Rock the Blockchain: Vote

Instructor: Mike Borowczak | COSC 4010

Mission

Create a secure electronic voting platform using blockchain technology

Why blockchain?

It allows distributed consensus that is tamper resistant and tamper evident

What is a blockchain?

A blockchain is an (again, distributed) **immutable** linked list where each node contains a hash of all previous nodes, along with any information wishing to be stored, such as financial transactions, votes, or even digital kitties.

How?

Two development teams, one leveraging existing technology, the other developing an original blockchain implementation

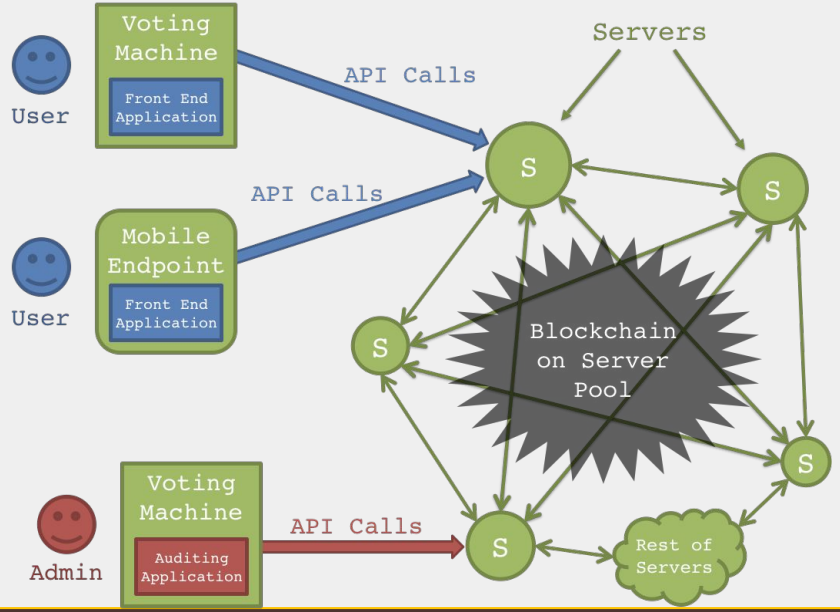
Who?

Twenty-four students divided into four teams:
Reinvent
Reuse
UI
DevOps/Support

Re-Invent

A Wyoming Blockchain Built From The Ground Up.

- Goal
  - To Create a Functional Electronic Voting System From The Ground Up Dedicated To Wyoming



Re-Invent

- Why?
  - To learn how a blockchain really works.
  - Eliminate contractual or financial obligation to a third party.
  - Keep Wyoming’s data in Wyoming.
  - To reduce bloat and unwanted features and create a more streamlined system.
  - To show that it can be done.

Re-Invent

- Process
  - Were there other implementations that we could use as templates?
  - Would a traditional blockchain be best?
  - Decided to preserve user anonymity and privacy by using two blockchains working in tandem.
  - Needed to work with other teams to build network and front end API’s to bring it all together.

Re-Invent

- Challenges
  - Current Blockchain implementations are focused almost solely on cryptocurrencies but voting is a completely different beast.
  - Quick and secure networking code.
  - Auditability while maintaining anonymity.
  - Juggling front end requirements with backend possibilities.

Re-Invent

- Results
  - A custom blockchain implementation, written in Python using the Flask framework.
  - No-Stress data input, extraction, and delivery protocols using standard JSON.
  - An application interface and endpoints for serving data through calls over HTTP.
  - A testing suite developed alongside other system components.

Re-Invent

- Future
  - Improved frontend and backend functionality.
  - Blockchain optimization and potential structural changes.
  - Improved security and voter authentication.
  - Making a more robust database and network infrastructure.
  - Working with civil authorities to provide any additional functionality.

Ethereum

“Election security is national security, and we have to start acting like it.” - Amy Klobuchar

- Smart Contract
  - Voting
  - Write-in
  - Multi-option
- Write-In
  - Checks
- Multi-Option
  - One or more votes
- Vote Tally
  - Immediate results
- Why
  - Practicality
  - Real World
  - Solidity Programming
- Additional
  - Proposals
  - Identicons
- Results

```
/// Create a new ballot to choose one of `proposalNames`.
function Ballot(bytes32[] proposalNames, uint options) public {
    assert(options <= proposalNames.length);
    assert(options > 0);
    chairperson = msg.sender;
    Options = options;
    voters[chairperson].weight = options;


    // For each of the provided proposal names,
    // create a new proposal object and add it
    // to the end of the array.
    for (uint i = 0; i < proposalNames.length; i++) {
        // `Proposal({...})` creates a temporary
        // Proposal object and `proposals.push(...)`
        // appends it to the end of `proposals`.
        proposals.push(Proposal({
            name: proposalNames[i],
            voteCount: 0
        }));
    }
}
```

Ethereum


Proposal: Ichigo vs Zero Two
To cast your vote, make a selection.
Zero Two
Ichigo


Verum Electus Ξ
localhost:3000/draft_ballots/5/preferences/2/edit
Proposal: Ichigo vs Zero Two
To cast your vote, make a selection.
Zero Two
Ichigo
Save & continue
Verum Electus / © 2018 Raylyn Pettigrew & Lucas Nicodemus. All rights reserved.
Block: 7,025,038 (synced) (kovan / 14)

Ethereum

TxHash	Block	Age	From		To	Value	[TxFee]
0xf4d81b3eb04bf87...	6957248	5 days 23 hrs ago	0x00fce88102cad2a...	IN	0x4453840c052514...	0 Ether	0.00149109
0x2d7200308fcc15c...	6953861	6 days 5 hrs ago	0x003235dcc48f8d...	IN	0x4453840c052514...	0 Ether	0
0xffe04698f40ca7d...	6953852	6 days 5 hrs ago	0x00fce88102cad2a...	IN	0x4453840c052514...	0 Ether	0.00099406
0x20d150ddd116ac...	6953832	6 days 5 hrs ago	0x007c78829a6b66f...	IN	0x4453840c052514...	0 Ether	0
0xb2483b58d98d2d...	6953634	6 days 6 hrs ago	0x007c78829a6b66f...	IN	0x4453840c052514...	0 Ether	0
0x0c81290343c802...	6953631	6 days 6 hrs ago	0x00fce88102cad2a...	IN	0x4453840c052514...	0 Ether	0.00099406
0x2275f6396fd9f77...	6953621	6 days 6 hrs ago	0x005711eb7d0de2...	IN	0x4453840c052514...	0 Ether	0
0xe89f628e3b7bbc...	6953615	6 days 6 hrs ago	0x00fce88102cad2a...	IN	0x4453840c052514...	0 Ether	0.00099406
0xb7712b33e133b8...	6953540	6 days 6 hrs ago	0x00fce88102cad2a...	IN	0x4453840c052514...	0 Ether	0.00099406
0x9efe33130e0dab3...	6953377	6 days 6 hrs ago	0x00fce88102cad2a...	IN	0x4453840c052514...	0 Ether	0.00099374
0x24b68fe0a0b72b...	6953328	6 days 6 hrs ago	0x00788c17a5d2fc0...	IN	0x4453840c052514...	0 Ether	0.00188532
0xcb12c929c0adc6...	6953319	6 days 6 hrs ago	0x00fce88102cad2a...	IN	0x4453840c052514...	0 Ether	0.00099374
0x2771af3d0e69cec...	6953236	6 days 6 hrs ago	0x00ea7ef4dffad43f...	IN	0x4453840c052514...	0 Ether	0.000000000001
0xe2ca166b79b1e1...	6953228	6 days 6 hrs ago	0x00fce88102cad2a...	IN	0x4453840c052514...	0 Ether	0.00099406
0x499e859e256387...	6953212	6 days 6 hrs ago	0x00fce88102cad2a...	IN	Contract Creation	0 Ether	0.02086538

Ethereum

Overview

Transaction Information

Tools & Utilities

TxHash:	0x20d150ddd116acad81203237c13d85d8af9dece627ee0b9e0be7b4c59b7f5a42
Block Height:	6953832 (79298 block confirmations)
TimeStamp:	6 days 6 hrs ago (Apr-21-2018 10:59:04 PM +UTC)
From:	0x007c78829a6b66fcedf8168fb445657c723dbce3
To:	Contract 0x4453840c0525146fb80c1719becd72dbd162847b Warning! Error encountered during contract execution [Reverted]
Value:	0 Ether ($0.00)
Gas Limit:	940000
Gas Used By Txn:	22439
Gas Price:	9 wei (0.000000009 Gwei)
Actual Tx Cost/Fee:	0.0000000000002 Ether ($0.000000)
Nonce:	1
Input Data:	Function: vote(uint256 optionId) *** MethodID: 0x0121b93f [0]: 0000000000000000000000000000000000000000000000000000000000000000

Convert To UTF8

UI Team

- Main Voting Application
  - Easy to Use
  - Visually Appealing
  - Secure Communication to Back End

UI Team

- Mobile Application
  - Vote from Home [Proof-of-Concept]
- Requires a QR code to verify voting registration and identity.
- May be expanded to require biometric identification.

UI Team

- Administrator Application
  - Facilitate Voting Applications
  - Utilize the Server
- Project Website
  - https://masonj88.github.io/blockdoc/

Q&A