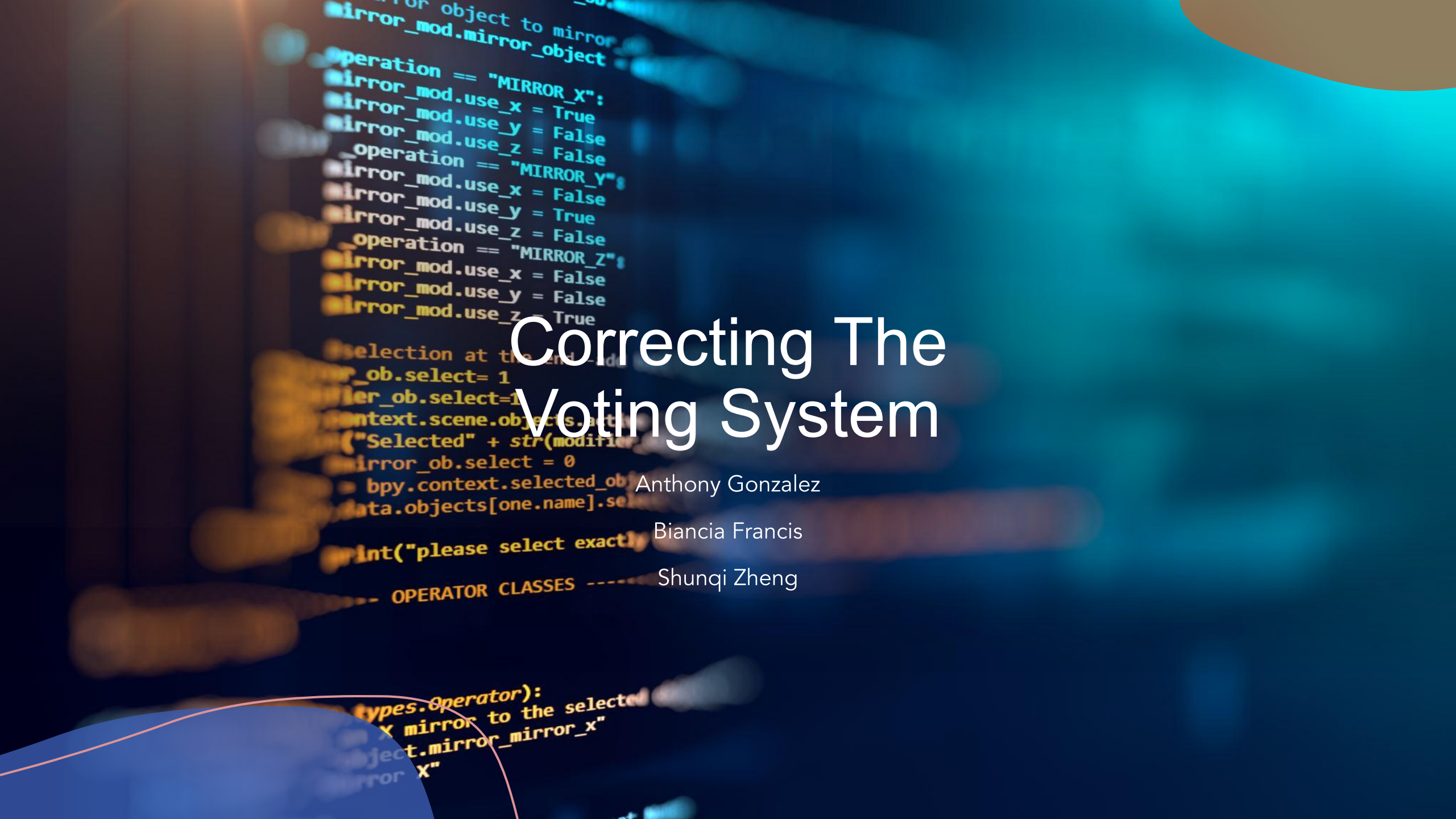


Correcting The Voting System

Anthony Gonzalez

Biancia Francis

Shunqi Zheng

Overview

- The problem statement
- Proposed Solution
- Results
- Smart Contracts
- ER Diagram of Data Storage and Transfer
- UML Diagram
- Cryptophrase Generation
- UI Representation

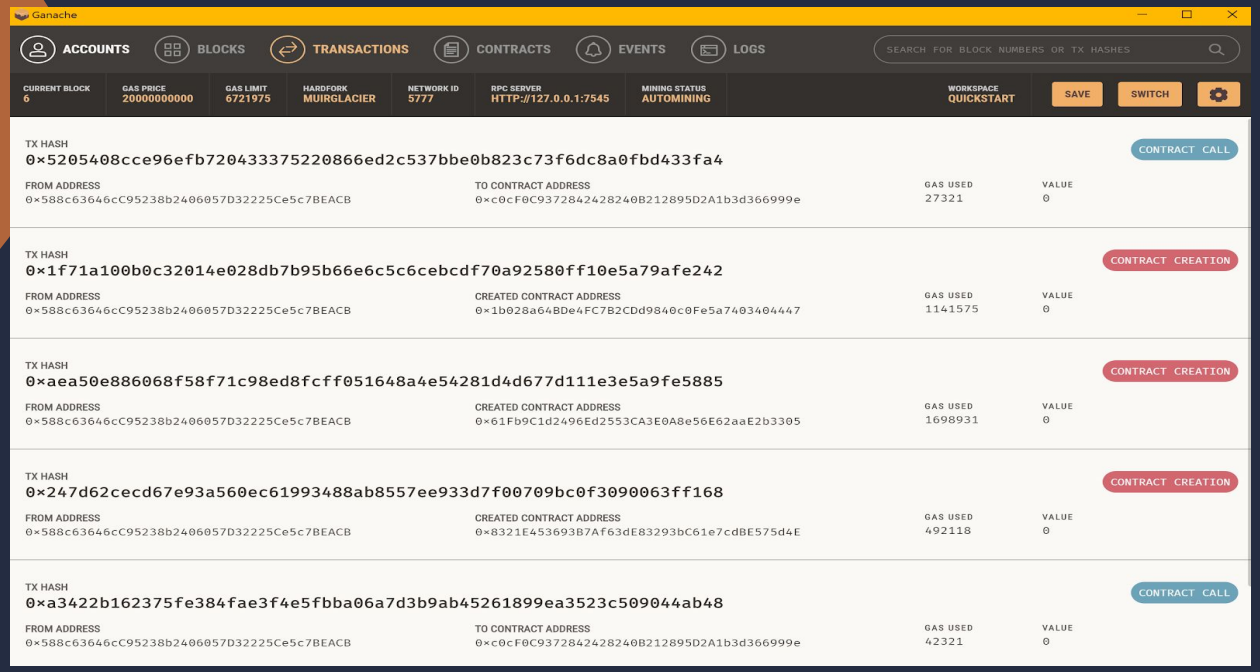
The Problem Statement

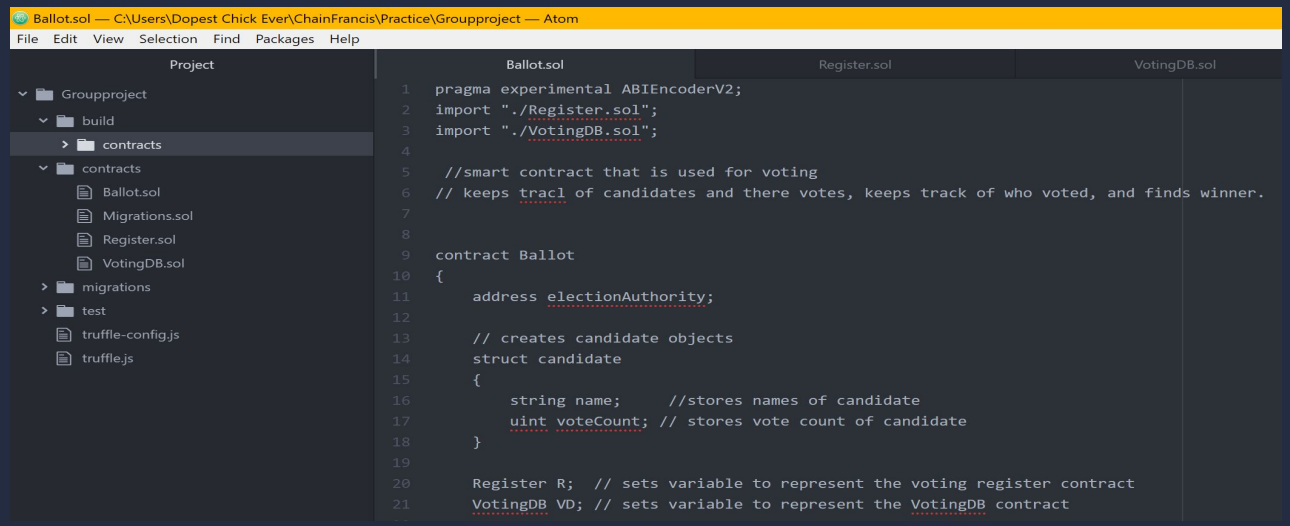
- What our research aimed to resolve was the miscalculation of votes during election periods
- Voters continue to experience the closed door treatment whereby votes are casted, then authorities alter the received information to benefit a specific candidate
- The lack of voter visibility and accessibility and there is no room for voters to challenge the final vote count
- The current voting system is old and dated and as a result, the voting inadequacies continue to occur year over year

The Proposed Solution

- We proposed to implement the Blockchain technology of smart contracts, namely; Ballot, Register and Voting, to remove the layer of authorities who are usually responsible for the counting of the ballots
- Our solution was to designed provide security, increase storage with access to past voting history and for future outlook, provide scalability as well as reliability
- Crypto keys were also utilized in the process to aid the identification process of each individual re their registered address

Results





- Three contracts were deployed using powershell and the ganache platform, as well as atom, as the start of a new phase of vote collection
- Voters had access to their records via a crypto phrase once they registered
- Query functions are now set up to assist in the management of the data
- Ballot contract holds all the relevant information for the election

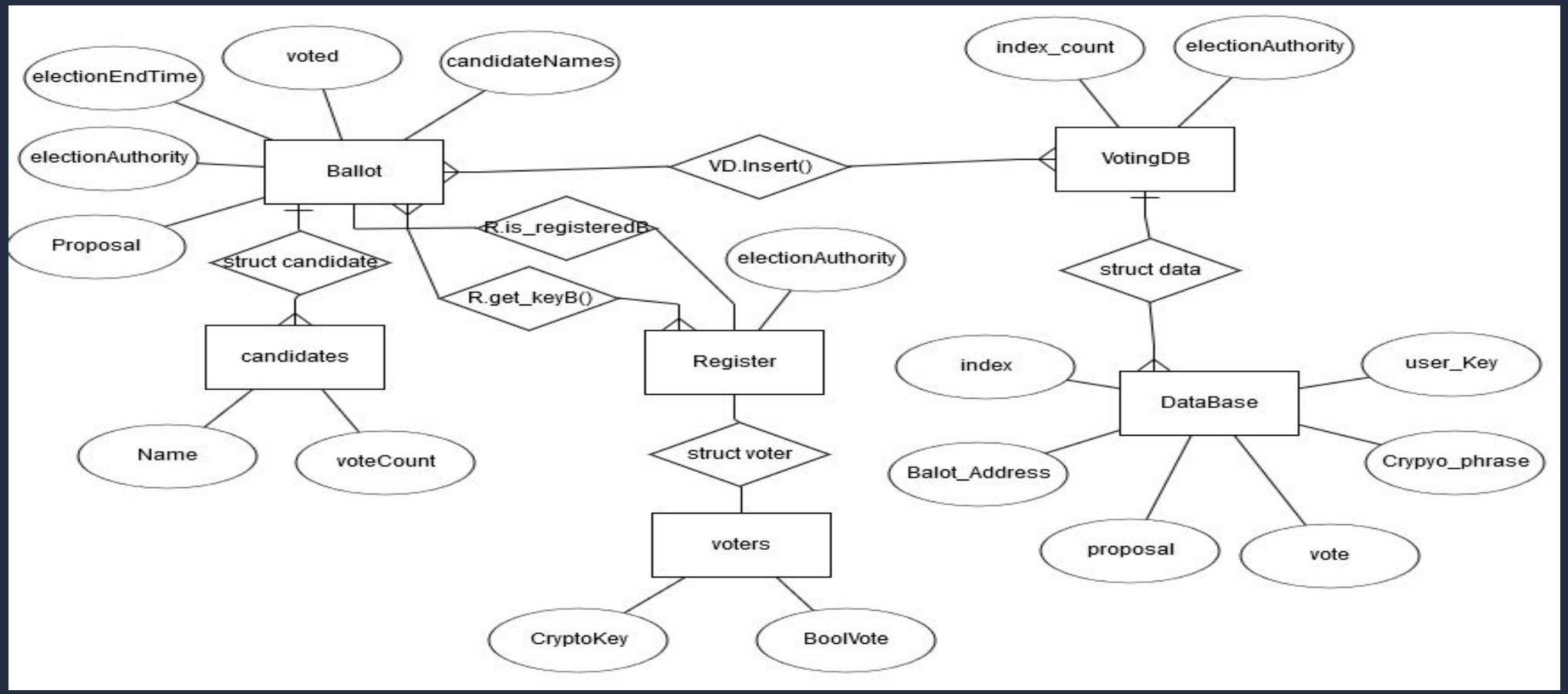
Smart Contracts

To fulfil different aspects such as voter registration, ballot creation/voting, and storage/access of voting history three separate smart contracts were made to help resolve the issues from the problem statement as well as to aid in scalability/reuse.

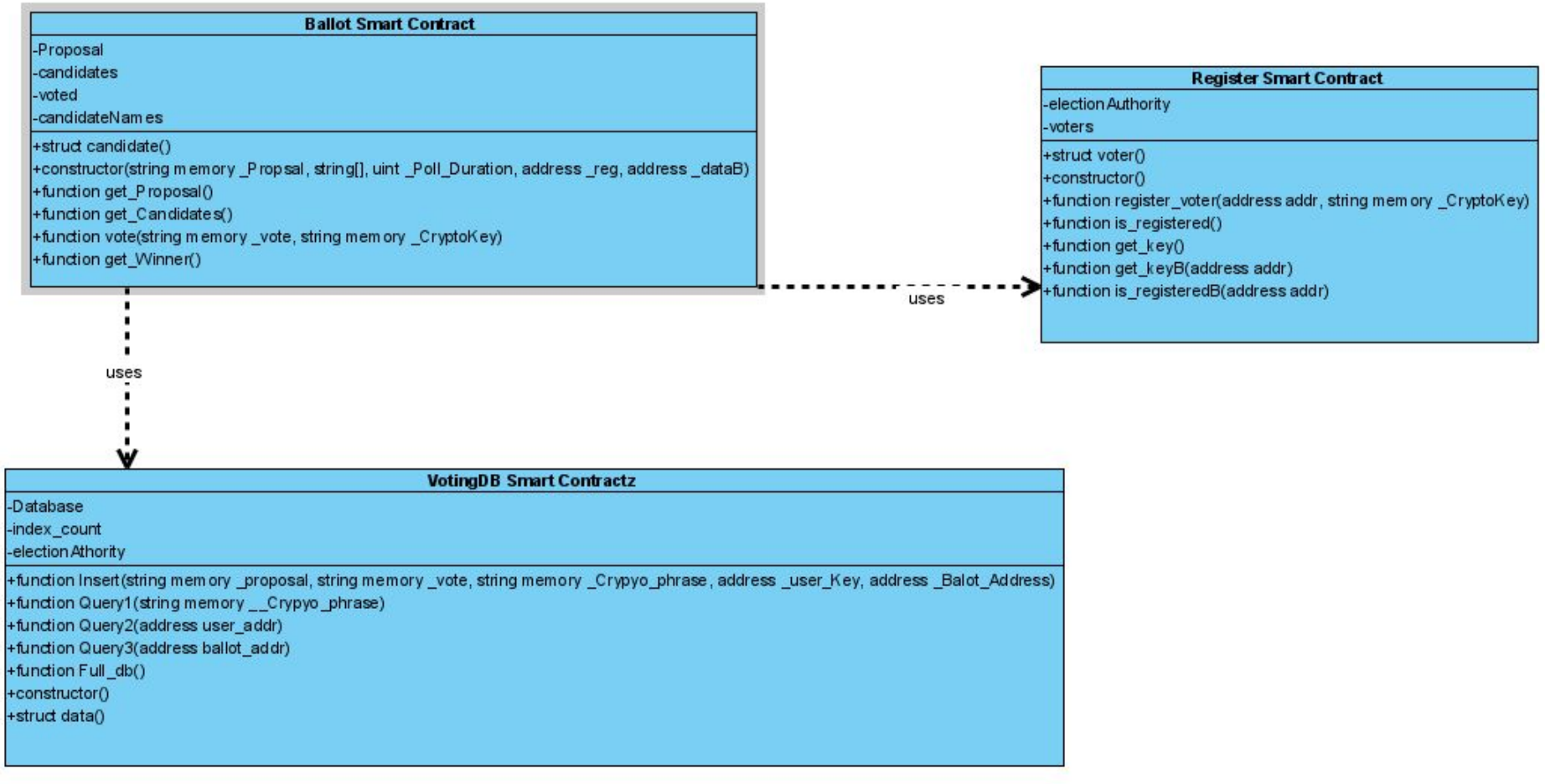
The smart contracts include

- Register.sol
  - Registers voters and stores their voting eligibility and crypto phrase
- Ballot.sol
  - Sets voting parameters, is where voters vote, and counts/sends result.
- VotingDB.sol
  - Stores data from of votes from Ballot.sol and allows users to query the data based on a voters public address, a users crypto phrase, or the address of Ballot.sol

ER diagram of data storage and transfer of smart contracts

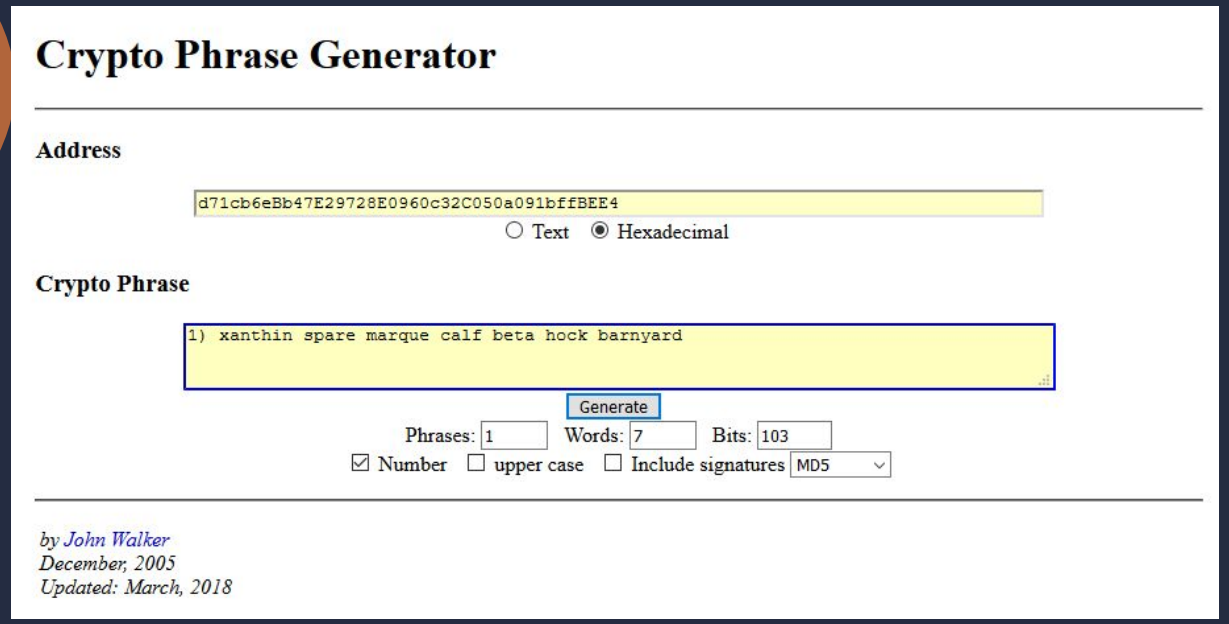


UML diagram



- This shows the interactions between the smart contracts
- Ballot.sol uses functions form Register.sol to confirms a voters credentials then uses a function in votingDB.sol to add votes to the VotingDB.sol databse.

Crypto phrase generation



This crypto phrase generator utilizes the same backend and a modified front end of John Walker's "Pass Phrase Generator".

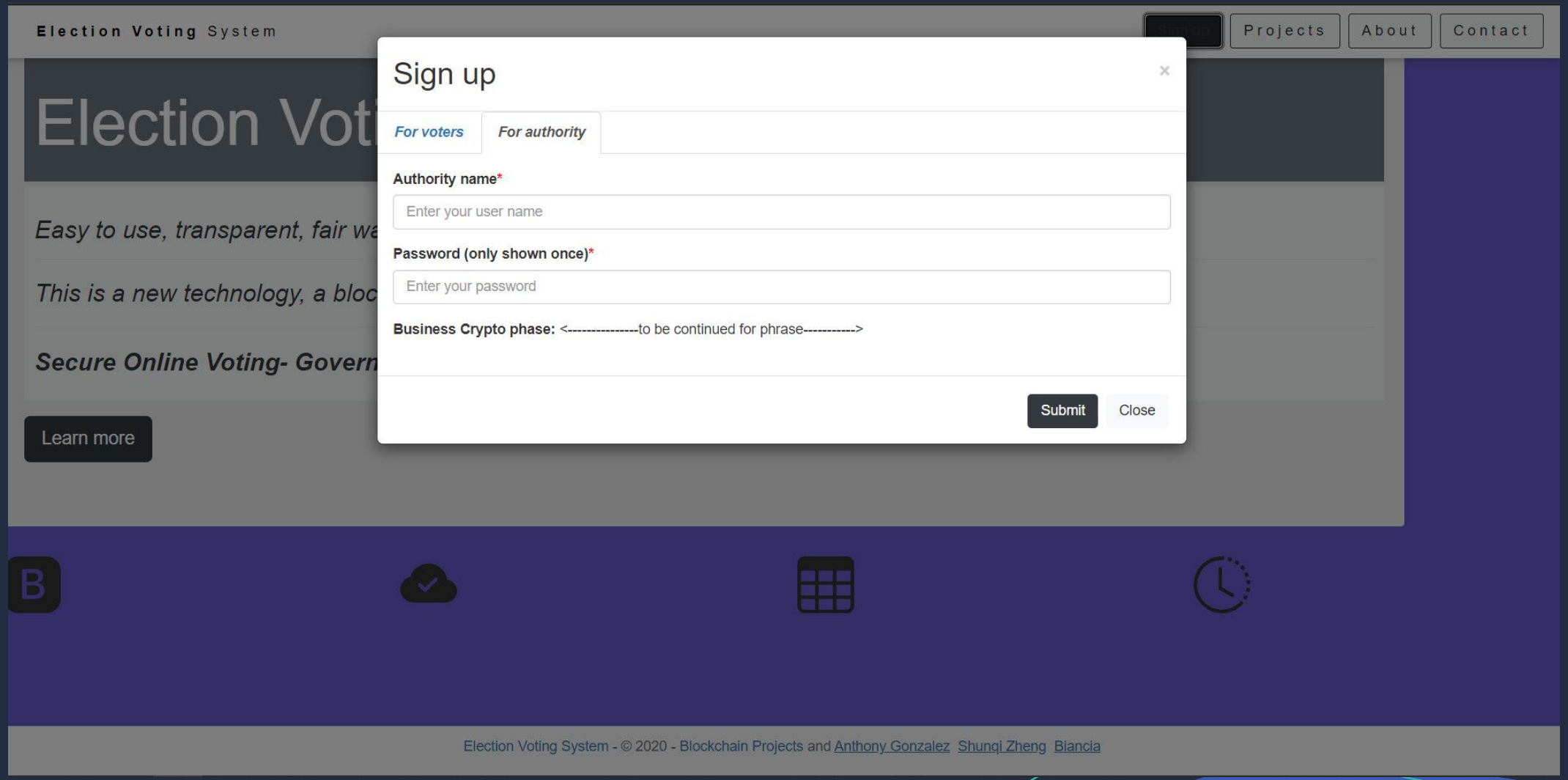
which is a public domain, open source project that generates unique pass phrase based on hexadecimal values or string inputs.

For the purposes of this project each voter address was entered into the generator and produced their own unique crypto phrase.

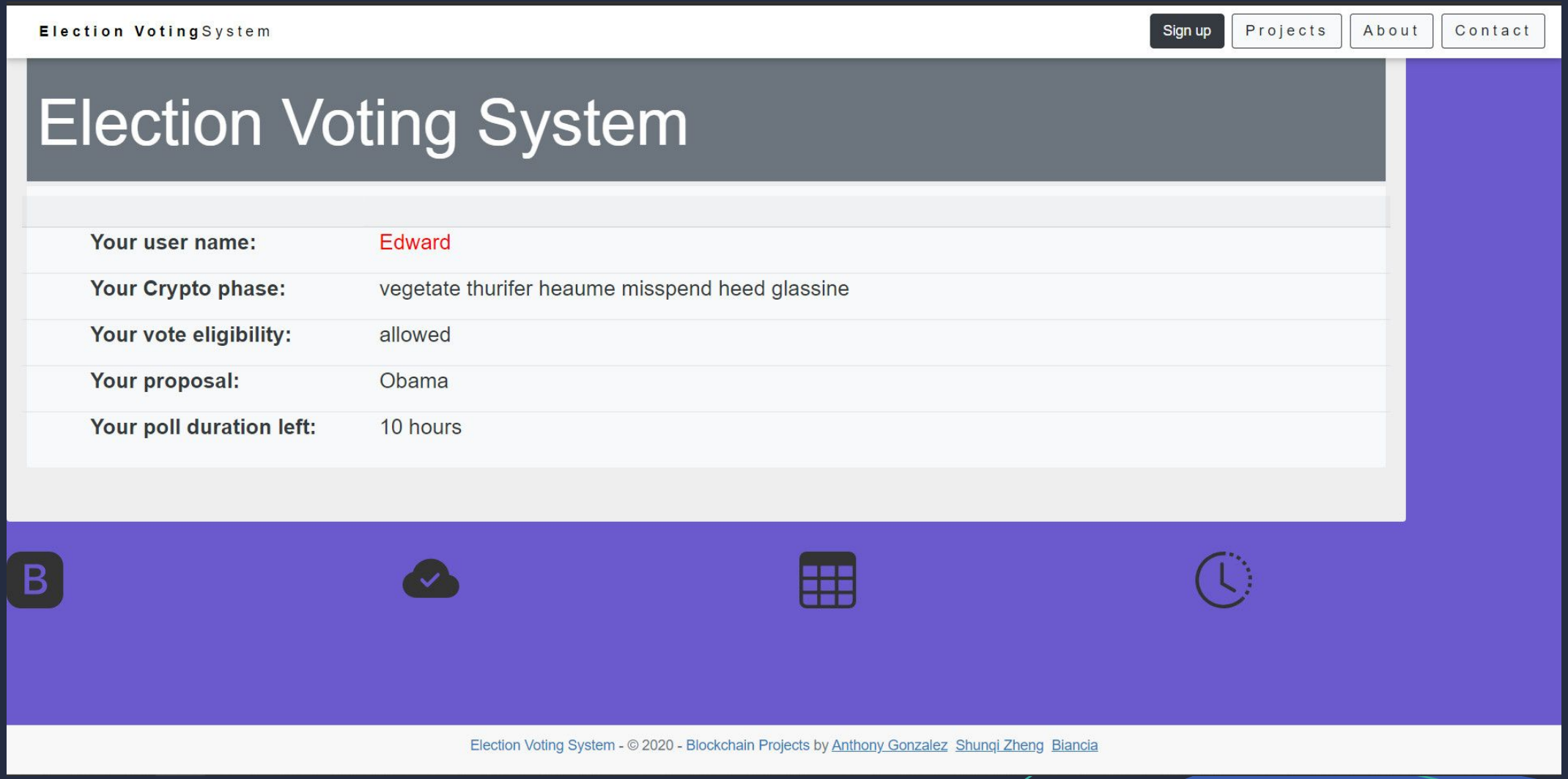
This phrase is then entered into a register voter function with the voters public key.

this is currently done outside this page, but in future iterations it would ideally be done with in the same UI space

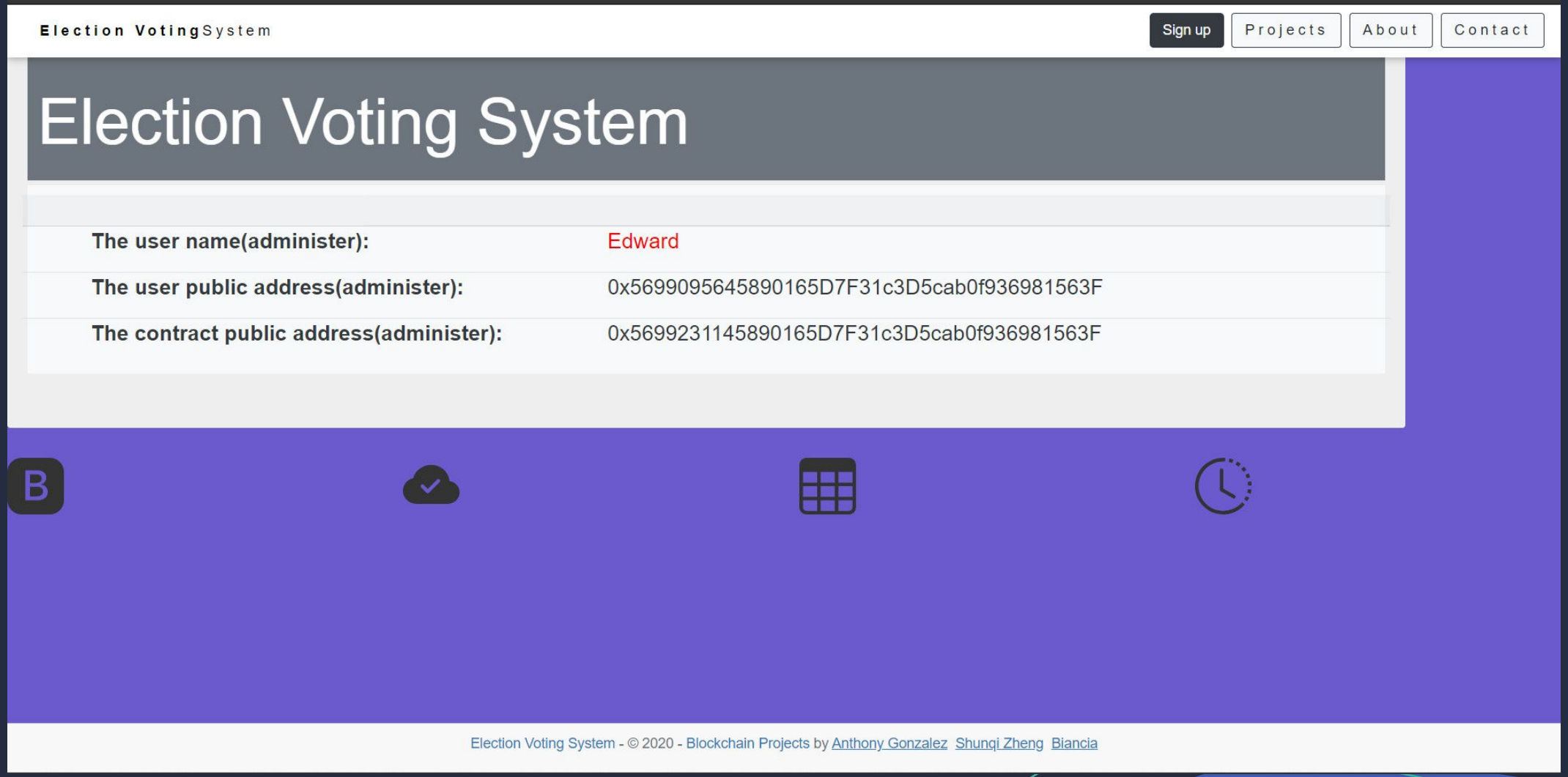
UI: Homepage and Sign up



UI: For individual



UI: Voting Database



Conclusion

- The problem statement
- The Proposed Solution
- Results
- Smart Contracts
- ER Diagram of Data Storage and Transfer
- UML Diagram
- Cryptophrase Generation
- UI Representation

References

Walker, J. (n.d.). Pass Phrase Generator. Retrieved August 05, 2020, from https://www.fourmilab.ch/javascrypt/pass_phrase.html

Gürsoy, G., Brannon, C.M. & Gerstein, M. Using Ethereum blockchain to store and query pharmacogenomics data via smart contracts. BMC Med Genomics 13, 74 (2020). https://doi.org/10.1186/s12920-020-00732-x

Rumeysa Bulut, Alperen Kantarcı, Safa Keskin, Şerif Bahtiyar

Blockchain-Based Electronic Voting System for Elections in Turkey

https://www.researchgate.net/publication/337527299_Blockchain-Based_Electronic_Voting_System_for_Elections_in_Turkey

QUESTIONS?