Batch: A1	**Roll No.: 16010121033**
Experiment No. 10	

Title: Creation of a simple application using any web development tools to demonstrate the working of block chain

Objective: Implement a basic E-voting system based on blockchain.

Expected Outcome of Experiment:
Design, implement and test a blockchain-based e-voting solution, utilizing the Ethereum platform and Solidity language, to ensure security, transparency, and the privacy of voters.

CO	Outcome
CO1	Describe the basic concepts of Blockchain and Distributed Ledger Technology
CO2	Apply cryptographic hash required for Blockchain.
CO3	Categorize and discuss the consensus in Blockchain.
CO4	Infer the components of Ethereum ecosystem.
CO5	Design a private Blockchain platform.

Books/ Journals/ Websites referred:
https://ieeexplore.ieee.org/document/9491734

https://ieeexplore.ieee.org/document/9670245

https://ieeexplore.ieee.org/document/9887759

https://ieeexplore.ieee.org/document/10169552

https://ieeexplore.ieee.org/document/10053410

https://ieeexplore.ieee.org/document/10125883

https://www.investopedia.com/terms/b/blockchain.asp

Blockchain for Electronic Voting System—Review and Open Research Challenges
Uzma Jafar,* Mohd Juzaiddin Ab Aziz, and Zarina Shukur

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614/

A secure end-to-end verifiable e-voting system using blockchain and cloud server Somnath Panja, Bimal
Roy https://www.sciencedirect.com/science/article/abs/pii/S2214212621000557

Conceptual Architecture of a Blockchain Solution for E-Voting in Elections at the University Level
Simona-Vasilica Oprea, Adela Bâra, Anca-Ioana Andreescu and Marian Pompiliu Cristescu
https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10049991

Votereum: An Ethereum-Based E-Voting System Linh
Vo-Cao- Thuy; Khoi Cao-Minh; Chuong Dang-Le-Bao; Tuan A. Nguyen
https://ieeexplore.ieee.org/document/8713661

Abstract:-

In an era of rapid technological advancements, traditional voting systems face challenges related to security, transparency, and efficiency. Digipolls, a blockchain-based E-voting system, aims to address these concerns by leveraging the capabilities of blockchain technology. At the heart of Digipolls is the use of smart contracts on the Ethereum blockchain, which provide a secure and tamper-proof way to record votes. By utilizing a decentralized ledger, Digipolls eliminates the risks of vote manipulation and removes the need for intermediaries, thus streamlining the voting process and reducing human error. The system also features a user-friendly interface, accessible through web and mobile platforms, ensuring that voters from all backgrounds can easily participate. Digipolls envisions a future where elections are more transparent, secure, and inclusive, contributing to a fairer and more democratic society.

Related Theory: -

The core of a blockchain-based E-voting system revolves around three key components:

1. Smart Contracts: Self-executing contracts where the agreement terms between voter and election organizer are written directly into lines of code. It will manage voter registration, validation, and the voting process.
2. Blockchain: A distributed ledger that maintains an immutable and transparent record of votes, ensuring the voting data cannot be altered once it is recorded.
3. Cryptographic Hash: Utilized to securely store votes and voter information. Each transaction (vote) is encrypted and linked to the previous one, creating a secure and traceable voting record.

Development Tools and Environments:

Ganache:

- Ganache is a personal blockchain used for Ethereum development. It allows developers to deploy, test, and debug smart contracts in a controlled, local environment before moving to a live network.
- In the context of an E-voting system, Ganache can be used to simulate the voting process, check for bugs, and ensure the system works as intended before deploying it to the Ethereum mainnet or a private blockchain.

Truffle:

- Truffle is a development framework for Ethereum. It provides a suite of tools for building, testing, and deploying smart contracts.
- In the E-voting system, Truffle simplifies the deployment of smart contracts, enables testing of contract functionalities, and allows for debugging, making the development process more efficient.

MetaMask:

- MetaMask is a browser extension and cryptocurrency wallet that enables interaction with the Ethereum blockchain. It acts as a bridge between the web browser and the blockchain.
- For the E-voting application, MetaMask allows users to manage their Ethereum accounts, sign transactions, and securely interact with the smart contracts deployed on the blockchain.

Solidity:

- Solidity is a programming language used to write smart contracts on the Ethereum blockchain. It is specifically designed to create decentralized applications (DApps) that run on the Ethereum Virtual Machine (EVM).
- In the E-voting project, Solidity is used to write the logic for voter registration, voting validation, and vote counting, ensuring the system is secure and automated.

Remix IDE:

- Remix IDE is an online integrated development environment used for writing, testing, and deploying smart contracts written in Solidity. It provides a user-friendly interface and tools to compile, deploy, and debug smart contracts.
- In the E-voting project, Remix allows for quick testing and iteration of smart contract code, enabling developers to refine and perfect the voting logic before final deployment.

(We tested the smart contracts on Remix ide and used VS code for further exploration of application)

Implementation Details:

1. Enlist all the Steps followed and various options explored

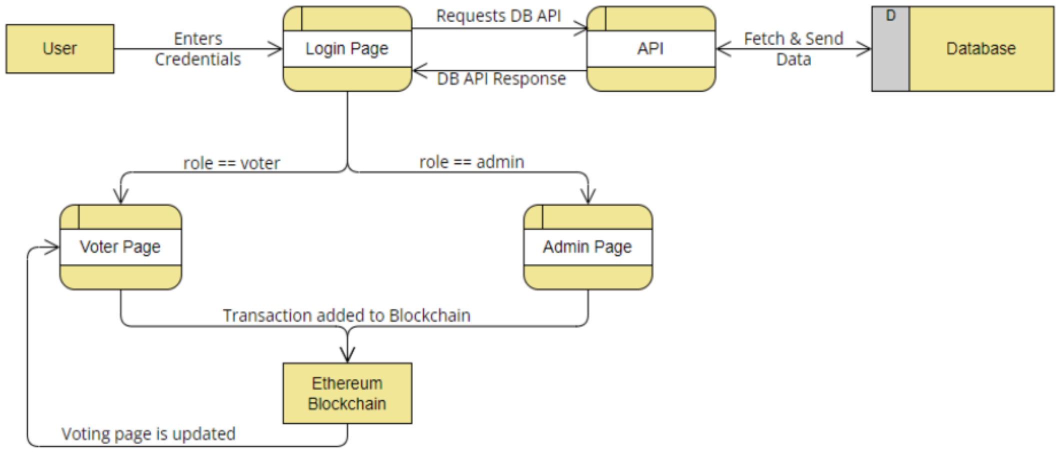
1. Setup Development Environment:

- Tools used: Remix IDE for smart contract development, MetaMask for wallet and account management, and Ganache (for a private Ethereum blockchain).
- Use HTML, JavaScript, and Web3.js for the front-end interface.
- Created an Ethereum wallet in MetaMask for testing.

2. Create Smart Contracts:
    - Developed smart contracts using Solidity to handle voting logic.
    - The contracts will manage the registration of candidates, recording votes, and preventing double-voting.
    - Deployed the contract on the local blockchain (Ganache) for testing.
3. Web Application Development:
    - Designed a simple web interface using HTML, CSS, and JavaScript.
    - Connected the front-end to the blockchain using Web3.js.
    - Developed voting functionalities: viewing candidates, voting, and displaying real-time vote counts.
4. Testing:
    - Verified the registration process, voting functionality, and vote counting.
    - Checked for vulnerabilities in the contract to avoid manipulation or breac**hes.**

2. Explain your program logic.

User enters the credentials (voter id & password) and they are matched with the database. If the match is found user is either redirected to admin page or voter page as per their role corresponding to the credentials in the database. Once the admin is logged in he/she can start the voting process by adding candidates and defining dates. Voter can vote once the voting process has been started. Once the voter has voted the transaction is recorded to the blockchain and the voting page is updated with real-time votes.



3. Explain the Importance of the approach followed by you

The use of blockchain technology for an E-voting system ensures a tamper-proof and decentralized solution, eliminating the need for intermediaries. It enhances transparency, allows for public verification, and reduces the risks associated with traditional voting systems, such as voter manipulation or inaccurate counting. By leveraging smart contracts, the system is automated and self-verifying, significantly reducing operational costs and increasing trustworthiness.

Additionally,

1. Security: The proposed system aims to provide a secure platform for conducting elections, eliminating the possibility of tampering with votes, and ensuring that the election results are transparent and verifiable.

2. Transparency: The proposed system aims to provide complete transparency to the voters, allowing them to view the entire voting process, including the vote counting and results.

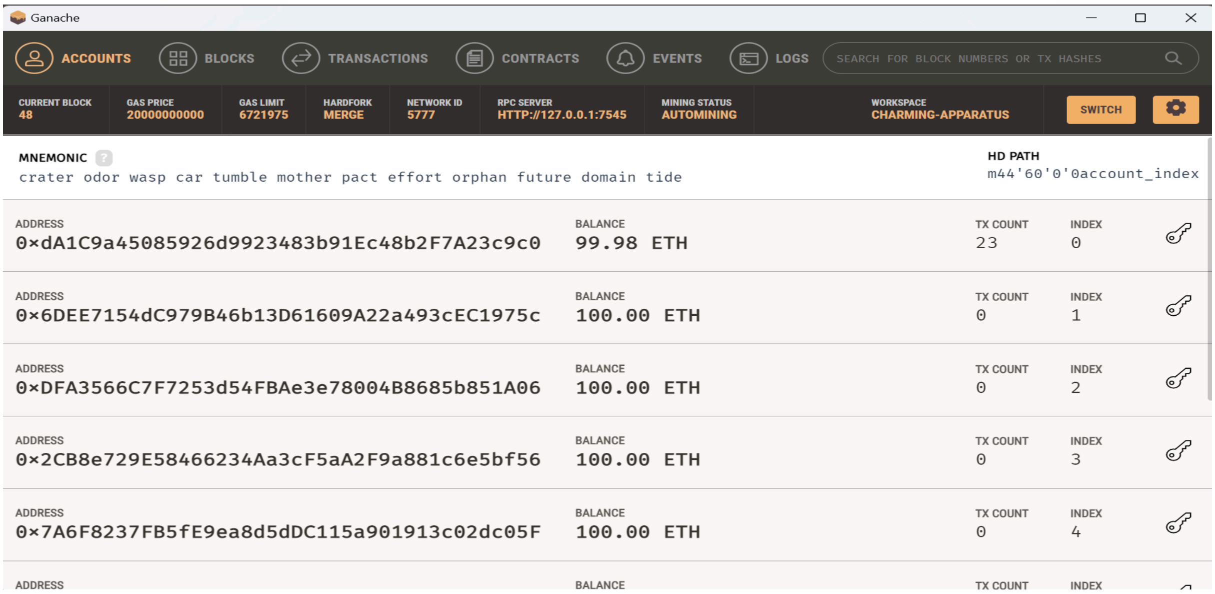
3. Accessibility: The proposed system aims to make the voting process more accessible to all eligible voters by eliminating the need for physical presence at a polling station, thus increasing voter turnout.

4. Efficiency: The system aims to increase the efficiency of the voting process by reducing the time and resources required to conduct elections. Since the system is

automated and eliminates the need for intermediaries, it can significantly reduce the cost and time associated with traditional voting methods.

5. Trust: The proposed system aims to increase trust in the voting process by providing a transparent and tamper-proof mechanism for recording and tallying votes.

Implementation:



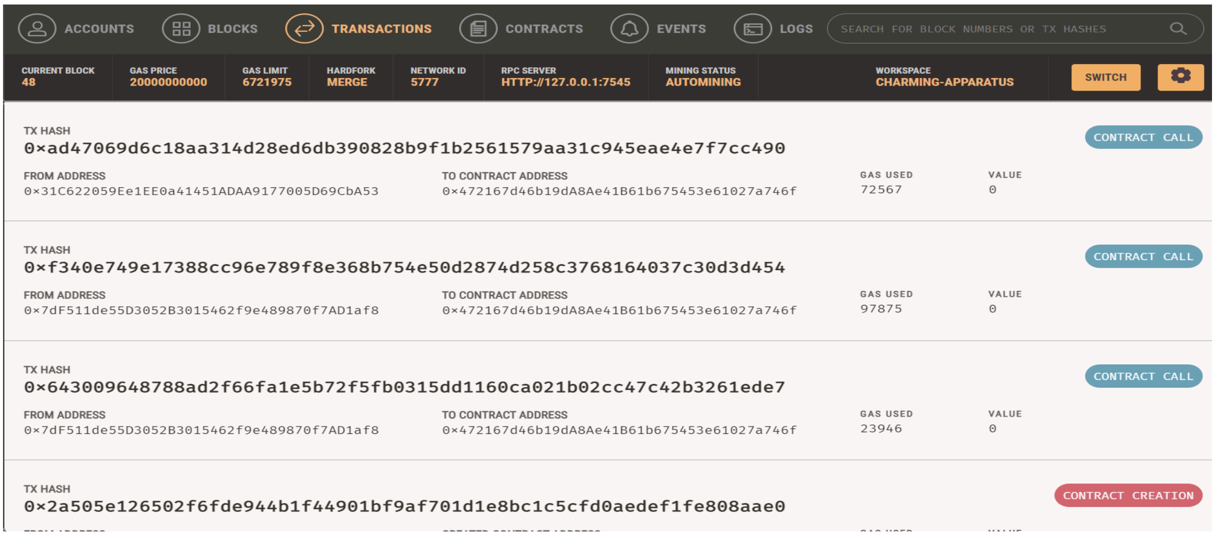
CURRENT BLOCK 48 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK MERGE | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING | WORKSPACE CHARMING-APPARATUS

MNEMONIC
crater odor wasp car tumble mother pact effort orphan future domain tide

HD PATH
m44'60'0'0account_index

ADDRESS	BALANCE	TX COUNT	INDEX
0×dA1C9a45085926d9923483b91Ec48b2F7A23c9c0	99.98 ETH	23	0
0×6DEE7154dC979B46b13D61609A22a493cEC1975c	100.00 ETH	0	1
0×DFA3566C7F7253d54FBAe3e78004B8685b851A06	100.00 ETH	0	2
0×2CB8e729E58466234Aa3cF5aA2F9a881c6e5bf56	100.00 ETH	0	3
0×7A6F8237FB5fE9ea8d5dDC115a901913c02dc05F	100.00 ETH	0	4

Ganache Interface – Accounts



CURRENT BLOCK 48 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK MERGE | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING | WORKSPACE CHARMING-APPARATUS

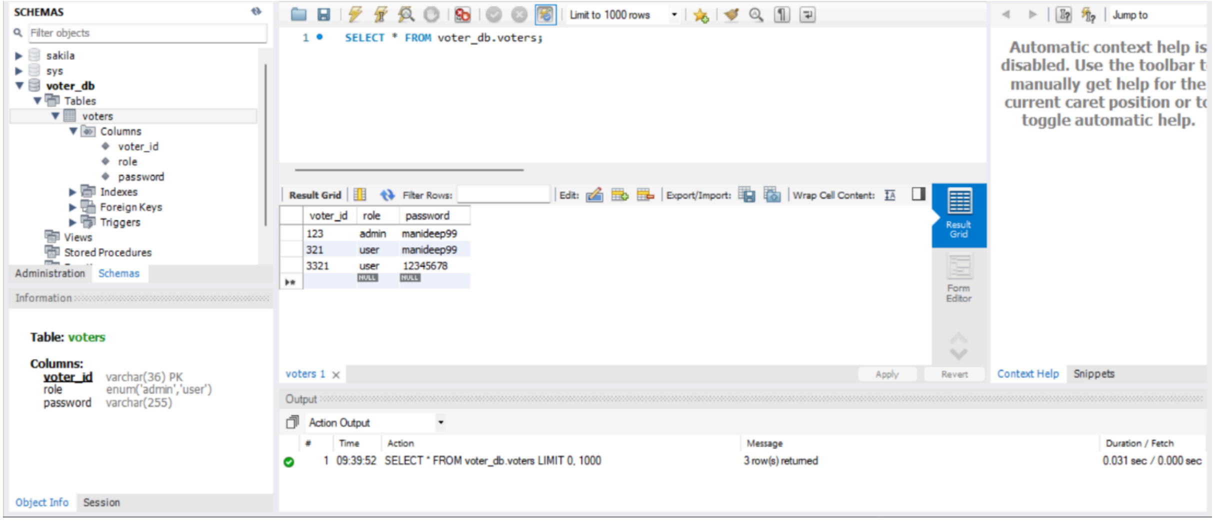
TX HASH
0×ad47069d6c18aa314d28ed6db390828b9f1b2561579aa31c945eae4e7f7cc490
CONTRACT CALL
FROM ADDRESS 0×31C622059Ee1EE0a41451ADAA9177005D69CbA53
TO CONTRACT ADDRESS 0×472167d46b19dA8Ae41B61b675453e61027a746f
GAS USED 72567
VALUE 0

TX HASH
0×f340e749e17388cc96e789f8e368b754e50d2874d258c3768164037c30d3d454
CONTRACT CALL
FROM ADDRESS 0×7dF511de55D3052B3015462f9e489870f7AD1af8
TO CONTRACT ADDRESS 0×472167d46b19dA8Ae41B61b675453e61027a746f
GAS USED 97875
VALUE 0

TX HASH
0×643009648788ad2f66fa1e5b72f5fb0315dd1160ca021b02cc47c42b3261ede7
CONTRACT CALL
FROM ADDRESS 0×7dF511de55D3052B3015462f9e489870f7AD1af8
TO CONTRACT ADDRESS 0×472167d46b19dA8Ae41B61b675453e61027a746f
GAS USED 23946
VALUE 0

TX HASH
0×2a505e126502f6fde944b1f44901bf9af701d1e8bc1c5cfd0aedef1fe808aae0
CONTRACT CREATION

Ganache Interface - Transactions



```
SELECT * FROM voter_db.voters;
```

voter_id	role	password
123	admin	manideep99
321	user	manideep99
3321	user	12345678
	NULL	NULL

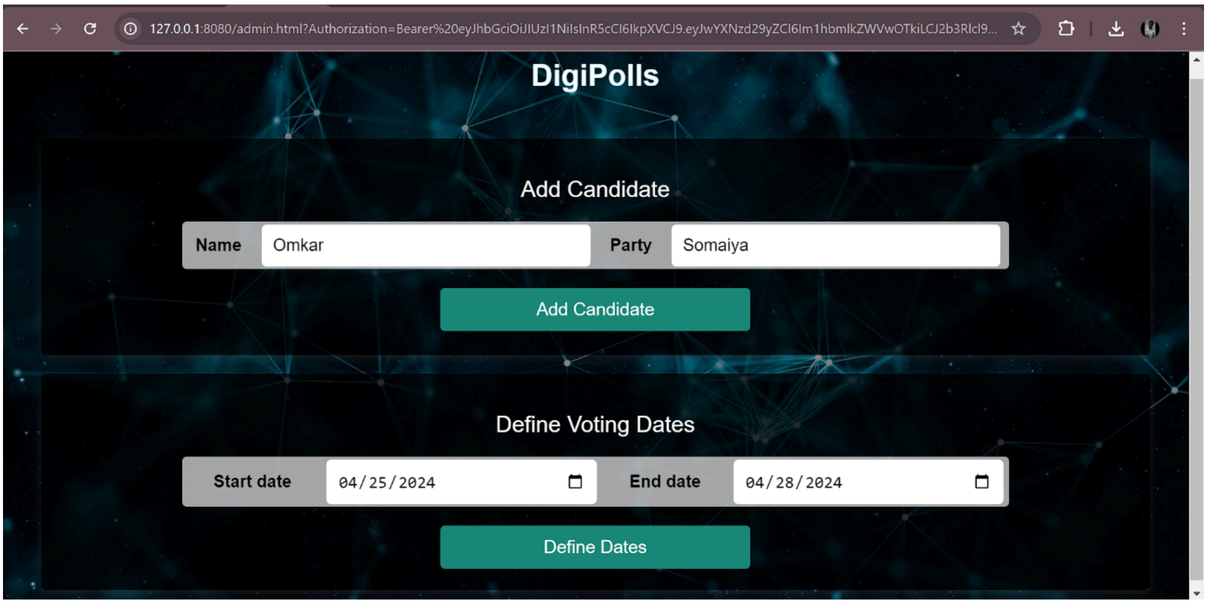
Table: voters

Columns:
voter_id varchar(36) PK
role enum('admin','user')
password varchar(255)

Automatic context help is disabled. Use the toolbar t manually get help for the current caret position or tc toggle automatic help.

#	Time	Action	Message	Duration / Fetch
1	09:39:52	SELECT * FROM voter_db.voters LIMIT 0, 1000	3 row(s) returned	0.031 sec / 0.000 sec

Database



127.0.0.1:8080/admin.html?Authorization=Bearer%20eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwYXNzd29yZCI6Im1hbmlkZWVwOTkiLCJ2b3Rlcl9...

DigiPolls

Add Candidate

Name: Omkar

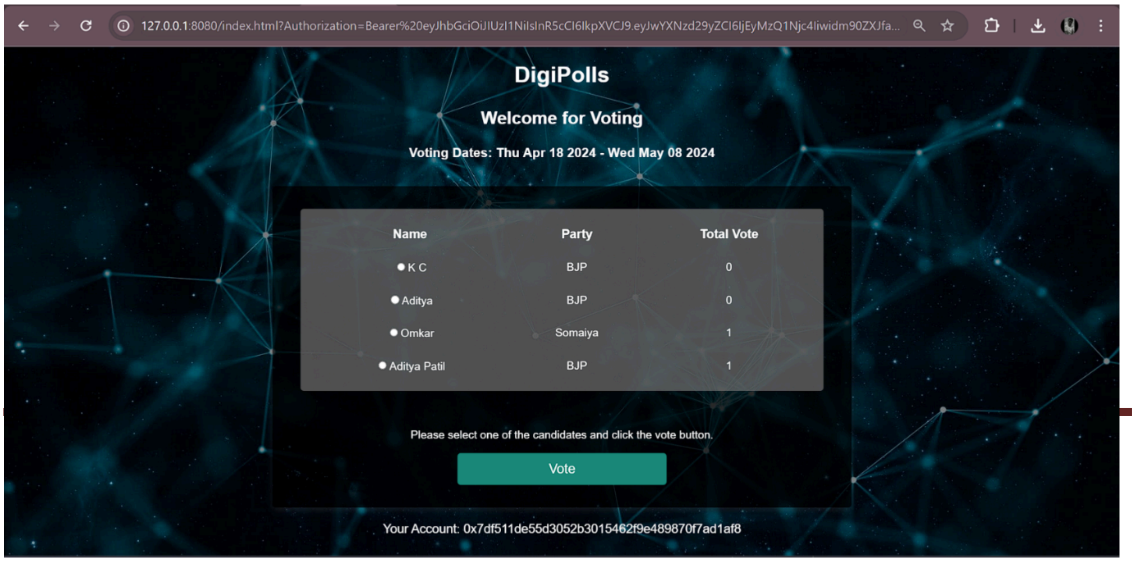
Party: Somaiya

Define Voting Dates

Start date: 04/25/2024

End date: 04/28/2024

Admin portal



127.0.0.1:8080/index.html?Authorization=Bearer%20eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwYXNzd29yZCI6IjEyMzQ1Njc4Iiwidm90ZXJfa...

DigiPolls

Welcome for Voting

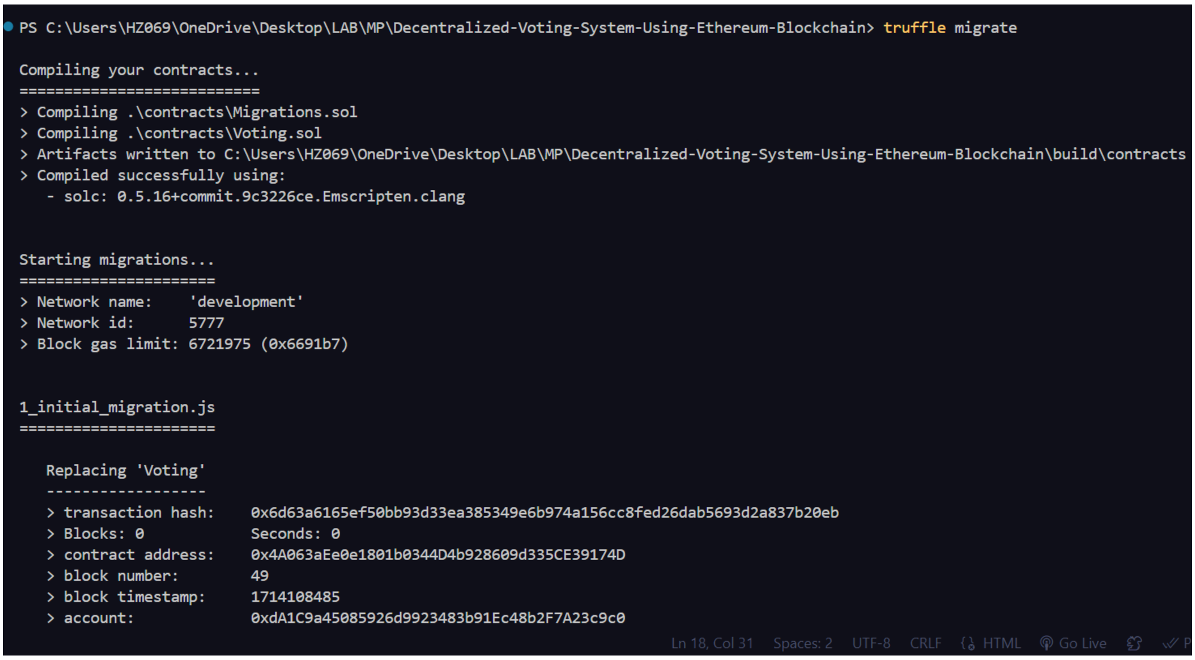
Voting Dates: Thu Apr 18 2024 - Wed May 08 2024

Name	Party	Total Vote
○ K C	BJP	0
○ Aditya	BJP	0
○ Omkar	Somaiya	1
○ Aditya Patil	BJP	1

Please select one of the candidates and click the vote button.

Your Account: 0x7df511de55d3052b3015462f9e489870f7ad1af8

Voter portal



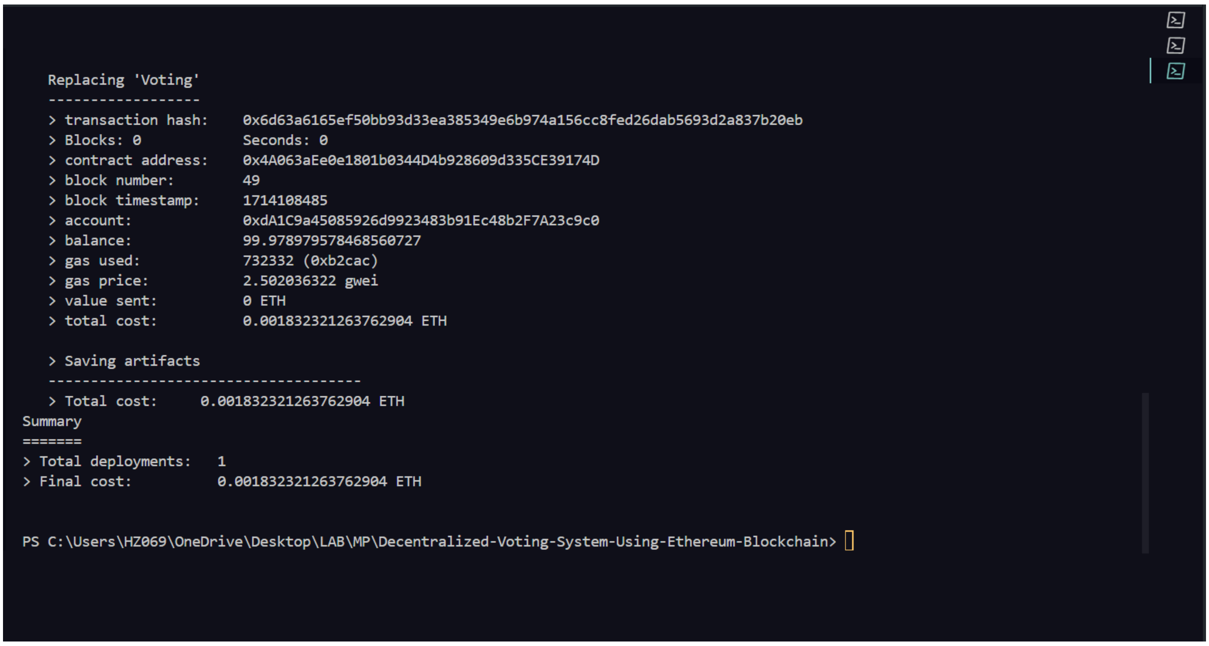
```
PS C:\Users\HZ069\OneDrive\Desktop\LAB\MP\Decentralized-Voting-System-Using-Ethereum-Blockchain> truffle migrate

Compiling your contracts...
===========================
> Compiling .\contracts\Migrations.sol
> Compiling .\contracts\Voting.sol
> Artifacts written to C:\Users\HZ069\OneDrive\Desktop\LAB\MP\Decentralized-Voting-System-Using-Ethereum-Blockchain\build\contracts
> Compiled successfully using:
   - solc: 0.5.16+commit.9c3226ce.Emscripten.clang


Starting migrations...
======================
> Network name:    'development'
> Network id:      5777
> Block gas limit: 6721975 (0x6691b7)


1_initial_migration.js
======================

   Replacing 'Voting'
   ------------------
   > transaction hash:    0x6d63a6165ef50bb93d33ea385349e6b974a156cc8fed26dab5693d2a837b20eb
   > Blocks: 0            Seconds: 0
   > contract address:    0x4A063aEe0e1801b0344D4b928609d335CE39174D
   > block number:        49
   > block timestamp:     1714108485
   > account:             0xdA1C9a45085926d9923483b91Ec48b2F7A23c9c0
```

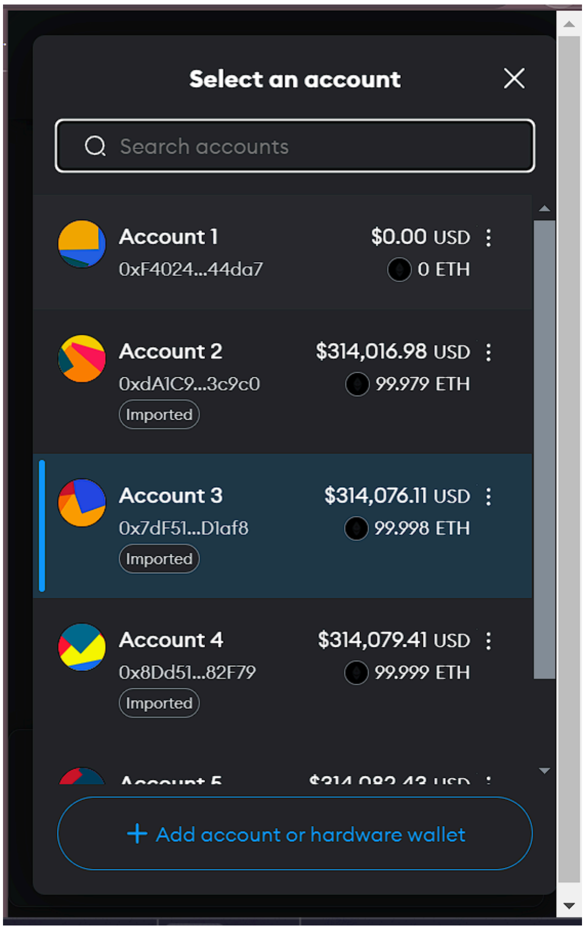


```
   Replacing 'Voting'
   ------------------
   > transaction hash:    0x6d63a6165ef50bb93d33ea385349e6b974a156cc8fed26dab5693d2a837b20eb
   > Blocks: 0            Seconds: 0
   > contract address:    0x4A063aEe0e1801b0344D4b928609d335CE39174D
   > block number:        49
   > block timestamp:     1714108485
   > account:             0xdA1C9a45085926d9923483b91Ec48b2F7A23c9c0
   > balance:             99.978979578468560727
   > gas used:            732332 (0xb2cac)
   > gas price:           2.502036322 gwei
   > value sent:          0 ETH
   > total cost:          0.001832321263762904 ETH

   > Saving artifacts
   -------------------------------------
   > Total cost:     0.001832321263762904 ETH
Summary
=======
> Total deployments:   1
> Final cost:          0.001832321263762904 ETH


PS C:\Users\HZ069\OneDrive\Desktop\LAB\MP\Decentralized-Voting-System-Using-Ethereum-Blockchain> 
```

Terminal Output after Voting



Select an account

Search accounts

Account 1 $0.00 USD
0xF4024...44da7 0 ETH

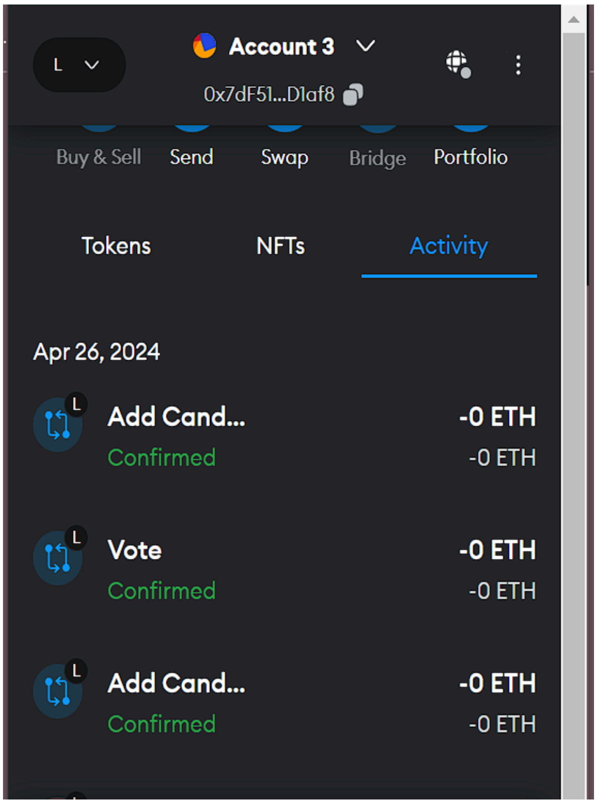
Account 2 $314,016.98 USD
0xdA1C9...3c9c0 99.979 ETH
Imported

Account 3 $314,076.11 USD
0x7dF51...D1af8 99.998 ETH
Imported

Account 4 $314,079.41 USD
0x8Dd51...82F79 99.999 ETH
Imported

Account 5 $314,083.43 USD

+ Add account or hardware wallet



Account 3
0x7dF51...D1af8

Apr 26, 2024

Add Cand... -0 ETH
Confirmed -0 ETH

Vote -0 ETH
Confirmed -0 ETH

Add Cand... -0 ETH
Confirmed -0 ETH

Metamask

Scope for future work

In future iterations, digipolls can be enhanced by implementing additional features such as real-time vote counting, secure voter identification mechanisms, advanced data analytics for voter insights, and integration with emerging technologies like artificial intelligence and biometrics. These enhancements will further enhance the efficiency, security, and accessibility of the voting process, making it more inclusive and trustworthy.

Conclusion:-

This project successfully demonstrates the potential of blockchain technology to provide a transparent, secure, and decentralized voting system. The application showcases the strength of blockchain in maintaining data integrity and public transparency. Future enhancements could include scaling the application to a real-world scenario using the public Ethereum blockchain or integrating biometric authentication for enhanced security.