Blockchain

Mini Project

Title: E-Voting

BE C11 - Group 1

Group Members:

Karan Adwani – 2103009
Priyanka Bajaj - 2103012
Hardik Bhagat - 2103017
Akshay Jagiasi - 2103062

Problem Statement

Project Title: Decentralized and Anonymous Voting System Using Blockchain Technology

The primary objective of this project is to design and implement a blockchain-based decentralized voting system where users can log in using their Ethereum identity, cast one vote within a specified timeframe, and ensure that the process is transparent, immutable, and anonymous. The project's goals are:

- Authenticate voters via their Ethereum addresses.
- Prevent double voting by ensuring each voter casts exactly one vote.
- Maintain the anonymity of voters using cryptographic methods.
- Record all votes immutably on the blockchain, ensuring transparency.
- Enforce time-based voting to limit the period in which users can vote.

Motivation

The motivation for this project stems from the need to address the vulnerabilities of traditional voting systems by utilizing a decentralized approach. With the increased adoption of blockchain, this project aims to create a secure, transparent, and anonymous voting platform, reducing the likelihood of fraud and manipulation.

Key motivating factors include:

- **Ensuring voter anonymity** to protect users' privacy.
- **Preventing double voting** by enforcing "one vote per user."
- **Providing immutability and transparency** of votes, making the entire voting process verifiable by the public.

Problem description

Identity Verification

Challenge: The system must ensure that only eligible and authenticated users are allowed to vote. Each user must be uniquely identified to prevent unauthorized voting, but without requiring sensitive personal information.

Solution: Ethereum’s unique address system will be used to authenticate voters. Voters will log in with their Ethereum wallet, and the system will validate whether this address is eligible to vote. Only one vote can be cast per Ethereum address.

One Voter, One Vote

Challenge: A major issue in traditional voting systems is the risk of multiple votes being cast by the same person, leading to fraudulent results.

Solution: The system will use smart contracts to enforce "one voter, one vote." Once a vote is cast from an Ethereum address, the smart contract will prevent that address from voting again. This ensures that no user can cast more than one vote, eliminating double voting.

Voter Anonymity

Challenge: In many voting systems, there is a risk of linking voters to their votes, which can compromise the privacy of the process. This must be avoided to ensure free and unbiased voting.

Solution: While Ethereum addresses are unique, it is crucial that the votes are not linked back to specific users. Cryptographic techniques, such as zero-knowledge proofs or ring signatures, can be used to ensure that although the vote is verified, the voter’s identity remains anonymous. The vote itself is recorded immutably on the blockchain, but there is no direct connection between the voter and their vote.

System Requirements

Functional Requirements

The system must allow users to log in using their Ethereum addresses and cast one vote per address. A smart contract will be responsible for enforcing the "one

vote per user" rule. It will also ensure that all votes are recorded anonymously on the blockchain.

The system must restrict votes to a specific timeframe. Only votes cast within this period will be accepted, and votes submitted outside the voting window will be rejected.

All votes must be recorded immutably and should be available for public verification. However, the system must ensure that there is no direct link between the voter’s Ethereum address and the vote.

Non-Functional Requirements

The system must be scalable, capable of handling a large number of voters without performance issues. It must also be secure from tampering or unauthorized access. The system should process votes quickly and efficiently, ensuring minimal delay between a vote being cast and its confirmation on the blockchain.

A smooth and intuitive user experience is essential. Users should not require an understanding of blockchain to use the voting system effectively.

Design and Architecture

System Overview

The voting system is a decentralized application (dApp) built on the Ethereum blockchain. It consists of a frontend user interface where voters interact with the system, and backend smart contracts that handle vote authentication, recording, and tallying.

Voters will interact with the system through a web-based interface. They will log in using their Ethereum wallet (e.g., MetaMask), cast their vote, and the vote will be recorded on the blockchain. Smart contracts will ensure that each voter casts only one vote and that all votes are stored immutably.

The system’s backend, implemented using Ethereum smart contracts, handles:

- Voter authentication.
- Vote recording.
- Enforcement of the "one voter, one vote" rule.
- Time-based restrictions on voting.
- Automatic vote tallying after the voting period ends.

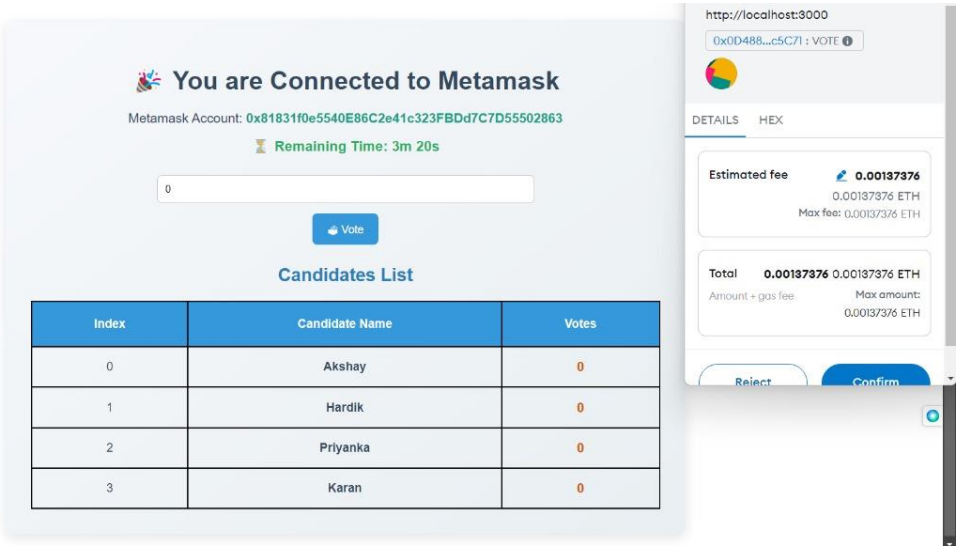
System Flow

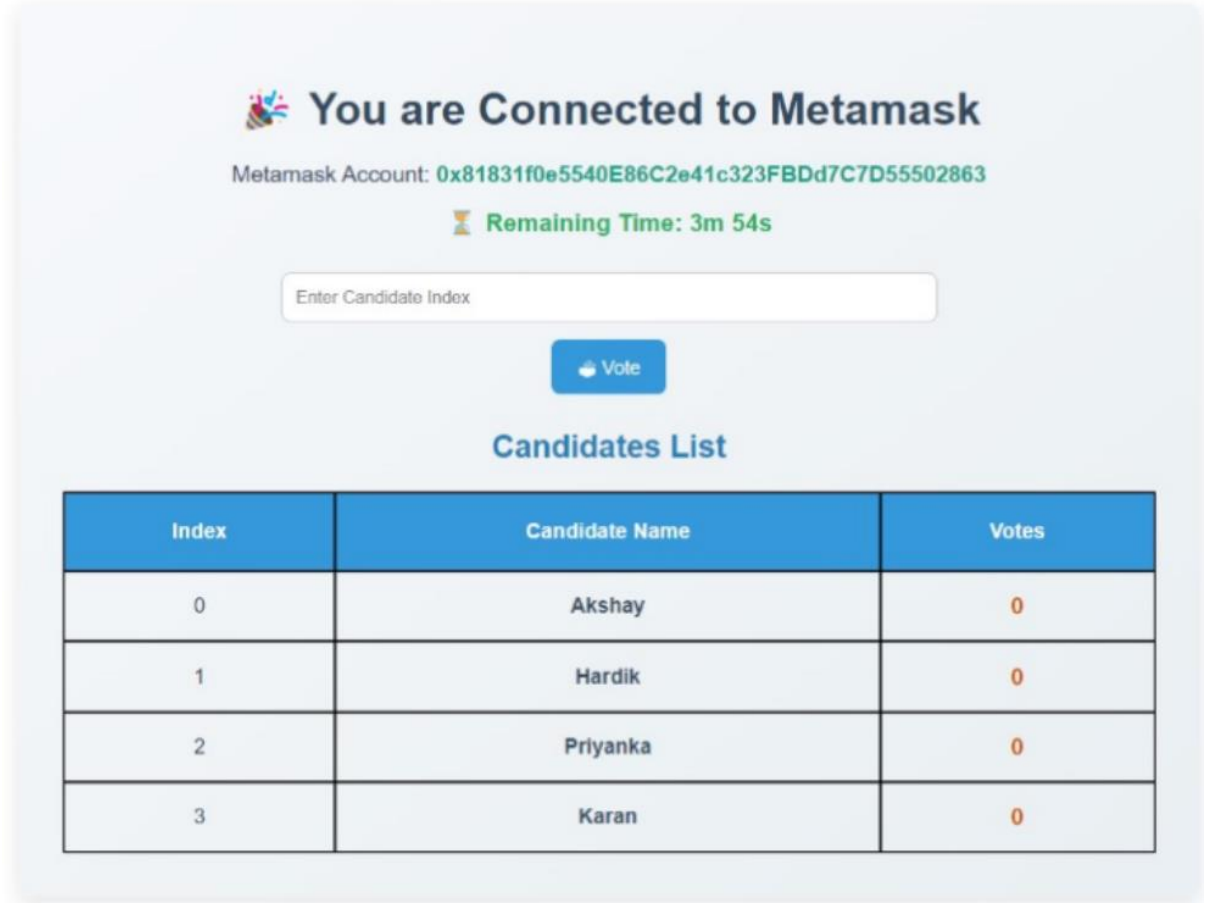
1. **Login**: Voters log in using their Ethereum address through a wallet like MetaMask. The smart contract verifies that the user is eligible to vote.
2. **Vote Casting**: The voter selects their choice and submits it. The smart contract verifies the vote and checks if the voter has already cast a vote.
3. **Vote Recording**: The vote is recorded on the blockchain. The system ensures that votes are anonymized and stored immutably.
4. **Time Frame Management**: The system accepts votes only during the specified voting period. Votes submitted outside this period are automatically rejected.
5. **Result Calculation**: Once the voting period ends, the smart contract tallies the votes automatically and publishes the results. The vote data remains available for audit and verification.

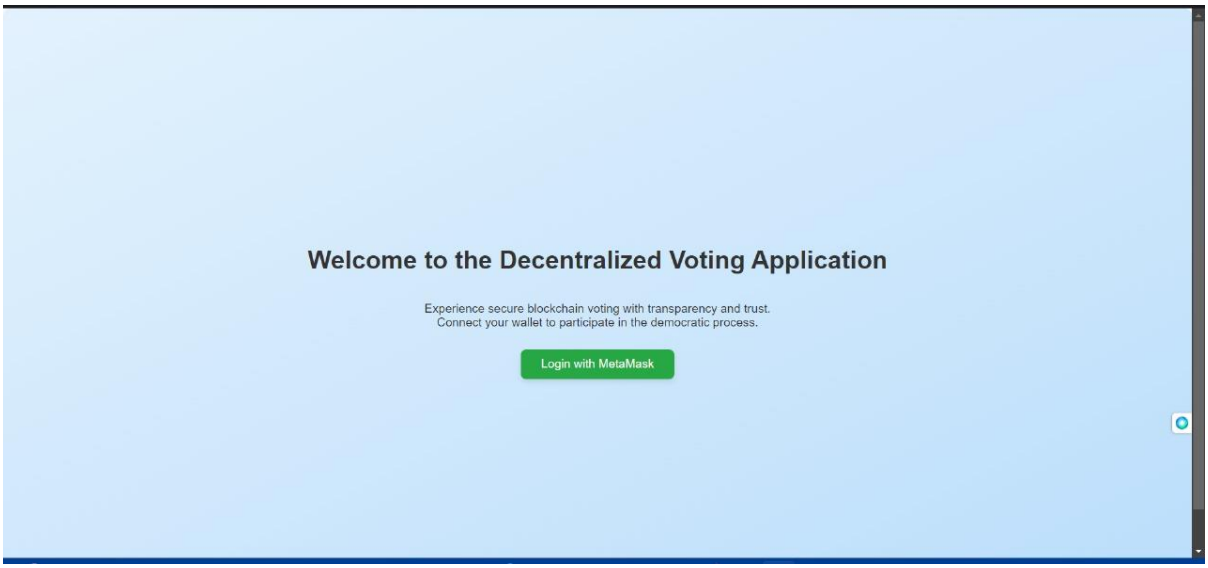
Conclusion

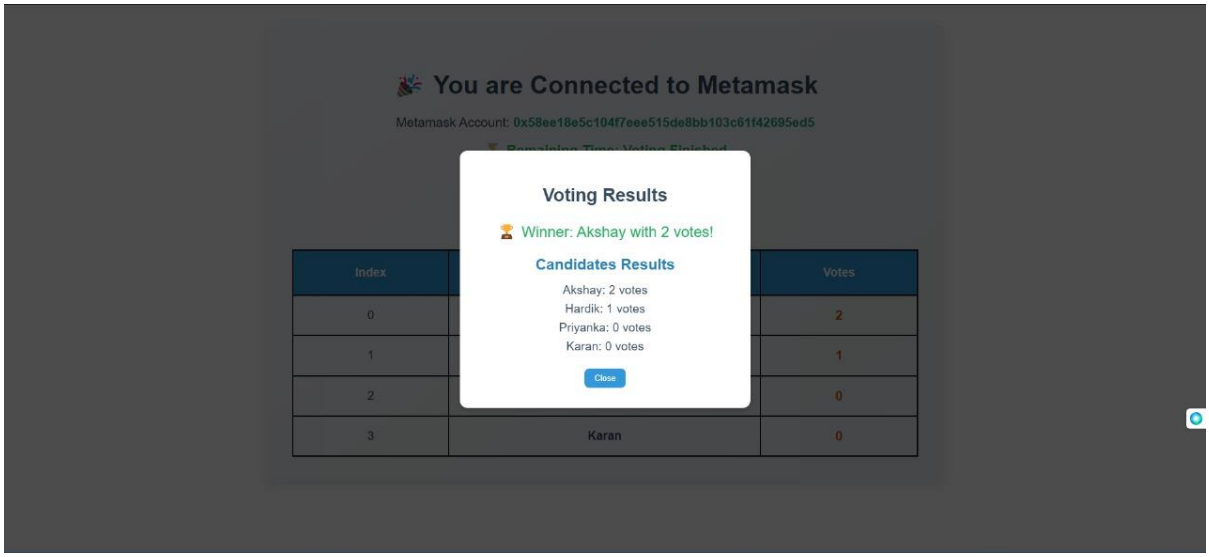
This project aims to develop a secure, decentralized, and anonymous voting system using Ethereum blockchain technology. By leveraging blockchain's transparency, immutability, and cryptographic security, the system will address the challenges of traditional voting systems, such as double voting, voter fraud, and privacy concerns. The resulting platform will ensure that votes are cast securely, recorded immutably, and counted transparently, while preserving the privacy of voters.

Output


You are Connected to Metamask
Metamask Account: 0x81831f0e5540E86C2e41c323FBDd7C7D55502863
Remaining Time: 3m 20s
0
Vote
Candidates List
Index
Candidate Name
Votes
0
Akshay
0
1
Hardik
0
2
Priyanka
0
3
Karan
0
http://localhost:3000
0x0D488...c5C71 : VOTE
DETAILS
HEX
Estimated fee
0.00137376
0.00137376 ETH
Max fee: 0.00137376 ETH
Total
0.00137376
0.00137376 ETH
Amount + gas fee
Max amount:
0.00137376 ETH
Reject
Confirm


You are Connected to Metamask
Metamask Account: 0x81831f0e5540E86C2e41c323FBDd7C7D55502863
Remaining Time: 3m 54s
Enter Candidate Index
Vote
Candidates List
Index
Candidate Name
Votes
0
Akshay
0
1
Hardik
0
2
Priyanka
0
3
Karan
0


Welcome to the Decentralized Voting Application
Experience secure blockchain voting with transparency and trust.
Connect your wallet to participate in the democratic process.
Login with MetaMask



You are Connected to Metamask

Metamask Account: 0x81831f0e5540E86C2e41c323FBDd7C7D55502863

Remaining Time: 2m 51s

You have already voted

Candidates List

Index	Candidate Name	Votes
0	Akshay	1
1	Hardik	0
2	Priyanka	0
3	Karan	0