Secure Electronic Voting via Blockchain

Joe Johnson, Cameron Jordal, Colton Trebbien

Random test

Issues with Current Paper Voting System

- Slow to Tally Votes
- Lack of Public Ledger
- Voter Fraud Worries
- Centralization (Easier to Tamper With)
- Ease of Access

How do we ensure and verify the security and anonymity of votes in an electronic voting system?

What is Blockchain?

- Blockchain is a distributed ledger technology, secured by cryptographic hashing, that can be validated by anyone on a blockchain network.
- Important parts of blockchain:
  - Block - data structure that holds the transaction
  - Chain - each block has a unique hash value as well as a the previous blocks hash (link)
  - P2P Network - Each peer has equal rights in blockchain network and provides computing power without the need for a central host.
  - Other parts include the Ledger, nodes, nonce and often uses public-key cryptography and cryptographic hash functions.

What is Stored on the Block in the Voting System?

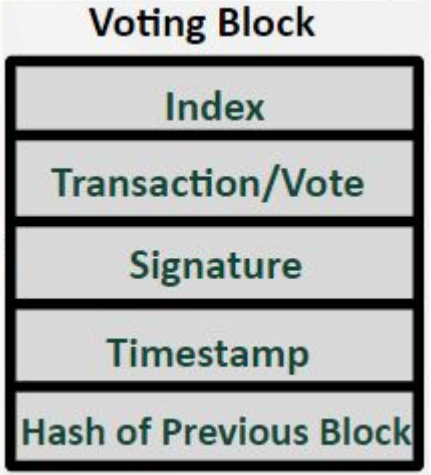
Index - Block Number.

Transaction/Vote - Senders ID, Recipient ID, token

Signature - Hash of vote encrypted with voters private key

Timestamp - Report of the time of submission.

Hash of Previous Blocks - SHA-256 Algorithm to Compute hash of the previous block.



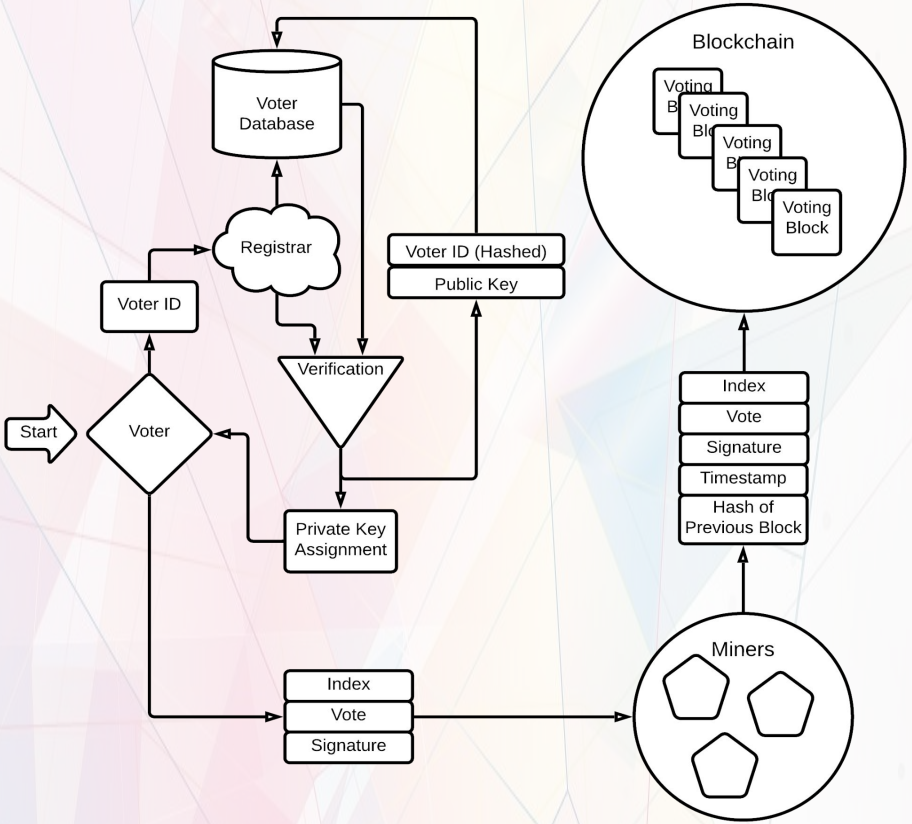
Our System

Two main components:

1. Anonymized registration
2. Anonymous voting

Almost all components are public, but voter identity is private.

Only non-public information is the list of valid voter IDs.



Conclusions

Strengths

- Decentralization
- Verification
- Anonymity
- Transparency
- Security
- Mobility
- Speed/Efficiency

Weaknesses

- Private Key Loss
- Receipt
- Trust
- Mimicry

Secure Electronic Voting via Blockchain

Joe Johnson, Cameron Jordal, Colton Trebbien
University of Oregon

Introduction

- Current voting systems are slow and outdated.
- The accessibility and mobility electronic voting provides is very promising.
- The integrity of an electronic vote can be hard to verify.

Research Question

How do we ensure and verify the security and anonymity of votes in an electronic voting system?

Blockchain Voting System

- **Index** - Block Number.
- **Transaction/vote** - Senders ID, Recipient ID, token
- **Signature** - Hash of vote encrypted with voters private key
- **Timestamp** - Report of the time of submission.
- **Hash of Previous Blocks** - SHA-256 Algorithm to Compute hash of the previous block.

Voting Block

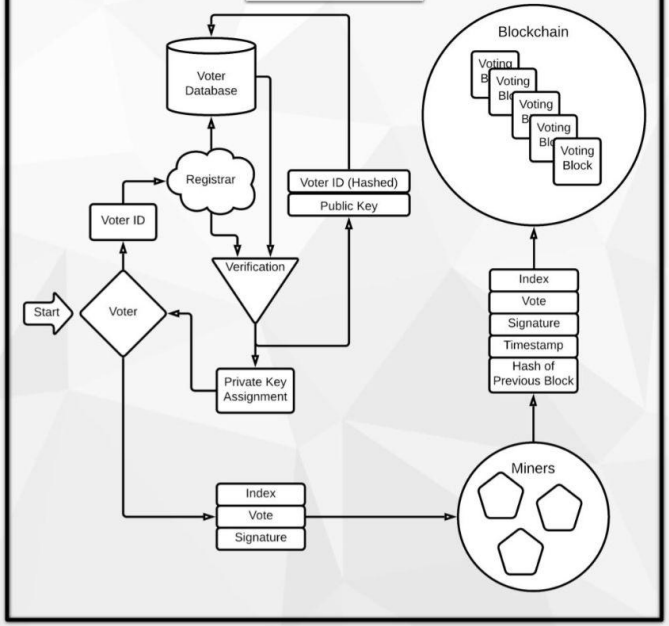
Index
Transaction/Vote
Signature
Timestamp
Hash of Previous Block

Blockchain

Blockchain is a distributed ledger technology, secured by cryptographic hashing, that can be validated by anyone on a blockchain network.

While originally created for e-currency, the system can also be used to validate transactions of any sort, including votes.

Architecture



Conclusions

Strengths

- **Decentralization** - no one weak point and no one central controlling authority.
- **Verification** - Since voter registration and votes are public, anyone can check to see if any tampering has taken place.
- **Anonymity** -Personal information is kept secret.
- **Transparency** - Votes are stored on an immutable public ledger visible to everyone, leading to trustworthiness and legitimacy.
- **Security** - Votes added to the blockchain are secured with asymmetric cryptographic hashing, which makes tampering with votes close to impossible.
- **Mobility** - Voters can vote from anywhere.
- **Speed/Efficiency** - Processing time is faster. No human error in counting/verifying.

Weaknesses

- **Private Key Loss** - If private key is lost, it is gone for good.
- **Receipt** - Private key and voter ID, which could be used to prove to others who you voted for.
- **Trust** - You must trust the software you're voting on.
- **Mimicry** - Voter database could be potentially manipulated by impersonating the registrar and sending a fake voter ID hash and public key.