PROJECT PROPOSAL

COSC670: Cryptocurrencies and Blockchain
Spring 2024

- Ryan Tiffany
- Devere Weaver
- Pouria Tayebi

28 February 2024

I. System Goal

The goal of our blockchain-based web app is to empower users to engage in decentralized decision-making through the creation and participation in polls. By leveraging blockchain technology, we aim to provide a transparent, secure, and tamper-resistant platform where users can create their own polls on various topics of interest and allow others to vote on them. Through decentralization, we aim to eliminate the need for intermediaries, ensuring that poll results are verifiable and trustworthy. Our app seeks to democratize the polling process, giving individuals and organizations the ability to gather opinions and make informed decisions in a transparent and inclusive manner.

II. Use Cases

Users of the application include any person seeking to host a decentralized vote or polling of some sort where the goal is having a cryptographically secure voting process. This group of users can include, for example, community officials, students, professors, corporate board members, etc. When a user wishes to hold a vote, all voters can use their wallets to verify identity and participate in the vote, which is logged as a transaction on the underlying blockchain.

Some examples of the types of voting include voting in an academic institution, local elections, corporate governance, community decision-making, organizational decision-making, and token holder voting in blockchain projects.

Some potential use cases of the system:

1. Creating a Poll
   - Actor: User or group of users who wish to create a poll
   - Description: The users will be able to use the application to create a custom poll that can be used by the target voters. They will decide the parameters of the vote, such as how long the polling is open.

2. Taking a Vote
   - Actor: User or group of users who wish to host a vote
   - Description: After creating a poll, the user will be able to use the application to open the poll and take the votes of the verified voters.

3. Casting a Vote
   - Actor: Users of the system who wish to participate in the poll
   - Description: The voters can use the application to vote when participating in an election.

4. Verifying Voter Identity

- Actor: The application system
- Description: Before a voter can participate, they must verify their identity with the system using their wallet. The voter identification system will adhere to unreusability, preventing voters from casting more than one vote.

5. Tallying Results
- Actor: The application system
- Description: Once voting has completed, the application will then read the blockchain's transaction data to process and return the live results to the voters.

III. Other Features

Web-services: The voting system will require web services to handle user authentication, data storage, and communication between the client-side interface and the blockchain network. These web services will be responsible for securely managing user accounts, validating votes, and ensuring the integrity of the voting process.

Security: Security is a critical aspect of any voting system. The proposed system will implement several security measures, including end-to-end encryption of user data and secure authentication mechanisms. Additionally, the system will include measures to prevent double voting and ensure the anonymity of voters.

Mashups: The voting system will integrate with external services to provide additional functionality and enhance the user experience. For example, the system may integrate with social media platforms to allow users to share their voting choices, or with news websites to provide real-time updates on election results. These mashups will be designed to enhance user engagement and provide valuable information to voters.

Blockchain Integration: The heart of the voting system will be its integration with a blockchain network. The blockchain will serve as a decentralized and tamper-proof ledger for recording votes, ensuring transparency and accountability in the voting process. Smart contracts will be used to automate various aspects of the voting process, such as vote counting and result verification. Additionally, it can include extra features such as a list of voters or the demographic of voters if the resources allow.

User Interface: The system will feature a user-friendly interface that allows voters to easily cast their votes and view election results. The interface will be designed to be accessible on a variety of devices, including smartphones, tablets, and desktop computers (initially only aiming for desktop). It can also include features such as real-time updates on voter turnout and election results.

Data Privacy: The system will prioritize user data privacy and will comply with relevant data protection regulations. Personal data will be securely stored and encrypted, and users will have control over their data and the ability to delete it if desired.

Auditability: The system will be designed to be auditable, allowing independent verification of the voting process and results. This will help ensure the integrity of the voting process and build trust among voters.