Ethocracy - A decentralised blockchain based voting system

User Manual

Submitted:

07/05/2021

Contributors:

Bartlomiej Kiraga - 17327333

Rónán Mac Gabhann - 17478562

Supervisor:

Dr. Geoffrey Hamilton

1 Introduction

The purpose of this document is to outline the process involved in installing and using the Ethocracy voting application.

2 Installation

In this section we will outline the installation and set up processes required to run the application.

2.1 Requirements

System Requirements

OS: Windows 10 / macOS X / Ubuntu LTS / Fedora 34

Any modern device running an appropriate operating system for our software requirements can run this application.

Mobile devices can not support the development build due to the need for development tools such as Truffle, but would be able to interface with a live, deployed instance. This is outside of the scope of our project and would require a server and investment in the form of ETH (Ether).

Software requirements

- Nodejs v12.19.0+
- npm v6.14.8+
- Truffle v5.1.55
- Google Chrome or Mozilla Firefox web browser
- MetaMask

Nodejs is used to host a server and catalogue active elections.

Node package manager (npm) is used to install third party dependencies.

Truffle is used to simulate a local Ethereum blockchain to facilitate our development build.

Google Chrome or Mozilla Firefox is used alongside MetaMask to interact with a ReactJS interface to the smart contracts on the blockchain. The web browser displays UI elements and keeps track of local variables whereas Metamask is used to send data in the form of transactions to the blockchain.

2.2 Dependencies Installation Guide

1. Install npm and node.js
    a. For Ubuntu, input the following into the terminal:

    ```
    sudo apt install nodejs npm
    ```

    b. For Fedora 34, input the following into the terminal:

    ```
    sudo dnf install nodejs npm
    ```

    c. For Windows/macOS X:
        i. Visit https://nodejs.org/en/download/
        ii. Download and run the appropriate installer.

2. Install Truffle using the following command in the local terminal:

    ```
    npm install -g truffle
    ```

3. Using your native browser, download and install a supported web browser:

    a. Google Chrome is available for download here: https://www.google.com/chrome/
    b. Mozilla Firefox is available for download here: https://www.mozilla.org/en-US/firefox/new/

4. Install MetaMask as an addon to Chrome or Firefox:
    a. Visit https://metamask.io/download.html
    b. The download link will redirect you to the appropriate browser add ons hub where you can finish the installation process.
    c. Ensure the extension is enabled under Settings > Extensions.
5. (Windows only): Download and install Git for Windows from https://git-scm.com/download/win

With these tools we are ready to install third party libraries(npm), simulate a blockchain locally (Truffle), connect to the web interface (web browser) and send data to our blockchain (MetaMask).

2.3 Blockchain Setup Guide

Clone the application files from GitLab using the following command in the local terminal:

```
git clone https://gitlab.computing.dcu.ie/kiragab2/2021-ca400-kiragab2-macgabr2.git
```

Navigate to /2021-ca400-kiragab2-macgabr2/src/Ethocracy inside of the cloned repository. And input the following commands into the terminal in order:

1. To compile the smart contracts into ABI (Application Binary Interface):

   ```
   truffle compile --all
   ```

2. To create a local sample blockchain:

   ```
   truffle develop
   ```

3. To deploy your compiled ABIs onto your local sample blockchain:

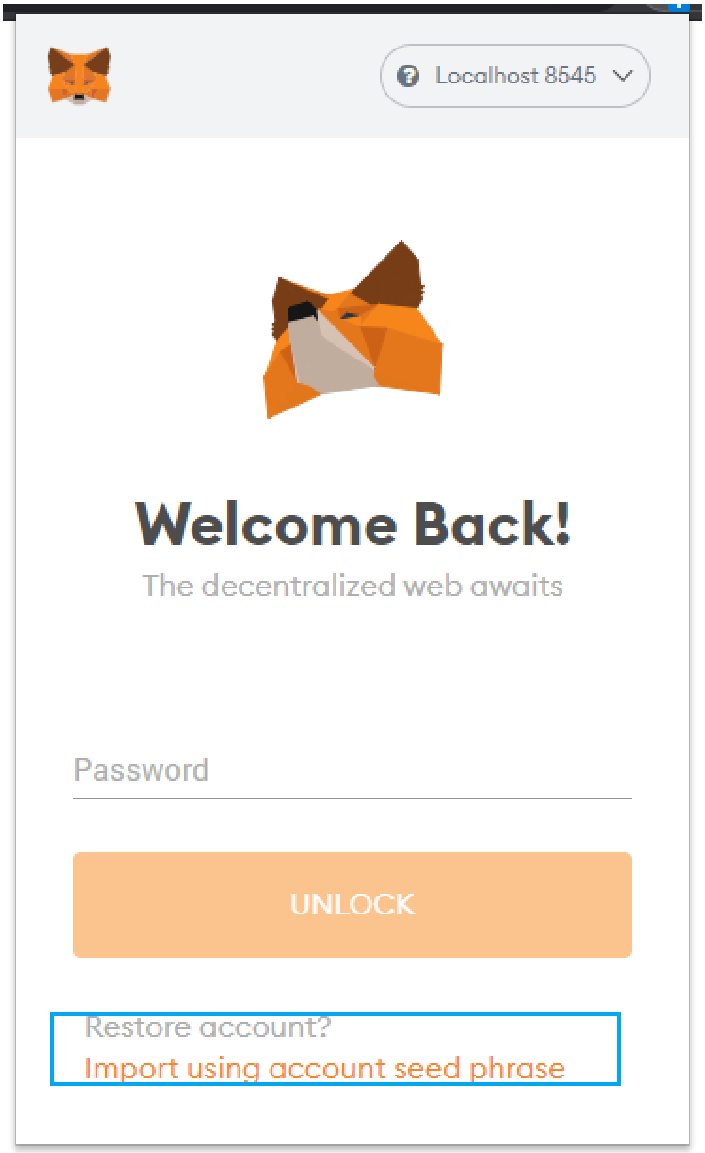
   ```
   truffle migrate --reset
   ```

The blockchain serves as a publicly shared ledger which includes all transactions to and from different addresses on the blockchain. Voters will each have their own address, and in step 3 smart contracts which act as programs stored on the blockchain are given their own address. Voters will send data to these smart contracts in the form of transactions to cast their encrypted ballot. These smart contracts will release the results when the election has ended.

Normally, voters and/or election administrators would be required to pay “gas” fees to perform computations and transact data on the Ethereum network, however, since we are simulating the blockchain on our own computer, these gas fees can be waived and all relevant computations and transactions will be done locally.

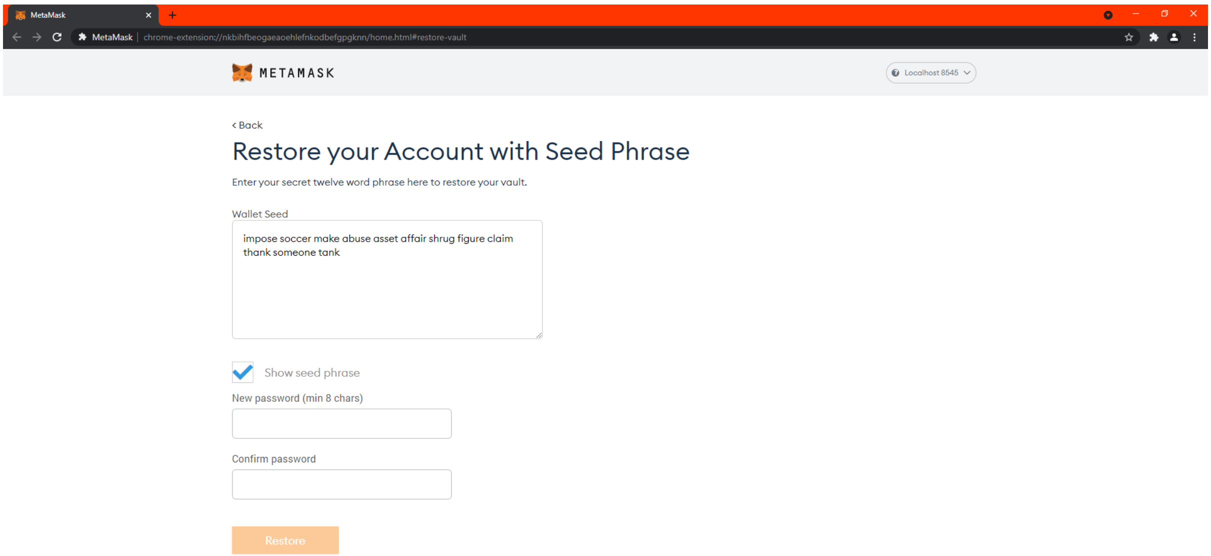
2.4 MetaMask Setup Guide

A MetaMask account is required to load the webpage and its features. Click the fox icon in the toolbar or addons menu to bring up the sign in page below.


Welcome Back!

The decentralized web awaits

To make things easier to set up, select “Import using account seed phrase” and you will be redirected to the page below.


MetaMask
MetaMask
chrome-extension://nkbihfbeogaeaoehlefnkodbefgpgknn/home.html#restore-vault
METAMASK
Localhost 8545
< Back

Restore your Account with Seed Phrase

Enter your secret twelve word phrase here to restore your vault.

Wallet Seed

impose soccer make abuse asset affair shrug figure claim thank someone tank

☑ Show seed phrase

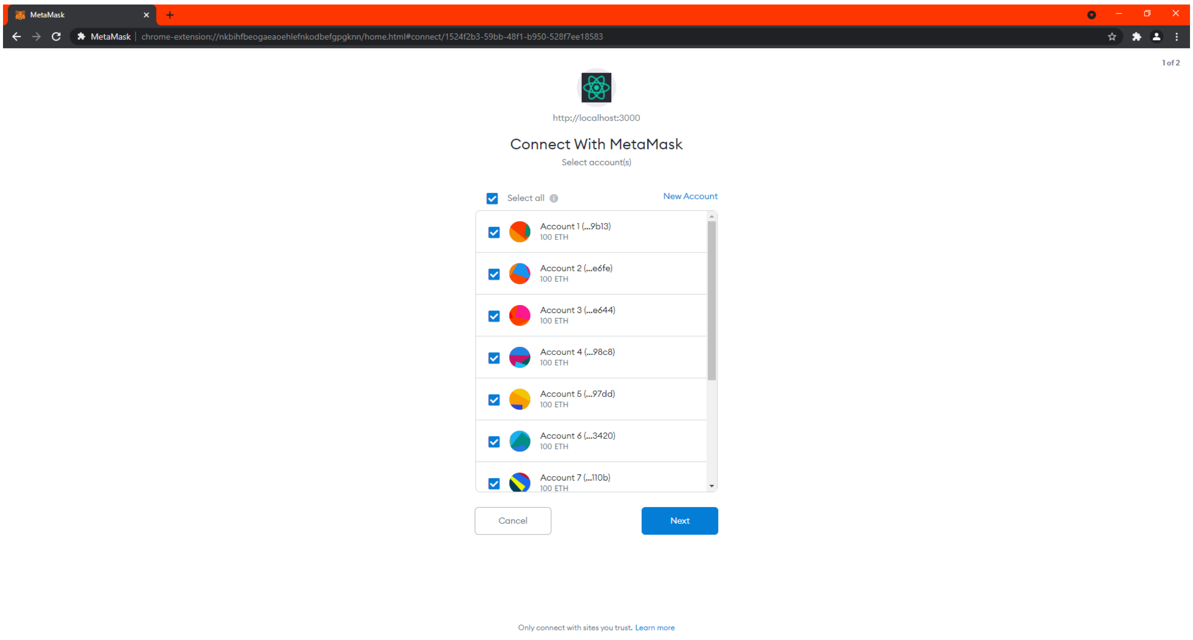
New password (min 8 chars)

Confirm password

You can import accounts using the following seed phrase:

impose soccer make abuse asset affair shrug figure claim thank someone tank

Copy and paste this seed phrase into the “Wallet Seed” entry, and create a password. This seed phrase will generate 10 accounts with 100 ETH to spend on the localhost:8545 network.



MetaMask
MetaMask | chrome-extension://nkbihfbeogaeaoehlefnkodbefgpgknn/home.html#connect/1524f2b3-59bb-48f1-b950-528f7ee18583
1 of 2

http://localhost:3000

Connect With MetaMask

Select account(s)

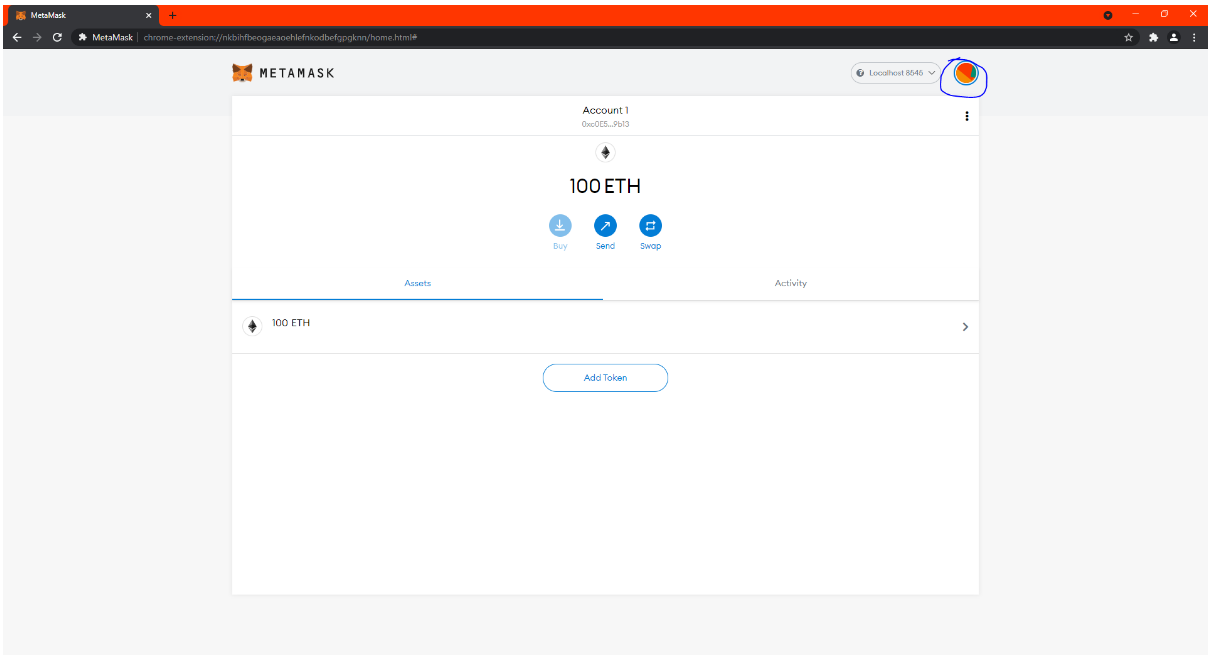
☑ Select all　　New Account

☑ Account 1 (...9b13) 100 ETH
☑ Account 2 (...e6fe) 100 ETH
☑ Account 3 (...e644) 100 ETH
☑ Account 4 (...98c8) 100 ETH
☑ Account 5 (...97dd) 100 ETH
☑ Account 6 (...3420) 100 ETH
☑ Account 7 (...110b) 100 ETH

Only connect with sites you trust. Learn more

“Select all” accounts. Each account represents a voter and new accounts can be added at any time.

On a successful wallet import you should see the page below, where wallets can be cycled through the highlighted button in the top right corner.



MetaMask
MetaMask | chrome-extension://nkbihfbeogaeaoehlefnkodbefgpgknn/home.html#
METAMASK
Localhost 8545

Account 1
0xc0E5...9b13

100 ETH

Buy
Send
Swap
Assets
Activity

100 ETH

2.5 Application Setup Guide

Now that we have our blockchain set up, our smart contracts deployed, and our MetaMask ready, we will set up our interface to interact with it.

Navigate to /2021-ca400-kiragab2-macgabr2/src/Ethocracy/client and input the following commands into the terminal in order:

1. To install npm dependencies:

```
npm install
```

2. To run the client:

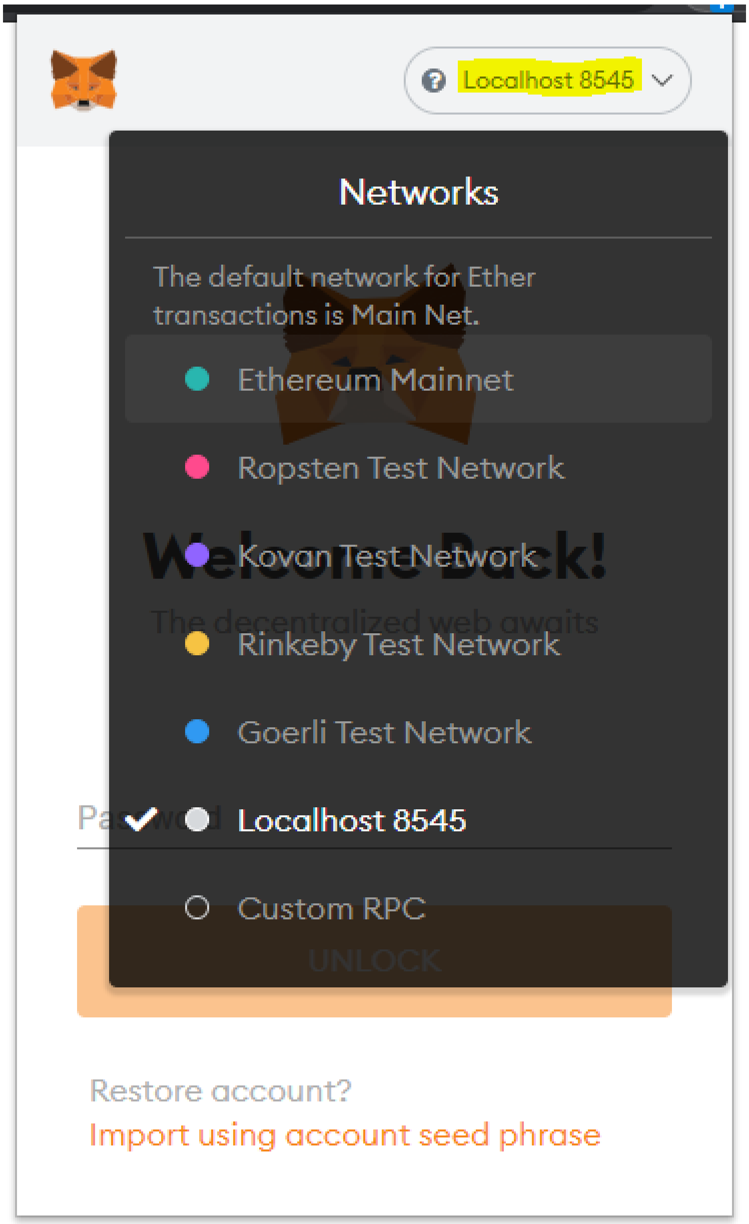
```
npm run dev
```

The interface should now be accessible at localhost:3000

3 Usage

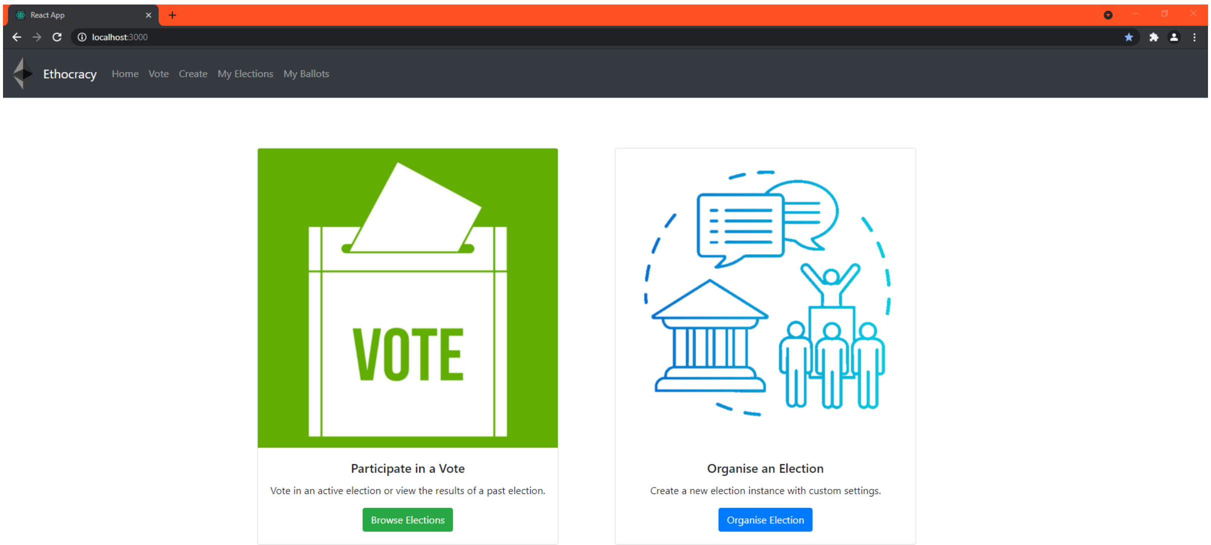
3.1 Landing Page

If you are having problems reaching the landing page, ensure you are signed into MetaMask and connected to our local blockchain at localhost:8545



The default network for Ether transactions is Main Net.

Upon signing in the user should be brought to the landing page. Here the user can choose between participating in a vote, or organising an election themselves. We will start off by organising an election.



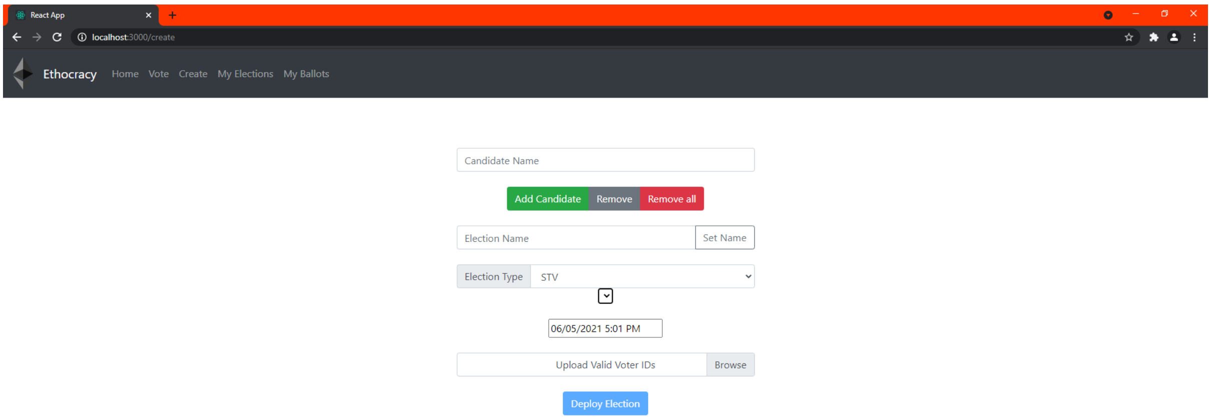
Participate in a Vote

Vote in an active election or view the results of a past election.

Organise an Election

Create a new election instance with custom settings.

3.2 Election Deployment



Election Type: STV

06/05/2021 5:01 PM

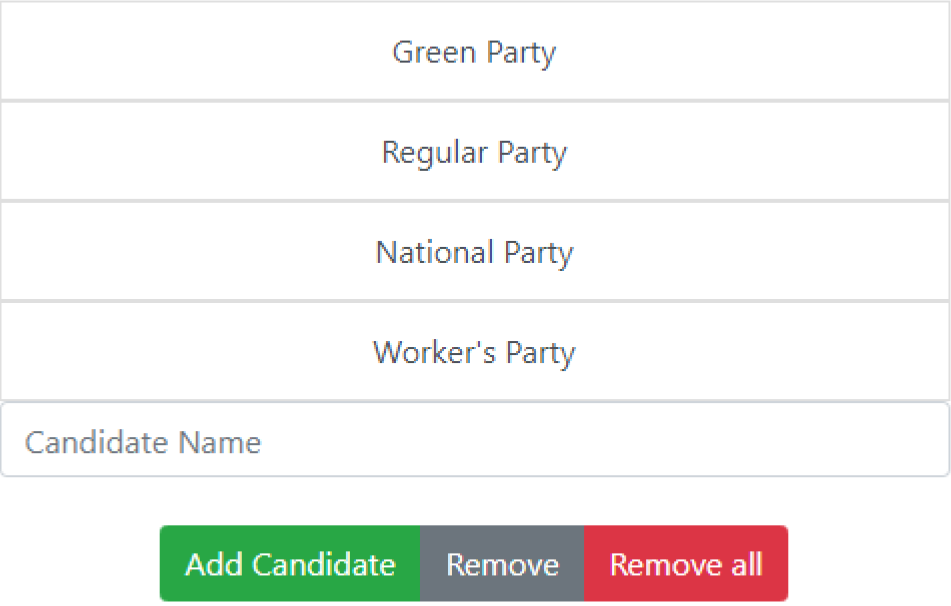
You’ll arrive at the election deployment page, where you can set election parameters and deploy your own instance of an election to the blockchain where authorised voters can interact with it. The below steps walk you through setting up a sample election.

1. Create a text file containing valid voter identification numbers separated by commas.

For example:
1955693353,2908926482,4816510405,3208580699,4763676177,5169435420,7025449739,6198738570,0832271041,0850843842

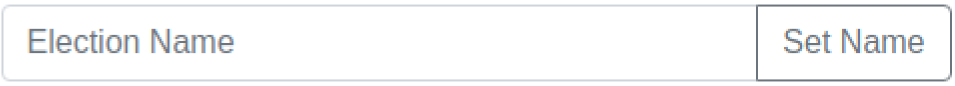
2. Share Voter IDs with registered, authorised voters.

3. In the “Create” page of the application add election candidates’ names by using the “Add Candidate” field. Chosen candidate names appear above the field after each addition and can be removed by clicking on their names, or by using the provided buttons.

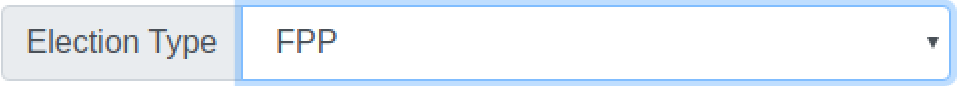


Note: Smart Contracts only handle ASCII characters to save on gas

4. In the “Election name” field input a unique election name. Eg. “National Elections”

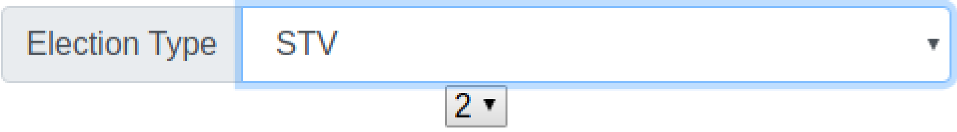


5. Choose either First Past the Post or Single Transferable Vote to determine how the ballots are cast and how votes are tallied.



Election Type FPP

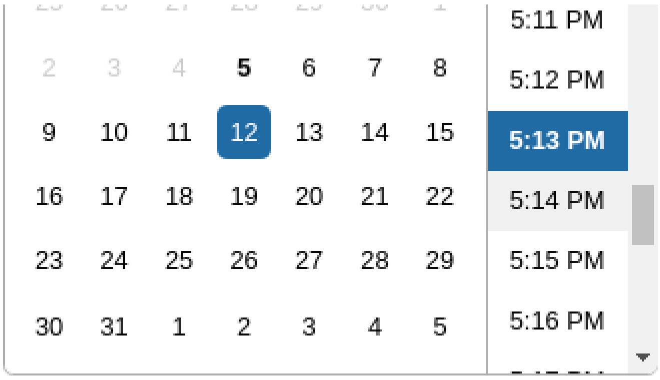
6. In the case of selecting the Single Transferable Vote election type, also input the number of seats available.



Election Type STV

2

7. Set the deadline of the election using the date picker field.

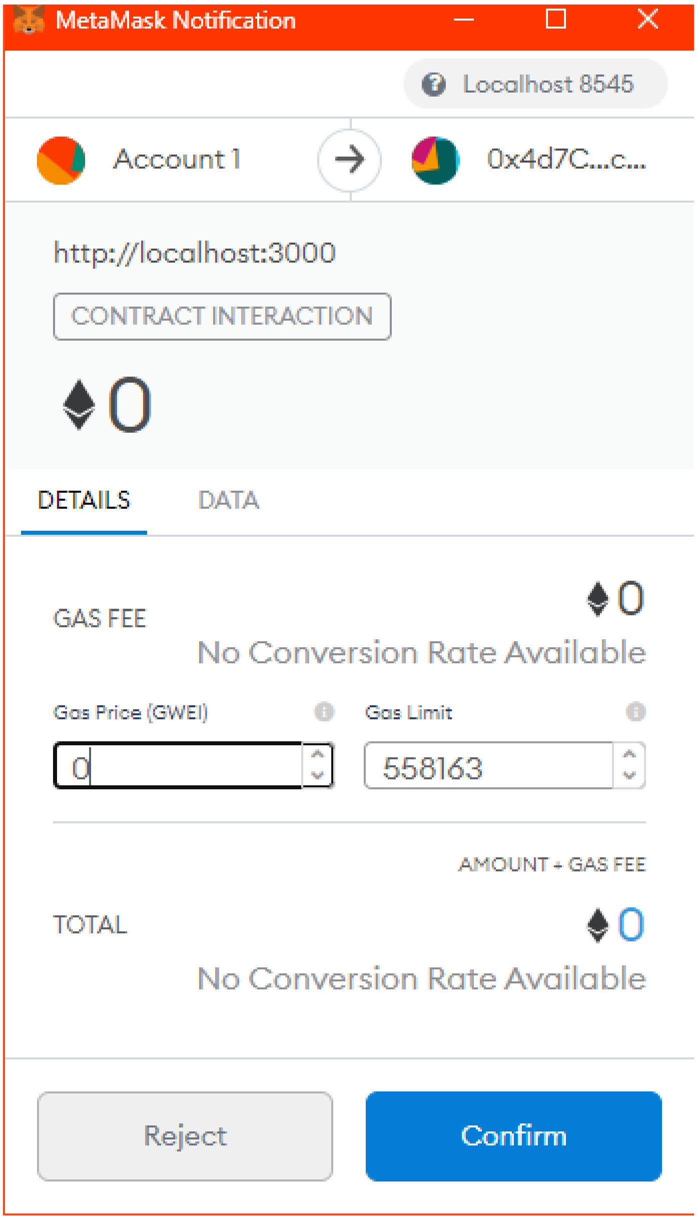


2	3	4	**5**	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

5:11 PM
5:12 PM
5:13 PM
5:14 PM
5:15 PM
5:16 PM

8. Select the “Add Voters” option and upload for the voter ID text file you created in step one.

9. Send your election data to the blockchain by pressing the “Deploy Election” button. You may be asked to confirm this transaction via MetaMask and click Confirm. (If you are told you do not have the required gas to do so, set “Gas Price GWEI” to 0).



MetaMask Notification

Localhost 8545

Account 1 → 0x4d7C...c...

http://localhost:3000

CONTRACT INTERACTION

♦0

DETAILS DATA

GAS FEE ♦0
No Conversion Rate Available

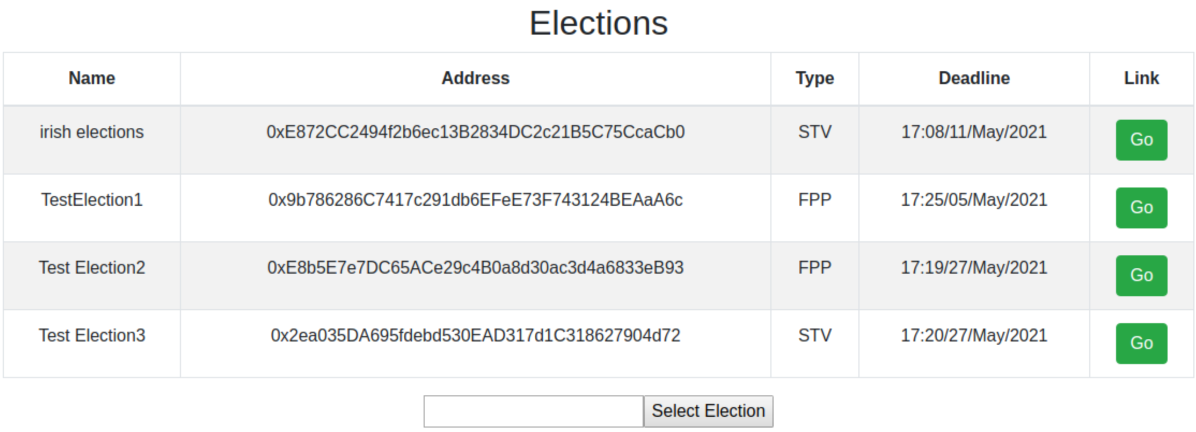
Gas Price (GWEI): 0
Gas Limit: 558163

AMOUNT + GAS FEE
TOTAL ♦0
No Conversion Rate Available

10. All of the user’s created elections can be seen after clicking the “My Elections” section of the navigation bar, it will also be publicly visible in the “Vote” section to all users.

3.3 Election Voting

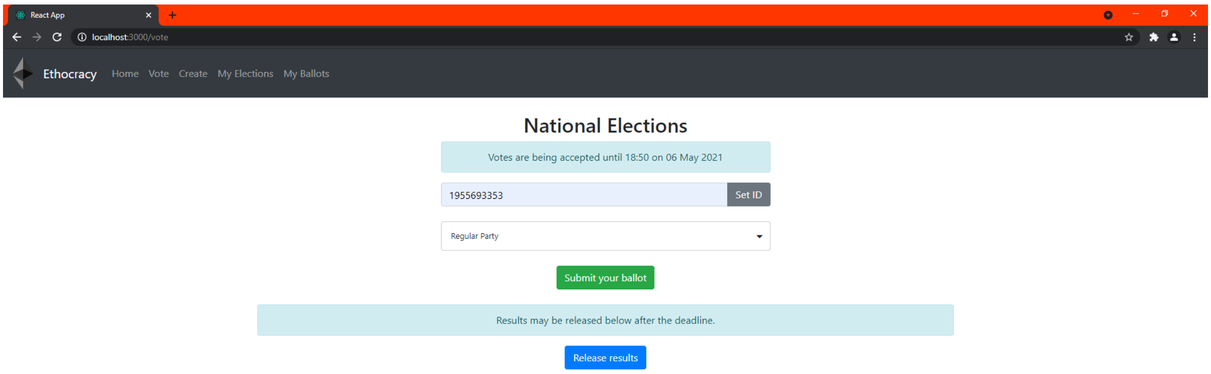
1. In the “Vote” page of the application, input the chosen election address into the text field located below the table of elections, or alternatively click the green “Go” button located to the side of the chosen election.



Elections

Name	Address	Type	Deadline	Link
irish elections	0xE872CC2494f2b6ec13B2834DC2c21B5C75CcaCb0	STV	17:08/11/May/2021	Go
TestElection1	0x9b786286C7417c291db6EFeE73F743124BEAaA6c	FPP	17:25/05/May/2021	Go
Test Election2	0xE8b5E7e7DC65ACe29c4B0a8d30ac3d4a6833eB93	FPP	17:19/27/May/2021	Go
Test Election3	0x2ea035DA695fdebd530EAD317d1C318627904d72	STV	17:20/27/May/2021	Go

2. Input a valid user Voter ID and select your preferred candidate. Here our valid voter ID is 1955693353 and our preferred candidate is the Regular Party.



National Elections

Votes are being accepted until 18:50 on 06 May 2021

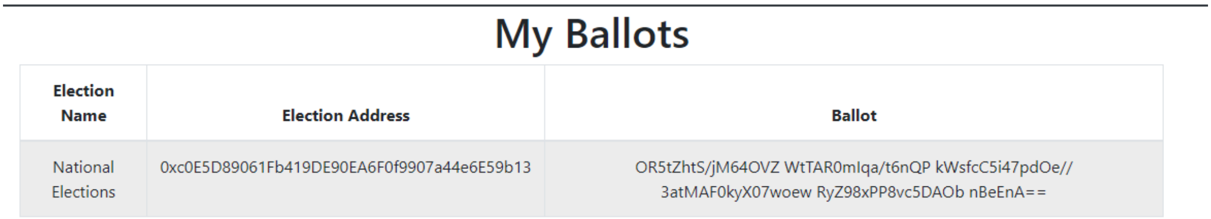
1955693353

Regular Party

Results may be released below after the deadline.

3. Select your preferred candidate from the drop down candidate list. If the election is of the Single Transferable Vote type, you may select multiple candidates in the order of preference. Press the “Submit your ballot” button when you’re happy with your selection. You will again be asked to confirm the transaction by MetaMask.

4. To confirm the existence of the cast ballot, click on the “My Ballots” navigation bar element which will display all ballots cast by the user. (Note that this does not provide you with information on who you voted for, as that form of proof is purposefully not given to voters in real-world voting to prevent voters being forced to vote for a particular candidate, or voters selling their vote using said proof as evidence)



My Ballots

Election Name	Election Address	Ballot
National Elections	0xc0E5D89061Fb419DE90EA6F0f9907a44e6E59b13	OR5tZhtS/jM64OVZ WtTAR0mIqa/t6nQP kWsfcC5i47pdOe// 3atMAF0kyX07woew RyZ98xPP8vc5DAOb nBeEnA==

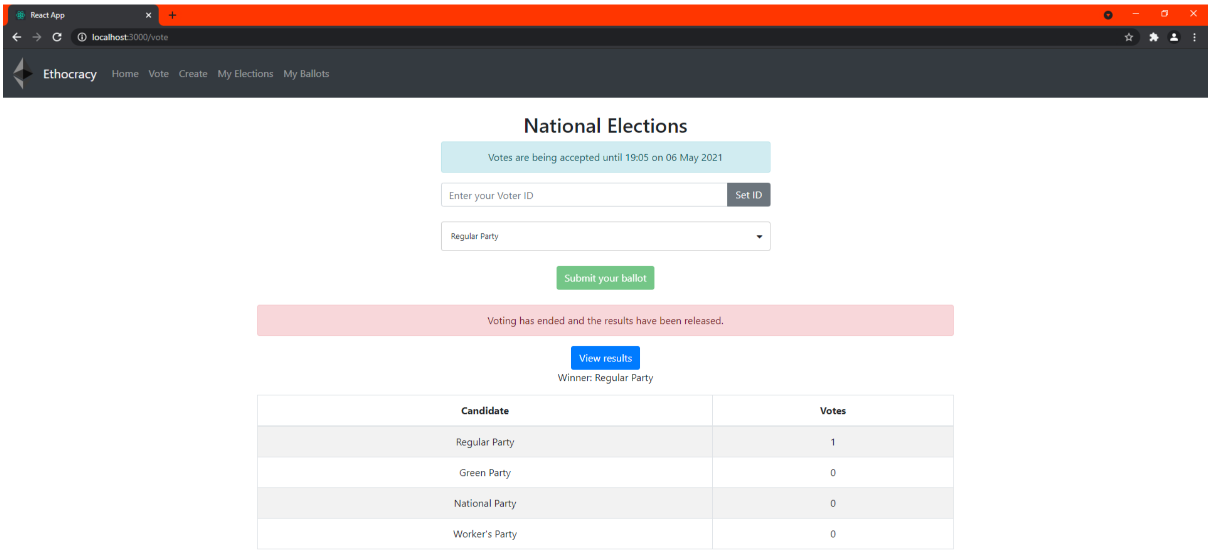
3.4 Election Results

1. To display the results of an election, navigate to the “Vote” section of the app.

2. Select the election from the election list by pasting its address into the “Select Election” field or by clicking the “Go” button located beside it.

3. If the election voting stage is over a user has to release the results by clicking the Release results button. This only has to be done by a single user once after the deadline has passed.

4. The results are then displayed in a tabular format whenever a user selects the “View Results” option.



National Elections

Votes are being accepted until 19:05 on 06 May 2021

Voting has ended and the results have been released.

Winner: Regular Party

Candidate	Votes
Regular Party	1
Green Party	0
National Party	0
Worker's Party	0

Regular Party has won the election with 1 vote