Blockchain-based Virtual Voting System

MINOR PROJECT - II

Submitted by:

Prateek Vats (9919103005)
Prabhash Singh (9919103177)
Raghav Bansal (9919103180)
Rana Aishwarya Pratap Singh (9919103198)

Under the supervision of:

Dr. Payal Khurana Batra
Assistant Professor (Senior Grade)

Department of CSE/IT
Jaypee Institute of Information Technology University ,Noida

May 2022

ACKNOWLEDGEMENT

I would like to place on record my deep sense of gratitude to **Dr. Payal Khurana Batra**, **Assistant Professor (Senior Grade)**, Jaypee Institute of Information Technology, India for her generous guidance, help and useful suggestions.

Prateek Vats (9919103005)
Prabhash Singh (9919103177)
Raghav Bansal (9919103180)
Rana Aishwarya Pratap Singh (9919103198)

DECLARATION

We hereby declare that this submission is our own work and that, to the best of our knowledge and beliefs, it contains no material previously published or written by another person nor material.

Place: Noida
Date: 08-05-2022

Name: **Prateek Vats**
Enrolment No.: **9919103005**

Name: **Prabhash Singh**
Enrolment No.:**9919103177**

Name: **Raghav Bansal**
Enrolment No.: **9919103180**

Name: **Rana Aishwarya Pratap Singh**
Enrolment No.: **9919103198**

CERTIFICATE

This is to certify that the work titled “Blockchain-based Virtual Voting System” is submitted by **Prateek Vats(9919103005),Prabhash Singh(9919103177), Raghav Bansal(9919103180), Rana Aishwarya Pratap Singh(9919103198)** of B.Tech of Jaypee Institute of Information Technology, Noida has been carried out under my supervision.

Dr. Payal Khurana Batra
Assistant Professor (Senior Grade)

Abstract

Building a secure electronic voting system that offers the fairness and privacy of current voting schemes, while providing the transparency and privacy offered by electronic systems has been a challenge for a long time. In this project, we evaluate an application of blockchain as a service to implement distributed electronic voting systems. which improves the security and decreases the cost of hosting a nationwide election.

The purpose of this research project is to develop a decentralized e-voting system that incorporates blockchain technology and encryption to achieve decentralized e-voting without the need for a trusted third party. The voting process is transparent and public while protecting voter anonymity, the privacy of data transmission, and the verifiable results of the voting..

Table of Contents

Introduction

After every election, EVM has been in the news over the last few years as politicians and activists have raised questions about the lack of transparency and authenticity of election results. There is a sense of Question raised on transport without appropriate security of EVM.

Electronic voting machines (EVMs) were supposed to be the cure for the malady of booth-capturing in elections in India, but in the present form of use, they have only worsened the problems. Moreover, EVMs also do not meet the legal requirements set out in the Information Technology Act, 2000.

The duties of the ECI as set out in Article 324 of the Constitution include ensuring that elections conducted by it are free and fair and reflect the will of the voters. But what is. There can be so many reasons. One is whether the majority of the country wanted this or the election might be rigged. To cover this point of perspective we have to come up with a better voting system so that major citizens of the state/Country can ensure that the candidate they voted for gets elected.
Blockchain can ensure voter anonymity, vote confidentiality and end-to-end verification which will lead to better efficiency and trustability in the voting system.

Moving to vote online can make the process more comfortable, more flexible, and accessible to more people. However, the current electronic voting system EVMs and Ballot papers are vulnerable to data compromise and thus resulting in voting manipulations.
A blockchain can help in addressing these risks. This technology has the potential for enhancing the security of voters' personal data, increasing the transparency of the voting process, and making it easier to verify election results.

WHAT IS BLOCKCHAIN?
The blockchain is a digital ledger that records information in a way that makes it difficult for hackers to alter. It provides a safe and secure way for individuals to interact directly with each other without involving third parties like governments, banks, or other institutions. The growing list of records, called blocks, is linked together using cryptography. Peer-to-peer networks verify each transaction, which is then time-stamped and added to a chain of data. Once the transaction is recorded, the data cannot be changed.

BLOCKCHAIN

- ➢ Block chain is decentralized and distributed technology.
- ➢ Block chain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system.
- ➢ Any transaction or activity done through block chain technology cannot be hacked. Since the block chain does integrity checks. When an integrity check fails it denies the process.
- ➢ Block chain achieves Authentication, Authorization, Accounting (AAA).

BLOCKCHAIN STRUCTURE

- ➤ Every block is connected with the other with the hash value
- ➤ The last value of the first block and the starting value of the second block should match.
- ➤ The very first block of the chain is known as genesis block or Oth block

How Blockchain solves voting problems.

Using blockchain, the voting process can be made more secure, transparent, immutable, and reliable. How? Let’s take an example. Suppose you are an eligible voter who goes to a polling booth and casts a vote using EVM (Electronic Voting Machine). But since it’s circuitry after all and if someone tampers with a microchip, you may never know that your vote reaches the person for whom you voted or was diverted into another candidate’s account? Since there’s no tracing back of your vote. But, if you use blockchain- it stores everything as a transaction and hence gives you a receipt of your vote (in the form of a transaction ID) and you can use it to ensure that your vote has been counted securely.

Suppose a normal digital voting system (website/app) is launched to digitize the process and all confidential data is stored on a single admin server/machine using SQL. If someone hacks or spies on it, they can change the candidate's vote count.

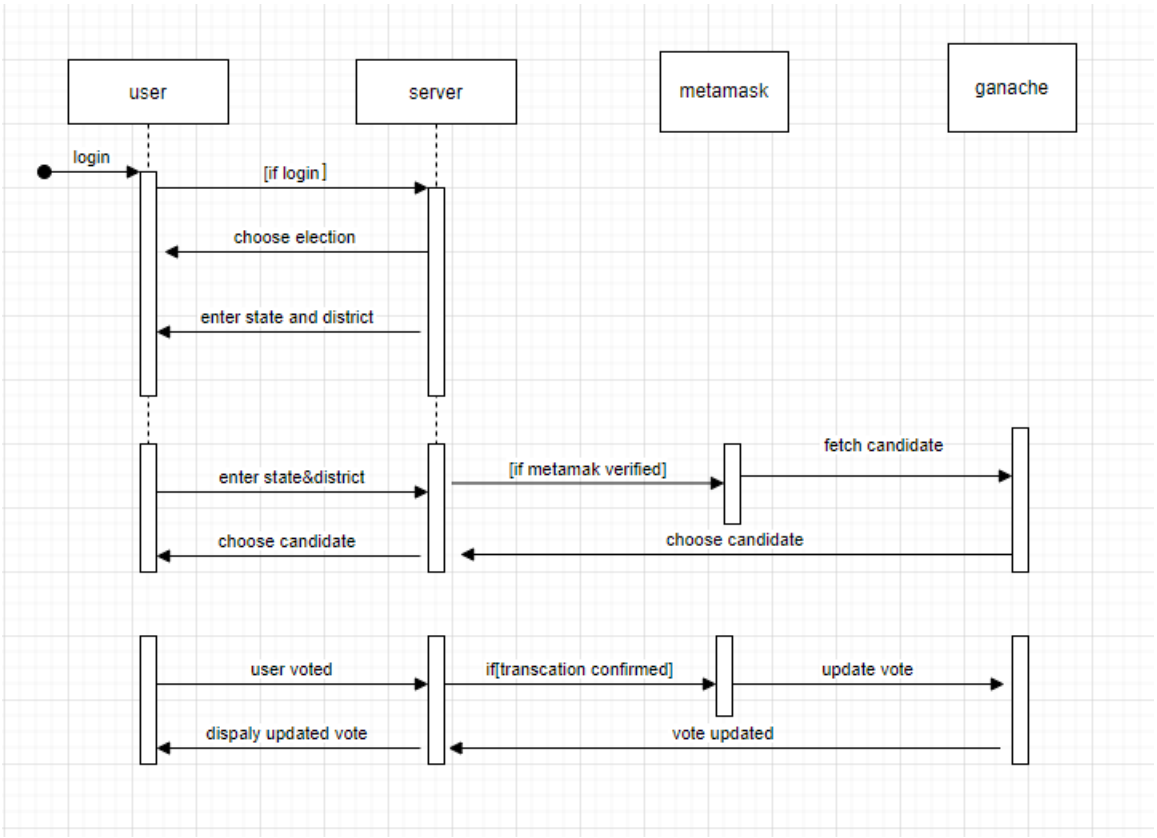
Background Study

The traditional voting process consists of manual work. In the traditional voting process for registration, voters have to come along with their national identity cards and have to wait in long queues for their turn to be verified. After the completion of the voting process, the presiding officers collect the ballot box and transfer it to the nearby counting centers for voter verification and counting. and in case of fraud or miscounting, there is no solution.

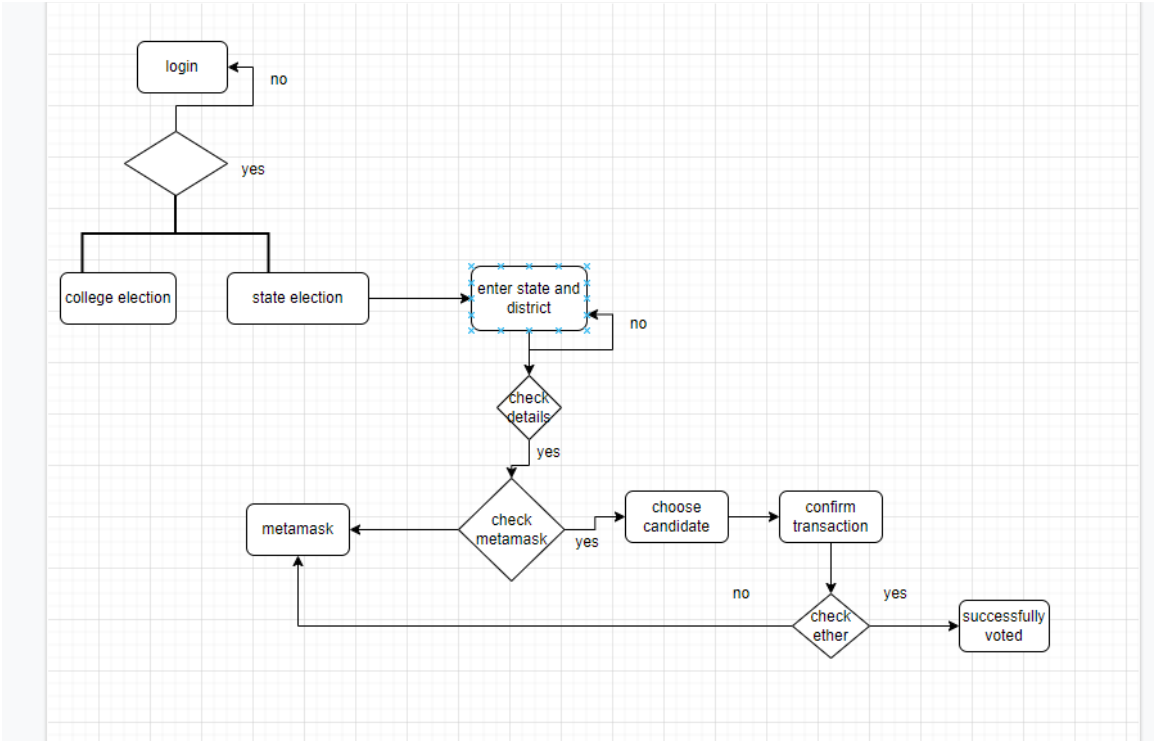
Then we had the Electronic Voting System(EVM) as the next technology but it had its problem. It came with a microchip and if someone tampers with a microchip, voters will never know that their vote reaches the person for whom they voted or was diverted into another candidate's account. To solve this issue of trust, our Blockchain-based voting system comes to the rescue. It uses distributed ledger technology which is stored in every device and is impossible to hack. In it, transparency will also be retained and counting of voting will also be stored in the blockchain which also provides fast counting.

S.No	Title	Author	Description
1	Block chain based multi party authorization for accessing IPFS encrypted data	Ammar Ayman, Mohammad moussa madine, Hamad Al Zaabi Ibrar Yaqoob, Khaled Salah, Raja Jayaraman	Implementation of a fully decentralized blockchain based multiparty authorization Pros: secure and trustable Cons: no integrity check
2	Designing authentication and authorization system using block chain technology	Yuki Ezawa, Makoto Takita, Yoshiaki Shiraishi, Shohei Kakei, Masanori Hirotomo, Misami Mohri , Masakatu Morii.	Implementation of blockchain as database for storing credentials Cons: challenges on data sharing
3	A decentralized web authentication system using ethereum based blockchain	Shibasis Patel, Anisha sahoo, Bhabendu Kumar Mohanta, Sowmyashree S Panda, Debasish	Implementation of authentication service based on ethereum blockchain called Dauth Pros: decentralized and

		Jena	tamper resistant Cons: adoption for ethereum based blockchain is low
4	An privacy - preserving cross organizational authentication/ authorization /accounting system using block chain technology	Peggy Joy Lu, Lo Yao Yeh, Jing-Long Huang.	Implementation of blockchain based AAA system for cross organizational authentication Pros: tamper proof Cons: no integrity check



Activity diagram



Requirement Analysis

Software Requirements:

1. ganache
2. truffle
3. web3
4. npm
5. solidity
6. HTML
7. javascript
8. metamask
9. MongoDB

Hardware Requirements

1. Intel 6th gen or above
2. 2GB RAM or above

Detailed Design

We have added a login authentication system with Node/ExpressJs and MongoDB Database, we have completely migrated our project to offline mode using Truffle and now our votes will be permanent instead before when we used to close the browser we used to lose our data in Blockchain but now it's permanent using Truffle and Ganache. Earlier we have used the Ethereum Ropsten test network but now we are using our local Ganache ether as they are permanently stored in our system even after restarting the system.

Metamask is a browser extension for Chrome that offers users a means to manage their local ganache accounts, Ethereum accounts, and private keys, as well as gain access to websites that utilize Web3.js.

A smart contract is a computer program or a transaction protocol that is intended to automatically execute, control or document legally relevant events and actions according to the terms of a contract or an agreement.

1.College.sol - Created a Smart Contract which is a set of rules which are stored on a blockchain and automatically executes when called on the blockchain.

2.Frontend- Created desired HTML files for frontend with CSS/bootstrap and added functionality for voting with javascript and it connects it with solidity

3. Ganache - Open/Run Ganache and create a new workspace

4. Metamask - Open metamask import accounts from ganache local blockchain

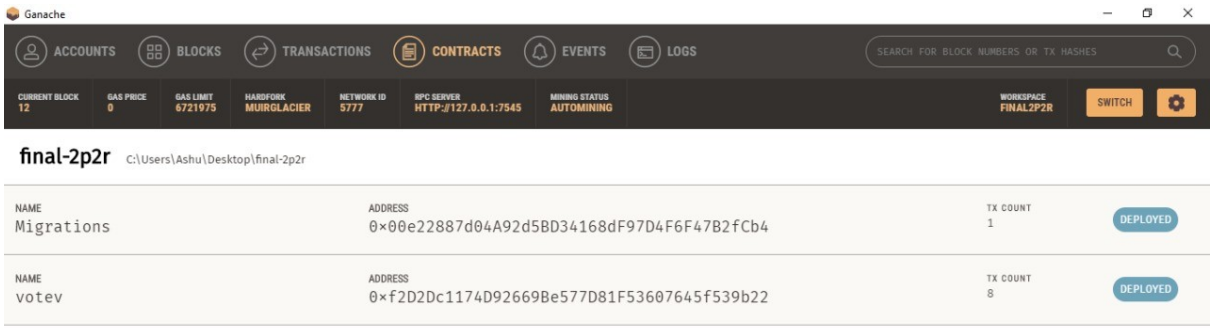
5. Mongodb - Open Mongodb create database and documents

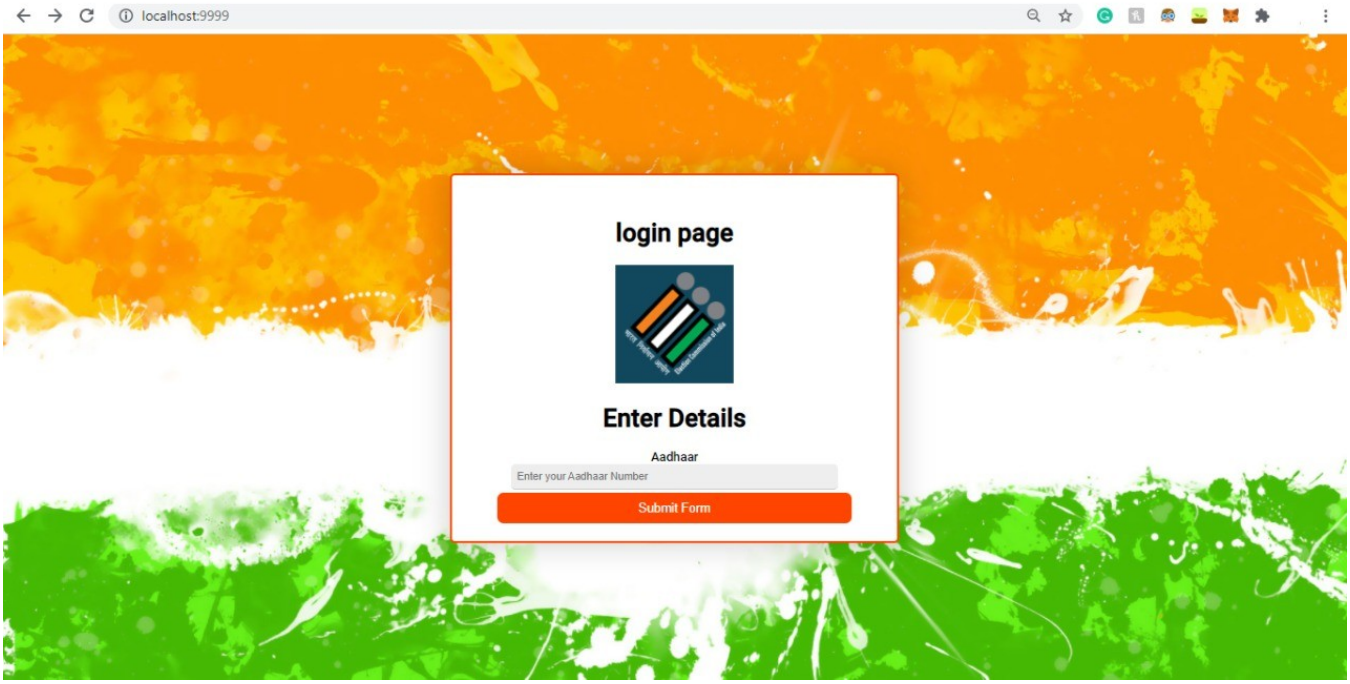
6. Server.js - Create Connection with MongoDB.and give the desired location for static files

7. Run nodemon server.js

Implementation

First, we deploy smart contracts on the blockchain

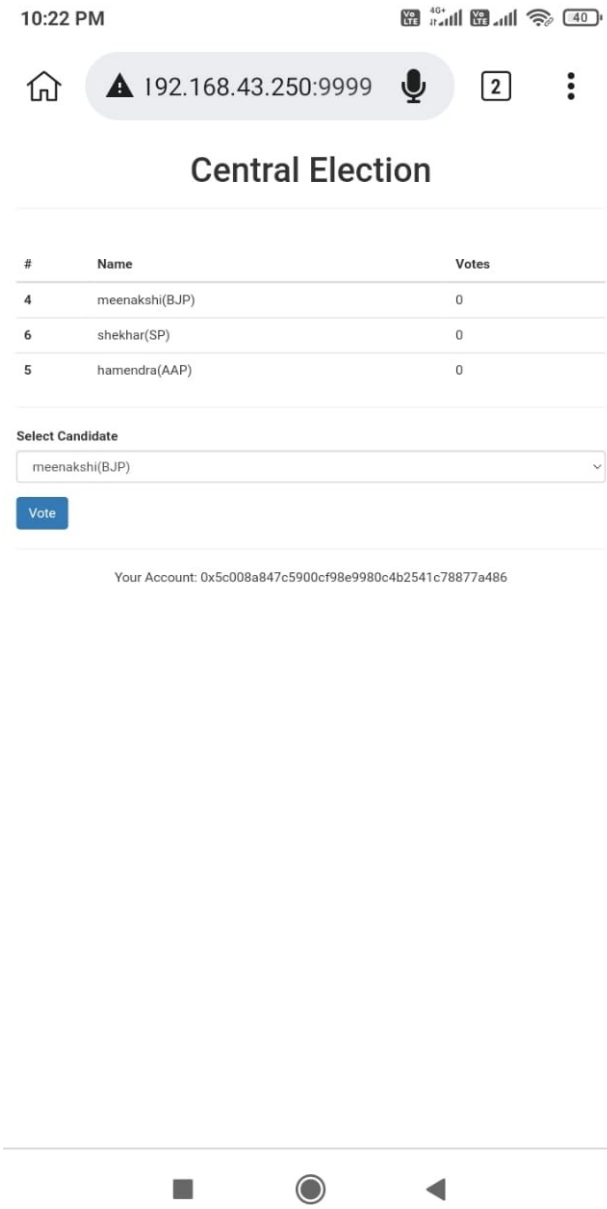




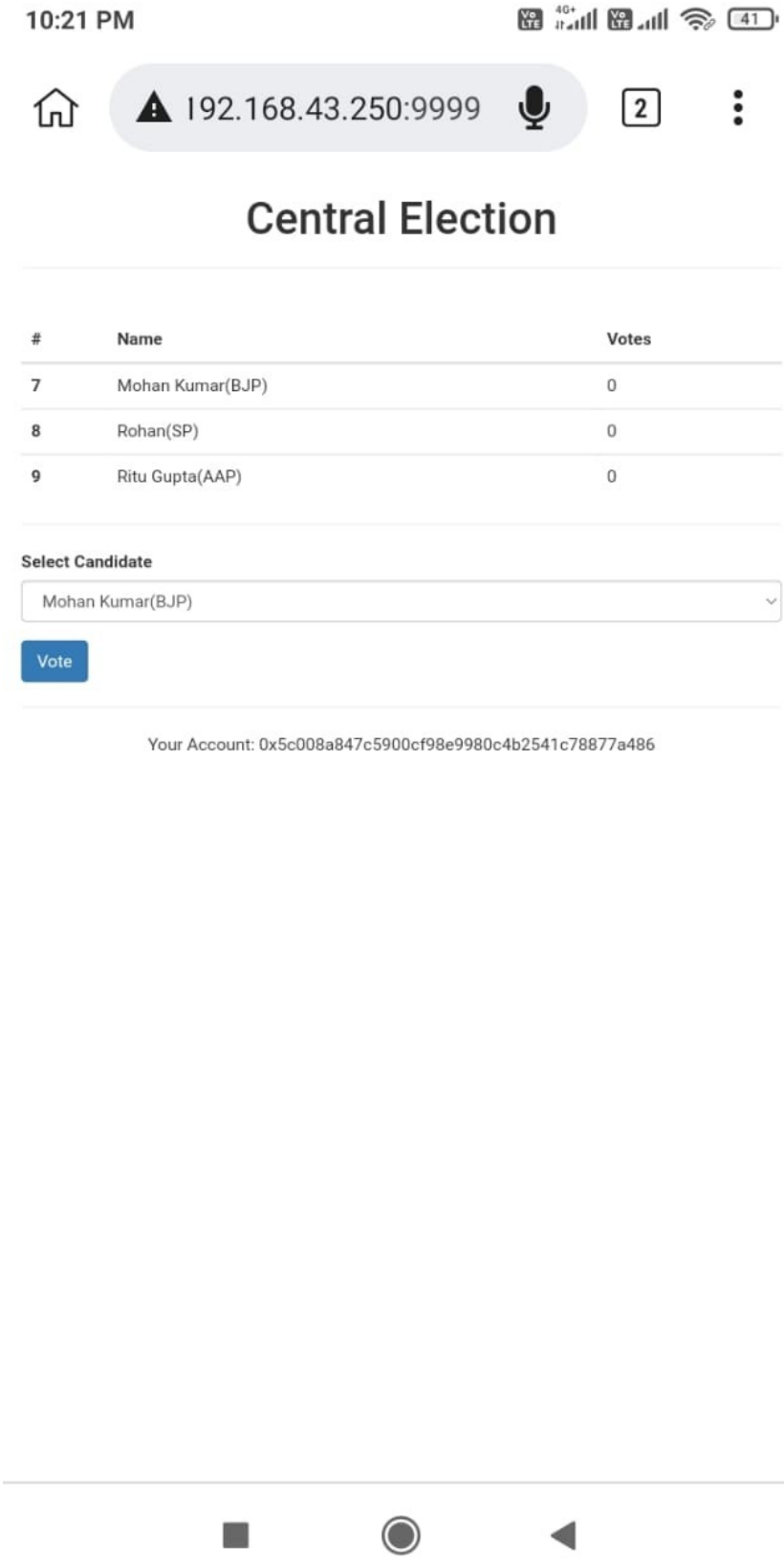
Select your state and district


11:24 PM
192.168.43.250:9999
2
vote
Vote India
state
up
district
gautambudhnagar
Vote

We have selected : UP and District:Gautam Budh Nagar

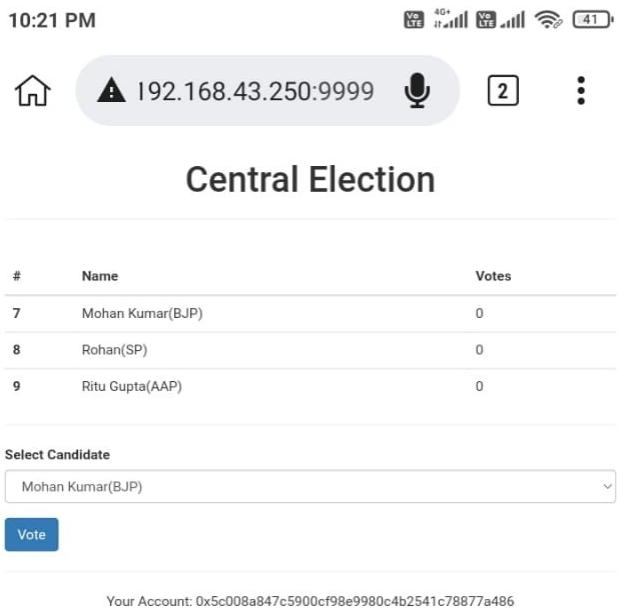


We have selected : Rajasthan and District:Alwar

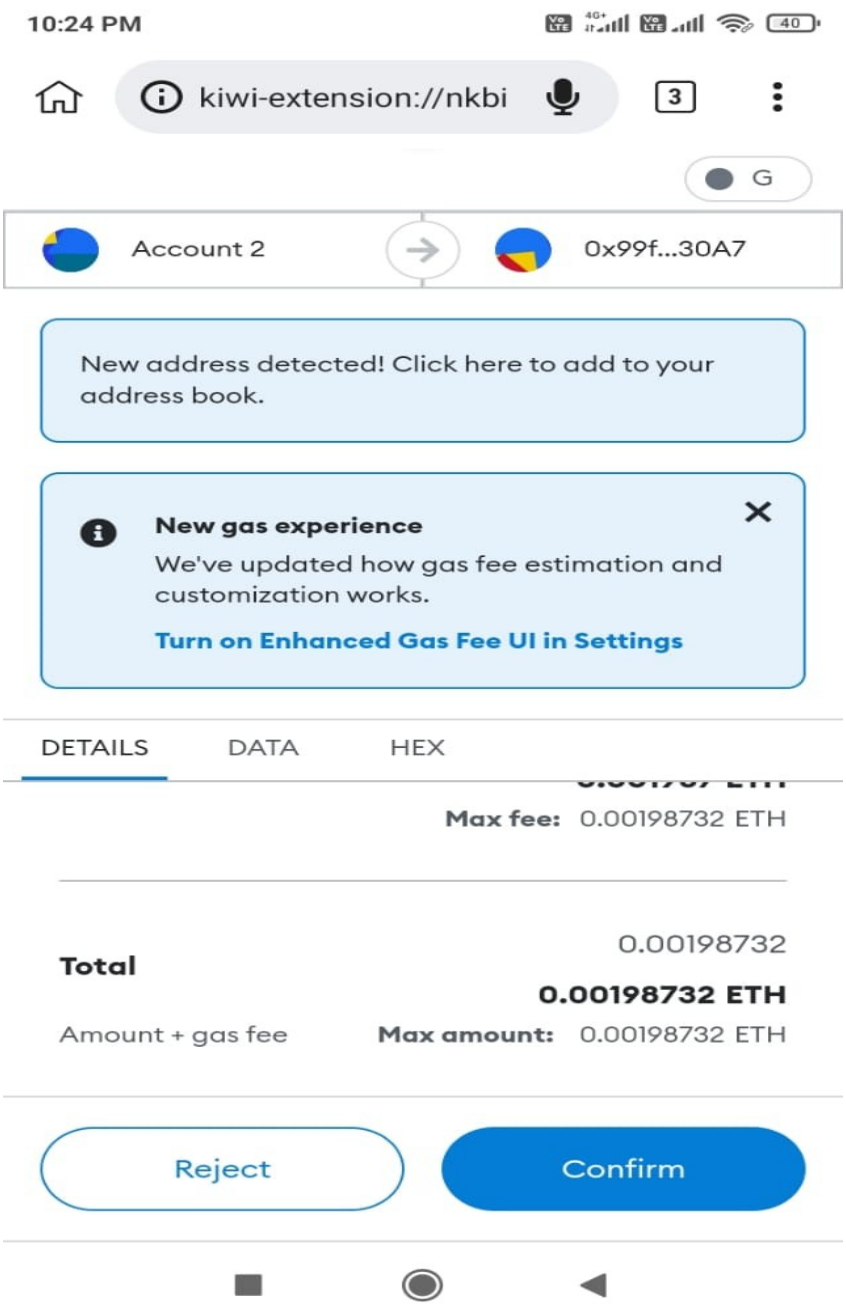


Experimental Results and Analysis

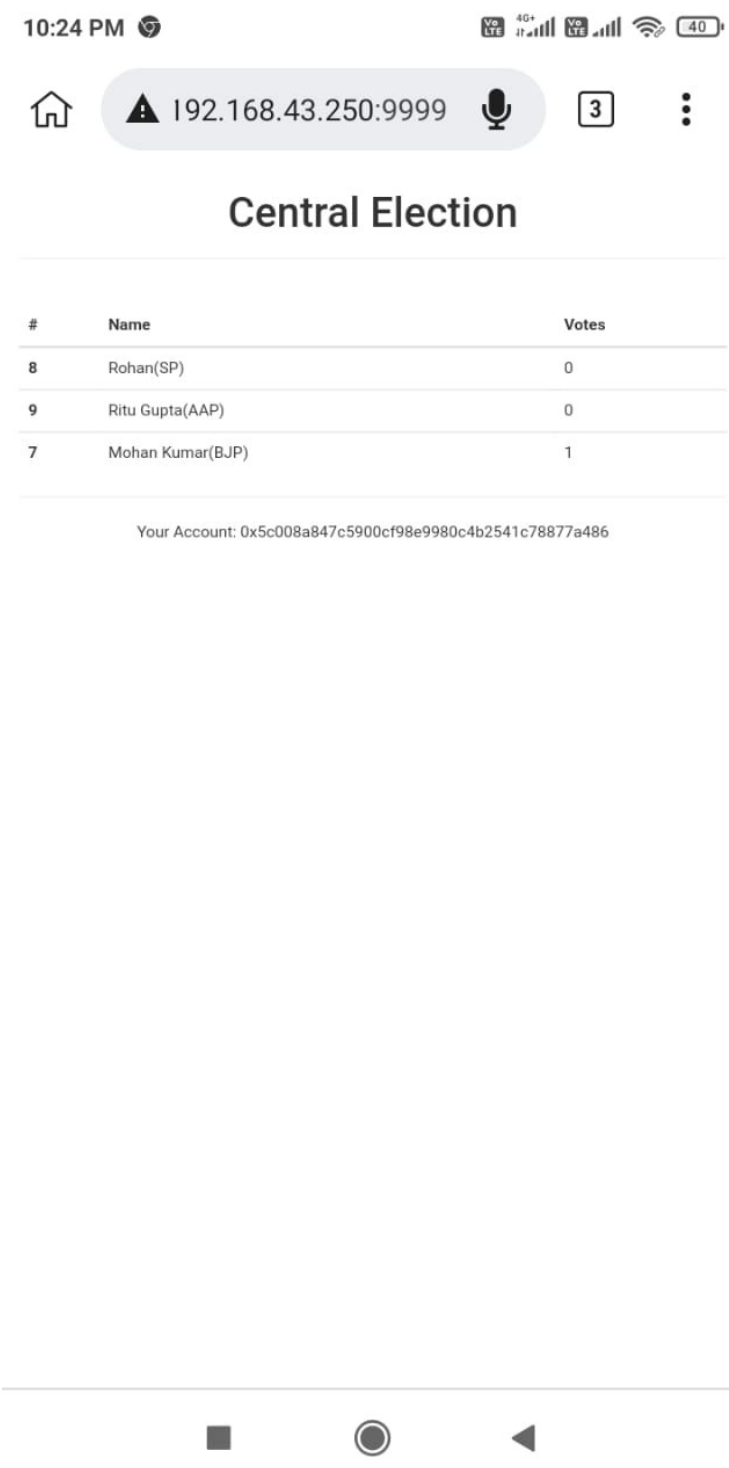
We are going to vote for Mohan Kumar from BJP, this is captured before the state of voting.



Now we are going to vote and get it approved on metamask:



As we can see from Mohan Kumar of BJP, the vote count has increased from 0 to 1.



Conclusion

Conclusion:

We have implemented the Blockchain-based virtual voting machine which has proved itself to be a replacement for the current technology that can be used for voting. It has a decentralized ledger that makes it impossible to manipulate votes once voted. We can also do the verification that one account only voted once by checking the transaction history.

We have brought the technology of blockchain voting on cellphones to vote.

Future Scope:

Using Android Biometric authentication

Real time GPS login address capturing.

References

[1] Journal Article
https://www.researchgate.net/publication/321947971_Decentralized_E-Voting_Systems_Based_on_the_Blockchain_Technology

[2]“Metamask Documentation”, https://docs.metamask.io/

[2] “Truffle Documentation” https://trufflesuite.github.io/ganache/

[3] https://www.ijert.org/research/e-voting-using-blockchain-IJERTV10IS030138.pdf

[4]“https://www.irjmets.com/uploadedfiles/paper//issue_2_february_2022/18926/final/fin_irjmets1644221156.pdf