BITS F452 – BLOCKCHAIN TECHNOLOGY

Final Evaluation

App name: **E-Voting Decentralized Application**

Team Members:

Shaik Mohammed Shaquib(2019A7PS1325H)

Muhammad Bilal Pathan(2019A7PS0149H)

Mohammed Masood Akram(2019A4PS0871H)

Team Number: G14

Video Link:

Preliminaries:

1.)NPM

2.)Truffle

3.)Ganache

4.)Metamask

5.)Coding Language:solidity,html,javascript,css

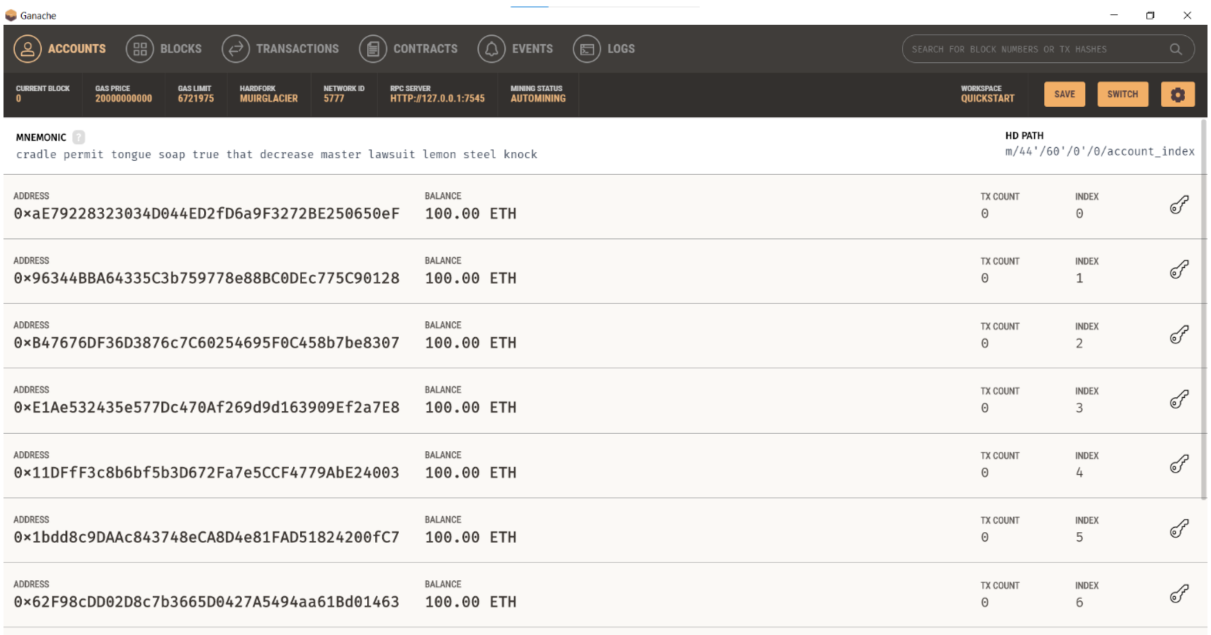
Working:

After logging in to the voting website, the voter must use the Metamask Chrome Extension to connect to the local blockchain. The page is reloaded once the user is connected, and the user may see the candidates and the current votes. Below that is the option to vote for a candidate; the voter selects the candidate and clicks on vote; a metamask pop-up appears, informing the user of the Ethereum transaction that must be completed; once the user clicks on Vote, the vote is given to the selected candidate, assuming the voter has not voted previously. A failed transaction will occur if the user has already voted and attempts to vote again. The vote will not be counted.

Implementation and Results:

1.)**<u>Setting up Ganache:</u>**

The first thing we need to do is start up Ganache and run local blockchain. There will be no transaction after setting up ganache because we haven't done any yet. There is no transaction, as can be seen in the screenshot below.



CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE
0	20000000000	6721975	MUIRGLACIER	5777	HTTP://127.0.0.1:7545	AUTOMINING	QUICKSTART

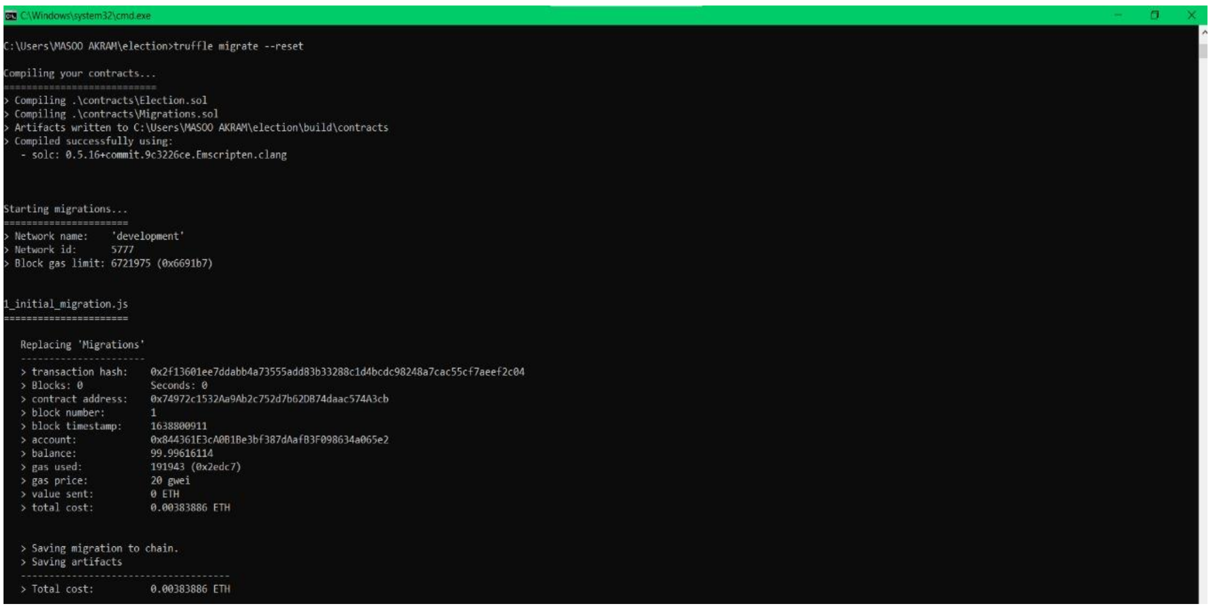
MNEMONIC
cradle permit tongue soap true that decrease master lawsuit lemon steel knock

HD PATH
m/44'/60'/0'/0/account_index

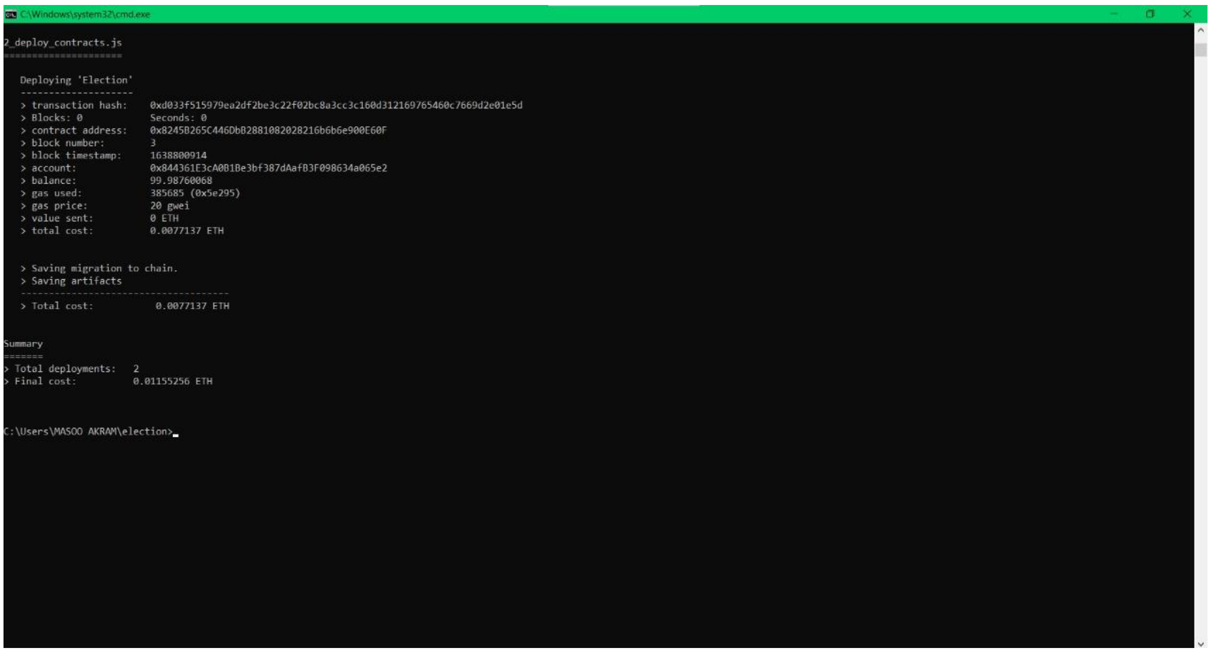
ADDRESS	BALANCE	TX COUNT	INDEX
0×aE79228323034D044ED2fD6a9F3272BE250650eF	100.00 ETH	0	0
0×96344BBA64335C3b759778e88BC0DEc775C90128	100.00 ETH	0	1
0×B47676DF36D3876c7C60254695F0C458b7be8307	100.00 ETH	0	2
0×E1Ae532435e577Dc470Af269d9d163909Ef2a7E8	100.00 ETH	0	3
0×11DFfF3c8b6bf5b3D672Fa7e5CCF4779AbE24003	100.00 ETH	0	4
0×1bdd8c9DAAc843748eCA8D4e81FAD51824200fC7	100.00 ETH	0	5
0×62F98cDD02D8c7b3665D0427A5494aa61Bd01463	100.00 ETH	0	6

By issuing a command on the command line, we can now move the smart contract to the blockchain using the truffle framework.

We've also used cmd to access the NPM directory. The following commands are used to accomplish this:

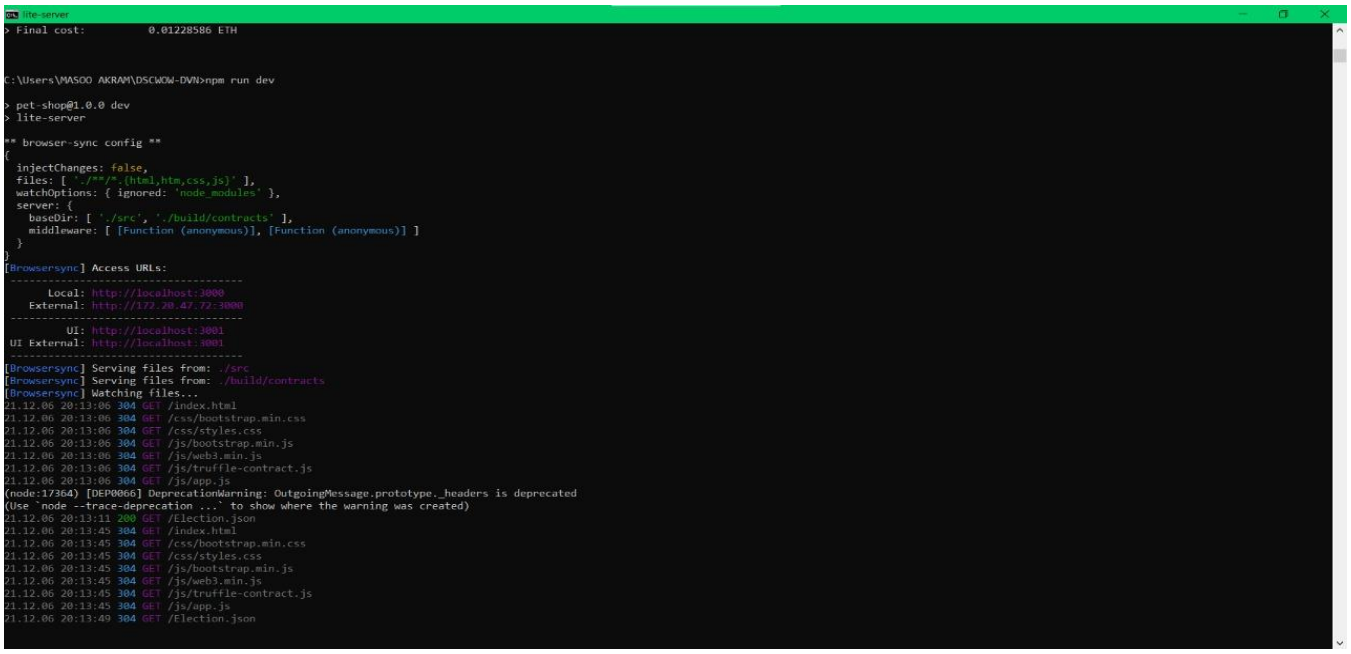


```
C:\Windows\system32\cmd.exe

C:\Users\MASOO AKRAM\election>truffle migrate --reset

Compiling your contracts...
===========================
> Compiling .\contracts\Election.sol
> Compiling .\contracts\Migrations.sol
> Artifacts written to C:\Users\MASOO AKRAM\election\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 'Migrations'
   ----------------------
   > transaction hash:    0x2f13601ee7ddabb4a73555add83b33288c1d4bcdc98248a7cac55cf7aeef2c04
   > Blocks: 0            Seconds: 0
   > contract address:    0x74972c1532Aa9Ab2c752d7b62DB74daac574A3cb
   > block number:        1
   > block timestamp:     1638800911
   > account:             0x844361E3cA0B1Be3bf387dAafB3F098634a065e2
   > balance:             99.99616114
   > gas used:            191943 (0x2edc7)
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.00383886 ETH


   > Saving migration to chain.
   > Saving artifacts
   -------------------------------------
   > Total cost:          0.00383886 ETH
```



```
C:\Windows\system32\cmd.exe

2_deploy_contracts.js
=====================

   Deploying 'Election'
   --------------------
   > transaction hash:    0xd033f515979ea2df2be3c22f02bc8a3cc3c160d312169765460c7669d2e01e5d
   > Blocks: 0            Seconds: 0
   > contract address:    0x8245B265C446DbB2881082028216b6b6e900E60F
   > block number:        3
   > block timestamp:     1638800914
   > account:             0x844361E3cA0B1Be3bf387dAafB3F098634a065e2
   > balance:             99.98760068
   > gas used:            385685 (0x5e295)
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.0077137 ETH


   > Saving migration to chain.
   > Saving artifacts
   -------------------------------------
   > Total cost:           0.0077137 ETH


Summary
=======
> Total deployments:   2
> Final cost:          0.01155256 ETH



C:\Users\MASOO AKRAM\election>_
```

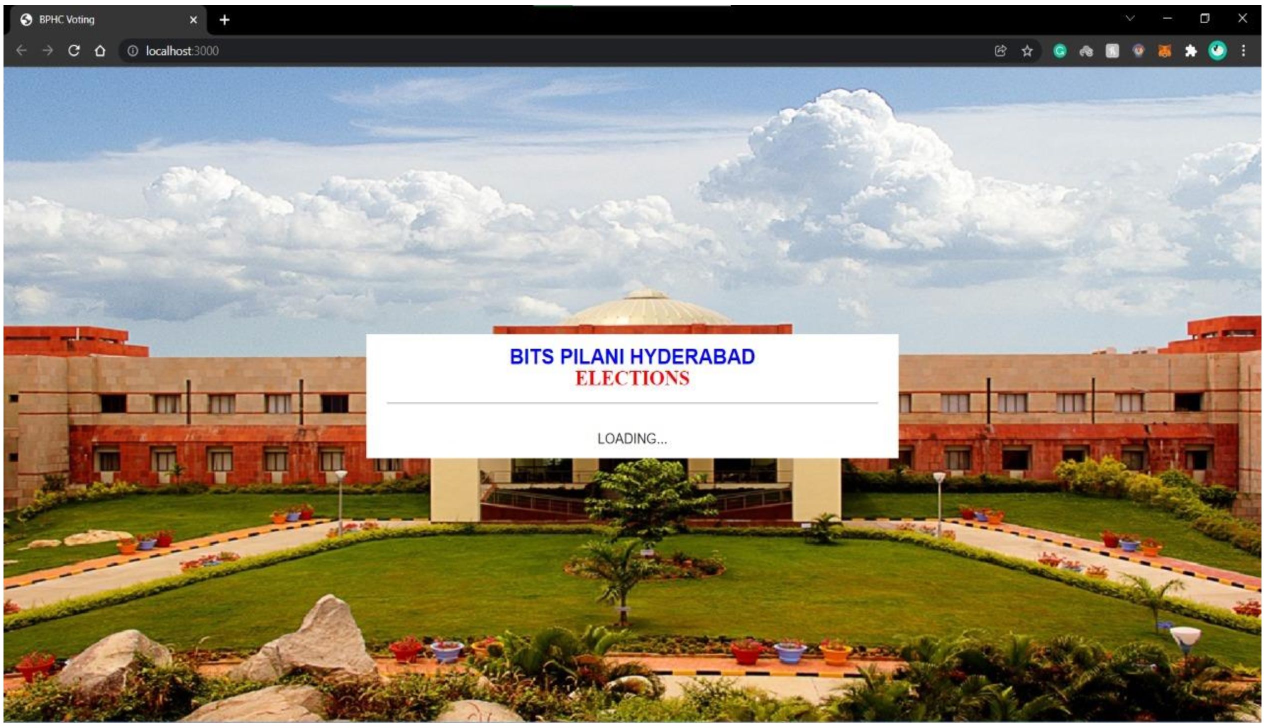
Snapshot of CMD for Truffle Framework



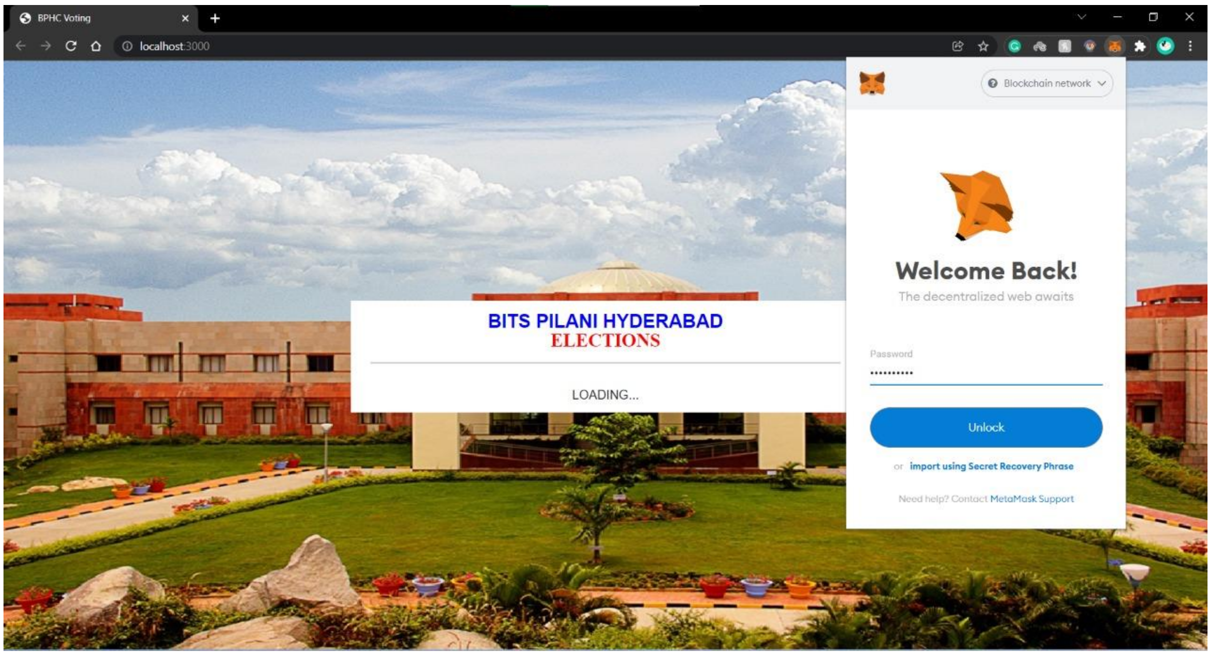
```
lite-server
> Final cost:          0.01228586 ETH



C:\Users\MASOO AKRAM\DSCWOW-DVN>npm run dev

> pet-shop@1.0.0 dev
> lite-server

** browser-sync config **
{
  injectChanges: false,
  files: [ './**/*.{html,htm,css,js}' ],
  watchOptions: { ignored: 'node_modules' },
  server: {
    baseDir: [ './src', './build/contracts' ],
    middleware: [ [Function (anonymous)], [Function (anonymous)] ]
  }
}
[Browsersync] Access URLs:
 --------------------------------------
       Local: http://localhost:3000
    External: http://172.20.47.72:3000
 --------------------------------------
          UI: http://localhost:3001
 UI External: http://localhost:3001
 --------------------------------------
[Browsersync] Serving files from: ./src
[Browsersync] Serving files from: ./build/contracts
[Browsersync] Watching files...
21.12.06 20:13:06 304 GET /index.html
21.12.06 20:13:06 304 GET /css/bootstrap.min.css
21.12.06 20:13:06 304 GET /css/styles.css
21.12.06 20:13:06 304 GET /js/bootstrap.min.js
21.12.06 20:13:06 304 GET /js/web3.min.js
21.12.06 20:13:06 304 GET /js/truffle-contract.js
21.12.06 20:13:06 304 GET /js/app.js
(node:17364) [DEP0066] DeprecationWarning: OutgoingMessage.prototype._headers is deprecated
(Use `node --trace-deprecation ...` to show where the warning was created)
21.12.06 20:13:11 200 GET /Election.json
21.12.06 20:13:45 304 GET /index.html
21.12.06 20:13:45 304 GET /css/bootstrap.min.css
21.12.06 20:13:45 304 GET /css/styles.css
21.12.06 20:13:45 304 GET /js/bootstrap.min.js
21.12.06 20:13:45 304 GET /js/web3.min.js
21.12.06 20:13:45 304 GET /js/truffle-contract.js
21.12.06 20:13:45 304 GET /js/app.js
21.12.06 20:13:49 304 GET /Election.json
```

Snapshot of CMD for NPM directory

2.)<u>User Interface:</u>Users engage with the e-voting system through the user interface. The user will see the UI as seen in the image below. The loading screen will remain active until the electorate logs in using metamask.



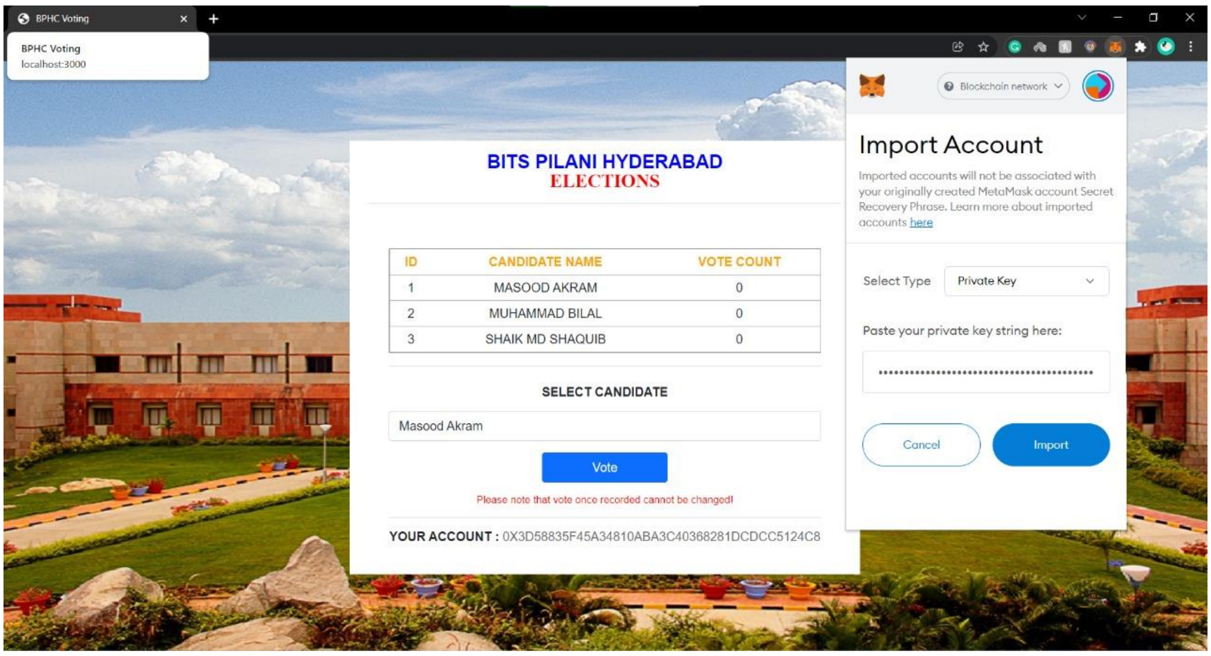
Snapshot of Loading Screen


BPHC Voting
localhost:3000
Blockchain network
Welcome Back!
The decentralized web awaits
Password
Unlock
or import using Secret Recovery Phrase
Need help? Contact MetaMask Support

BITS PILANI HYDERABAD
ELECTIONS

LOADING...

Logging in via Metamask



Import Account

Imported accounts will not be associated with your originally created MetaMask account Secret Recovery Phrase. Learn more about imported accounts here

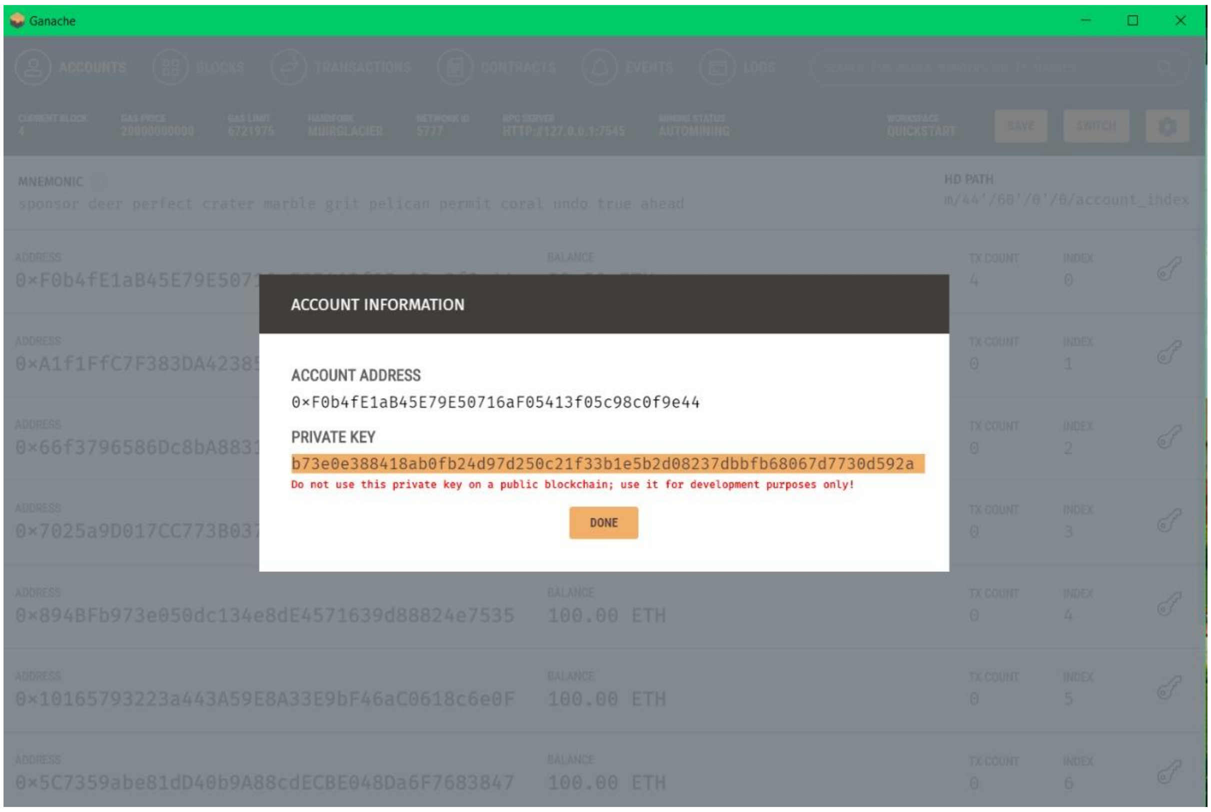
BITS PILANI HYDERABAD
ELECTIONS

ID	CANDIDATE NAME	VOTE COUNT
1	MASOOD AKRAM	0
2	MUHAMMAD BILAL	0
3	SHAIK MD SHAQUIB	0

Please note that vote once recorded cannot be changed!

YOUR ACCOUNT : 0X3D58835F45A34810ABA3C40368281DCDCC5124C8

Main Screen



CURRENT BLOCK 4 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK MUIRGLACIER | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING | WORKSPACE QUICKSTART

MNEMONIC
sponsor deer perfect crater marble grit pelican permit coral undo true ahead

HD PATH
m/44'/60'/0'/0/account_index

ADDRESS	BALANCE	TX COUNT	INDEX
0×F0b4fE1aB45E79E5071		4	0
0×A1f1FfC7F383DA4238		0	1
0×66f3796586Dc8bA8831		0	2
0×7025a9D017CC773B037		0	3
0×894BFb973e050dc134e8dE4571639d88824e7535	100.00 ETH	0	4
0×10165793223a443A59E8A33E9bF46aC0618c6e0F	100.00 ETH	0	5
0×5C7359abe81dD40b9A88cdECBE048Da6F7683847	100.00 ETH	0	6

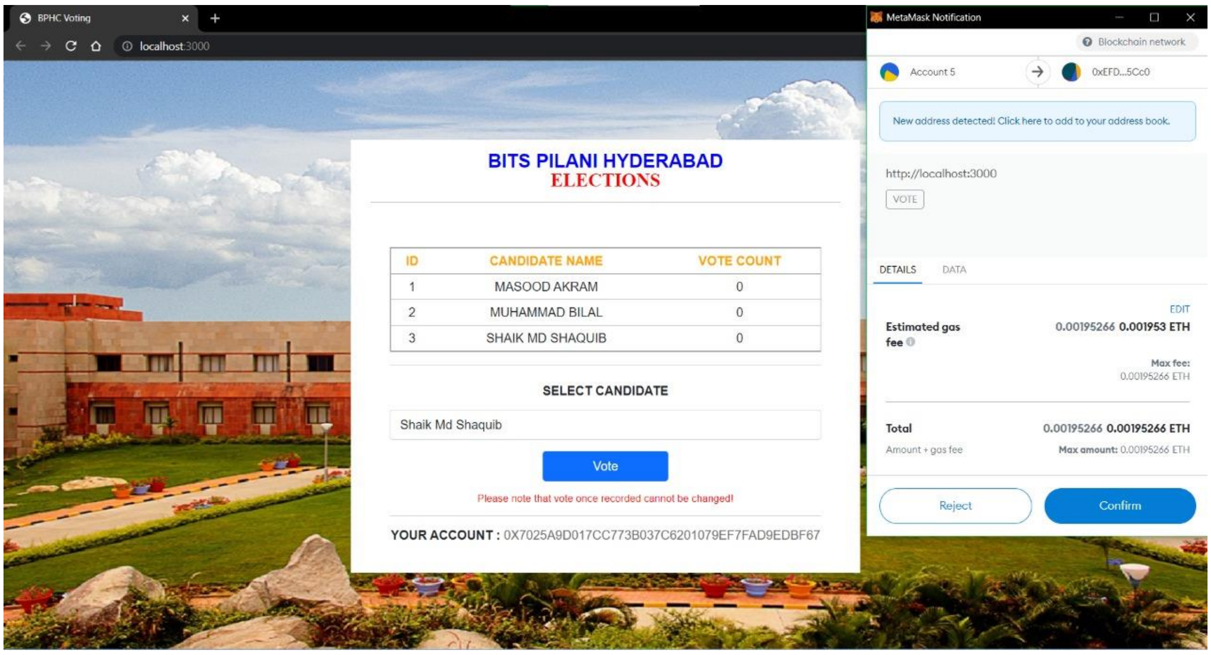
ACCOUNT INFORMATION

ACCOUNT ADDRESS
0×F0b4fE1aB45E79E50716aF05413f05c98c0f9e44

PRIVATE KEY
b73e0e388418ab0fb24d97d250c21f33b1e5b2d08237dbbfb68067d7730d592a
Do not use this private key on a public blockchain; use it for development purposes only!

Private Key

The electorate selects a candidate, and the metamask pop-up appears when the vote button is selected to finalise the transaction.



BITS PILANI HYDERABAD
ELECTIONS

ID	CANDIDATE NAME	VOTE COUNT
1	MASOOD AKRAM	0
2	MUHAMMAD BILAL	0
3	SHAIK MD SHAQUIB	0

SELECT CANDIDATE
Shaik Md Shaquib

Please note that vote once recorded cannot be changed!

YOUR ACCOUNT : 0X7025A9D017CC773B037C6201079EF7FAD9EDBF67

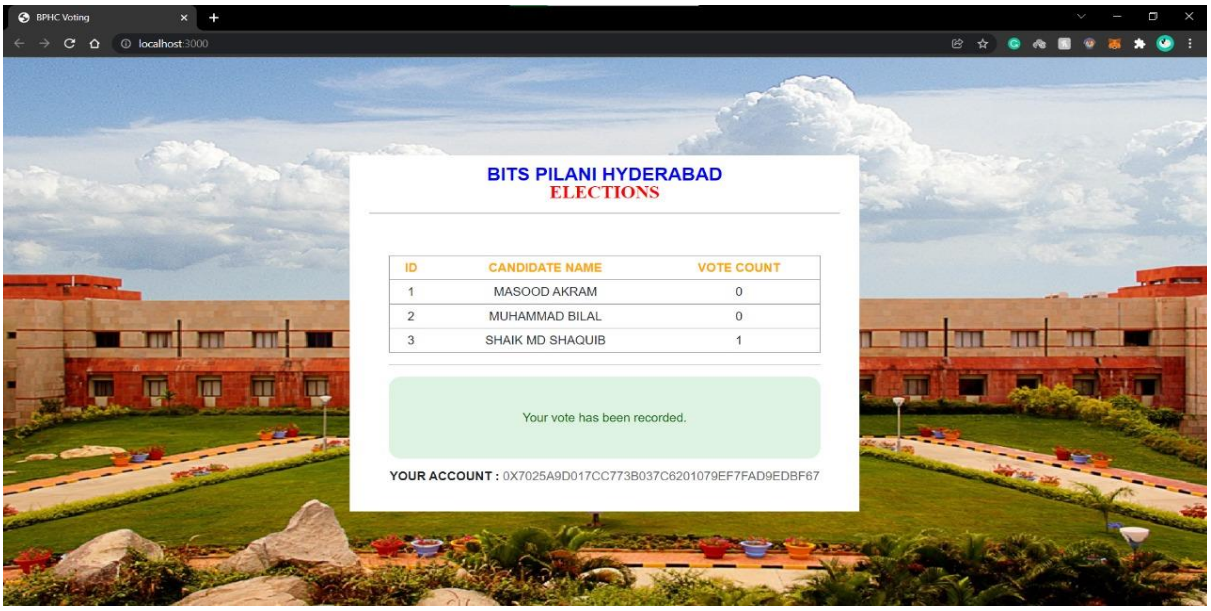
Blockchain network
Account 5 → 0xEFD...5Cc0
New address detected! Click here to add to your address book.
http://localhost:3000
VOTE
DETAILS DATA
EDIT
Estimated gas fee 0.00195266 0.001953 ETH
Max fee: 0.00195266 ETH
Total 0.00195266 0.00195266 ETH
Amount + gas fee
Max amount: 0.00195266 ETH

Snapshot of confirming Transaction

After confirmation, the voter is taken to the main page, where just the results are displayed, but you can no longer vote. Others can also vote by importing their accounts in the same way.

3.)**Checking Transaction:**

The transaction list will be made public to allow users to easily tally their votes. By glancing at the transaction list, people can check the votes they've cast. A transaction list as a whole will be similar to one presented below.



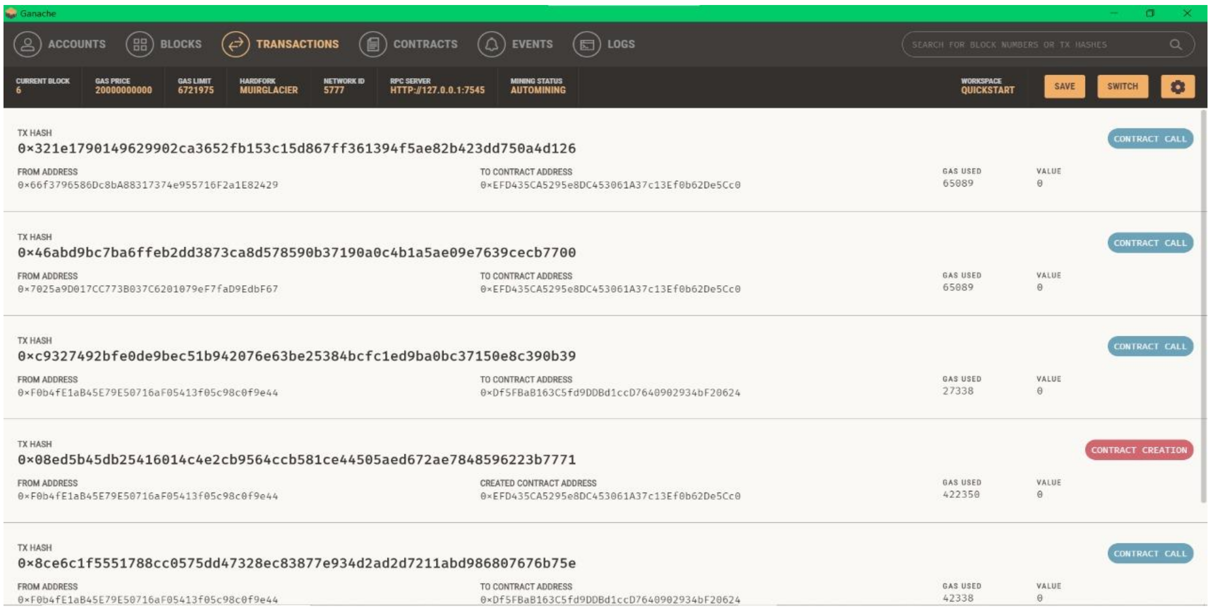
BITS PILANI HYDERABAD
ELECTIONS

ID	CANDIDATE NAME	VOTE COUNT
1	MASOOD AKRAM	0
2	MUHAMMAD BILAL	0
3	SHAIK MD SHAQUIB	1

Your vote has been recorded.

YOUR ACCOUNT : 0X7025A9D017CC773B037C6201079EF7FAD9EDBF67

Snapshot of Result on Main Page



```
CURRENT BLOCK  GAS PRICE    GAS LIMIT  HARDFORK     NETWORK ID  RPC SERVER              MINING STATUS   WORKSPACE
6              20000000000  6721975    MUIRGLACIER  5777        HTTP://127.0.0.1:7545   AUTOMINING      QUICKSTART

TX HASH                                                                                                          CONTRACT CALL
0x321e1790149629902ca3652fb153c15d867ff361394f5ae82b423dd750a4d126
FROM ADDRESS                                  TO CONTRACT ADDRESS                           GAS USED   VALUE
0x66f3796586Dc8bA88317374e955716F2a1E82429    0xEFD435CA5295e8DC453061A37c13Ef0b62De5Cc0    65089      0

TX HASH                                                                                                          CONTRACT CALL
0x46abd9bc7ba6ffeb2dd3873ca8d578590b37190a0c4b1a5ae09e7639cecb7700
FROM ADDRESS                                  TO CONTRACT ADDRESS                           GAS USED   VALUE
0x7025a9D017CC773B037C6201079eF7faD9EdbF67    0xEFD435CA5295e8DC453061A37c13Ef0b62De5Cc0    65089      0

TX HASH                                                                                                          CONTRACT CALL
0xc9327492bfe0de9bec51b942076e63be25384bcfc1ed9ba0bc37150e8c390b39
FROM ADDRESS                                  TO CONTRACT ADDRESS                           GAS USED   VALUE
0xF0b4fE1aB45E79E50716aF05413f05c98c0f9e44    0xDf5FBaB163C5fd9DDBd1ccD7640902934bF20624    27338      0

TX HASH                                                                                                          CONTRACT CREATION
0x08ed5b45db25416014c4e2cb9564ccb581ce44505aed672ae7848596223b7771
FROM ADDRESS                                  CREATED CONTRACT ADDRESS                      GAS USED   VALUE
0xF0b4fE1aB45E79E50716aF05413f05c98c0f9e44    0xEFD435CA5295e8DC453061A37c13Ef0b62De5Cc0    422350     0

TX HASH                                                                                                          CONTRACT CALL
0x8ce6c1f5551788cc0575dd47328ec83877e934d2ad2d7211abd986807676b75e
FROM ADDRESS                                  TO CONTRACT ADDRESS                           GAS USED   VALUE
0xF0b4fE1aB45E79E50716aF05413f05c98c0f9e44    0xDf5FBaB163C5fd9DDBd1ccD7640902934bF20624    42338      0
```

Screenshot of Transaction List

------------------------THE END---------------------