Blockchain Voting

...

Overview

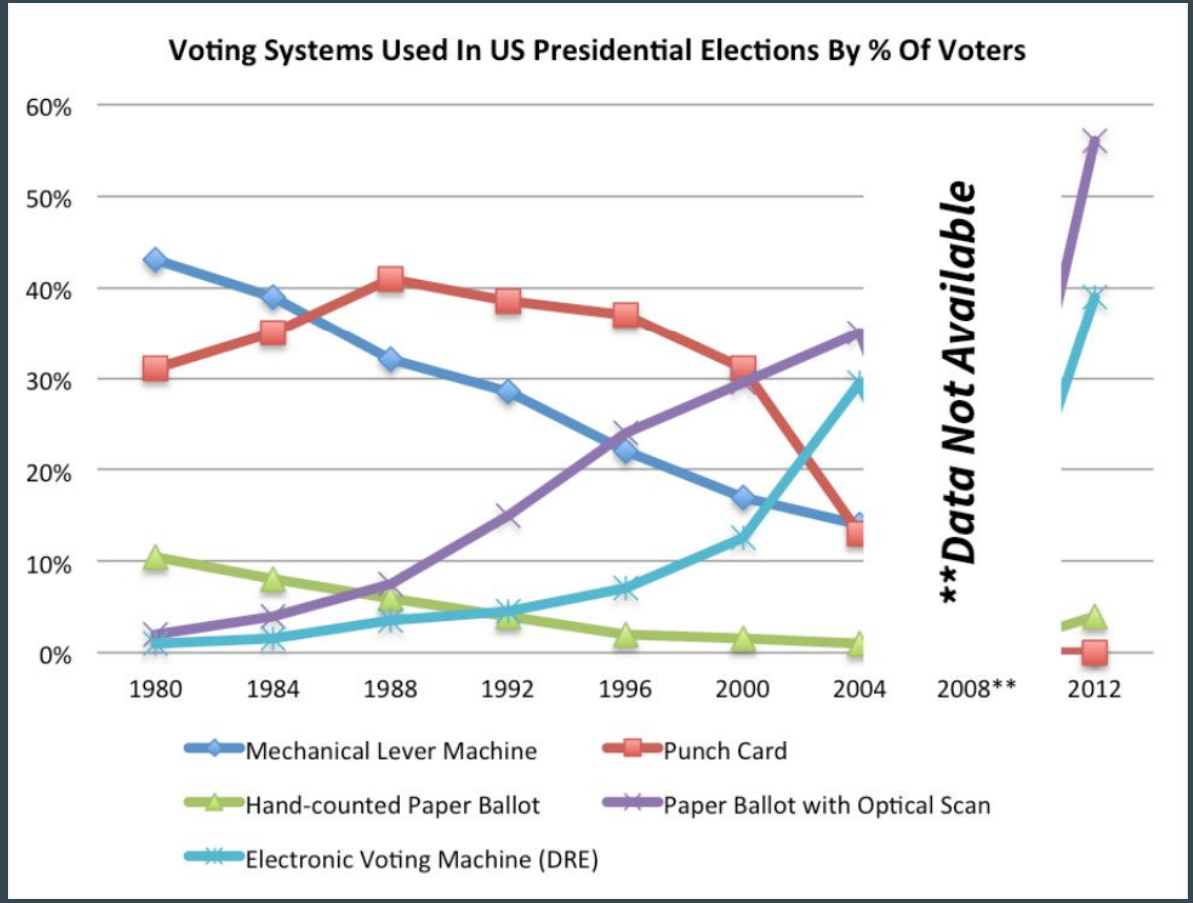
- **Motivation**
- FollowMyVote
- BitCongress
- Final Thoughts

2016 is an Election Year!

- Punch cards & lever machines -> voting machines -> ???
- Flaws of current voting practices
  - Potentially skewed results?
- Challenges of auditing elections

Motivation

Going electronic...



Source: [1] FollowMyVote whitepaper; Adam Kaleb Ernest (2014)

Motivation

- Voter privacy
- Auditing uncertainties
  - Reduce electoral fraud
- Increase voter motivation?

FollowMyVote

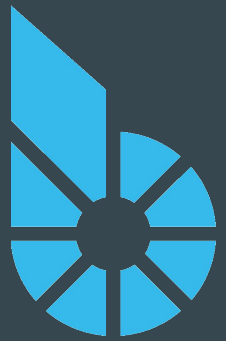
- Blockchain-based voting platform
- Built on BitShares
  - Forked from Bitcoin
  - Smaller cryptocurrency (~$10 MM market cap)

BitShares


$100M
$50M
$0M
Market Cap
0.00010000 BTC
0.00005000 BTC
0.000 BTC
Price (BTC)
24h Vol
0M
Sep '14
Jan '15
May '15
Sep '15
Jan '15
Jul '15
Market Cap
Price (USD)
Price (BTC)
24h Vol

BitShares

- Deligated Proof-of-Stake (DPOS)
- Momentum algorithm
- “Decentralized autonomous companies”



FollowMyVote

- “Request” network to start an election, for ballots, etc.
- Cast your ballots with transactions
- Delegates verify voting transactions

FollowMyVote

Intended properties:

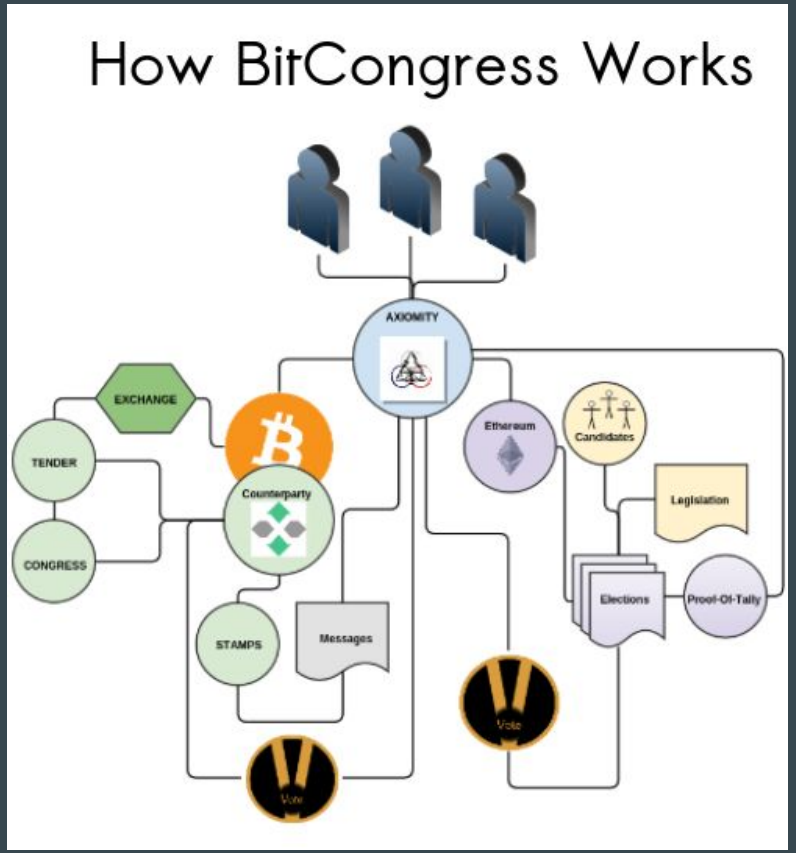
- Autonomy
- Anonymity
- Forgiveness
- Fairness
- Efficiency

BitCongress

- “Government is your control over yourself, why let someone else, let alone a small few, make decisions for you on your behalf?”
- “This system allows legislation to be created, elections to be created and votes to be instantly counted, to implement instant legislation changes within the network.”
- “One can ponder if representatives are needed when technology can instantly display ones choice across the wire & display it globally”

Network Structure

- Axiomity
  - XCP
  - BTC
  - VOTE
  - CONGRESS
  - STAMPS
- counterparty
- ethereum
- bitcoin
- smart contract elections



Counterparty - Financial tools

Create Custom Tokens

Custom Counterparty tokens can be used for a wide range of purposes and act as their own cryptocurrency, while still running on the Bitcoin blockchain. Unlike ordinary bitcoin, custom tokens can be used to issue dividends, confer voting rights, as electronic tickets, access to content, and more. Tokens are easily created in Counterwallet at the cost of 0.5 XCP for alphanumeric tokens, or free for numeric tokens.

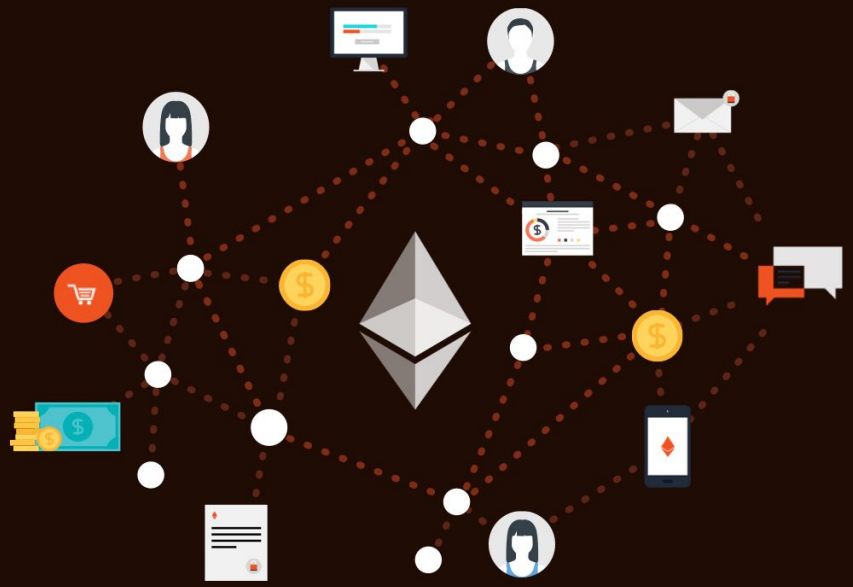
Ethereum - smart contracts

WHAT IS ETHEREUM?

Ethereum is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference.

Ethereum is how the Internet was supposed to work.

Ethereum was crowdfunded during August 2014 by fans all around the world. It is developed by ETHDEV with contributions from great minds across the globe.

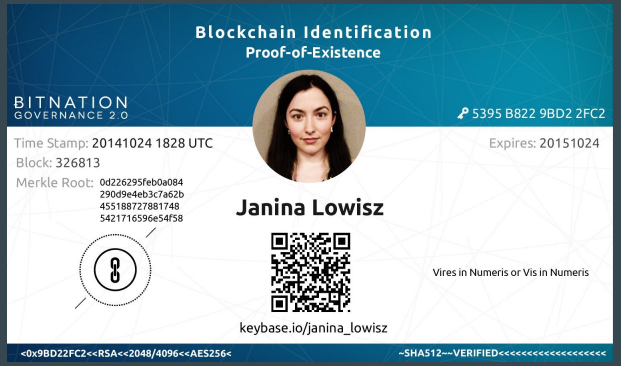


Elections

- VOTE - chain of digital signatures
- election is smart contract between voters and legislation/candidate
- Each election holds addresses, private keys & requests and sends tokens to a voter's address and a tally count that goes up on each vote completed
- Components
  - election timed lifespan
  - set of rules, candidates
  - legislation
  - budget
  - accessible URL
  - address: divisible

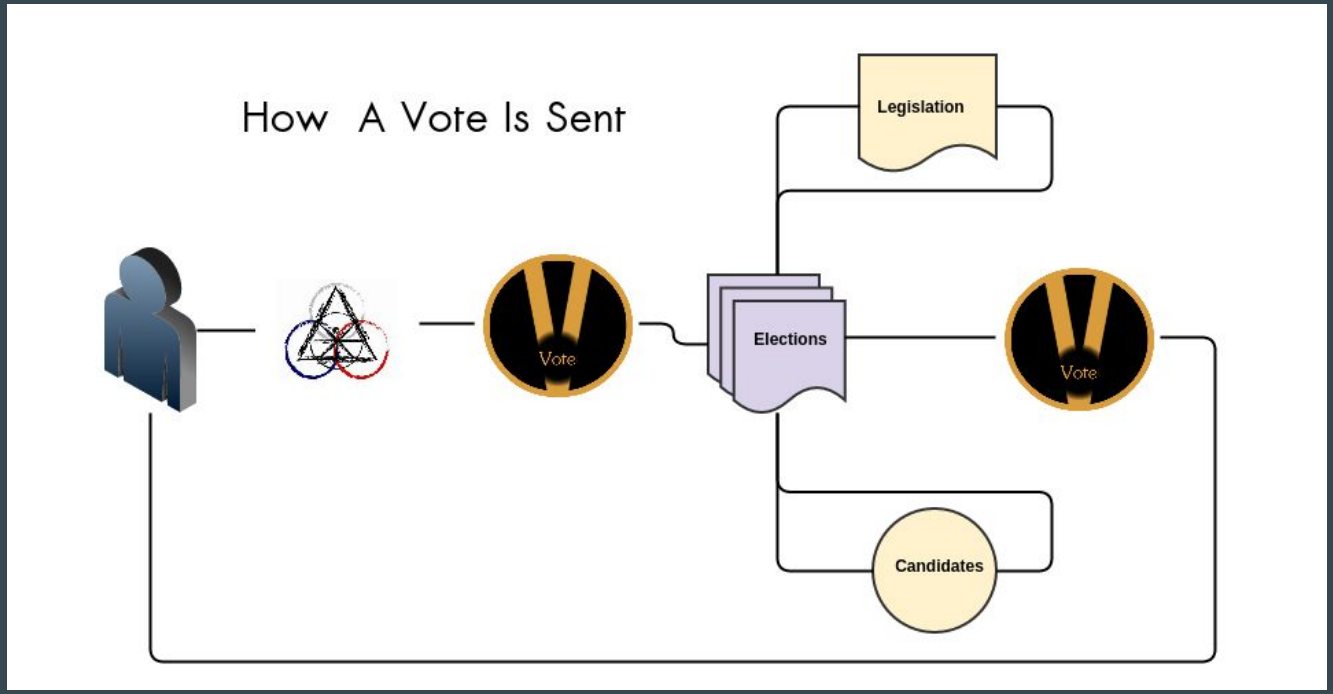
Voter

- tally count for each vote from a voting address
- successful vote: voting address hashed with proof of tally tokens in and put it blockchain (ethereum)
- proof of tally for each vote verified by axiomity and election
  - gives voter profile a active/inactive/fraudulent status
- A single vote is given to an address associated with a *Blockchain ID* upon registration with bitcongress



Elections

- Axiomity used to view/create elections
  - anyone can create addendums
- new elections:
  - legislation posted = smart contract created with custom rules established in axiomity
  - when voted for (yay or nay), VOTE token sent to election
  - when election ends, VOTE returned to respective voter
- CONGRESS, a special token
  - sent to activate a smart contract
  - activate winner contract, register winner and return VOTE tokens


How A Vote Is Sent
Legislation
Vote
Elections
Vote
Candidates

Miners

Why would VOTEs be put on a blockchain?

- Counterparty
  - VOTE tokens are BTC transaction, have mining fees
- Ethereum
  - Smart contracts require ether to execute
  - existence of transaction fees

Challenges

- Large scale platform, elections have linear structure
  a. restricted by votes
  b. concurrent elections not possible
- Everyone can submit elections
  a. issues of scale
  b. contradiction check
  c. race conditions
- Decentralization
  a. Blockchain ID and bitcongress are intermediaries
  b. possible bottleneck

BitCongress

- Bitcongress utilizes existing and robust frameworks
- Potential to be effective and practical
- However... there exist important issues

Final Thoughts

- It’s hard to decentralize voting
- Sybil attacks
- How can you verify identity without sacrificing anonymity?