VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Winter Semester 2022-23

School of Computer Science and Engineering

Slot: A2+TA2 Course Code: CSE1006

Course Title: Blockchain and Cryptocurrency Technologies

Submitted to:

Prof. Jothi K R

Title: VOTING SYSTEM USING SMART CONTRACTS

REPORT

Name	Registration Number
Tiya Bhat	20BCI0101

ABSTRACT

This project aims to develop a decentralized voting system using smart contracts. The proposed system is designed to increase the transparency and security of voting, as well as reduce the possibility of fraud and manipulation. The system is based on the blockchain technology, which ensures the immutability and transparency of the voting records. The smart contract used in the system automates the entire voting process, from the registration of voters to the counting of votes, without the need for a central authority. The system also ensures anonymity and confidentiality of votes.

INTRODUCTION

Voting is a fundamental process in democratic societies that allows citizens to participate in decision-making processes. However, the traditional voting system has been plagued by various issues, including fraud, manipulation, and lack of transparency. With the advancement of technology, it is possible to develop a more secure and transparent voting system using blockchain technology and smart contracts.

Smart contracts are contracts that automatically carry out the conditions of the parties' agreement after being entered into a line of code. They allow for automation of processes and execution of transactions without the need for intermediaries. This makes smart contracts an ideal technology for implementing a decentralized voting system.

The proposed voting system using smart contracts is designed to provide transparency, security, and efficiency in the voting process. The system utilizes the immutability and transparency of the blockchain to ensure the integrity of the voting records. The smart contract automates the entire voting process, from the registration of voters to the counting of votes, without the need for a central authority. The system also provides anonymity and confidentiality of votes.

TOOLS USED

- **Smart Contract:** Smart contracts are identifiable and irreversible applications that execute in a decentralized climate (e.g., blockchain). When the smart contract has been conveyed no one can alter the code or change its execution behavior. Smart contract execution assurances to tie parties together to an agreement as written.
- **Solidity:** Solidity is a curly-bracket language. It is influenced by C++, Python and JavaScript, and is designed to target the Ethereum Virtual Machine (EVM).
- **MetaMask:** It is a chrome extension that is used to test ethereum networks using fake accounts.
- **Web3.js:** It is a collection of libraries that allowed us to interact with a local or remote ethereum node using HTTP, IPC or WebSocket.
- **Sepolia Test Network:** The Sepolia test-net allows blockchain developments to test their work in a live setting, but without the need for real ETH and main-net 2KEY tokens.
- **Remix.ethereum.org:** It is an online compiler which is used for the compilation of .sol file i.e., smart contracts.
- **HTML/CSS/JavaScript:** For the frontend of the web application

LITERATURE SURVEY

Digital Voting: A Blockchain-based E-Voting System using Biohash and Smart Contract by Syada Tasmia Alvi, Mohammed Nasir Uddin, Linta Islam

The voting process is the tool used to put the public's opinion into action and improve system administration. Conventional voting hasn't been popular in recent years with either the public or the government. Given how easily ballots may be tampered with, they are not totally secure. It also raises concerns about transparency and voter safety. Also, it takes too long to count the votes. A fascinating topic in the current voting system is the modification of voting globally. To address these issues in many countries, the voting process involves digital technology. Digitalization by itself cannot totally resolve the problems.

Also, there are numerous techniques to manipulate or alter digital technologies in order to obstruct voting. Fairness, independence, and impartiality should all be present in the voting process. This research effort creates a voting system by combining digitalization and blockchain technology after analyzing the aforementioned issues. Our voting system's primary objectives are to provide voter security, anonymity, privacy, and integrity. Our suggested digital voting systems have accomplished data integrity, voter anonymity, privacy, and security through the use of merkle trees and fingerprint hashes.

Decentralized E-voting system based on Smart Contract by using Blockchain Technology by Ali Mansour Al-madani, Ashok T. Gaikwad, Vivek Mahale, Zeyad A.T. Ahmed

The use of the Internet is expanding today, and some nations have adopted the electronic voting system since it cuts down on the time and expense associated with traditional voting. A web browser and a server are necessary when the voter wants to use the web application to access the E-voting system. The voter accesses a centralized database via a web browser. Due to the use of a central database system and the fact that the voting results are not displayed in real time, there are certain security concerns with the use of a centralized database for the voting system. The goal of this study is to use blockchain to create a highly secure E-voting system. A decentralized paradigm offered by blockchain makes the network dependable, secure, adaptable, and able to provide real-time services.

A Secure Decentralized Trustless E-Voting System Based on Smart Contract by Jiazhuo Lyu, Zoe L. Jiang, Xuan Wang, Zhenhao Nong, Man Ho Au, Junbin Fang

E-voting is very important for social activities. The privacy of each voter and the credibility of the voting results are always the top priorities when creating a secure e-voting system. In this work, we design a decentralized smart contract-based trustless electronic voting system. A trustworthy public message board and trusted computing environment are provided by the smart contract on Blockchain to ensure the accuracy of the vote results. Linkable ring signatures are used to group a signing ring for each voter in order to conceal the identity of

each voter and prevent duplicate voting. Moreover, threshold encryption without a trusted third party is used to make secret-key covertly prior to the tally stage in order to ensure that all voters will see the voting result simultaneously or that nobody can obtain it. Furthermore, all voters have equal access to the authority (faith) of the voting system. The outcome won't be impacted, even when some of them are nasty. The Ethereum private network is where the contract is implemented. Furthermore, offered are some feasibility and cost analyses related to money and time.

Blockchain-Based E-Voting System by Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson, Mohammad Hamdaqa, Gísli Hjálmtýsson

It has long been difficult to create a safe electronic voting system that provides the transparency and flexibility provided by electronic systems, while maintaining the fairness and privacy of present voting schemes. In this draught article, we assess a blockchain application for implementing distributed electronic voting systems. The study offers a novel blockchain-based electronic voting system that tackles some of the drawbacks of current systems and assesses some of the well-known blockchain frameworks in order to build a blockchain-based e-voting system. With the explanation of a case study, namely the election process and the deployment of a blockchain-based application, which increases security and lowers the cost of hosting a national election, we specifically assess the potential of distributed ledger technology.

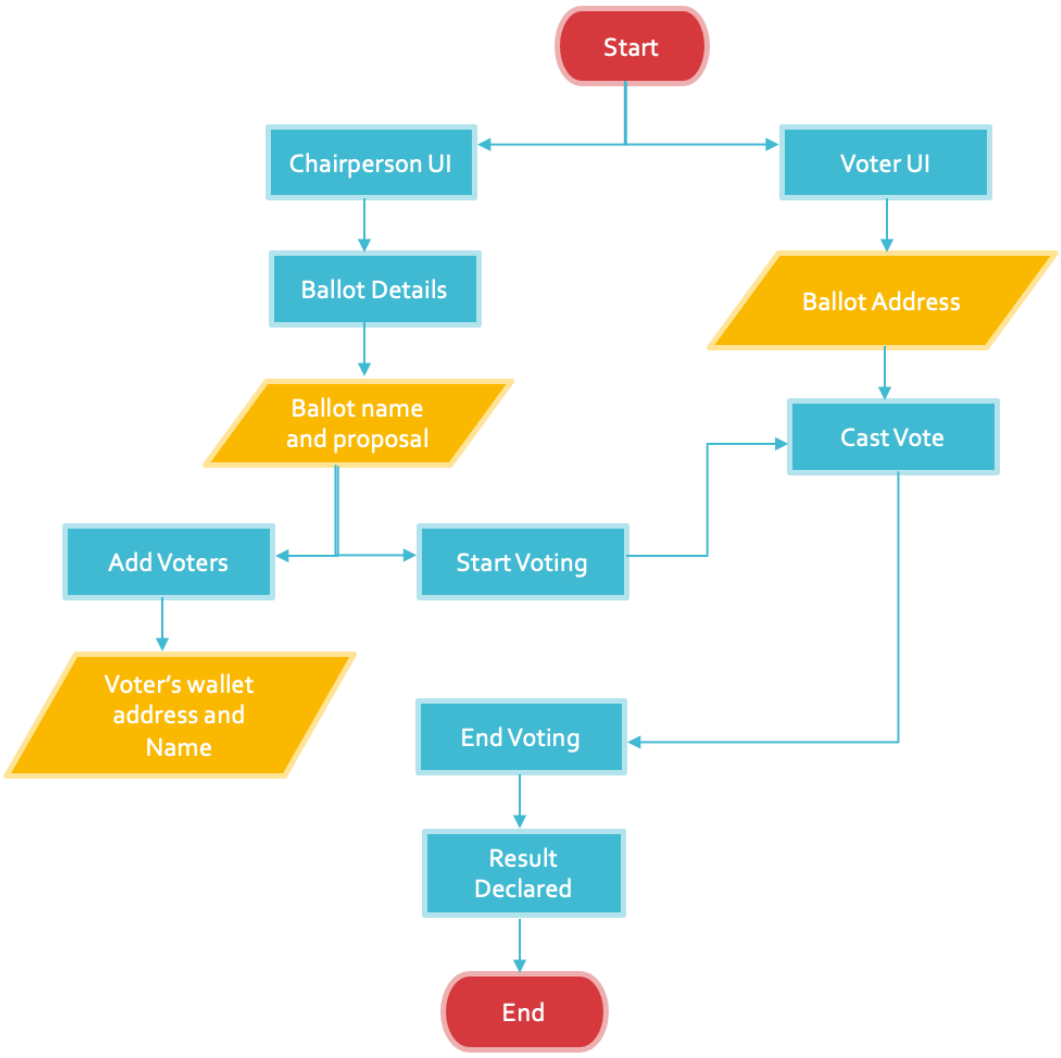
E-Voting System Using Hyperledger Fabric Blockchain and Smart Contracts by Javier Díaz-Santiso and Paula Fraga-Lamas

A new reality has emerged as a result of the present epidemic, affecting bureaucratic formalities in a variety of ways, including resource management, health security, and processes. Particularly in the election processes, where the controversy over the adoption of other more cutting-edge and contemporary options, like electronic voting, is reopened by the challenge of meeting the social distance and mobility limits (e-voting). The design and construction of a decentralized electronic voting system, which has the potential to offer a higher level of openness, security, and cost-effectiveness, are presented in this article. Votes are cast via the Hyperledger Fabric blockchain and smart contracts, which

are then recorded in an unchangeable manner to give voters anonymity and confidence in the integrity of the election process. Furthermore, encouraging outcomes of the e-voting system's performance in terms of latency and transaction load are shown.

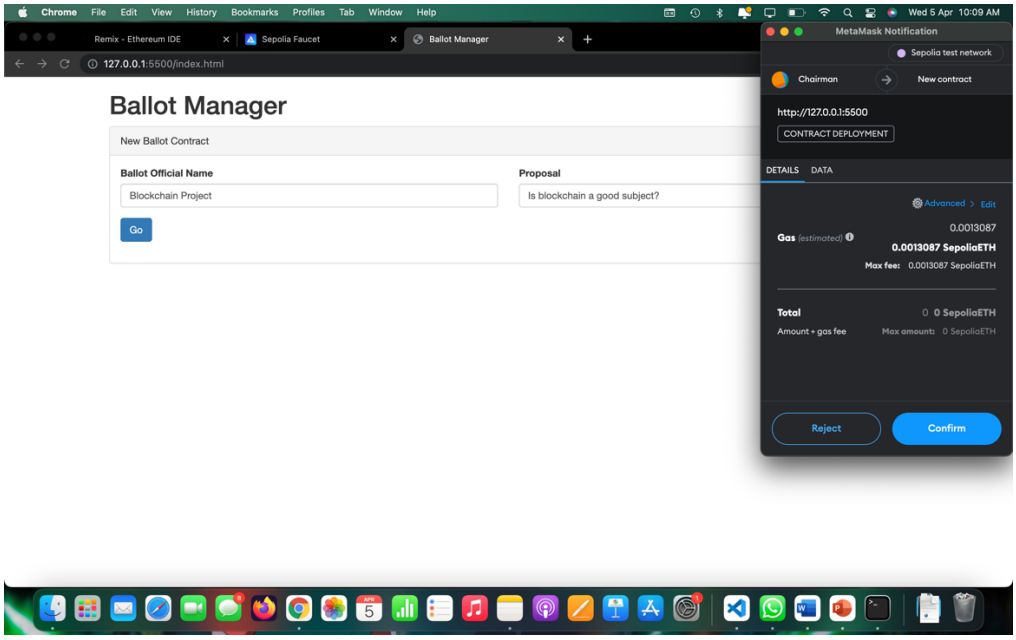
DESIGN

This project deals with creating a web application for the voting process. There will be one Chairperson for the voting process and the rest will be voters. There will be two interfaces of the web app, one for the Chairperson and the other for the voters. The Chairperson will be able to login to the web app, create a ballot, add voters, start and end the voting process. The Voters can cast their vote after entering the ballot address generated after the Chairperson proposes the ballot. After the Chairperson ends voting, results are available to everyone.

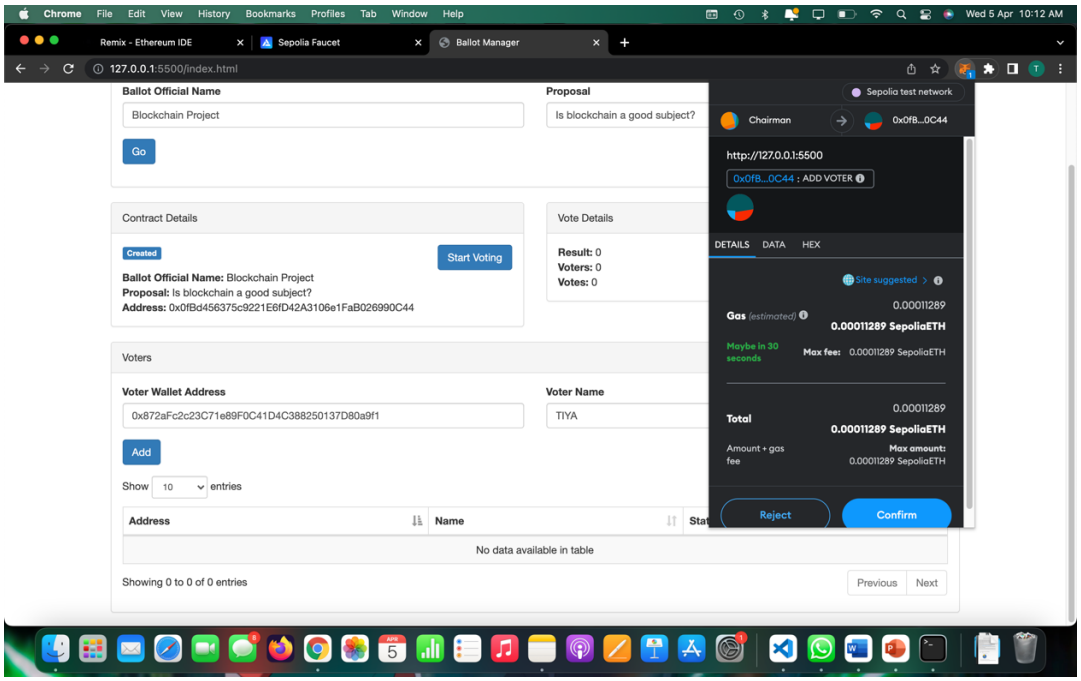


IMPLEMENTATION

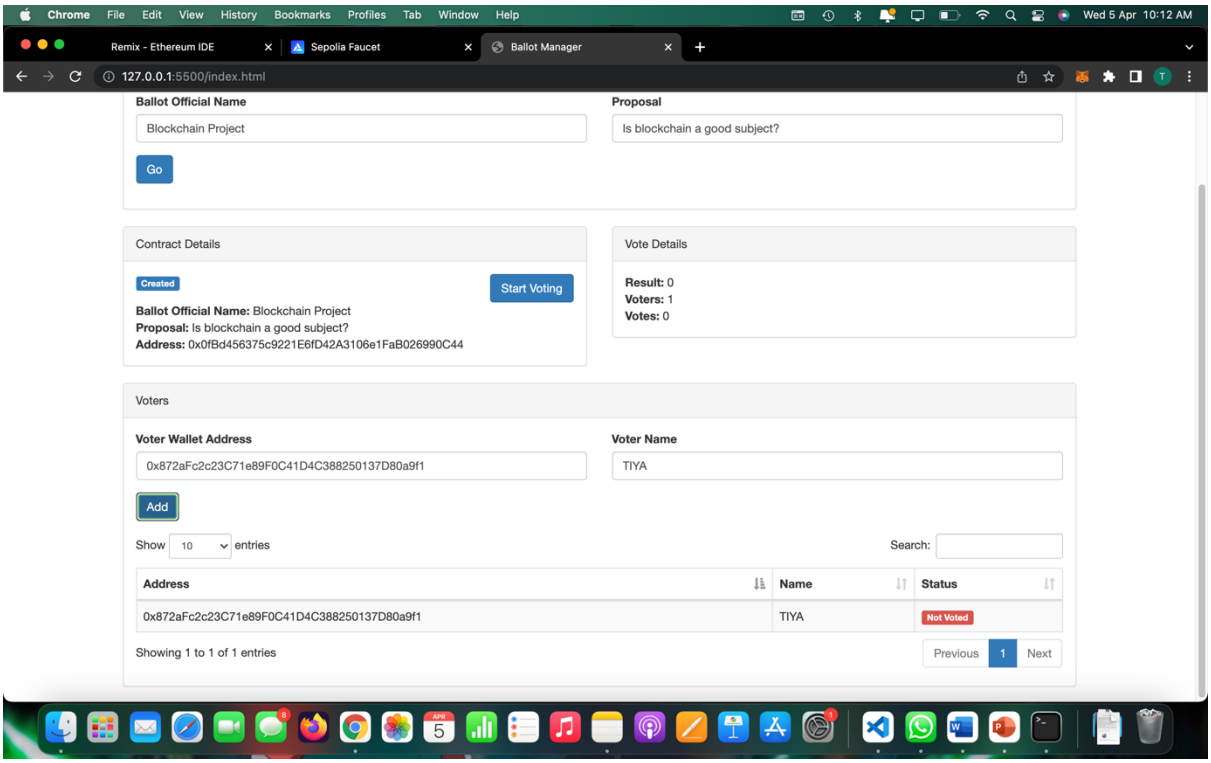
1. **Chairperson creates a new ballot** with name and proposal. When clicked on Go, MetaMask asks the chairperson to complete the transaction.



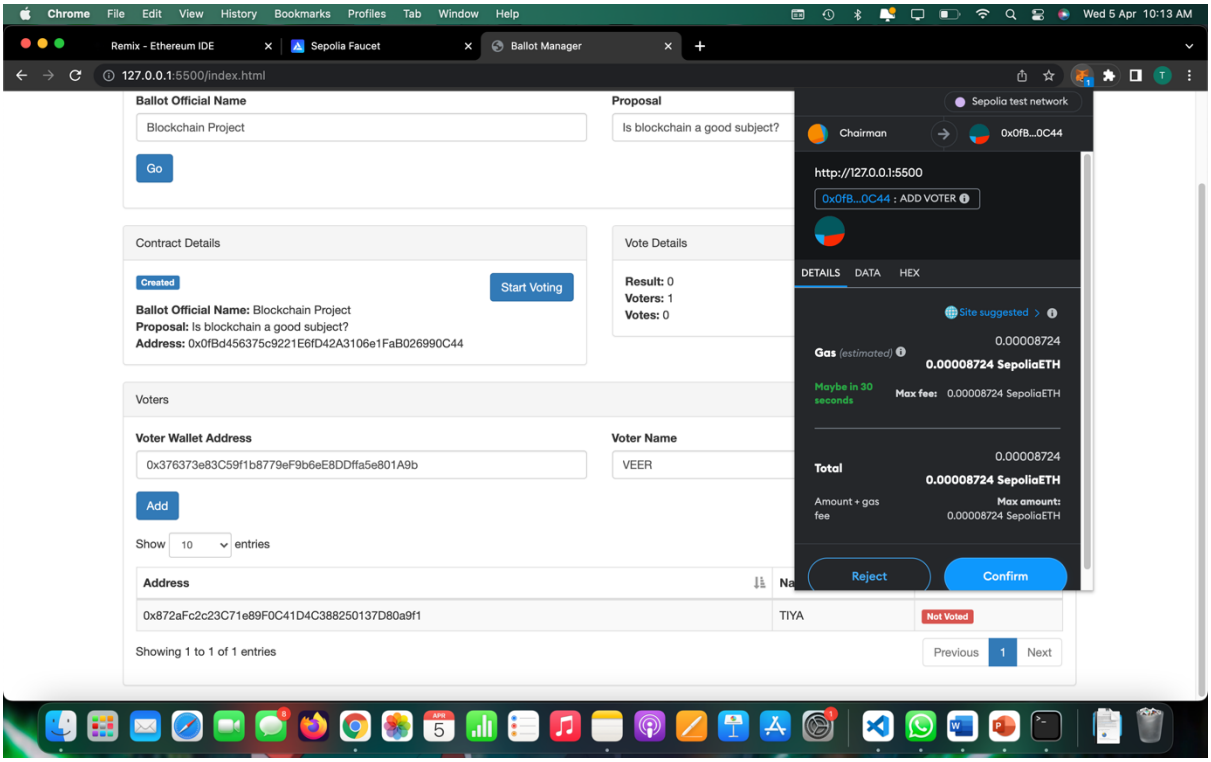
2. As the transaction is complete, options like **Add voters** and **Start voting** become available. **He adds a new voter using their wallet address.** Again, MetaMask asks the Chairperson to complete the transaction to add the voter.

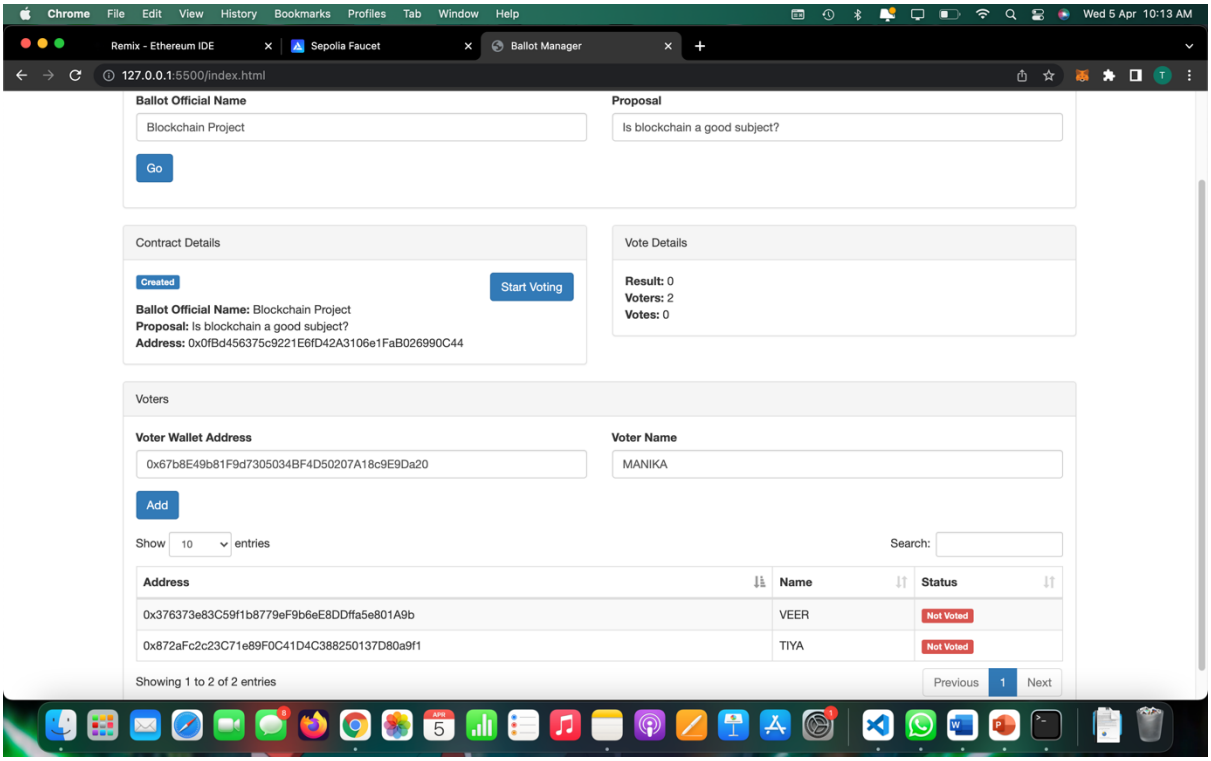


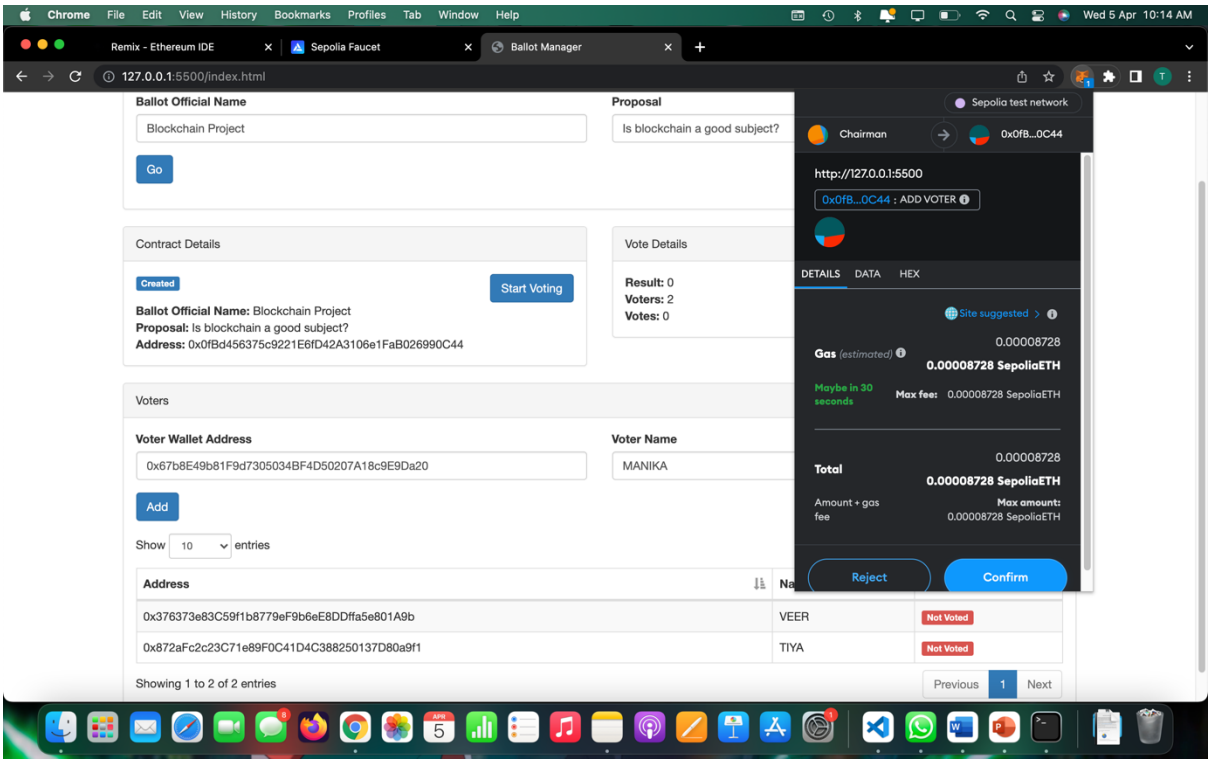
3. **Voter is added** after transaction is complete.

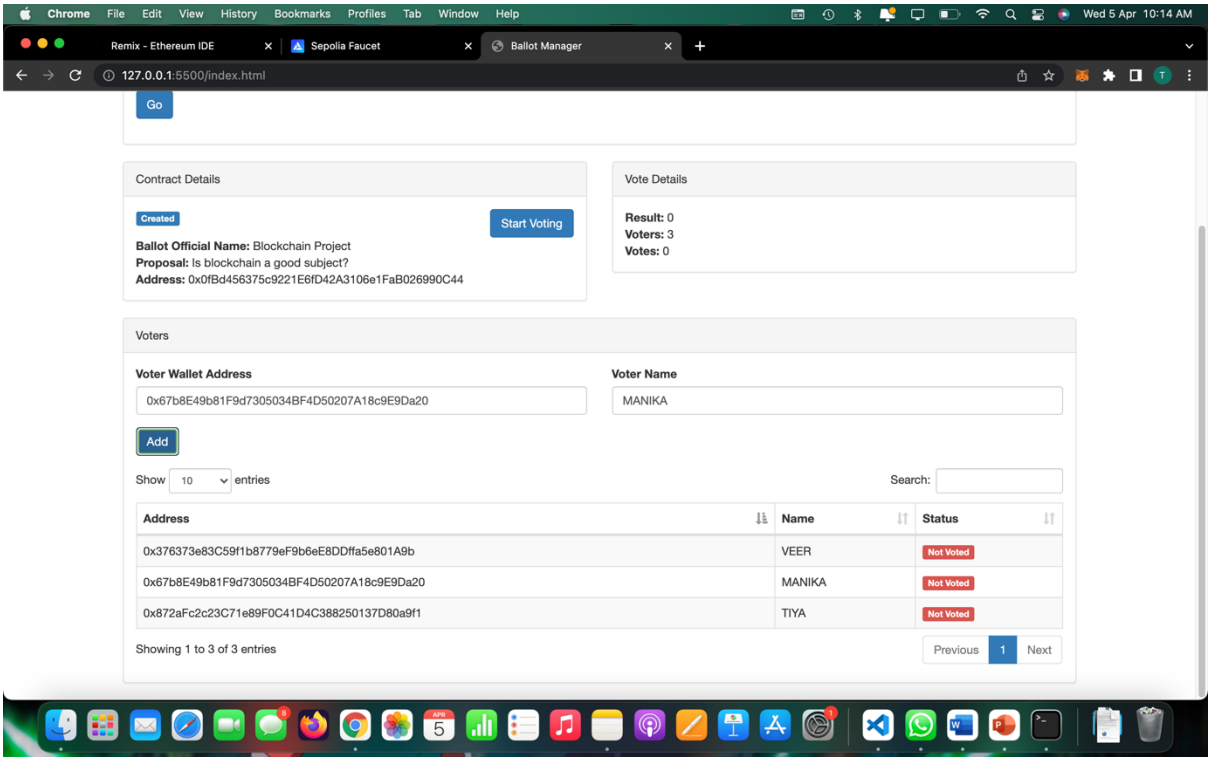


4. Two more voters are added using the same process.

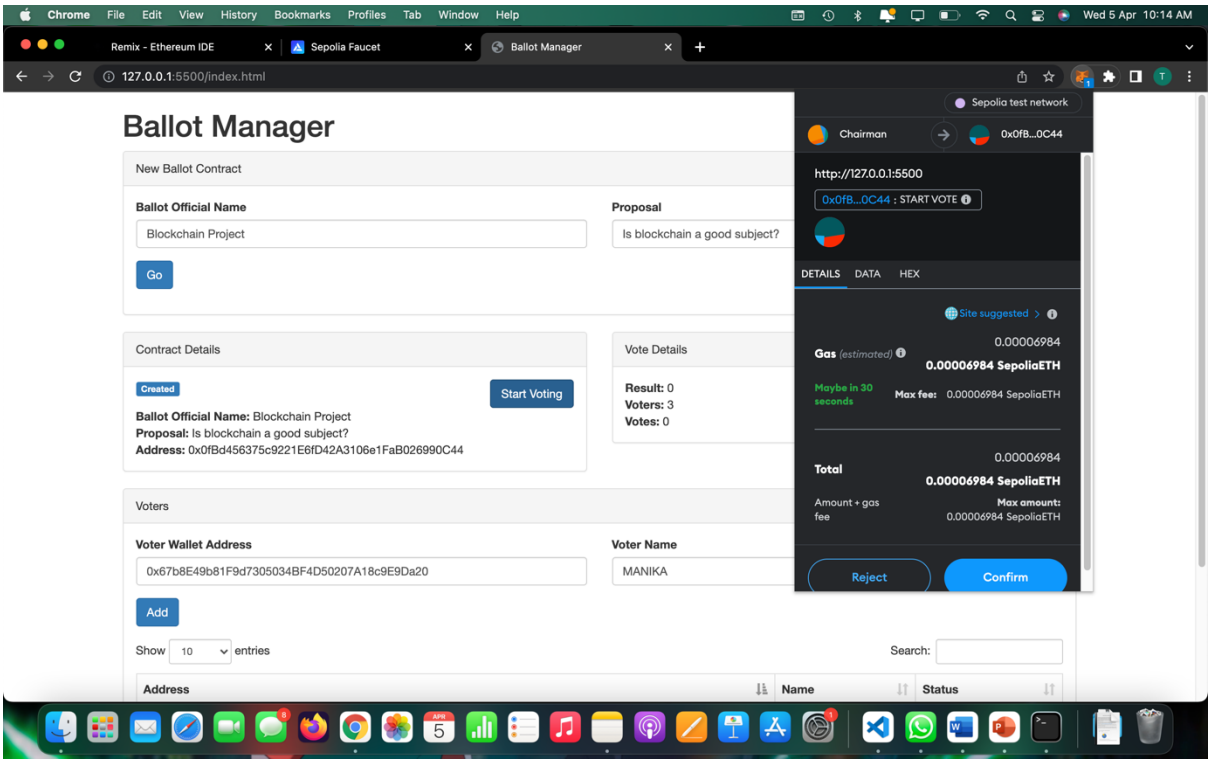



Chrome File Edit View History Bookmarks Profiles Tab Window Help
Wed 5 Apr 10:13 AM
Remix - Ethereum IDE
Sepolia Faucet
Ballot Manager
127.0.0.1:5500/index.html
Ballot Official Name
Blockchain Project
Proposal
Is blockchain a good subject?
Go
Contract Details
Created
Start Voting
Ballot Official Name: Blockchain Project
Proposal: Is blockchain a good subject?
Address: 0x0fBd456375c9221E6fD42A3106e1FaB026990C44
Vote Details
Result: 0
Voters: 2
Votes: 0
Voters
Voter Wallet Address
0x67b8E49b81F9d7305034BF4D50207A18c9E9Da20
Voter Name
MANIKA
Add
Show 10 entries
Search:
Address
Name
Status
0x376373e83C59f1b8779eF9b6eE8DDffa5e801A9b
VEER
Not Voted
0x872aFc2c23C71e89F0C41D4C388250137D80a9f1
TIYA
Not Voted
Showing 1 to 2 of 2 entries
Previous
1
Next

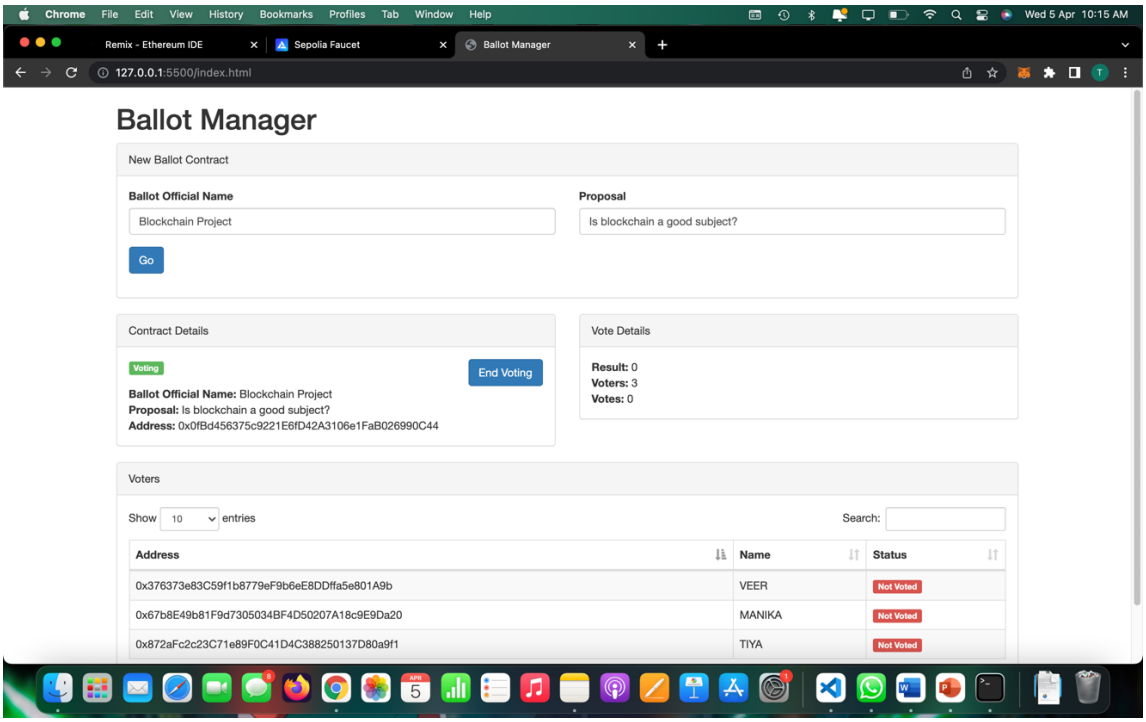

Chrome File Edit View History Bookmarks Profiles Tab Window Help
Wed 5 Apr 10:14 AM
Remix - Ethereum IDE
Sepolia Faucet
Ballot Manager
127.0.0.1:5500/index.html
Ballot Official Name
Blockchain Project
Proposal
Is blockchain a good subject?
Go
Sepolia test network
Chairman
0x0fB...0C44
http://127.0.0.1:5500
0x0fB...0C44 : ADD VOTER
DETAILS
DATA
HEX
Site suggested
Gas (estimated)
0.00008728
0.00008728 SepoliaETH
Maybe in 30 seconds
Max fee: 0.00008728 SepoliaETH
Total
0.00008728
0.00008728 SepoliaETH
Amount + gas fee
Max amount:
0.00008728 SepoliaETH
Reject
Confirm
Contract Details
Created
Start Voting
Ballot Official Name: Blockchain Project
Proposal: Is blockchain a good subject?
Address: 0x0fBd456375c9221E6fD42A3106e1FaB026990C44
Vote Details
Result: 0
Voters: 2
Votes: 0
Voters
Voter Wallet Address
0x67b8E49b81F9d7305034BF4D50207A18c9E9Da20
Voter Name
MANIKA
Add
Show 10 entries
Address
0x376373e83C59f1b8779eF9b6eE8DDffa5e801A9b
VEER
Not Voted
0x872aFc2c23C71e89F0C41D4C388250137D80a9f1
TIYA
Not Voted
Showing 1 to 2 of 2 entries
Previous
1
Next



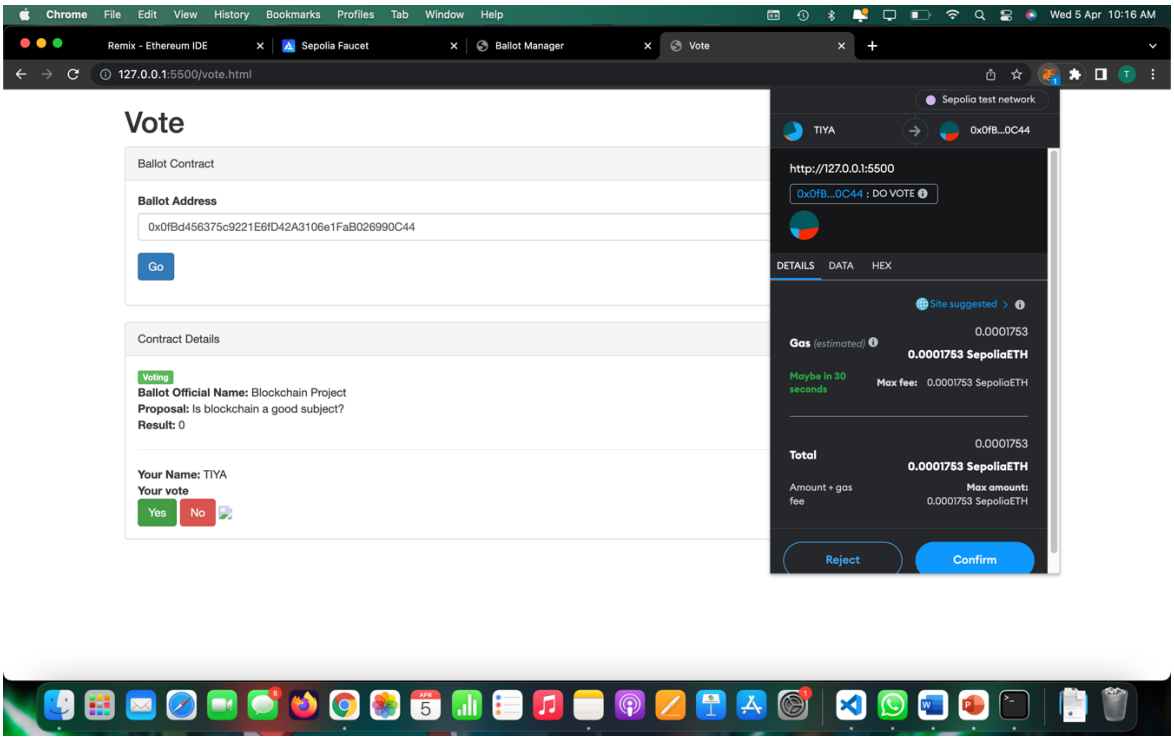
5. All the voters are added, and the Chairperson now clicks on **Start Voting** to start the process. Again, a transaction is to be made by the Chairperson.



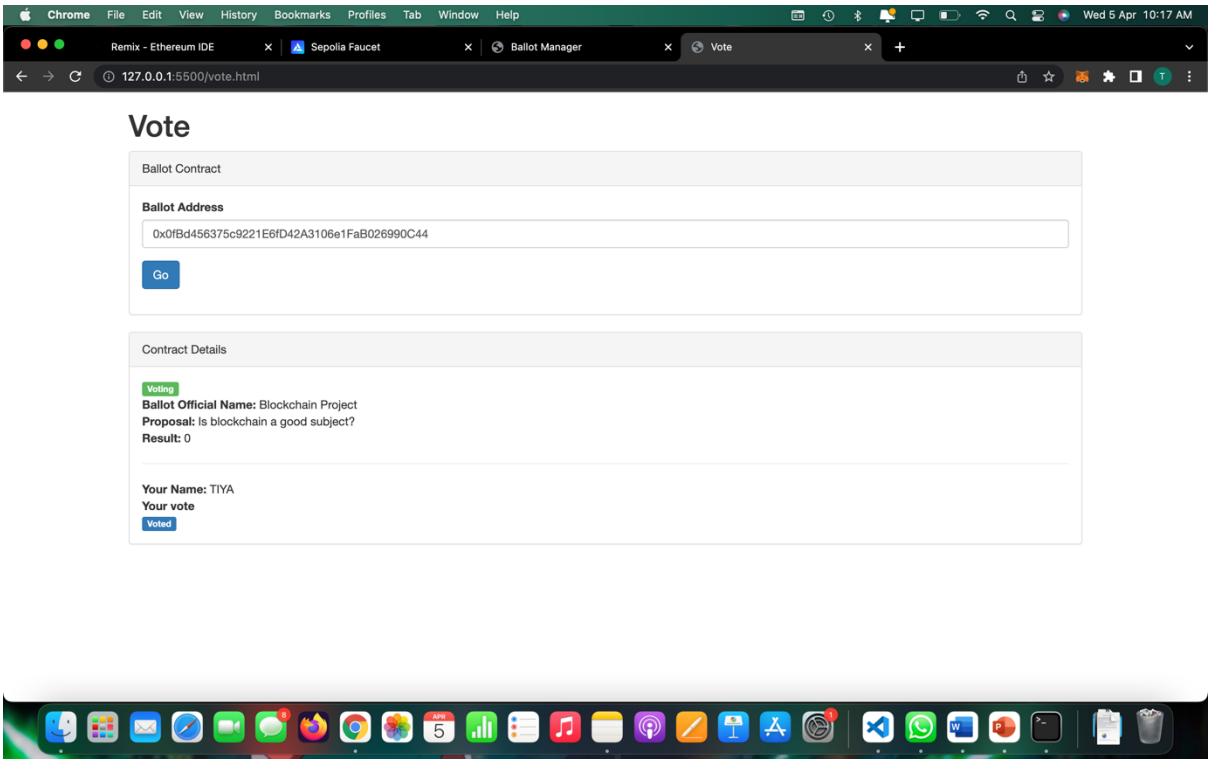
6. The voting process has now started and the Start Voting button changes to End Voting.



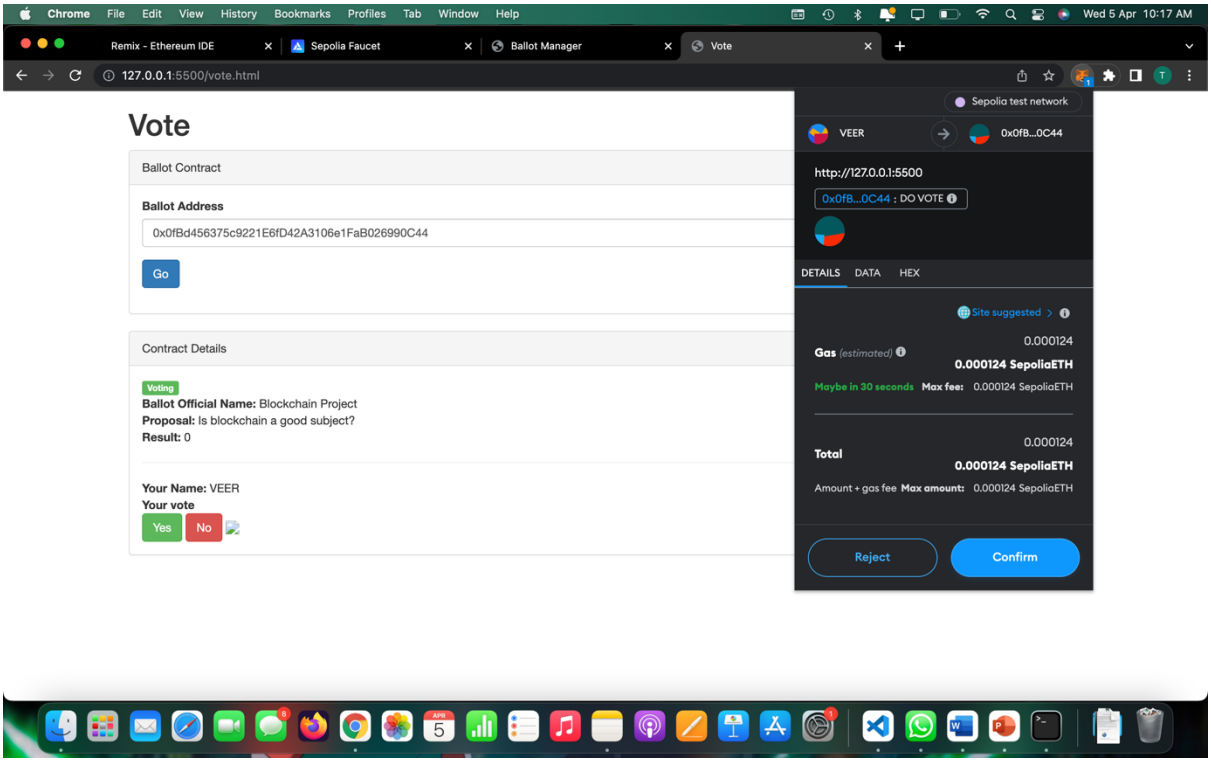
7. In the Voter interface, the ballot address is entered. The voter who's MetaMask account is opened is asked to cast the vote. To cast the vote, voter needs to confirm the transaction.

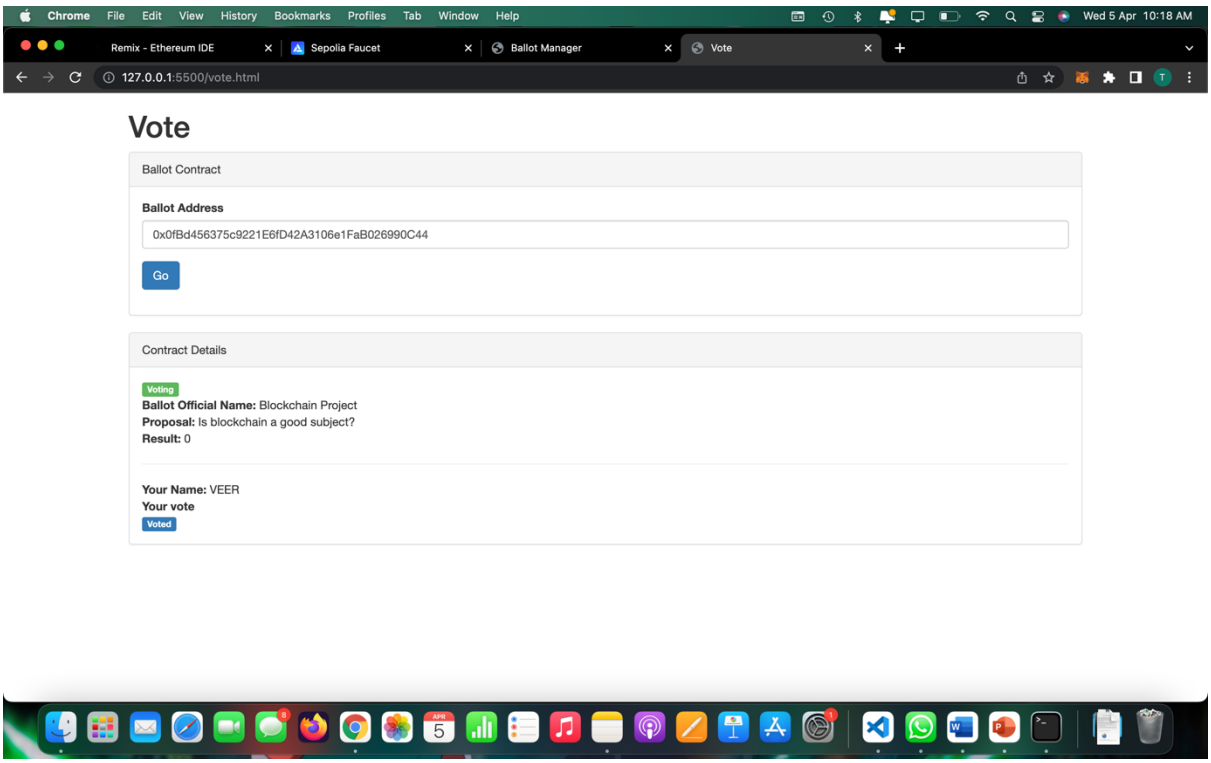


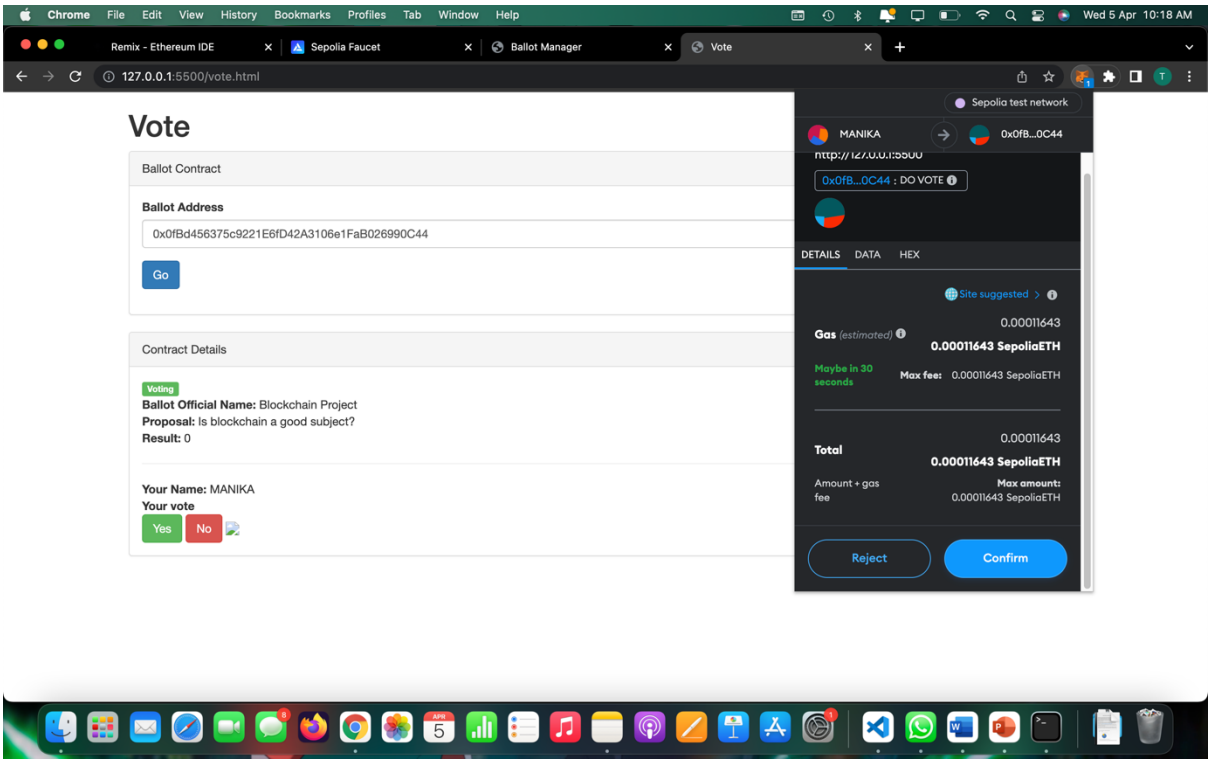
8. The vote is casted after the transaction is confirmed.

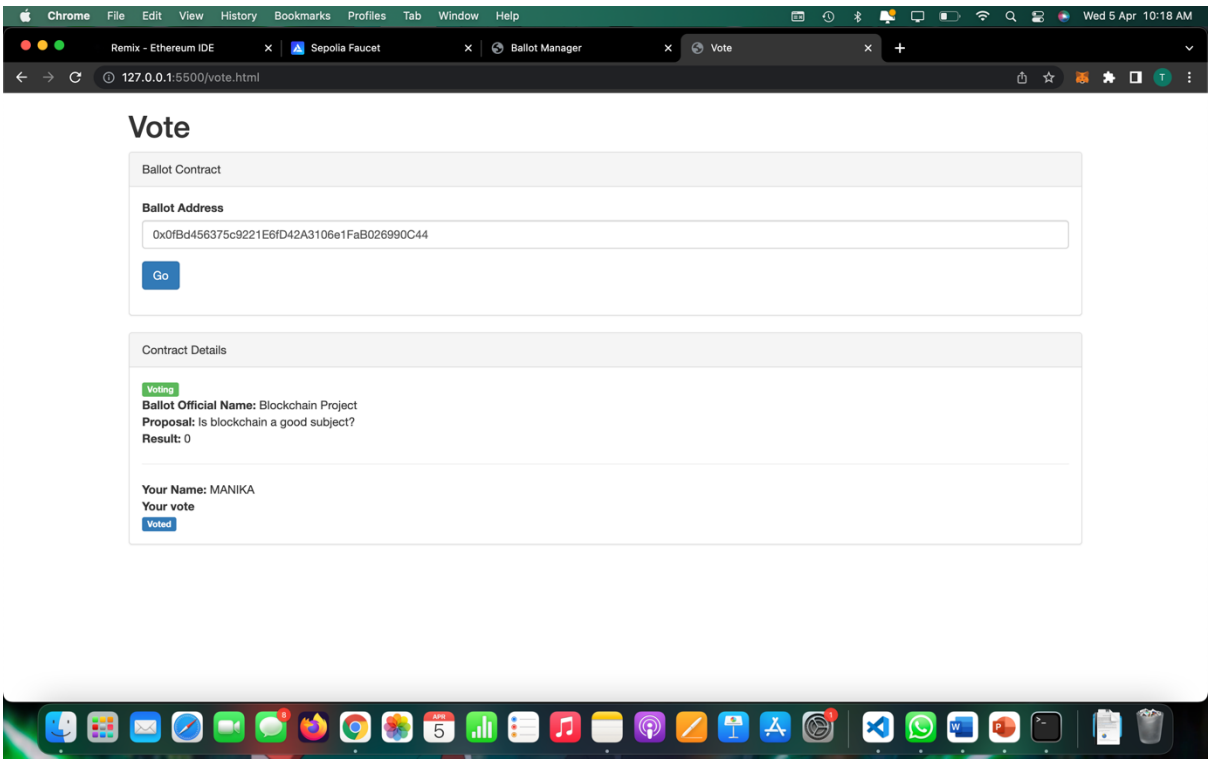


9. Same is repeated for the other 2 voters.

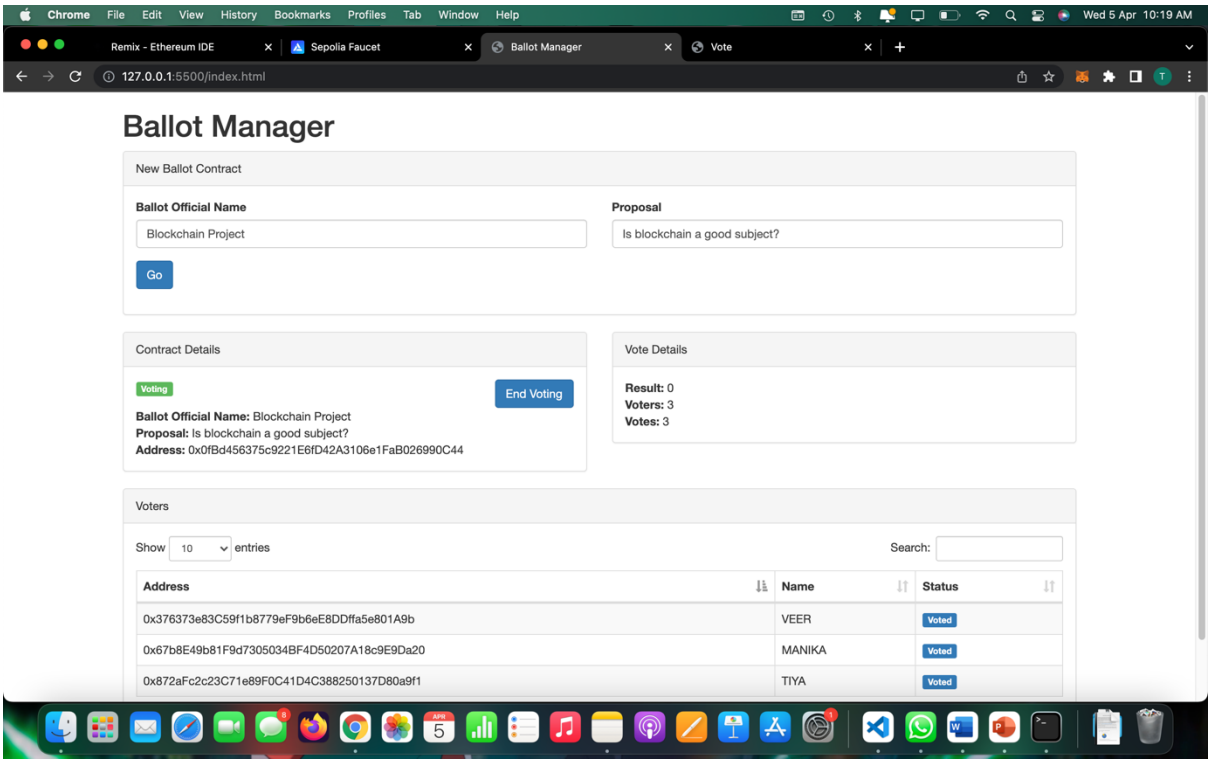



Chrome File Edit View History Bookmarks Profiles Tab Window Help
Wed 5 Apr 10:18 AM
Remix - Ethereum IDE
Sepolia Faucet
Ballot Manager
Vote
127.0.0.1:5500/vote.html
Vote
Ballot Contract
Ballot Address
0x0fBd456375c9221E6fD42A3106e1FaB026990C44
Go
Contract Details
Voting
Ballot Official Name: Blockchain Project
Proposal: Is blockchain a good subject?
Result: 0
Your Name: VEER
Your vote
Voted

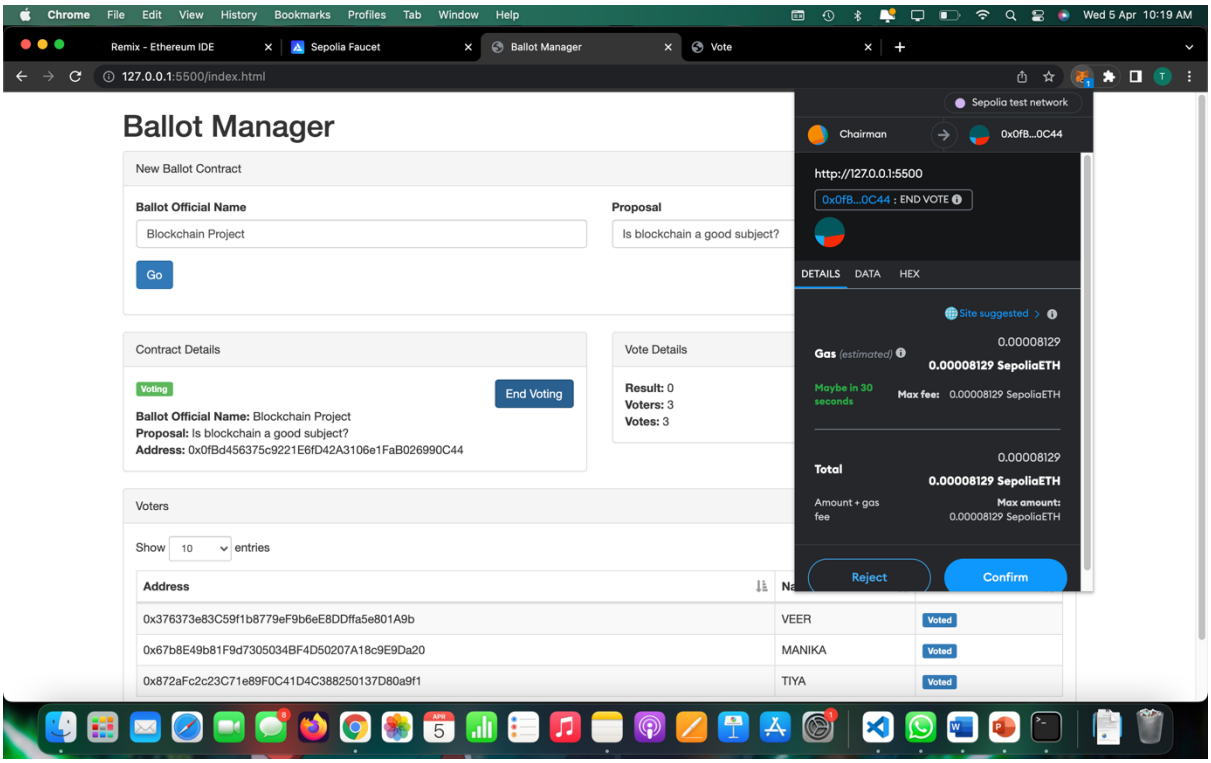

Chrome File Edit View History Bookmarks Profiles Tab Window Help
Wed 5 Apr 10:18 AM
Remix - Ethereum IDE
Sepolia Faucet
Ballot Manager
Vote
127.0.0.1:5500/vote.html
Vote
Ballot Contract
Ballot Address
0x0fBd456375c9221E6fD42A3106e1FaB026990C44
Go
Contract Details
Voting
Ballot Official Name: Blockchain Project
Proposal: Is blockchain a good subject?
Result: 0
Your Name: MANIKA
Your vote
Yes
No
Sepolia test network
MANIKA
0x0fB...0C44
0x0fB...0C44 : DO VOTE
DETAILS
DATA
HEX
Site suggested
Gas (estimated)
0.00011643
0.00011643 SepoliaETH
Maybe in 30 seconds
Max fee: 0.00011643 SepoliaETH
Total
0.00011643
0.00011643 SepoliaETH
Amount + gas fee
Max amount:
0.00011643 SepoliaETH
Reject
Confirm



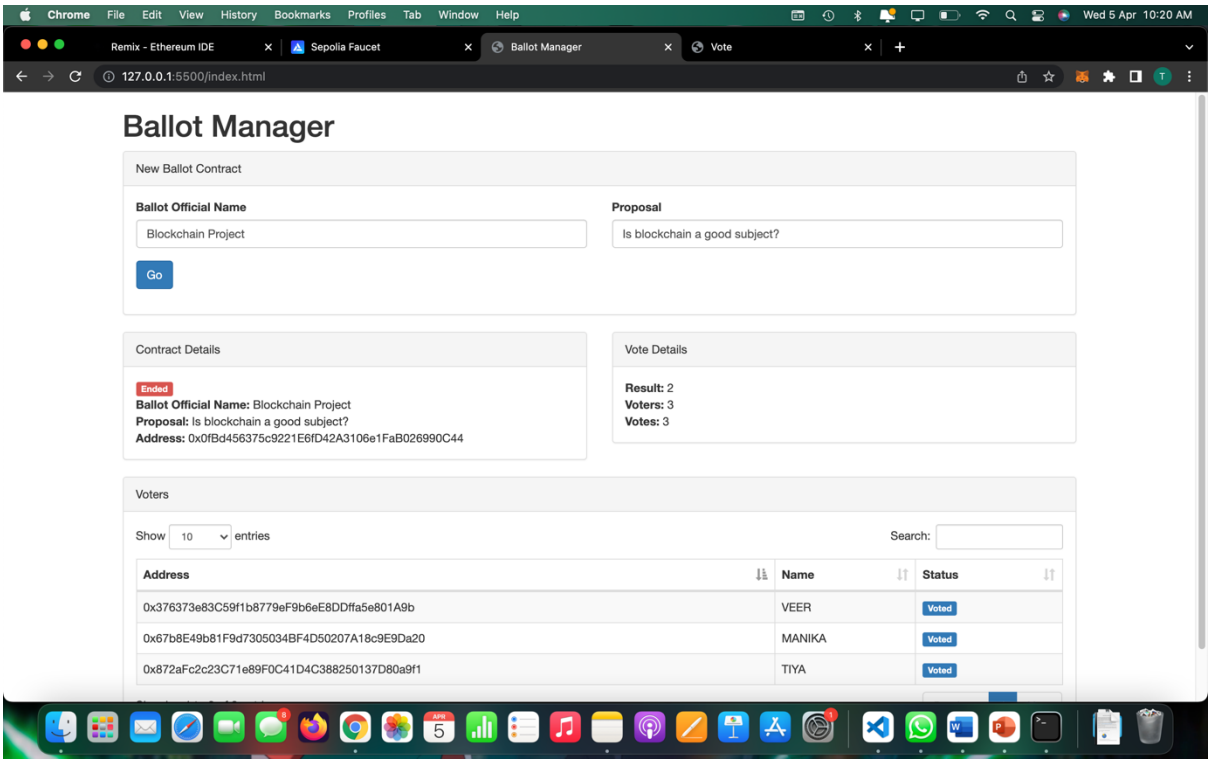
10. Now all the voters have voted and the chairperson can see that in the Voters table. Now the Chairperson can end the voting process.



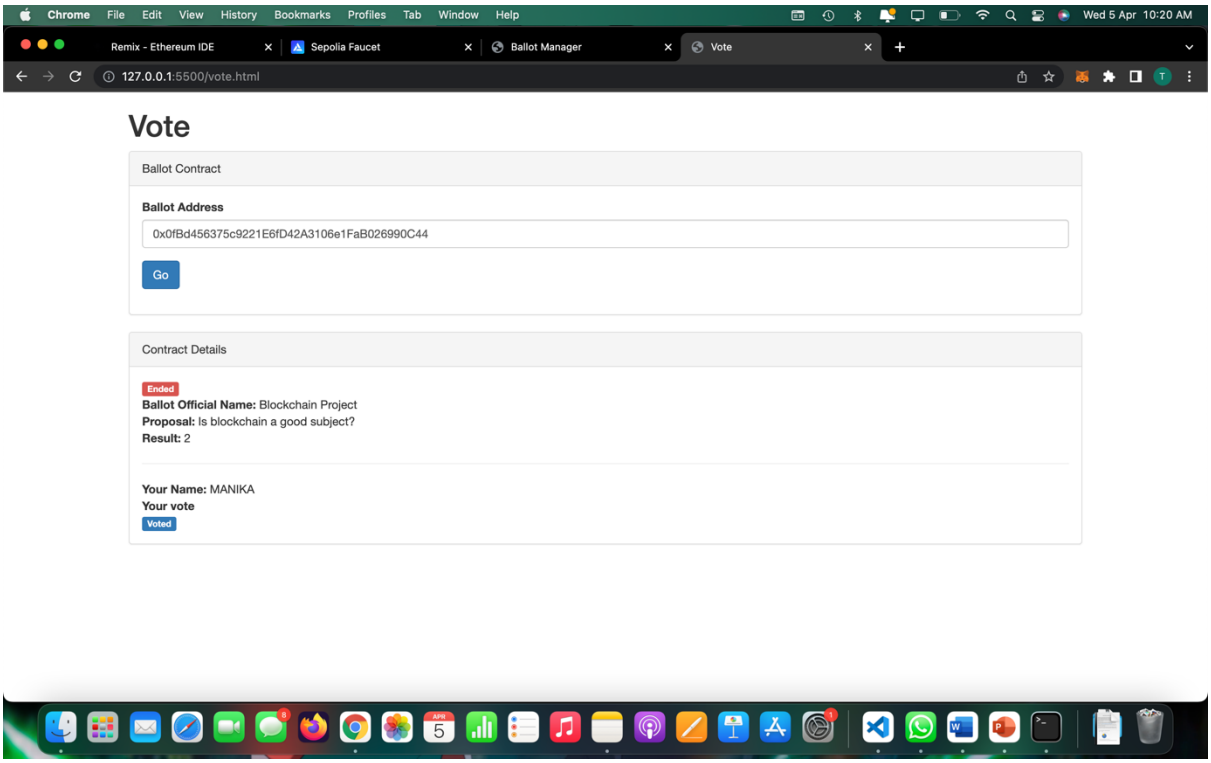
11. After clicking on the End Voting button, a transaction needs to be confirmed.



12. The voting has now ended and results are declared which shows Result: 2. This means 2 votes are in favor (Yes).



13.Results are also displayed on the voter interface.



RESULT AND DISCUSSION

This project is a successful implementation of a decentralized voting system using blockchain technology. The system ensures transparency, immutability, and security in the voting process. The Chairperson has full control over the voting process and can monitor it in real-time. The voters can cast their votes without fear of tampering or fraud, and the results are available to everyone once the Chairperson ends the voting process.

The web application was built using HTML, CSS, JavaScript, and Web3.js. The smart contract was written in Solidity, and the blockchain used was Ethereum. The web app was hosted on a local server using Python's **http.server** module. The Chairperson interface provided a simple and intuitive way for the Chairperson to create a ballot, add voters, start and end the voting process. The ballot creation process was straightforward, and the Chairperson had to provide the necessary details such as the ballot name, proposal, etc. The Chairperson could add voters by entering their Ethereum wallet addresses, which would enable them to cast their votes. The Chairperson could start and end the voting process at any time and could monitor the voting process in real-time.

The Voter interface allowed voters to cast their votes after entering the ballot address generated after the Chairperson proposed the ballot. The interface was user-friendly and straightforward, and the voters could vote as they wanted. The voter could only cast one vote, and once submitted, the vote was immutable and tamper-proof.

However, some limitations were observed, such as the need for voters to have Ethereum wallets and the possibility of the Chairperson adding unauthorized voters. Nonetheless, these limitations can be addressed in future versions of the project.

Overall, the project Voting System using Smart Contracts was a successful implementation of a decentralized voting system using blockchain technology. It demonstrated the potential of blockchain technology in revolutionizing the voting process and ensuring transparency, immutability, and security.

CONCLUSION

On a Blockchain, there is no single point of failure since every node in the chain contributes to keeping the chain going. When deployed on the Blockchain, a smart contract is unchangeable. When a smart contract is deployed, the business logic is set in stone. When the contract is deployed, the chairman has no power to amend the rules, such as switching from a one-man one-vote system to a one-man two-vote system. Thus, a smart contract based voting system is very reliable and better than conventional paper ballot and EVM.

REFERENCES

1. Alvi, S. T., Uddin, M. N., & Islam, L. (2020, August). Digital voting: A blockchain-based e-voting system using biohash and smart contract. In *2020 third international conference on smart systems and inventive technology (ICSSIT)* (pp. 228-233). IEEE.
2. Al-Madani, A. M., Gaikwad, A. T., Mahale, V., & Ahmed, Z. A. (2020, October). Decentralized E-voting system based on Smart Contract by using Blockchain Technology. In *2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and*

Computing (ICSIDEMPC) (pp. 176-180). IEEE.

3. Lyu, J., Jiang, Z. L., Wang, X., Nong, Z., Au, M. H., & Fang, J. (2019, August). A secure decentralized trustless E-voting system based on smart contract. In *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)* (pp. 570-577). IEEE.
4. Hjálmarsson, F. Þ., Hreiðarsson, G. K., Hamdaqa, M., & Hjálmtýsson, G. (2018, July). Blockchain-based e-voting system. In *2018 IEEE 11th international conference on cloud computing (CLOUD)* (pp. 983-986). IEEE.
5. Díaz-Santiso, J., & Fraga-Lamas, P. (2021). E-Voting System Using Hyperledger Fabric Blockchain and Smart Contracts. *Engineering Proceedings*, *7*(1), 11.
6. 1.What is a smart contract? Available at *https://blockchainhub.net/smart-contracts/*
7. 2. TechCrunch, (2018). Liquid democracy uses blockchain to fix politics, and now you can vote for it [Online]. Available at: *https://techcrunch.com/2018/02/24/liquid-democracy-uses-blockchain/*
8. 3. Geth.ethereum.org. (2018). Go Ethereum. Available at: https://geth.ethereum.org/

SOURCE CODE FOR SMART CONTRACTS

```
pragma solidity ^0.5.0;

contract Ballot {
    struct vote{
        address voterAddress;
        bool choice;
    }

    struct voter{
        string voterName;
        bool voted;
    }

    uint private countResult = 0;
    uint public finalResult = 0;
    uint public totalVoter = 0;
    uint public totalVote = 0;
```

```
    address public ballotOfficialAddress;
    string public ballotOfficialName;
    string public proposal;

    mapping(uint => vote) private votes;
    mapping(address => voter) public voterRegister;

    enum State { Created, Voting, Ended }
    State public state;

    //creates a new ballot contract
    constructor(
        string memory _ballotOfficialName,
        string memory _proposal) public {
        ballotOfficialAddress = msg.sender;
        ballotOfficialName = _ballotOfficialName;
        proposal = _proposal;

        state = State.Created;

    }

    modifier condition(bool _condition){
        require(_condition);
        _;
    }

    modifier onlyOfficial() {
        require(msg.sender ==ballotOfficialAddress);
        _;
    }

    modifier inState(State _state) {
        require(state == _state);
        _;
    }

    event voterAdded(address voter);
    event voteStarted();
    event voteEnded(uint finalResult);
    event voteDone(address voter);

    //add voter
    function addVoter(address _voterAddress, string memory _voterName)
        public
        inState(State.Created)
        onlyOfficial
    {
        voter memory v;
        v.voterName = _voterName;
        v.voted = false;
```

```
        voterRegister[_voterAddress] = v;
        totalVoter++;
        emit voterAdded(_voterAddress);
    }

    //declare voting starts now
    function startVote()
        public
        inState(State.Created)
        onlyOfficial
    {
        state = State.Voting;
        emit voteStarted();
    }

    //voters vote by indicating their choice (true/false)
    function doVote(bool _choice)
        public
        inState(State.Voting)
        returns(bool voted)
    {
        bool found = false;
        if (bytes(voterRegister[msg.sender].voterName).length != 0 &&
!voterRegister[msg.sender].voted){
            voterRegister[msg.sender].voted = true;
            vote memory v;
            v.voterAddress = msg.sender;
            v.choice = _choice;
            if(_choice){
                countResult++; //counting on the go
            }
            votes[totalVote] = v;
            totalVote++;
            found = true;
        }
        emit voteDone(msg.sender);
        return found;
    }

    //end votes
    function endVote()
        public
        inState(State.Voting)
        onlyOfficial
    {
        state = State.Ended;
        finalResult = countResult; //move result from private countResult to public
finalResult
        emit voteEnded(finalResult);
    }
}
```

PLAGIARISM CHECK

https://papersowl.com/free-plagiarism-checker