Table of Contents

ABSTRACT

An electoral system or voting system is a set of rules that determine how elections and referendums are conducted and how their results are determined. Political electoral systems are organized by governments. Current voting systems like ballot box voting or electronic voting suffer from various security threats such as DDoS attacks, polling booth capturing, vote alteration and manipulation, malware attacks, etc, and also require huge amounts of paperwork, human resources, and time. This creates a sense of distrust among existing systems. The microchip or server can be hacked. Blockchain voting, if implemented properly, can boost voter turnout and offer more accessible and transparent elections. Citizens can easily cast their votes via their personal computers or mobile phones after completing identity verification. Voting records are easily verifiable and vote tallying is conveniently confirmed in real-time on the network. Blockchain voting saves time, reduces costs, and paves a path for direct democracy. However, blockchain voting is not yet ready. Where the User can cast vote using their personal devices. While using blockchain technology it prevents from DDoS attack and any other malware. It uses peer to peer network so no centralized authority.

LIST OF FIGURES

LIST OF ABBREVIATIONS

Abbreviation	Meaning
UI	User Interface
DDoS	Distributed Denial-of-Service
P-to-P	Peer to Peer
EC	Election Commission
ECA	Electoral Count Act
ESS	Election Systems & Software
CV	Curriculum Vitae
LCD	Liquid Crystal Display
UML	Unified Modeling Language
GUI	Graphical User Interface

1. INTRODUCTION

1.1 Overview

Electronic voting systems have been the subject of active research for decades, with the goal to minimize the cost of running an election, while ensuring the election integrity by fulfilling the security, privacy and compliance requirements. Replacing the traditional pen and paper scheme with a new election system has the potential to limit fraud while making the voting process traceable and verifiable

1.2 Problem statement

To create a system that caters the problem of current voting system like ballot box voting or electronic voting which suffer from various security threats such as DDoS attacks, polling booth capturing, vote alteration and manipulation, malware attacks, etc. and also require huge amounts of paper work, human resources, and time spent during voting in long queues.

1.2.1 List of problems

1. Long Queues during elections
2. Security Breaches like data leaks, vote tampering.
3. Lot of paperwork involved, hence less eco-friendly and time consuming.
4. Difficult for differently-abled voters to reach polling booth.

1.3 Scope

The connection to the blockchain provides a means of anonymity while at the same time, providing transparency of the elections. Deployment of a smart contract also enables all changes being made to the contract to be visible by all parties involved on the blockchain.

1.4 Proposal

The above problems can be overcome by online-voting using blockchain technology. Where the User can cast vote using their personal devices. While using blockchain technology it prevents from DDoS attack and any other malware. It uses P-to-P network

1.5 Aim and Objectives

The main objective of this project is: To create a voting system sitting on the Ethereum blockchain where every vote is like a token and there are a set number of tokens in circulation based on the number of voters and the candidates with such accountability and transparency are achieved.

1. To limit voting fraud.
2. To avoid long queuing to cast votes.
3. To minimize the cost of elections.
4. To enable voters to vote in the comfort of their home, or worldwide.
5. To be able to verify if a vote has been counted.
6. To maintain transparency and anonymity in elections

1.6 Significance

The Significance of this project is to help:

1. In a voting process whereby every vote is uploaded and can be seen in the blockchain represented on a smart contract and anonymity is preserved and transparency is achieved.
2. To build a voting system that is safe enough to use in the comfort of our homes.
3. To make sure votes aren't manipulated by any parties involved in the election.

1.7 Project Beneficiaries

The beneficiaries of this project are the users of the application. They may range from students engaging in elections to employees in a workplace taking part in elections, or even citizens engaging in national elections.

2. LITERATURE SURVEY

S.No.	Source (2023)	Title of Research paper	Methodology	Key Findings	Limitations
[1]	P. Rajendra Prasad and R. Z. Ahmed (IEEE)	Secured E-Voting System Implementation Using Block-Chain Network	Content Analysis	The proposed blockchain-based e-voting system is secure, transparent, and tamper-proof.	The system still needs to be developed further to make it more user-friendly
[2]	S. Khedkar, K. Mahajan and M. Shirole (ICBIR)	Optimization of Blockchain Based E-voting	Method Optimisation	The system is capable of handling a large number of votes without compromising security.	The system needs to be tested on a large scale to ensure that it is scalable.
[3]	A. Balti, A. Prabhu, S. Shahi, et.al (ICSCSS)	A Decentralized and Immutable E-Voting System using Blockchain	Research and familiarisation	The system is more resistant to attack than traditional e-voting systems.	The system needs to be further analysed to address the security risks.
[4]	S. Goswami, R. Pandey, S. Nagar, et.al (ICSCCC)	Blockchain based voting system - A Review	Review existing system	The system can be automated using smart contracts, which reduces the risk of human error.	There are likely to be bugs and security vulnerabilities
[5]	S. N, G. S, S. E and V. K (ICAECA)	E - Voting Using Blockchain	Feature extraction	The use of encryption to secure the ledger. This ensures that only authorized voters can view their own votes.	The system requires a high level of technical literacy from voters.

S.No.	Source (2023)	Title of Research paper	Methodology	Key Findings	Limitations
[6]	P. Kadam, P. Nikam, H. Raut, et.al (CONIT)	Blockchain Based e-Voting System	Cost and comparison of proposed system	The system can be used to vote on a variety of issues, not just elections.	The cost of setting up and maintaining a blockchain-based e-voting system can be high.
[7]	Y. Li, Y. Li, T. Hong, et.al (IEEE)	Design and Implementation of Blockchain-based Anonymous Electronic Voting System	Methodology to keep person's Identity secret	The system can be used to vote anonymously, which protects voter privacy. This could encourage more people to vote.	The system can be complex to set up and use, which can be a barrier to adoption.
[8]	S. B. Gopal, M. Jayaprasath, C. Poongodi, et.al (ICSCDS)	Blockchain based E-Voting Application – A Survey	Survey on existing technology	The system can be used to audit the results of an election, which makes it more transparent and accountable.	The system may not be accessible to everyone, such as people who do not have access to the internet or computers.
[9]	Y. A. F. Ali, O. T. M. Ahmed, M. A. M. Diab, et.al (ICSCA)	Blockchain-Based Online E-voting System	Mixed methods	The system can be used to track the voting process, which makes it more secure and reliable.	The system can be vulnerable to security risks, such as hacking and data breaches.
[10]	A. Raizada and B. Sharma (AISC)	Reliable Block chain-Based Digital System of Voting	Analysis of system	The system can be used to educate voters about the voting process	The system may need to be regulated by governments which cost more than usual.

3. System Workflow

3.1 Overview

Project methodology (also known as a system development methodology, software development life cycle, software development process, software process) is widely known as splitting of software development work into distinct phases (or stages) containing activities with the intent of proper planning and management. It is mostly considered a subset of the systems development cycle.

Since this is a basic system the information required was obtain from observing truffle and other Ethereum resources.

Common methodologies include the waterfall model, prototyping, spiral model sequential model. Many projects have considered a life-cycle "model", a more general term for a category of methodologies and a software development "process" a more straight to the point term to refer to a specific process chosen by an individual organization.
There are many methodologies that could have been used to develop this project. For the successful development of this project however, an appropriate design methodology had to be used. I therefore decided to use the waterfall model as my development methodology. A brief description of the Waterfall model is given in the next sub-heading.

3.2 Waterfall Model

The waterfall model (Illustrated below) was the first published model of the software development process derived from the engineering processes .The term waterfall model was used due to the cascaded nature of one phase of the model relative to other phases

The model has been broken down into phases or stages and these stages map onto the fundamental development activities.

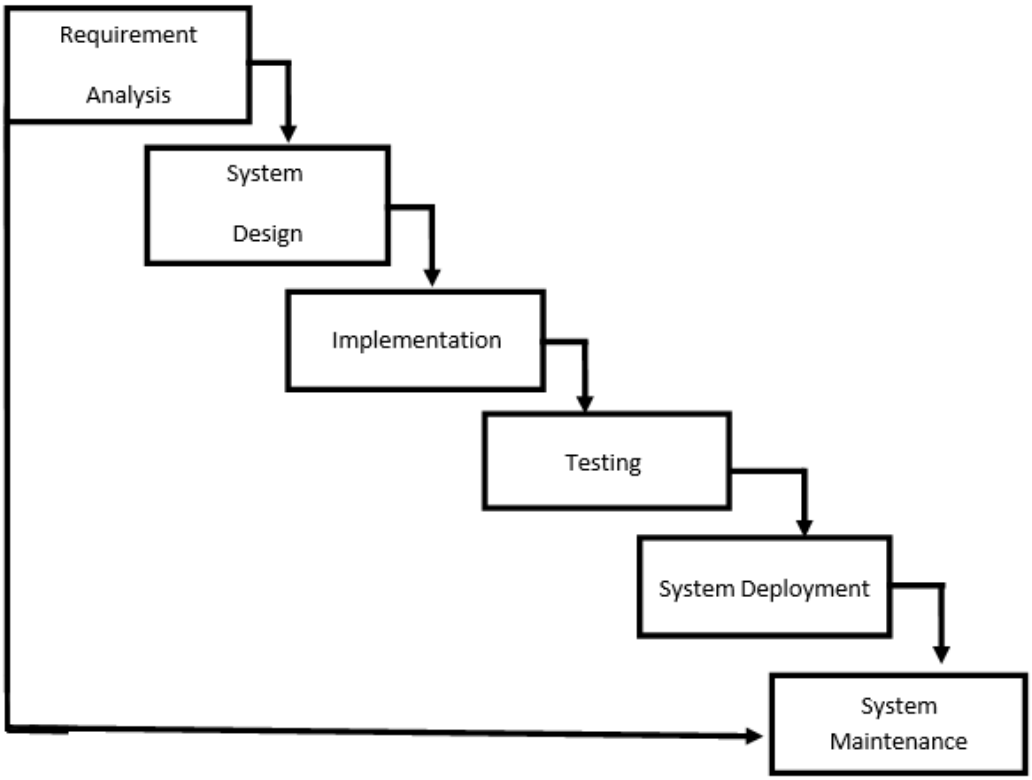

Fig. 3.1 Waterfall model

3.2.1 Requirement Specifications

3.2.1.1 Functional Requirements

Functional requirements are the requirements of the system that describe the functionalities or services that the system is expected to provide to the users come what may. The system shall provide the following functionalities to users when they have not yet save any preferences:

1. The system should be able to reflect changes in the web page for users to view.
2. The system should be able to change the state of the blockchain.
3. The system should provide a user friendly interface for users to interact with easily.
4. The system should have mechanism that tallies entries.
5. The system should display accurate voting results based on the smart contract.

3.2.1.1.1 Normal Interactive Mode

1 Voter Registration

In order to use the system the voters must register to system.

This system will be used only by the people who have been registered to the system. Main actor of the registration operator is the voter. The registration operator is approved by the ECAs. The system shall allow online voter registration.

2 Approve Applicant

By using this function, ESS approves the application sent by the voters in order to use the E Voting. Without the approval of ESS the voters can't use their account or elect. The main actor is the ESS. The system shall allow ESS to approve the voters.

3 Delete Voters

ESS deletes voters from the system who cannot use their vote officially. The main actor is the ESS. The system shall allow ESS to delete account if the voter is not legal.

4 Open Candidate Account

The EC's profile must be created by the ECA. This functionality helps to perform this action. The ECA is the main actor of this functionality. The system shall allow ECA to create EC account.

5 Login/Logout

All of the system users login to system by their email or phone and passwords. All of the users are the main actor of functionality. The system will allow users to login and logout.

By using this function all the user may change their password that enters the system.

The system shall allow the entire user to change their password.

6 View EC Information

This function allows the voters to reach information about the EC such as their CVs, promises etc. The system shall allow voters to check ECs profile.

7 Ask To Candidate

By using this functionality the voters can direct questions to the Ecs about their election campaigns. The system shall allow the user to interact with Ecs.

8 CV Edit

This function provides the EC to edit his CV information on his own profile.

The system shall allow EC to update CV.

9 Add / Edit Promises

By using that function the EC's may add or edit promises to their own profile.

The system shall allow EC to add or edit promises.

10 Read/Answer Question

This function provides Ecs to read or answer questions about their election campaigns.

The system shall allow EC to read and answer a voter question.

11 View Election Result

This functionality provides voters to see the current or past years' election result in a proper way. The main actor is the voter.

12 Notification

This function provides notification to the user of the system to know what is going on and results of the election and days left.

The system shall provide the notification for the system user.

3.2.1.1.2 Election Mode

1 Open System

This function provides ECA to start the system during the Election Day or before. The ECA can control the hall system like changing normal interface to election mode.

The system shall allow ECA to turn system to election mode.

2 Online Vote

This is the main function of the system that provides online voting for the general public.

At the Election Day the voter only use the online voting function.

The system shall allow voters to vote at Election Day only.

3 Enter Offline Votes

By using this function the ESSs enters the offline votes to the system. The system shall allow ESS to enter offline votes.

4 View result

At the end of the day the system announces the station results, city result, worked result, zone result, and region results.

The system shall provide results for the user to see results.

3.2.1.2 Non-Functional Requirements

Non-functional requirements are requirements that does not directly concern the functions performed by the application.

The non-functional requirements include:

1 Speed: The values and the state are within the blockchain and do not need to be externally retrieved to the page, this enhances speed.

2 User Friendly: The system is designed in a user friendly interface.

3 Robustness: The system is built in such a way that no one can inject any unwanted data or impose any threat on the system.

4 Availability: the project is an online hence it shall be available to users as long as they are internet enabled

5 Performance: The system shall respond to the user in not less than two seconds from the time of the request submittal

6 Accuracy: The system shall produce accurate results from the data captured into the system.

3.2.2 Architectural Review

The architecture of the system fits the functionality and aids in the ease of use of the user interface.

3.2.3 Technology Review

These include the programming languages and tools used to develop the software. The following below are the tools used in the designing the application:

3.3 Hardware Requirements

1. i3 Processor Based Computer
2. 8 GB RAM
3. 20 GB Hard Disk
4. LCD display
5. Internet Connection

3.4 Software Requirements

1. Remix IDE
2. Ganache
3. Solidity

3.5 Use Case Diagram

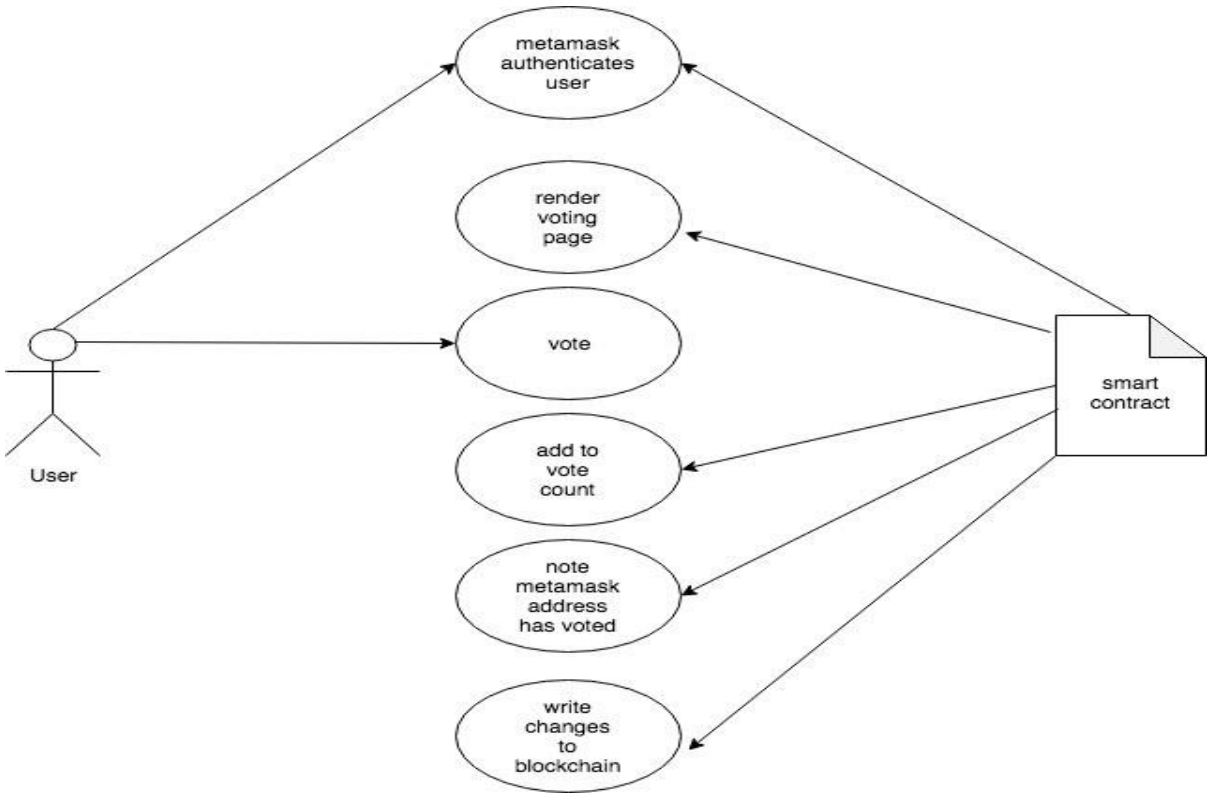

Fig. 3.2 Use Case Diagram

In a use case diagram for a blockchain-based voting system, we outline the essential interactions and functionalities of the system from the perspective of different actors involved. These actors typically include Voters, Administrators, and the Blockchain Network itself. Each actor has specific roles and interactions within the system.

This use case diagram provides a visual representation of how various actors interact with the blockchain-based voting system and the specific actions they can perform.

3.6 Activity Diagram

Activity diagram is defined as a UML diagram that focuses on the execution and flow of the behaviour of a system instead of implementation. It is also called object-oriented flowchart.

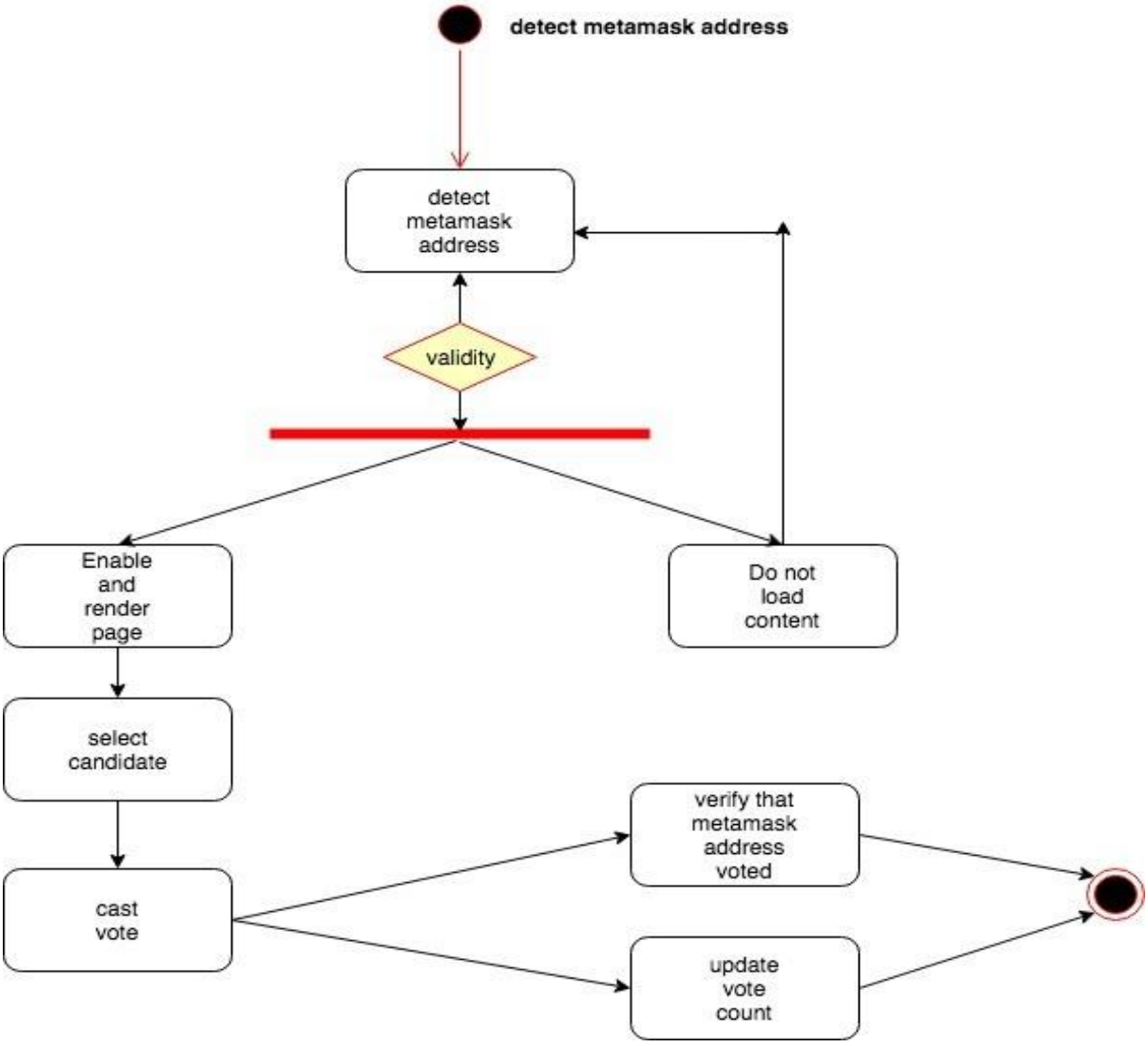

Fig. 3.3 Activity Diagram

3.7 System Architecture

A system architecture diagram would be used to show the relationship between different components. Usually they are created for systems which include hardware and software and these are represented in the diagram to show the interaction between them.

The voting system utilizing blockchain technology is designed with a robust and secure architecture to ensure the integrity and transparency of the electoral process. At its core, the system leverages a decentralized network of nodes, each running a blockchain protocol, which stores and validates every vote cast in the election. These nodes are distributed across a wide geographic area, reducing the risk of a single point of failure and enhancing resilience against attacks.

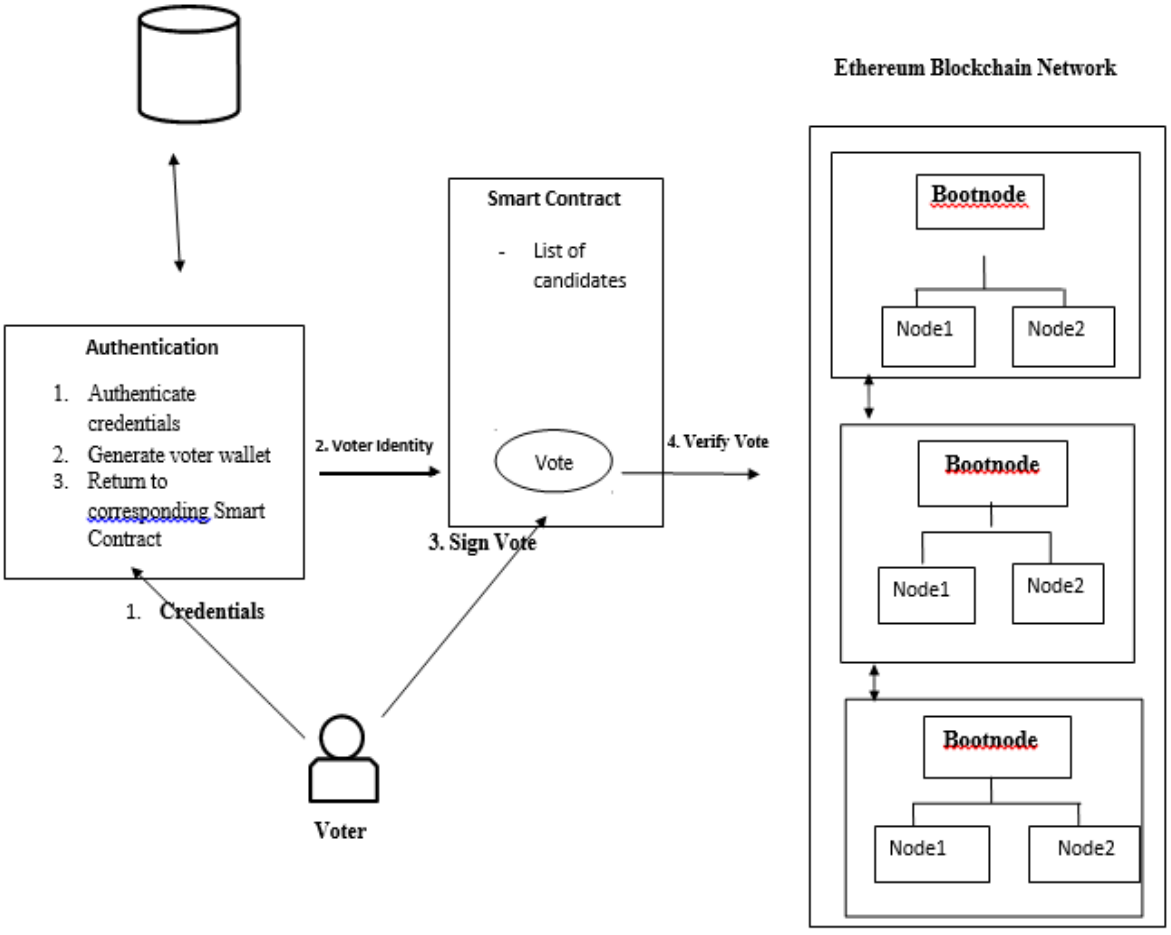

Fig. 3.4 System Architecture

3.8 Process view

In this view we try to describe the flow of activities which are mainly can be done by this System the process view of a blockchain-based voting system provides real-time access to election data, allowing for immediate result calculations without the need for intermediaries.

Through a user-friendly interface, voters can securely cast their ballots remotely, reducing geographical barriers and enhancing accessibility. This digitalization of the voting process not only expedites the election process but also enables advanced features like end-to-end verifiable voting and the elimination of fraudulent votes. By leveraging blockchain technology, the process view of voting systems offers the potential to revolutionize the democratic process, making it more inclusive, secure, and transparent for citizens around the world

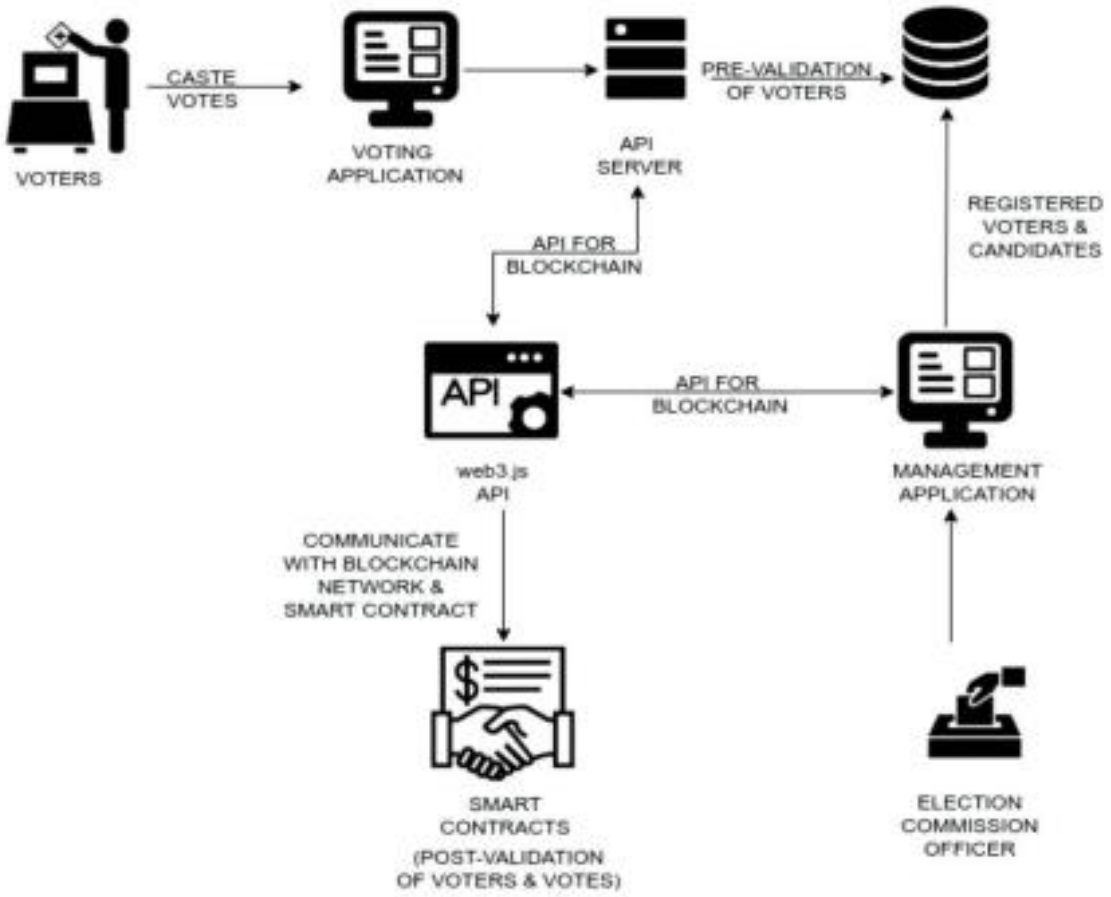

Fig. 3.5 Process view

Each vote is recorded as a tamper-resistant transaction on a decentralized blockchain ledger. This process view ensures that every cast ballot is encrypted and time-stamped, creating an immutable and publicly accessible record of all votes. Voters can verify their own transactions, ensuring their choices are accurately recorded.

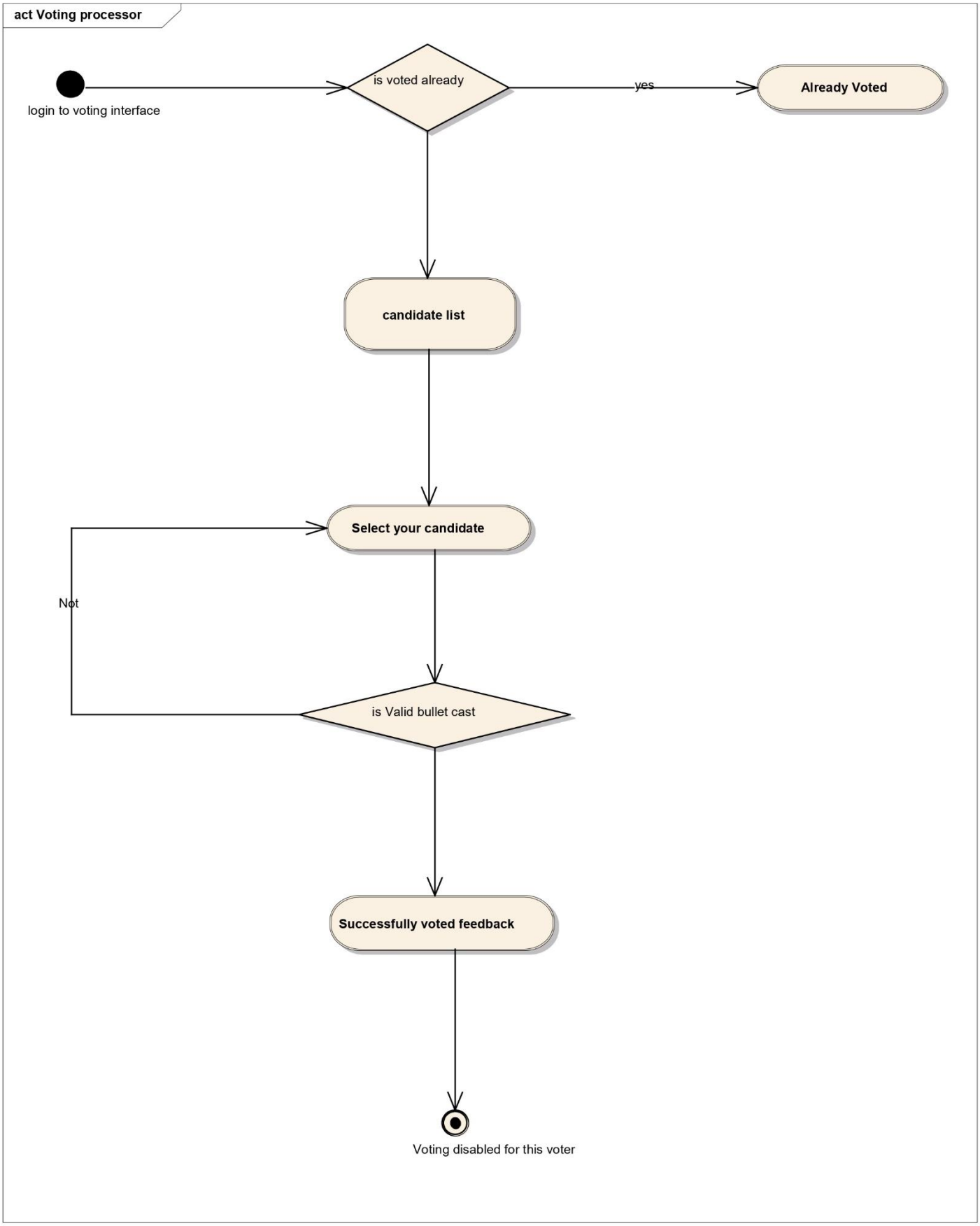

Fig. 3.6 Activity diagram for model package

3.9 User Interface

User Interface Design is concerned with how users communicate with the system. User Interface Design focuses on anticipating what users might need to do and ensuring that the interfaces has elements that are easy to access, understand, and use to facilitate those actions.

The system must provide a user interface for all types of users (ECA, ESS, EC, and Voter) that are available through all Web browsers and the Android application interface is only for voters.
The user interface for voter must be different for Election Mode and Normal Interactive Mode.
The proposed system has two sides the website and the mobile application

1. the website
2. the GUI of the website must be responsive in order to have ease of access while accessing remotely
3. the website shall have attractive and easily manageable interface after login
4. the website shall reload and kill session in each 3 minutes interval while no action is performed
5. the website shall protect any wrong entry of the user
6. the website shall interact with the server as fast as possible
7. the mobile app shall have an icon which is related to the system
8. the mobile app shall be actively interact with the server

Fig. 3.7 UI of the System

4. PROPOSED ALGORITHM

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract VotingSystem {
    address private owner;

    struct Candidate {
        string name;
        uint256 voteCount;
    }

    mapping(address => bool) private hasVoted;
    mapping(address => Candidate) private candidates;

    constructor() {
        owner = msg.sender;
    }

    function addCandidate(string memory _name, address
     _candidateAddress) public  {
        require(msg.sender == owner, "Only the owner can
           perform this action.");
        candidates[_candidateAddress] = Candidate(_name, 0);
    }
    function vote(address _candidateAddress) public  {
        require(!hasVoted[msg.sender], "You have already
           voted.");
        hasVoted[msg.sender] = true;
        candidates[_candidateAddress].voteCount++;
    }
    function getData(address _candidateAddress)  public view
        returns(string memory,uint){
        require(msg.sender == owner, "Only the owner can
           perform this action.");
        return(candidates[_candidateAddress].name,
               candidates[_candidateAddress].voteCount);
    }
}
```

5. RESULTS AND DISCUSSION

5.1 Efficiency of the Proposed System

Blockchain voting, if implemented properly, can boost voter turnout and offer more accessible and transparent elections. Citizens can easily cast their votes via their personal computers or mobile phones after completing identity verification. Voting records are easily verifiable and vote tallying is conveniently confirmed in real-time on the network. Blockchain voting saves time, reduces costs, and paves a path for direct democracy.

However, blockchain voting is not yet ready. Votes cast via a blockchain-based voting system are not entirely anonymous, as voters can show proof of how they voted through the transaction data. This type of voting system is also vulnerable to denial-of-service attacks that delay voters from submitting their votes on time.

The blockchain technology underpinning this platform allows voters to verify that their votes are counted, and that the votes are recorded correctly without compromising their own anonymity allow independent vote-monitoring bodies to audit the vote counting and codes used to make sure that the system is free from fraud.

A 51% attack is a potential threat to our proposed design. The basis of the attack being that someone could theoretically control a majority of the digital voting mining hash-rate, leading to them being able to manipulate the public ledger. The chances of this type of attack occurring are slim due to the immense cost needed to purchase hardware capable of this scale of processing.

5.2 Comparison of Existing and Proposed System

Currently available blockchain-based voting systems have scalability issues. These systems can be used on a small scale. Still, their systems are not efficient for the national level to handle millions of transactions because they use current blockchain frameworks such as Bitcoin, Ethereum, Hyper ledger Fabric, etc. The scalability issue arises with blockchain value suggestions; therefore, altering blockchain settings cannot be easily increased.

6. CONCLUSION

The current voting system can be improvised and secured by applying a web based voting solution. Blockchain technology has potential to be implemented in a far more secure and accessible voting system. The proposed blockchain-based e-voting system manages the election process, which makes the voting process simpler, voters can just simply login and exercise their right to vote. We believe that blockchain based voting systems can replace the traditional voting system in future. With the risks of terrible poor key management and the possibility of serious failures, blockchain voting still has a long way to go before large-scale application. Further to this we also need to ensure they are not forced to vote in a particular way so we have incorporated a double-check service where by users shall be prompted a second time to confirm their submission before the vote is sent; this also then allows us to almost eradicate accidental votes. Our service proposal comprises of a geographically distributed network comprising of machines from both government and public infrastructure; this infrastructure houses two distinctly separate blockchain, one for voter information such as who has voted and the other for vote information such as what has been voted. These blockchain are held completely separately to remove any threat to link votes for certain parties back to individual voters while maintaining the ability to track who has voted and how many votes are actually present.

REFERENCES

[1] P. Rajendra Prasad and R. Z. Ahmed, "Secured E-Voting System Implementation Using Block-Chain Network," 2023 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), Bangalore, India, 2023, pp. 1-6, doi: 10.1109/CONECCT57959.2023.10234779.

[2] S. Khedkar, K. Mahajan and M. Shirole, "Optimization of Blockchain Based E-voting," 2023 8th International Conference on Business and Industrial Research (ICBIR), Bangkok, Thailand, 2023, pp. 700-705, doi: 10.1109/ICBIR57571.2023.10147663

[3] ABalti, A. Prabhu, S. Shahi, et.al, "A Decentralized and Immutable E-Voting System using Blockchain," 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), Coimbatore, India, 2023, pp.1434-1439, doi:10.1109/ICSCSS57650.2023.10169552

[4] S. Goswami, R. Pandey, S. Nagar, et.al, "Blockchain based voting system - A Review," 2023 Third International Conference on Secure Cyber Computing and Communication (ICSCCC), Jalandhar, India, 2023, pp. 433-438, doi: 10.1109/ICSCCC58608.2023.10176665.

[5] S. N, G. S, S. E and V. K, "E - Voting Using Blockchain," 2023 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), Coimbatore, India, 2023, pp. 1-4, doi: 10.1109/ICAECA56562.2023.10199732.

[6] P. Kadam, P. Nikam, H. Raut, et.al, "Blockchain Based e-Voting System," 2023 3rd International Conference on Intelligent Technologies (CONIT), Hugli, India, 2023, pp. 1-6, doi: 10.1109/CONIT59222.2023.10205939

[7] Y. Li, Y. Li, T. Hong, et.al, "Design and Implementation of Blockchain-based Anonymous Electronic Voting System," 2023 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), Beijing, China, 2023, pp. 1-6, doi: 10.1109/BMSB58369.2023.10211580

.

[8] S. B. Gopal, M. Jayaprasath, C. Poongodi, et.al, "Blockchain based E-Voting Application – A Survey," 2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 2023, pp. 1340-1347, doi: 10.1109/ICSCDS56580.2023.10104596

[9] Y. A. F. Ali, O. T. M. Ahmed, M. A. M. Diab, et.al, "Blockchain-Based Online E-voting System," 2023 International Conference on Smart Computing and Application (ICSCA), Hail, Saudi Arabia, 2023, pp. 1-8, doi: 10.1109/ICSCA57840.2023.10087767.

[10] A. Raizada and B. Sharma, "Reliable Block chain-Based Digital System of Voting," 2023 International Conference on Artificial Intelligence and Smart Communication (AISC), Greater Noida, India, 2023, pp. 378-382, doi: 10.1109/AISC56616.2023.10085374