**Application of Blockchain technology in online voting**

Security Scholar Nikolas Roby, 2017
University of Maryland University College

Abstract

This research focused on the design of a next generation voting system built on the foundation of the blockchain. Voters expect the voting process to be anonymous, but verification of candidate tallies should be possible. Votes should be impossible to tamper with and illegitimate votes should not be counted. All vote counting would be performed in a publicly observable way. Currently a voter cannot verify his/her vote was indeed counted appropriately. Voters today are expected to 'trust' the polling station and voting process. When designing a new voting system, a core tenet would be to remove all need for "trust," and place strong emphasis on open verification of the process and the votes. A similar problem was addressed with digital currency such as Bitcoin and Etherium.

On the blockchain, each group of transactions is hashed together, along with a hash of the previous block, and the entire blockchain would be publicly accessible. Using a blockchain for digital voting could record both voter and candidate ID, as well as the time. The voter IDs are a public/private keypair, not traceable to a voter's identity.

Polling stations are able to keep the votes off the main blockchain for the purposes of keeping the totals hidden until their release. Each vote is verified in a smart contract before being sent to the candidate or ballot measure. In our system, the smart contract is that a "vote" is given to a candidate if it satisfies certain conditions, such as the amount being cast is equal to exactly one vote, verification that the polling station concurs that the voter wallet is valid, and that the vote occurred in a valid date range. The smart contract includes multisignature element, meaning that both the polling station and voter need to sign before release to the blockchain. By combining elements of the cryptographic hashes, blockchain, smart contracts, multisignature, and sidechains, it is possible to build an open, verifiable, and anonymous voting system for the modern world.

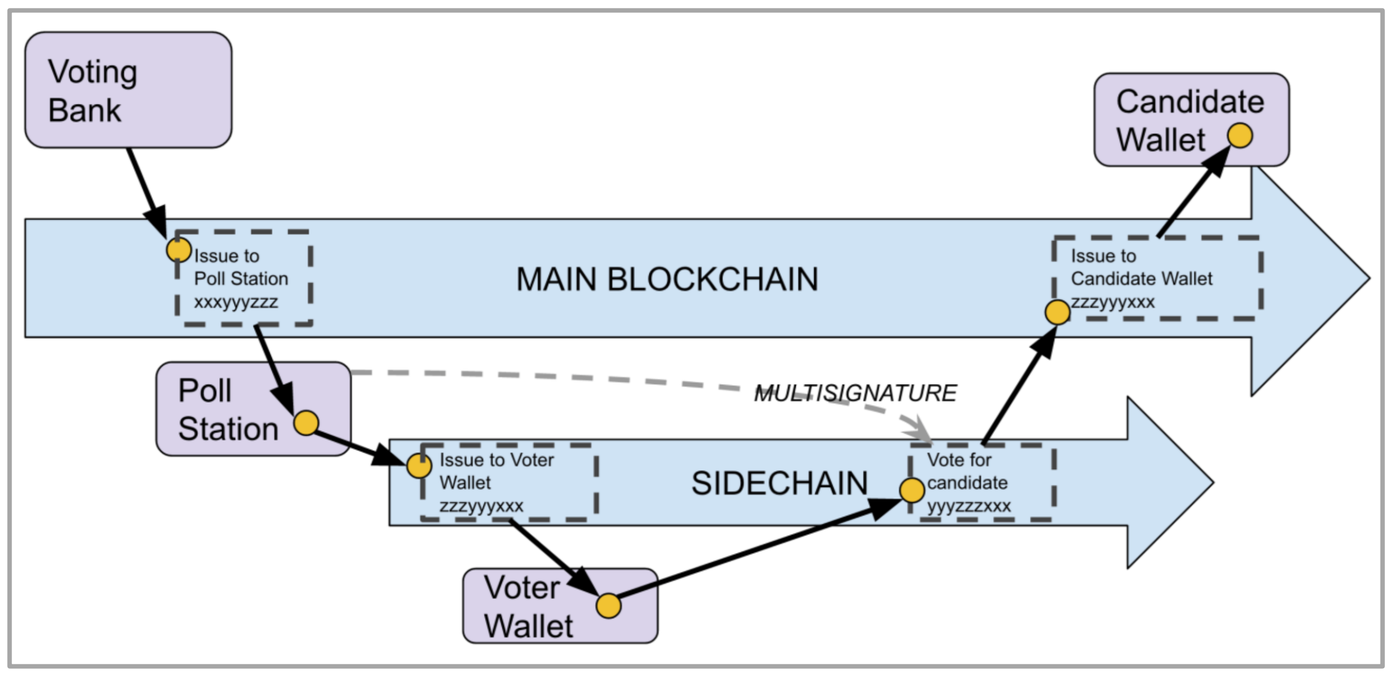
*Keywords:* Blockchain, Voting, Smart Contract, Sidechain, Etherium, Bitcoin

RSAConference Security Scholar

# Application of Blockchain technology in online voting

Security Scholar Nikolas Roby
University of Maryland University College (UMUC)

## Voting securely, anonymously, & verifiably on a Blockchain



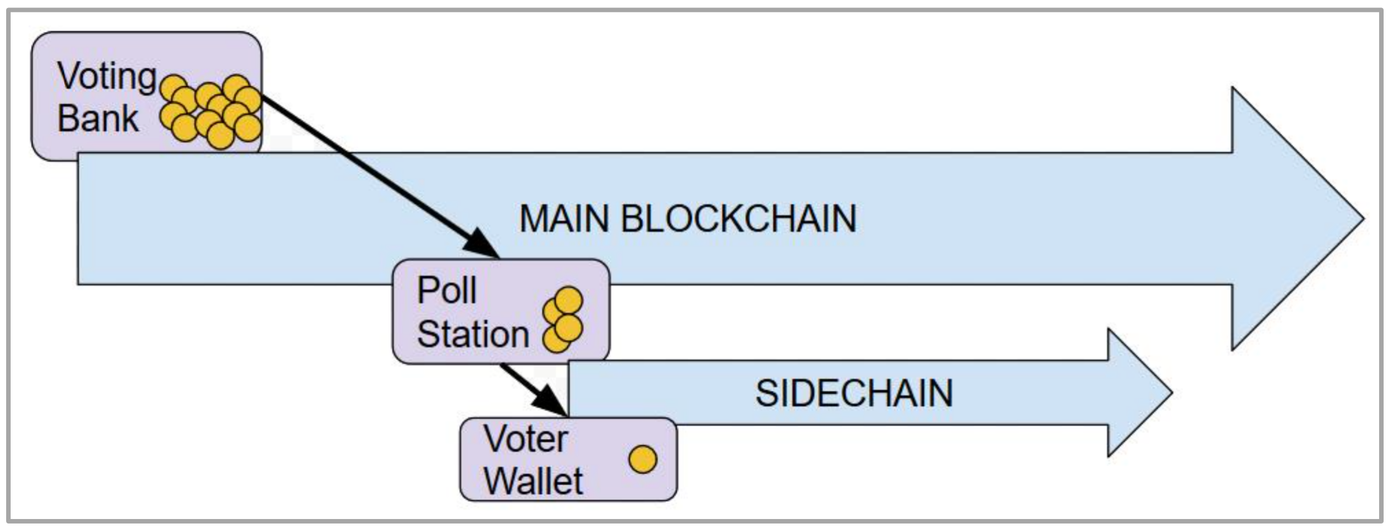

Research in using Blockchain technology as applied to a digital voting system. The blockchain records all transactions (including votes) in a distributed ledger allowing public inspection of votes cast for a candidate, but the identity is not revealed.

This allows publicly verifiable voting, while maintaining anonymity and prevents fraudulent votes. Research was in designing a system is to allow voting under duress and revealing an entire district's votes at the same time.

## Approach

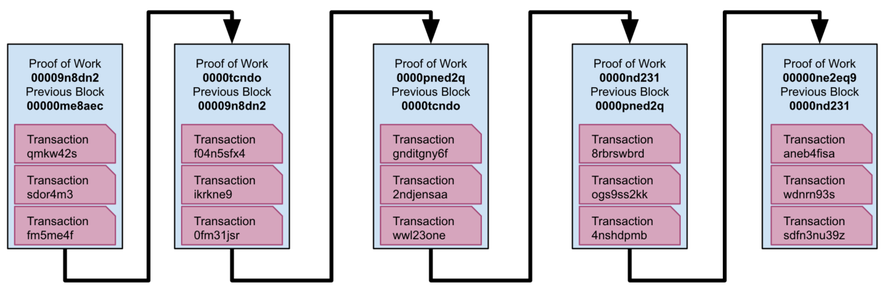
Use Distributed Ledger (blockchain) to issue digital voting tokens to a poll station. Then the poll station issues tokens to individual voters and records voting on a sidechain. At the end of the voting, the entire side chain is committed to the main voting blockchain. The specific blockchain would be Etherium, and the voting would be performed using smart contracts, preventing malicious or incompetent administrators.

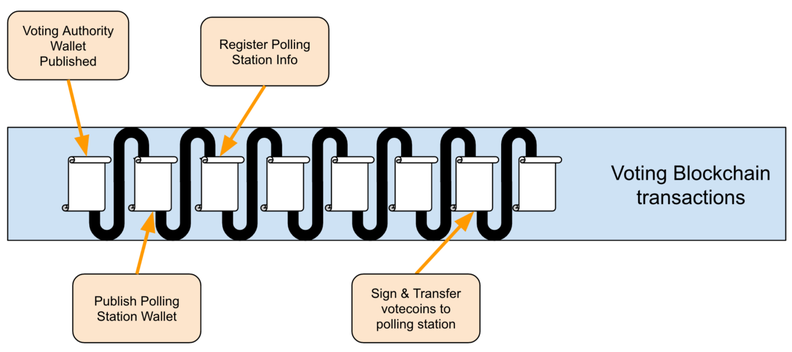
At the end of voting, the polling station will apply a multi signature to the most recent vote from each voter, and the smart contract will transfer it to the candidate or ballot measure.




## Results

Using a Blockchain for matters of public record is a great fit. The blockchain is widely use in financial markets including Bitcoin due to the properties of being distributed and publicly verifiable transactions. These are the same properties that are attractive when applied to digital voting. Each block of votes is hashed, and that hash is fed into the next block.




Balancing anonymous voting and verification is difficult and places the most importance on issuance of the initial voting tokens. After that, each token is easily tracked from issuance, to voter, to ballot.

Future work is creating a functioning "smart contract" on Etherium and using it in small scale elections or online voting.

### References

Vitalik Buterin. (2016). Privacy on the blockchain. Retrieved from https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/

Satoshi Nakamoto. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

Vitalik Buterin. (2016). Privacy on the blockchain. Retrieved from https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/