**Decentralized Voting System on Ethereum**

**Project report in partial fulfilment of the requirement for the award of the degree of**

**Bachelor of Technology**

**In**

**CSE (IOT, BCT, CYS)**

**Submitted By**

Pinaki Pritam Singha University Roll No. 12021002029065  
Trideep Saha University Roll No. 12021002029040  
Ratul Das University Roll No. 12021002029046  
Kuntaleeka Kundu University Roll No. 12021002029016  
Tathagata Ghosh University Roll No. 12021002029039  
Suchak Sarkar University Roll No. 12021002029071  
Yagnasree Chakraborty University Roll No. 12021002029062  
Aniket Marik University Roll No. 12021002001073  
Nilarghya Nandan University Roll No. 12021002029036  
Sayan Maity University Roll No. 12021002029198

**Under the guidance of**

Prof. Dr. Siddartha Roy

Department of CSE (IOT, BCT, CYS)



UNIVERSITY OF ENGINEERING & MANAGEMENT, KOLKATA

University Area, Plot No. III – B/5, New Town, Action Area – III, Kolkata – 700160.

**CERTIFICATE**

This is to certify that the project titled **Decentralized Voting System on Ethereum** submitted by Pinaki Pritam Singha (University Roll No. 12021002029065), Trideep Saha (University Roll No. 12021002029040), Ratul Das (University Roll No. 12021002029046), Suchak Sarkar (University Roll No. 12021002029071), Sayan Maity (University Roll No. 12021002029198) Kuntaleeka Kundu (University Roll No. 12021002029016), Tathagata Ghosh (University Roll No. 12021002029039), Yagnasree Chakraborty (University Roll No. 12021002029062), Aniket Marik (University Roll No. 12021002001073) and Nilarghya Nandan (University Roll No. 12021002029036) students of UNIVERSITY OF ENGINEERING & MANAGEMENT, KOLKATA, in partial fulfilment of requirement for the degree of Bachelor of Computer Science (IOT, BCT, CYS), is a Bonafede work carried out by them under the supervision and guidance of Prof. Dr. Siddartha Roy during 6th Semester of academic session of 2023 - 2024. The content of this report has not been submitted to any other university or institute. I am glad to inform that the work is entirely original and its performance is found to be quite satisfactory.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of Guide

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of Head of the Department

**ACKNOWLEDGEMENT**

We would like to take this opportunity to thank everyone whose cooperation and encouragement throughout the ongoing course of this project remains invaluable to us.

We are sincerely grateful to our guide Prof. Dr. Siddartha Roy of the Department of CSE (IOT, BCT, CYS), UEM, Kolkata, for his wisdom, guidance and inspiration that helped us to go through with this project and take it to where it stands now.

Last but not the least, we would like to extend our warm regards to our families and peers who have kept supporting us and always had faith in our work.

Pinaki Pritam Singha

Trideep Saha

Ratul Das

Suchak Sarkar

Sayan Maity

Kuntaleeka Kundu

Tathagata Ghosh

Yagnasree Chakraborty

Aniket Marik

Nilarghya Nandan

**TABLE OF CONTENTS**

**ABSTRACT...............................................................................................5**

**CHAPTER – 1: INTRODUCTION..........................................................................6**

**CHAPTER – 2: LITERATURE SURVEY.............................................................7**

**CHAPTER – 3: PROBLEM STATEMENT ..........................................................8**

**CHAPTER – 4: PROPOSED SOLUTION .............................................................9**

**CHAPTER – 5: EXPERIMENTAL SETUP AND RESULT ANALYSIS...........10**

**CHAPTER – 6: CONCLUSION & FUTURE SCOPE..........................................18**

**BIBLIOGRAPHY .....................................................................................................19**

# ABSTRACT

Decentralized voting via the Ethereum blockchain [2] offers a secure and transparent method for online voting. It operates as a decentralized application on the Ethereum network, enabling participants to cast votes and review results directly, without intermediaries. Through blockchain recording, votes are immutable, preventing manipulation. Smart contracts automate the process, ensuring transparency and security. This approach provides a dependable and efficient solution for conducting trustworthy elections.

# INTRODUCTION

Blockchain technology [3] has emerged as a groundbreaking innovation, facilitating secure and transparent transactions without the need for intermediaries. At its core, blockchain operates as a distributed digital ledger, enabling participants within a network to validate and share transactions securely. Unlike traditional centralized systems, blockchain is inherently decentralized, meaning that data is stored across a network of computers rather than a central database. This decentralized structure enhances security, as it becomes inherently difficult for malicious actors to manipulate or compromise the data.

Initially popularized by Bitcoin [4], the first decentralized cryptocurrency, blockchain technology has transcended its origins to find applications in diverse sectors such as finance, supply chain management, healthcare, and notably, voting systems. Blockchain operates by organizing data into blocks that are interlinked to form a chain. Each block contains a unique cryptographic hash generated from its contents, serving to establish a secure connection to the preceding block.

Once a block is added to the blockchain, it becomes immutable, meaning that its contents cannot be altered or deleted without the consensus of the network participants. This immutability ensures the integrity and transparency of the data stored on the blockchain, mitigating the risk of tampering and fraud.

The decentralized nature of blockchain technology presents immense potential for revolutionizing the way elections are conducted. By harnessing the security, transparency, and immutability of blockchain, decentralized voting systems have the capability to address many of the challenges inherent in traditional voting mechanisms.

In a decentralized voting system leveraging the Ethereum blockchain, each voter possesses a unique digital identity. When a voter casts their ballot, the vote is recorded on the blockchain in a tamper-proof manner, safeguarding its integrity. Moreover, decentralized voting systems eliminate the necessity for intermediaries, such as government agencies, to oversee the electoral process, thereby enhancing efficiency and reducing vulnerability to corruption or manipulation.

Additionally, decentralized voting systems have the capacity to enhance voter participation by enabling individuals to cast their votes from any location with internet connectivity. This inclusivity fosters a more democratic electoral process, characterized by increased voter engagement and turnout.

In summary, a decentralized voting system utilizing the Ethereum blockchain holds the promise of delivering substantial benefits to the electoral process. By enhancing security, transparency, and accessibility, such systems have the potential to reshape elections, ensuring their integrity and legitimacy while fostering democratic principles.

# LITERATURE SURVEY

Highly advanced security methods are necessary to introduce effective online voting system in the whole world. The aspect of security and transparency is a threat from global election with the conventional system. General elections still use a centralized system where one organization that manages it. Some of the problems that can occur in traditional electoral systems are with an organization that has full control over the database and system, it is possible to manipulate with the database. This paper presents a survey on some previous voting system that is used by different countries and organizations

Electronic Voting Systems:

Electronic voting systems [5] face challenges related to authentication, data privacy, integrity, transparency, and verifiability. Blockchain technology offers promising solutions to many of these issues. However, scalability has emerged as a significant barrier to fully realizing the potential of blockchain, particularly in electronic voting contexts. This study aims to address scalable blockchain-based electronic voting systems and associated challenges, while also anticipating future developments. Conducted through a systematic literature review, the study examined 76 English-language articles from prominent databases spanning from January 1, 2017, to March 31, 2022. The review identified established proposals, their implementations, verification methods, cryptographic solutions, and performance parameters. It also assessed the advantages, obstacles, and common scalability approaches in blockchain systems. Furthermore, the study outlined potential research directions for developing scalable electronic voting systems based on blockchain technology. By considering voting requirements, advantages, disadvantages, and providing guidelines, this research aids future endeavours in proposing and developing scalable voting solutions.

Blockchain based on E-voting:

Blockchain technology has garnered significant attention as a decentralized and distributed public ledger within peer-to-peer networks [6]. Its linked block structure and trusted consensus mechanism enable the synchronization of data modifications, facilitating the development of a tamper-proof digital platform for data storage and sharing. There is growing recognition of blockchain's potential applicability across various interactive online systems, including the Internet of Things, supply chain management, and voting systems. This survey aims to explore recent contributions addressing security and privacy issues in blockchain-based e-voting systems. Additionally, the paper offers a comparative analysis of the security and privacy requirements of existing e-voting systems based on blockchain.

# PROBLEM STATEMENT

The increasing digitization of various aspects of society has led to a growing interest in electronic voting (e-voting) systems as a means of modernizing and improving democratic processes. However, traditional e-voting systems often face significant challenges related to security, privacy, transparency, and verifiability. These challenges stem from the centralized nature of most electronic voting systems, which rely on a single authority or entity to manage and oversee the voting process. This centralized approach introduces vulnerabilities, such as the risk of tampering, hacking, or manipulation of voting data.

To address these issues, there has been a surge of interest in leveraging blockchain technology for e-voting. Blockchain offers a decentralized and distributed ledger system that can potentially enhance the security, transparency, and integrity of e-voting processes. By utilizing blockchain, e-voting systems can store votes in a tamper-proof and transparent manner, making it virtually impossible for unauthorized parties to alter or manipulate the voting data.

Furthermore, concerns about the privacy and anonymity of voters in blockchain-based e-voting systems remain significant. While blockchain provides transparency and immutability, ensuring voter privacy without compromising the integrity of the voting process presents a complex challenge. Additionally, the implementation and integration of blockchain technology into existing e-voting infrastructures require careful consideration of technical, legal, and regulatory factors.

In summary, the problem statement revolves around the need to develop scalable, secure, and privacy-preserving e-voting systems using blockchain technology. This entails overcoming challenges related to scalability, privacy, regulatory compliance, and the integration of blockchain into existing voting frameworks. Addressing these challenges is essential to realizing the potential benefits of blockchain in enhancing the integrity and trustworthiness of e-voting processes.

# PROPOSED SOLUTION

The proposed decentralized voting system utilizing the Ethereum blockchain offers a solution geared towards transparent and secure elections. Through the utilization of smart contracts on the Ethereum network, the system facilitates anonymous voting while upholding the integrity and immutability of the voting data. This approach is designed to enhance voter confidence in the election process and mitigate the risks associated with fraud or manipulation.

Enumerating the advantages of the proposed system:

* Decentralization ensures that no single entity controls the voting process.
* Transparency is maintained throughout the entire voting process.
* The system is designed to be tamper-proof.
* Eligible voters can participate in the voting process from any location worldwide.
* This method of voting is cost-effective.
* Election results are provided in real-time.

The objectives of the proposed research encompass several key areas:

* Security: Establishing a secure platform to conduct elections, preventing tampering with votes, and ensuring transparent and verifiable election results.
* Transparency: Providing voters with complete transparency throughout the voting process, including vote counting and result announcement.
* Accessibility: Enhancing accessibility to the voting process for all eligible voters by eliminating the requirement for physical presence at polling stations, thereby potentially increasing voter turnout.
* Efficiency: Improving the efficiency of the voting process by reducing the time and resources needed to conduct elections. The automated nature of the system, coupled with the elimination of intermediaries, can significantly diminish the costs and duration associated with traditional voting methods.
* Trust: Bolstering trust in the voting process by implementing a transparent and tamper-proof mechanism for recording and tallying votes.

# EXPRERIMENTAL SETUP AND RESULT ANALYSIS

Requirements:

* NodeJS
* Truffle
* Ganache
* Solidity
* Metamask
* Python
* FastAPI
* MySQL
* HTML-CSS

Code [1]:

1. Migrations.sol

pragma solidity ^0.5.15;

contract Migrations {

address public owner;

uint public last\_completed\_migration;

modifier restricted() {

require(msg.sender == owner, "Access restricted to owner");

\_;

}

constructor() public {

owner = msg.sender;

}

function setCompleted(uint completed) public restricted {

last\_completed\_migration = completed;

}

function upgrade(address new\_address) public restricted {

Migrations upgraded = Migrations(new\_address);

upgraded.setCompleted(last\_completed\_migration);

}

}

1. Voting.sol

pragma solidity ^0.5.15;

contract Voting {

struct Candidate {

uint id;

string name;

string party;

uint voteCount;

}

mapping (uint => Candidate) public candidates;

mapping (address => bool) public voters;

uint public countCandidates;

uint256 public votingEnd;

uint256 public votingStart;

function addCandidate(string memory name, string memory party) public returns(uint) {

countCandidates ++;

candidates[countCandidates] = Candidate(countCandidates, name, party, 0);

return countCandidates;

}

function vote(uint candidateID) public {

require((votingStart <= now) && (votingEnd > now));

require(candidateID > 0 && candidateID <= countCandidates);

//daha önce oy kullanmamıs olmalı

require(!voters[msg.sender]);

voters[msg.sender] = true;

candidates[candidateID].voteCount ++;

}

function checkVote() public view returns(bool){

return voters[msg.sender];

}

function getCountCandidates() public view returns(uint) {

return countCandidates;

}

function getCandidate(uint candidateID) public view returns (uint,string memory, string memory,uint) {

return (candidateID,candidates[candidateID].name,candidates[candidateID].party,candidates[candidateID].voteCount);

}

function setDates(uint256 \_startDate, uint256 \_endDate) public{

require((votingEnd == 0) && (votingStart == 0) && (\_startDate + 1000000 > now) && (\_endDate > \_startDate));

votingEnd = \_endDate;

votingStart = \_startDate;

}

function getDates() public view returns (uint256,uint256) {

return (votingStart,votingEnd);

}

}

1. Main.py (for API and Database)

import dotenv

import os

import mysql.connector

from fastapi import FastAPI, HTTPException, status, Request

from fastapi.middleware.cors import CORSMiddleware

from fastapi.encoders import jsonable\_encoder

from mysql.connector import errorcode

import jwt

# Loading the environment variables

dotenv.load\_dotenv()

# Initialize the todoapi app

app = FastAPI()

# Define the allowed origins for CORS

origins = [

"http://localhost:8080",

"http://127.0.0.1:8080",

]

# Add CORS middleware

app.add\_middleware(

CORSMiddleware,

allow\_origins=origins,

allow\_credentials=True,

allow\_methods=["\*"],

allow\_headers=["\*"],

)

# Connect to the MySQL database

try:

cnx = mysql.connector.connect(

user=os.environ['MYSQL\_USER'],

password=os.environ['MYSQL\_PASSWORD'],

host=os.environ['MYSQL\_HOST'],

database=os.environ['MYSQL\_DB'],

)

cursor = cnx.cursor()

except mysql.connector.Error as err:

if err.errno == errorcode.ER\_ACCESS\_DENIED\_ERROR:

print("Something is wrong with your user name or password")

elif err.errno == errorcode.ER\_BAD\_DB\_ERROR:

print("Database does not exist")

else:

print(err)

# Define the authentication middleware

async def authenticate(request: Request):

try:

api\_key = request.headers.get('authorization').replace("Bearer ", "")

cursor.execute("SELECT \* FROM voters WHERE voter\_id = %s", (api\_key,))

if api\_key not in [row[0] for row in cursor.fetchall()]:

raise HTTPException(

status\_code=status.HTTP\_401\_UNAUTHORIZED,

detail="Forbidden"

)

except:

raise HTTPException(

status\_code=status.HTTP\_401\_UNAUTHORIZED,

detail="Forbidden"

)

# Define the POST endpoint for login

@app.get("/login")

async def login(request: Request, voter\_id: str, password: str):

await authenticate(request)

role = await get\_role(voter\_id, password)

# Assuming authentication is successful, generate a token

token = jwt.encode({'password': password, 'voter\_id': voter\_id, 'role': role}, os.environ['SECRET\_KEY'], algorithm='HS256')

return {'token': token, 'role': role}

# Replace 'admin' with the actual role based on authentication

async def get\_role(voter\_id, password):

try:

cursor.execute("SELECT role FROM voters WHERE voter\_id = %s AND password = %s", (voter\_id, password,))

role = cursor.fetchone()

if role:

return role[0]

else:

raise HTTPException(

status\_code=status.HTTP\_401\_UNAUTHORIZED,

detail="Invalid voter id or password"

)

except mysql.connector.Error as err:

print(err)

raise HTTPException(

status\_code=status.HTTP\_500\_INTERNAL\_SERVER\_ERROR,

detail="Database error"

)

1. Login.js

const loginForm = document.getElementById('loginForm');

loginForm.addEventListener('submit', (event) => {

event.preventDefault();

const voter\_id = document.getElementById('voter-id').value;

const password = document.getElementById('password').value;

const token = voter\_id;

const headers = {

'method': "GET",

'Authorization': `Bearer ${token}`,

};

fetch(`http://127.0.0.1:8000/login?voter\_id=${voter\_id}&password=${password}`, { headers })

.then(response => {

if (response.ok) {

return response.json();

} else {

throw new Error('Login failed');

}

})

.then(data => {

if (data.role === 'admin') {

console.log(data.role)

localStorage.setItem('jwtTokenAdmin', data.token);

window.location.replace(`http://127.0.0.1:8080/admin.html?Authorization=Bearer ${localStorage.getItem('jwtTokenAdmin')}`);

} else if (data.role === 'user'){

localStorage.setItem('jwtTokenVoter', data.token);

window.location.replace(`http://127.0.0.1:8080/index.html?Authorization=Bearer ${localStorage.getItem('jwtTokenVoter')}`);

}

})

.catch(error => {

console.error('Login failed:', error.message);

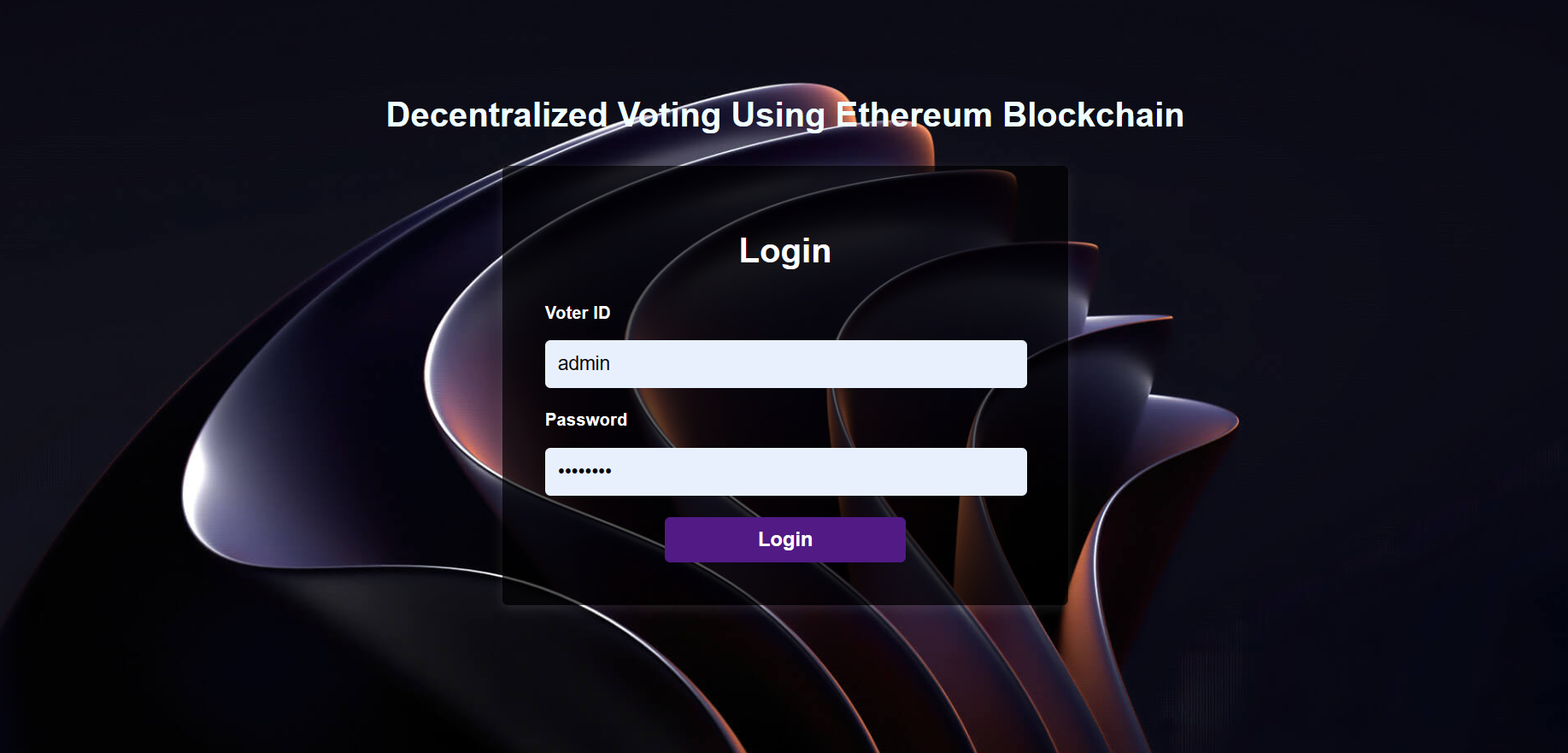
});

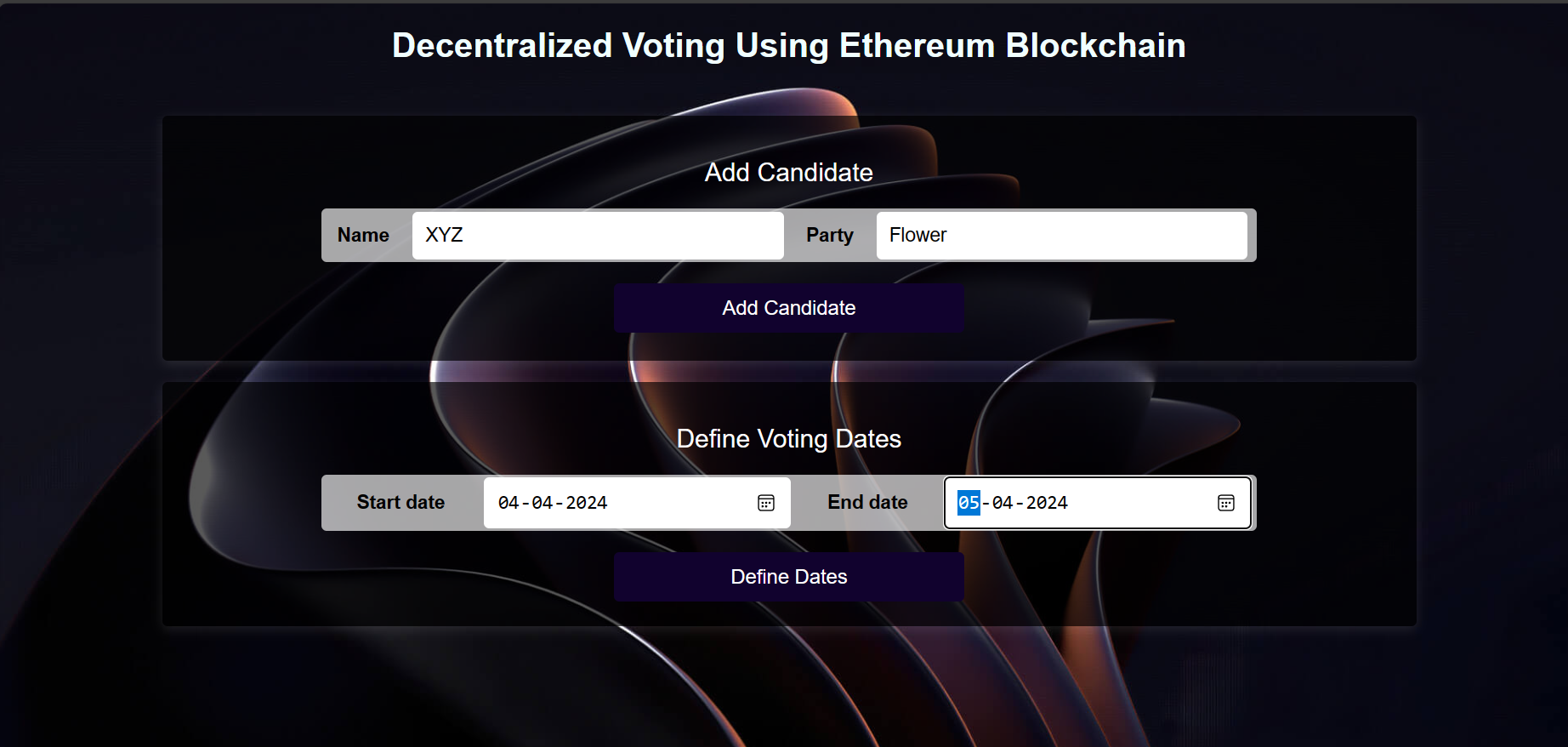
});

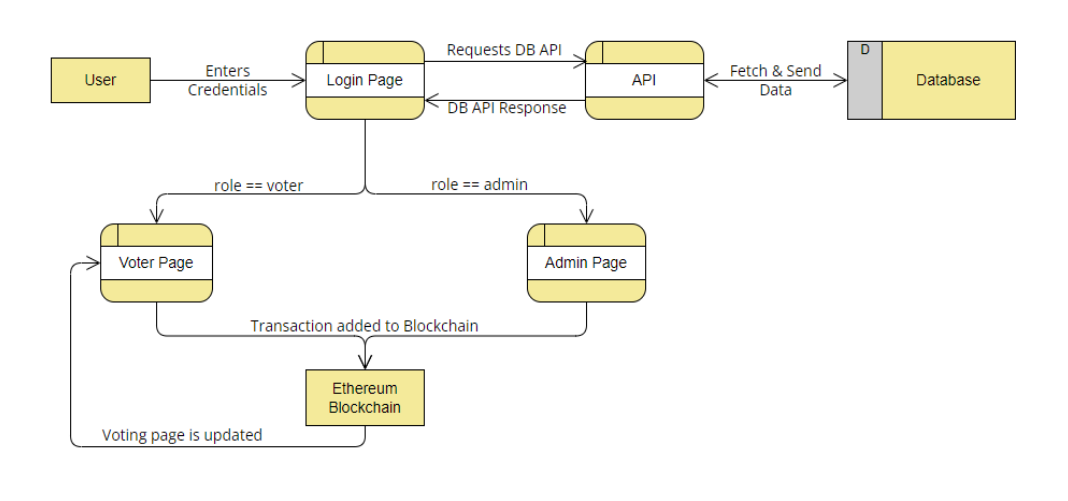
Result Analysis:

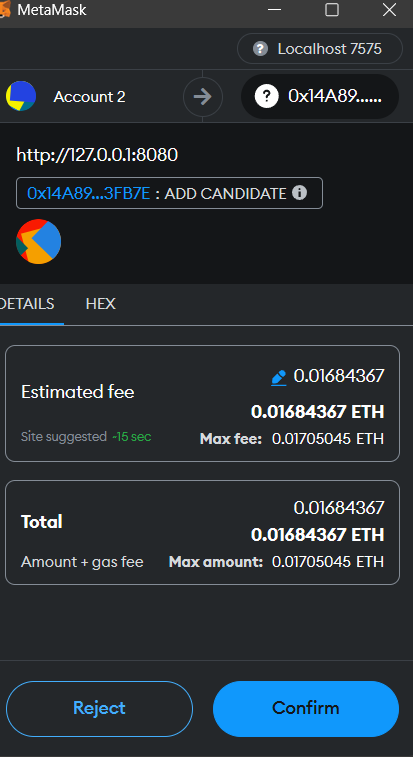
Results indicated successful functionality across registration, ballot creation, voting, tallying, and result display. Security measures were effective in ensuring vote security, anonymity, and protection against tampering. Usability assessment found the interface to be intuitive. Voting accuracy and integrity were confirmed.

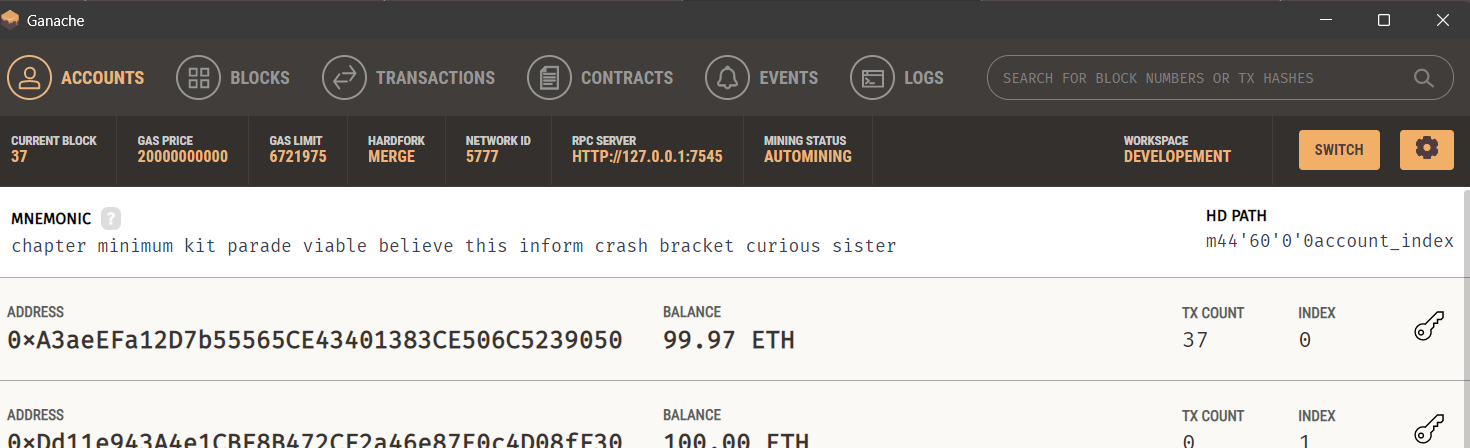
Screenshots:











# CONCLUSION & FUTURE SCOPE

Utilizing Ethereum Blockchain, decentralized voting presents a robust and transparent solution for ensuring secure elections. Through blockchain technology, it guarantees the integrity of votes and establishes a tamper-proof platform. With ongoing improvements, including enhancing user experience, scalability, and integration with other innovative technologies, decentralized voting holds the potential to transform the democratic process. It empowers citizens to engage in a reliable and efficient voting system, marking a significant stride toward fostering a more democratic and accountable society.

Future Scope:

Future iterations of the decentralized voting system could incorporate additional features, such as real-time vote tallying, secure voter identification mechanisms, advanced data analytics for insightful voter analysis, and integration with emerging technologies like artificial intelligence and biometrics. These enhancements would further elevate the efficiency, security, and accessibility of the voting process, promoting inclusivity and instilling greater trust in the electoral system.

# BIBLIOGRAPHY

[1] Github Repository Reference [https://github.com/PixMusicaX/Decentralized\_Voting\_System Created 4th April, 2024]

[2] ETH Development Documentation [https://ethereum.org/en/developers/docs/ Accessed 24th March, 2024]

[3] Blockchain in G4G [https://www.geeksforgeeks.org/blockchain-technology-introduction/ Accessed 24th March, 2024]

[4] Bitcoin on Wikipedia [https://en.wikipedia.org/wiki/Bitcoin Accessed 26th March, 2024]

[5] A Survey of Blockchain Based on E-voting Systems by Yousif Osman Abuidris, Kumar et al.

[6] Survey on Voting System using Blockchain Technology by Mayur Shirsath, Zade, Talke, et al.