A Blockchain-Based Voting system

Project Submitted in Partial Fulfilment of the Requirement

for the Degree of

B.Sc.

In

Computer Science [SOFTWARE ENGINEERING]

By

ELI ASIKARO WALTER

To

The Department of Computer Science

Baze University, Abuja

May, 2024

**DECLARATION**

This is to certify that this Thesis entitled blockchain based voting system, which is submitted by Eli Asikaro Walter in partial fulfilment of the requirement for the award of degree for B.Sc. in Information Technology to the Department of Computer Science, Baze University Abuja, Nigeria, comprises of only my original work and due acknowledgement has been made in the text to all other materials used.

Date: 11 May 2024 Name of Student: Eli Asikaro Walter

**APPROVED BY** …………………

**HOD**

Dept. of Computer Science

**CERTIFICATION**

This is to certify that this Thesis entitled [blockchain based voting system], which is submitted by Eli Asikaro Walter in partial fulfilment of the requirement for the award of degree for B.Sc. in Information Technology to the Department of Computer Science, Baze University Abuja, Nigeria is a record of the candidate’s own work carried out by the candidate under my/our supervision. The matter embodied in this thesis is original and has not been submitted for the award of any other degree.

Date: Supervisor:

**APPROVAL**

This is to certify that the research work, Dental Management System and the subsequent preparation by Eli Asikaro Walter with BU/20C/IT/4734 has been approved by the Department of Computer Science, Faculty of Computing and Applied Science, Baze University, Abuja, Nigeria.

By

Dr Morolake O. Lawrence

Supervisor Date

Dr. C. V Uppin

Head of Department Date

Prof Peter Ogedebe

Dean, Faculty of Computing and Applied Science Date

Prof. Choji Davou nyap

External Examiner Date

**DEDICATION**

This project thesis is dedicated to God for seeing me through from the beginning to the end, to my parents Walter Chidi Asikaro and Happiness Asikaro for their financial support and advices which have guided me throughout my life till this point, i would not have been able to get this far this efficiently without their help. I also want to dedicate my project to the department of computing BAZE UNIVERSITY for their support through my project supervisor, project coordinator, Head of department and the Dean of my faculty. Thank you all.

# ABSTRACT

The project explores the creation of a blockchain-based voting system in a time when worries about the accuracy of voting methods are becoming more and more prevalent. By utilising blockchain technology's decentralised and immutable properties, the system seeks to improve voting processes' accessibility, security, and trustworthiness. This project contributes to the development of democratic practices for the digital age through careful design and analysis. This study presents a blockchain-based voting system developed through incremental development, employing a Firebase database for metadata storage and smart contracts which are stored on the Ethereum Blockchain integrated with the ethers.js module and Infura node to store voting data. The system ensures complete immutability of results, resistance to fraudulent voting, efficiency with response times below 10 seconds, efficient user authentication using cryptocurrency wallets, access from any part of the world, inclusion of people with disabilities, and a simple means of verifying the authenticity of the results. Leveraging blockchain technology, the system secures election integrity through decentralised storage, while smart contracts and cryptographic techniques enhance security. By addressing serious flaws in conventional voting procedures, these developments promote inclusivity, openness, and faith in democratic processes.

**TABLE OF CONTENTS**

[**ABSTRACT vi**](#_gjdgxs)

[**LIST OF TABLES**](#30j0zll)**….……………………………………….…………………………………………………………….IX**

[**LIST OF FIGURES………………………………..….…………………………………...…………………………......X**](#1fob9te)

[**LIST OF ABBREVIATIONS……..……………………….……………...……………………………………….....XI**](#3znysh7)

[**CHAPTER 1: INTRODUCTION 1**](#_2et92p0)

[1.1](#_tyjcwt) Overview 1

[1.2](#_3dy6vkm) Background and Motivation 1

[1.3](#_1t3h5sf) Statement of the Problem 2

[1.4](#_4d34og8) Aim and Objectives 2

[1.5](#_2s8eyo1) Significance of the Project 2

[1.6](#_3rdcrjn) Project Risks Assessment 3

[1.7](#_26in1rg) Scope/Project Organization 4

[**CHAPTER 2: LITERATURE REVIEW 5**](#_lnxbz9)

[2.1](#_35nkun2) Introduction 5

[2.2](#_1ksv4uv) Historical Overview 5

[2.3 Related Work 6](#_44sinio)

[2.4](#_41mghml) Summary 6

[**CHAPTER 3: REQUIREMENTS, ANALYSIS, AND DESIGN 7**](#_1v1yuxt)

[3.1](#_4f1mdlm) Overview 7

[3.2](#_19c6y18) Proposed Model 7

[3.3](#_2mn7vak) Methodology 7

[3.3.1](#_3tbugp1) Method 1 (e.g Interview) 7

[3.3.2](#_11si5id) Method 2 (e.g Observation) 7

[3.4](#_28h4qwu) Tools and Techniques 7

[3.5](#_nmf14n) Ethical Consideration 7

[3.6](#_37m2jsg) Requirement Analysis 7

[3.7](#_1mrcu09) Requirements Specifications 7

[*3.7.1*](#_46r0co2) *Functional Requirement Specifications 8*

[*3.7.2*](#_3l18frh) *Non-Functional Requirement Specifications 8*

[3.8](#_4k668n3) System Design 9

[*3.8.1*](#_2zbgiuw)  *Application Architecture 9*

[*3.8.2*](#_1egqt2p) *Use Case 9*

[*3.8.3*](#_2dlolyb) *Data Design 10*

[*3.8.4*](#_2iq8gzs) *Activity Diagrams 10*

[*3.8.5*](#_1x0gk37) *Dataflow Diagram 10*

[*3.8.6*](#_4h042r0) *Control Flow Diagram 10*

[*3.8.7*](#_2w5ecyt) *Entity-Relationship Diagram (ERD) 11*

[*3.8.8*](#_pkwqa1) *User Interface Design 11*

[*3.9*](#_39kk8xu) *Summary 11*

[**CHAPTER 4: IMPLEMENTATION AND TESTING 12**](#_1opuj5n)

[4.1](#_48pi1tg) Overview 12

[4.2](#_2nusc19) Main Features 12

[4.3](#_1302m92) Implementation Problems 12

[4.4](#_3mzq4wv) Overcoming Implementation Problems 12

[4.5](#_2250f4o) Testing 12

[*4.5.1*](#_haapch) *Tests Plans (for Unit Testing, Integration Testing, and System Testing) 12*

[*4.5.2*](#_319y80a) *Test Suite (for Unit Testing, Integration Testing, and System Testing) 13*

[*4.5.3*](#_1gf8i83) *Test Traceability Matrix (for Unit Testing, Integration Testing, and System Testing) 13*

[*4.5.4*](#_40ew0vw) *Test Report Summary (for Unit Testing, Integration Testing, and System Testing) 13*

[*4.5.5*](#_2fk6b3p) *Error Reports and Corrections 13*

[4.6](#_upglbi) Use Guide 14

[4.7](#_3ep43zb) Summary 14

[**CHAPTER 5: DISCUSSION, CONCLUSION, AND RECOMMENDATIONS 15**](#_1vsw3ci)

[5.1](#_4fsjm0b) Overview 15

[5.2](#_2uxtw84) Objective Assessment 15

[5.3](#_1a346fx) Limitations and Challenges 15

[5.4](#_3u2rp3q) Future Enhancements 15

[5.5](#_2981zbj) Recommendations 15

[5.6](#_odc9jc) Summary 15

[**REFERENCES**](#_1nia2ey) **62**

[**APPENDICES**](#_47hxl2r) **63**

Appendix A - Project document

Appendix B- interview

Appendix C- Source code

Appendix D- User Manual

**LIST OF TABLES**

Table 1 Project risks assessment

Table 2 Summary of related works

Table 3 Functional Requirement Specifications

Table 4 Non-Functional Requirement Specifications

Table 5 Test Suite Performed

Table 6 Test Traceability Matrix

Table 7 Test Report Summary

**LIST OF FIGURES**

Figure 1 Proposed Model Diagram

Figure 2 Application Architecture

Figure 3 Use Case Diagram

Figure 4 Data Design Diagram for the smart contract

Figure 5 Data Design Diagram for the firebase DB

Figure 6 Activity Diagram

Figure 7 Data Flow Diagram

Figure 8 Control Flow Diagram

Figure 9 Entity Relationship Diagram

Figure 10 Sign-in Page

Figure 11 Home page

Figure 12 Create a new group page

Figure 13 Group page(poll has not started)

Figure 14 Start poll page

Figure 15 Poll page

Figure 16 Results page

Figure 17 Archive page

Figure 18 Sidebar

Figure 19 Learn more page

Figure 20 Wallet sign in code

Figure 21 Wallet sign-in prompt

Figure 22 Code to create a group

Figure 23 Function being called in the smart contract to create a group

Figure 24 Group Created Successfully

Figure 25 Sign-out function

**LIST OF ABBREVIATIONS**

CPU Central Processing Unit

ERD Entity Relationship Diagram

IT Information Technology

NFT Non Fungible Token

DEFI Decentralised Finance

DAO Decentralised Autonomous Organisation

# CHAPTER 1: INTRODUCTION

## 1.1 Overview

This chapter lays the foundation for why this project is relevant and what led to its inception, as well as some reasons why this solution is superior to other proposed solutions. It includes the specific aim of this project and the objectives that will fulfil the aim, possible bottlenecks, and measures for preventing and/or mitigating the effects of these events.

## 1.2 Background and Motivation

Numerous issues with traditional voting methods necessitate creative fixes. Long-standing worries about fraud, manipulation, and a lack of transparency have dented the integrity and confidence in democratic processes by a large portion of society. Increased accessibility, efficiency, and reduced costs are promised with the development of electronic voting (e-voting) systems. Nevertheless, cyber vulnerabilities coupled with the opaque counting procedures and the overall centralised nature of the initial iterations of e-voting systems frequently cast further doubt or suspicion on the validity of the results of a poll because, with those versions of e-voting systems, data manipulation is possible (TheCable, 2023).

The pressing need for innovative solutions led to exploring new technologies such as blockchain. A Blockchain is a distributed and decentralised digital ledger that records transactions across a network of computers called nodes, which contain a copy of all data on the blockchain (GeeksForGeeks, 2023). The blockchain is designed to be secure, transparent, and resistant to modification of the data(transactions) it contains. The fundamental concept of a blockchain involves a chain of blocks, where each block contains a list of transactions. These transactions are secured using cryptographic principles and are linked together in a chronological and linear order, meaning future blocks contain the hash of the previous block, hence the name blockchain.

New technologies such as blockchain technology have the potential to revolutionise the voting process by improving its security, transparency, and accountability. The fundamental characteristics of blockchain, such as data immutability, decentralisation, and cryptographic security, offer exciting opportunities to solve problems present in conventional and electronic voting systems that have been present for a long time and renew trust in the democratic process by members of the society, some of such problems include costs, logistical complexity, ease of accessibility by potential participants and people with disabilities.

According to Abuidris & Kumar (2019), the primary driving forces behind investigating blockchain-based voting systems are:

1. Enhanced Security: Decentralised data storage on a blockchain makes it far more resistant to manipulation and hacking than centralised electronic voting methods. Each vote is securely embedded in the public ledger and cryptographically protected, making tampering with individual votes or the overall vote count impractical and impossible to go unnoticed because when a change to the state (data) of a smart contract occurs, the hash of the block which the smart contract is stored changes.
2. Enhanced Transparency: Every vote cast is recorded in an unchangeable audit trail since every transaction on the blockchain is visible to the general public. This feature increases/fosters public trust and confidence in the voting process by enabling independent verification of the voting procedure and results.
3. Decreased Fraud: Smart contracts on the blockchain can be used to enact one-vote-per-person limits and secure voter identification. Since user authentication voting is achieved using a crypto wallet, the risk of voter impersonation is low because crypto wallets are protected with a 12- 24 word (in some cases even more) phrase consisting of randomly generated words that are nearly impossible to guess or brute force, the use of crypto wallets to vote entirely protects the voter's identities which also mitigates voter intimidation and vote buying, All these features jointly reduce the risk of fraud in the voting process.
4. Enhanced Accessibility: Voting systems based on blockchain technology can facilitate safe and easy voting from any location with an internet connection, potentially boosting voter turnout and overcoming geographical, logistical, and financial obstacles. The use of web or mobile-based applications to implement voting systems allows for the implementation of measures aimed at enabling disabled people to cast their votes. An example of such measures is using semantic HTML tags, and the ‘alt’ attribute in the tags makes it possible for screen readers to accurately convert the content to speech for people who have visual impairments.

## 1.3 Statement of the Problem

The current aged and centralised methods of voting need to be improved under the pressure of increasingly overwhelming obstacles as the world moves into the digital age. With their roots in manual and fully centralised procedures and paper ballots, these traditional methods start to fall short of the needs of contemporary democracy at major societal levels and the needs of the people who participate in the voting process.

The compelling story of the challenges facing the traditional voting system, such as how expensive it can get to set up polls, how inaccessible it can be, and how centralised the entire process is, which gives rise to the risk of corruption or bias by the coordinators is revealed raising questions about the fundamentals of safe, transparent, and equitable voting process.

The Following issues are most important:

1. The traditional voting system is plagued by issues that undermine the integrity and effectiveness of the voting processes. They often suffer from problems such as voter bribery and intimidation, data manipulation, ballot box theft, and rioting.
2. Electronic voting systems, which were created to address this issue, still suffer from factors such as security breaches and doubts about result authenticity caused by the centralised nature of electoral institutions. All these issues erode trust in voting processes.
3. Large-scale elections with paper ballots or voting machines require careful logistical planning to manage and organise. Preventing long lines, expenses, and administrative obstacles that could lower voter turnout and undermine the effectiveness of the voting process is the difficult part of the job.
4. The traditional voting system's lack of real-time transparency further limits public inspection and accountability. Access to the entire electoral process is typically restricted for voters, which makes it difficult for them to hold the system responsible and raises questions about possible manipulation behind closed doors.
5. The traditional voting method's heavy reliance on paper votes adds to environmental concerns such as pollution, littering, and wastage of record storage space. The difficulty lies in identifying viable substitutes that lessen the environmental impact of elections while maintaining voting integrity and security.

## 1.4 Aim and Objectives

The main aim of this project is to design and implement an efficient, tamper proof, and secure blockchain-based voting system that solves the current challenges of traditional voting processes, and ensures that polls held using this system are fair, transparent, and decentralised.

The objectives of this project are :

1. To Design a decentralised voting architecture with a user-friendly interface tailored to support the inclusion of people with disabilities and provide access to the real-time vote count of every candidate/option during the voting process.
2. To implement a scalable system to accommodate a large number of voters and groups, Optimise smart contract constructs and executions to reduce transaction costs, improve function execution time, and implement measures to prevent or mitigate data loss in the application.
3. To evaluate the performance of the voting data from each group(how efficiently and effectively voting data is processed and stored in the system), the privacy of the voters, and their votes is maintained.

## 1.5 Significance of the Project

1. This project is crucial in the effort to revolutionise the current troubled electoral procedure by solving critical issues in the existing systems, such as transparency, integrity, and verifiability. If implemented correctly, this project will benefit Academia and Nigerian society and improve the world of politics.
2. This project offers tangible benefits to the academic world, providing new insights into electronic voting and practical use cases for blockchain technology beyond its traditional roles as a payment system or a medium for speculative investment.
3. The societal and global impact of this project is profound. It has the potential to catalyse electoral reforms, leading to a reduction in social unrest and public resentment towards the democratic process. Moreover, it assures poll participants that their votes are secure and counted, thanks to the unalterable and always-online nature of the blockchain storing the voting data, unlike the current Bimodal Voter Accreditation System(BVAS) machines.
4. This project could also solve the problem of fully holding elected officials accountable at the school, union, government, and international organisation levels.
5. Overall, this project has the potential to foster the development of a more democratic and cohesive society due to the decentralised nature of a blockchain-based voting system, which means no one individual or party has complete administrative control over the system.

## 1.6 Project Risks Assessment

Table 1: Risks

| This technology could still have unforeseen vulnerabilities because it is still relatively new in the public eye. | Regular security checks and penetration testing can help discover and fix vulnerabilities. |
| --- | --- |
| The technology used may not detect when a wallet is disconnected to log the user out. | implementation of custom logic to detect disconnection and log the user out. |
| Abuse of the voting process e.g users creating multiple wallet addresses to authenticate themselves and spam votes. | implementation of wallet address registration during the creation of polls and use of conditional logic to determine if the address trying to cast a vote is eligible. |

## 1.7 Scope/Project Organization

The Evolution of blockchain technology and the related literature review is documented in Chapter 2, the gathering of requirements, analysis, and design of the system is documented in Chapter 3, the process of implementing and testing the project is documented in Chapter 4, some Discussions, conclusion of the project, and recommendations are documented in Chapter 5. Further sections note the references for this project as well as additional information related to this project.

# CHAPTER 2: LITERATURE REVIEW

## Introduction

A Blockchain is a distributed and decentralised digital ledger that records transactions across a network of computers called nodes, which contain a copy of all data on the blockchain. It is designed to be secure, transparent, and resistant to modification of the data(transactions) it contains (GeeksForGeeks, 2023). The fundamental concept of a blockchain involves a chain of blocks(Future blocks contain the hash of the previous block, hence the name blockchain), where each block contains a list of transactions.

Initially conceived for cryptocurrency transactions and investing, blockchain technology has evolved into a transformative force across numerous industries and sectors. From Peer-to-peer (P2P) trading to Supply chain management, intellectual property protection to cross-border payments, and Tokenization of assets, blockchain has revolutionised how we conduct business. Its genesis can be traced back to the creation of Bitcoin on the 31st of October 2008 by an anonymous software engineer/ team of software engineers known as “Satoshi Nakamoto.” This groundbreaking concept of a decentralised, secure, and immutable ledger has paved the way for a new era of technological innovation (Pinkerton, 2023).

Over the last decade, blockchain technology’s potential began to stretch beyond currency, notably with the invention of smart contracts (and special programming languages and libraries on existing languages for creating, deploying and interacting with smart contracts, e.g. solidity, web3.js, ethers.js, hardhat.js) and decentralised applications (DAPP’S) on various blockchain platforms, the most popular platforms being the Binance Smart Chain, Ethereum chain and more recently the Solana chain (Yakovenko 2023). As blockchain technology grew in popularity, developers and other contributors addressed the scalability challenges which caused further traction for it in supply chain management, finance, and data storage.

This overview traces the remarkable journey of blockchain from its inception to its current state, underscoring its potential to reshape industries and sectors, foster transparency, and catalyse the creation of new products and services. The future of blockchain holds immense promise, and its transformative impact is only beginning to be realised.

## Historical Overview

The origins of blockchain technology can be traced back to the 1970s when the concepts of cryptography and secure digital communication began to evolve. Researchers and cryptographers like David Chaum and Whitfield Diffie made significant contributions. However, the concept of a decentralised digital ledger was fully realised in the release of the Bitcoin whitepaper in 2008.

According to Pinkerton (2023), The genesis of blockchain technology began in 2008 with the introduction of Bitcoin by a computer programmer identified as Satoshi Nakamoto. This was done with the release of a whitepaper titled “Bitcoin: A Peer-To-Peer Electronic Cash System”. Then, in January 2009, bitcoin was officially released for trading.

In 2010, other developers and businesses started to see more use cases for the technology in securing, verifying, and storing digital transactions. Because of this, new blockchain projects started to emerge; notably in 2011, the Litecoin project, which is more efficient than Bitcoin for transactions (Investopedia team, 2024) and Namecoin which aimed to decentralise domain name registration.

In 2013, ethereum was introduced and was subsequently released in 2015. This event was revolutionary for the decentralisation movement because it birthed smart contracts, which are programs that serve as immutable, self-executing contracts between parties (Copeland, 2023). This innovation gave rise to another innovation called decentralised applications(DAPPS). The advent of DAPPS further demonstrated that blockchain technology was still an untapped industry with many potentials for innovation for and outside finance despite issues that started to emerge, such as energy consumption and scalability.

In 2016, the price of various cryptocurrencies started to increase. A new fundraising mode called” Initial coin offering” (ICO), which mimics how companies conduct an initial public offering in the stock market by using the blockchain-based tokens as a security to raise funds, was established to support a project (Frankenfield, 2022). This fundraising method brought about investor safety concerns because scammers developed a new tactic called rug pulling, which involved deceiving people into buying into an ICO. The demand and hype will cause the price of the token to rise. The scammers will then sell (dump) their tokens as project creators (they usually have massive amounts of tokens); this causes the tokens investors own to become worthless, effectively stealing off the invested money. Regulations by the SEC (Securities Exchange Commission) of many countries helped combat this problem.

The year 2017 is famously known as when prices of virtually all cryptocurrencies rapidly increased. New coins were being created virtually every day, and it was a viable way for early investors in a cryptocurrency to “cash out” on people who bought in late. Eventually, this became a massive bubble with the average person trying to buy in for a quick profit. This system became unsustainable because cryptocurrency’s primary purpose at the time was to be a store of value. However, market conditions incentivized people not to hold on to cryptocurrencies for long due to the fear of being part of the late people to sell(usually at a loss). This problem, coupled with cyber attacks on several crypto exchanges, led to significant losses of customer funds and increased government scrutiny, eventually leading to the collapse of the price of almost all cryptocurrencies (Chen,2023). Beyond 2017, after the hype settled, developers and institutions focused on addressing the energy and scalability issues, which led to the creation of new tokens and further adoption of the technology, with large corporations and organisations recognizing the potential of blockchain technology to streamline operations and increase transparency. Many of them established alliances like Enterprise Ethereum Alliance and Hyperledger to develop and promote enterprise-grade blockchain solutions that address scalability, privacy, and interoperability in the world of business.

From 2018 to 2019, after the cryptocurrency market’s rapid growth (bubble) in 2017, the industry experienced a significant market reversal. It saw the prices of many cryptocurrencies, including Bitcoin, retrace by about 75% from its peak, and many ICO-funded projects failed. This period, often called the “crypto winter” served as a reality check for the industry’s speculators, forcing actively involved participants to focus on developing practical use cases (Gehmlich, 2022). This event caused various governments to implement various regulations. These regulations stretched from classifying cryptocurrencies as commodities or securities to mandating exchanges implement Know Your Customer (KYC) verification and Anti-money laundering measures.

During the crypto winter, stablecoins, which are just cryptocurrencies pegged to the value of traditional fiat currencies, became an essential component of the cryptocurrency ecosystem. They offered price stability, making them suitable for everyday transactions and financial services(Seth, 2023).

Central banks worldwide started exploring the concept of Central Bank Digital Currencies (CBDCs). These digital currencies issued and regulated by central banks aim to provide the advantages of cryptocurrencies while maintaining government oversight and control over the monetary system. To date, more and more central banks are still working towards implementing their digital currencies; some countries have even gone as far as considering making bitcoin or other altcoins legal tender (National bureau of economic research, 2022). El Salvador being the first to do so in September 2021.

From 2020, the industry really started to get exciting, with the introduction of Decentralised finance (De-Fi), Non Fungible Tokens(NFT’s), The metaverse and play to earn games.

1. Non Fungible Tokens - Non Fungible Tokens are unique digital identifiers stored on a blockchain. These are used to certify ownership and authenticity of digital assets such as art, music, virtual property and other collectables and enable transfer of these assets between parties (Vidal-Tomas, 2022). NFT’s have gained attention due to its potential to benefit and protect artists.
2. Metaverse - The metaverse is a convergence of Augmented reality(AR), Virtual reality(VR), and blockchain technology which aims to create a seamless and interconnected digital world where people can interact with one another like it were the real world, and explore digital landscapes (Vidal-Tomas, 2022).
3. Play to earn games - According to BSC News (2024), The concept of play to earn games is transforming the gaming industry, with players being able to earn cryptocurrencies or other digital assets by playing a game. The idea is that players utilise their time and skill in playing the game and receive rewards that often have real-world value, based on metrics such as their success in the game. In addition to that, players can also make use of their digital assets in the game e.g virtual property becoming a venue for a game match.
4. Decentralised finance (De-Fi) - The aim of de-fi projects is to mimic traditional financial services such as borrowing, lending, trading, and annual percentage rates (APR’s) / interest rates using smart contracts(Sharma, 2023). This effectively eliminates the need for a third party to dictate or control operations.

Blockchain technology's evolution has recorded significant milestones, challenges, and innovations, from its humble beginnings as the base technology for Bitcoin to its applications being felt in finance, supply chain management, and others. Blockchain technology has evolved into a disruptive force with the potential to transform several industries and how users interact with the digital world. Blockchain technology's future potential is worth paying attention to, with ongoing developments promising greater scalability, security, and utility, further solidifying its place in the digital world.

## 2.3 Related Work

Electronic Voting has been an area of study for many years, and many products have been released to facilitate this process. However, each has had issues of its own, commonly Transparency, Security, and Data integrity. Blockchain technology is the closest researchers have come to finding a solution for these common problems. With promises of security, immutability, and openness, blockchain technology has entered the political/social democratic process. This essay conducts a critical analysis of blockchain-based voting system projects. It analyses the innovation's technical foundations, examines its advantages and disadvantages, and speculates on whether it might be widely used in democratic elections.

### 2.3.1 I-Voting app

The GuardTime & Estonian government-commissioned Estonian pilot project ( deliverable being the I-Voting app) is an excellent illustration of a blockchain-based voting system. Using a mobile application, voters used their national ID cards to sign their ballots digitally. Using Byzantine Fault Tolerance (BFT) consensus to protect encrypted vote storage on the blockchain ensures tamper-proof and transparent record-keeping. Furthermore, a “blind signature” method that anonymizes voters throughout the voting process protects against vote-buying and coercion (Aboknin, Shir, 2021; GuardTime, 2020; The New Yorker, 2020).

Strengths:

1. Enhanced auditability and transparency: Blockchain technology makes every vote publicly verifiable, instilling confidence in the political process.
2. Enhanced security and tamper-proofness: Blockchain technology’s unchangeable nature ensures that votes cannot be altered or manipulated, providing a robust and secure voting environment.
3. Reduced expenses and fraud: Because the system is decentralised, there is no longer a need for human vote counting or physical polling places, which might cut expenses and logistical complexity and reduce the possibility of fraud.
4. Enhanced ease of access and convenience: With internet connectivity, voters can safely and virtually cast their ballots from any location, leading to a rise in voter turnout.

Weaknesses:

1. The blockchain network faces scalability problems in the event of massive elections involving millions of votes.
2. Although the system protects voters’ identities when they cast ballots, there are still concerns about metadata collection and the possibility of outside observation.
3. Some groups of people would not be able to vote in blockchain-based elections because they lack access to the required infrastructure and technology.

### 2.3.2 The Voatz Mobile voting app

This is another notable exploration of blockchain-based voting; leveraging cloud and blockchain architecture, according to Kenny (2019) Voatz allows authenticated registered users to receive, mark, and submit a secret ballot of the correct style from virtually anywhere in the world. Every ballot submitted is encrypted and stored on a network of blockchain servers housed worldwide, managed by some of the largest cloud infrastructure providers. Voatz was used by the residents of Utah in a statewide election, marking the first time blockchain tech has been used for an election; in 2018, Voatz was also used by West Virginia active uniformed Americans outside the US as powered by the Uniformed and Overseas Citizens Absentee Voting Act.

Strengths:

1. To reduce physical location barriers, voatz aimed to increase accessibility through remote and mobile voting.
2. Leveraging distributed blockchain servers to provide tamper-proof and auditable records.

Weaknesses:

1. Reliance on mobile devices might exclude specific demographics, including older people, raising accessibility concerns.
2. Significant concerns exist about Voatz secretly sending voting patterns to the government.

### 2.3.3 The Democracy Earth Blockchain

The Democracy Earth Blockchainfor Liquid Democracy aims to create a participatory and dynamic system of governance by proposing a concept known as Liquid Democracy, which combines the advantages of both direct and Representative democracy to create a completely democratic voting system, empowering voters to vote directly in voting events or delegate their voting power to a trusted party (gwarzocha, et al 2020). Democracy Earth uses Proof of Humanity to verify votes, removing the need for servers and databases.

Strengths:

1. Enhanced flexibility: It provides the users with the flexibility to participate in decision-making or delegate their voting power based on specific expertise, hence enhancing the democratic process.
2. Blockchain enhances transparency and immutability.

Weaknesses:

1. The concept of liquid democracy is new and may require comprehensive user education to ensure users fully understand and grasp the platform and its utility.
2. Scalability is a huge concern for a more extensive user base.

### 2.3.4 Follow-my-vote

This voting system uses elliptic curve cryptography(it validates new transactions to the blockchain and ensures that the transactions are authorised to execute) to address issues relating to trust, security, and accessibility with traditional voting systems. Pilot programs have been implemented, and presently, there are real-world evaluations to measure the viability of the voting system. As FollowMyVote (n.d.) explains, they use this technology to create votes. During the registration process, voters create two ECC key pairs. The voter reveals their identity to a verifier, who certifies the first key-pair (the identity key-pair) as belonging to that voter. The voter anonymously registers their second key-pair (the voting key-pair) as belonging to one of the identity keys. However, the way this is done, no one can determine which identity key owns her voting key. They can then create transactions that state their votes on the contests in an election and use their voting private key to sign those transactions.

Strengths:

1. Using end-to-end verifiability, follow-my-vote ensures users can Independently verify that their votes have been recorded and counted.
2. Follow-my-vote leverages blockchain accessibility to provide universal accessibility to voting, ensuring users can securely participate from every part of the world. It offers secure and robust protocols, discoverability, and peer-to-peer connectivity.

Weakness

1. As for early adopters, there will be a case of barrier to entry created by digital illiteracy and access to education. This factor is a setback because users may need time to adapt to the new voting system.

### 2.3.5 Case Study

Blockchain technology is studied within a laboratory scope and is mainly applied to a small-scale election system. This application offers several advantages, such as simplicity, neutrality, security, and transparency, aiming to address deficiencies in traditional paper ballot election systems (Fauzi et al, 2018).

Strengths:

1. Significantly reduced result tampering.
2. The results are easy to verify.

Weakness:

1. Implementing ECC algorithms correctly can be complex, especially in environments that are resource-limited, such as embedded systems.

### 2.3.6 Votereum

Votereum introduces a decentralised voting platform built on smart contract technology. By leveraging blockchain's immutability and programmability through smart contracts (Vo-Cao-Thuy et al, 2019). Votereum aims to provide a transparent and incorruptible framework for elections. Votereum aims to revolutionise how votes are cast and counted.

Strengths:

1. With the voting process automated through smart contracts, Votereum ensures that predefined rules are executed seamlessly, eliminating the need for intermediaries. This enhances transparency and significantly reduces the possibility of human error, piquing the interest of those seeking a more efficient and reliable electoral system.
2. Smart contracts are immutable, which ensures that records are tamper-proof and transparent, ensuring integrity in the electoral system.

Weaknesses:

1. User adoption may be a crucial challenge, as the user experience is essential to ensure widespread acceptance of the platform.
2. At the time, smart contracts were vulnerable to many security risks; this is a critical challenge for the Votereum platform.

### 2.3.7 CryptoVote

CryptoVote is designed to provide a privacy-centric and community-driven voting experience on the blockchain. Leveraging advanced cryptographic techniques, A web interface for running ranked-choice voting elections powered by the ShuffleSum algorithm and the Damgard-Jurik(mainly applicable to voting because of its additive homomorphic- meaning it is possible to combine ciphertexts in such a way as to obtain the encryption of the sum of the corresponding plaintexts and it can be structured as a threshold cryptosystem) cryptosystem. Rank choice voting allows voters to express nuanced preferences, supporting widely popular and less mainstream candidates without the concern of wasting their votes (Boucher et al, 2019). CryptoVote uses the Damgard-Jurik.

Strength:

1. CryptoVote incorporates zero-knowledge proofs, a robust cryptographic feature, to ensure the utmost confidentiality of individual votes. This feature enables the verification of votes without revealing the specific choices made by voters, providing a high level of security and privacy.

Weaknesses**:**

1. Homomorphic encryption introduces computational overhead, potentially affecting the efficiency and scalability of the voting system, especially during large-scale elections.
2. The hybrid model requires additional education for voters to understand the dual-layer security approach, and widespread adoption could face initial challenges.

### 2.3.8 TokenVote

This application adopts a hybrid model, integrating blockchain technology with homomorphic encryption to address the transparency and privacy concerns inherent in electronic voting. TokenVote is a general-purpose, multi-chain governance system for blockchain-based tokens developed by SecureVote (Xu & Weber, 2019).

Strengths:

1. SecureVote's use of a public blockchain is a key strength, as it ensures transparency and immutability. This feature empowers voters, allowing them to independently verify the integrity of the voting process, a crucial aspect of any secure voting system.
2. The integration of homomorphic encryption enables the secure computation of votes without revealing individual choices, ensuring voter privacy.
3. The hybrid model strikes a delicate balance between ensuring the voting process's transparency and safeguarding individual voters' privacy, addressing concerns from both perspectives.

Weaknesses**:**

1. During large-scale elections, Homomorphic encryption introduces computational overhead, which can potentially affect the voting system's efficiency and scalability.
2. Widespread adoption could face initial challenges, and hybrid models may require additional education for voters to understand the dual-layer security approach.

### 2.3.9 Horizon State

Horizon Stateis a blockchain-based voting and decision-making platform. It extends beyond traditional voting systems, enabling decentralised decision-making for organisations and communities. A user can use their cryptographic hash, which is a special string of characters used to identify their vote. Everyone is able to see the vote cast using this hash. However, only the voter will be able to identify the vote as theirs. The platform operates using Decision Tokens (horizon State,n.d.).

Strengths:

1. Immutable Records**:** Using blockchain ensures that voting records are tamper-proof and publicly verifiable.
2. With an amicable user interface that provides new users with a seamless and friendly experience, the South Australian Department of Cabinet benefited from transparent results made available promptly after the poll.

Weaknesses:

1. Horizon State's effectiveness relies on the stability and security of its underlying blockchain infrastructure. Any disruptions in the blockchain network could impact the reliability of the voting system.
2. Regulations surrounding blockchain and electronic voting may vary across jurisdictions. Horizon State might encounter challenges navigating and complying with diverse legal frameworks, potentially limiting its deployment in certain regions.

### 2.3.10 Agora

**Agora** is a protocol made for voting. Using a consensus algorithm designed for voting, a global community of node operators organised following hybrid permission or a permissionless model is incentivized to verify election results by the $VOTE token (Agora, 2018). Agora piloted the first test of blockchain voting in a national election in Sierra Leone in their 2018 presidential election. Agora’s end-to-end verifiable blockchain technology allows participants to verify the accuracy of election results.

Strengths:

1. Agora’s ecosystem’s central strengths are in cryptographic security and a distributed and decentralised network architecture. The technology protects election data against manipulation from any third party seeking to subvert the election process, including the Agora team.
2. Agora uses anonymization and verifiable algorithms to maintain voters’ privacy.

Weaknesses:

1. Agora is an entirely internet-based application; this might be challenging for countries with low internet speed/access.
2. Educational barriers remain one of the primary drawbacks of internet/blockchain-based voting.

### 2.3.11 Votem

A blockchain-based application that uses a protocol known as proof-of-votes (POV) to conduct end-to-end verifiable elections on the blockchain. Proof of votes provides irrefutable evidence of the result of a valid vote that was cast as intended and substantiated by a user. Using blockchain technology, proof of votes performs verifiable key generation for elections public key, verifiable vote anonymization(encrypted by homomorphic crypto process) via mix-networks and verifiable vote decryption (Votem, 2018). In proof of votes, an election is run on a blockchain network, where each node participating in the network is explicitly granted permission by the authority conducting the election. These permissions include producing blocks, participating in the blockchain consensus algorithm, notarizing blocks, being an election key trustee, or being a mix-network node.

Strengths:

1. Every action on proof of votes is transacted on the blockchain, meaning all actions take place in real time and can actively be verified by anybody interested. This is advantageous as it leads to end-to-end verification of election proceedings.
2. The Votem mobile application provides a user-friendly interface, offering enhanced accessibility to a broad range of voters. The emphasis on user experience contributes to increased participation.

Weaknesses:

1. Building public trust in the security and reliability of blockchain-based voting is crucial for the adoption of platforms like Votem. Continuous education and transparent communication about security measures are essential.
2. Adhering to diverse legal frameworks and regulatory requirements across jurisdictions challenges global adoption. Votem needs to navigate and comply with varying election laws.

### 2.3.12 Luxoft-Government Alliance Blockchain

Deployed on the Ethereum network, Luxoft e-votes partners with Digital ID registration companies to create a robust tamper proof, anonymity of voters, and security audits to voters; servers are spread across different rejoins to ensure a more robust system. The e-voting platform is open-sourced, so anyone can study and understand how the technology was created and how it actually works, promoting complete transparency. Luxoft e-votes is built on the Hyperledger Fabric built with Go and Javascript. It uses Elliptic Curve Cryptography(ECC), which is a type of public-key cryptography that relies on the mathematics of elliptic curves over finite fields.) and ElGamal(ElGamal is a public-key cryptosystem that enables secure communication through asymmetric key encryption.) cryptographic algorithm. E-votes are based on the Practical Byzantine Fault Tolerance- a consensus algorithm designed to attain a consensus in a distributed system even with the presence of malicious nodes/Byzantine faults.(Suvorov, 2018;Abuidris et al, 2019)**.**

Strengths:

1. Luxoft e-voting technology is open-sourced, which increases voters' confidence in the election result.
2. Ethereum is currently one of the strongest and most popular blockchain networks, which means that educational content and useful tips are readily available.

Weaknesses:

1. Ethereum is very expensive when the network is busy. Gas fees go higher than $30 per transaction. This factor significantly increases the cost of an election, rendering the use of e-votes ineffective cost-wise.
2. Using third-party web2 applications might create a security vulnerability for voting applications.

### 2.3.13 Polyas voting system

Polyas uses Private/local Blockchains to modernise, secure, and simplify the election process. It uses the Elliptic Curve Cryptography (a version of public-key cryptography) algorithm to secure votes cast. To maintain user privacy and safeguard important information in digital communication, data storage, and online interactions. Polyas deploys several privacy-enhancing technologies including ECC and end-to-end encryption(Abuidris et al, 2019).

Strengths:

1. Polyas offers remote electronic voting options, allowing voters to participate in elections from the comfort of their homes or other locations with internet access.
2. Polyas Solutions aims to comply with legal requirements and standards for elections, considering the regulatory frameworks of different jurisdictions.

Weaknesses:

1. Some people do not have access to reliable internet and are not computer literate. This factor excludes some voters from participating in the process.
2. For less tech-literate users, the online voting process may seem confusing or frustrating, leading to errors and or resentment toward the system.

### 2.3.14 Helios Voting system

Helios employs advanced cryptographic protocols to ensure the security and integrity of votes, including homomorphic encryption and allowing votes to be encrypted while enabling computation on the encrypted data. Helios enables voters to check the accuracy of the tally after a voter submits their encrypted vote to the voting system, the voting booth stores the vote in IPFS before receiving the address of the file used to locate it later (Lam, 2018). Using the Ethereum smart contract, helios retrieves the user votes from IPFS and publishes the address on the blockchain.

Strengths:

1. Using the IPFS and Ethereum, helios can easily be accessible from anywhere, and the popularity of these systems means educational content is available for new users.
2. The platform focuses on providing transparent verification processes, allowing voters to independently verify that their votes have been accurately recorded and counted.

Weaknesses:

1. While online systems offer features like end-to-end encryption, manipulating voters through disinformation campaigns or social engineering is a serious risk.
2. The complexity of the system and potential technical intricacies make it challenging for the public to understand and audit the voting process.

### 2.3.15 Uniswap DAO

The Uniswap DAO (Decentralised Autonomous Organisation) boasts a staggering membership of over 310,000 individuals. These members wield significant power, as they can influence the $1.6B treasury, governance, and roadmap of the DEX by holding $UNI Cryptocurrency tokens (The official cryptocurrency of Uniswap). Any holder of the Uniswap token can submit a proposal. However, it must gather a total 25,000 votes in support before it can further be deliberated on. The second phase is called a consensus check, where the individual who initiated the proposal must outline the core changes, persuade other participants, and gather at least 50,000 yes votes. Finally, the third phase called a governance phase has a requirement of 40 million worth of yes-votes for the proposal to be adopted. It is important to note that these vote requirements are not based on the number of votes but on the total sum of all the voters' wallet balance of $UNI tokens, which must be up to 25k tokens in the first phase, 50k tokens in the second phase, and 40M in the third phase (Uniswap, n.d; Ashleigh, 2020).

Strengths:

1. This System has a very transparent voting process.
2. The Uniswap DAO is very resistant to censorship.
3. The community entirely governs the Ecosystem due to its efficient voting system.

Weaknesses:

1. However, the Uniswap DAO has its vulnerabilities. One significant risk is the potential for flash loan voting attacks. These attacks occur when an individual takes out a flash loan, which is a loan of UNI tokens from the treasury, and uses it to vote on a malicious proposal. This sudden influx of tokens gives the attacker temporary control over the majority vote without risking their funds. This is a severe threat that the Uniswap DAO must be vigilant about.
2. Uniswaps User Interface is notorious for being complex, especially for beginners.
3. It is implemented on the Ethereum blockchain, so transactions such as casting a vote are very costly compared to other blockchains.

### 2.3.16 The DAO

A token-based voting that gives the holders voting power and the ability to vote on proposed projects; voting power is directly tied to the number of DAO tokens a user has; the DAO was implemented on the Ethereum blockchain, and its core functionalities are powered by the smart contracts (Blockchains inc, n.d.).

Strength:

1. Voting security as only holders of the token are allowed to cast votes; this ensures only the verified votes are cast.

Weaknesses:

1. The DAO suffered a significant security vulnerability in its smart contract code, leading to a major exploit. This event resulted in the loss of a substantial amount of Ether. It prompted a controversial hard fork in the Ethereum blockchain to mitigate the exploit's effects.
2. The DAO raised legal and regulatory questions, and its failure led to discussions about the legal status and responsibilities of decentralised autonomous organisations.

### 2.3.17 Decentriland DAO

Decentraland is a virtual world where players/users can buy, build, and monetize virtual land, properties, and other forms of assets using its native $MANA Cryptocurrency token. The Decentriland DAO governs the platform's vision and rules. Users who have MANA tokens have the privilege to vote for and propose infrastructure upgrades, land distribution, and other policy changes (Decentriland, n.d.). This DAO is based on the Ethereum blockchain and is powered by smart contracts.

Strengths:

1. The platform is fully community-owned and decentralised.
2. The Decentriland DAO is fully censorship-resistant.
3. The platform offers an excellent and immersive experience.

Weaknesses:

1. The System is dependent on Ethereum scaling solutions.
2. It is still in its early stages of development.
3. It is built on the Ethereum blockchain, so transactions such as casting a vote are very costly compared to other blockchains.

### 2.3.18 AAVE DAO:

AAVE is a platform created to allow people to borrow cryptocurrencies and allow others(AKA Liquidity providers) to lend cryptocurrencies. Here, the lenders earn interest on their deposits while the borrowers pay interest on their loans. The AAVE DAO is used to vote on crucial parameters such as the reserve limit(The number of lender funds to be kept on hand in case a large number of lenders suddenly want to withdraw their deposits), collateralization ratios, and new asset listings (Kulechov, 2023). AAVE DAO is deployed on the Ethereum blockchain.

Strengths:

1. The platform became popular in the crypto space very quickly. AAVE is known for its high liquidity and large user base.
2. All DAO operations and governance decisions are documented on the blockchain, ensuring transparency and public auditability. This bolsters trust and promotes accountability within the broader community.

Weaknesses:

1. Reaching a consensus within a large and diverse community becomes more challenging and time-consuming with growth. This leads to delays in decision-making and hinders the protocol's responsiveness to market changes.
2. Large token holders(Whales) or coordinated groups can influence the voting outcome if they hold significant voting power. This leads to decisions that benefit specific groups/ a minority of users over the community.
3. Participating in governance requires good technical expertise concerning blockchain technology and smart contracts. This limits the participation of users with no technological background from contributing to the decision-making process.

### 2.3.19 Maker DAO

The Maker DAO was created for the purpose of maintaining $DAI, which is a decentralised stablecoin (Price is virtually stagnant at all times) pegged to the value of the U.S. dollar. Holders of the $MKR cryptocurrency token govern this system by managing collateral requirements, stability fees, and Oracle feeds (Makerdao, n.d.). The users lock up Cryptocurrency tokens as collateral in order to mint (create) new $DAI tokens, and the system algorithmically adjusts interest rates in order to maintain the peg.

Strengths:

1. Algorithmic stability.
2. Community governance.
3. Censorship resistance.

Weaknesses:

1. The system is reliant on oracles.
2. It is a very complex system to use.

### 2.3.20 The Graph DAO

The graph is used to index data for Web3 applications, enabling developers to efficiently query data from the blockchain. The Graph DAO enables holders of the native $GRT token to collectively decide which data sources are indexed and rewards for subgraph developers who build indexing protocols for specific DAPPs (The Graph Foundation,2022).

Strengths:

1. GRT token holders vote on key decisions like subgraph selection, protocol upgrades, and fee allocation. They also promote community ownership, alignment with user needs, and community-driven development.
2. The system is fully open-sourced.
3. Efficient data access due to indexing.

Weaknesses:

1. The protocol itself creates a risk of centralization because while aiming for decentralisation, the protocol currently relies on a centralised indexer and coordinator, posing the risk of censorship and other security risks.
2. Funding for future protocol development and incentivizing long-term participation by existing users is a significant ongoing challenge.

## Summary

The inception of cryptocurrencies dates back to 2008, when Satoshi Nakamoto, an anonymous individual or group, created Bitcoin. Blockchain technology, a decentralised ledger, was made popular by Bitcoin. In response to Bitcoin’s drawbacks, other cryptocurrencies (altcoins) like Litecoin first appeared in 2011. When Ethereum was established in 2015,at that time it made it possible for ICOs and decentralised applications (Dapps) to operate. 2017 saw a market boom but also some turbulence. Institutional and general attention were piqued by the increase in value of bitcoin. Blockchain integration across sectors, NFTs, and DeFi all contributed to the industry’s evolution. In 2021, institutional adoption rose. Because of their ability to revolutionise the financial environment as well as the growth of new niches such as play to earn gaming and NFT trading. Cryptocurrencies continue to shape the financial landscape, reflecting the transformative potential of blockchain technology and the need for further government regulations to prevent bad actors from abusing this technology. Table 2 is the summary of related works

Table 2: Summary of related works

| Authors | Title | Methodology | Limitations |
| --- | --- | --- | --- |
| Aboknin, Shir, 2021; | Piloting a blockchain based voting system: A case study in Estonia. Government Information Quarterly | Using a mobile application, voters used their national ID cards to sign their ballots digitally. Using Byzantine Fault Tolerance (BFT) consensus to protect encrypted vote storage on the blockchain ensures tamper-proof and transparent record-keeping. Furthermore, a “blind signature” method that anonymizes voters throughout the voting process protects against vote-buying and coercion. | The blockchain network faces scalability problems in the event of massive elections involving millions of votes.Although the system protects voters’ identities when they cast ballots, there are still concerns about metadata collection and the possibility of outside observation, and Some groups of people would not be able to vote in blockchain-based elections because they lack access to the required infrastructure and technology. |
| Kenny, 2019 | Denver will allow smartphone voting for thousands of people (but probably not you) | Voatz allows authenticated registered users to receive, mark, and submit a secret ballot of the correct style from virtually anywhere in the world. Every ballot submitted is encrypted and stored on a network of blockchain servers housed worldwide, managed by some of the largest cloud infrastructure providers. | Reliance on mobile devices might exclude specific demographics, including older people, raising accessibility concerns. Significant concerns exist about Voatz secretly sending voting patterns to the government. |
| Gwarzocha, et al, 2020 | The Democracy Earth Blockchain for Liquid Democracy the 21st Century | Aims to create a participatory and dynamic system of governance by proposing a concept known as Liquid Democracy, which combines the advantages of both direct and Representative democracy to create a completely democratic voting system | The concept of liquid democracy is new and may require comprehensive user education to ensure users fully understand and grasp the platform and its utility.And Scalability is a huge concern for a more extensive user base. |
| FollowMyVote, n.d. | Online voting software:Blockchain the end to end process, cryptographically secure voting | Uses elliptic curve cryptography(it validates new transactions to the blockchain and ensures that the transactions are authorised to execute) to address issues relating to trust, security, and accessibility with traditional voting systems. | As for early adopters, there will be a case of barrier to entry created by digital illiteracy and access to education. This factor is a setback because users may need time to adapt to the new voting system. |
| Fauzi et al, 2018 | The study of blockchain technology in election system | Blockchain technology is studied within a laboratory scope and is mainly applied to a small-scale election system. This application offers several advantages, such as simplicity, neutrality, security, and transparency, aiming to address deficiencies in traditional paper ballot election systems. | Implementing ECC algorithms correctly can be complex, especially in environments that are resource-limited, such as embedded systems. |
| Vo-Cao-Thuy el al, 2019 | Votereum: An Ethereum-Based E-Voting System | By leveraging blockchain's immutability and programmability through smart contracts, Votereum aims to provide a transparent and incorruptible framework for elections. | User adoption may be a crucial challenge, as the user experience is essential to ensure widespread acceptance of the platform.And At the time, smart contracts were vulnerable to many security risks; this is a critical challenge for the Votereum platform. |
| Boucher et al, 2019 | Crypto-vote | Leveraging advanced cryptographic techniques, A web interface for running ranked-choice voting elections powered by the ShuffleSum algorithm and the Damgard-Jurik cryptosystem. Rank choice voting allows voters to express nuanced preferences, supporting widely popular and less mainstream candidates without the concern of wasting their votes. CryptoVote uses the Damgard-Jurik | Homomorphic encryption introduces computational overhead, potentially affecting the efficiency and scalability of the voting system, especially during large-scale elections. And the hybrid model requires additional education for voters to understand the dual-layer security approach, and widespread adoption could face initial challenges. |
| Xu et al, 2019 | Case Study: SecureVote: Taking a Dapp from MVP to Production | integrating blockchain technology with homomorphic encryption to address the transparency and privacy concerns inherent in electronic voting. TokenVote is a general-purpose, multi-chain governance system for blockchain-based tokens developed by SecureVot | During large-scale elections, Homomorphic encryption introduces computational overhead, which can potentially affect the voting system's efficiency and scalability.Widespread adoption could face initial challenges, and hybrid models may require additional education for voters to understand the dual-layer security approach. |
| Horizon State, n.d. | Technology for 21st century elections | It extends beyond traditional voting systems, enabling decentralised decision-making for organisations and communities. A user can use their cryptographic hash, which is a special string of characters used to identify their vote. Everyone is able to see the vote cast using this hash. However, only the voter will be able to identify the vote as theirs. The platform operates using Decision Tokens. | Horizon State’s effectiveness relies on the stability and security of its underlying blockchain infrastructure. Any disruptions in the blockchain network could impact the reliability of the voting system. And Regulations surrounding blockchain and electronic voting may vary across jurisdictions. Horizon State might encounter challenges navigating and complying with diverse legal frameworks, potentially limiting its deployment in certain regions. |
| Agora, 2018 | Bringing our voting systems into the 21st century | Using a consensus algorithm designed for voting, a global community of node operators organised following hybrid permission or a permissionless model is incentivized to verify election results by the $VOTE token. | Agora is an entirely internet-based application; this might be challenging for countries with low internet speed/access. And educational barriers remain one of the primary drawbacks of internet/blockchain-based voting. |
| Votem, n.d. | An end-to-end verifiable digital voting protocol using distributed ledger technology (blockchain) | Uses a protocol known as proof-of-votes (POV) to conduct end-to-end verifiable elections on the blockchain. Proof of votes provides irrefutable evidence of the result of a valid vote that was cast as intended and substantiated by a user. Using blockchain technology, proof of votes performs verifiable key generation for elections public key, verifiable vote anonymization(encrypted by homomorphic crypto process) via mix-networks and verifiable vote decryption. In proof of votes, an election is run on a blockchain network, where each node participating in the network is explicitly granted permission by the authority conducting the election. These permissions include producing blocks, participating in the blockchain consensus algorithm, notarizing blocks, being an election key trustee, or being a mix-network node. | Building public trust in the security and reliability of blockchain-based voting is crucial for the adoption of platforms like Votem. Continuous education and transparent communication about security measures are essential. And adhering to diverse legal frameworks and regulatory requirements across jurisdictions challenges global adoption. Votem needs to navigate and comply with varying election laws. |
| Abuidris et al,2019 | A Survey of Blockchain Based on E-voting Systems | Luxoft e-votes partners with Digital ID registration companies to create a robust tamper proof, anonymity of voters, and security audits to voters; servers are spread across different rejoins to ensure a more robust system. The e-voting platform is open-sourced, so anyone can study and understand how the technology was created and how it actually works, promoting complete transparency. Luxoft e-votes is built on the Hyperledger Fabric built with Go and Javascript. It uses Elliptic Curve Cryptography(ECC), which is a type of public-key cryptography that relies on the mathematics of elliptic curves over finite fields.) and ElGamal(ElGamal is a public-key cryptosystem that enables secure communication through asymmetric key encryption.) cryptographic algorithm. E-votes are based on the Practical Byzantine Fault Tolerance- a consensus algorithm designed to attain a consensus in a distributed system even with the presence of malicious nodes/Byzantine faults. | Ethereum is very expensive when the network is busy. Gas fees go higher than $30 per transaction. This factor significantly increases the cost of an election, rendering the use of e-votes ineffective cost-wise. And Using third-party Web2 applications might create a security vulnerability for voting applications. |
| Abuidris et al, 2019 | A Survey of Blockchain Based on E-voting Systems | Uses Private/local Blockchains to modernise, secure, and simplify the election process. It uses the Elliptic Curve Cryptography (a version of public-key cryptography) algorithm to secure votes cast. To maintain user privacy and safeguard important information in digital communication, data storage, and online interactions. Polyas deploys several privacy-enhancing technologies including ECC and end-to-end encryption. | Some people do not have access to reliable internet and are not  computer literate. This factor excludes some voters from participating in the process. And for less tech-literate users, the online voting process may seem confusing or frustrating, leading to errors and or resentment toward the system. |
| Lam, 2018 | From Helios to Voatz: Blockchain Voting and the Vulnerabilities It Opens For The Future | Helios Voting system employs advanced cryptographic protocols to ensure the security and integrity of votes, including homomorphic encryption and allowing votes to be encrypted while enabling computation on the encrypted data. Helios enables voters to check the accuracy of the tally.after a voter submits their encrypted vote to the voting system, the voting booth stores the vote in IPFS before receiving the address of the file used to locate it later. Using the Ethereum smart contract, Helios retrieves the user votes from IPFS and publishes the address on the blockchain | While online systems offer features like end-to-end encryption, manipulating voters through disinformation campaigns or social engineering is a serious risk. And the complexity of the system and potential technical intricacies make it challenging for the public to understand and audit the voting process. |
| Uniswap, n.d; | The governance process | Any holder of the Uniswap token can submit a proposal. However, it must gather a total 25,000 votes in support before it can further be deliberated on. The second phase is called a consensus check, where the individual who initiated the proposal must outline the core changes, Persuade other participants, and gather at least 50,000 yes votes. Finally, the third phase called a governance phase has a requirement of 40 million worth of yes-votes for the proposal to be adopted. | There is a huge risk of flash loan voting attacks and the uniswap user interface is notorious for being complex. |
| Blockchains-inc, n.d. | The DAO | A token-based voting that gives the holders voting power and the ability to vote on proposed projects; voting power is directly tied to the number of DAO tokens a user has; the DAO was implemented on the Ethereum blockchain, and its core functionalities are powered by the smart contracts. | The DAO suffered a significant security vulnerability in its smart contract code, leading to a major exploit. This event resulted in the loss of a substantial amount of Ether. It prompted a controversial hard fork in the Ethereum blockchain to mitigate the exploit's effects. |
| Decentriland, n.d. | Decentriland DAO | The Decentriland DAO governs the platform's vision and rules. Users who have MANA tokens have the privilege to vote for and propose infrastructure upgrades, land distribution, and other policy changes. This DAO is based on the Ethereum blockchain and is powered by smart contracts. | The System is dependent on Ethereum scaling solutions, also it is still in its early stages of development, and it is built on the Ethereum blockchain, so transactions such as casting a vote are very costly compared to other blockchains. |
| Kulechov, 2023 | AAVE: crypto liquidity token protocol | The AAVE DAO is used to vote on crucial parameters such as the reserve limit(The number of lender funds to be kept on hand in case a large number of lenders suddenly want to withdraw their deposits), collateralization ratios, and new asset listings, AAVE DAO is deployed on the Ethereum blockchain. | Larger more diverse communities lead to difficulties in decision making, individuals with a large amount of tokens are able to sway the outcome of a poll. |
| makerdao, n.d. | The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System | Holders of the $MKR cryptocurrency token govern this system by managing collateral requirements, stability fees, and Oracle feeds. The users lock up Cryptocurrency tokens as collateral in order to mint (create) new $DAI tokens, and the system algorithmically adjusts interest rates in order to maintain the peg. | The system is reliant on oracles and is complex to use. |
| The Graph Foundation, 2022 | Introducing Graph AdvocatesDAO - A Decentralised Body Overseeing Community Grants & the Advocates Program | The Graph DAO enables holders of the native $GRT token to collectively decide which data sources are indexed and rewards for subgraph developers who build indexing protocols for specific DAPPs. | The protocol itself creates a risk of centralization because while aiming for decentralisation, the protocol currently relies on a centralised indexer and coordinator, posing the risk of censorship and other security risks. And funding for future protocol development and incentivizing long-term participation by existing users is a significant ongoing challenge. |

# CHAPTER 3: REQUIREMENTS, ANALYSIS, AND DESIGN

## 3.1 Overview

This chapter provides a detailed description of the functional and non-functional requirements of this project, the application design and architecture and the approach taken to analysis and design.

## 3.2 Methodology

Software development is the creating, testing and maintenance of software products. According to GeeksForGeeks (2023) software development methodologies are frameworks/ models that guide the software development process by defining roles, activities and deliverables for the software development team.Some types methodologies include

1. Waterfall Methodology- is a sequential and linear approach to software development, requiring the completion of each step before going on to the next. The project is divided into phases, which usually include gathering requirements, designing the system, implementing it, testing it, deploying it, and maintaining it. It travels along a predetermined, organised route. Advantages of this method include: Presence of documentation, clarity and its default suitability for projects that have stable requirements, However its disadvantages are its lack of flexibility to changes in requirements, and lateness in issue detection because testing is done after the development phase.
2. Agile Methodology- is an incremental and iterative software development methodology that prioritises client feedback, adaptability, and teamwork. It includes a number of approaches, including Extreme Programming (XP), Scrum, and Kanban. Agile development divides the project into manageable chunks with little advance planning and permits modifications in response to changes in project scope along the way. Advantages of this approach include:better adaptability to changing requirements, continuous improvement and a high degree of user involvement. However its disadvantages come from its user involvement as this leads to the method being communication intensive, and it may be difficult to implement under strict requirements from project or regulatory constraints.
3. Incremental Methodology - With the incremental model, software is developed iteratively in smaller steps. New features or functionalities are introduced in each iteration, which represents a fraction of the entire system. This enables the system to be tested and partially implemented at each increment. The advantages of this method is: it reduces the risk of project failure by providing tangible results early, it is also flexible to changes in requirements, but its disadvantages stem from its need for very careful planning to decide what increments to start with and dependencies between increments may further complicate the development process.
4. Building and delivering features is the main goal of feature-driven development (FDD), an iterative and model-driven methodology. It works especially well for extensive projects with lots of features. To encourage clarity and methodical development, feature-specific development (FDD) divides the development process into teams that are each in charge of a specific feature.

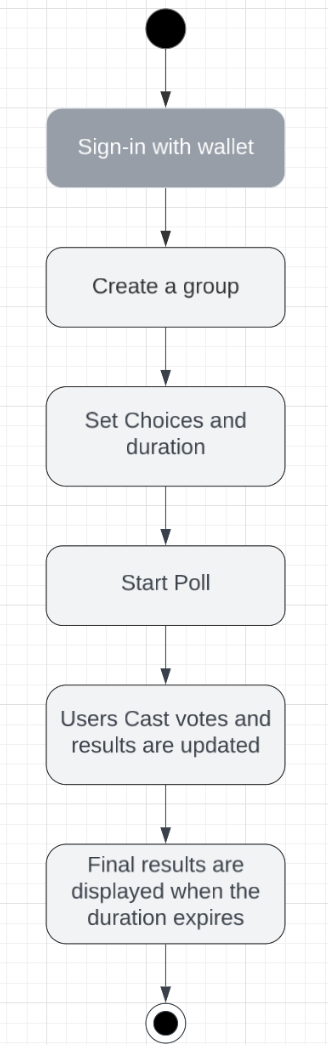
The methodology that will best fit this project is the incremental development because the blockchain space is constantly coming up with new innovations and findings on existing products which may lead to changes in the project and each component of the system requires a completely different set of tools. Thankfully these tools are very integrable/ built to work together.

## 3.3 Proposed Model

The user interface(frontend) uses the request method from the JavaScript Ethereum object to enable users sign-in using any of the popular wallets that support the ethereum network. This allows the user have access to the application, then the frontEnd uses the ethers.js module, the ERC20 ABI(Application binary interface) which is just an object that defines the implementation of all the functions to be accessed in the smart contract, the smart contracts contract address, and the infura provider(ethereum node) to create an instance of the smart contract. With this instance the system can make function calls directly to the target smart contract on the blockchain.

In order to protect the privacy of users who are part of a poll a **hashtable (Mapping) data-structure** whose visibility is marked as **private** is used on the smart contract to store the list of registered voters for each poll, and no functionality is implemented to read from the mapping on the smart contract, so no actor can actually know what users are registered once the list of registered voters has been saved. It is mandatory for the group/poll administrator to specify the wallet addresses of each of the participants of the poll, so only people who are registered will be able to participate, to ensure privacy of the poll from people who have no business with it, the polls themselves will be displayed in groups, similar to how apps like google classroom work, where each lecture (poll in this case) is stored in a group (classroom in this case). The firebase DB is used to store the metadata of the group, to ensure efficient loading of content for the user and to reduce cost, this is because writing the metadata to the smart contract will cost money, slow down the smart contract, and result is slow loading of content, especially when the blockchain network is congested.

Given that, the process of voting entails the administrator of the poll initiating the creation of a group by specifying the event and the people who will participate in the poll by providing the list of wallet addresses of all participants. Next, the administrator has to start the poll in the created group, this prompts them to specify the candidates/options to be voted for, and a duration for the poll, then the poll commences and the standings are updated whenever a vote is cast, when the duration elapses, the final results are displayed. Figure 1 describes this process diagrammatically.

****

**Figure 1 Proposed model diagram**

## 3.3.1 Interview

The questions asked during the interviews are:

1. What do you think would make an E-voting system more trustworthy?
2. What complaints do you have about existing methods that you suggest should be corrected in this system?
3. How would you describe an ideal e-voting system?

The outcome of the conducted interviews can be found in appendix B.

## 3.4 Tools and Techniques

The tools that will be used in implementation of this voting system include :

1. Ethereum blockchain - This blockchain is the best fit for the project because it is the most popular choice for developers who create blockchain based applications, so it would be easier to solve any errors and find educational resources.
2. Solidity programming language will be used to create the smart contract which is responsible for storing the list of registered users and the poll results.
3. Remix and Visual studio code will be used as the IDE’s and Github will be used for version control.
4. The Front End will be created using the JavaScript language, React.js library, ethers.js, css and sass.
5. ethers.js will be used for facilitating interaction between the application and the smart contract via the Infura provider/node.
6. Firebase will be used for deployment of the frontend and storing the metadata of the group. This is because storing this data on the blockchain will make the system more expensive to use. Additionally, with firebase it is possible to deploy both the database and the frontend with a simple set of console commands and completely free.
7. Sepolia testnet will be used for testing smart contracts. Sepolia testnet is a simulation of the ethereum blockchain, it is used to deploy smart contracts to see how they function.

## 3.5 Ethical Consideration

1. Security and privacy - There are cyber threats to voter privacy and anonymity. But implementation of good cryptographic techniques and proper security testing, the security and privacy of voters can be assured.
2. Transparency and accountability - The point of blockchain voting systems is to improve trust in democratic processes through transparency and accountability. Transparency and accountability can be upheld by providing a means of verifying the accuracy of the process.
3. Decentralisation vs Centralisation - There is a need for balance between both that ensures orderliness and no opportunity for administrators to abuse power.
4. Compliance with Legal and regulatory frameworks for data privacy and usage.

## 3.6 Requirement Analysis

1. The app should provide an efficient and secure sign-in method.
2. The users should be able to initiate transactions such as casting votes and creating groups.
3. The users should be able to create and join groups.
4. The users should be able to view the current results in real time.
5. Only users whose wallet addresses were registered when the group was created are allowed to cast votes.
6. The user's privacy should be maintained.
7. The UI must be properly navigable and user friendly.

## 3.7 Requirements Specifications

1. User interface - The Visual representation of the app for interaction between users and the system.
2. Smart Contract - This is used to store the list of registered voters, eligible voters, and results of the poll.
3. Firebase DB - This is used for storing the group’s metadata. This enables faster loading of the group's content.
4. Crypto Wallets - This mechanism will facilitate user authentication and casting votes.
5. Ethereum blockchain - This is the platform the applications core functionality will be built on.

The system prompts the user to sign-in using their wallet, the wallet will be used to confirm transactions and identify the user (the ethers.js module will be used to facilitate interaction between the wallet and the blockchain), The user can request to create a group if they aren't in one. This prompts them to enter the wallet addresses of participants for the poll (anybody whos wallet address is not entered won't be able to join the group or cast a vote), and a duration for the poll, or join a Group, the current results are read from the blockchain using the ethers.js module anytime a vote is cast. In the end the aggregates, rankings, and statistics will be displayed.

### 3.7.1 Functional Requirement Specifications

Functional requirements are the services a system must be able to provide, or functions a system should be able to perform.The functional requirements of this project are outlined in table 3.

Table 3: Functional Requirement Specifications

| **Req. No.** | **Description** | **Type** |
| --- | --- | --- |
| R-101 | Sign-in using a cryptocurrency wallet. | Function |
| R-102 | Creating a group and registering users | Function |
| R-103 | Starting a poll. | Function |
| R-104 | Casting a vote. | Function |
| R-105 | Updating and displaying current results in real time and viewing the accurate statistics of the final result when the poll is over. | Function |
| R-106 | Archiving groups | Function |
| R-107 | Logging out. | Function |

### 3.7.2 Non-Functional Requirement Specifications

Non-functional requirements specify how the system should perform its functions. These requirements focus on what qualities the system must possess such as performance, usability, and security. The Non-functional requirements of this project are outlined in table 4

Table 4: Non-Functional Requirement Specifications

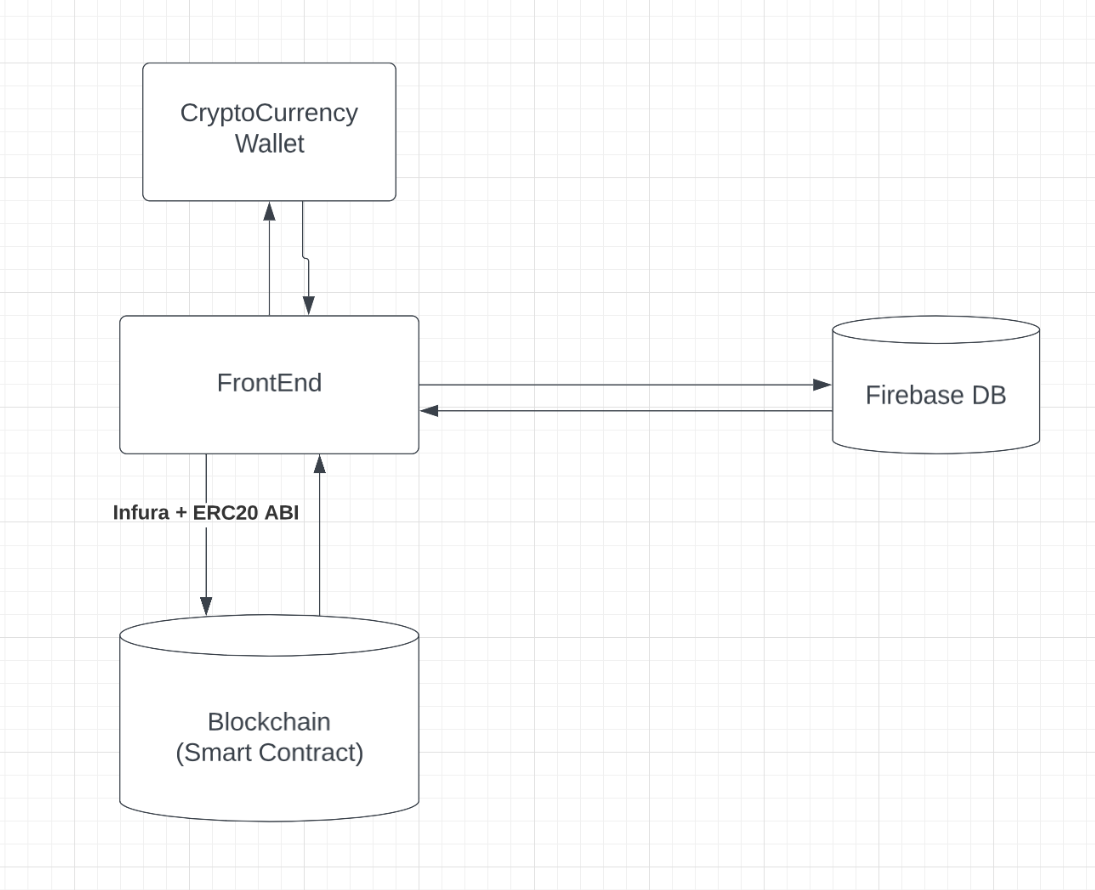
| **Req. No.** | **Description** | **Type** |
| --- | --- | --- |
| R-108 | The system must be able to handle multiple groups hosting polls at the same time, and efficiently store their data separately. | Usability |
| R-109 | The FrontEnd shall follow the best coding practices for accessibility and simplicity, to ensure an inclusive experience for users with disabilities. | Usability |
| R-110 | Users will receive feedback on every transaction within 10 seconds on average. | Performance |
| R-011 | The Smart contract must check that a person casting a vote is registered for the poll and has not voted before before registering the vote. | Security |

## 3.8 System Design

Blockchain technology has emerged as a game-changer in the quest for secure and transparent voting. This section will explore the design and architecture of a blockchain-based voting system and a diagrammatic depiction of the application is shown in figure 3.

1. UI - This is the front end of the application which the user interacts with.
2. Crypto wallet - This is the mechanism for creating and signing into accounts, casting votes, it facilitates all interaction with the blockchain.
3. Firebase DB - This is used to store the users of the application and the groups they are in, this is for the purpose of verifying if they are allowed to join a group on the application.
4. Ethereum blockchain - This is the platform used for the deployment of smart contracts whose state variables are used to store data such as the choice candidate in a poll. The ERC20 ABI is a standard way to interact with a smart contract on the blockchain.
5. Infura node - This will serve as the node which the voting app will use to communicate with the ethereum blockchain, requests are made to the node via an api and the node directly interacts with the blockchain.

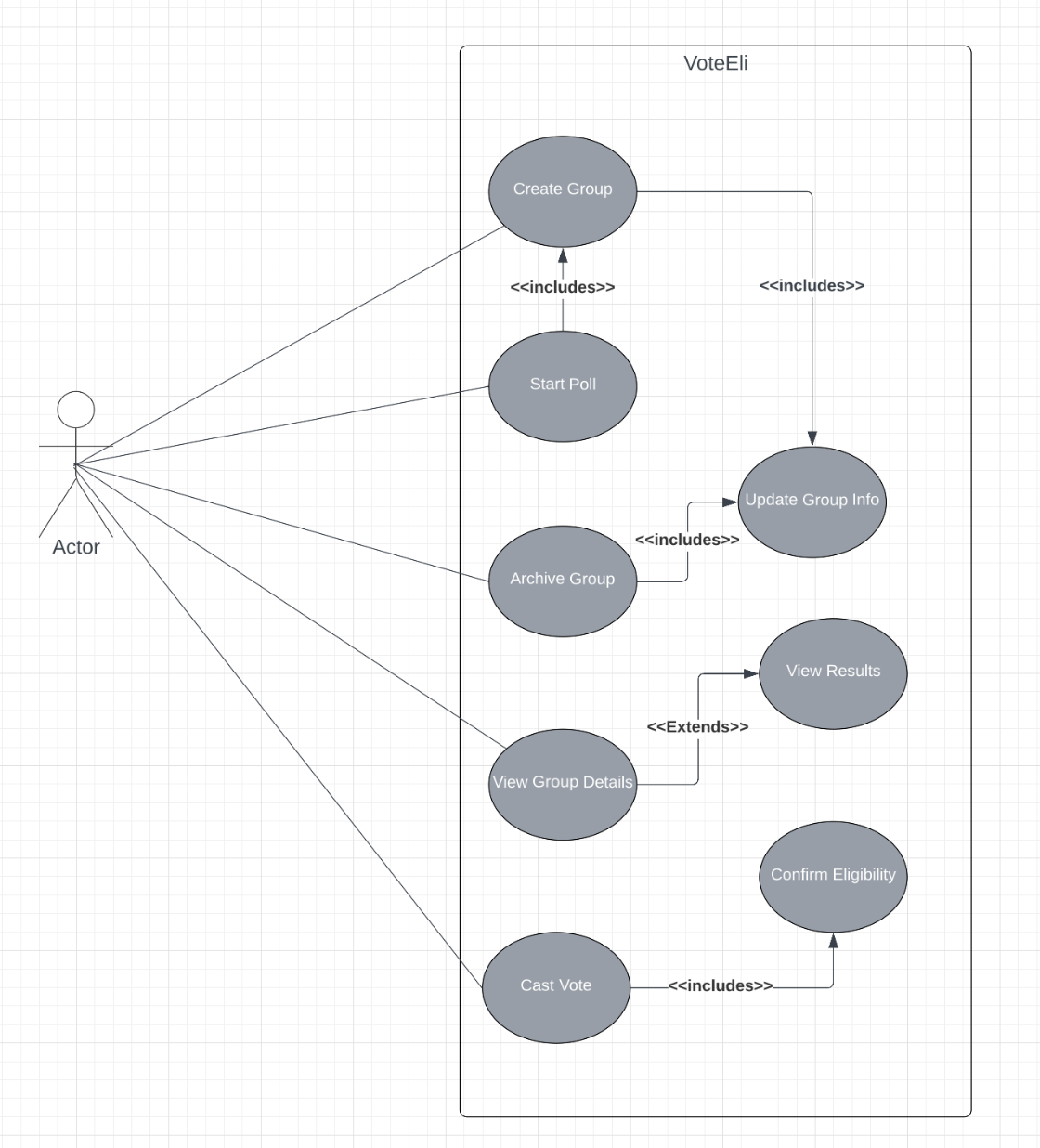
### 3.8.1 Application Architecture



**Figure 2 Application Architecture**

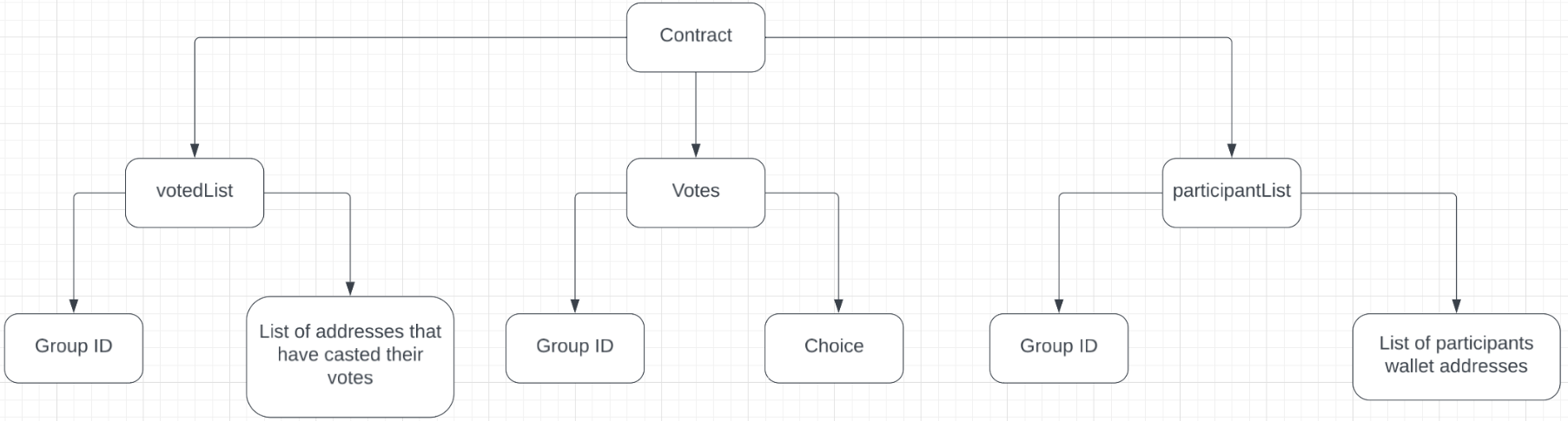
### 3.8.2 Use Case

The use-case diagram displayed in figure 4 describes the application from the users perspective by identifying the functions they can carry out.

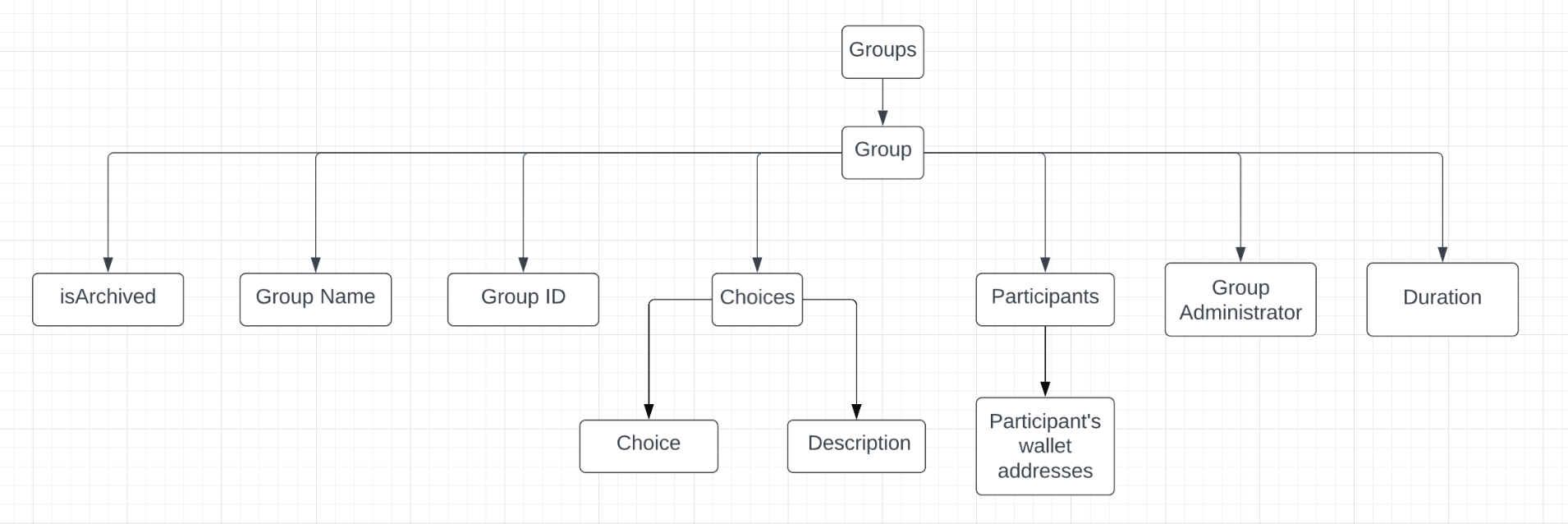


**Figure 3 Use Case diagram**

### 3.8.3 Data Design

****

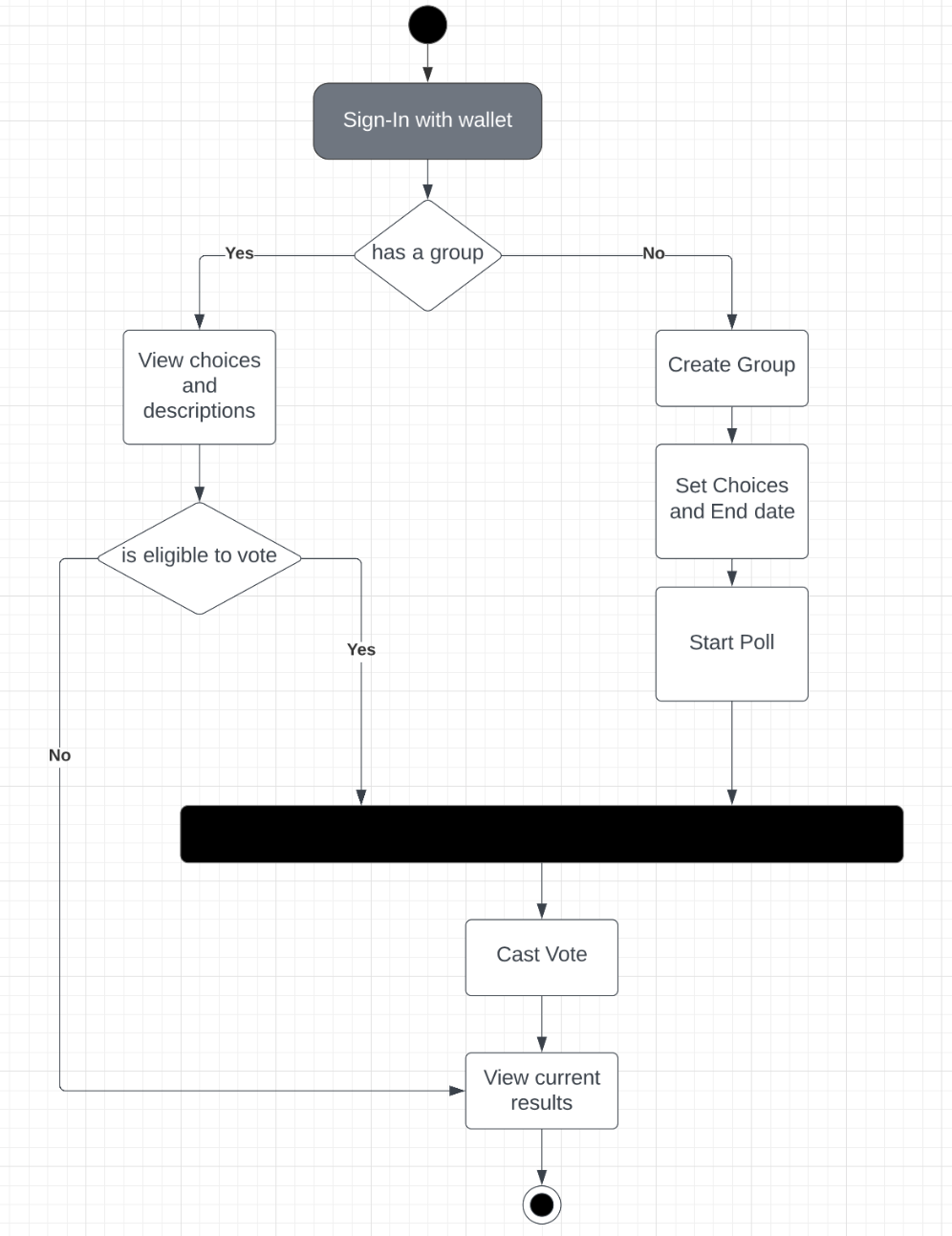
**Figure 4 Data design diagram for the smart contract**

****

**Figure 5 Data design diagram for the firebase DB**

### 3.8.4 Activity Diagrams

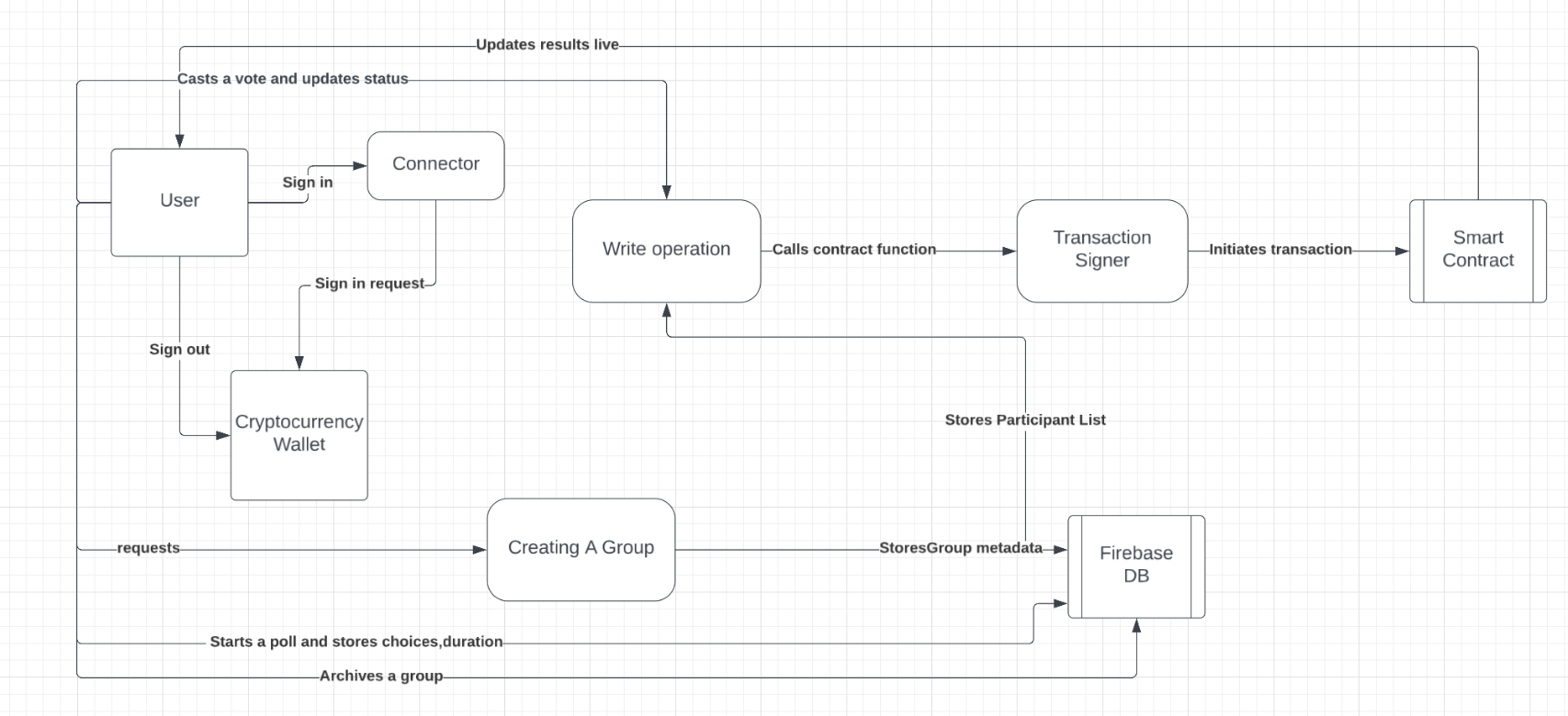
The activity diagram displayed in figure 6 details the steps a user will take to cast a vote.

****

**Figure 6 Activity Diagram**

### 3.8.5 Data flow Diagram

The diagram shown in figure 7 describes how data flows from one aspect of the system to another.



**Figure 7 Data flow diagram**

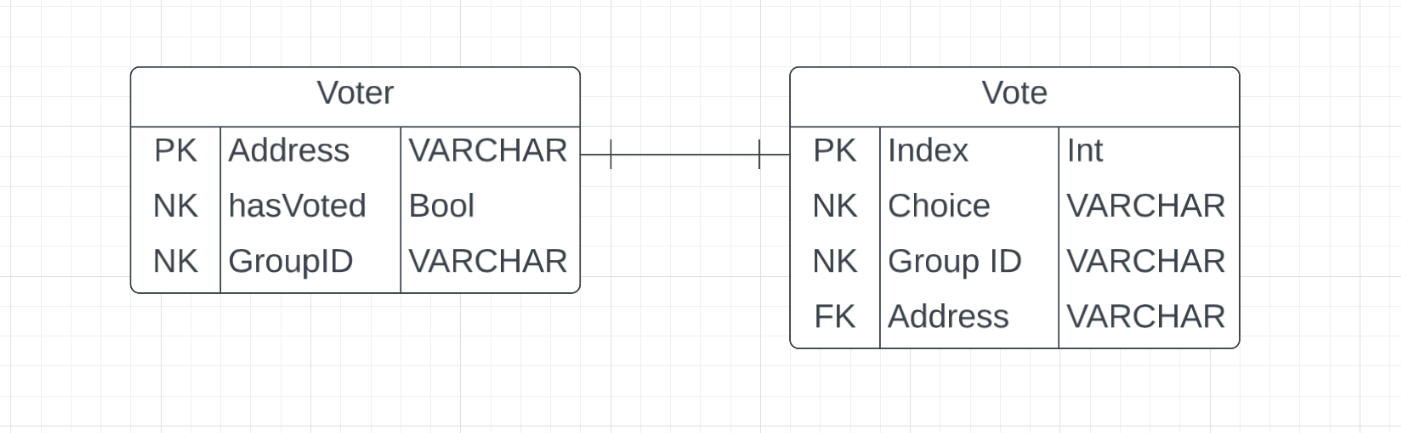
### 3.8.6 Control Flow Diagram



**Figure 8 Control flow diagram**

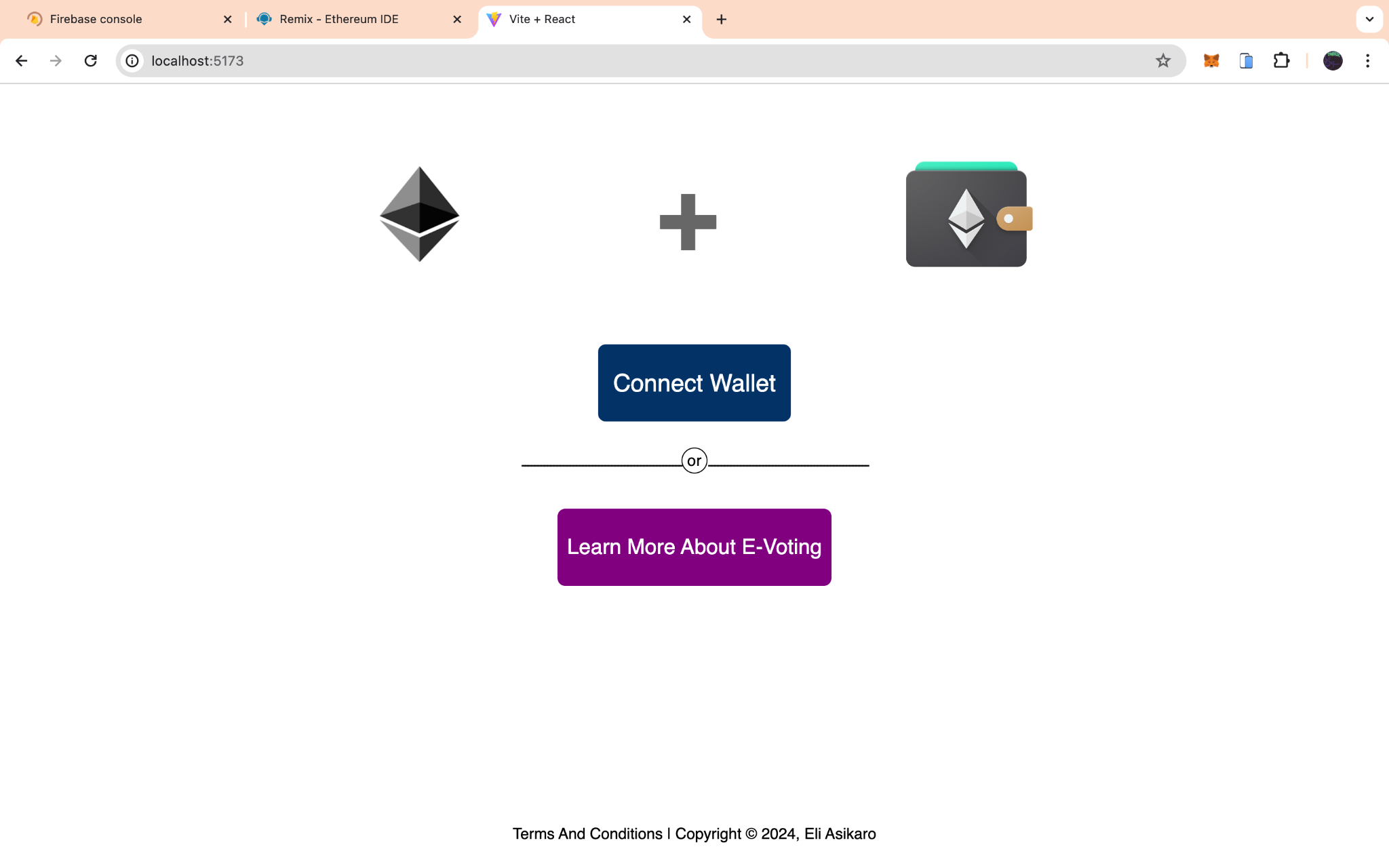
### 3.8.7 Entity-Relationship Diagram (ERD)

The diagram shown in figure 9 describes how the smart contract stores data, the **voter** entity represents each participant and whether they have voted or not, and what group they are registered for, the **vote** entity represents the votes participants cast, in this relationship, one voter may cast only one vote in a group.

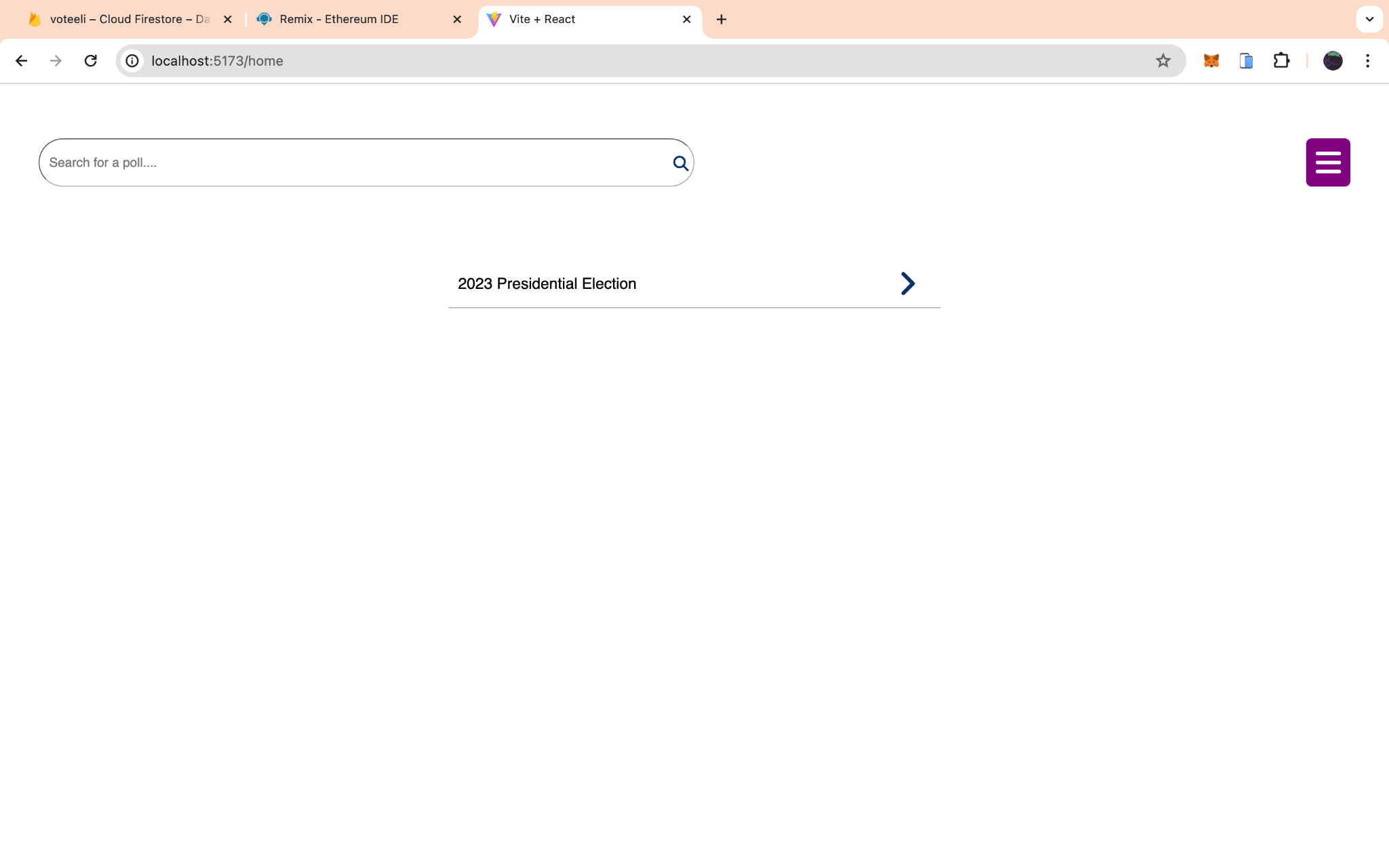


**Figure 9 Entity Relationship Diagram**

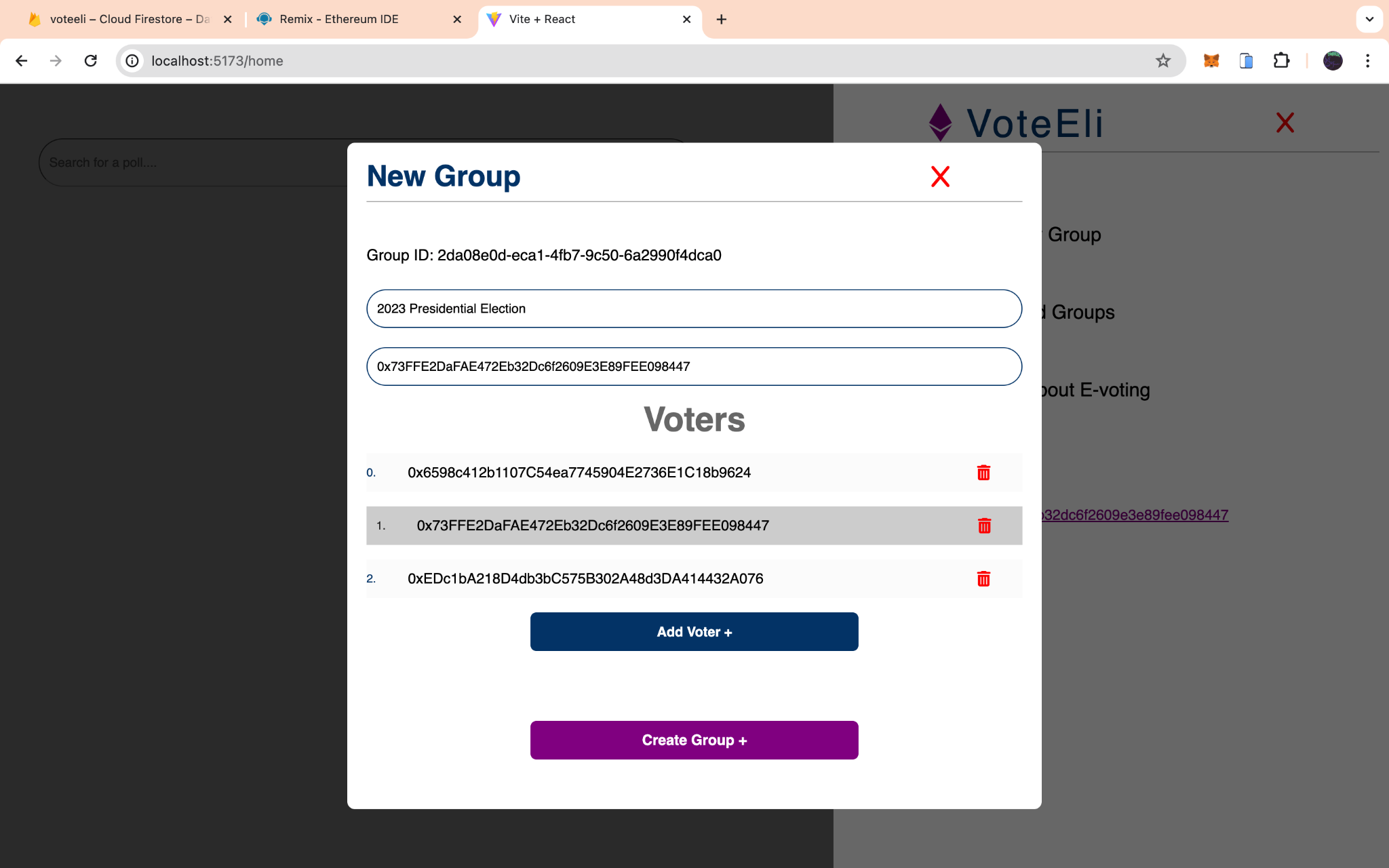
### 3.8.8 User Interface Design



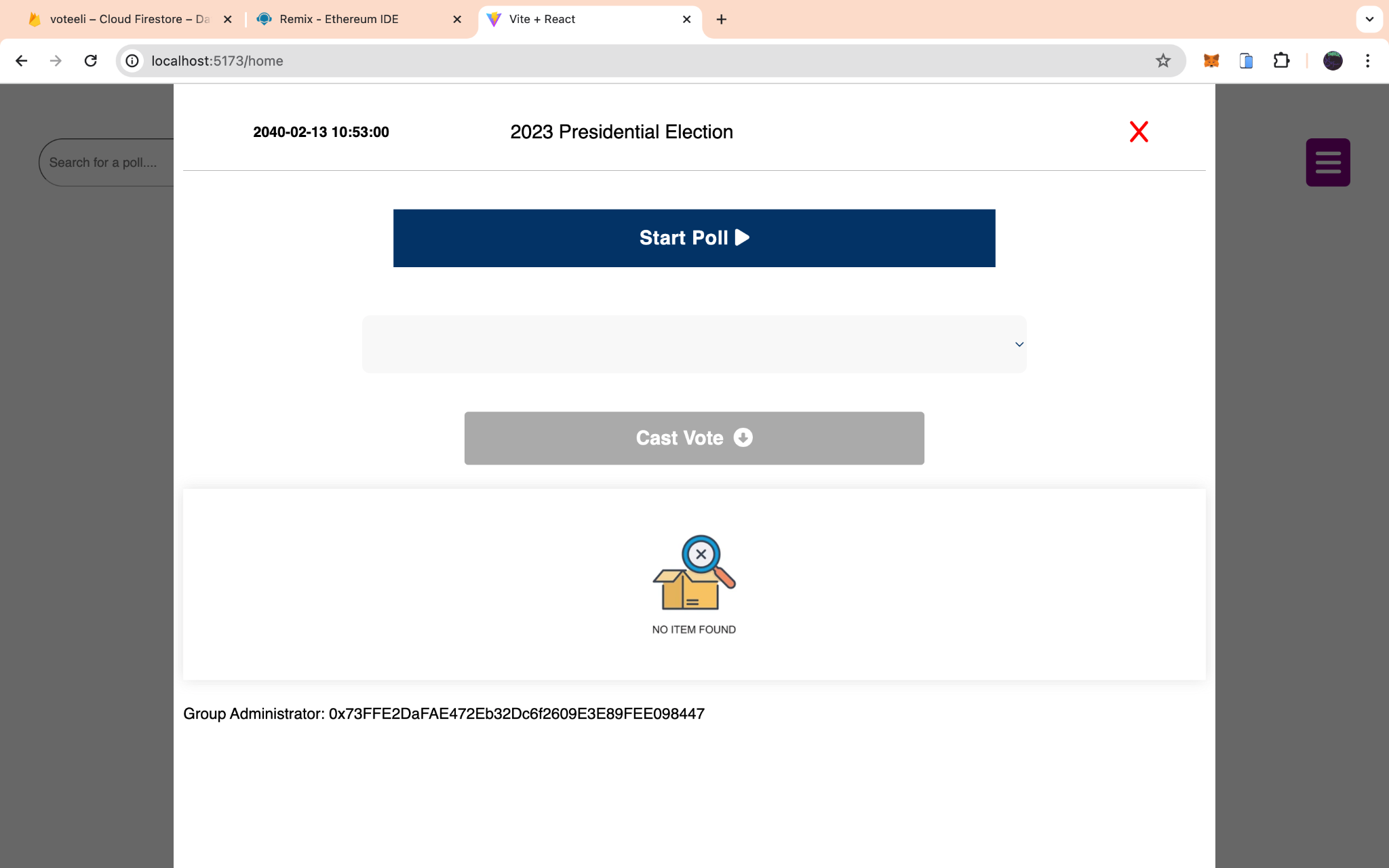
**Figure 10 Sign In page**



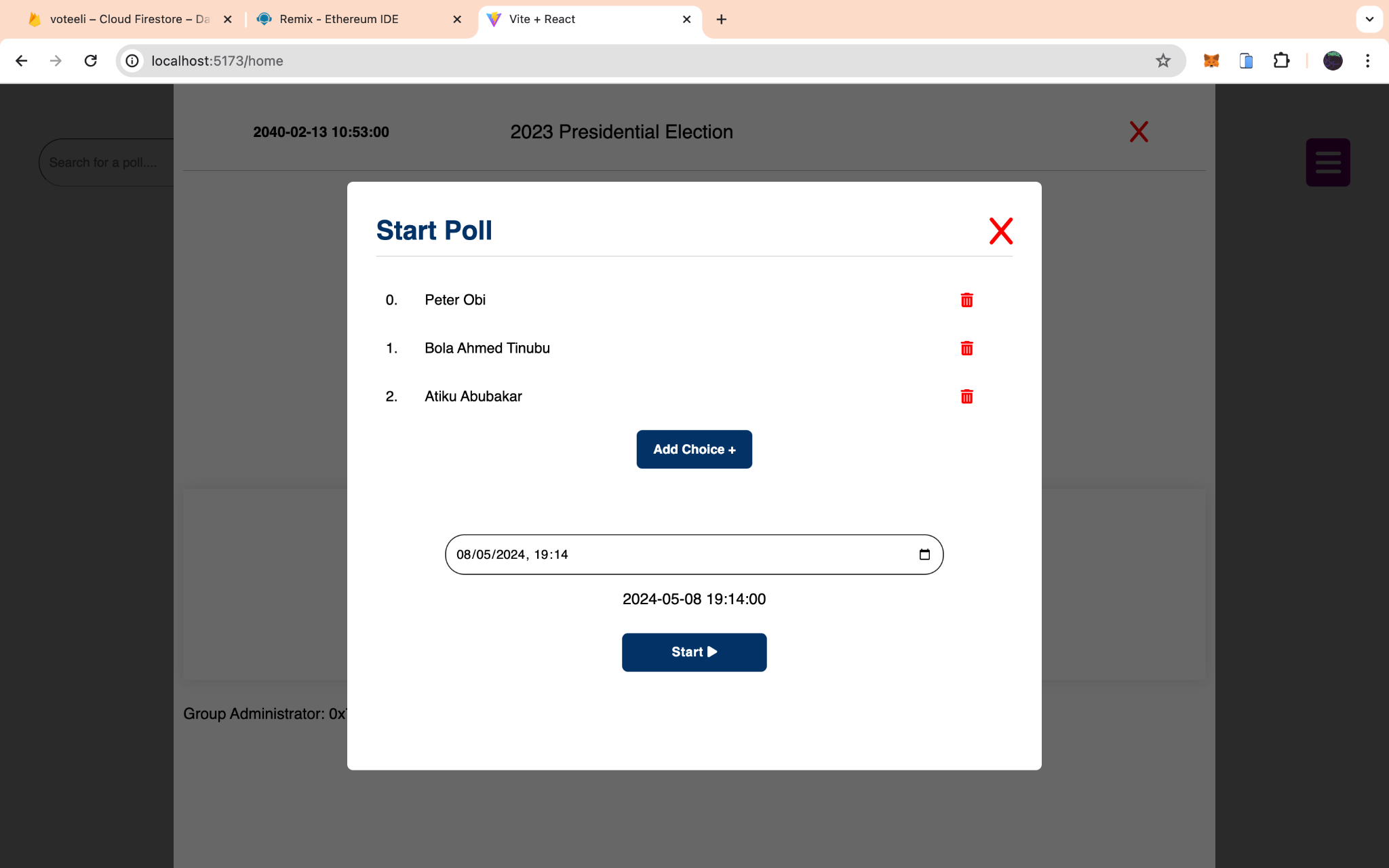
**Figure 11 Home page**



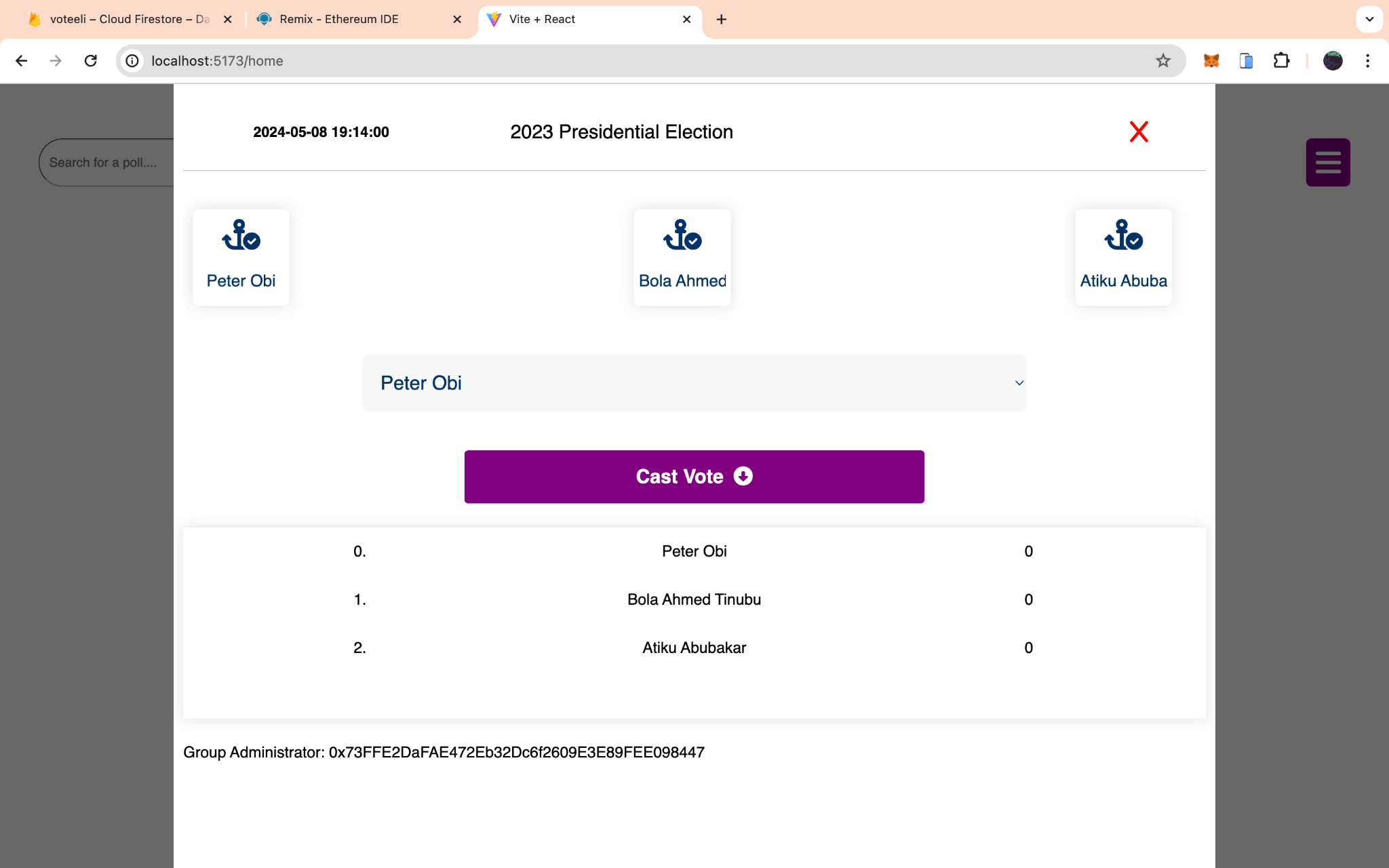
**Figure 12 Creating a new group**



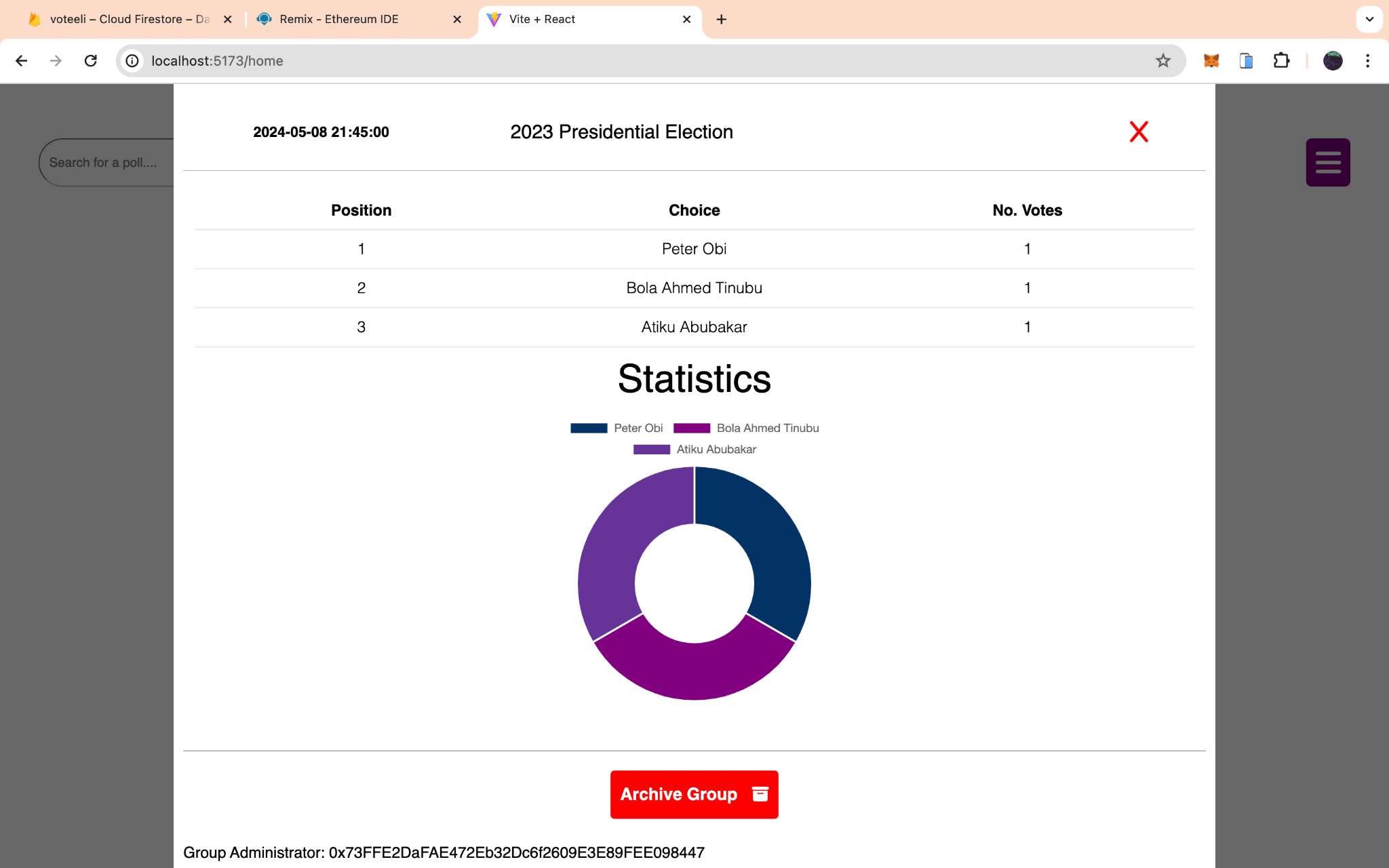
**Figure 13 Group Page (The poll has not started)**



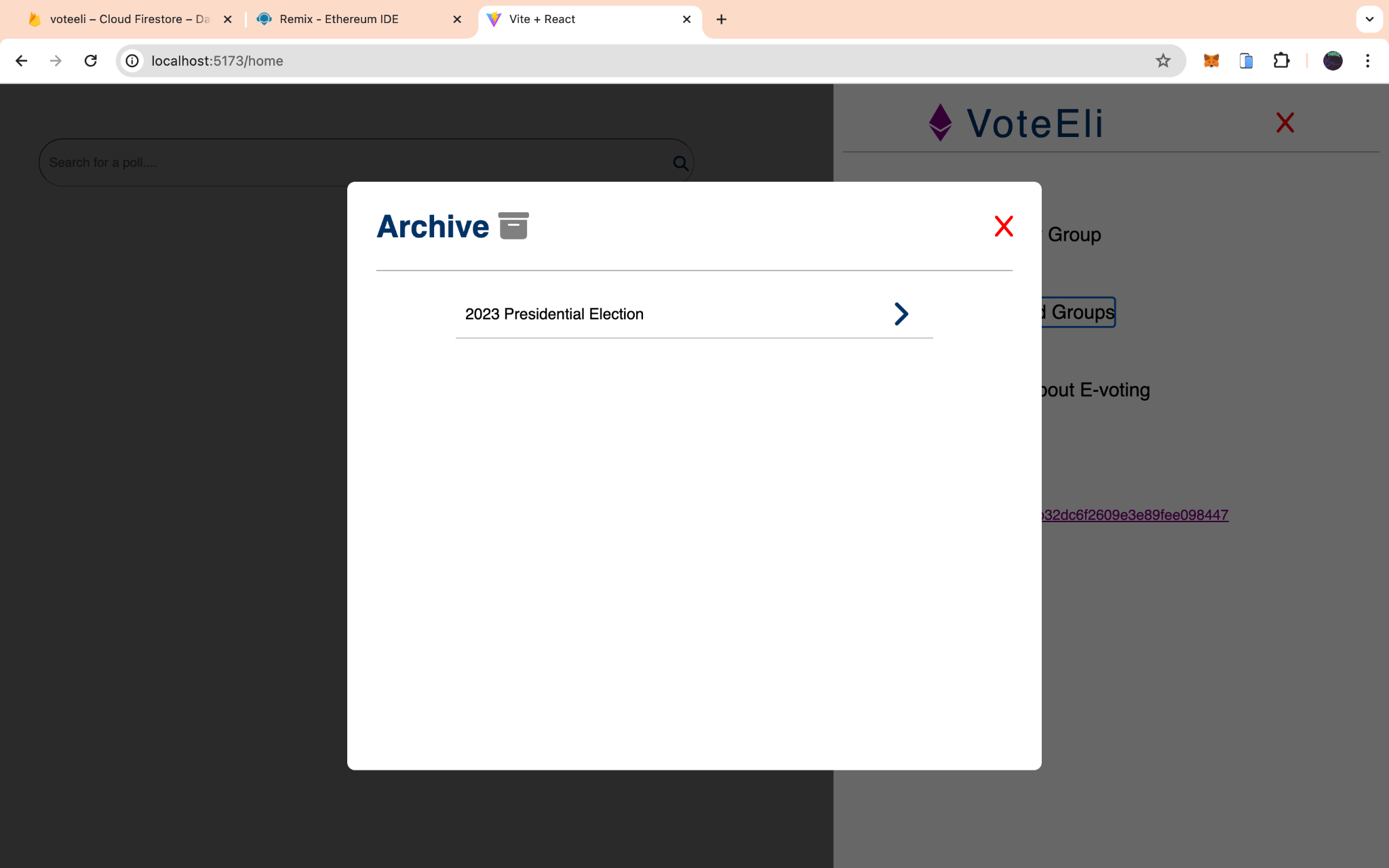
**Figure 14 Start poll page**

****

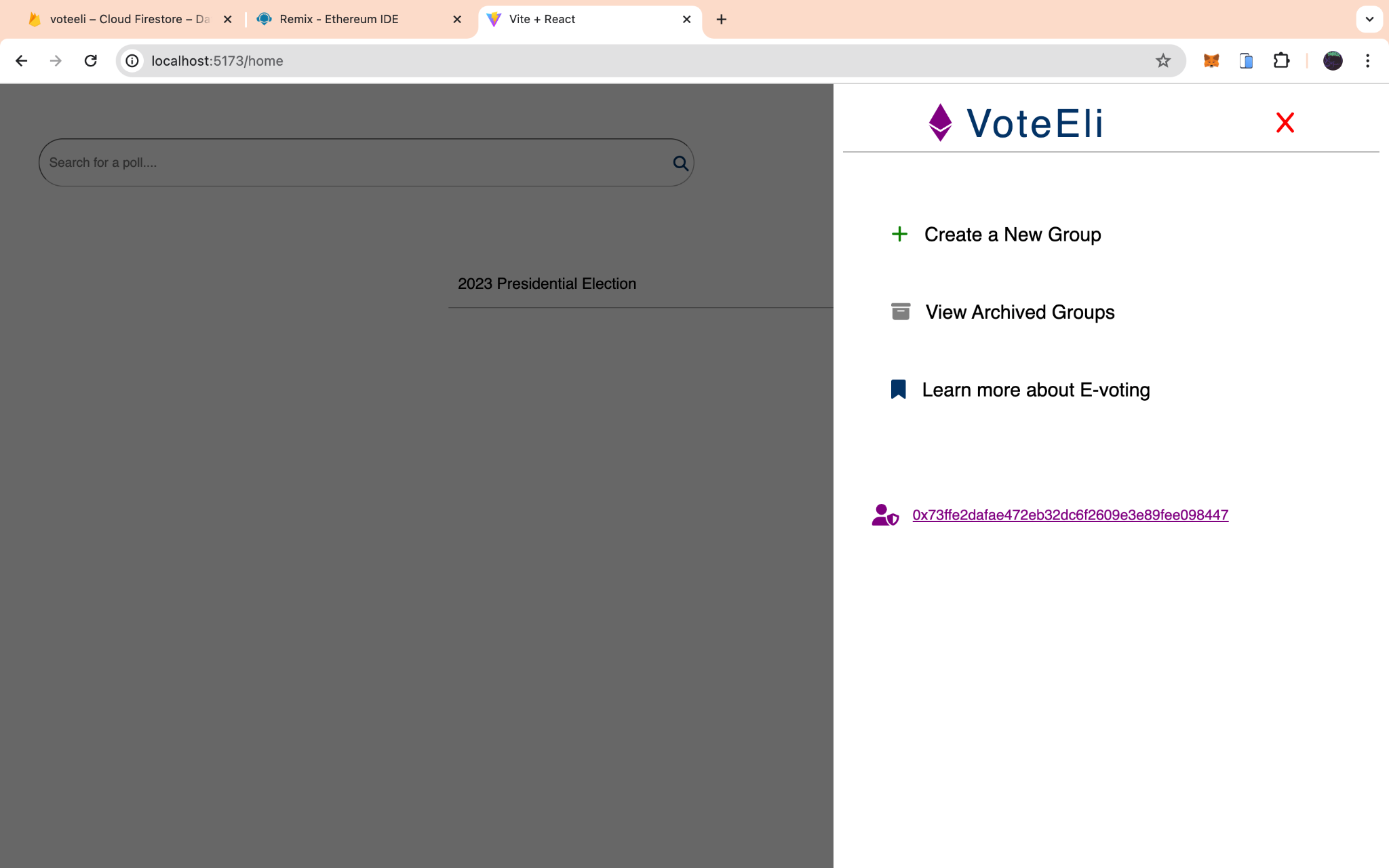
**Figure 15 Poll Page**

****

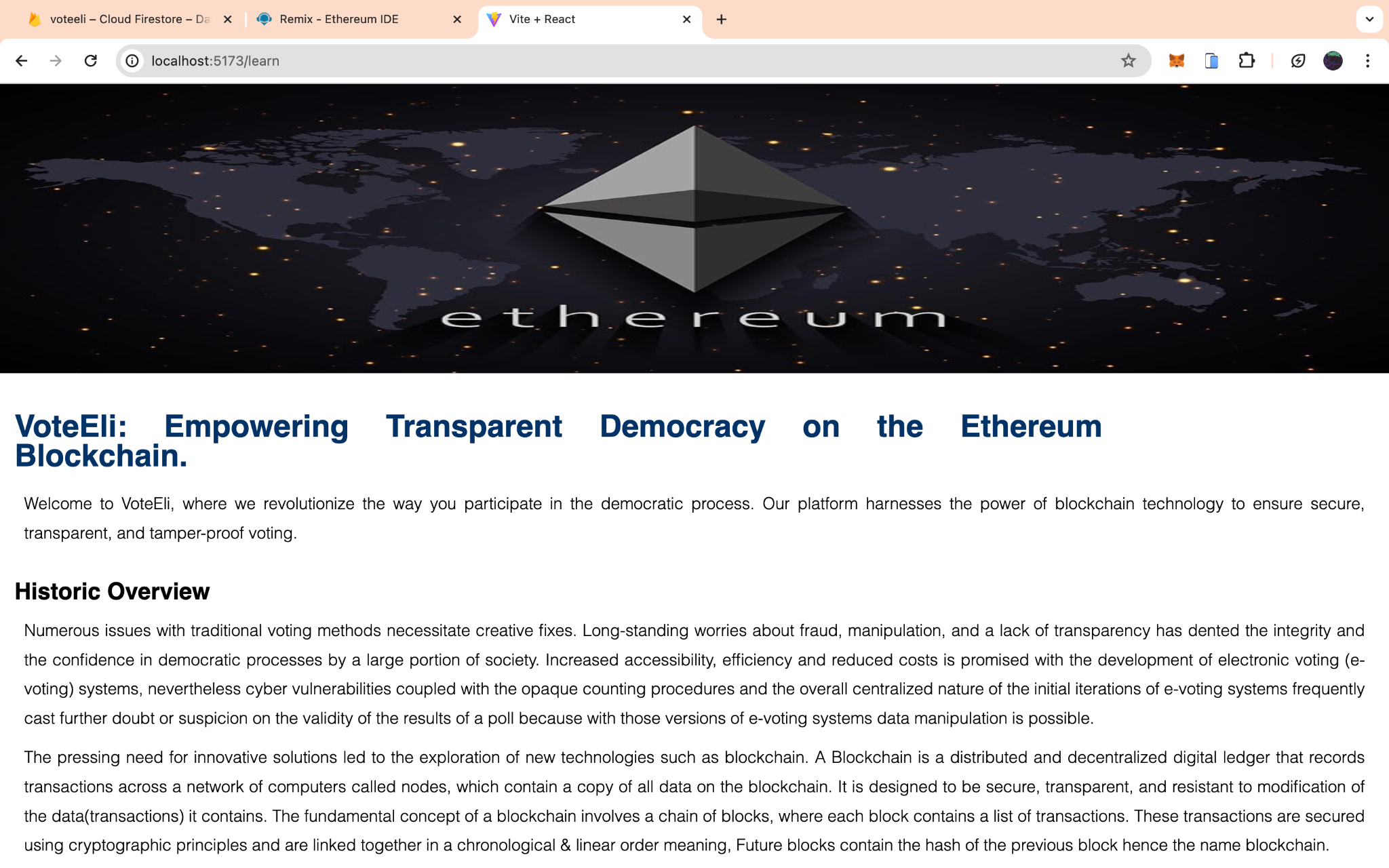
**Figure 16 Results Page**

****

**Figure 17 Archive Page**

****

**Figure 18 SideBar menu**

****

**Figure 19 Learn more page**

### 3.9 Summary

Waterfall, agile, FDD, and incremental methodologies are different approaches to software development, each with its strengths and weaknesses. Incremental development is the best choice for this project because it best serves its requirements, such as getting tangible results early, receiving feedback from external sources, and having the flexibility to incorporate changes in the project’s requirements.

Considerations for this project are mainly from a legal/regulatory and usability standpoint. Some significant requirements are user friendliness, transparency, security, and being able to provide users with all necessary privacy features while not compromising the system’s ease of use. These goals will be achieved using a combination of the blockchain and a relational database, which stores metadata associated with a poll; this measure aims to reduce the costs associated with writing to the blockchain.

The deliverables outlined above will play a crucial role in guiding the implementation and testing of the final product.

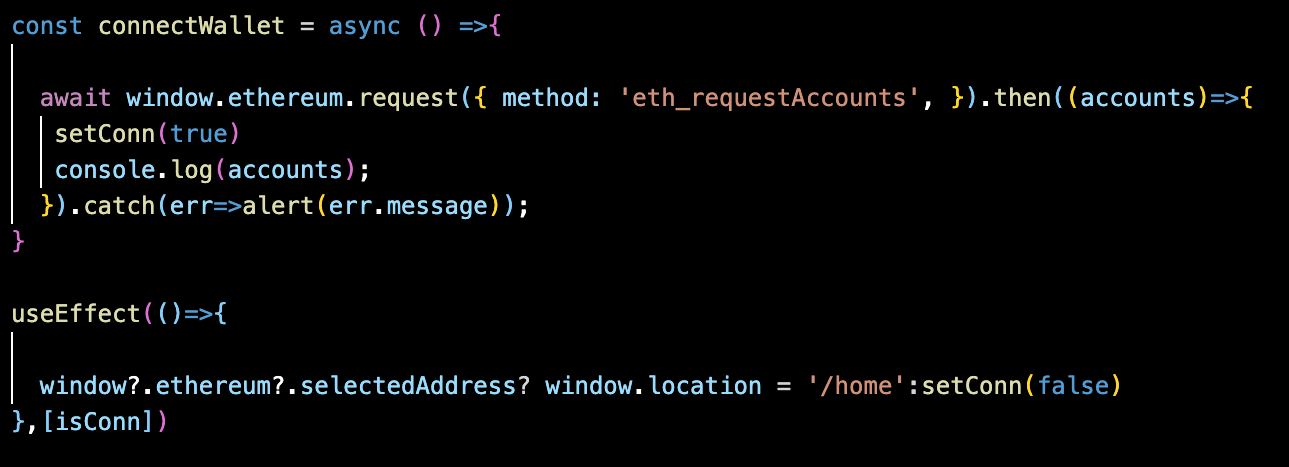
# CHAPTER 4: IMPLEMENTATION AND TESTING

## 4.1 Overview

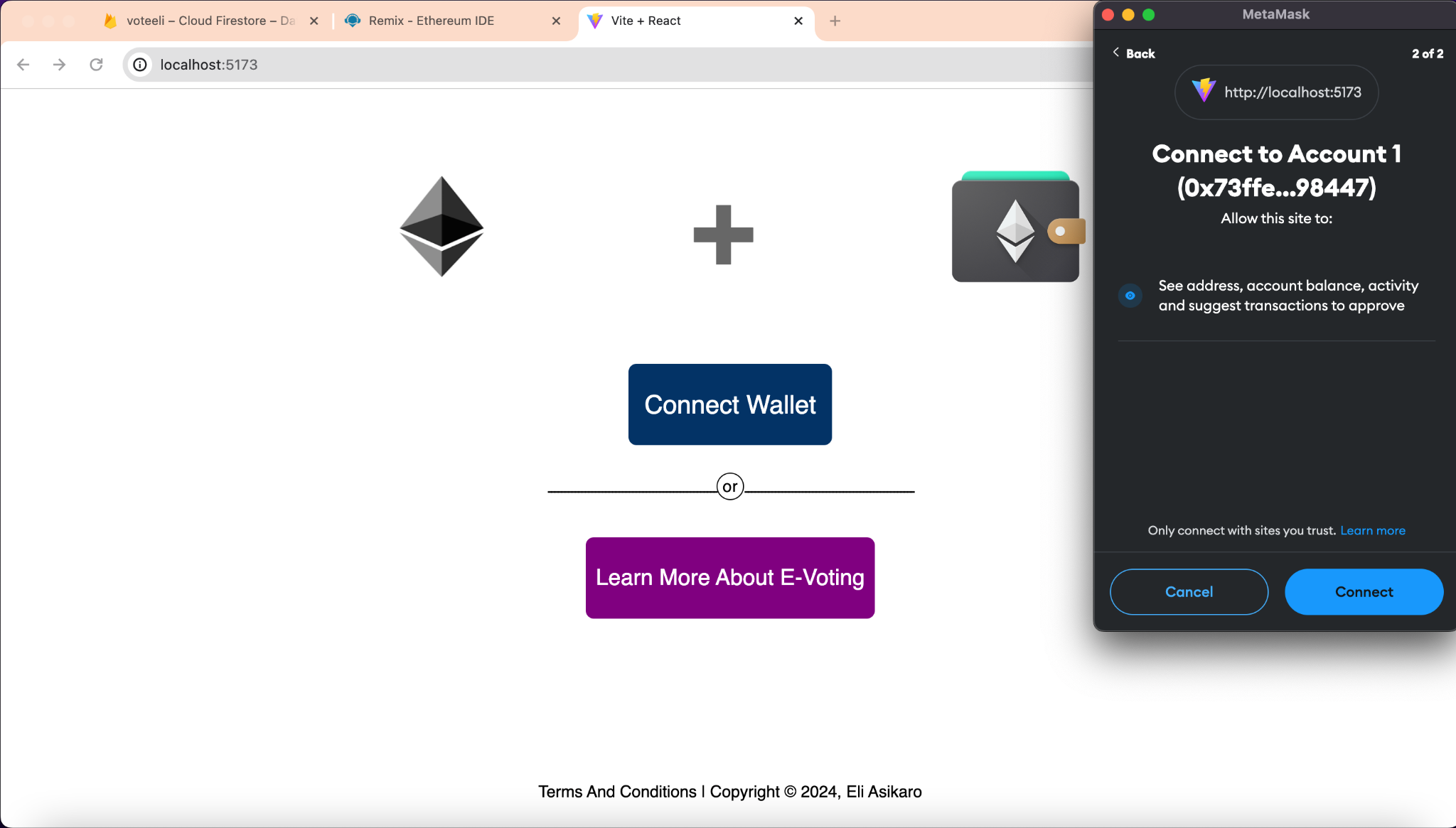
This chapter describes the core features that are implemented for this system, the issues encountered during its implementation and how each problem was resolved, as well as the various types of tests conducted, the aim of each testing step, and the results obtained from each step this includes the errors found and the corrections made to the implementation and design. Finally, a guide on how to use the system.

## 4.2 Main Features

1. Sign In using a cryptocurrency wallet. Figure 20 is the code snippet for enabling wallet sign-in, and figure 21 is the resulting prompt to confirm the sign-in on the wallet

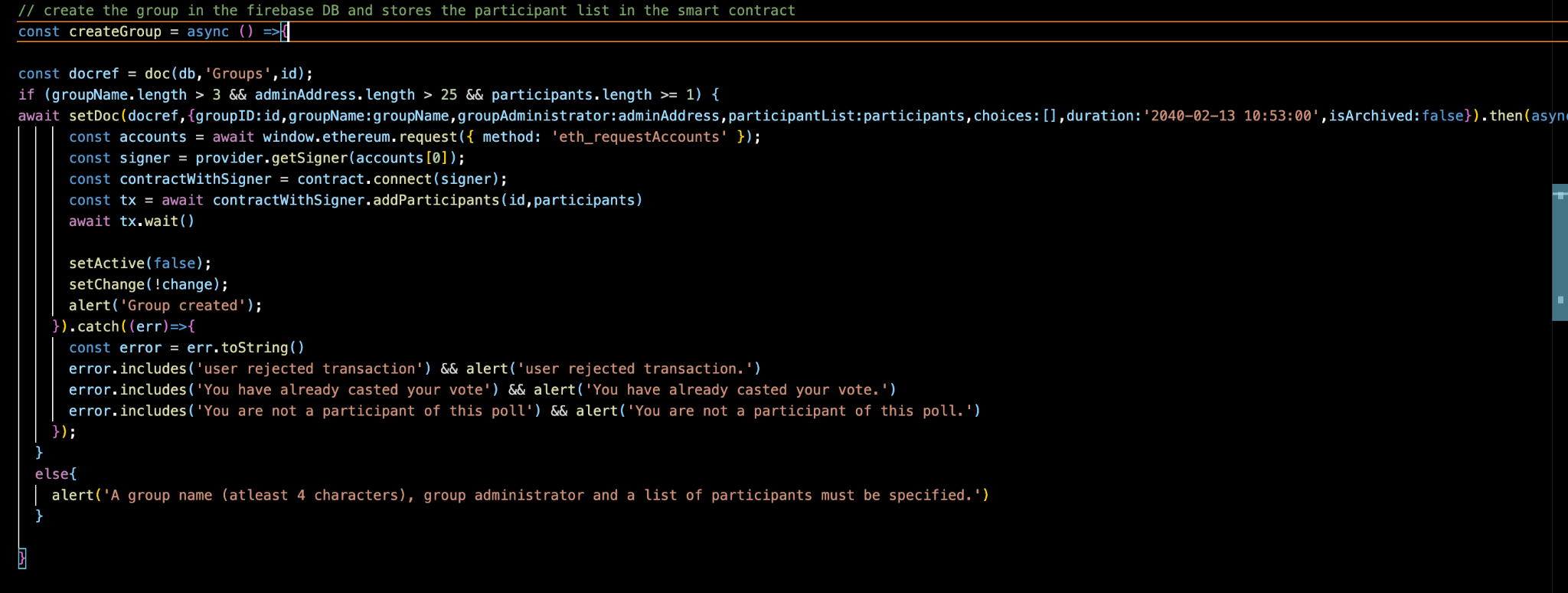


**Figure 20: wallet sign-in code**

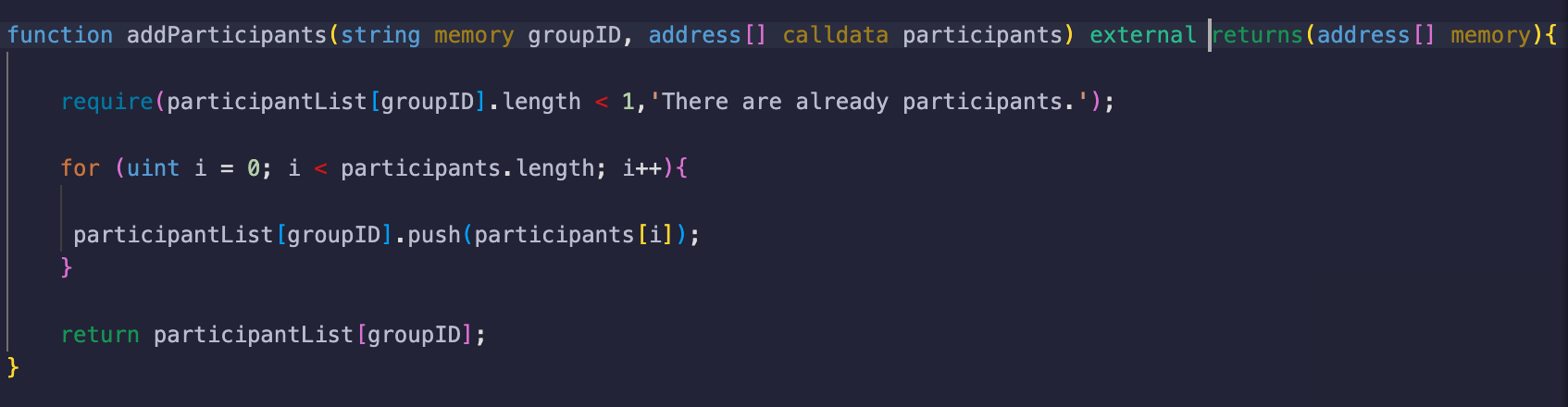
****

**Figure 21 wallet sign-in prompt**

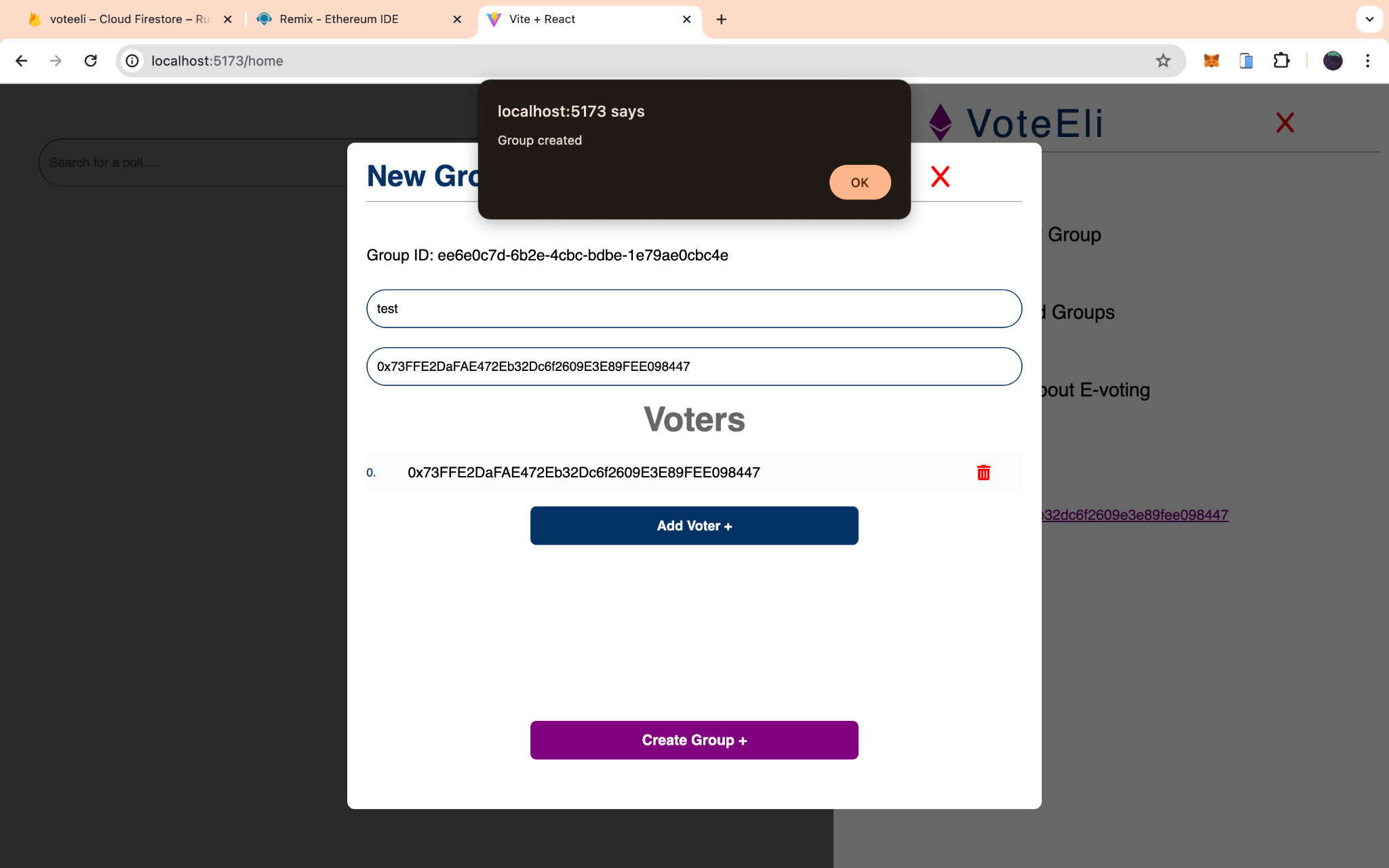
1. Registering participants for a poll.
2. Create a group(an isolated space where administrators can start a poll and users can cast votes for that event under a set duration). Figure 12 displays the form to create a group and registering participants is required and figure 21 shows the code that enables creating a group



**Figure 22 Code to create a group**



**Figure 23 Function being called in the smart contract to create a group**

****

**Figure 24 Group Created successfully**

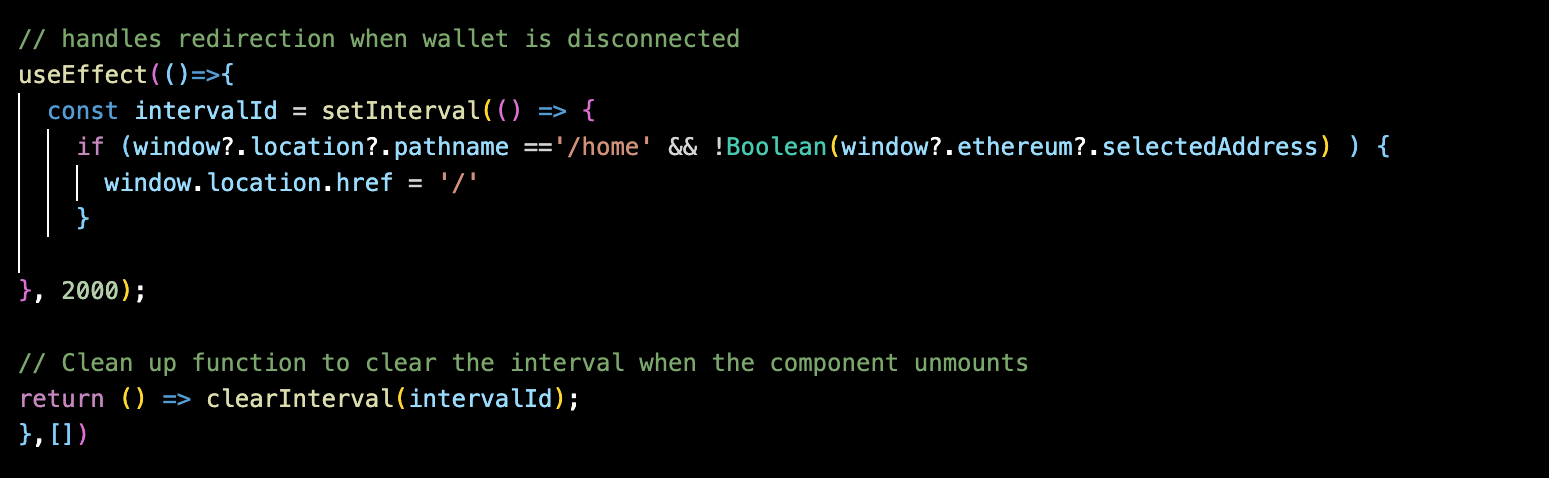
1. Starting a poll.
2. Casting a vote on the blockchain.
3. Automatic Sign out once the wallet is disconnected. Figure 24 displays the code to sign a user out once the wallet has been disconnected.
4. Displaying live results.
5. Complete resistance to double voting, result alteration, and other forms of fraud. The code that enables this feature can be found in Appendix C

## 4.3 Implementation Problems

1. The wallet connect protocol which was initially to be used (as it is the industry standard) had an inconsistent and difficult to understand documentation and all watched tutorials were either outdated (using older versions and syntaxes) or not in english.
2. There isn't a standard mechanism for detecting when a wallet is disconnected from the application.
3. The list of registered participants for a poll was initially stored only on the firebase DB for cost reduction and efficiency, but during implementation it was revealed that this approach creates room for malicious actors to rig a poll by obtaining the Group ID from the network response, obtaining the Smart Contracts Address and ABI from the blockchain and writing a simple program to cast as many votes as they like.
4. The solidity programming language did not support a lot of tasks such as comparison of strings stored in different memory locations and updating arrays in the mapping (hash table) data structures with values from a new array.

## 4.4 Overcoming Implementation Problems

1. Further research of this problem revealed that javascript has an in-built request method in the window.ethereum object for connecting to cryptocurrency wallets. This function was able to help connect the application to a crypto wallet seamlessly.
2. To compensate for the lack of a mechanism to detect if a wallet has been disconnected, it was necessary to create a function that runs every two seconds to check if there is an active connection. If there isn't one, the function signs the user out of the application.This is shown in figure 25
3. To solve this problem a copy of the participant list was stored in the smart contract and a conditional statement was implemented in the function that stores a vote to ensure the address casting the vote is included in the participant list.
4. It was necessary to manually implement these functionalities using custom code, this resulted in not so efficient code. For example, comparing strings stored in different memory locations was done by hashing both strings (this moves those hashed values to one location) then directly comparing their hashes, in the case of overwriting arrays stored in the mapping (hash table) data structure, as seen in figure 23 this was done by using a loop to push each value from the new array to the old one.



**Figure 25 Sign-out function**

The result of the code in figure 25 is a redirect back to the sign-in page seen in figure 10

## 4.5 Testing

Testing is an essential part of software development that involves using the applications functionalities in the intended environment (with inputs where necessary) in order to ensure the desired result is always achieved.

### 4.5.1 Tests Plans (for Unit Testing, Integration Testing, and System Testing)

The plan for testing this blockchain-based voting system will address the system requirements stated in chapter 3 to determine that all goals and functionalities were implemented correctly.

The features to be tested/ test cases include

1. Sign-in using a cryptocurrency wallet.
2. Creating a group and registering users.
3. Hosting multiple polls simultaneously and accurately.
4. Starting a poll.
5. Preventing registered users from double voting and unregistered users from voting at all.
6. Casting a vote.
7. Updating and displaying current results in real time and viewing the accurate statistics of the final result when the poll is over.
8. Blockchain response time.
9. Archiving groups.
10. Logging out.

The environments this application will be tested in are the local environment and production environment(testnet) and the tools used are :

1. Browsers: Safai, Chrome, Firefox
2. OS: Mac OS, IOS
3. Testing software: Chrome DevTools, Sepolia testnet, Metamask Sepoli network.
4. All Devices the application will be tested on: Iphone 13, ipad mini 5, Macbook Air i3

The tests done are

### 4.5.2 Test Suite (for Unit Testing, Integration Testing, and System Testing)

Table 4: Test Suite Performed

| **Req. No.** | **Description** | **Type** |
| --- | --- | --- |
| R-101 | Sign-in using a cryptocurrency wallet. | Function |
| R-102 | Creating a group and registering users | Function |
| R-103 | Starting a poll. | Function |
| R-104 | Casting a vote. | Function |
| R-105 | Updating and displaying current results in real time and viewing the accurate statistics of the final result when the poll is over. | Function |
| R-106 | Archiving groups | Function |
| R-107 | Logging out. | Function |
| R-108 | Hosting multiple polls simultaneously and accurately. | Performance |
| R-110 | Blockchain response time. | Performance |
| R-111 | Preventing registered users from double voting and unregistered users from voting at all. | Security |

### 4.5.3 Test Traceability Matrix (for Unit Testing, Integration Testing, and System Testing)

| **Req. No.** | **Requirement** | **Priority** | **Test Case. No.** | **Test Case Result** |
| --- | --- | --- | --- | --- |
| R-101 | Sign-in using a cryptocurrency wallet. | High | TC1 | Pass |
| R-102 | Creating a group and registering users | High | TC2 | Pass |
| R-103 | Starting a poll. | High | TC3 | Pass |
| R-104 | Casting a vote. | High | TC4 | Pass |
| R-105 | Updating and displaying current results in real time and viewing the accurate statistics of the final result when the poll is over. | High | TC5 | Pass |
| R-106 | Archiving groups. | Low | TC6 | Pass |
| R-107 | Logging out. | Medium | TC7 | Pass |
| R-108 | Hosting multiple polls simultaneously and accurately. | High | TC8 | Pass |
| R-110 | Blockchain response time. | Medium | TC9 | Pass |
| R-111 | Preventing registered users from double voting and unregistered users from voting at all. | High | TC10 | Pass |

### 4.5.4 Test Report Summary (for Unit Testing, Integration Testing, and System Testing)

| **Test Case** | **Description** | **Input** | **Expect Result** | **Actual Result** | **Status** |
| --- | --- | --- | --- | --- | --- |
| Sign-In | The user should be able to sign in to the application using their cryptocurrency wallet | initiation and Authorization of connection to cryptocurrency wallet | The user should be redirected to the home page where the groups they are currently in should be displayed if any | The user was redirected to the home page and the 2023 election group the user is in was displayed | Passed |
| Creating a group | The user should be able to register users and create a group in order to host a poll | The group ID (Auto-generated), Group administrators address, addresses of all participants, the group name, and initiation of the function | The input should be stored in the firebase DB, and the list of participants should be stored in the smart contract | The expected result was achieved | Passed |
| Starting a poll | The Administrator should be able to start a poll by specifying the deadline and the choices to be available in the poll | The list of candidates, the descriptions, the deadline of the poll, and initiation of the poll | The data should be stored in the firebase DB and the poll should start immediately.And if a regular user tries to start the poll, they should receive an error message instead | The expected result was achieved | Passed |
| Cast a vote | Only eligible participants should be able to cast a | Selecting a candidate and initiating the function | The request should be sent to the smart contract and it should verify that the user was registered and has not voted yet. if so it should register the vote and update the live results shown to the users, else return an error message | The expected result was achieved | Passed |
| Blockchain response time | The blockchain should be able to respond to requests in within 10 seconds on average unless the network is congested | Deployment of the smart contract on the sepolia testnet and use of a script to call the functions on the smart contract 100 times | when the mean response time is computed it should be less than 10 seconds | The mean response time is 6.38 seconds | Passed |
| hosting several groups at the same time | The application should allow several different users to be able to create groups for different events and host polls at the same time in a non conflicting manner | Use of this application three (3) different devices to create groups and start polls | The votes/result of each poll should be stored accurately and displayed only in the group that they are meant for | The expected result was achieved | Passed |
| Viewing final results | Registered participants should be able to view the rankings, statistics and summary of final results | Click on a group after the poll has ended | The rankings, aggregate votes, and relevant statistics should be properly represented | The expected result was achieved | Passed |
| Archiving | The administrator (only them) should be able to archive a group once the poll has ended. | Initiate the archive function | The group should be moved from the home page to the archived list and an un-archive button that successfully un-archives the group should be displayed | The expected result was achieved | Passed |
| Logging out | The user should be redirected to the sign in page if their wallet is disconnected | Disconnection of the wallet | The application should redirect the user back to the login page | The expected result was achieved | Passed |

### 4.5.5 Error Reports and Corrections

No errors were detected during the testing phase

## 4.6 Use Guide

The steps taken to use this system can be broken down to 3 steps.

1. Connect your cryptocurrency wallet, after doing that the user will be redirected to the home page.
2. At the home page, if the user is looking to cast a vote on a poll and they are registered, the group should appear in their list of groups, then they can click the desired group, select a candidate and cast their vote. Then the live results will be displayed.
3. At the home page, if the user wishes to create a group to host a poll they can do so by clicking the top right **menu icon,** then clicking on the **create a group button,** then they are required to fill in the form and start the poll by specifying the choices and deadline of the poll, then it will begin.

A more detailed and diagrammatic description can be seen in figure 7.

## 4.7 Summary

This chapter outlined the core features of the application, the issues faced implementing the application and how they were resolved. Then further outlines the tests on the application to ensure the requirements were met and works as expected.

# CHAPTER 5: DISCUSSION, CONCLUSION, AND RECOMMENDATIONS

## 5.1 Overview

In this chapter, the achievements earned while undertaking this project as well as the challenges faced during the project, some recommendations, and future enhancements for this system will all be discussed.

## 5.2 Objective Assessment

Judging by the aims, objectives, and requirements of this project stated in chapter 1 and 3, it is accurate to say that all goals were successfully achieved in this project with minimal challenges and seamless integration of all components.

## 5.3 Limitations and Challenges

1. Communication with the blockchain is often slow.
2. Costs tend to significantly increase in times where the network is congested, although the Ethereum 2.0 update promises to solve this issue.
3. The use of a function that runs every two (2) seconds to check if a wallet connection still exists may decrease performance.

## 5.4 Future Enhancements

1. Addition of an interactive user guide to the UI.
2. Addition of a customer care option.
3. Improvement of the applications accessibility for individuals using screen readers.
4. Creation of a mobile application.
5. Updates to the smart contract code and redeployment when the Ethereum 2.0 update is released. This is needed to ensure the code constructs are up-to standard.

## 5.5 Recommendations

1. Careful consideration and selection of an option before casting a vote on the system, as votes cannot be updated.
2. It is advised to either make use of a browser extension wallet or access this application through the built-in browser of a cryptocurrency wallet for seamless usage.

## 5.6 Summary

This voting system is an excellent implementation of a completely tamper-proof blockchain-based voting system which is accessible from any geographical location, user friendly, and navigable.

# 

# REFERENCES

TheCable. (2023). The opportunities, risks, and challenges of the electronic voting system <https://www.thecable.ng/the-opportunities-risks-and-challenges-of-the-electronic-voting-system/>

Geeks For Geeks. (2023). Introduction to blockchain technology. <https://www.geeksforgeeks.org/blockchain-technology-introduction/?ref=lbp>

Abuidris, Y.O.,Kumar, R. (2019). A Survey of Blockchain Based on E-voting Systems. <https://www.researchgate.net/publication/340081625_A_Survey_of_Blockchain_Based_on_E-voting_Systems>

Diamond, S. (2020). Voting no to paper ballots. <https://www.eballot.com/blog/voting-no-to-paper-ballots>

Pinkerton, J. (2023). The history of bitcoin.

<https://money.usnews.com/investing/articles/the-history-of-bitcoin>

Frankenfield,J. (2018). Initial Coin Offering (ICO). <https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp>

Gehmlich, B. (2022). Crypto bear market and the lessons to take into 2022

<https://gigster.com/blog/the-2018-crypto-bear-market-and-the-lessons-to-take-into-2022/>

National bureau of economic research. (2022). El-Salvador's experiment with bitcoin as legal tender. <https://www.nber.org/digest/202207/el-salvadors-experiment-bitcoin-legal-tender>

Seth,S. (2023). Implementing monetary and fiscal policy.

<https://www.investopedia.com/terms/c/central-bank-digital-currency-cbdc.asp#:~:text=Key%20Takeaways,implementing%20monetary%20and%20fiscal%20policy.>

Vidal-Tomas, D. (2022). The new crypto niche, NFTs, play-to-earn, metaverse tokens. <https://www.researchgate.net/publication/359980878_The_new_crypto_niche_NFTs_play-to-earn_and_metaverse_tokens>

Sharma, R. (2023). What is decentralized finance (DEFI) and how does it work? <https://www.investopedia.com/decentralized-finance-defi-5113835#:~:text=Decentralized%20finance%2C%20or%20DeFi%2C%20uses,transact%20financially%20with%20each%20other.>

Chen, G. (2023). A historical recap of bull and bear markets. <https://www.cryptospend.com.au/blog/a-historical-recap-of-past-crypto-bull-and-bear-markets>

Polyas. (n.d.). Online voting with polyas. <https://www.polyas.com/>

Agora team. (n.d.). Bringing our voting systems into the 21st century,<https://static1.squarespace.com/static/5b0be2f4e2ccd12e7e8a9be9/t/5f37eed8cedac41642edb534/1597501378925/Agora_Whitepaper.pdf>

Uniswap team. ( n.d.). The governance process. <https://uniswap.org/governance>

Ashleigh. (2020). Community governance process. <https://gov.uniswap.org/t/community-governance-process/7732>

Horizon State Team,(n.d.), Technology for 21st century elections, <https://horizonstate.com/horizon-state-solutions/horizon-state-elections/>

Xu,X.,Weber, I. (2019). Case Study: SecureVote: Taking a Dapp from MVP to Production.<https://www.researchgate.net/publication/331527636_Case_Study_SecureVote_Taking_a_Dapp_from_MVP_to_Production>

Boucher, N., Saowakon,P., Swanson, K.,& Govedic, L. (2019). Cryptovote. <https://courses.csail.mit.edu/6.857/2019/project/14-Boucher-Saowakon-Swanson-Govedic.pdf>

Andrew Kenney, (2019). Denver will allow smartphone voting for

thousands of people (but probably not you).

<https://www.solutionsjournalism.org/stories/denver-will-allow-smartphone-voting-for-thousands-of-people-but-probably-not-you>

Aboknin L., Shir, A. (2021). Piloting a blockchain-based voting system: A case study in Estonia. Government Information Quarterly. <https://downloads.hindawi.com/journals/mpe/2024/5591147.pdf>

Guardtime, (2020). Estonia's i-Voting system <https://guardtime.com/>

Geeks for geeks, (2023), Software development methodologies <https://www.geeksforgeeks.org/>

Agora team, (2018), Bringing our voting systems into the 21st century <https://www.agora.vote/technology>

Follow My Vote Team, ( n.d.), Online voting software:Blockchain the end to end process, cryptographically secure voting

<https://followmyvote.com/blockchain-voting-the-end-to-end-process/>

Gwarzocha,[Bowlsby](https://participedia.net/user/110904),S. F., [Gakhal,](https://participedia.net/user/417734) J. (2020). The Democracy Earth Blockchain for Liquid Democracy the 21st Century,

<https://participedia.net/case/4675>

[Vo-Cao-Thuy](https://www.semanticscholar.org/author/Linh-Vo-Cao-Thuy/1412613639),L., [Cao-Minh](https://www.semanticscholar.org/author/Khoi-Cao-Minh/1412610151),K., [Dang-Le-Bao](https://www.semanticscholar.org/author/Chuong-Dang-Le-Bao/1412605418),C., & [Nguyen](https://www.semanticscholar.org/author/Tuan-A.-Nguyen/153387597),T. (2019). Votereum: An Ethereum-Based E-Voting System. <https://www.semanticscholar.org/paper/Votereum%3A-An-Ethereum-Based-E-Voting-System-Vo-Cao-Thuy-Cao-Minh/a3985d63d3d7f342f08a72c2ddfb3975630cbf2f>

Kulechov, S. (2023). Aave crypto liquidity token protocol <https://www.gemini.com/cryptopedia/aave-crypto-liquidity-token-protocol>

MakerDAO team, (n.d.). The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System, <https://makerdao.com/da/whitepaper/>

The Graph Foundation. (2022). Introducing Graph AdvocatesDAO - A Decentralized Body Overseeing Community Grants & the Advocates Program. <https://thegraph.com/blog/advocates-dao/>

Decentriland team,(n.d.).Decentriland DAO. <https://decentraland.org/dao/>

Blockchains inc. ( n.d.). The standard DAO framework. <https://github.com/blockchainsllc/DAO>

Antonopoulos,A. (2018). Mastering Ethereum. <https://github.com/ethereumbook/ethereumbook>

Yakovenko,A. (2023). Solana: A new era of blockchain technology. <https://solana.com/solana-whitepaper.pdf>

Investopedia team. (2024).What is litecoin(LTC)?How it works,History,Trends and Future. <https://www.investopedia.com/terms/l/litecoin.asp>

Votem. (2018). An end-to-end verifiable digital voting protocol using distributed ledger technology (blockchain). <https://votem.com/no-more-contested-elections/>

Fauzi, C.,Wisnu, R., Surano, R. & Delina, J. (2019). The study of blockchain technology in the election system. [watermark.silverchair.com/040010\_1\_online.pdf](http://watermark.silverchair.com/040010_1_online.pdf)

BSC News. (2024). Earning While Playing – How DeFi Is Transforming Gaming into an Income Source. <https://www.bsc.news/post/earning-while-playing---how-defi-is-transforming-gaming-into-an-income-source>

Copeland, T. (2023). A brief history of ethereum. <https://www.theblock.co/learn/245716/a-brief-history-of-ethereum>

# APPENDICES

**Appendix A - Project Document**

All documents related to this project can be found in the repository <https://github.com/ChukwuEmeka-16/BazeUniProject2024.git>

**Appendix B - Interview**

Date: 13th january 2024

Interviewer: Eli Asikaro Walter

Location: Mazfallah Shopping Complex

The following proceedings summarise the insights and findings from four interviews conducted on the 16th of january 2024 with various stakeholders regarding e-voting systems. The interviews aimed to understand their perspectives on the characteristics of an ideal voting system.

Interviewee 1

Name: Daniel Olaitan

Position: Businessman

Key insights

1. Emphasised the importance of transparency and accountability in e-voting systems.
2. Advocated for robust security measures to prevent result tampering.
3. Described the ideal voting system as a geographically accessible and user friendly means of casting votes.

Interviewee 2

Name: Rhoda Asikaro

Position: Artist

Key insights

1. Highlighted the need for a user-friendly interface that does not require a significant learning curve.
2. Described the ideal voting system as one that is geographically accessible, inclusive of disabled people and is easy to verify the results.

Interviewee 3

Name: Yusra Adeyeri

Position: Cyber security Specialist

Key insights

1. Highlighted the need for measures to prevent double voting, invalid votes and other forms of ballot fraud.
2. Described an ideal voting system as one where users can study as votes are processed and stored, verify the results and ensure that results can never be altered.

Interviewee 4

Name: Moses Kaduna

Position: Fashion Designer

Key insights:

1. Highlighted the need for a transparent system that functions very quickly and is easy to use.
2. Described the ideal voting system as one that is secure, fast, easy to use and accessible by anyone anywhere in the world.

Synthesis of findings

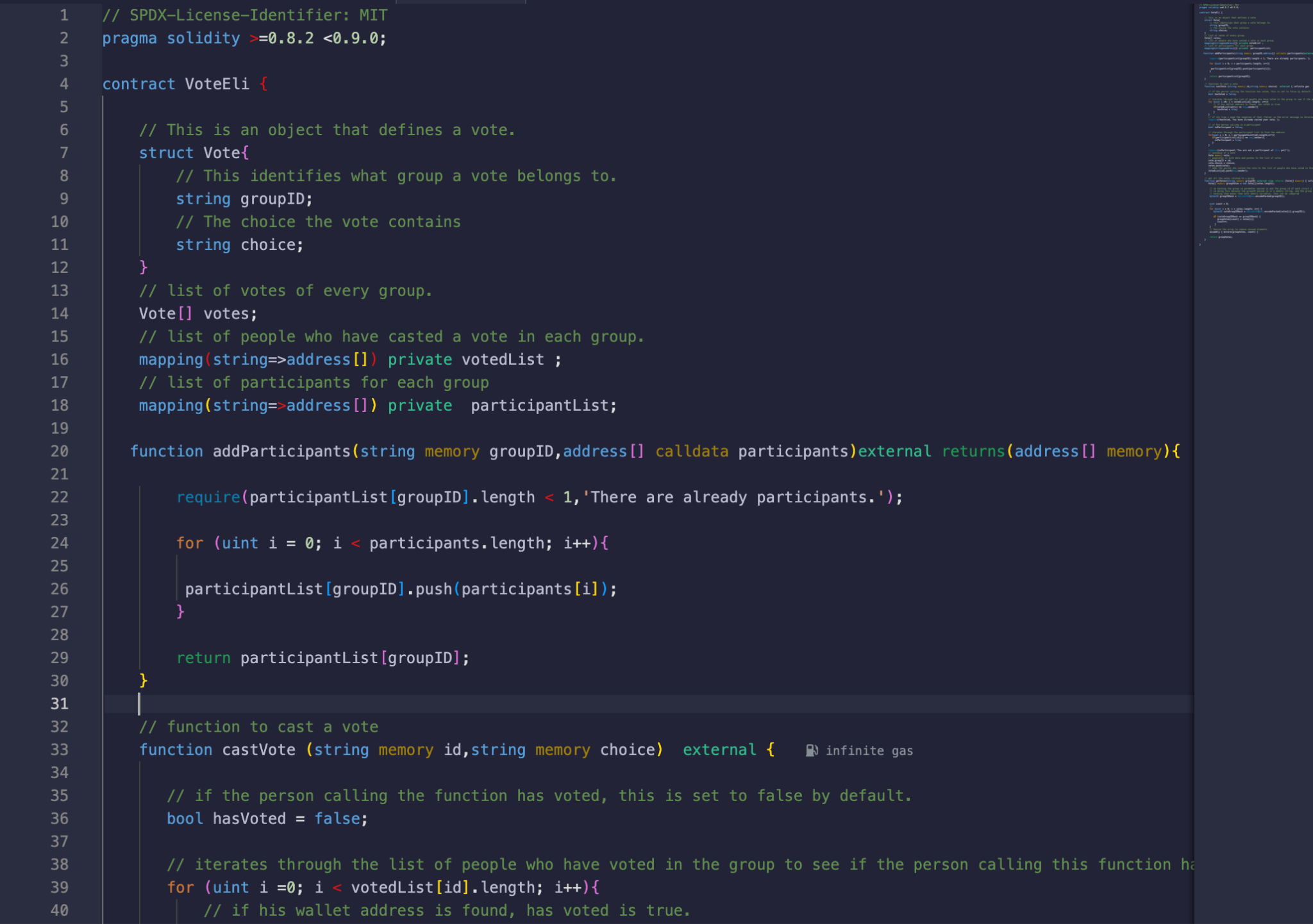
1. Common themes identified across interviews include the importance of immutability,security, transparency, accessibility and user friendliness.
2. Concerns about the risk of cyber attacks, system glitches, and lack of transparency in existing voting systems.
3. Agreement on the ideal voting system as one that is tamperproof, fast, inclusive of everyone and auditable

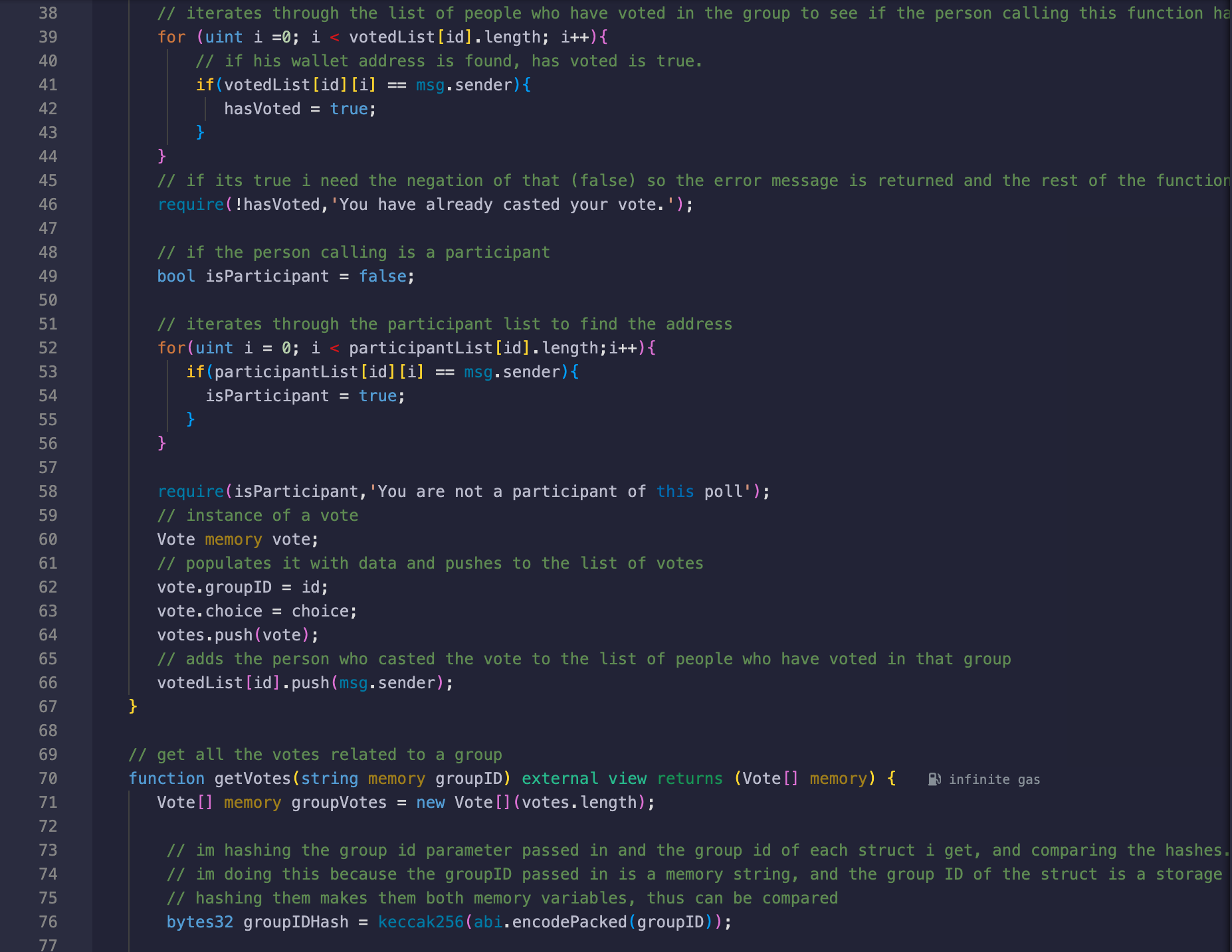
Conclusion

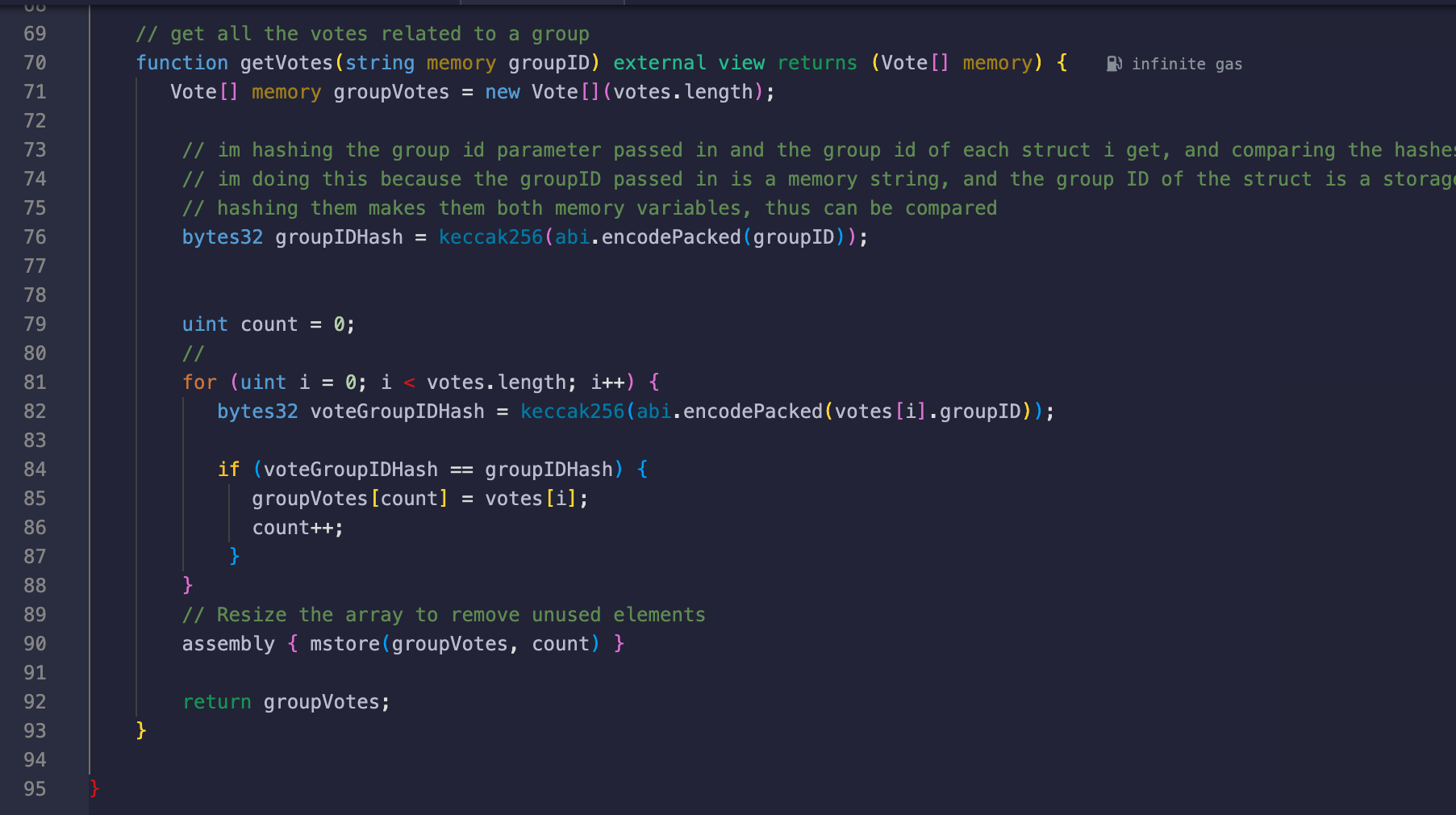
In light of complaints that had previously been received, the interviews revealed areas that required enhancement and offered insightful information about the qualities of reliable electronic voting systems. The combined results emphasise the significance of security, usability, and transparency when developing the optimal voting system, highlighting the necessity of a well-rounded strategy that takes stakeholder concerns into account while preserving the integrity of the democratic process.

End of Interview Proceedings.

**Appendix C – Source Codes**







**Appendix D User Guide/Manual**

How to create a group and start a poll.

1. Sign in using a cryptocurrency wallet
2. Activate the sidebar menu and click on ‘create a new group’
3. A form will be shown, enter the name of the event, the administrators address, and the list of addresses who will be permitted to cast votes in the poll. Then click on ‘Create group’
4. A group will be created.
5. To start the poll, click on the newly created group.
6. Activate the form to start a poll by clicking on the ‘Start Poll’.
7. A Form will be shown, enter the choices that the participants will vote on, and the duration the poll should be held for. Finally, click on the start button for the poll to commence.

How to cast a vote

1. Sign in using a cryptocurrency wallet.
2. CHoose the desired group.
3. At the middle there is a selector that contains all available choices, choose the desired one.
4. Cast a vote by licking on the ‘Cast vote’ button
5. Once the vote is cast, the standings will be updated

How to log out

1. Navigate to the wallet used to sign in and disconnect manually from there.

How to archive a group

1. Only the administrator may archive a group, this can be done only when the poll duration expires.

To learn more about the application, activate the sidebar and click the ‘Learn more about e-voting’ button.

To verify the authenticity of the group, request for your administrator to share their wallet address, then compare it with the one found at the bottom of the group page

To run this application locally

1. Use a suitable IDE like VScode
2. Run the ‘npm i’ command to install all requirements
3. This is a vite application so run ‘npm run dev’ to activate the application
4. Ensure to have either a browser extension wallet or paste your local url (e.g http://localhost:5050) in a cryptocurrency wallet.