BALLOT BOX

CAST YOUR VOTE SAFELY

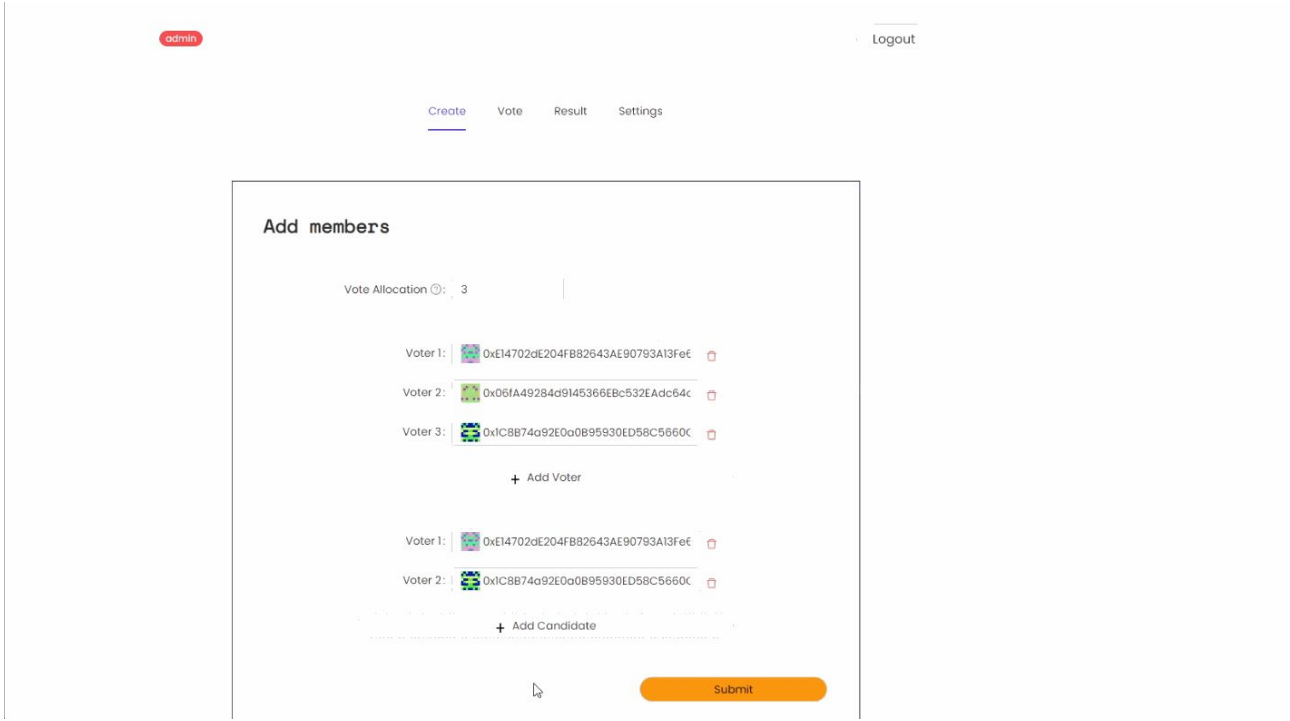
Team 6

Kinshuk Chopra 2018239 | Sandeep Kumar Singh 2018363 | Sarthak Arora 2018307

Website : https://wonderful-fermi-06e25d.netlify.app/

Link

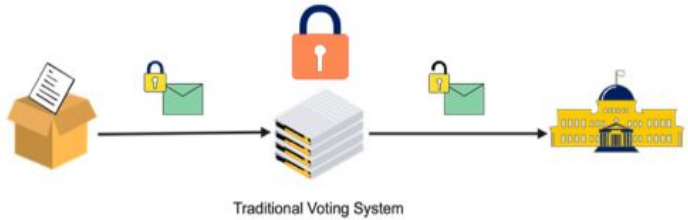
Project Overview



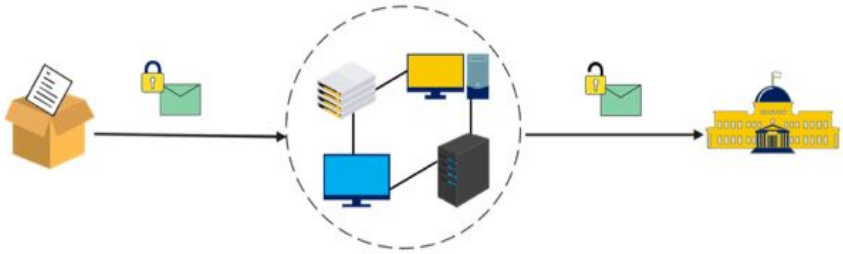
- End to end secure & Cost-efficient
- Guaranteeing voters privacy
- Multi-Weight Vote Mechanism
- Admin can add Voters
- Admin can add Candidates

Motivation

With the onset of electronic voting in the 21st century, **blockchain** can play an important role in electronic voting as the current approach is vulnerable to **errors** and **exploitation**. Using blockchain today's voters can exercise their democratic rights and responsibilities online, track their voting status as well as verify when **counts** are made. **Features like multi weighted and multi voting is not yet explored** using blockchain and could potentially have a huge impact on the voting technologies.



Traditional Voting System



Blockchain Voting System

Related Work: Academic

A Decentralized Voting System by *Ahlkvist et al*

- Investigate the feasibility of designing a decentralised e-voting system and implementing a **proof-of-concept** prototype that ensures **transparency**, **privacy**, **correctness**, and **integrity**.
- They were able to build a promising prototype but were unable to overcome the Scalability Trilemma, which states that as decentralisation increases, scalability and security suffer.
- The issue with the scalability of transaction throughput in public blockchains was perhaps the most obvious trade-off.

Blockchain-Based E-Voting System by *Hjálmarsson et al*

- For countries of greater size, Hjálmarsson et al. explain that some measures must be taken to **limit transaction throughput per second**, such as the parent & child architecture.
- This reduces the number of transactions stored on the blockchain to a **1:100 ratio** without jeopardising the network's security.

Related Work: Academic

Secure Digital Voting System based on Blockchain Technology by *Khan et al*

- They describe a system that was created to support a voting application in a real-world setting while taking into account specific requirements like **privacy**, **eligibility**, **convenience**, **receipt-freeness**, and **verifiability**.
- The transaction's cryptographic hash (ID) is emailed to the voter as proof that the vote was cast, and it can later be tracked outside the constituency's boundaries.
- Multiple systems have been developed that are not directly voting systems but are based on similar principles.

Blockchain for Electronic Voting System—Review and Open Research Challenges by *Jafar et al*

- According to Jafar et al., they do not fully understand all of the risks associated with the security and scalability of blockchain-based electronic voting systems because more research is needed.
- Users may be exposed to unanticipated security risks and flaws if they use blockchain voting methods.

Related Work: Commercial

Follow My Vote

- Inspired by a voting booth
- Proper verification by the organization to open the ballot box.

Voatz

- Voatz uses smartphone-based voting as well as biometric confirmation.

Polyas

- Uses blockchain to create an electronic voting system for the public and private sectors.
- Polyas is used by a lot of big companies in Germany.

Related Work: Commercial

Polys

- Transparent crypto-algorithm-backed blockchain-based online voting platform.
- Polys assists student councils, and unions in organising polls

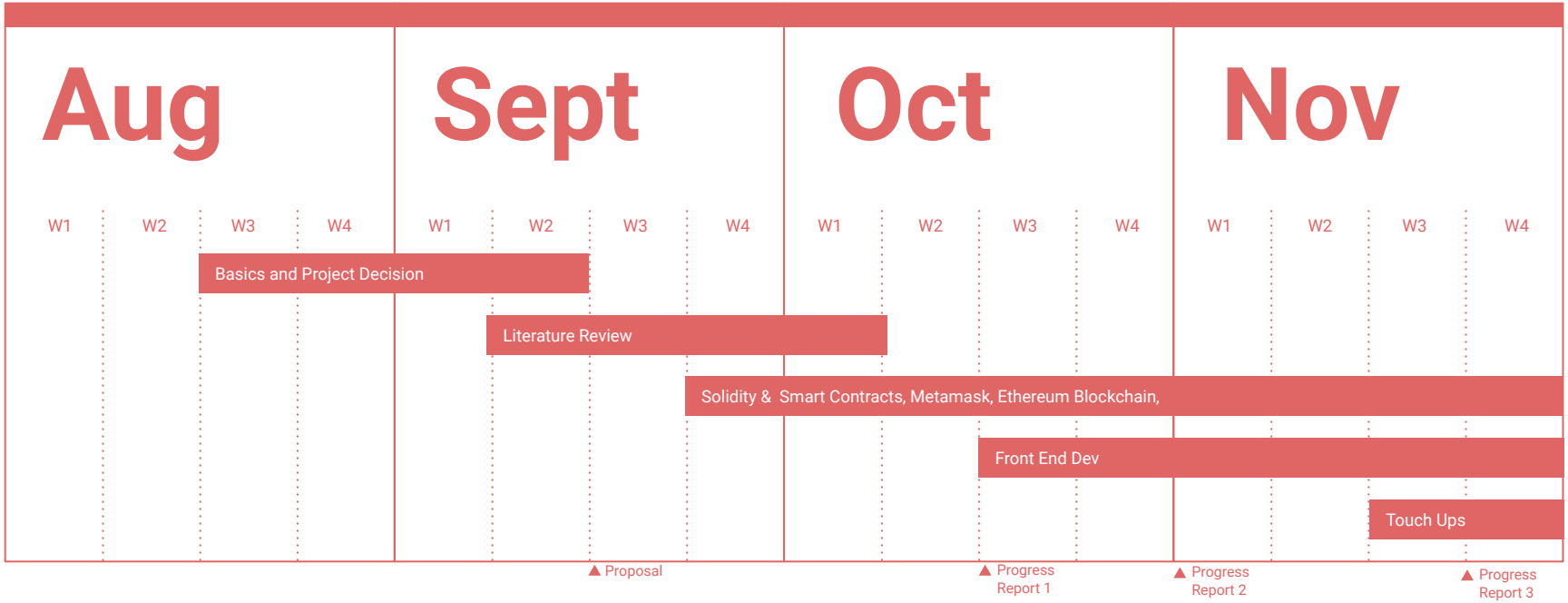
Agora

- Architecture based on a custom blockchain, unique participatory security, and a legitimate consensus mechanism.
- Vote is the native token.

Our Aim

- Create an **blockchain based e-voting platform**.
- This would include multi-stakeholder profiles like **admin, candidate and voter**.
- We aim to **implement a multi-weighted and multi-votes voting mechanism** in a blockchain.
- We aim to **create a secure and cost-efficient way to conduct elections**, also all the **codebase including the contracts would be made public**.
- This platform can then be **further upgradable** to be used in more complex level elections.

Timeline

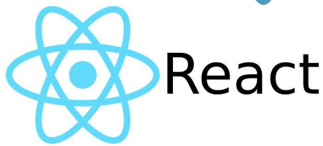

Aug
Sept
Oct
Nov
W1
W2
W3
W4
Basics and Project Decision
Literature Review
Solidity & Smart Contracts, Metamask, Ethereum Blockchain,
Front End Dev
Touch Ups
Proposal
Progress Report 1
Progress Report 2
Progress Report 3

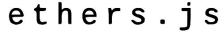
Tech Stack

- **Solidity and Remix IDE** for implementing smart contracts.
- **Metamask** was used to connect our browser with the Ethereum network as an Ethereum Node without having the need to download the blockchains.
- **HardHat** was used as a development environment to compile, deploy, test, and debug our Ethereum application and contracts.
- **Ethers JS** was used to interact with the Ethereum Blockchain and its ecosystem.
- **React JS and Netlify** were used for building and deploying frontend.
- **Express JS and Heroku** were used for building and deploying backend.

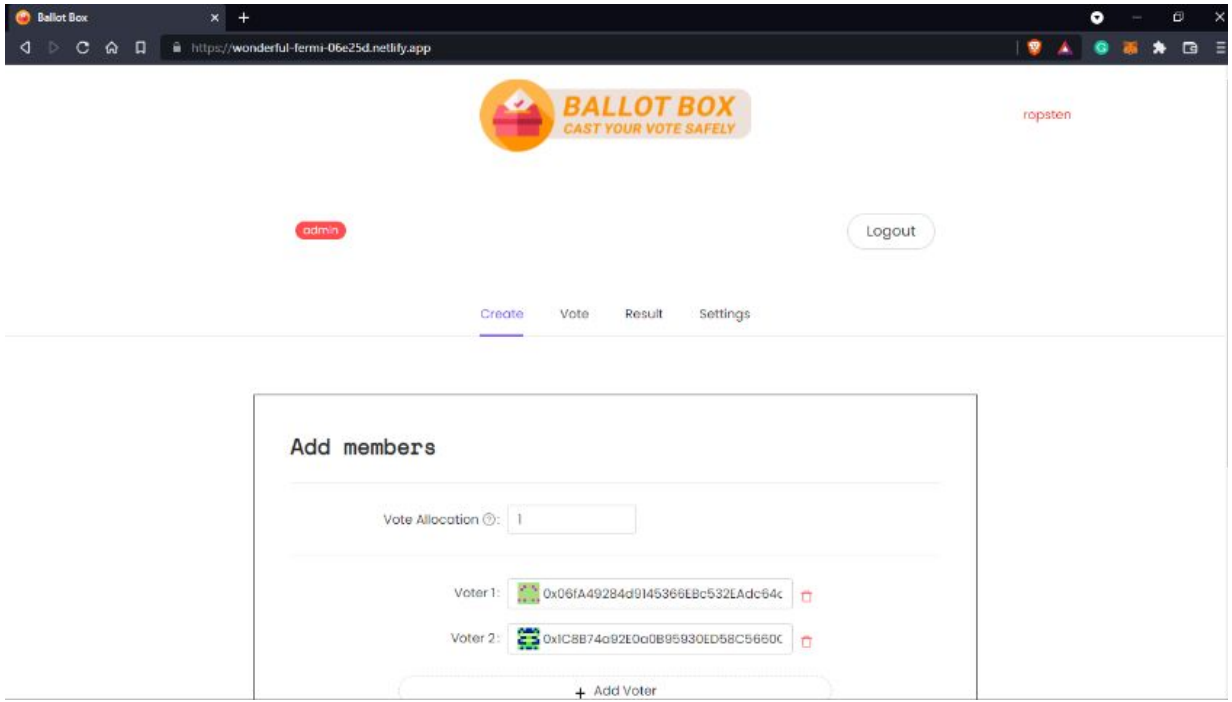






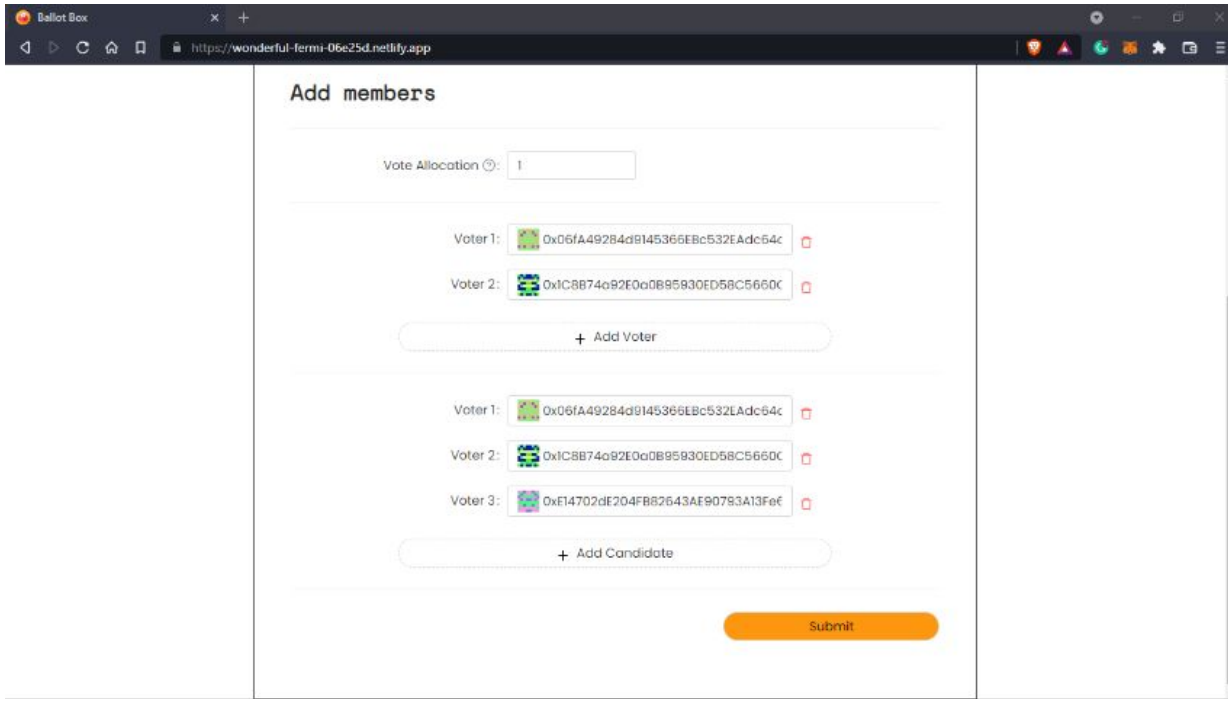



Final Output



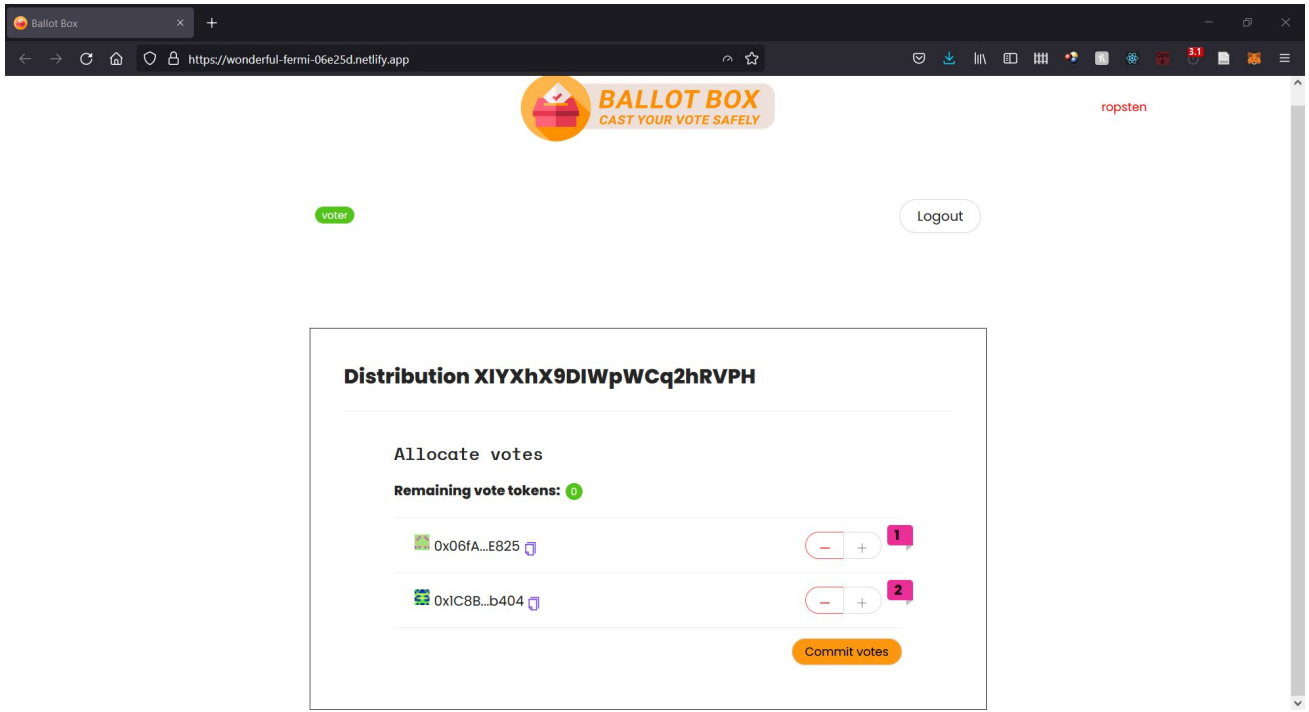
Election Creation Form

Final Output



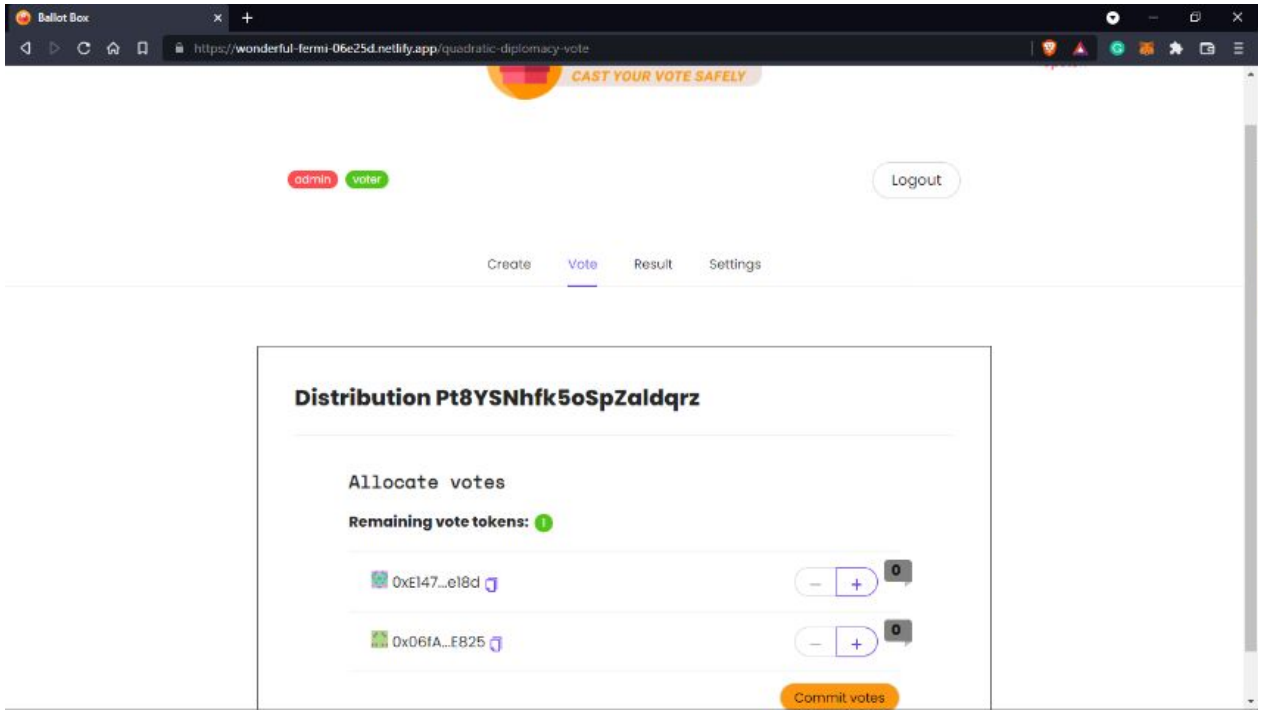
Election Creation Form

Final Output



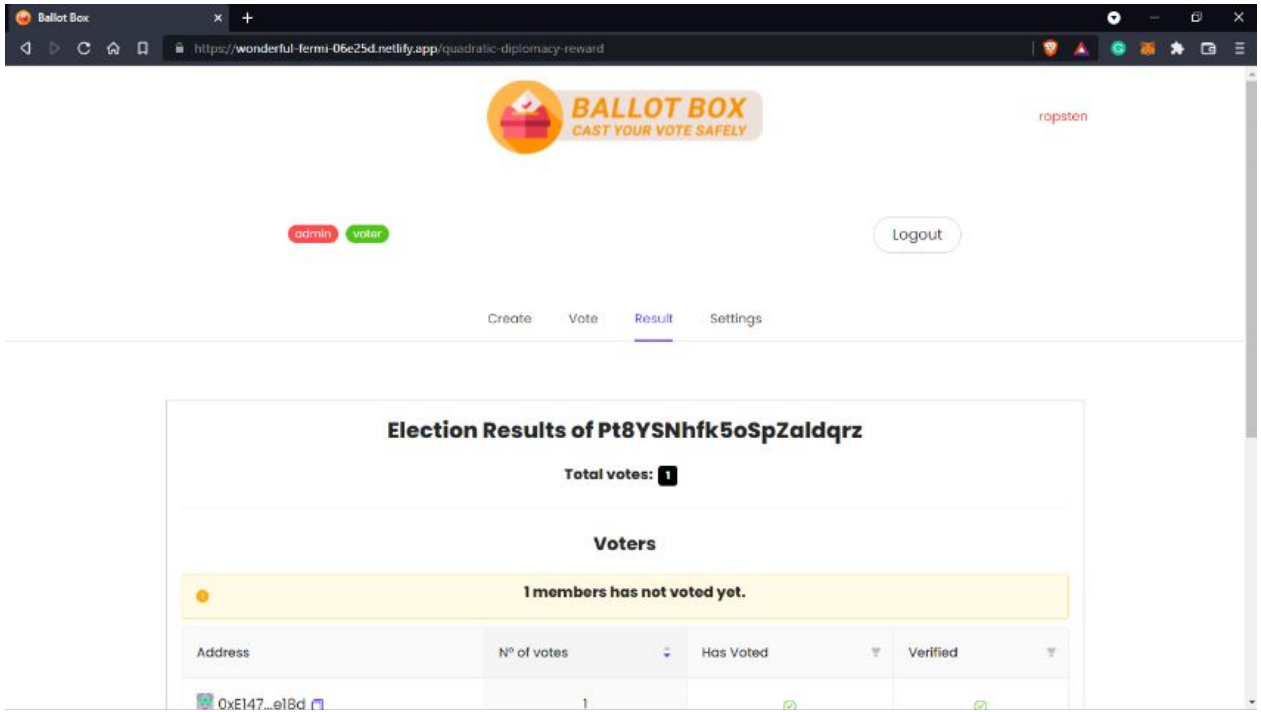
Voting Interface

Final Output



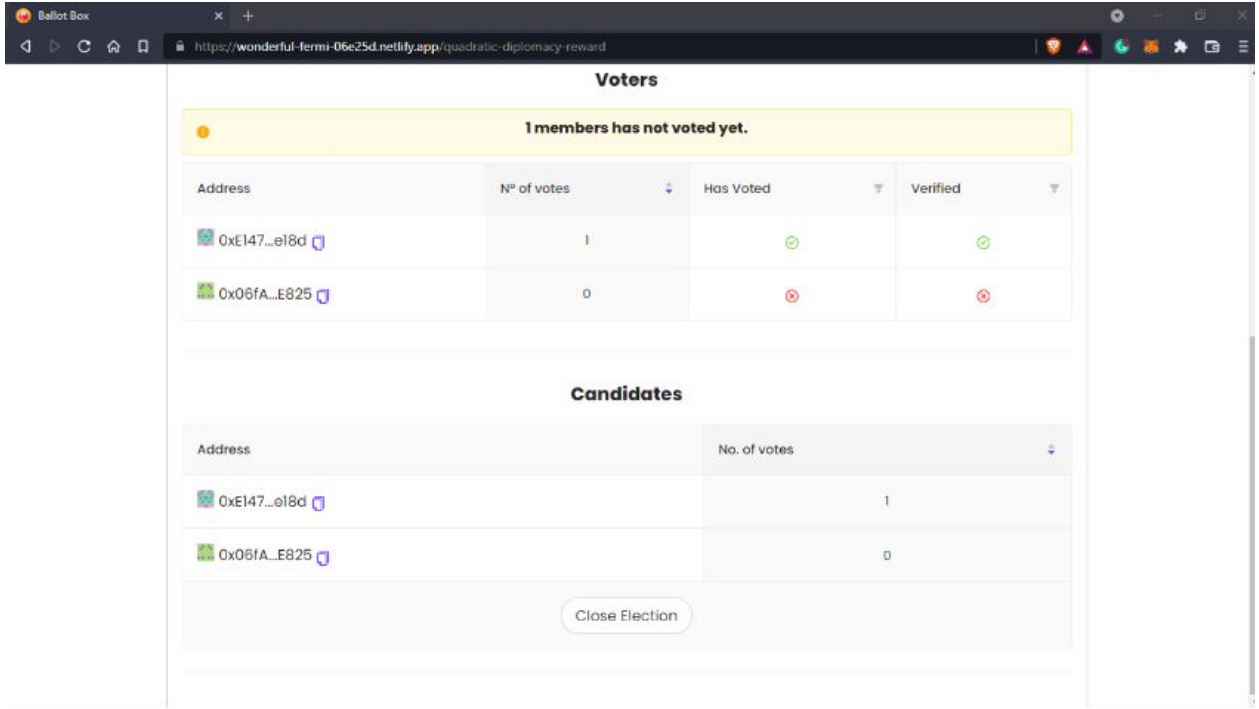
Voting Interface for the admin who is also a voter

Final Output



Results of Election as viewed by Admin

Final Output



Real time election results and ability to close the election

Final Output: Video

Learnings

- The team did an **extensive literature review** and market search for e-voting mechanism. This increased team's knowledge about how blockchain is being used in these domains.
- All team members were new to blockchain tech stack. Thus, handson with **Solidity**, **Metamask**, **Ethers.js** and **Hardhat** was a great learning experience.
- Team also learnt various drawbacks and tradeoffs of various blockchain technologies. This increased practical hands on experience of the team working on such technologies.
- Many teammates had very little experience with front end development, so we had to learn and implement react as well.

Challenges

- **Blockchain** and the related techstack was a new domain for the team to work on. Initially the learning was slow but the team took up pace as the project progressed.
- Only 1 team member had previous experience with web development as well, so other team members had to learn tech apart from blockchain as well.
- Once a **contract** was **deployed**,it was impossible to make any changes to it, which lead to a few extra deployments of contracts on the network.
- Working in a new domain lead to many unforeseeable issues.

Future Work

- Scalability can be improved. Currently system can hold only 1 election at a time. In future, **multi-election** support could also be added.
- Add an extra layer of security by integrating **Aadhar number** with the respective wallet address.
- UI can be made more user friendly.
- Increase the speed of the application by forking to a faster network such as the **BSC(Binance smart chain network)**(drawback it is centralized).

Contribution

- Kinshuk Chopra: Smart Contracts, Features, Front-End Development,Testing, Reading Literature, Exploring Applications interaction with Ethereum Network
- Sandeep Singh: Smart Contracts, Features, Front-End Development, Testing, Exploring Solidity, Reading about Hardhat, Metamask.
- Sarthak Arora: Smart Contracts, Features, Front-End Development,Testing, Exploring Applications,Exploring App’s Interaction with Ethereum Network

References

- https://docs.soliditylang.org/en/v0.8.10/
- https://reactjs.org/
- https://hardhat.org/
- https://docs.ethers.io/v5/
- https://expressjs.com/
- https://www.leewayhertz.com/blockchain-development/
- https://onlinelibrary.wiley.com/doi/10.4218/etrij.2019-0362
- https://www.mdpi.com/1424-8220/21/17/5874/pdf
- https://academic.oup.com/cybersecurity/article/7/1/tyaa025/6137886
- https://www.ibm.com/topics/smart-contracts
- https://101blockchains.com/blockchain-roadmap/

Thank You.

A Presentation by Team 6

Kinshuk Chopra 2018239 | Sandeep Kumar Singh 2018363 | Sarthak Arora 2018307