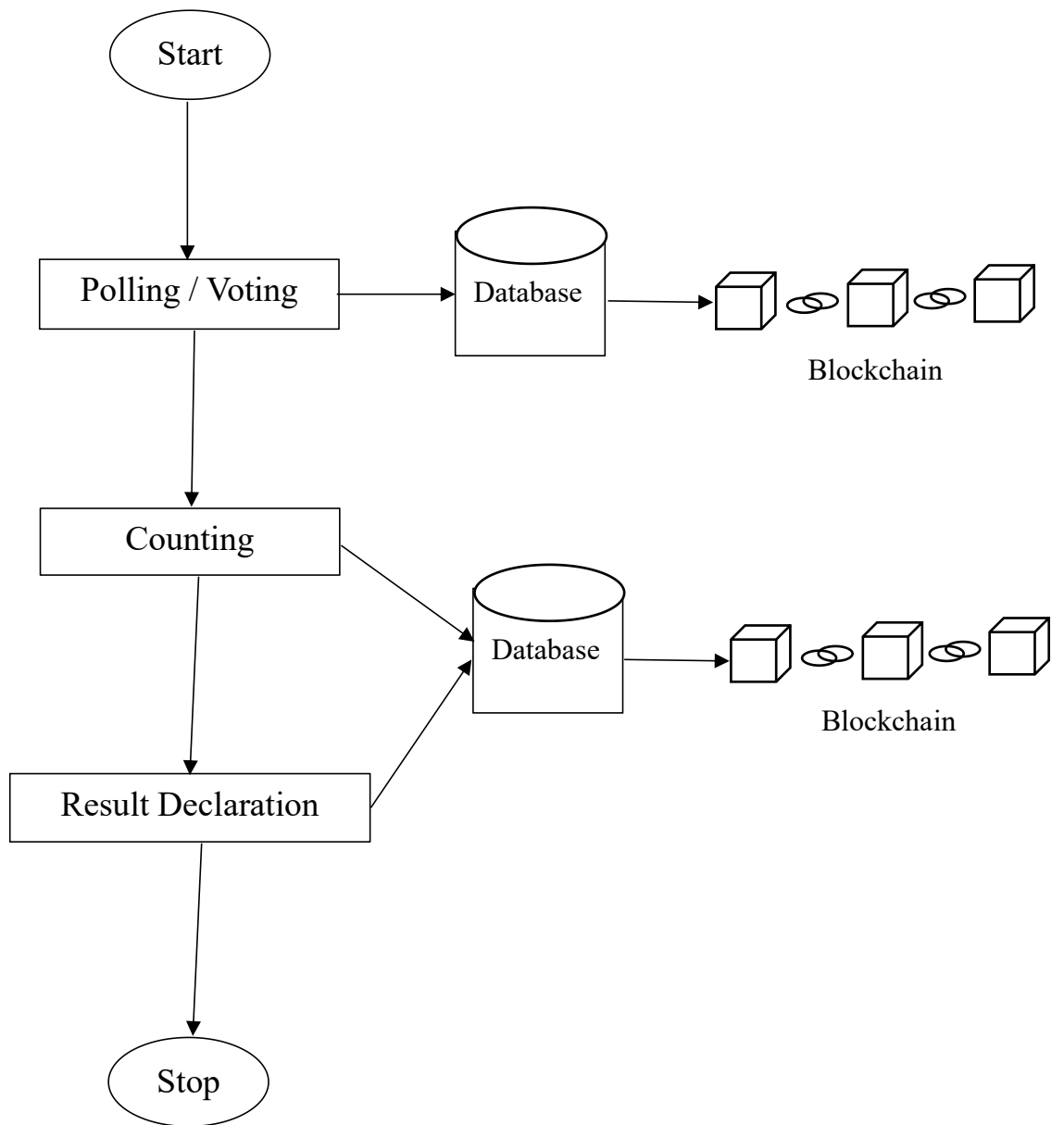
Fig-3 : ER Diagram of e-Chunab
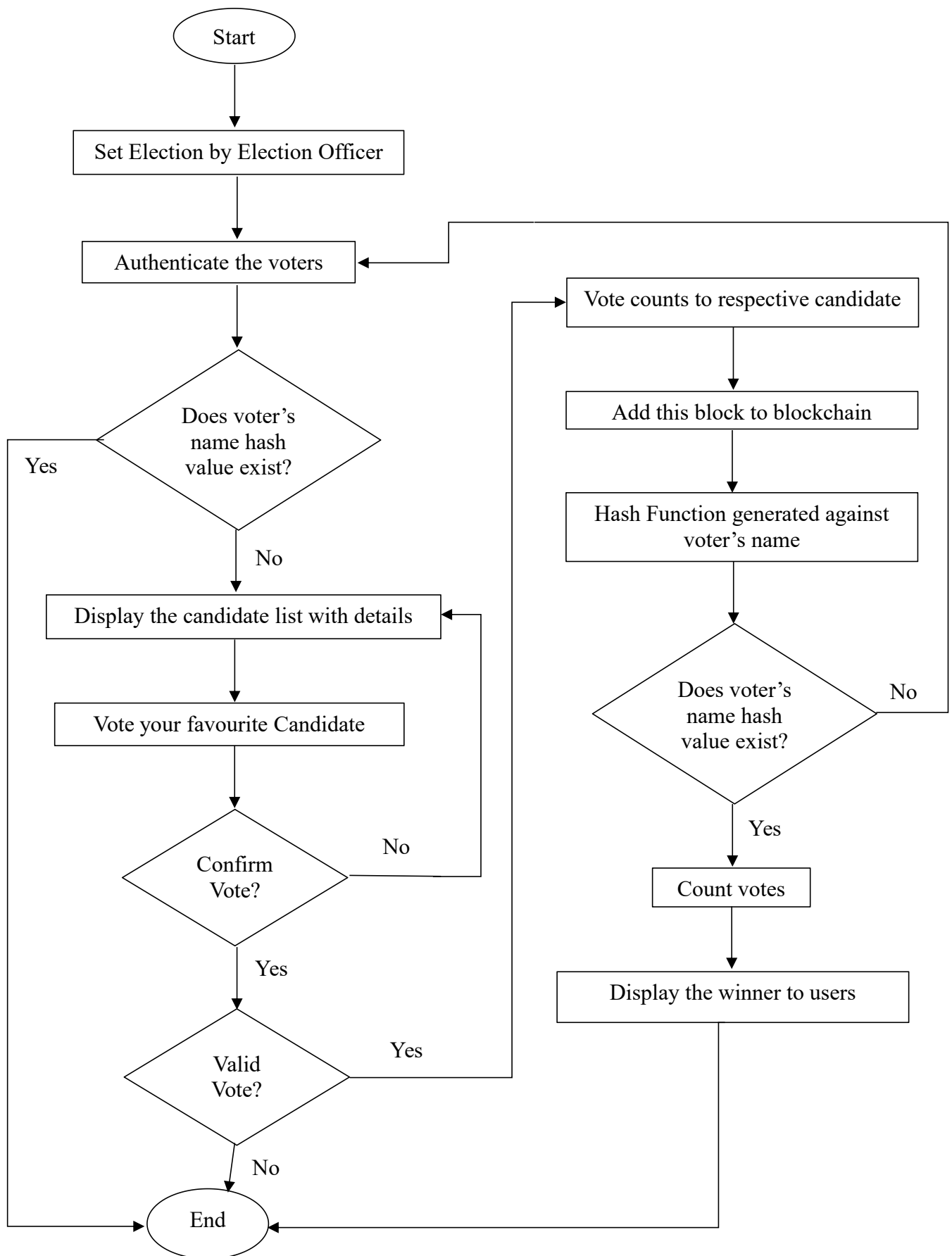
Fig-4 :- Flow chart for e-Chunab
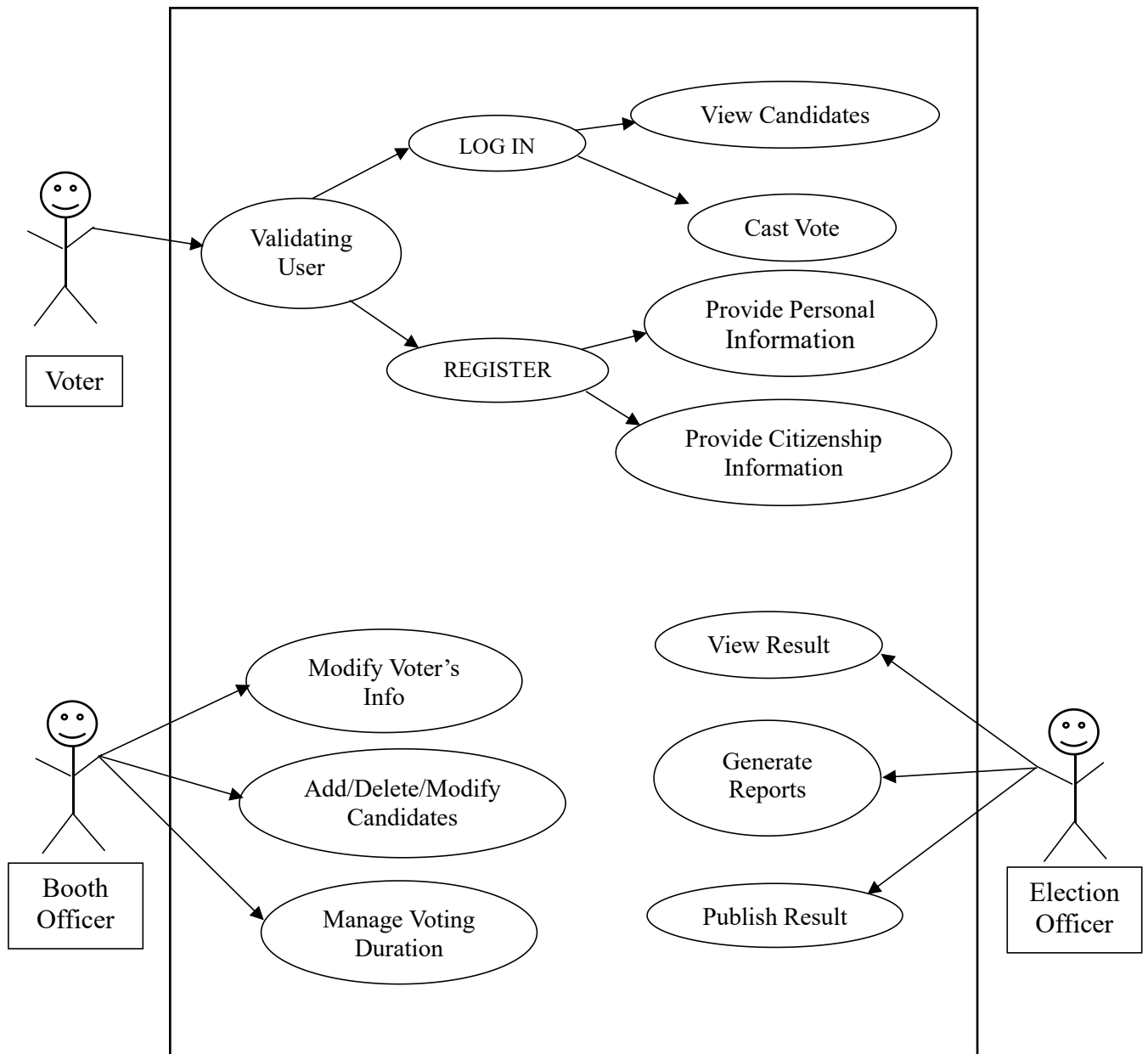
Fig-5 : Use-case Diagram

Fig-6 : e-chunab polling and counting process

Activity	June 30	July 5	July 15	July 25	Aug 4	Aug 14	Aug 24	Sept 3
Proposal	▇							
Research		▇						
Requirement Analysis			▇					
Designing				▇				
Development					▇			
Testing						▇		
Maintenance							▇	
Documentation								▇

	Proposal	Research	Requirement Analysis	Designing	Development	Testing	Maintenance	Documentation
Begin Date	June 27	July 2	July 6	July 13	July 20	Aug 4	Aug 10	Aug 17
▇ Duration	5 days	4 days	7 days	11 days	14days	6 days	8 days	5days

Fig-7 : Gantt Chart

7. Expected Outcome & Conclusion

This project is aimed at simplifying 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 on 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 can solve the problem of voting process and reach out to many who are capable to vote.

REFERENCES

[1] http://blockgeeks.com/guides/what-is-blockchain-technology/

[2] https://www.trufflesuite.com/docs/ganache/overview

[3] https://docs.metamask.io/guide/#account-management

[4] https://www.investopedia.com/articles/investing/031416/bitcoin-vs-ethereum-driven-different-purposes.asp

[5] Ahmed Ben Ayed, "A Conceptual Secure Blockchain based Electronic Voting System", IJNSA, Vol.9, No.3, May 2017.

[6]https://www.researchgate.net/publication/311444386_Fraud_detection_for_online_businesses_a_perspective_from_blockchain_technologylo

[7] https://en.wikipedia.org/wiki/Feasibility_study