Project Report

1. INTRODUCTION

Extensive research has been done on electronic voting systems that enable voters to vote at their convenience using a mobile phone, computer or any other electronic device. Still, none of these technologies have been incorporated on a larger scale due to inherent security threats/concerns that these systems might pose to the integrity of the voting process. In this paper, we discuss electronic voting system using blockchain , a secure and robust system that ensures anonymity of the voter, transparency, and robust functioning

1.1 Project Overview

1.2

The blockchain is a digital platform for digital assets. It consists of a continuously growing list of records known as blocks that are linked and secured using cryptography. Major usage of Blockchain has been in all cryptocurrency transactions, mainly Bitcoin . However, they are increasingly being used in a number of other applications because of their inherent resistance to modification to the transaction/block/whole distributed ledger - Blockchain.

1.3 Purpose

The primary purpose of electronic voting machines (EVMs) using cryptography is to enhance the security, integrity, and privacy of the voting process in elections.

Cryptography is used to ensure that each vote cast remains intact and unaltered throughout the entire voting and tabulation process. This helps prevent tampering or manipulation of votes.

2.LITERATURE SURVEY

A. Votereum: An Ethereum-based E-voting system : Linh Vo-Cao-Thuy, Khoi Cao-Minh, Chuong Dang-Le-Bao and Tuan A. Nguyen,2019,“Votereum: An Ethereum-based E-voting system”,University of Information Technology Vietnam National University HCMC, Vietnam, it 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

B. Online Voting: Voting System Using Blockchain: Vaibhav Anasune, Pradeep Choudhari,MadhuraKelapure and Pranali Shirke Prasad Halgaonkar,“Online Voting: Voting System Using B-chain”,2019,article gives a short review on various methodologies that are used in current voting. The paper will help to build a system that will face the present and upcoming challenges and will remove drawbacks from these previous architectures

.

C. Survey on Blockchain Based E-Voting Recording System Design: G Bhavan,i“Survey on Blockchain Based E-Voting Recording System Design”,2018,By adopting blockchain in the distribution of databases on e-voting systems can reduce one of the cheating sources of database manipulation. For encrypting data fetched from fingerprint sensor we are going to use AES algorithm. This research discusses the recording of voting result using blockchain algorithm from every place of election

1.4 Existing problem

Electronic voting machines (EVMs) using cryptography have their share of challenges and potential issues, which can vary depending on the specific implementation and the regulatory environment.EVMs can still be susceptible to security vulnerabilities, including software bugs, hardware vulnerabilities, and potential cyberattacks. While cryptography can provide security, it is not foolproof, and weaknesses in the system can be exploited.

1.5 References

[1]Emre Yavuz ; Ali Kaan Koç ; Umut Can Çabuk ; Gökhan Dalkılıç (2018) Towards secure e-voting using ethereum blockchain

KC Tam ,(2018) ,Transactions in Ethereum

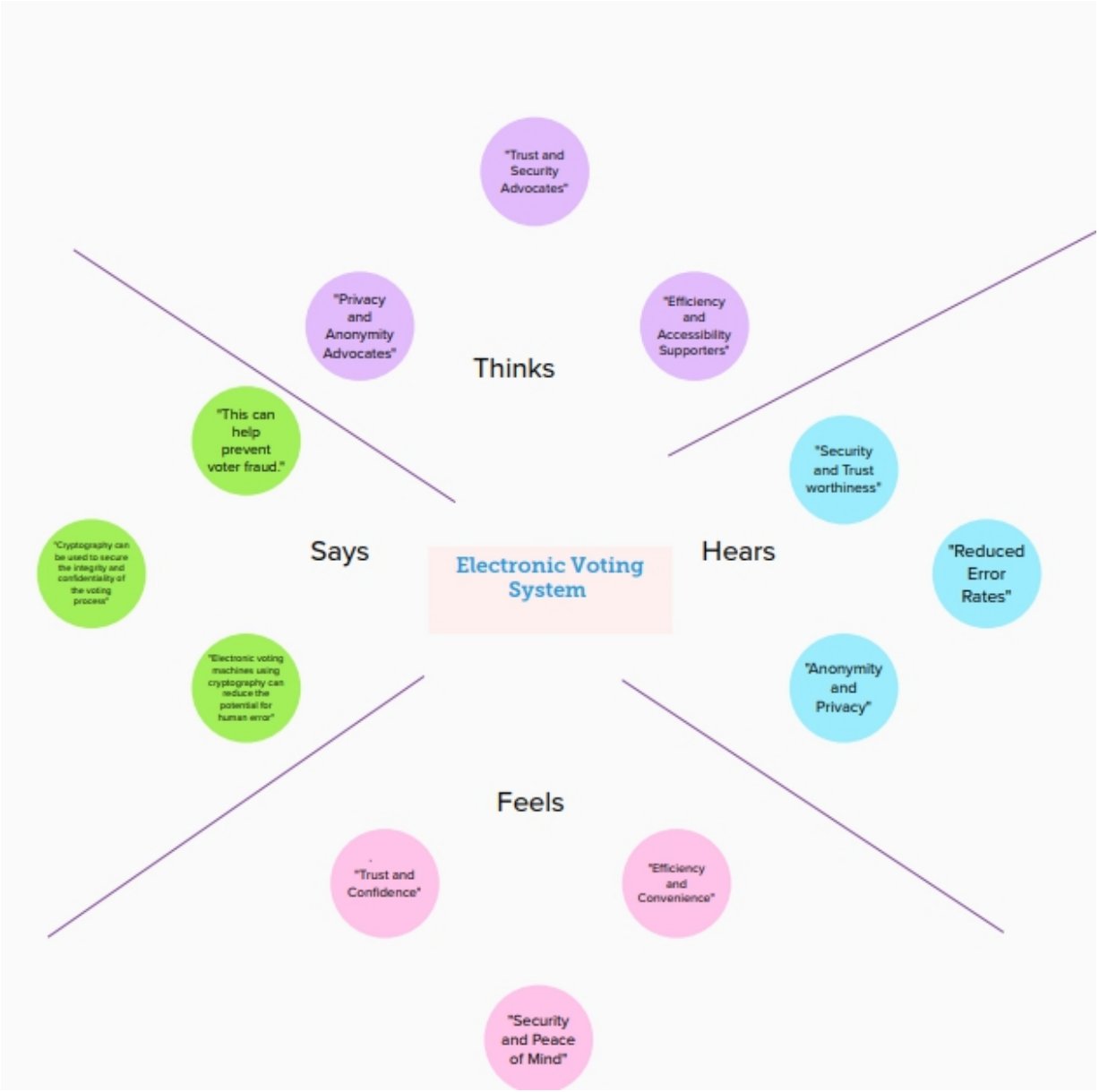
2.3Problem Statement Definition

The widespread adoption of electronic voting machines (EVMs) with cryptographic features in the electoral process faces a number of critical challenges that impact the security, integrity, and public trust in the voting system. Despite the potential benefits of using cryptography to enhance the electoral process, there are notable concerns and problems that need to be addressed

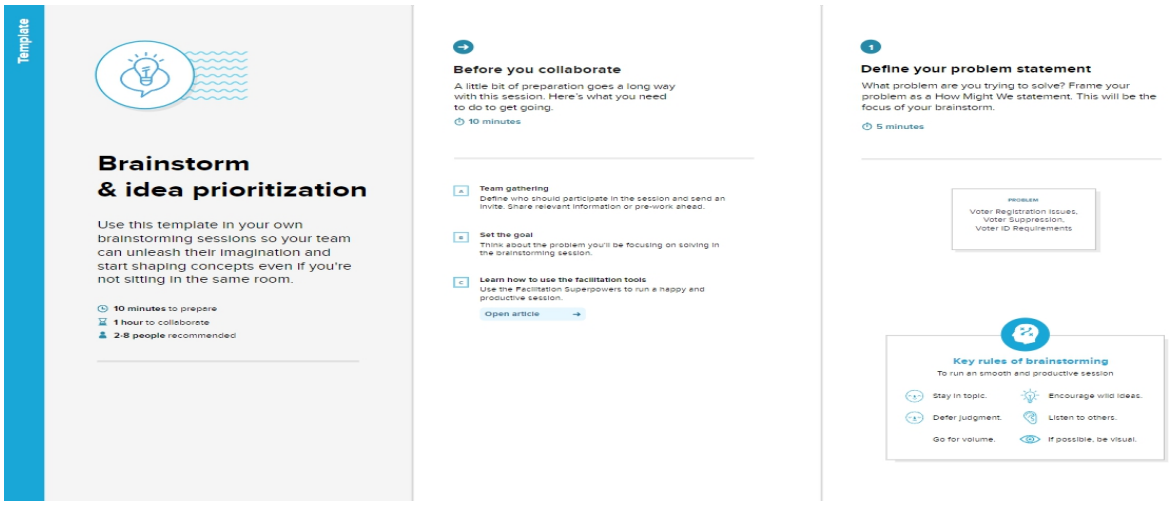
3.IDEATION & PROPOSED SOLUTION

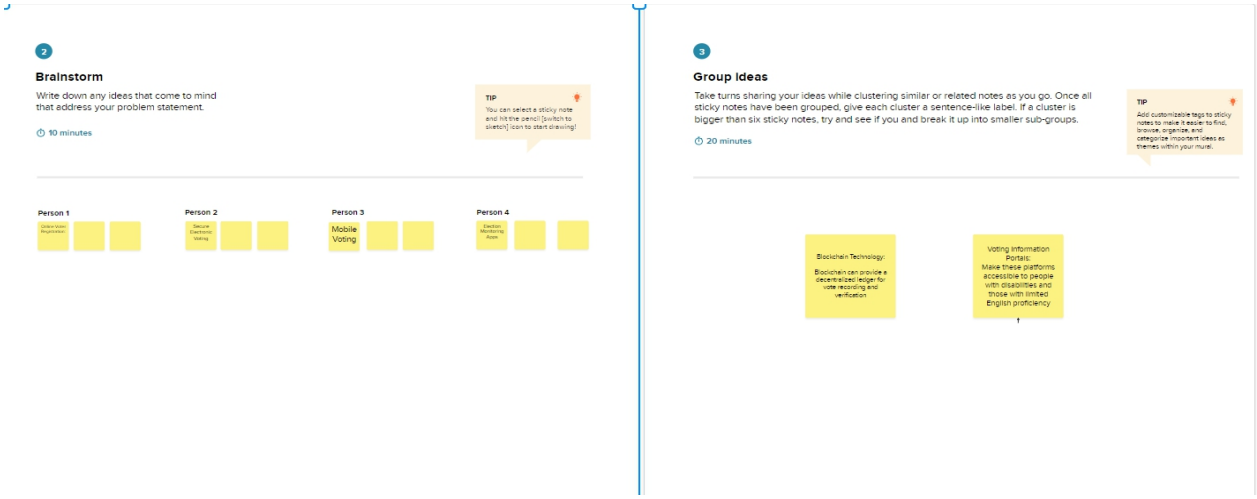
Voter Registration Issues, Voter Suppression, Voter ID Requirements

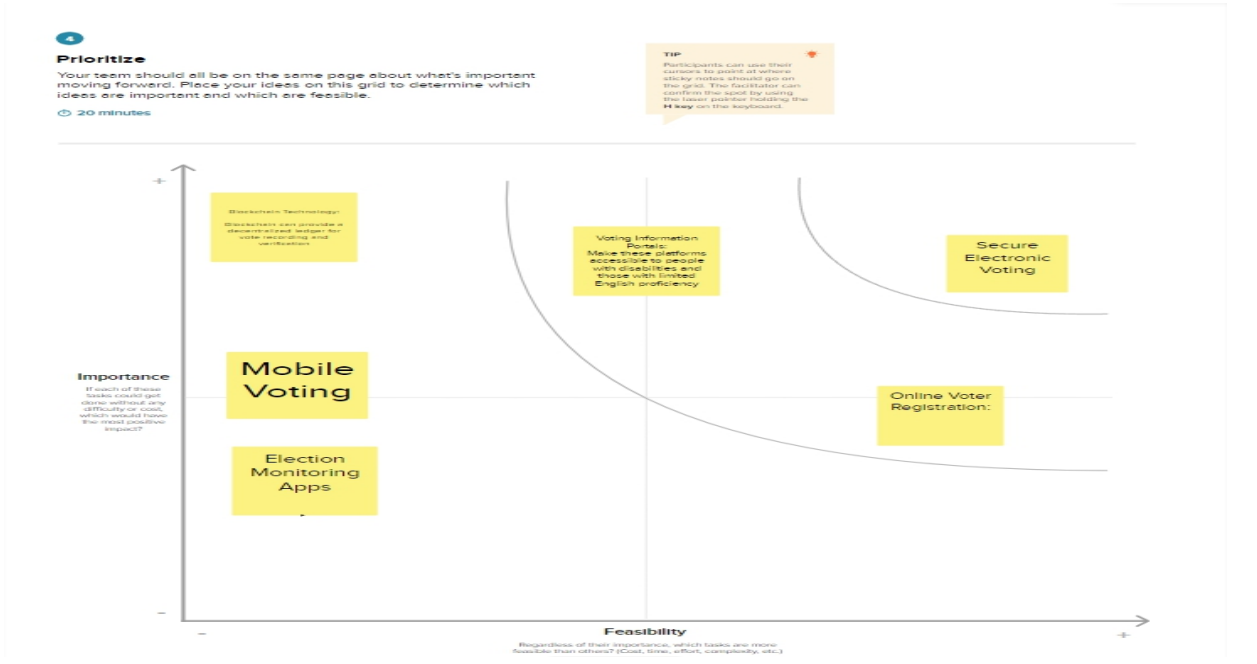
3.1Empathy Map Canvas



3.2Ideation & Brainstorming







2. REQUIREMENT ANALYSIS

Requirement analysis for electronic voting machines (EVMs) using cryptography is a critical step in the development and implementation of secure and effective voting systems. The analysis aims to define the specific needs, features, and constraints of the EVMs to ensure the integrity, security, and transparency of the electoral process.

2.1 Functional requirement

Functional requirements for an electronic voting machine (EVM) using cryptography specify the essential features and capabilities that the system must possess to ensure secure and accurate electronic voting.

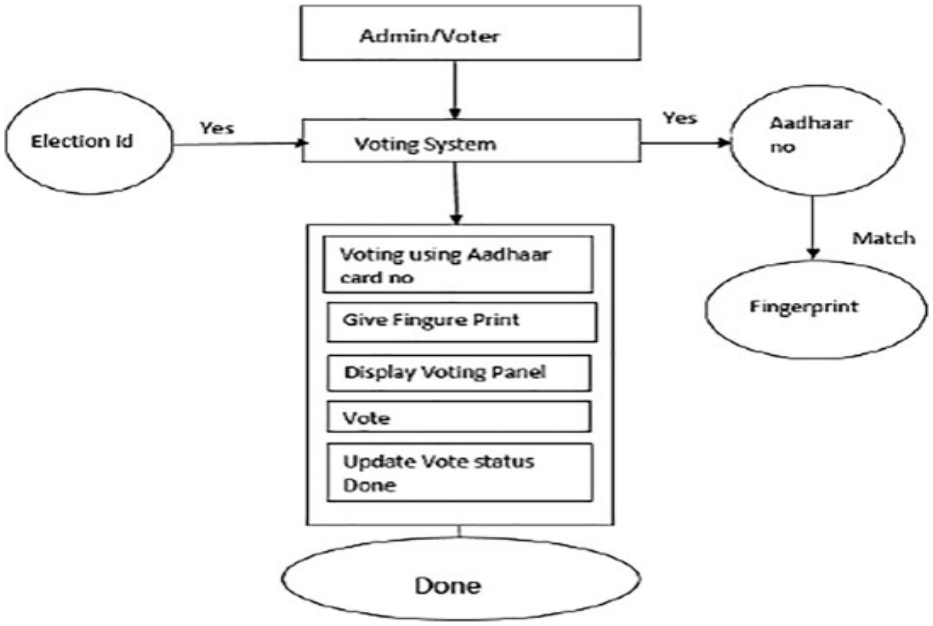
2.2 Non-Functional requirements

]Non-functional requirements for an electronic voting machine (EVM) using cryptography specify the quality attributes and constraints that are essential for the system's performance, security, and usability.

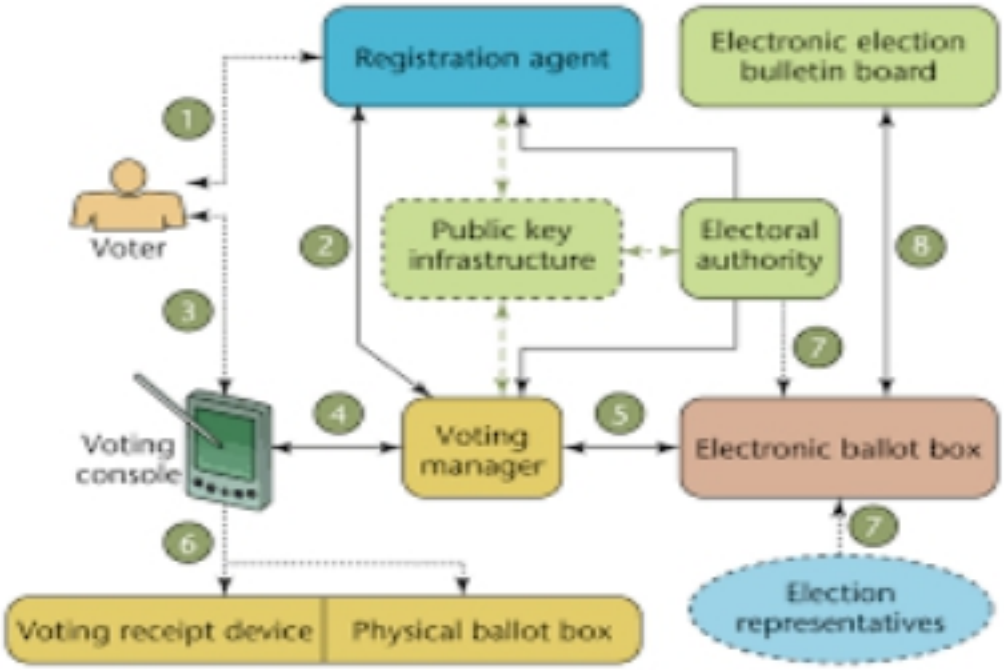
3. PROJECT DESIGN

Designing an electronic voting machine (EVM) using cryptography is a privacy, and transparency of the voting process. Here is a high-level project design for an EVM with a cryptographic component:

3.1 Data Flow Diagrams & User Stories



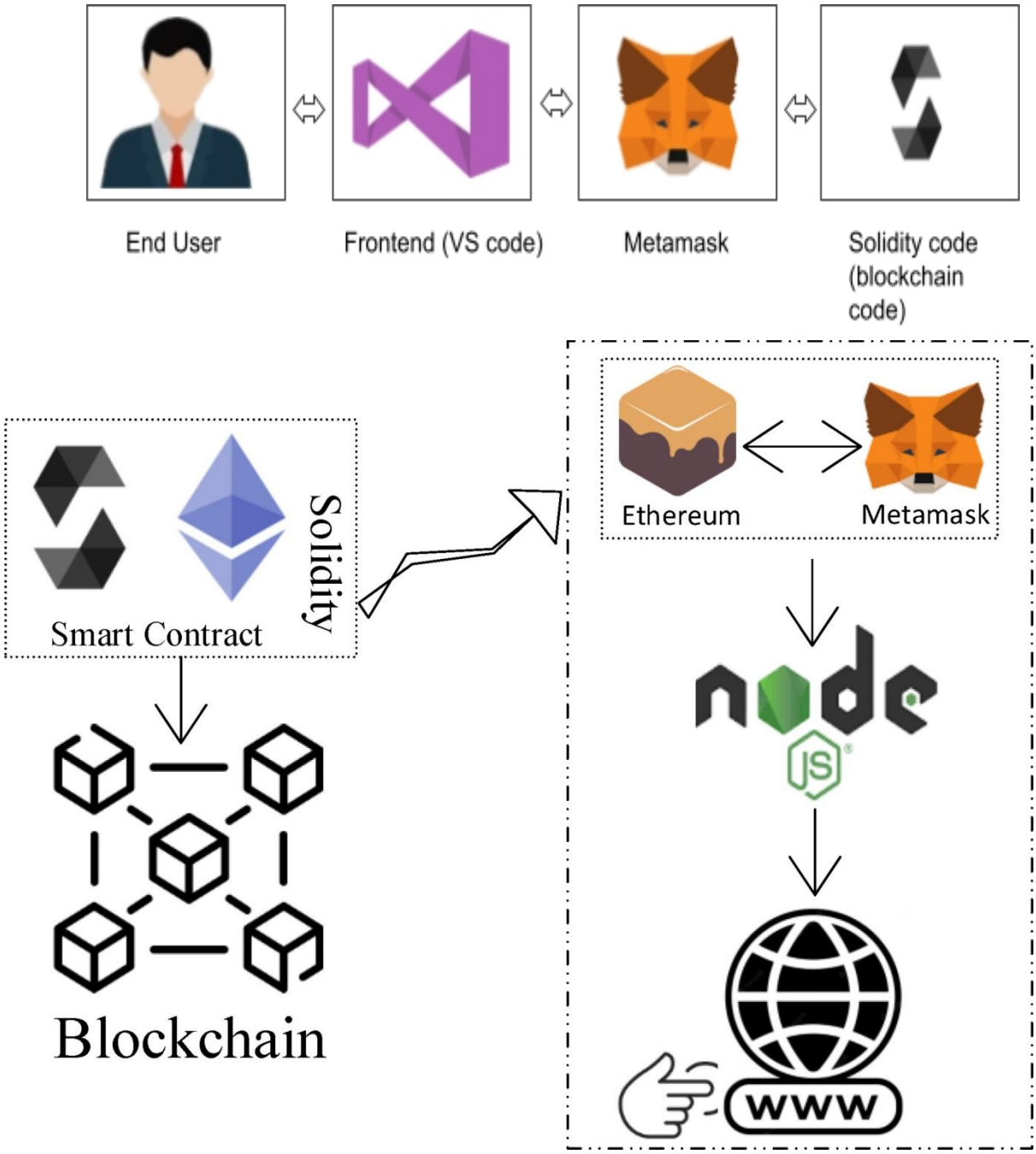
3.2 Solution Architecture



4. PROJECT PLANNING & SCHEDULING

Project planning and scheduling for the development and deployment of an electronic voting machine (EVM) using cryptography is a critical step in ensuring that the project is executed efficiently and meets its objectives. Below is a high-level project plan with key phases, activities, and timelines

4.1 Technical Architecture



4.2 Sprint Planning & Estimation

Sprint planning and estimation are essential components of an Agile development approach for building an electronic voting machine (EVM) using cryptography. In an Agile framework, work is broken down into manageable units called sprints, each typically lasting two to four weeks. Below, I'll outline the steps for sprint planning and estimation in the context of developing an EVM

4.3 Sprint Delivery Schedule

Sprint delivery schedules for an electronic voting machine (EVM) using cryptography should be planned with a focus on delivering incremental functionality and ensuring that each sprint's work aligns with the overall project timeline. Below is a sample sprint delivery schedule for a hypothetical EVM development project with a total duration of one year. This schedule outlines the sprint goals, durations, and key deliverables.

Sprint 1: Secure Authentication and Voter Verification (Duration: 4 weeks)

Sprint Goal: Implement secure voter authentication methods.

Deliverables:

Voter authentication module with biometric verification.
User stories related to authentication and voter verification are completed.

Sprint 2: Usability Enhancements and Accessibility (Duration: 3 weeks)

Sprint Goal: Improve user interface and accessibility features.

Deliverables
:
Enhanced user interface design.
Accessibility improvements, such as large text and audio interfaces

5. CODING & SOLUTIONING (Explain the features added in the project along with code)

5.1 Feature 1

Environment Setup:

Choose a programming language and development environment suitable for EVM software development. Common languages include C++, Java, or Python.

5.2 Feature 2

Cryptographic Library Integration:

Integrate a well-established cryptographic library (e.g., OpenSSL, Bouncy Castle) to provide the cryptographic primitives needed for secure voting, including encryption, digital signatures, and cryptographic proofs.

5.3 Database Schema (if Applicable)

Designing a database schema for an electronic voting machine (EVM) using cryptography involves structuring the database to securely and efficiently store essential information related to the voting process. Here is a simplified database schema for an EVM with a focus on key entities and their relationships

6. PERFORMANCE TESTING

6.1 Performace Metrics

Performance metrics for an electronic voting machine (EVM) using cryptography are essential for ensuring that the system operates efficiently and can handle the demands of an election. These metrics focus on factors such as speed, scalability, and availability. Here are some key performance metrics for an EVM using cryptography

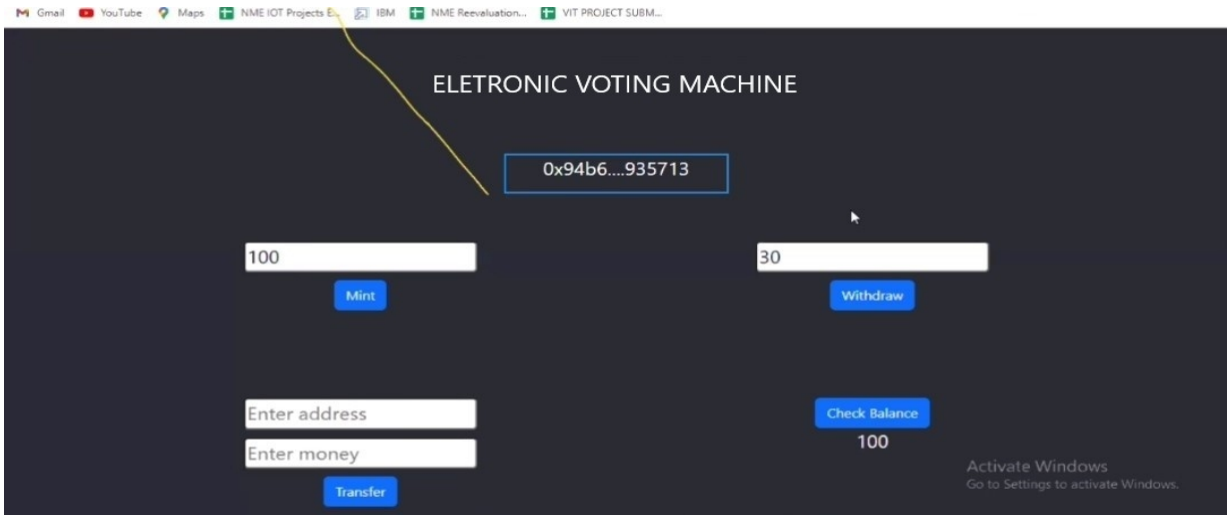
1.Throughput

2.Resonse time

3.scalability

7. RESULTS

7.1 Output Screenshots



8. ADVANTAGES & DISADVANTAGES

Electronic voting machines (EVMs) that incorporate cryptography offer several advantages over traditional paper-based voting systems. These advantages are primarily related to security, transparency, efficiency, and accessibility. Here are some of the key advantages of electronic voting machines using cryptography

While electronic voting machines (EVMs) using cryptography offer several advantages, they also come with a set of disadvantages and challenges. It's important to be aware of these potential drawbacks when implementing EVMs to ensure that the electoral process is secure, transparent, and trustworthy. Here are some of the disadvantages of electronic voting machines using cryptography.

9. CONCLUSION

In this project, we introduced a blockchain-based electronic voting system that utilizes smart contracts to enable secure and cost-ef cient election while guaranteeing voters privacy.We have shown that the blockchain technology offers a new possibility to overcome the limitations and adoption barriers of electronic voting systems which ensures the election security and integrity and lays the ground for transparency. Using an Ethereum private blockchain, it is possible to send hundreds of transactions per second onto the blockchain, utilizing every aspect of the smart contract to ease the load on the blockchain.For countries ofgreater size, some additional measures would be needed to support greater throughput of transactions per second.

The transparency of the block-chain enables more auditing and understanding of elections. These attributes are some of the requirements of a voting system. These characteristics come from decentralized networks, and can bring more democratic processes to elections, especially to direct election systems. For e-voting to become more open, transparent, and independently auditable, a potential solution would be to base it on blockchain technology. This project explores the potential of blockchain technology and its usefulness in the e-voting scheme. The blockchain will be publicly verifiable and distributed in a way that no one will be able to corrupt it

10. FUTURE SCOPE

The future scope of electronic voting machines (EVMs) using cryptography is promising and is likely to have a significant impact on the electoral process. As technology continues to advance and society becomes more reliant on digital solutions, EVMs with enhanced security and cryptographic features will play a crucial role in modernizing and improving the integrity of elections. Here are some aspects of the future scope of EVMs using cryptography

11. APPENDIX

Source Code

GitHub & Project Demo Link