Blockchain Voting

CS4501 - Cryptocurrency Cabal

07 December 2015

A.J. Varshneya
ajv4dg@virginia.edu

Sugat Poudel
sp5pe@virginia.edu

Xhama Vyas
xdv4zc@virginia.edu

Contents

Abstract

In this report, we consider the notion of blockchain voting as a means of decentralizing the democratic process to promote election fairness and security. We seek to examine voting in the context of cryptosystems to explore the question of whether it is possible to implement voting systems with a number of desirable qualities. Can a voting system be fair, auditable, coercion-resistant, anonymous, autonomous, decentralized, and/or accessible? How might such a system be implemented? In answering these questions, we evaluate two existing proposals for a blockchain-based voting protocol, considering their weaknesses and proposing ideas to make these schemes more robust.

Motivation

Existing Voting Systems

The United States has historically favored centralized voting methods. Through the decades, punch cards and lever machines gave way to voting machines and optically scanned ballots. Most prevalently used in the 2012 election year were electronic voting machines and optically scanned ballots. Electronic voting machines themselves are susceptible to hardware and software attacks. Optical ballots are susceptible to a misintention of votes attack, in which a potential attacker with access to the voting system configuration files could swap around the ballot, causing a losing candidate to emerge victorious. Both of these systems are vulnerable and depend on a central auditing authority trusted to count the votes.

Vulnerability

Voting systems today are far from perfect, in fact they are frequently vulnerable to a variety of attacks. Even in the United States, one of the most successful democracies in the history of the world, there have been numerous cases of potential voter fraud, murky ballot handling, flawed registration processes, and vulnerable technology. Allegations of illegitimacy in elections are sufficiently prevalent throughout the world today to warrant a non-trivial wikipedia entry for controversial elections. As the world becomes more democratized, and as we move towards a reliance on electronic voting technologies to support our elections, increased security is a necessity. The increasing popularity of electronic voting will present further vulnerabilities as accessibility increases. Furthermore, the ability to have a meaningful influence on an election with the execution of exploits on computer-based voting systems would increase motivation for attacks. In any case, present vulnerabilities in electoral systems throughout the world make necessary substantial improvements even if these weaknesses are not yet being exploited.

In 2012, a man in Albuquerque, New Mexico successfully registered his dog to vote using a made up birthdate and Social Security number. While he never actually voted using his dog's identity, the ability to procure a voter registration card for an imaginary person is a testament to the lack of security in the system. Overlap in voter registrations between states has also recently come to light as a potential vulnerability. The Interstate Voter Crosscheck Program is an attempt to make updating voter rolls between states more efficient and has found hundreds of thousands of instances of people registered in more than one state. While they have uncovered few cases of fraud, this is another serious flaw in the current system that could be exploited. As of 2014, there are seventeen states that do not require identification to vote at the ballot box. A motivated party could reasonably take advantage of this vulnerability to cast ballots for registered but abstaining voters.

Figure 1: Buddy Tolbert (D) New Mexico

Perhaps even more concerning than the above listed weaknesses are vulnerabilities in voting machine technologies. A security evaluation of Sequoia voting systems by a research group at the University of California, Santa Barbara found a number of vulnerabilities that could be quickly and efficiently implemented by an attacker. The researchers were able to overwrite firmware on target machines and modify it to be malicious such that they could perform a number of attacks including denial-of-service, modifying votes, voiding votes, and voting multiple times. Furthermore, they were able to forge *SmartCards* which the system uses to authenticate and authorize voters to cast ballots. The electoral systems we use to conduct democracy should not have such weaknesses.

Figure 2: Sequoia Optech Eagle

While there have been a number of instances of voter fraud in the United States, most cases so far seem to be accidental, inconsequential, or both. Still, these incidents beg the question, can elections be made auditable and anonymous? Can a voter’s identity be private but verifiable? The key issues that we seek to investigate in this report are whether elections can be made to be fair, secure, and efficiently verifiable using blockchain-based schemes.

Blockchain-based Solutions

There are two blockchain-based proposals for online voting systems that have recently received a fair amount of press and discussion. They are *Follow My Vote*, a nonprofit organization based in Blacksburg, Virginia, and *BitCongress*, a project by Bitcoin Kinetics.

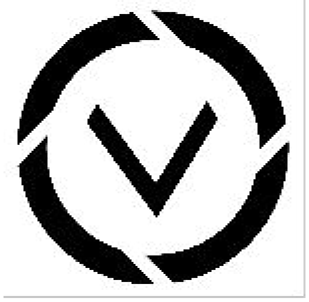


Figure 3: Follow My Vote logo

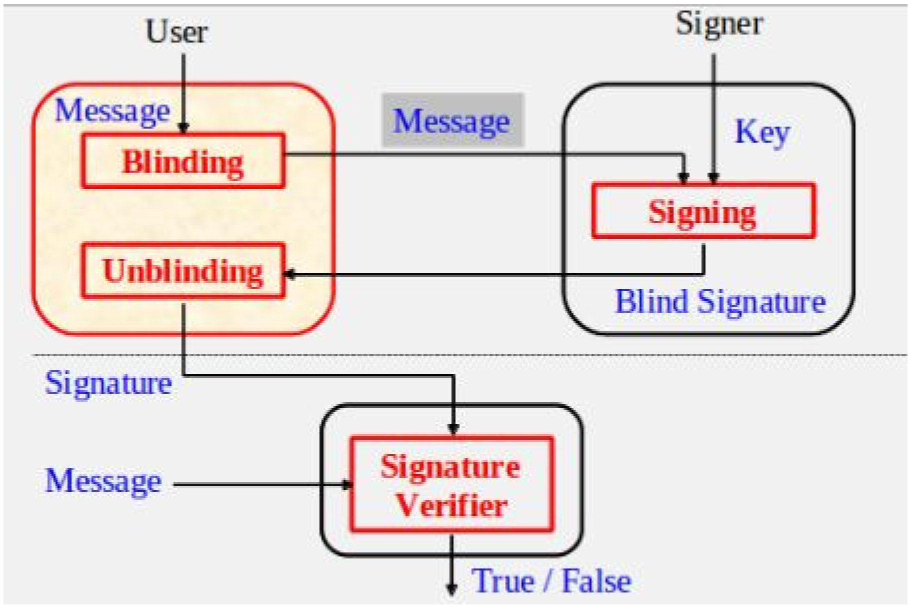
Follow My Vote

Follow My Vote is a proposed online voting platform that is currently in development. The developers' goal is to build a system with the following properties.

Autonomy	Controlled by the users as a decentralized autonomous company; all software is open source, members agree to new rules and updates to the protocol by continuing to update to new releases.
Anonymity	Use of public/private keys, addressing scheme makes users pseudonymous.
Forgiveness	Users can change their votes if their cast ballots before an election deadline.
Fairness	Users can vote for multiple candidates as opposed to just one.
Efficiency	Elections are electronic, online, and accessible to users.

The current project has a developed frontend, but as of yet no blockchain integration. While the exact protocol has not yet been publically released, the general idea is to use a blind signature scheme with tokens transacted representing votes. In Follow My Vote's scheme, there is a signing/verifying party who first signs a blinded token from a voter. Then, in the future, the voter submits their unblinded token with a public key to the verifier. The verifier signs the voter's ballot to confirm that the voter is unique and has a valid ballot. Finally, the voter logs the now-unblinded token to ensure that only one ballot is counted per unblinded token.

Figure 4: Blind signature scheme



The Follow My Vote system is to be built on top of BitShares, a crypto-equity platform forked from Bitcoin. BitShares is different from Bitcoin in that it uses a *delegated proof-of-stake* (DPOS) scheme as opposed to the strictly *proof-of-work* scheme used by Bitcoin. While proof-of-work based systems rely on achieving consensus based on the amount of computing power a node brings to the network, proof-of-stake systems base a user's ability to influence the network by their share of coin in the network. A delegated proof-of-stake scheme then extends this concept by allowing users to delegate their influence to certain users--delegates--whom they consider trustworthy to verify transactions as blocks in exchange for fees from the users involved in transactions.

Another difference between BitShares and Bitcoin is that BitShares uses an algorithm to verify transactions called *Momentum* as opposed to the SHA-256 based proof of work in Bitcoin. This algorithm is similar in nature to the more well known 'scrypt' algorithm in that it is meant to be memory-speed-limited, meaning it is difficult to implement an ASIC miner to efficiently solve these puzzles. While this has not yet been proven for *Momentum*, there is a 5000 dollar bounty to anyone who can prove a GPU/ASIC miner can be used.

Within BitShares there is also a notion of a *decentralized autonomous company* (DAC). A DAC is in essence a corporation that operates independently of any central human control, with rules deciding its actions dictated by open-source software running on its stakeholder's machines. Stakeholders can purchase shares/tokens in the corporation and may be given tokens by the corporation in exchange for providing some service to it. If a DAC is profitable, dividends may also be distributed among the stakeholders.

Follow My Vote seeks to piggyback on BitShares by creating a "voting DAC", in which tokens are votes and transactions are equivalent to casting ballots. Users generate a public key and address to use as their pseudonym and then request to be verified by outside groups (i.e. the U.S. government, political parties, etc.) so that they can vote in elections. After being verified, a user can request to vote in active elections on the blockchain, using the blind signature scheme outlined above to cast their ballots.

This system has some of the properties intended by the developers as outlined above, but there are also a number of issues that we see in its proposed implementation. The first two characteristics in the table are particularly debatable. The system is *autonomous* in the sense that the software is open source and technically independent of a central authority. However, when we consider the issue of verifying the identities of users we find that it is difficult to verify one's credentials without centralization. In the case of a political election in the United States, the central authority would be the government. We need a group like this to prevent against *Sybil attacks*, in which an attacker forges many pseudonyms on a network to gain undue influence over the network--in elections, this is what we call ballot stuffing.

The system is *anonymous* in the sense that voters are not clearly identifiable in the blockchain and Follow My Vote claims their blind signature scheme keeps users anonymous from the verifiers. However, voters are still clearly onymous to the central authority that enfranchises them. The scheme is *forgiving* in that users are apparently able to alter their vote at any time before an election deadline, as it seems to be suggested that the network will be designed to recognize the newest transaction from a user as the valid ballot casting for any given election. It is conceivably *fair*, by their definition, in that users should be able to cast ballots for multiple candidates. Finally, the system is clearly *efficient* in that it is relatively accessible and should require no more effort than that needed to vote today.

BitCongress

A decentralized voting scheme allows us to inherently solve some of the current issues relating to voting such as accountability, auditability and fairness. A peer to peer network running an implementation of an electronic voting system would allow for "votes" to be tallied and transferred without the need for a centralized validation and verification system. However, such a system carries its own set of problems. Since accountability lies with the voters and a trust based system would not work, the system needs to prohibit double voting. BitCongress proposes a solution to this issue by using a "hash based proof-of-work and proof-of-tally"[1] that would create a public chain of records for voting transactions and the elections themselves that cannot be changed without recreating the entire chain. This would serve as undeniable proof for the voting transactions and the elections that took place and give the results inherent auditability.

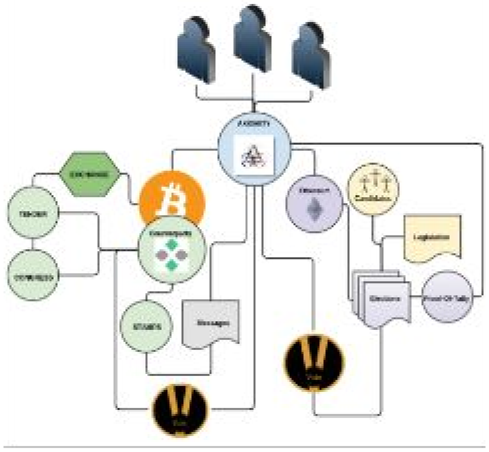


Figure 5: BitCongress overview

BitCongress was started by Morgan Rockwell, who states that "Government is your control over yourself, why let someone else, let alone a small few, make decisions for you on your behalf?" [1] Rockwell clearly emphasizes a transparent democratic system where legislations and elections can be created and votes can be counted instantly garnering results and changes promptly. The blockchain structure used is similar to the one used by the cryptocurrency Bitcoin however it involves multiple platforms and components in order to generalize to a democratic system. BitCongress is a voting platform composed of three main systems: *bitcoin*, *counterparty* and *ethereum*. In addition, *axiomity* is the in house system created to interface with all the components. It provides the graphical user interface for the user to commit votes, create legislations, discuss amendments and view their voting record. Axiomity as an interface is analogous to a Bitcoin wallet, which provides an interface for your activities in the blockchain.

Similar to a Bitcoin transaction, an electronic vote is defined as a trail of digital signatures where each time one votes, they sign the over the previous transaction and encumber it to the public key of the candidate or the legislation they are voting for. BitCongress uses counterparty to create a custom vote token to be used as an actual vote. In principle this works similar to a Bitcoin however it has further constraints and behaviors in order to fit the democratic model. Counterparty is a financial tools platform allowing users to conduct business, trade and engage in advanced financial contracts that is powered by the Bitcoin blockchain thus making it inherently decentralized. Counterparty works by storing additional data in regular Bitcoin transactions specifically in the `OP_RETURN` opcode of the locking script. Counterparty cannot transact with actual bitcoins thus uses an in house currency, XCP, in order to function. XCP is created by burning bitcoins thus tying their values directly and making XCP usable as a valuable asset. Using counterparty, user can create tokens at the cost of 0.5 XCP per token. BitCongress uses this function to create vote tokens meaning that a voting transaction is a Bitcoin transaction with respective fees incentivizing miners to put them on the BTC blockchain.

An election is defines as a smart contract, a programmatic protocol that facilitates the verification and enforcement of contract terms and clauses. An election smart contract will be a multisignature contract held between voters and candidates/ legislations. It will be running a set of constraints for a defined period of time allowing acceptance of votes using its public key, register and process votes using the voter’s public key and return the vote after the election is concluded. In this system, the voter only possess a single vote over their lifetime. With this system, new vote tokens would not need to be issued after each election eliminating a central body. In order to check voting for nonexistent elections or verifying voters is to be aware of all present and past elections. Thus, elections must be publicly announced and incorporated into a blockchain such that all participants would have to agree on a single history of election order, votes and results. Ethereum is a decentralized platform that solely run smart contracts. This platform consists of its own blockchain and is powered by an asset of value called ether. This asset is used by programs "... to pay the network for resources they consume." [3] Moreover "volunteers earn [ether] by either validating transactions, securing the network." [3] This is similar to a miner in Bitcoin that earn rewards by including transactions in the blockchain thus including elections in the ethereum blockchain would be incentivized as well.

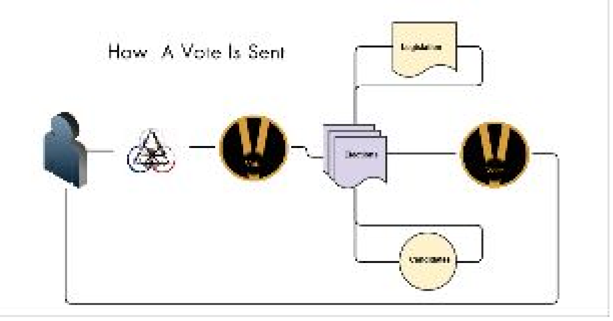


Figure 6: BitCongress voting process

Elections have defined constraints within the ethereum smart contract system. An election will have "an election timed lifespan, set of rules, candidates, legislation, budget & an accessible URL that can be accessed by the public." [1] It will have a public address and can communicate with the counterparty (inherently Bitcoin) blockchain to transfer votes from voter to candidate and back to voter. Votes are transferred to a candidate specific address or in the case of a legislation, a yes or no address. Upon registering each vote, the election smart contract responds by increasing the tally count that is reflected in the axiomatic interface.

A decentralized proof-of-tally is also maintained for each voter that is updated by an election upon registering the voter's vote. This gives a profile for each voter along with their voting history and is used in voter verification. Although a useful concept, the BitCongress specification does not provide details as to how this is exactly implemented. For instance, how is this information maintained throughout the blockchain such that it is easily accessible for verification purposes. Moreover, anyone can register to become a voter through BitCongress allowing them to participate in democratic processes. Each address becomes associated with a system like Blockchain ID, allowing a person to be mapped to only one address. This ultimately requires a centralized authority with identity information to verify a voter and give an address in order to interact with BitCongress.

BitCongress is an ambitious endeavor relying on several blockchain platforms to support a full fledged democratic system. Although it can currently feasible to implement using dependent tools, it still needs to overcome some issues. BitCongress aims to be a large platform to be used for all democratic purposes. However with the current system of linear elections, each voter can only participate in one election at a time, making concurrent elections impossible bringing up issues of scale.

With this decentralized system, anyone can create elections or submit legislations. What is to avoid people from created conflicting elections or legislations such that the two invalidate each other. To avoid this there needs to be a filter or an additional check but with the use of natural language it becomes hard to automate this process. The only way to fix this is to have a third party intermediary, which goes against Rockwell's philosophy of decentralization. Moreover, voter registration absolutely requires a central body because it concerns the issue of real identity. This creates a centralized bottleneck for the decentralized system at hand. Also there is no specific mention of a system in place to avoid voters from sending vote token to other voters, which could lead to problems of fairness.

The BitCongress platform relies on three separate systems in order to properly function meaning that the state of the system is directly reliant on the state of the dependencies. In the event that one of the dependency falls through, the entire democratic platform comes crashing down. There needs to be enough of an assurance that all three systems are sound. This is true of bitcoin and consequently counterparty however ethereum is fairly new thus does not have the same sized network or backing. It would be better to have redundancies in place to avoid this issue such as using separate blockchains with the same data so the entire BitCongress infrastructure would be safe even if one component fails.

Despite these looming issues, using blockchain structures to vote in the BitCongress system addresses a lot of the problems associated with voting such as accountability and auditability as with a public ledger all voting transaction remain public thus we can hold elections results directly accountable to all the votes transacted to the election addresses. Also any attempts to double vote will be checked against by the majority of miners before they include the votes in the blockchain thereby eliminating chances of fraud.

Final Thoughts

While Follow My Vote and BitCongress are interesting and novel approaches to online voting, we think that these schemes for voting on the blockchain are not robust enough to supplant current voting schemes. Firstly, these implementations incur a technical cost in understanding cryptocurrency systems which may represent a bottleneck in adopting these technologies. Furthermore, the proposed systems are riddled with implementation issues and vulnerabilities that may affect the end products. The idea of a complete decentralization is also infeasible considering identity confirmation must occur in any official setting. Verifying users' credentials requires a central authority in order to avoid Sybil attacks on the system.

Many issues also arise when one considers adapting blockchain voting platforms to scale for use in a non-local setting. We think that these tools are instead more powerful in smaller use cases. For instance, a constituency might use Follow My Vote or BitCongress to generate a consensus for their representatives and subsequently hold the representative accountable to represent their views. Using a blockchain as a consensus mechanism has great potential and consequently important ramifications should they continue to be developed. While current proposals are far from perfect, they are a step in the right direction towards cryptographically secure electoral systems.

Sources / Useful Links

1. Ethereum home
2. BitCongress white paper
3. Follow My Vote white paper
4. Follow My Vote YouTube channel
5. UCSB Sequoia evaluation
6. Buddy Tolbert
7. Bitcoin subreddit
8. BitShares subreddit
9. https://en.wikipedia.org/wiki/Sequoia_Voting_Systems
10. https://en.wikipedia.org/wiki/Electronic_voting
11. https://en.wikipedia.org/wiki/Decentralized_autonomous_organization
12. https://en.wikipedia.org/wiki/Sybil_attack