Decentralized Voting System Using Blockchain

Abstract:

The rapid evolution of blockchain technology has opened up new avenues for reimagining traditional systems, and one such critical application is the decentralized voting system. This project delves into the intricacies of developing and implementing a robust voting mechanism utilizing the Ethereum blockchain. The primary objective is to leverage the inherent security and transparency features of blockchain to create a voting system that not only mitigates fraud and manipulation but also instills trust and confidence in the electoral process.

Project Background:

Traditional voting systems have faced issues such as fraud, manipulation, and lack of transparency. With the rise of blockchain technology, a decentralized voting system emerges as a potential solution to address these concerns. Ethereum, a popular blockchain platform, offers smart contract functionality, making it a suitable candidate for creating secure and transparent voting systems.

The project's motivation stems from the need to establish a tamper-resistant and verifiable voting mechanism that instills confidence in the electoral process. By utilizing blockchain, we aim to eliminate intermediaries, reduce the risk of manipulation, and enhance the overall integrity of the voting system.

Drawbacks of existing voting system:

The existing voting systems without blockchain technology have several disadvantages, which can potentially impact the integrity, security, and transparency of the electoral process. Few drawbacks are as shown below.

- **Lack of Transparency:** In many traditional voting systems, the process lacks transparency, making it difficult for voters to verify that their votes were accurately recorded and counted. This lack of transparency can lead to a lack of trust in the electoral process.

- **Centralized Control:** Many existing voting systems are centralized, meaning that a single authority or organization has control over the entire process. This centralized control introduces the risk of manipulation and bias, as the entity in charge may have the power to influence results.

- **Limited Accessibility:** Traditional voting systems may not be easily accessible to all citizens, particularly those with disabilities or those who are geographically distant. This can result in a lack of inclusivity and may prevent some individuals from exercising their right to vote.

- **Susceptibility to External Interference:** Without advanced security measures, traditional voting systems are susceptible to external interference, such as hacking attempts or manipulation of results by malicious actors.

Implementing blockchain technology in voting systems can address some of these issues by providing a decentralized, transparent, and secure platform for recording and verifying votes. **Blockchain's features, such as immutability and transparency, can enhance the integrity of the** voting process and increase trust among voters.

Tech stack used for the project:

- Node.js
- Web3.js
- Solidity
- Metamask
- MySQL database
- Python

Architecture of decentralized voting system:

A blockchain-based decentralized voting system harnesses the inherent characteristics of blockchain technology to foster transparency, security, and immutability within the electoral process. This high-level architectural overview outlines the key components and considerations for implementing such a system:

1. Blockchain Network:

a. Consensus Mechanism: Select an appropriate consensus mechanism aligned with the specific requirements of the voting system. Proof-of-Work (PoW), Proof-of-Stake (PoS), or alternative consensus algorithms can be explored.

b. Blockchain Type: Determine whether the blockchain will be public, private, or a consortium blockchain. Public blockchains offer open access, while private blockchains restrict participation to authorized entities.

2. Smart Contracts:

a. Smart Contract Development: Develop smart contracts to govern the voting process. These self-executing contracts encapsulate the terms of the agreement directly within the code.

b. Smart Contract Functionality: Implement smart contracts to handle voter registration, candidate registration, vote casting, and result tabulation. Rigorous security audits should be conducted to prevent vulnerabilities and exploits.

3. Voter Registration:

a. Tamper-Proof Registry: Utilize the blockchain's distributed ledger to establish a tamper-proof voter registry. Each eligible voter should possess a unique digital identity stored on the blockchain.

b. Secure Authentication: Implement a robust authentication mechanism to verify the identity of voters, ensuring the integrity of the registration process.

3. Candidate Registration:

Candidate Registration Mechanism: Establish a secure and transparent process for candidates to register on the blockchain. Their information and eligibility criteria can be integrated into the smart contract.

4. Voting Process:

a. Secure Voting Interface: Develop a secure interface connected to the blockchain for voters to cast their ballots.

b. Immutable Vote Recording: Record each vote as a transaction on the blockchain, guaranteeing transparency and immutability.

c. Voter Anonymity: Implement mechanisms to preserve voter anonymity while maintaining the integrity of the voting process.

5. Immutable Record:

The decentralized and distributed nature of the blockchain to ensure that once a vote is recorded, it cannot be altered or deleted. This immutability bolsters the integrity of the electoral process.

6. Result Tabulation:

a. Automated Result Tabulation: Integrate smart contracts with the ability to automatically tabulate results based on the recorded votes.

b. Transparent and Accessible Results: Ensure that the results are transparent and accessible to all participants within the network.

7. Security Measures:

a. Robust Cybersecurity: Implement comprehensive security measures to safeguard against cyber threats, hacking, and unauthorized access.

b. Regular Auditing: Implement regular audits and system updates to address any potential vulnerabilities.

8. User Interface:

a. User-Friendly Interface: Develop a user-friendly interface that enables voters to register, cast their votes, and verify the voting results seamlessly.

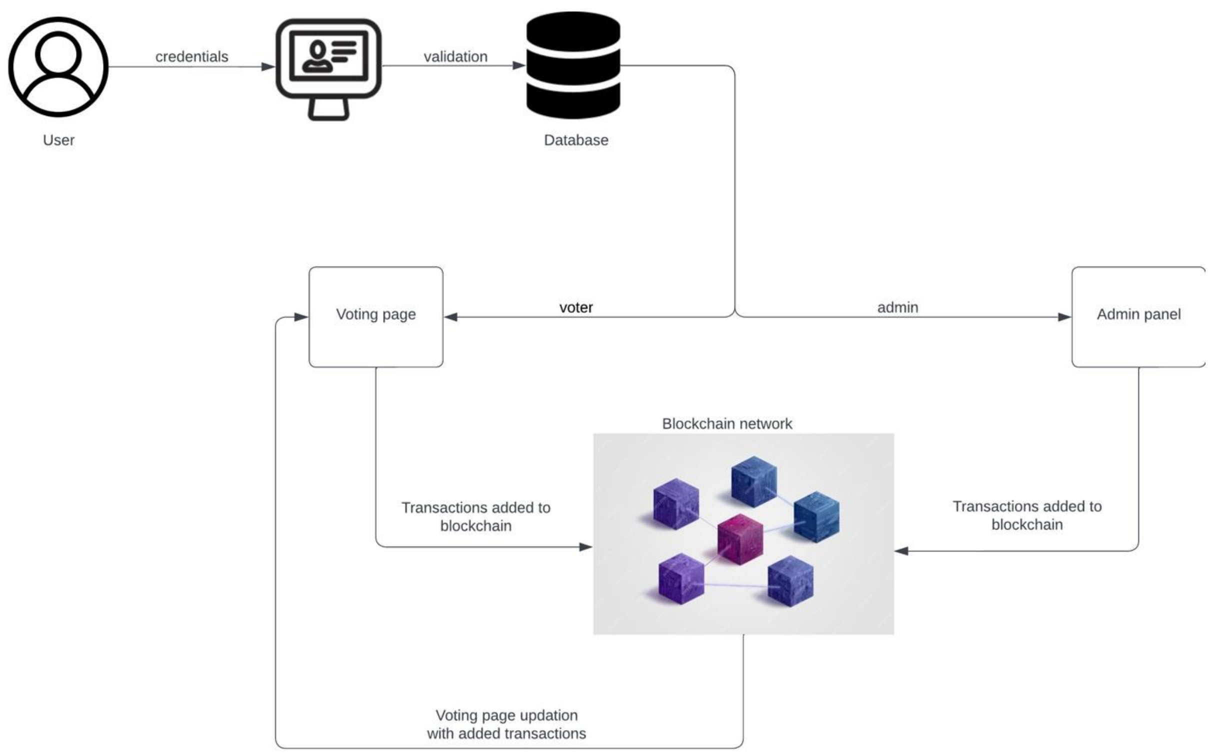
b. Independent Vote Verification: Consider providing a mechanism for voters to independently verify that their votes have been recorded accurately.

9. Decentralized Storage:
Store critical data, such as voter information and election results, in a decentralized manner across the blockchain network to prevent a single point of failure.

10. Testing and Auditing:
Conduct thorough testing and security audits before deploying the system to ensure its reliability and security.

It's important to note that while blockchain technology offers certain advantages for a decentralized voting system, challenges and considerations such as scalability, privacy, and legal compliance should be carefully addressed in the development and deployment of such systems. Additionally, the regulatory environment and social acceptance of blockchain-based voting systems may vary, so it's essential to consider these factors in the implementation process.

Proposed decentralized voting system:



The figure shown above is the proposed architecture of the decentralized voting system developed in this project. First the user enters the credentials and then they are matched with the values from the database. The credentials include voter id and password. Depending on the credentials, if the user is a voter, then he is redirected to the voting page and if the user is an admin, then it goes to the admin page.

After the administrator logs in, they have the authority to initiate the voting process by adding candidates and setting dates. Once the voting process commences, voters can cast their votes, with each transaction being securely recorded on the blockchain. The voting page is dynamically updated in real-time to reflect the current tally of votes after each voter has participated.

The main purpose of using blockchain in this implementation is to ensure transparency and security throughout the process. The envisioned system seeks to establish a secure platform for conducting elections, eradicating the potential for vote manipulation and ensuring the transparency and verifiability of election results. Its goal is to afford voters complete transparency, enabling them to observe the entire voting process, encompassing vote counting and result declaration. The system strives to enhance the accessibility of the voting process for all eligible individuals by removing the necessity for physical presence at a polling station, thereby augmenting voter turnout. Additionally, it targets an improvement in the efficiency of the voting process by reducing the time and resources traditionally required for elections. Given its automated nature and the elimination of intermediaries, this system has the potential to significantly curtail the costs and time associated with conventional voting methods. The overarching objective is to instill trust in the voting process by offering a transparent and tamper-proof mechanism for recording and tabulating votes.

Design of decentralized voting system:

1. Smart contract development:

The core of the decentralized voting system is the creation of smart contracts on the Ethereum blockchain. These contracts encapsulate the intricate rules and logic governing the voting process. Each eligible voter is assigned a unique cryptographic address, and their votes are immutably recorded on the blockchain. The smart contracts not only ensure transparency and automation but also establish a trustless environment integral to the electoral process.

2. User Interface Design:

Ensuring accessibility and user-friendliness is paramount. Hence, a comprehensive graphical user interface (GUI) has been meticulously developed. This interface enables voters to seamlessly interact with the decentralized system. Through the GUI, voters can cast their votes, verify transactions, and monitor the voting process in real-time. The user interface acts as a bridge between the complexities of blockchain and the end-user, making participation in the voting process intuitive and straightforward.

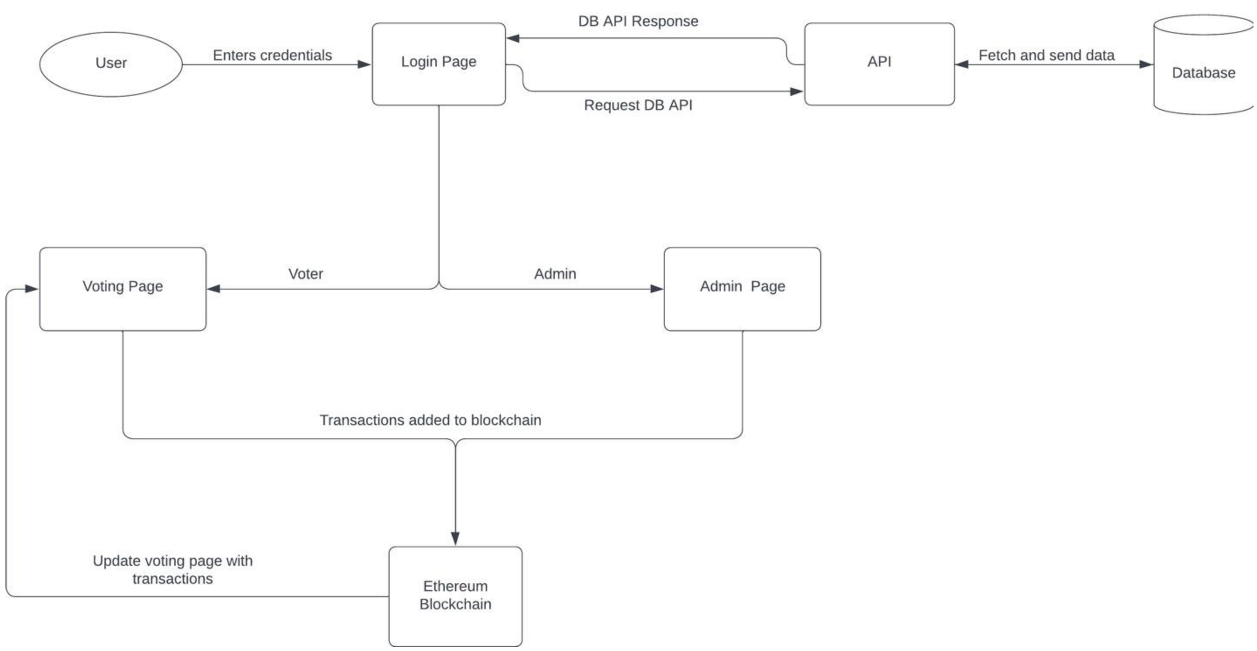
3. Testing and Deployment:

The development lifecycle includes rigorous testing to validate the functionality and security of the decentralized voting system. Various simulated voting scenarios and stress tests are conducted to identify and address potential vulnerabilities. Following successful testing, the system is deployed on the Ethereum mainnet, making it accessible for real-world use. Continuous monitoring and updates are integral to the system's evolution, ensuring its resilience and adaptability to emerging challenges.

Working of the application:

Voters register their identities using a secure authentication, ensuring voter authenticity and preventing double voting. This can be achieved through blockchain-based identity verification or secure multi-party computation techniques. JWT token is implemented for authentication and authorization of voters. The friendly user interface helps the user navigate freely across the website, view candidate information and cast votes. The choice of voters is encrypted and stored on the Ethereum blockchain. This ensures the prevention of tampering of votes casted. The smart contract tallies the votes and can generate tamper-proof results. It ensures the votes are counted transparently and accurately.

The working of the designed system can be understood from data flow diagrams. We can develop different levels of data flow diagrams for understanding the complete workflow in a step-by-step manner. The following is a level 3 dataflow diagram which showcases the complete workflow within the application and helps in better understanding the working of the decentralized system.

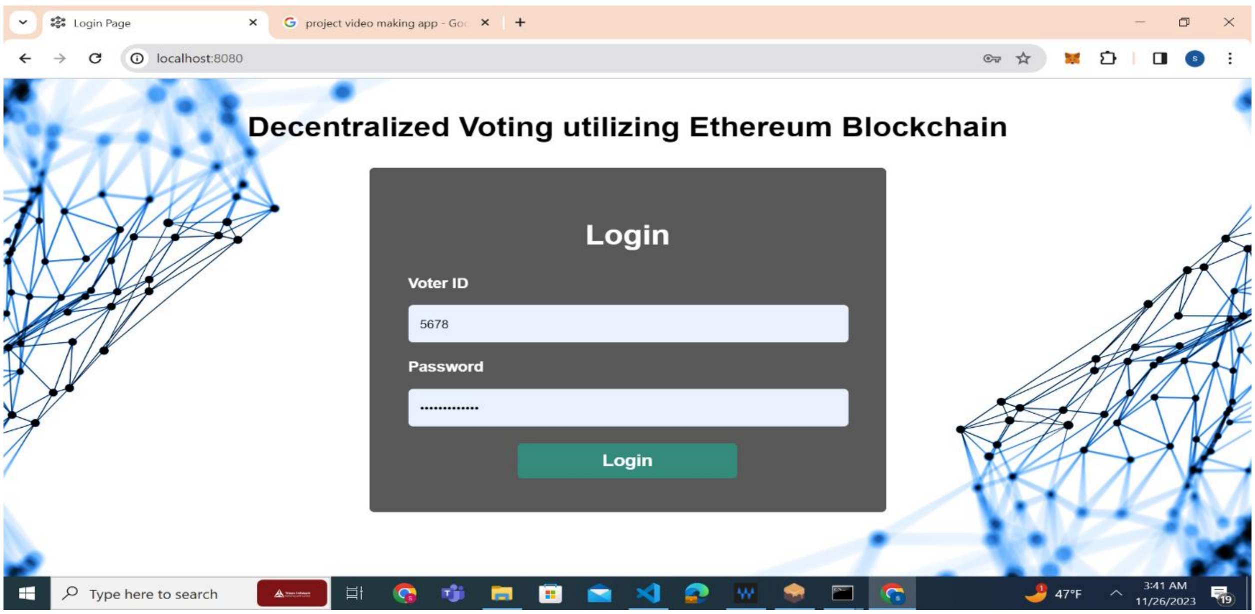


The user initially enters the credentials in the login page. This sends a request to the database API and matches the entered credentials with the data from the database. As a response, the user is classified as a voter, or an admin based on the credentials entered. If the user is a voter, he/she is redirected to the voting page to cast the vote. If the user is an admin, then he/she is redirected to the admin page to where candidates can be added, and dates can be defined for voting. All the admin and voter transactions are added to the Ethereum blockchain. Then the voting page is updated with the new transactions added to the blockchain. Below shown are the scenarios involved in a user leveraging the decentralized voting system application.

Case-1: Check for JWT authorization

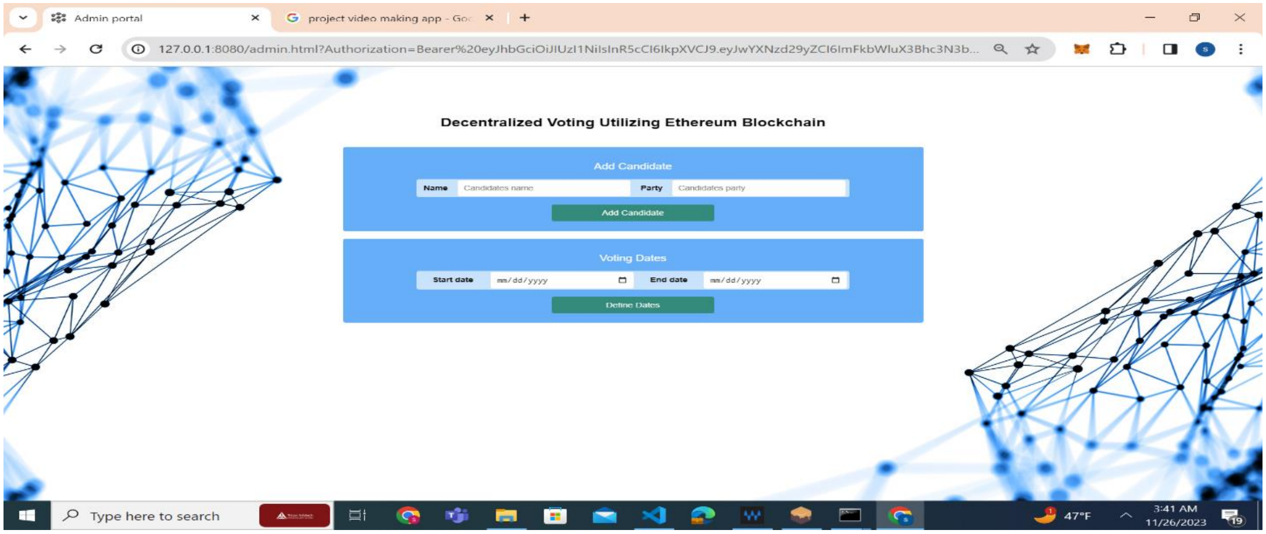
The user enters the credentials for login id and password. User cannot access the admin page or voting page without proper authorization.

Case-2: User login verification
After user enters the id and password, the values are compared with those in the database. If the credentials match with the values from database, the login is successful, otherwise an error is thrown saying the user is unauthorized.



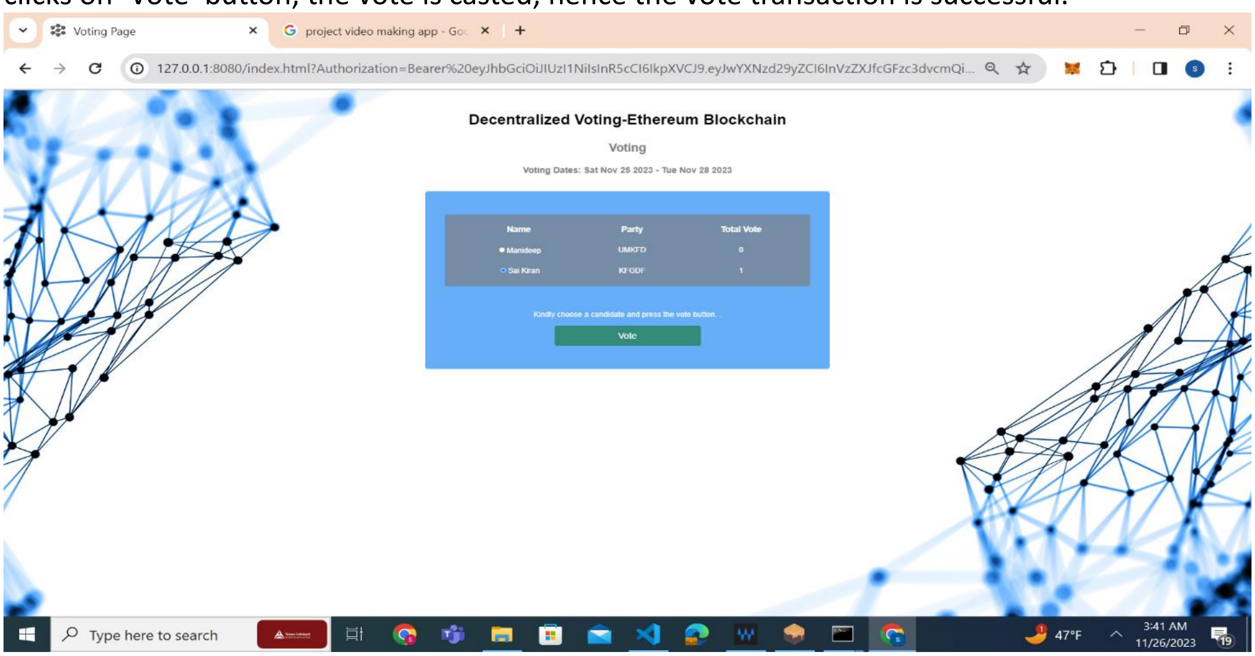
Case-3: Candidate/Date registration

Once the user is logged in as admin, he/she enters the name of candidate and party for registration. This should result in successful registration of the candidate.The admin has the privilege of deciding the voting dates. Giving start date and end date as inputs, the date transactions will be successful.



Case-4: Vote casting

Once the user logs in as voter, he/she can cast their vote. If the voter selects a candidate and clicks on ‘Vote’ button, the vote is casted, hence the vote transaction is successful.



Challenges faced and solutions implemented for the challenges:

Behind the successful implementation of decentralized voting system using Ethereum blockchain, there have been few challenges that hampered the pace of the development.

The team encountered challenges in refining the implementation of specific functionalities in the smart contracts. Ensuring the accuracy and effectiveness of the smart contract logic required meticulous attention, and the team worked diligently to address any minor issues that surfaced.

Coordinating last-minute UI adjustments with the finalization of smart contract implementation presented a challenge. Integrating updates to the user interface while ensuring seamless compatibility with the refined smart contract posed complexities that the team actively addressed.

Individual contributions:

Manideep Meda:

Manideep has effectively conducted testing of the implemented smart contracts to ensure their functionality and security. He has done aggressive user testing to gather valuable feedback on the UI and overall user experience, addressing usability concerns. He played a key role in developing and documenting a backup and recovery plan to ensure data integrity and availability. Testing the backup and recovery procedures.

Venkata Sai Kiran Reddy Pogula:

Sai Kiran created a detailed project timeline outlining key milestones, deadlines, and tasks for each week. He played a crucial role in conducting a security review of smart contract to identify and address any vulnerabilities. He worked on deploying the smart contract into the blockchain and conducted testing post the deployment. His efforts were productive in Integrating the front-end development environment with the backend (smart contract).

Sreeja Atluri:

Sreeja proactively worked on successfully integrating the front-end UI with the smart contracts for user registration and voting. She created comprehensive documentation, detailing the smart contract architecture and integration specifics. Her role was pivotal in optimizing the performance of the system to ensure responsiveness and efficiency. Addressing any remaining bottlenecks or areas where performance can be improved.

Simran Bathla:

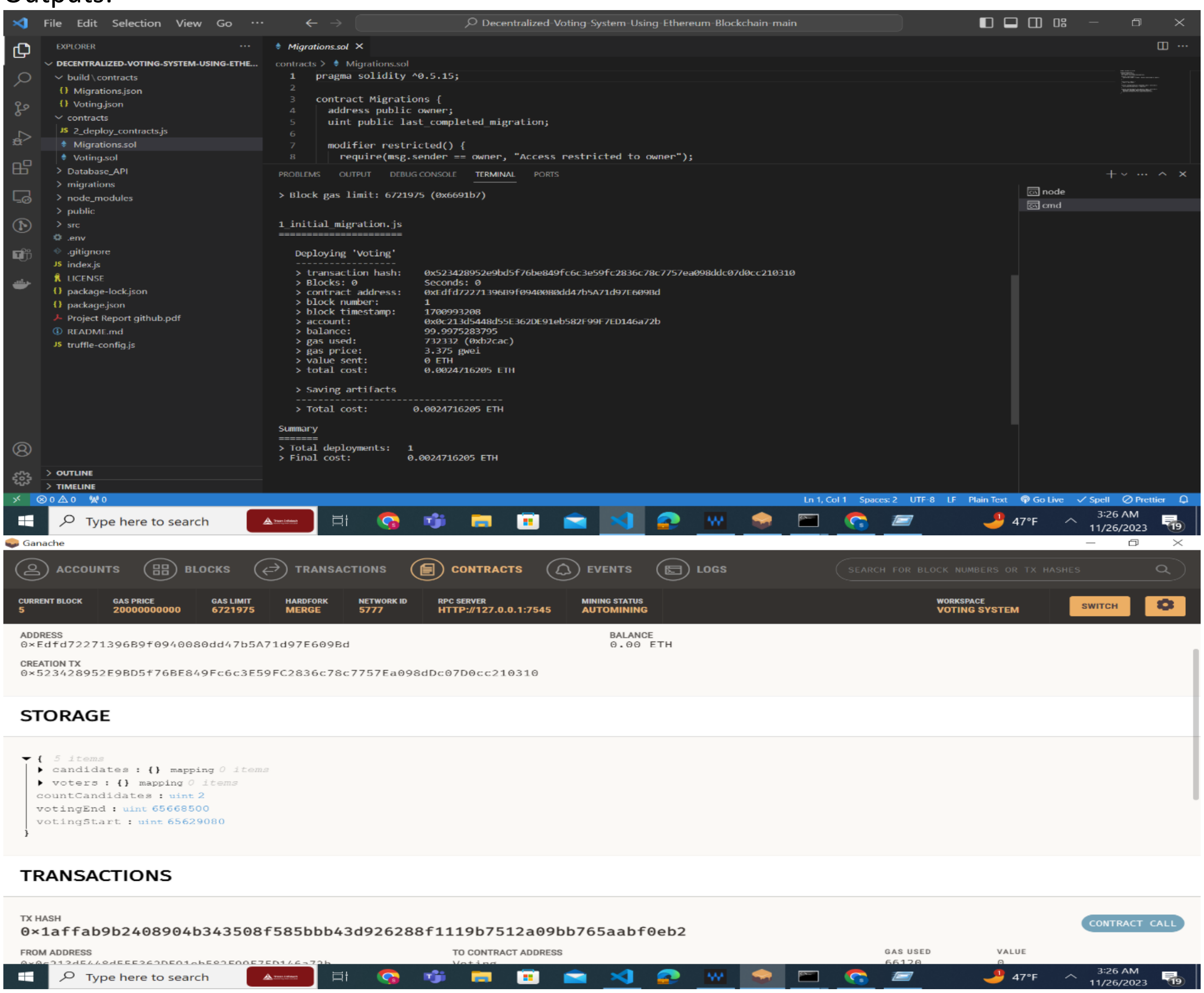
Simran developed templates for the user interface design, including layout and visual elements. Ensure that the design aligns with the project's objectives and user-friendly functionality. She successfully implemented user registration and login features and interfaces in the front-end. She designed the front end with the desired registration and submit buttons, and a view of all the available candidates, with an output window showing the voter’s vote.

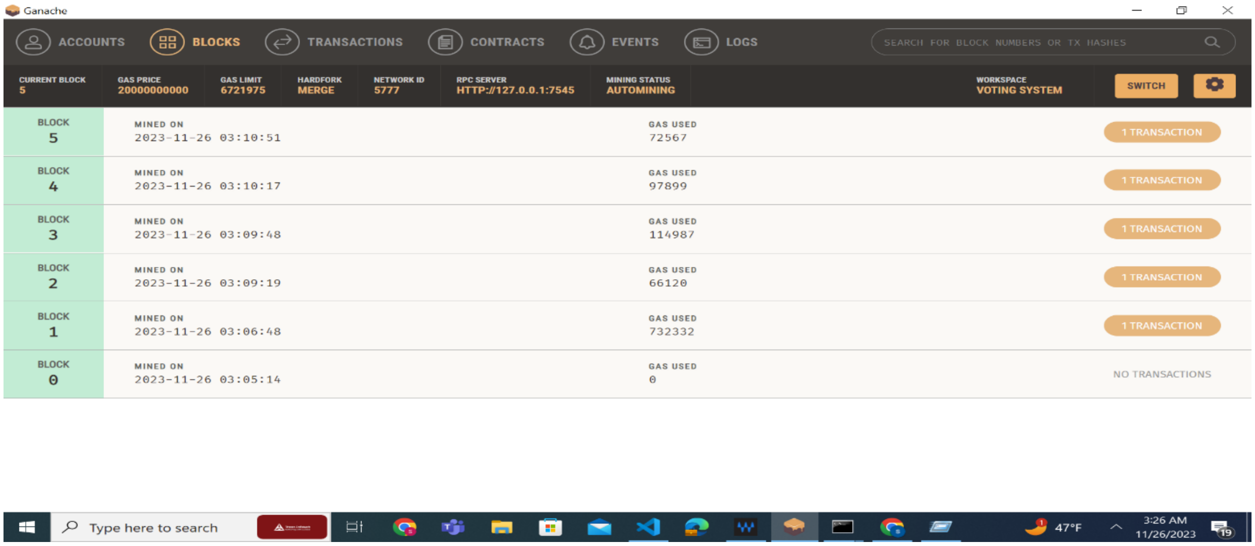
Conclusion:

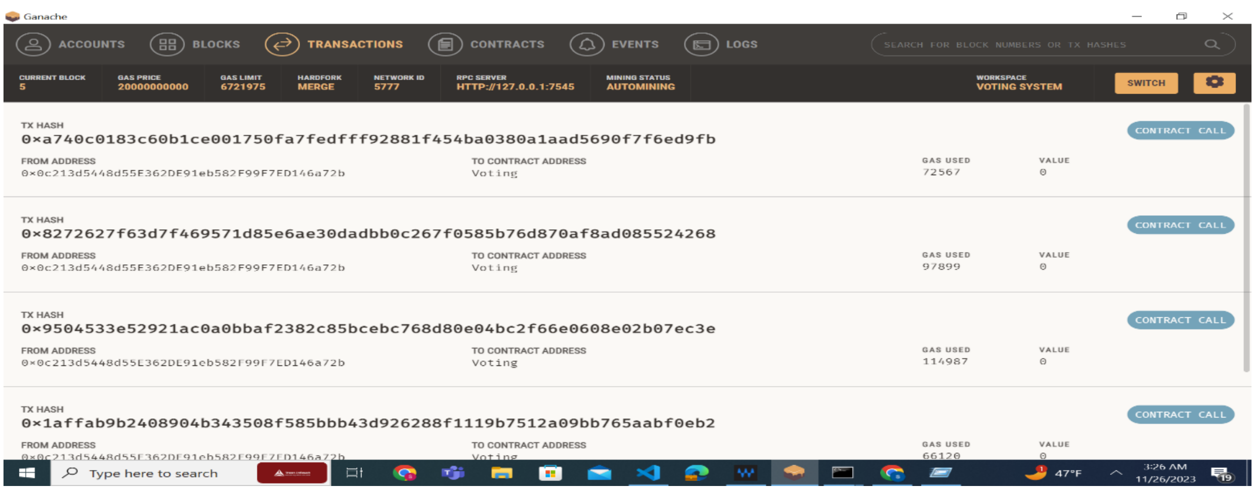
In summation, the decentralized voting system presented in this project represents a significant stride towards addressing the inadequacies of traditional voting systems. The smart contracts on the Ethereum blockchain establish a tamper-resistant and verifiable framework, contributing to a more trustworthy and efficient electoral process.

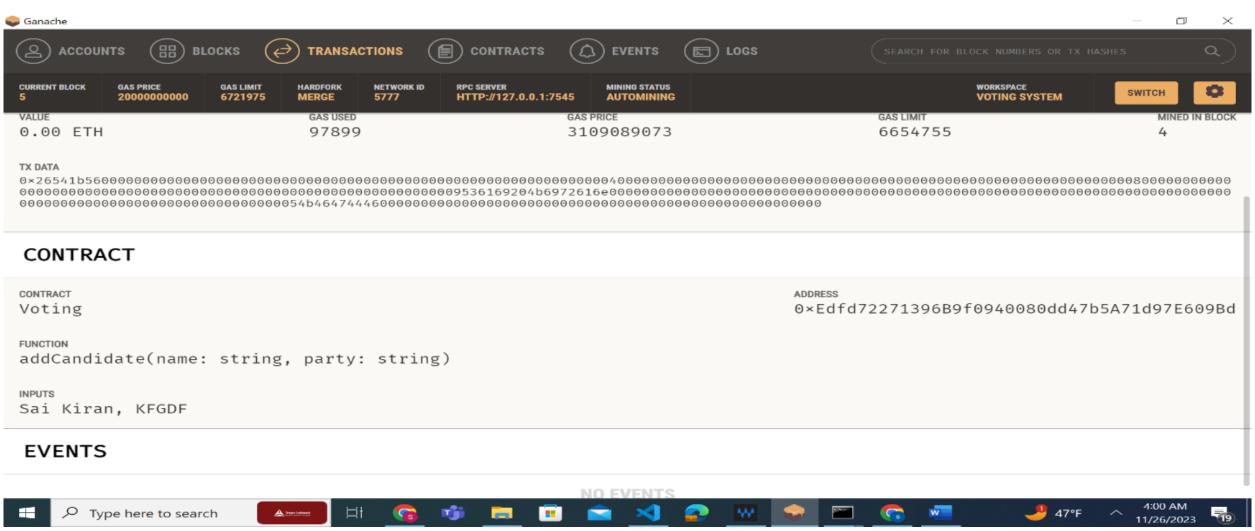
The user-friendly interface ensures accessibility for a diverse range of voters, fostering inclusivity. Robust security measures, including cryptographic techniques and the inherent features of decentralization, safeguard the integrity of the entire voting system. While this decentralized voting system is a promising advancement, the journey does not end here. Ongoing efforts are required to tackle scalability challenges and enhance user adoption, propelling the evolution of secure and transparent voting systems towards a more democratic future.

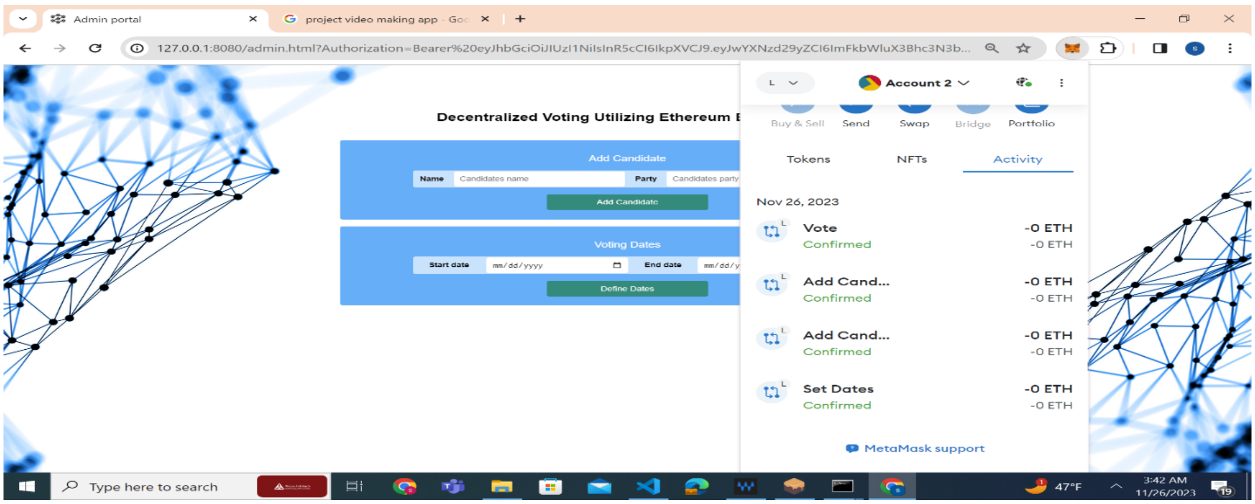
Outputs:




Ganache
ACCOUNTS
BLOCKS
TRANSACTIONS
CONTRACTS
EVENTS
LOGS
SEARCH FOR BLOCK NUMBERS OR TX HASHES
CURRENT BLOCK 5
GAS PRICE 20000000000
GAS LIMIT 6721975
HARDFORK MERGE
NETWORK ID 5777
RPC SERVER HTTP://127.0.0.1:7545
MINING STATUS AUTOMINING
WORKSPACE VOTING SYSTEM
SWITCH
BLOCK 5
MINED ON 2023-11-26 03:10:51
GAS USED 72567
1 TRANSACTION
BLOCK 4
MINED ON 2023-11-26 03:10:17
GAS USED 97899
1 TRANSACTION
BLOCK 3
MINED ON 2023-11-26 03:09:48
GAS USED 114987
1 TRANSACTION
BLOCK 2
MINED ON 2023-11-26 03:09:19
GAS USED 66120
1 TRANSACTION
BLOCK 1
MINED ON 2023-11-26 03:06:48
GAS USED 732332
1 TRANSACTION
BLOCK 0
MINED ON 2023-11-26 03:05:14
GAS USED 0
NO TRANSACTIONS
Type here to search
47°F
3:26 AM
11/26/2023


Ganache
ACCOUNTS
BLOCKS
TRANSACTIONS
CONTRACTS
EVENTS
LOGS
SEARCH FOR BLOCK NUMBERS OR TX HASHES
CURRENT BLOCK 5
GAS PRICE 20000000000
GAS LIMIT 6721975
HARDFORK MERGE
NETWORK ID 5777
RPC SERVER HTTP://127.0.0.1:7545
MINING STATUS AUTOMINING
WORKSPACE VOTING SYSTEM
SWITCH
TX HASH
0x a740c0183c60b1ce001750fa7fedfff92881f454ba0380a1aad5690f7f6ed9fb
CONTRACT CALL
FROM ADDRESS 0x0c213d5448d55E362DE91eb582F99F7ED146a72b
TO CONTRACT ADDRESS Voting
GAS USED 72567
VALUE 0
TX HASH
0x8272627f63d7f469571d85e6ae30dadbb0c267f0585b76d870af8ad085524268
CONTRACT CALL
FROM ADDRESS 0x0c213d5448d55E362DE91eb582F99F7ED146a72b
TO CONTRACT ADDRESS Voting
GAS USED 97899
VALUE 0
TX HASH
0x9504533e52921ac0a0bbaf2382c85bcebc768d80e04bc2f66e0608e02b07ec3e
CONTRACT CALL
FROM ADDRESS 0x0c213d5448d55E362DE91eb582F99F7ED146a72b
TO CONTRACT ADDRESS Voting
GAS USED 114987
VALUE 0
TX HASH
0x1affab9b2408904b343508f585bbb43d926288f1119b7512a09bb765aabf0eb2
CONTRACT CALL
FROM ADDRESS
TO CONTRACT ADDRESS
GAS USED 66120
VALUE 0
Type here to search
47°F
3:26 AM
11/26/2023


Ganache
ACCOUNTS
BLOCKS
TRANSACTIONS
CONTRACTS
EVENTS
LOGS
SEARCH FOR BLOCK NUMBERS OR TX HASHES
CURRENT BLOCK 5
GAS PRICE 20000000000
GAS LIMIT 6721975
HARDFORK MERGE
NETWORK ID 5777
RPC SERVER HTTP://127.0.0.1:7545
MINING STATUS AUTOMINING
WORKSPACE VOTING SYSTEM
SWITCH
VALUE 0.00 ETH
GAS USED 97899
GAS PRICE 3109089073
GAS LIMIT 6654755
MINED IN BLOCK 4
TX DATA
CONTRACT
CONTRACT Voting
ADDRESS 0xEdfd72271396B9f0940080dd47b5A71d97E609Bd
FUNCTION addCandidate(name: string, party: string)
INPUTS Sai Kiran, KFGDF
EVENTS
NO EVENTS
Type here to search
47°F
4:00 AM
11/26/2023


Admin portal
project video making app - Goo
127.0.0.1:8080/admin.html?Authorization=Bearer%20eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwYXNzd29yZCI6ImFkbWluX3Bhc3N3b...
Decentralized Voting Utilizing Ethereum E
Add Candidate
Name
Candidates name
Party
Candidates party
Add Candidate
Voting Dates
Start date
mm/dd/yyyy
End date
Define Dates
Account 2
Buy & Sell
Send
Swap
Bridge
Portfolio
Tokens
NFTs
Activity
Nov 26, 2023
Vote
Confirmed
-0 ETH
-0 ETH
Add Cand...
Confirmed
-0 ETH
-0 ETH
Add Cand...
Confirmed
-0 ETH
-0 ETH
Set Dates
Confirmed
-0 ETH
-0 ETH
MetaMask support
Type here to search
47°F
3:42 AM
11/26/2023