SECURE-VOTE: A VOTING DAPP ON THE METIS STARDUST BLOCKCHAIN

PROJECT REPORT

SUBMITTED BY

HARI KRISHNAN S R

TKM20MCA-2019

TO

THE APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE

OF

MASTER OF COMPUTER APPLICATIONS

THANGAL KUNJU MUSALIAR COLLEGE OF ENGINEERING

KERALA

JULY 2022

DECLARATION

I undersigned hereby declare that the project report **"SECURE-VOTE: A VOTING DAPP ON THE METIS STARDUST BLOCKCHAIN",** submitted for partial fulfilment of the requirements for the award of degree of Master of Computer Applications of the APJ Abdul Kalam Technological University, Kerala is a bonafide work done by me under supervision of **Prof. Alshaina S**. This submission represents my ideas in my own words and where ideas or words of others have been included, I have adequately and accurately cited and referenced the original sources. I also declare that I have adhered to ethics of academic honesty and integrity and have not misrepresented or fabricated any data or idea or fact or source in the submission. I understand that any violation of the above will be a cause for disciplinary action by the institute and/or the University and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been obtained. This report has not been previously formed the basis for the award of any degree, diploma or similar title of any other University.

KOLLAM HARI KRISHNAN S R

18/07/2022

THANGAL KUNJU MUSALIAR COLLEGE OF ENGINEERING

DEPARTMENT OF COMPUTER APPLICATIONS

CERTIFICATE

This is to certify that, this report entitled "**SECURE-VOTE: A VOTING DAPP ON THE METIS STARDUST BLOCKCHAIN**" is a bonafide record of the work submitted by **HARI KRISHNAN S R (TKM20MCA-2019),** under our guidance and supervision, in partial fulfilment of the requirements for the award of the Degree of **Master of Computer Applications** in **APJ Abdul Kalam Technological University.** This report in any form has not been submitted to any other University or Institute for any purpose.

Internal Supervisor Head of the Department External Examiner

ACKNOWLEDGEMENT

A successful project is a fruitful culmination of efforts by many people, some directly involved and some others indirectly, by providing support and encouragement. Firstly, I would like to thank almighty for giving me the wisdom and grace for making my project a memorable one. I thank him for steering me to the shore of fulfilment under his protective wings.

I express my sincere gratitude to **Dr. T A Shahul Hameed**, Principal of T.K.M College of Engineering for giving me an opportunity to present my project. I would like to thank **Dr. Fousia M Shamsudeen**, Assistant Professor and Head of the Department, MCA, TKMCE, for her constant support and encouragement throughout the project work.

With a profound sense of gratitude, I would like to express my heartfelt thanks to my guide **Prof. Alshaina S**, Department of Computer Applications, TKMCE, for her expert guidance, cooperation, and immense encouragement. I also extend my thanks to the entire faculty and staff of the Department of Computer Applications, TKMCE, who has encouraged me throughout this work.

I also express my thanks to my loving parents, brother and friends, for their support and encouragement in the successful completion of this project work.

HARI KRISHNAN S R

ABSTRACT

Large segments of society today no longer trust the traditional method of voting because they think it may be easily manipulated. Cryptographic techniques can be used to address several problems, assure the security of voting systems, and extend their widespread usage. Modern civilization is seeing a rise in the practice of electronic voting. It has a significant chance of lowering administrative expenses and raising participation rates. Moreover, the installation of polling stations and printing of ballot paper can be minimized. This voting technology allows voters to vote from the comfort of their own homes. A simple polling app is a great use case for blockchain technology. The voting process requires special attention to privacy, especially in the government area, but it will be public, auditable, tamper-proof, and unfiltered, and it can also provide a global voting process. A block chain polling system also makes it possible to build response incentive mechanisms for specific use cases. The creation of a voting system built on top of the Metis Stardust Test net blockchain is proposed in this work. Users can log in to vote in a particular poll, and each poll is confirmed using a transaction that can be viewed on the Stardust blockchain explorer.

CONTENTS

LIST OF FIGURES

Chapter 1

Introduction

According to the social environment today, a fair and transparent election is required for today's society. Democracy’s existence is based on the process of voting where voters elect their representatives. Vote counting is not transparent under the current electoral system. Voting fraud is a concern in many forms, including phoney voters, fraud in the voting booths, etc. People's confidence in the choices made by majority vote increased because of the traditional or paper-based polling approach. It has aided in making the democratic procedure and election system valuable for choosing representatives and governments that are more democratic. Since the commencement of the voting system, the secret voting model has been utilized to increase trust in democratic institutions. It is crucial to prevent a decline in voting confidence. According to recent research, the conventional voting process was not entirely sanitary, raising concerns about issues like justice, equality, and how well the desire of the people was recognized and represented in the form of governance.

Globally, engineers have developed innovative voting procedures that guarantee electoral integrity while providing some protection against corruption. New computerized voting procedures were made possible by technology, and while they are crucial, they have caused serious problems for democracy. Compared to manual polling, electronic voting enhances election dependability. It has improved the process' efficiency and integrity compared to the traditional voting approach. Electronic voting is frequently used in many choices due to its adaptability, ease of use, and low cost compared to conventional elections. Most activities are now centralised, managed, quantified, and monitored by an electronic voting system and licenced by the central authority, which presents a challenge for a transparent voting process and the electronic voting methods have a single controller that oversees the whole voting process. In some cases, due of the election commission's dishonesty, this process causes incorrect selections, which are hard to correct using current techniques. Modern electronic voting methods may be utilized to go around the central authority via the decentralized network. Therefore, the need for the creation of a secure, decentralized, fraud-free voting system arose. Blockchain-based decentralized voting systems can fix most of the problems with traditional voting systems. Block chain’s decentralized ledger technology confers several benefits. The main advantage is that anyone wishing to utilize cryptocurrencies on a blockchain only must create a random keypair and use it to manage a wallet connected to a public key. This is how anonymity is defined in a blockchain setting. The blockchain method ensures that the only person with access to the keypair can manage funds in the wallet.

When voting traditionally, an eligible voter would visit a polling place and use an EVM (Electronic Voting Machine) to cast their vote. However, because the vote cannot be traced back and since it is circuitry and can be tampered with, it is impossible to know whether the vote was cast for the person it was meant for or if it was diverted to the account of another candidate. However, if voting is implemented using blockchain, everything is stored as a transaction, giving the voter a receipt for his/her vote (in the form of a transaction ID) that he/she can use to confirm that their vote was securely counted. Imagine that the procedure has

been digitized using a voting system (website/app) and that all sensitive information is kept on a single administrative server or workstation. There is no way to know whether a hacker installs malware, carries out click jacking assaults to steal or negate the vote, or just attacks the central server, but if someone tries to hack it or snoop on it, he or she can affect the candidate's total vote. To prevent this, the system is protected by a unique attribute known as immutability if it is coupled with blockchain.

Blockchain is a decentralized computing and information-sharing platform that enables numerous authority domains to work together and cooperate in certain decision-making processes even though they do not trust one another. It uses an add and append method. Blockchain-based electronic voting will only function when the online voting system is completely independent of any one entity, not even the government.

Let’s take the case of SQL, PHP, or any other conventional database architecture. Votes can be added, changed, or removed. However, on a blockchain, data can only be added, and it cannot be changed or removed. The term "immutable ledger" comes from the fact that once anything is entered, it remains there permanently and cannot be changed. Peer-to-peer network systems are used by blockchain. A blockchain is a series of blocks that use distributed ledger technology to store all the user's data. But creating a blockchain system alone is insufficient.

Blockchain technology is in its infancy when it comes to voting. Thus, academics are working to capitalize on features like openness, confidentiality, and nonrepudiation that are crucial for voting applications. It also needs to be decentralized, meaning that other nodes shouldn't have to wait for the victim node to recover if one server crashes or something else occurs on a specific node. Ralph Merkle assessed the idea of block interconnectivity using the Merkle tree. A block of data's cryptographic hash is used to identify each node. Thus, a cryptographic hash of the labels of child nodes is used to label a non-leaf node. Any modification in the blockchain may be easily recognized because every block is related to every other block. The blockchain technology is not without flaws. A blockchain is difficult to scale, in contrast to other distributed solutions: Network speed is not improved by adding more nodes since each node must conduct every transaction individually and this procedure is not shared across the nodes.

1.1 Problem Statement

This project aims to eradicate the problem of traditional voting by introducing voter and vote anonymity and become failure proof as well as tamper proof by the introduction of blockchain.

1.2 Objective

The main goal of this project is to design and implement an efficient, secure, user friendly and interactive web-based voting system.

Specific Objectives:

- To develop a system that will implement ballot privacy.

- To develop a system that will implement coercion resistance.
- To develop a system that will implement individual verifiability.
- To reduce the overall cost of an election.

Chapter 2

Literature Survey

The full analysis of the literature that is relevant to a certain issue is known as a literature review. When doing a literature review, research questions are first developed, after which one attempts to provide a solution by looking up and analysing pertinent material. The ability to re-analyse the study's findings can lead to the development of fresh ideas, which is one benefit of literature reviews. A literature review summarises and explains the whole and most recent body of information about a subject that may be found in academic books and journal articles. One sort of literature review is completed as a stand-alone assignment for a course, and the other type is written as part of the introduction to or preparation for a bigger work, sometimes a thesis or research report. Both types of literature reviews may be assigned to students at the university level. Depending on the type of review you are writing, your topic, point of view, and type of hypothesis or thesis argument will all be influenced. Reading published literature reviews or the introductory sections of theses and dissertations in your own field of study, analysing the organisation of their arguments, and making note of how they approach the topics are some ways to appreciate the distinctions between these two types.

2.1 Purpose of the Literature Survey

i. It makes research on a certain issue accessible to readers by picking high-quality papers or studies that are relevant, significant, important, and valid and summarising them into a single report.
ii. It is an ideal starting place for scholars who are just starting out in a new field. by requiring them to describe, assess, and compare original research in that field.
iii. It assures that researchers do not replicate previously completed work.
iv. It might point the way forward for future study or suggest areas to focus on.
v. It emphasises the most important results.
vi. It finds discrepancies, gaps, and contradictions in the literature.
vii. It gives a constructive appraisal of other scholars' methodology and approaches.

2.2 Related Works

Ralf Kuesters et al. [1] designed an e-voting system. This voting system introduced the concept of tally-hiding. This e-voting system gave more importance to vote secrecy and ensured receipt-freeness. However, the developed system was unsupervised and there was no voter anonymity. There was also a high possibility of coercion.

A.C.Santha Sheela et al.[2] developed a safe Electronic Voting system software that uses the fingerprint as a method of authentication. The fingerprints are stored in databases and during the time of the election, they are validated. Using Zigbee technology, the election data

is instantly relayed to the closest data centres. Although it adds a layer of protection, this has a significant disadvantage in that there are no reliable third parties.

Kashif Mehboob Khan et al. [3] proposed an e-voting system that gave high priority to transparency. The proposed system was also able to achieve end-to-end verifiability through the use of cryptographic techniques. They also proposed the implementation of the e-voting system using a multichain platform. However, by using multichain, a smart contract cannot be implemented and if the user wants to track their tokens across IBC-enabled blockchain, they need to solve harder problems.

Voatz2 is a proprietary voting system based on mobile phones that uses a combination of permissioned blockchain, biometrics, and hardware-supported keystores to deliver end-to-end encrypted, voter verifiable voting. Michael A. Specter et al. [4] did a security examination of Voatz2. Specter et al. [4] pointed out that information regarding Voatz's implementation were never published and uncovered various dangers that caused a Washington county to stop using it, even though Voatz was used to conduct multiple genuine elections in the US.

A supervised electronic voting method was put up by Jens-Matthias Bohli et al. [5] and offers consumers a receipt that links a random number to the candidate of their choice. The user of this system can check to see if their vote has been counted during the tallying phase. It is not open source, though, and it leaves the connection between voter and vote in place.

Chapter 3

Methodology

3.1 Proposed System

The proposed system develops a simple decentralized polling webapp. It is developed on top of the Metis Stardust blockchain network. It is developed using Next JS, and Vercel is used for deployment. It is equipped with both the main net and test net of the Metis blockchain network. However, due to testing purposes and cost constraints, Secure-Vote is constrained to the Stardust test net as of now. As a result, the smart contract is deployed only on the test net. Blockchain solutions have been given fresh life by smart contracts. The smart contract of Secure-Vote is deployed on the test net with the help of Remix Ethereum IDE.

The main method for login to Secure-Vote is with the help of MetaMask. MetaMask offers both a browser extension and a mobile app. Everything a user needs to manage their digital assets is provided for them, including a key vault, secure login, a token wallet, and a token exchange is provided by MetaMask. Additionally, it gives users access to blockchain-based apps in the easiest yet most secure manner possible.

Users can log in with their MetaMask wallet and can create polls by transferring Metis coins to pay the gas price and can set time limits for the polls they create within the webapp. The creator of the poll can decide whether the voting process is free or whether the voters must pay Metis coins as a fee. METIS is an Ethereum token that is used as the internal unit of exchange for staking and making payments in the Metis crypto ecosystem. Metis coins are available on both Metis Andromeda and Metis Stardust. Metis Andromeda is the main net of the Metis blockchain network while Metis Stardust is the test net of Metis blockchain network. The test net is for testing purposes and the Metis coins in the test net doesn’t hold any commercial value.

Once the poll is created, an id is generated, and others can search for the poll by entering the id in the webapp and can vote for that specific poll by transferring Metis coins depending on whether the voting for the poll is free or paid. As an added layer of security, only the poll creator can see the live results of the poll that they created. Secure-Vote ensures that no one can cast a duplicate vote and if they try to do so, their transaction will be cancelled. Each transaction done on the transaction can be traced on the Metis Stardust Explorer website, thus ensuring the traceability of the votes.

3.2 System Architecture

The system mainly consists of five pages for the user to interact with. Through these pages, the user can login to the webapp and create or find a poll and can cast his/her vote.

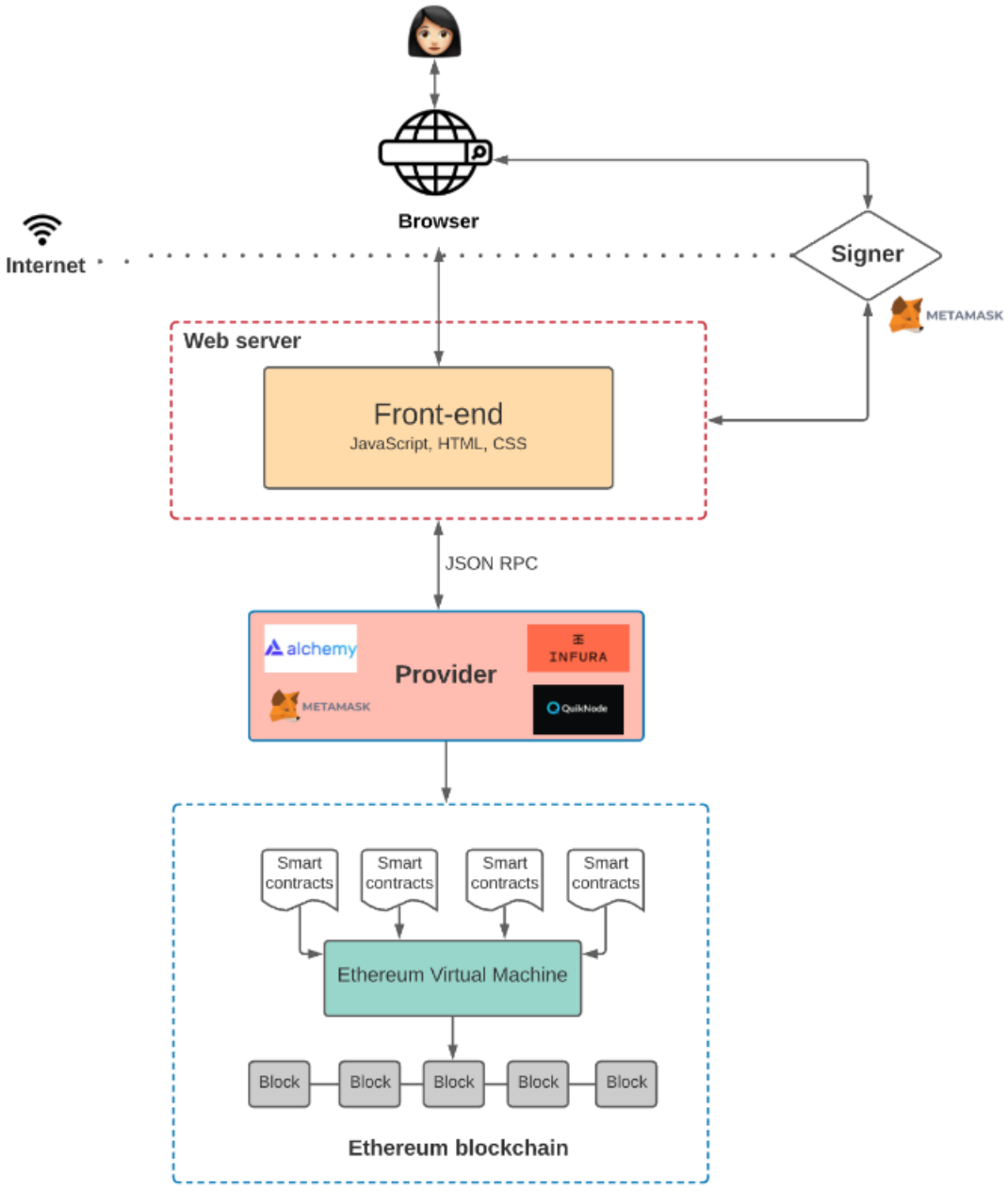

Fig 1.a System Architecture

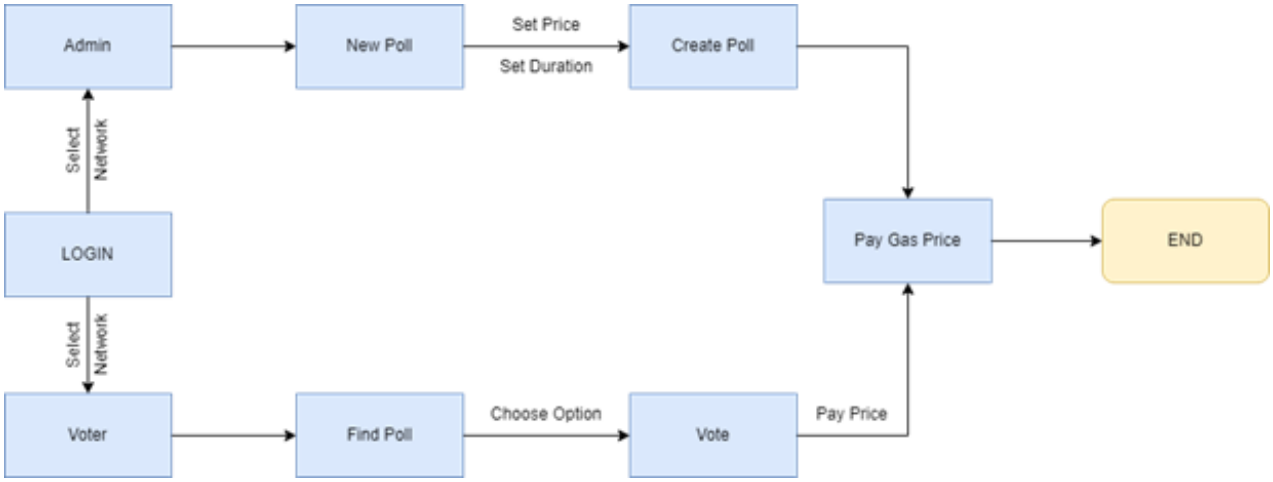

Fig 1.b System Architecture Flowchart

3.2.1 Login

When a user opens Secure-Vote for the first time, they are greeted with this page. A brief overview of Secure-Vote is provided on the login screen, and users are also given some basic instructions on how to use the app. Additionally, they are offered the choice between the Metis blockchain networks, Andromeda or Stardust. Following that, they may choose Connect Wallet to sign in using their MetaMask wallet. They are provided with a successful message after properly authenticating.

3.2.2 Dashboard

The dashboard is where users begin when they log in to Secure-Vote. There, a number of options are offered to them. They may view a list of the app's available options on the left side. The application also displays the user's poll information, including the total number of polls they have generated so far. Additionally, the dashboard itself contains a list of the active polls they have established. From the dashboard, they can create or fill out a poll. The users also has access to all the polls that they and other users have generated in the app under the recent polls tab.

3.2.3 Create Poll

There are two steps to creating a poll in Secure-Vote. The user must fill in the essential information, including the poll's name, description, and length, in the first stage. Additionally, they can decide if the polling is free or paid. Furthermore, the top of the page has a progress bar that displays the user's progress as they enter the necessary data. After providing the necessary information, they can proceed to step two. The choices that must be included in the poll may be included in the second phase, and after they do that, the poll can be properly created.

3.2.4 Fill Poll

According to the order of creation, Secure-Vote assigns a distinct poll id to each poll that is established. The users are provided a text box where they may enter the poll id of the poll, they want to participate in. After adding the poll id, users may select "Get Poll" to have the app immediately fetch the poll that corresponds to the poll id they submitted, allowing them to cast their vote.

3.2.5 Poll History

All the polls that have been generated inside Secure-Vote to date are included in the poll history. Inside the poll history, users may view the details of every poll that has been generated. The poll history displays data about the poll's title, description, duration in real time, poll id, and poll's creator.

3.3 Technologies Used

3.3.1 Next.js

A Node.js-based open-source web development framework called Next.js enables React-based web apps to produce static web pages and perform server-side rendering. The React documentation recommends using Next.js as one of the "Recommended Toolchains" while "Building a server-rendered webpage with Node.js." Standard React apps can only display their content in client-side browsers, whereas Next.js extends these capabilities to server-side programmes. Next.js is a proprietary product of Vercel, who also oversees and manages the open-source development of the programme.

Next.js is a react framework that includes features including server-side rendering and the creation of static web pages. React is a JavaScript library that is frequently used to build web applications that are JavaScript-rendered in the client's browser. The strategy has a number of disadvantages, according to developers, including the inability to serve users who do not have access to or have disabled JavaScript, potential security problems, noticeably slower page loading times, and a detrimental effect on the site's overall search engine optimization. By allowing some or all of the webpage to be displayed on the server before it is communicated to the client, frameworks like Next.js circumvent these problems. One of the most well-liked React frameworks is Next.js. It is one of many "toolchains" that are advised when launching a new app; all of them provide a layer of abstraction to aid with fundamental tasks. Node.js is necessary for Next.js, which can be installed via the Node Package Manager.

3.3.2 Node Package Manager

The package manager for the JavaScript programming language is called npm (node Package Manager), and it is supported by npm, Inc. The default package manager for the Node.js JavaScript runtime environment is npm. It consists of the npm registry, an online repository of free and paid-for private packages, and a command line client that is sometimes referred to as npm. The client accesses the registry, and the npm website allows users to browse and search for the available packages. The registry and package management are under the control of npm, Inc.

npm is a recommended feature included in the Node.js installation. A command-line client that talks with a distant registry is called npm. Users are now able to download and share JavaScript modules from the registry. The registry's packages are in CommonJS format and include a JSON metadata file. About 1.3 million packages are available in the main npm registry. Packages found in the register may be of low quality, insecure, or hazardous due to the lack of a verification process for submissions. Instead, npm relies on user complaints to get rid of subpar, risky, or hazardous packages. Developers may assess the quality of packages using information provided by npm, such as the quantity of downloads and the number of dependents.

The audit tool was added in npm version 6 to assist developers in identifying and fixing security issues in installed packages. The security vulnerabilities were sourced from Node Security Platform (NSP) reports and have been incorporated with npm following npm's purchase of NSP.

Both JavaScript tools that are delivered worldwide and packages that are local dependencies of a particular project may be handled using npm. npm can install all of a project's dependencies via the package.json file in a single command when used as a dependency management for a local project. The semantic versioning approach enables developers to automatically update their packages without making unneeded breaking changes by enabling each dependency in the package.json file to designate a range of permissible versions. npm also offers version-bumping tools that let developers tag their packages with a particular version. npm also includes the package-lock.json file, which holds the entry of the precise version used by the project, after examining semantic versioning in package.json.

3.3.3 Solidity

For the purpose of building smart contracts on several blockchain systems, most notably Ethereum, Solidity, which is an object-oriented programming language, is used. It was created by numerous previous contributors to the Ethereum core as well as Christian Reitwiessner and Alex Beregszaszi. Solidity programmes are executed via the Ethereum Virtual Machine.

Gavin Wood first suggested Solidity in August 2014; the Solidity team, under the direction of Christian Reitwiessner, later developed the language.

On Ethereum and other private blockchains, including the business focused Hyperledger Fabric blockchain, Solidity is the main language. A proof-of-concept utilising Solidity running on Hyperledger Fabric was released by SWIFT.

Programming in a statically typed language called Solidity allows for the creation of smart contracts that work with the Ethereum Virtual Machine (EVM).

For experienced web developers, Solidity's syntax is similar to that of ECMAScript; however, unlike ECMAScript, it supports static typing and variable return types. There are certain significant ways in which Solidity differs from other EVM-targeting languages like Serpent and Mutan. It enables arbitrary hierarchical mappings and structs, as well as sophisticated member variables for contracts. Inheritance, including multiple inheritance using C3 linearization, is supported by solidity contracts. The application binary interface (ABI) introduced by Solidity allows for numerous type-safe functions to be performed within a single contract (this was also later supported by Serpent). The "Natural Language Specification" documentation system for describing user-centric explanations of the effects of method-calls is another feature of the Solidity proposal.

In contrast to programmes written in conventional programming languages, which may be debugged, Solidity contracts do not allow for error correction or transaction reversal. Solidity adheres to the principle that "Code is Law," hence every smart contract that is put into use must have perfect coding.

There have been a few hacking incidents, including the 2016 DAO attack noted above in which US$60 million was taken, and the 2021 hack that resulted in a fork in the Ethereum system.

The biggest bitcoin exchange in the US, Coinbase, has unveiled a new technology called Solidify in order to avoid technical flaws and mishaps. This device is an AI auditing system that finds and categorises hazards associated with smart contracts.

3.3.4 MetaMask

A software cryptocurrency wallet called MetaMask is used to communicate with the Ethereum network. Users can utilise a browser extension or mobile app to access their Ethereum wallet, which can then be used to connect with decentralised applications. ConsenSys Software Inc., a blockchain software firm that specialises in Ethereum-based infrastructure and tools, is the company behind MetaMask.

With MetaMask, users may send and receive Ethereum-based coins and tokens, broadcast transactions, save and manage account keys, and securely connect to decentralised applications using a suitable web browser or the built-in browser of the mobile app. By defining interactions between Metamask and Smart Contracts using a JavaScript plugin like Web3js or Ether, developers connect Metamask to their decentralised apps.

In order to get the cheapest exchange rate, the Metamask application aggregates many decentralised exchanges (DEXs) to provide an integrated solution for trading Ethereum tokens. The service cost for this feature, known as MetaMask Swaps, is equal to 0.875 percent of the

transaction value. According to Bloomberg, MetaMask's browser plugin had more than 21 million active users as of November 2021.

In 2016, ConsenSys developed MetaMask. Only desktop browser extensions for Firefox and Google Chrome were supported by MetaMask before to 2019. The prevalence of MetaMask among bitcoin users and the fact that it lacked an official mobile app for a number of years made it difficult for Google to control the behaviour of malicious software masquerading as MetaMask on its Chrome Web Store and Google Play platforms. In one case, Google Play mistakenly deleted the official beta version of MetaMask before reversing the action on January 1, 2020, a week later. In order to conduct closed beta testing, MetaMask started releasing mobile app versions in 2019. In September 2020, they made its initial public release for iOS and Android. A built-in DEX aggregation service called MetaMask Swaps was added to the desktop in October 2020. A built-in DEX aggregation service called MetaMask Swaps was implemented to the desktop extension in October 2020. In March 2021, the product became accessible via mobile devices.

3.3.5 Smart Contract

A smart contract is a computer program or transaction log designed to automatically execute, control, or document legally relevant events or actions based on a contract or the terms of the contract. The goal of smart contracts is to reduce the need for trusted intermediaries, the cost of arbitration and enforcement, the loss of fraud, and the reduction of malicious accidental exceptions.

Nick Szabo, who created the phrase, initially advocated smart contracts in the early 1990s, defining them as "a collection of promises, stated in digital form, including protocols within which the parties fulfil on these promises." The phrase was first used to describe items in the rights management service layer of the Stanford Infobus, a component of the Stanford Digital Library Project, in 1998.

Similar to how money is transferred on a blockchain, deploying a smart contract on one involves submitting a transaction from a wallet for the network. The transaction has both the built-in smart contract code and a special recipient address. When that transaction is contained in a block that is uploaded to the blockchain, the smart contract's code will then be performed to produce the smart contract's initial state. Byzantine fault-tolerant algorithms are used to offer decentralised defence against attempts to tamper with the smart contract. Once published, a smart contract cannot be changed. Any form of calculation may be executed and stored by smart contracts on a blockchain. End users communicate with smart contracts through transactions. Other smart contracts may be activated by these smart contract actions. State changes and the movement of money from one smart contract or account to another might result from these interactions.

The most popular blockchain for implementing smart contracts is Ethereum. Smart contracts on Ethereum are frequently written in the Turing-complete programming language Solidity and converted into low-level bytecode in order to be executed by the Ethereum Virtual Machine.

Because of the stopping issue and other security concerns, languages like Vyper purposely avoid achieving turing-completeness. Additional smart contract programming languages that do not satisfy the Turing-completeness criteria include Simplicity, Scilla, Ivy, and Bitcoin Script. Regular expression analysis revealed that only 35.3% of the 53,757 Ethereum smart contracts had recursions and loops, which are relevant to the halting problem.

3.3.6 Remix IDE

Remix Plugin Engine, Remix Libraries, and of course Remix IDE are just a few of the sub-projects that it includes.

Web and desktop software called Remix IDE is open source. With a wide variety of plugins and simple GUIs, it encourages a quick development cycle. As a learning and teaching tool for Ethereum, Remix is utilised throughout the full process of creating contracts using the Solidity programming language.

The Remix IDE's in-browser coding is a unique and mostly useful feature. Users may create Solidity contracts directly from a browser with the aid of this open-source programme. For those people who would rather run it locally, there is also a desktop version.

Remix IDE features a number of modules that follow the structure of the majority of popular programming languages. A module for testing, debugging, and deploying smart contracts is among the three most often used ones. Remix also provides a number of libraries to speed up development.

The list of default IDE Modules are:

- File Explorers Module.
- Plugin Manager.
- Settings.
- Solidity Editor.
- Terminal.

The list of typical IDE Modules is:

- Compiler (Solidity).
- Deploy & Run.
- Debugger.
- Solidity Static Analysis.

Remix also has a list of libraries, they are

- Remix Analyzer – It helps you perform static analysis on Solidity smart contracts to check security vulnerabilities and bad development practices.
- Remix ASTWalker – Provides an easy way to read the AST of a smart contract written in Solidity.

- Remix Debug – It gives you all the basic tools to add debugging features for smart contracts.
- Remix Solidity – It's simply a wrapper around the Solidity compiler.
- Remix Lib – It's a commonplace for libraries being used across multiple modules.
- Remix Tests – It enables you to add Solidity unit testing to your continuous integration or tools.
- Remix URL Resolvers – It provides helpers for resolving the content from external URLs.

3.3.7 Testnet

An alternate Bitcoin block chain for testing is called the testnet. Testnet coins are never designed to have any value because they are different from real bitcoins. This enables bitcoin testers and application developers to conduct experiments without risking the disruption of the main bitcoin chain or using actual bitcoins.

The testnet has gone through three generations. Due to the fact that individuals were beginning to exchange testnet coins for actual money, Testnet2 was just the first testnet reset with a different genesis block. The current test network is called Testnet3. A third genesis block, a new rule to prevent the "difficulty was too high, is now too low, and transactions take too long to verify" issue, and blocks with edge-case transactions intended to test implementation compatibility were all included with the 0.7 release. To test the Segregated Witness concept made by Wuille, SegNet was set up on December 21st, 2015.

Compared to the main network, the testnet utilises a different genesis block. The testnet often has a substantially lesser transaction volume than the main block chain. The amount of data stored on disc as of January 2018 was 14 GB, which represented around 6 years' worth of testnet activity. About 12 GB of network traffic, peaking at 2 MB/s, was needed to download this data.

3.3.8 Mainnet

The completed blockchain project's that is available for usage by the general public is called mainnet. A mainnet, however, may be changed anytime projects or open-source organisations decide that the product needs upgrades and/or changes, much like a testnet.

A mainnet is a separate blockchain that operates on its own network using its own protocol and technologies. It is a live blockchain, as opposed to a testnet or projects that are built on top of other well-known networks like Ethereum, where its own coins or tokens are in use. Testnet is used by programmers to diagnose and test any new blockchain functionality. Consequently, the primary distinction between testnets and mainnets is that the former comprises an ongoing blockchain project, whilst the latter requires a fully established blockchain. Before the mainnet stage, a few important actions may be taken. A token sale is one of them, providing money for a product to create and test features. The mainnet stage is often pushed out once this phase has

been effectively deployed. This would indicate that the blockchain is operationally sound. In order to use their own currencies tethered to the Ethereum network, several blockchain firms choose to do so. These coins were ERC-20 tokens, which can only be used on the Ethereum network. The mainnet will be made available when the ICO has ended. Instead of the ERC-20, this is typically represented using a native coin. Mainnet exchange is the procedure' subsequent step. The ERC-20 tokens are exchanged in this for the new currency on the blockchain. The new coins will often be disposed of when the mainnet swap is finished. This is to make sure that just the new coins will be used, not the old ones.

3.3.9 Metis

Metis is an optimistic rollup-based Layer 2 (L2) scaling protocol. With its rollup approach, programmers may store data, execute transactions, and operate apps on a different layer than Ethereum.

Metis mirrors the Optimism Virtual Machine (OVM) that it calls the Metis Virtual Machine (MVM). But unlike its competitors, Metis utilizes multiple sequencers that will be pooled into on-chain units called Decentralized Autonomous Companies (DACs).

Similar to DAOs, DACs also have a number of real-world business functions. As a result, users may use tools for managing payroll, communicating, and doing other tasks like launching a sequencer pool or a new application on the MVM.

To construct and control the partnership and accomplish their business objectives, anyone may build a DAC using Metis. The execution of the partnerships may be supported and managed by Metis in a transparent and effective manner.

The protocol will randomly select a new sequencer for each block from the sequencer DAC to Send Ethereum any state changes. Only sequencers who have staked more METIS than the Dynamic Bond Threshold are qualified to confirm transactions. This functions as a tool to reduce the appeal of malevolent behaviour.

Users can also take part in the sequencer as Rangers to monitor activities. In exchange for $METIS, rangers will sample a variety of blocks and verify the state roots. They will be compensated, much as validators, if they find any differences, but persistently unsuccessful challenges might result in a network ban.

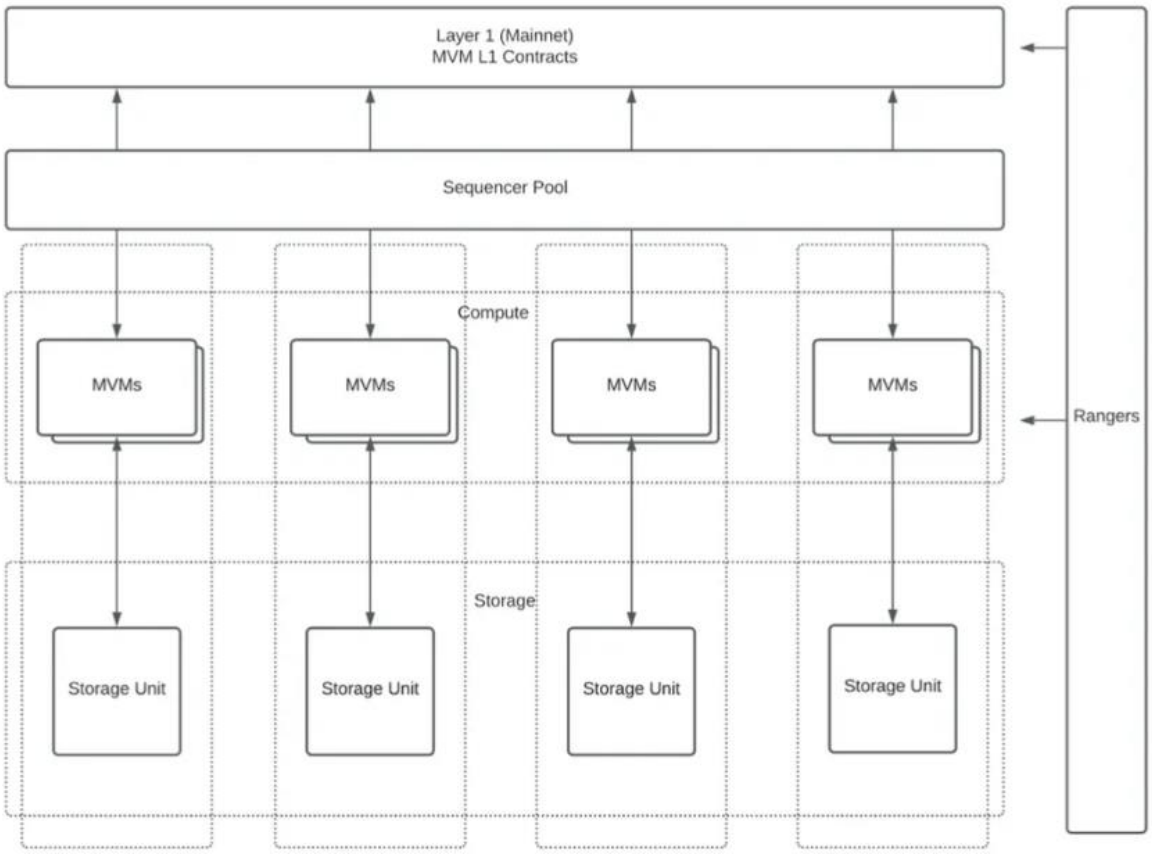

Fig 2. Metis Architecture

Metis aims to make creating dApps and DACs effortless for the everyday blockchain user. The team has optimized Metis to include new features such as:

- Multiple VMs and sequencers
- Framework with templates, APIs, and modules to assist with dApp development
- DACs that can manage their organizations independently
- Separation of computing and storage
- Private native storage layer
- Fast transactions at ~2,000 TPS with low gas fees
- One click deployment with pre-developed templates
- 100% EVM compatible

Metis blockchain network has a mainnet as well a testnet. The mainnet of Metis is known as Metis Andromeda and the testnet is known as Metis Stardust.

3.3.10 Polis - Metis Dashboard

Polis is a platform that allows users to log into any dApps built upon its platform. Users will receive an Ethereum address when creating an account. They can then transfer tokens to other users via their username or Ethereum address. Transaction records across all dApps will be shown on the Polis dashboard.

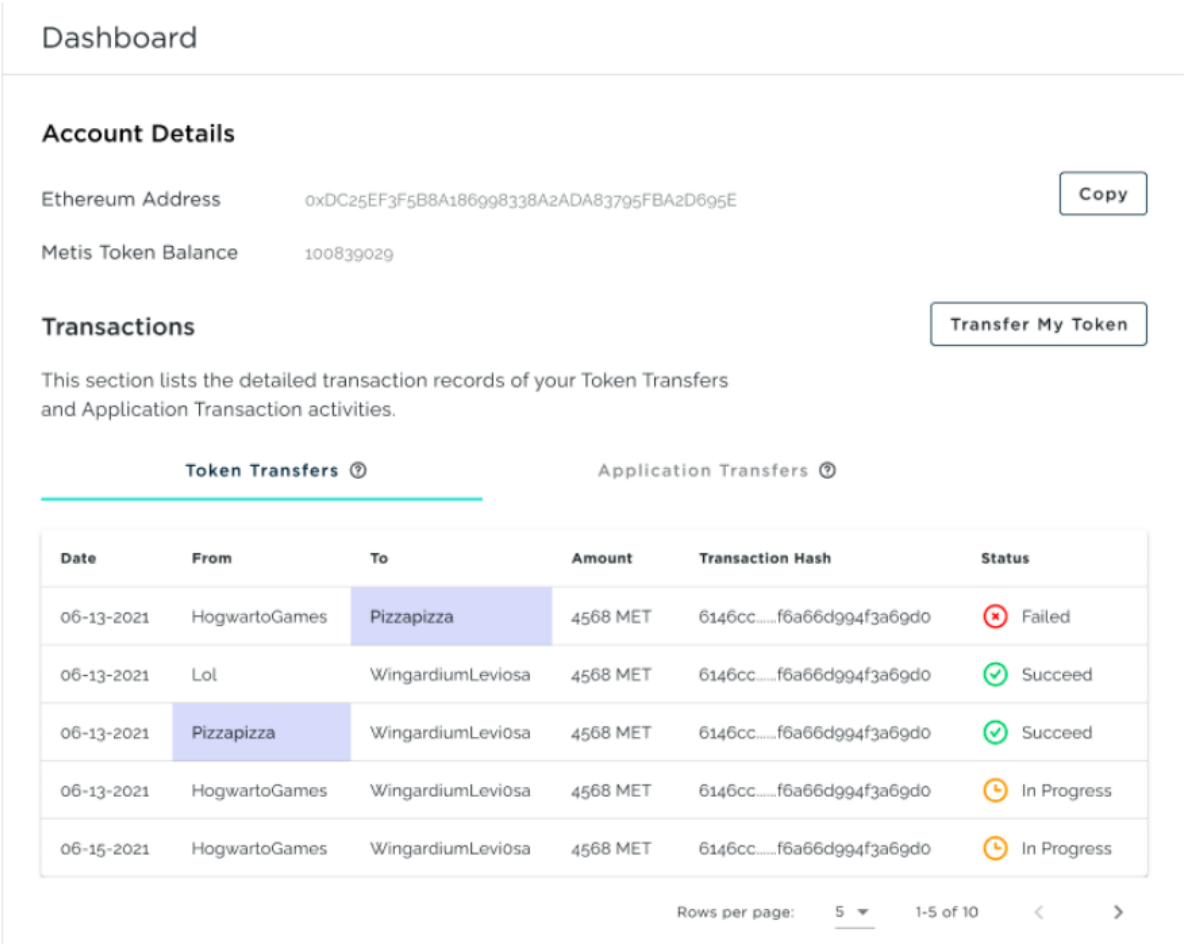

Fig 3. Polis – Metis Dashboard

3.4 Secure-Vote

Secure-Vote mainly consists of three phases- poll creation phase, voting phase and a tallying phase. The tallying phase is done automatically by the system and the rest two phases are user controlled. Two steps are included in the poll creation and voting phase.

3.4.1 Poll Creation phase

This is the initial step of Secure-Vote. The user must first choose the network shown in Secure-Vote, such as Andromeda main net or Stardust test net, then log in using their MetaMask wallet before they may start a poll. They must visit the chainlist.org website before logging in to make sure they have added the Andromeda and Stardust network to their wallet. Following that, customers may choose their preferred wallet address and log in to Secure-Vote. They are greeted with a successful message and directed to the dashboard after properly authenticating.

From there, they can click on the create a poll. They may also select "new poll," which will direct them to the poll creation page. They must fill out the name, description, and length of the poll there. They must also choose whether to charge for or not charge for their poll. The top of the page has a progress bar that displays the user's poll creation progress. Once they fill in all these details, they need to add the options for the poll and on completion of this steps they can click on create and their MetaMask wallet opens asking them to pay a gas price for contract interaction. After paying the gas price, a popup will open saying “Poll Created Successfully!” to acknowledge poll created successfully.

3.4.2 Voting phase

The user must sign in to Secure-Vote to cast a vote. The steps to login to Secure-Vote to cast a vote are the same as those for creating polls. Once they reach the dashboard, they can either click on "fill a poll" or "find a poll," which will redirect them to the "fill a poll" page. There they need to add the poll id of their desired poll and Secure-Vote will automatically retrieve the poll once they click ‘Get Poll’. After this, they need to select their desired option and click on "Vote". This causes their MetaMask wallet to open. If the poll is pay-to-vote, users must pay the fee set by the poll creator in addition to the gas price before they can effectively cast their ballot. Multiple votes from the same address will only count for the first vote; subsequent votes will result in a pop-up box informing the user that the transaction has been cancelled. An identical pop-up box will display, informing the user that their transaction has been cancelled if they attempt to vote in an expired poll.

3.4.3 Tallying phase

The key benefit of Secure-Vote is that only the person who created the poll can know the total number of votes received for each option. An added benefit is that the creator can also see the votes received in real-time. The poll's creator must log into Secure-Vote, just like during poll creation, to view the total number of votes received for each of the options. After logging in, the creator may access their poll on the dashboard's list of active polls. There, the poll's creator can view information about the poll, including its name, description, creation date, options added to the poll, and the remaining time until it expires. In addition to the options themselves, he/she can view the overall number of votes earned by each option, which is encased in brackets.

Chapter 4

Result and Discussion

The contract was successfully created and was deployed on to the Metis Stardust blockchain network. Users can login and logout of the webapp seamlessly using their MetaMask wallet. Since Secure-Vote is deployed with the help of a blockchain network, it is failure and tamper-proof. Transparency and anonymity are not provided by the traditional voting method but can be found in Secure-Vote. It is also superior to traditional voting by introducing voter and vote anonymity. With the introduction of Secure-Vote, voters can vote anonymously. Real-time results of the election are also available and can only be seen by the poll creator. Secure-Vote eradicates the risk of multiple votes by blocking multiple transactions from the same address. Whenever a contract interaction happens, that interaction details can be viewed in the Stardust explorer. The gas price of Metis blockchain at most of the time is very less compared to other blockchain networks like Bitcoin and Ethereum.

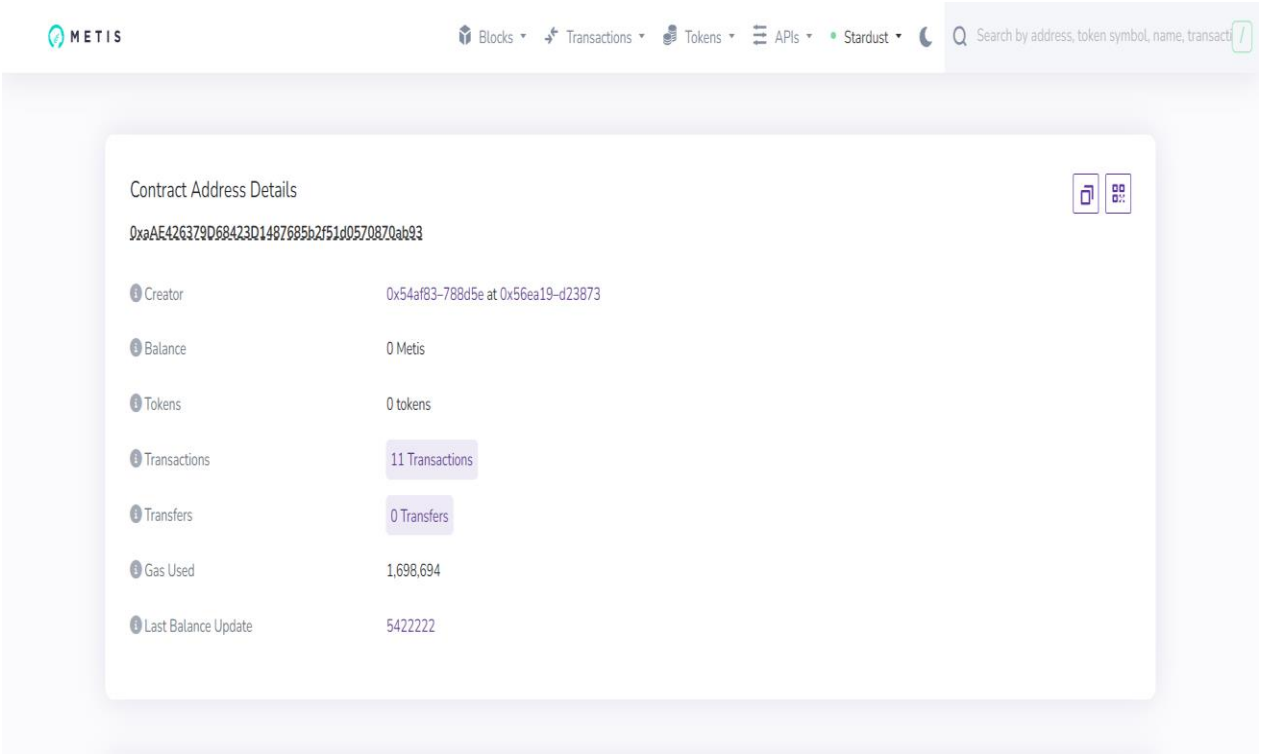

Fig 4. Contract Creation

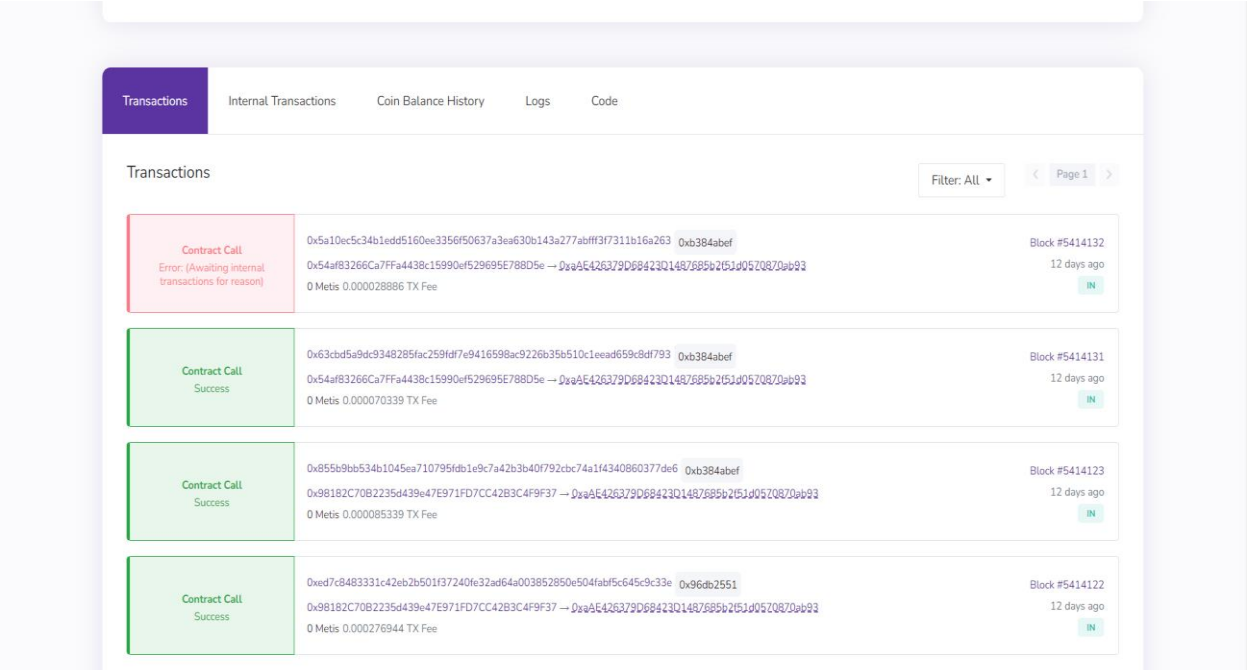

Fig. 5. Contract Calls

Chapter 5

Conclusion

The Crypto-voting system can stand out as a special example in both the technology world and the e-voting business. This system could be able to provide services that are both sufficiently dependable and adaptable. The use of this modern technology can achieve the following goals: a low-cost, reliable, and rapid voting system. Everyone desires an open and honest method of polling, which our blockchain-based polling software unquestionably offers, increasing trust in the electoral process. Additionally, by doing so, the pen-and-paper election will be eliminated, improving vote accuracy.

5.1Future Enhancement

Only voting on the test net is currently supported by the system. In the future, it might be configured to operate on the main network and integrated with other blockchain services. With the use of cloud messaging services, the system may also be connected to OTP services. An emotion recognition module may be added utilising image processing and machine learning methods to prevent coercion. Webcams can be used to detect the voter's facial expressions during the voting process. The voter's session will be paused or halted for a while and he or she will be asked to vote again after some time if the module notices any change in emotions like rage, fear, etc.

Chapter 6

References

[1] Küsters, R.; Liedtke, J.; Müller, J.; Rausch, D.; Vogt, A., “Ordinos: A verifiable tally-hiding E-voting system”, In: 2020 IEEE European Symposium on Security and Privacy (EuroS P), pp. 216–235. 2020.

[2] Sheela, A.C; Franklin, R., “E-Voting System Using Homomorphic Encryption Technique”. Journal of Physics: Conference Series, 2021.

[3] K. Khan; J. Arshad; M. Khan, "Secure Digital Voting System Based on Blockchain Technology", International Journal of Electronic Government Research, vol. 14, no. 1, 2018.

[4] Specter M.A.; Koppel, J.; Weitzner, D., “The ballot is busted before the blockchain: A security analysis of voatz, the first internet voting application used in U.S. federal elections”. In: 29th USENIX Security Symposium (USENIX Security 20). USENIX Association, 2020.

[5] Bohli, J.-M.; Müller-Quade, J.; Röhrich, S., “Bingo voting: Secure and coercion-free voting using a trusted random number generator”. In: International Conference on E-Voting and Identity. Springer, 2007.

[6] Shahzad, B.; Crowcroft, J., “Trustworthy Electronic Voting Using Adjusted Blockchain Technology”. IEEE Access, 7, 2019.

[7] Gao, S.; Zheng, D.; Guo, R.; Jing, C.; Hu, C., “An Anti-Quantum E-Voting Protocol in Blockchain with Audit Function”. IEEE Access, 7, 2019.

[8] Yi, H., “Securing e-voting based on blockchain in P2P network”, EURASIP Journal on Wireless Communications and Networking, 2019.

[9] Racsko, P., “Blockchain and Democracy”, Soc. Econ, 2019.

[10] Wang, B.; Sun, J.; He, Y.; Pang, D.; Lu, N., “Large-scale election based on blockchain”, Procedia Comput. Sci, 2018.

[11] Sagar Shah; Qaish Kanchanwala; Huaiqian MI., “Blockchain Voting System”, IEJRD, 2016.

[12] Rawat, D.B.; Chaudhary, V.; Doku, R., “Blockchain technology: Emerging applications and use cases for secure and trustworthy smart systems”, J. Cybersecur. Priv., 2021.

[13] A. Michael Froomkin, “Anonymity and Its Enmities”, 1995 J. ONLINE L. art. 4, par, 1995.

[14] Pawlak, M.; Poniszewska- Marańda, A., “Implementation of Auditable Blockchain Voting System with Hyperledger Fabric”, In International Conference on Computational Science; Springer: Berlin/Heidelberg, Germany, 2021.

[15] Jalal, I.; Shukur, Z.; Bakar, K.A.A., “A Study on Public Blockchain Consensus Algorithms: A Systematic Literature Review”, Preprints, 2020.

[16] “Blockchain Wikipedia” https://en.wikipedia.org/wiki/Blockchain

[17] “Peer to Peer Network” https://www.computerworld.com/article/2588287/networking/networking-peer-to-peer-network.html

[18] Imperial, M., “The Democracy to Come? An Enquiry into the Vision of Blockchain-Powered E-Voting Start-Ups”., Front. Blockchain, 2021.

[19] Hakak, S.; Khan, W.Z.; Gilkar, G.A.; Imran, M.; Guizani, N., “Securing smart cities through blockchain technology: Architecture, requirements, and challenges”, IEEE Netw., 2020.

[20] Szabo, N., “Formalizing and securing relationships on public networks”, First Monday, 1997.

[21] Zheng, Z.; Xie, S.; Dai, H.-N.; Chen, W.; Chen, X.; Weng, J.; Imran, M., “An overview on smart contracts: Challenges, advances and platforms”, Future Gener. Comput. Syst, 2020.

[22] McCorry, P.; Shahandashti, S.F.; Hao, F., “A smart contract for boardroom voting with maximum voter privacy”, IACR Cryptology ePrint Archive, 2017.

[23] Mohanta, B.K.; Jena, D.; Panda, S.S.; Sobhanayak, S., “Blockchain technology: A survey on applications and security privacy challenges”., Internet of Things, Vol.8.,2019.

Appendix

Screenshots

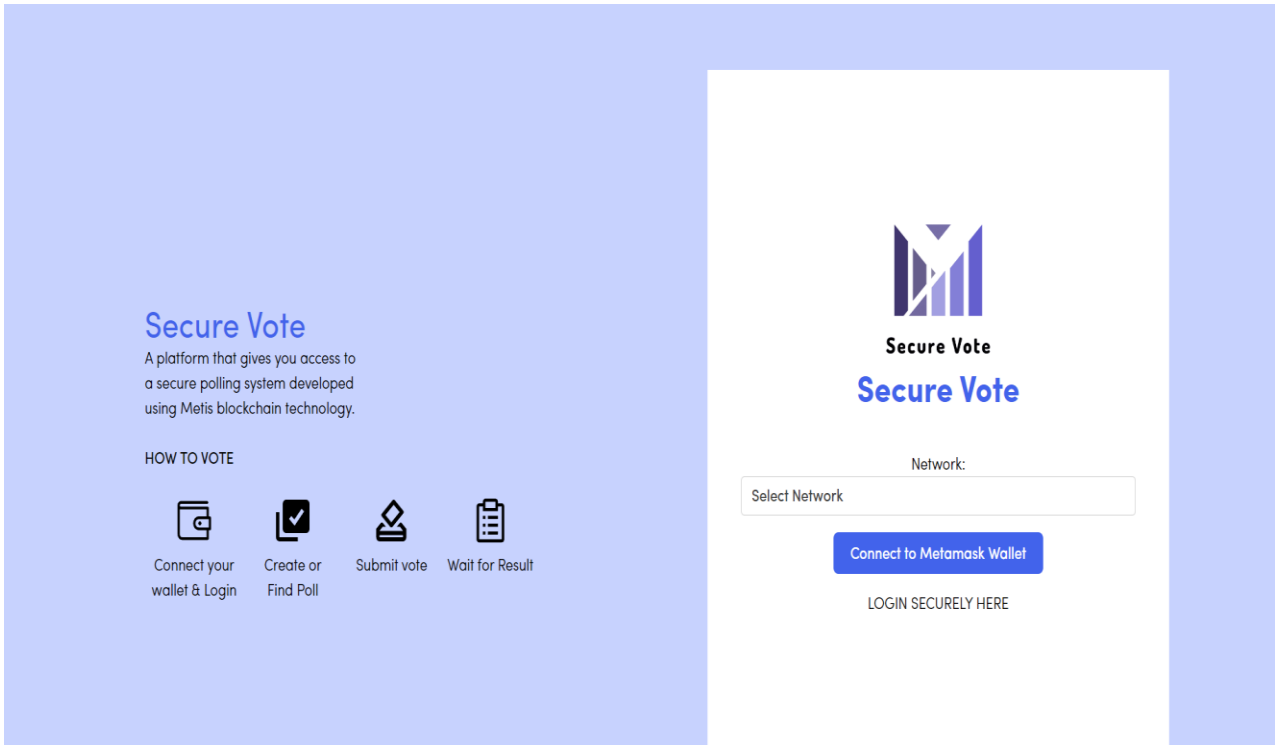

Fig A.1 Login Page

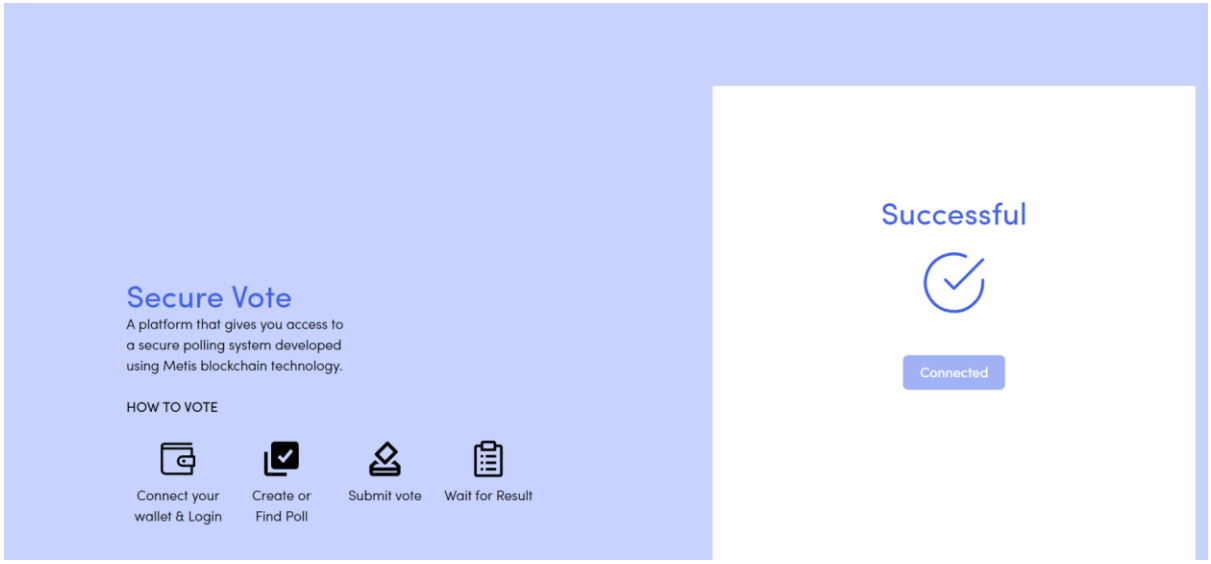

Fig A.2 Successful Authentication

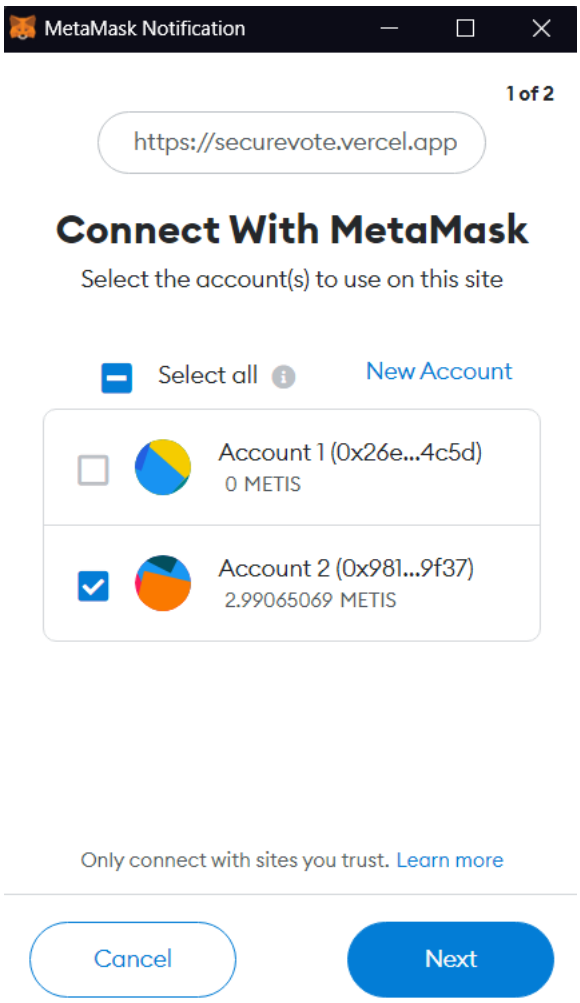

Fig A.3 Account Selection

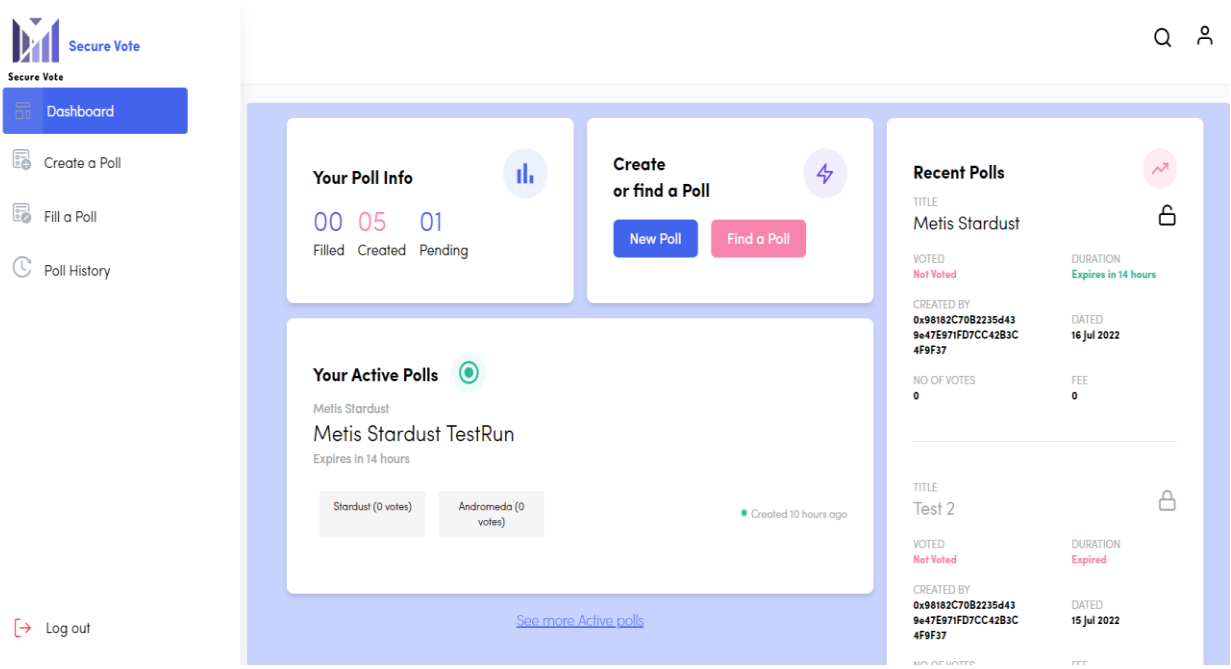

Fig A.4 Dashboard

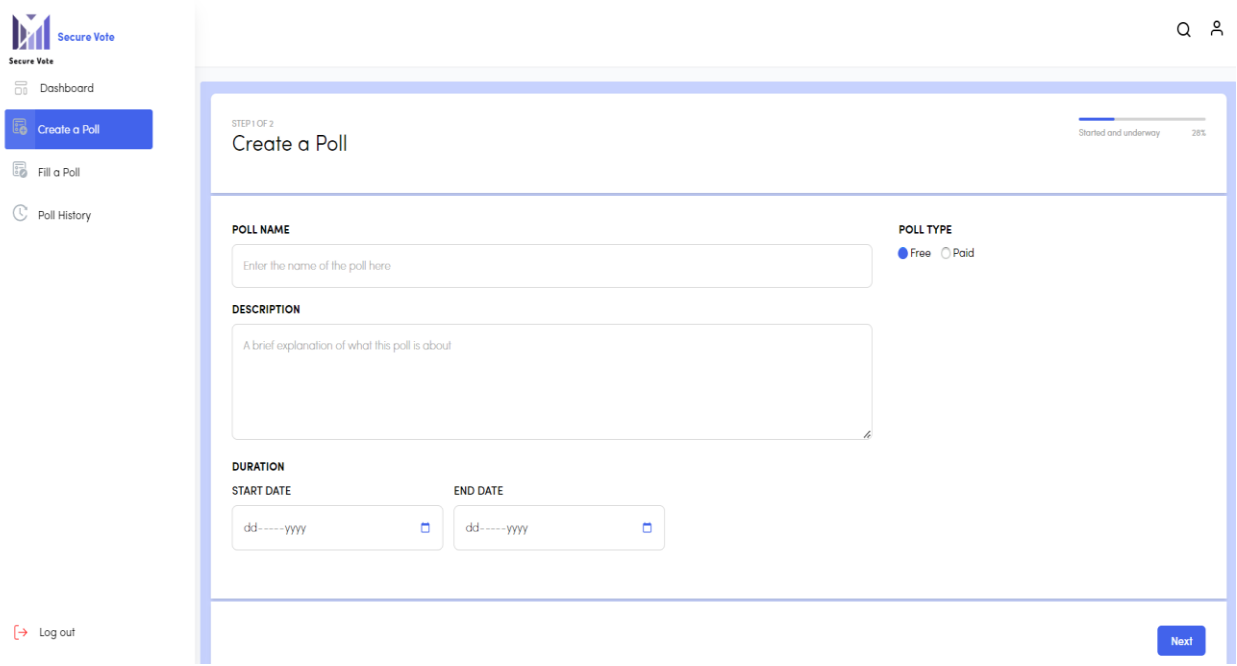

Fig A.5 Create Poll

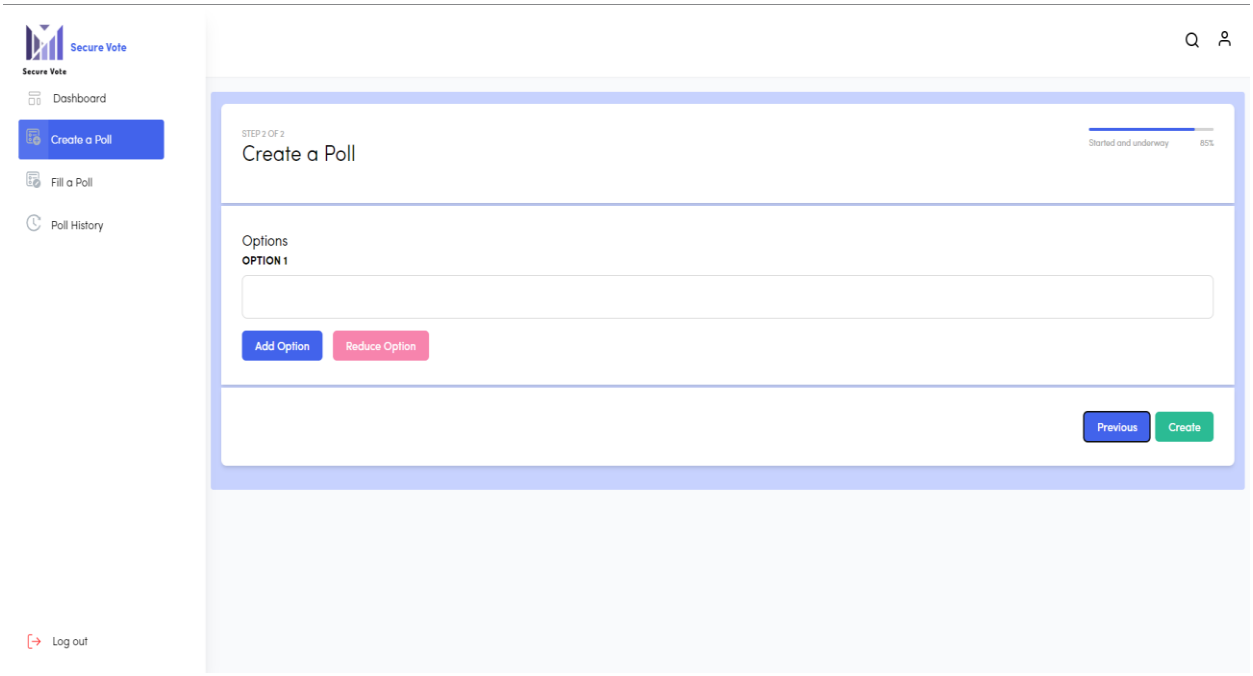

Fig A.6 Candidate Addition

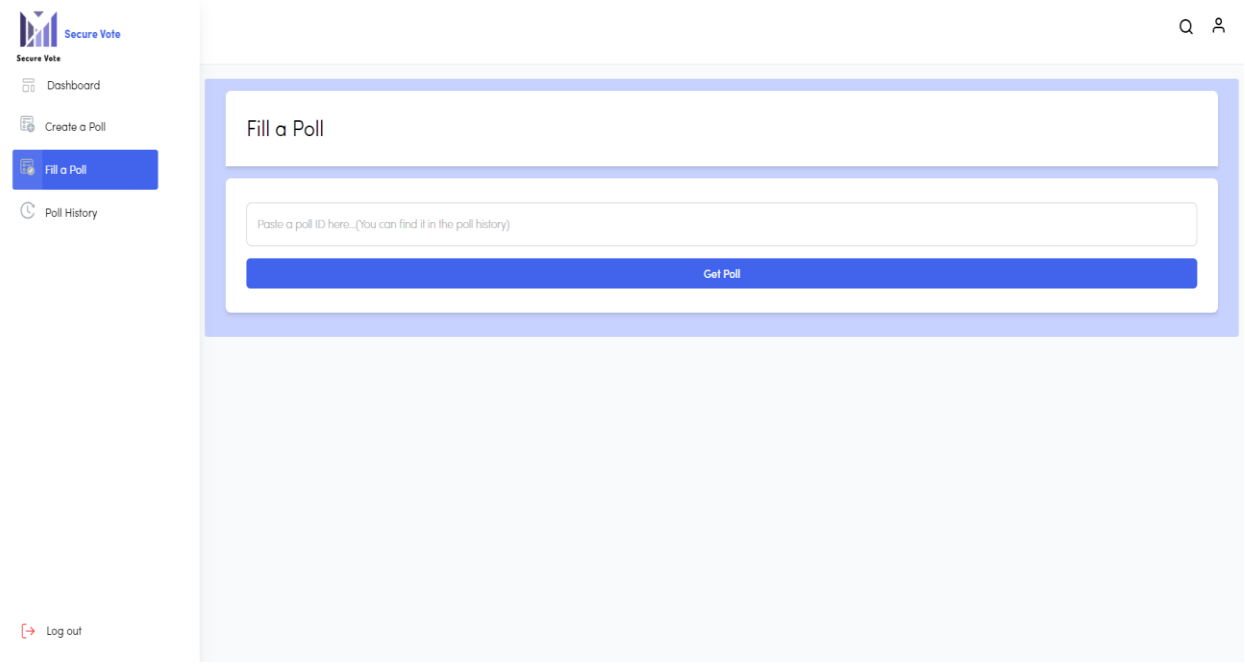

Fig A.7 Fill Poll

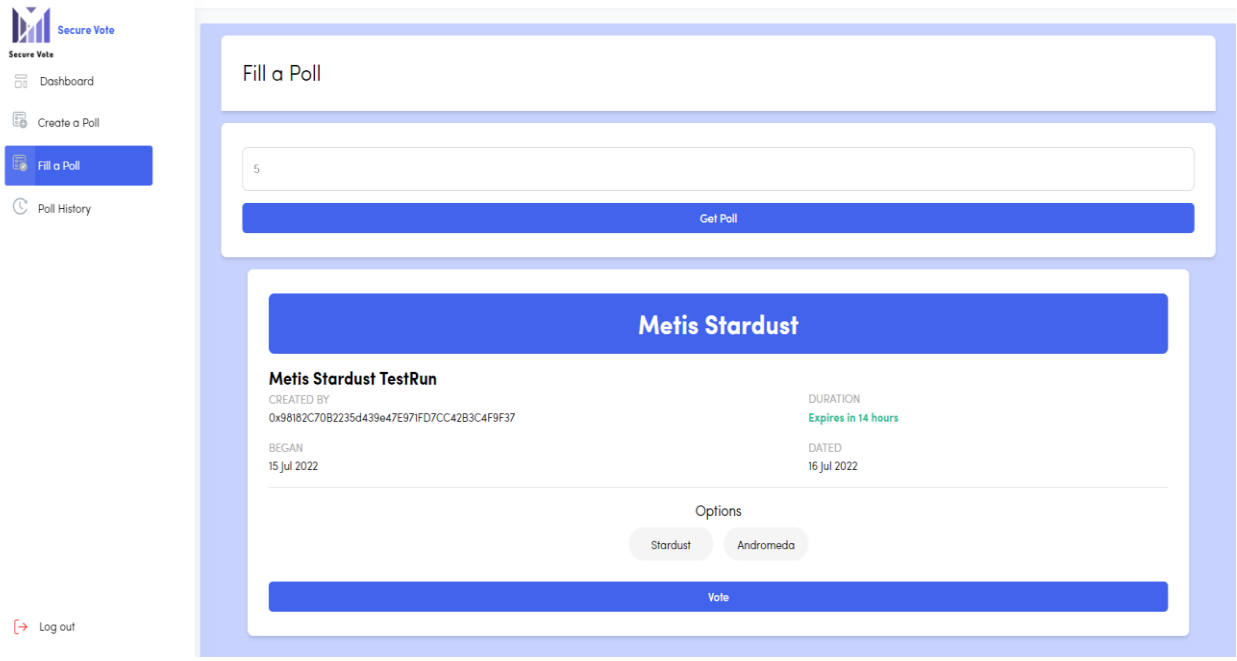

Fig A.8 Get Poll

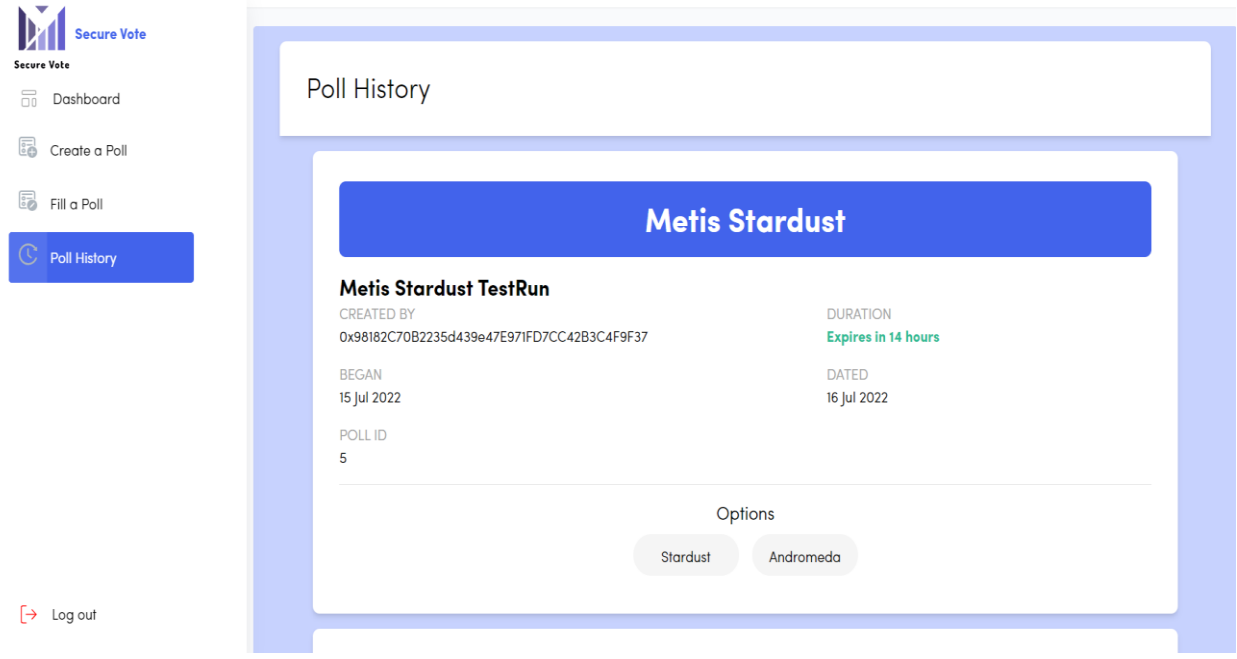

Fig A.9 Poll History

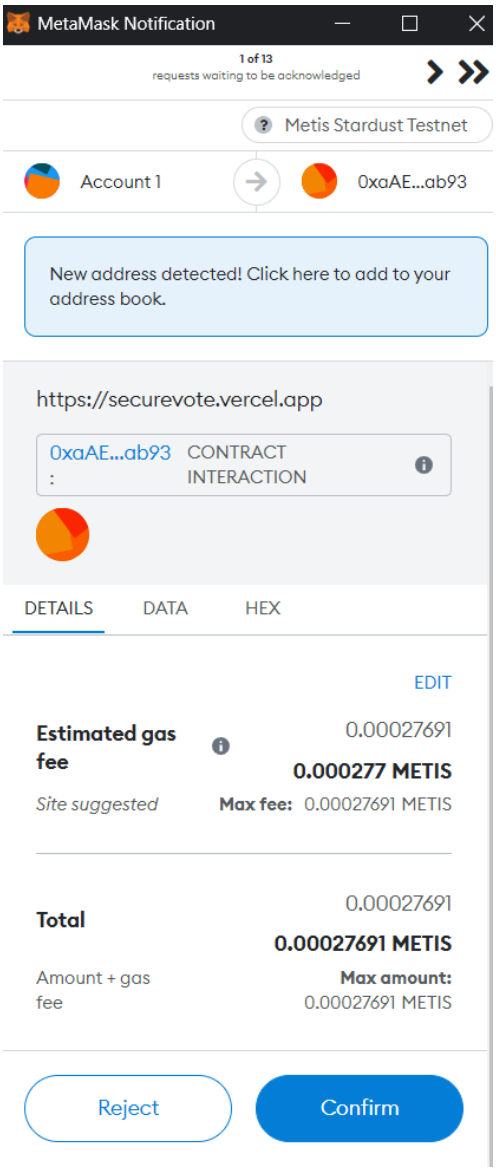

Fig A.10 Contract Interaction

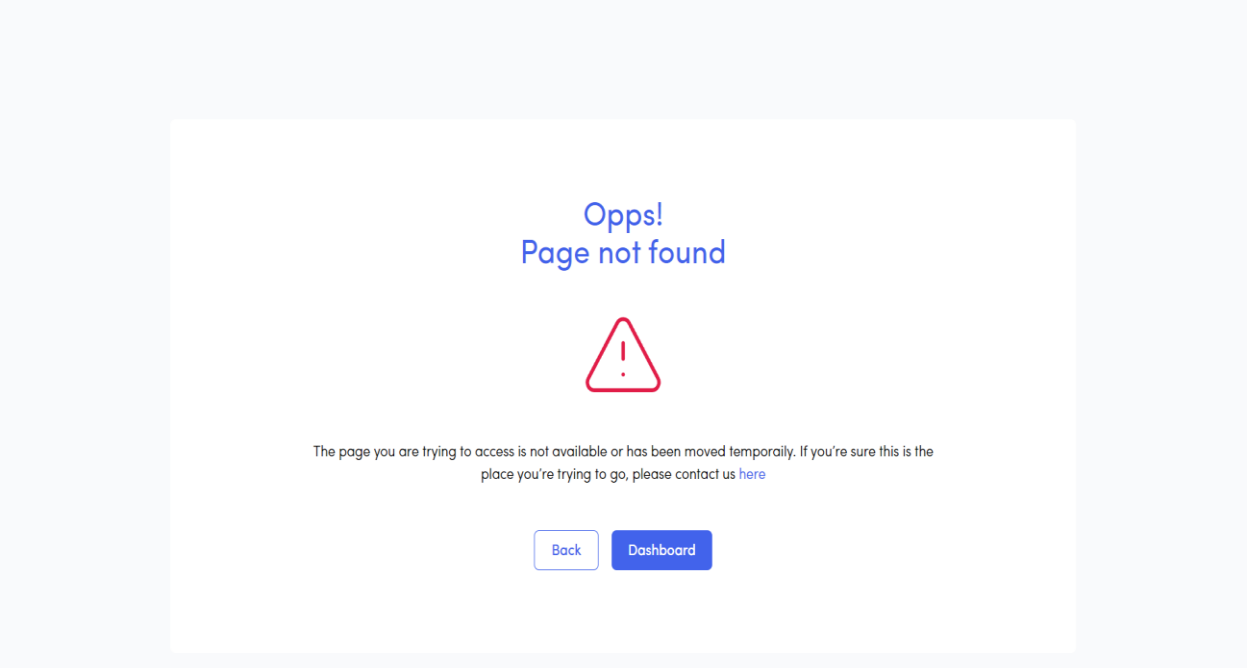

Fig A.11 Error 404