Democracy on the Blockchain

Amany Belay
Computer Science
Harvard College
Cambridge, USA
aabelay@college.harvard.edu

Anthony Kenny
Electrical Engineering
Harvard College
Cambridge, USA
anthony_kenny@college.harvard.edu

Owen Moore Niles
Computer Science, Philosophy
Harvard College
Cambridge, USA
oniles@college.harvard.edu

***Abstract*—This project proposes a digital alternative to the current paper ballot voting system. Our approach relies on a distributed ledger maintained by a network of independent nodes and boasts superior security, efficiency, and transparency relative to the current system. This approach to vote tabulation is advantageous because it is easy to eliminate the influence of malicious nodes, does not rely on physical paper ballots, and fosters trust through transparency.**

***Index Terms*—blockchain, election, network, voting**

I. Introduction

There are a number of flaws with the current system of counting ballots cast during elections that suggest that the current system is not the best solution. Our project proposes a more secure, more efficient, distributed alternative to the current system of counting ballots.

A. The Problem

The main problems that we have identified with the current voting system are that it a) is vulnerable to attacks from malicious individuals, b) wastes significant amounts of resources and energy, and c) is something of a black box.

In the most recent presidential election, voter fraud accusations were plentiful, demonstrating just how afraid Americans are of malicious individuals tampering with their elections. In reality, during the 2016 presidential election, there were only a handful of proven cases of voter fraud, each of which affected the outcome of the popular vote by a single digit number of votes [1]. Though these instances of voter fraud are not terribly concerning, they are proof that voter fraud exists. Furthermore, even small numbers of voter fraud add up. At the time of writing, there are more than one thousand proven cases of voter fraud in the Heritage Foundation voter fraud database [2]. The contents of this database provide still more convincing proof that the current voting system is not as secure as it should be.

Furthermore, the current system does not make efficient use of natural and human resources. Before each election, authorities must print at least enough ballots that they can issue one to every individual who is registered to vote. Once all of the votes have been cast and counted, these ballots are useless. Even if they are recycled, it is impossible to reclaim the energy that was required to produce them in the first place. In the event of a recount, still more energy must be expended to ensure correct election results, making the process even more inefficient.

Finally, voters cannot verify that their votes have been recorded correctly and counted toward the election results. This lack of transparency related to the generation of election results leads some individuals to distrust the government. Concerns that the government tampers with election results may or may not be legitimate, but we decided that a greater degree of transparency is not a bad thing.

B. Background

Ordinary electronic voting machines lack the necessary security for election overseers to have complete trust in them. In 2017, at the Defcon hacking convention in Las Vegas, actual voting machines were compromised in just over one and a half hours. Because of the uncertainty regarding these machines, paper ballots accompany electronic voting machines in most states. In this system, users do not know if their votes have been tabulated. This system is wildly inefficient, in terms of energy, material costs, labor costs, and there is still potential for corruption/human error. The blockchain has been proposed as a remedy for all of these issues.

Bitcoin and other cryptocurrencies have popularized blockchain technology in the past decade. The blockchain is revolutionary because it allows developers to create networks of nodes that reach a consensus about the contents of some distributed ledger. The blockchain allows the contents of that distributed ledger to be not only publicly visible, but also publicly verifiable.

Two companies, Agora Vote and Voatz have already begun to experiment with blockchain-based voting solutions. Agora Vote is a Swiss start-up that allows users to vote from their smartphones. They seek to address voter suppression, election fraud, and high material (paper) costs [3]. The project boasts an and end-to-end verifiable ecosystem in which voters can verify their vote at every step in the tallying process. It claims to be cryptographically secure, allowing individual users to see their own decrypted votes, but no other users.

While it has not been implemented in any official election to this date, the Agora team was able to obtain official observer status in the 2018 Sierra Leone presidential election. They counted ballots at a regional level with election officials, and were able to publish highly accurate election results 5 days before the official count ended.

Voatz is a Boston-based startup that seeks to make it possible to vote in any sort of election from ones smartphone [4]. Voatz relies on the security features like fingerprint/facial recognition in these newer devices, to authenticate voters. They also rely on the hardware-based security on these new devices to store private keys, to allow encrypted transactions to take place over the internet. The votes are then stored on a blockchain, which the election overseer controls. Voatz main goal is to make voting more accessible and convenient, given the fact that most people in the United States own a smartphone.

Voatz has mainly been used for small scale voting, like in town meeting or student government elections. However, Voatz was used in a pilot program for the 2018 Midterm elections in two West Virginia counties. Deployed soldiers were given the option to cast their votes from overseas using the Voatz app, and the pilot was successful.

All of these projects seek to utilize the inherent immutability of a robust blockchain as a way to securely store data. However, using an e-voting service such as the ones that Agora and Voatz provide prompts security concerns. The concerns have particularly focused on the interaction between the user and network, over the internet, which is public and thus inherently vulnerable [5]. If the integrity of a users correspondence with the network (their vote) is compromised, then the whole system loses its integrity. Even in 2018, networks, especially wireless networks, are far too vulnerable to be trusted with data as sensitive as that which is contained on voters ballots.

C. Project Goals

Our goal is to harness the power of modern technology to develop a completely digital platform for casting and counting ballots. We would like to write some simple proof-of-concept software that implements the fundamental logic and protocols to demonstrate that an entirely digital election solution is possible.

II. Proposed Approach

In order to create an alternative voting system with enhanced security, efficiency, and transparency, we plan to leverage a blockchain- based approach. We will take advantage of the built in security and transparency properties of blockchain technology, the efficiency of modern computing hardware and well-written software to solve all of the problems that we highlighted with the existing system of counting paper ballots.

We will develop our solution while operating under a small set of assumptions. Namely, we will assume that all of the cryptography, voter identification, and networking is done for us. Our implementation, then, will not be a full client, but only the core logic that a full client would extend if our project were to be deployed in the real world.

A. Secret Weapon

The blockchain as the basis for a distributed ballot tabulation system is our secret weapon. By making the blockchain the basis for an alternative voting system, we take advantage of the distributed and generally open source nature of blockchain protocols and software respectively. These distributed and open source qualities solve the problem that the current system is something of a black box. Provided that we can prove that our software and protocols are correct through rigorous testing, the simple fact that the entire system is digital solves the other three problems.

B. Intellectual Points

The distributed nature of this approach distinguishes it from the systems of election administration that we are used to. Traditionally, the centralized entity responsible for tabulating votes cast during an election is the organization that is holding the election in the first place. We propose the voters who participate in elections should be the ones responsible for verifying the vote totals. This would add an unprecedented amount of transparency to the election process that could help foster trust between voters and the organizations that are holding elections.

A major difference between our project and Agora's and Voatz's solutions is that our approach will still require voters to travel to polling locations and vote in person. We do not plan to develop any mobile applications for voters' personal devices to allow them to vote from home. Instead, our distributed voting software will run on each node in a network of special voting machines that are owned and operated by the organization who is holding the election (e.g. the government).

Even though the government will own and operate voting machines, we will achieve our goal of transparency by publishing both the blockchain of ballots and the software that each node runs online. When the blockchain itself and the software used to generate it are publicly available online, every voter can verify not only that his or her vote has been recorded correctly in the blockchain, but also that the votes in the blockchain are tabulated correctly.

The motivation behind our design decision to use proprietary nodes running open source software was that we wanted to address concerns about wireless network security that we discovered during our research. Although voting from a mobile app will almost always be more convenient than travelling to a polling location to vote, we believe that by increasing the density of polling locations, we can still make voting more convenient and accessible that it currently is, especially for those who live in rural areas. This solution also does not introduce any wireless security vulnerabilities into the conversation.

C. Success Criteria

Given the complexity of implementing a fully functional e-voting system immune to all sorts of attacks, we will limit the scope of our experiment. We seek to establish a blockchain implementation that will successfully protect against duplicate votes and faulty or tampered with voting machines.

Put succinctly, we will judge the success of our project on the following criteria:

1) A fully implemented, distributed blockchain network of nodes that simulate voting machines
2) Good nodes run software that will reject duplicate voters and thus not add those blocks to its chain.
3) Network will reject invalid blocks added to chain by Bad nodes

III. Implementation

A. Blockchain Structure

We modelled our blockchain as a distributed network of nodes, where each node would be a single voting machine. Each node, or voting machine would then run the blockchain software, add blocks to the chain as ballots come in, reach a consensus on new blocks added, and validate the chain.

For simplicity, there is one ballot per block of our blockchain. Each block also includes the time of its creation, the hash of the previous block in the blockchain, and a random *nonce* that changes the hash to match the proof of work difficulty.

B. Adding a Block

When a voting machine receives a new ballot, it will run the following three checks before approving the ballot and announcing that it has added a new block to its chain.

1) Is the block being added onto the end of the chain?
2) Is the proof of work valid?
3) Finally, is this the first ballot that this voter has cast?

This procedure runs both before the voting node adds this block to its chain and announces that to the network, but by every node in the network when a new block is announced. In this way, the network is protected against faulty or malicious nodes as long as the number of good nodes outnumber the bad ones (which is a fair assumption, given the unlikeliness of a majority of voting machines becoming compromised).

C. Submitting a Ballot

In addition to the checks listed above, the node submitting the vote must also compute a proof of work function that is difficult to compute, but trivial to verify. This proof of work prevents malicious nodes from spamming the network with invalid blocks or iterating over the entire chain and recalculating hashes in order to propagate a false version of the chain.

Our proof of work function is based on the one that most cryptocurrencies use. The hash of every block must satisfy a certain “difficulty” requirement. Specifically, the block’s hash must start with at least n 1’s, where n, the difficulty, is a nonnegative integer. The node must repeatedly choose arbitrary *nonces* until the new block’s hash satisfies this requirement.

IV. Results

Based on the results of the test that we wrote:

1) Our implementation will successfully simulate an election.
2) With all nodes being ”good”, every node shares the same chain.
3) A good node will not allow for duplicate votes to be added to the chain, and will reject them without even submitting the invalid chain to the network for consensus.
4) Finally, if a ”bad”, or malicious, node submits an invalid chain to the network, the rest of the nodes on the network will not accept the invalid chain.

Our code base is available on GitHub at https://github.com/owenniles/voting.

V. Conclusion

Based on our test results, we concluded that our code is a successful proof-of concept implementation of a blockchain voting platform.

A. Key Takeaways

We learned that blockchain theory fits a diverse range of applications. At first, it was difficult to see how we could use blockchain technology as the foundation for a new voting system, but once we understood that the blockchain was not solely applicable to cryptocurrencies, we realized that it was applicable almost any time there is a record that needs to be stored in a decentralized manner. The flexible nature of blockchain theory is partially responsible for its popularity in computer science.

B. Future Work

If we had more time to work on this project, we would have liked to run tests on a more complex simulated network. We also noticed that when we were running tests on simulated networks with more nodes, the tests ran increasingly slowly. This could be due to the fact that we were simulating the entire network on a single computer, but it is also likely that our implementation is not the most efficient solution and that we would need to refine it before deploying it at scale.

If our solution were to be deployed in a real world election, specialized voting machines would have to be manufactured. It would be interesting to explore what, if any, economic consequences would result from the production of these voting machines. What kind of new hardware markets would open up? How often would these machines need to be updated in order to patch hardware security vulnerabilities? It would be important to answer these questions before deploying our project in the real world.

References

[1] https://www.washingtonpost.com/news/the-fix/wp/2016/12/01/0-000002-percent-of-all-the-ballots-cast-in-the-2016-election-were-fraudulent/?noredirect=on&utm_term=.f87baac4c97b

[2] https://www.heritage.org/voterfraud

[3] https://static1.squarespace.com/static/5b0be2f4e2ccd12e7e8a9be9/t/5b6c38550e2e725e9cad3f18/1533818968655/Agora_Whitepaper.pdf

[4] https://voatz.com/faq.html

[5] https://www.cnet.com/news/blockchain-isnt-answer-to-voting-system-woes/