William Sun

Elaine Wong

Xueshan Bai

Xi Wang

Blockchains Midterm Project Report

Current Progress

So far, in this project, we have created a minimum viable product. We have learned about the Ethereum blockchain, development on it with Solidity, and the necessary tools for debugging smart contracts. In our resulting product, we have the following features:

- A single administrator can create the contract.
- A single administrator can specify the initiatives of the charity that can be voted on, and when voting ends.
- Anyone can donate to the contract.
- Anyone who has donated can vote for specific initiatives.
- After voting closes, anyone can trigger the contract to pay out to the initiative with the most votes.
- Values like the addresses corresponding to charity initiatives, and current vote totals, are easily observable.
- There are non-comprehensive efforts to prevent gas attacks and early stopping attacks. Based on our current product, we believe we are on track to finish on time.

Remaining Challenges

- We would like to implement unit testing (with Truffle)
- We would like to allow for the contract to have multiple administrators, requiring a multisig to perform administrative actions.
- We would like to build a simple front end.
- We would like to find a way to guarantee that the smart contract source code is reviewable, and can be linked to its Ethereum address.
- We would like to comprehensively patch any possible security issues that may arise if this contract is deployed in the real world, including

    - Gas attacks
    - Early stopping attacks
    - Attacks that render the smart contract’s ether unretrievable
- Handle the charities donating to themselves vulnerability
    - If a potential charity donates a lot of ether to overwhelm the legitimate votes, they can take everyone’s ether.