EasyChair Preprint

№ 7158

Decentralized Blockchain Voting System

Prashant Singh and Priyadarshi Shakya

December 6, 2021

Decentralized Blockchain voting system

Prashant Singh
B.Tech SCSE
Galgotias University,
Noida, India

prashant_singh.scsebtech
@galgotiasuniversity.edu.in

Priyadarshi Shakya
B.Tech SCSE
Galgotias University,
Greater-Noida, India

shakyapriyadorshi@gmail.
com

Abstract— Voting is the fundamental right for every nation. An Electronic Voting (E-Voting) system is a voting system in which the election process is notated, saved, stored, and processed digitally, which makes the voting management task better than the traditional paper-based method. Blockchain is offering new opportunities to develop new types of digital services. In this project, the concept of developing an electronic voting system using blockchain technology is implemented. The two-level architecture provides a secure voting process without redundancy of existing (not based on blockchain) systems. The blockchain-based voting project has two modules to make the whole project integrated and work along. One will be the Election Commission who will be responsible for creating elections, adding registered parties and candidates contesting for the election added under the smart contracts. The other end will be the voter's module where everyone can cast a vote for their respective Assembly Constituency and the vote will be registered on the blockchain to make it tamper proof.

Keywords- Blockchain, E-voting, smart contracts

INTRODUCTION

Modern democracies are built upon traditional ballot or electronic voting (e-voting). In these recent years, devices which is known as EVMs are hugely criticized due to irregular reports of the election results. There have been many questions regarding the design and internal architecture of these devices and how it might be susceptible to attacks. This paper has analyzed different techniques of tampering the EVMs. Online-voting is pushed as a potential solution to attract the young citizens and the non-resident of the country. For a robust online election scheme, several functional and security requirements are to be met such as transparency, accuracy, auditability, data privacy, etc.

EASE OF USE:

The web application will be accessible through desktop or mobile to provide the user with ease of access. We aim to provide accurate data. Our aim is to alleviate some stress from the user who feels anxious about being uninformed about what might be happening without them. Our app also serves as a learning opportunity for the members along with a great incentive to help people.

Literature Reviews:

In this paper, it has highlighted about the major problem in voting security where in the 2016 US Presidential Elections, EVM's were likely to be intercepted and votes were tampered. The study found that this old voting equipment is not only more prone to failures and crashes but is also notoriously easy to hack and tamper with. In this study by Ayed, Ahmed, et al., it has been proposed an electronic voting system based on the Blockchain technology. The system is decentralized and does not rely on trust. Any registered voter will have the ability to vote using any device connected to the Internet.

The Blockchain will be publicly verifiable and distributed in a way that no one will be able to corrupt it. Rifa and Budi has concluded that if we use of hash values in recording the voting results of each polling station linked to each other makes this recording system more secure and the use of digital signatures makes the system more reliable. The use of the sequence proposed in the blockchain creation process in this system considers that in an electoral system not required for mining as in the Bitcoin system because the voter data and numbers are clear and are not allowed to select more than once, the proposed sequence ensures that all nodes Which is legally connected and can avoid collision in transportation. Bin, Joseph, et al., has conclude that the current blockchain voting system cannot provide the comprehensive security features, and most of them are platform dependent, we have proposed a blockchain based voting system that the voters' privacy and voting correctness are guaranteed by homomorphic encryption, linkable ring signature, and PoKs between the voter and Blockchain.

Problem Formulation:

Identifying potential problems before the start of a project can save the organization significant amounts of time and money. Problem analysis is one of the most critical stages of project planning because this stage helps to guide all subsequent analysis and decision-making. If the project does not advance past this stage with solutions that the organization can implement, the project should not go forward in its current form.

Required tools:

Major tools required for the development of the web application:

1. **React -** React (also known as React.js or ReactJS) is an open-source JavaScript library for building user interfaces or UI components. It is maintained by Facebook and a community of individual developers and companies. React can be used as a base in the development of single-page or mobile applications.

2. **Solidity** – It is used for implementing smart contracts on various blockchain platforms most notably Ethereum.

3. **MetaMask** – It is a software cryptocurrency wallet used to interact with the Ethereum blockchain. It allows users to access their Ethereum wallet through a browser extension or mobile app, which can then be used to interact with decentralized applications.

4. **Web3JS** – a collection of libraries that allow us to interact with a local or remote Ethereum node using HTTP, IPC or WebSocket.

Product Features:

1. Eligibility: This property states that only eligible users can vote. Those who are provided with authentication by the Election Commission.

2. Privacy: Privacy is one of the most important aspects of democratic voting. Voter's privacy should be maintained. No one should be able to know how a particular person voted or to whom the voter voted.

3. Coercion resistance: No one should be able to force the voter and should not have the ability to distinguish between whether the voter voted the same way he/she was instructed to vote.

4. Verifiability: This property states that everyone involved in the voting process should be able to verify the results. This brings transparency in the election. Also, an individual voter should be able to verify whether his/her vote is counted or not.

5. Immutability: The voter's vote should be immutable. No one should be able to change the vote of any voter without proper concern of the voter. All the records should be immutable.

Feasibility Analysis:

A 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 not to solve the problem, but to determine whether the problem is worth solving. It is a preliminary study which is conducted before the real development of the project commences not keeping the factor of project's success. It creates a roadmap of what are the possible solutions if we choose a certain path. Evaluating the technical feasibility study is the trickiest part of a feasibility study. This is because now, not too many detailed designs of the system, making it difficult to access issues like performance, costs on etc. Several issues must be considered while doing a technical analysis. Understand the different technologies involved in the proposed system before commencing the project we must be very clear about what are the technologies that are to be required for the development of the new system. Overall, this study needs to demonstrate that the proposed system which needs to be developed is technically feasible.

Figures and Tables:

Sequence Diagram:

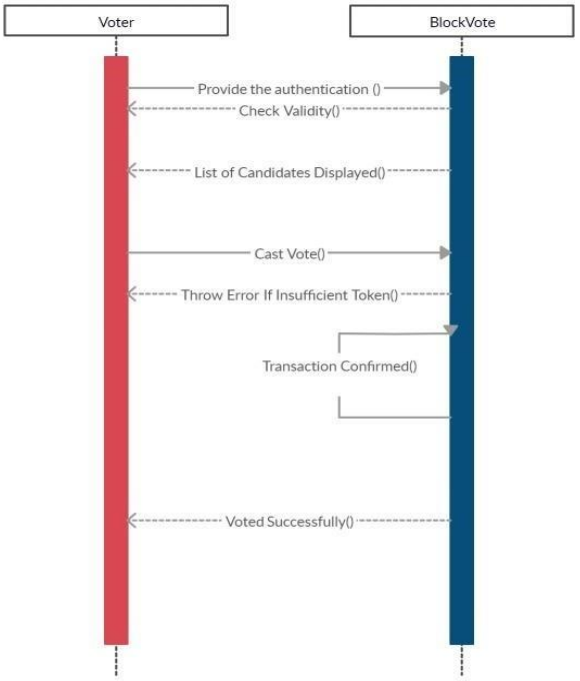
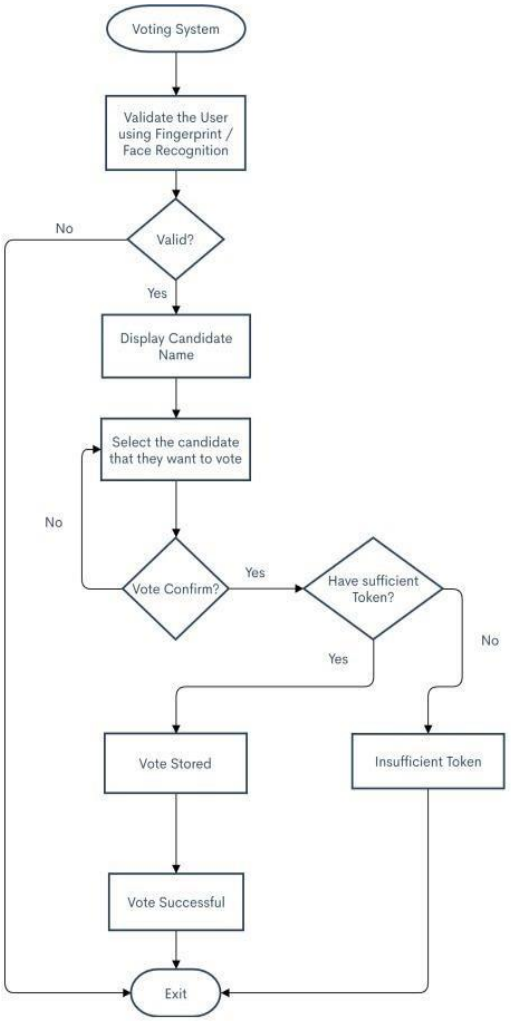


Figure 2: Sequence Diagram

Flow-chart:



ACKNOWLEDGMENT

We would like to thank our guide, Ms. Heena Khera for his continual support and unwavering guidance. Furthermore, we would like to thank the numerous moderators for their feedback.

References:

1. Wolchok, Scott, et al. "Security analysis of India's electronic voting machines." Proceedings of the 17th ACM conference on Computer and communications security.ACM,2010.
2. Ohlin, Jens David. "Did Russian cyber interference in the 2016 election violate international law." Tex. L. Rev. 95 (2016): 1579.
3. Ayed, Ahmed Ben. "A conceptual secure blockchain-based electronic voting system." International Journal of Network Security & Its Applications 9.3 (2017): 01-09.
4. Hanifatunnisa, Rifa, and Budi Rahardjo. "Blockchain based e-voting recording system design." 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA). IEEE, 2017.
5. Yu, Bin, et al. "Platform-independent secure blockchain-based voting system." International Conference on Information Security. Springer, Cham, 2018