Viability of the Usage of Blockchain Technology in Electronic Voting

Colin Waldron
A Term Project for CS:4980:0004 Spring 2020, Electronic Voting at the University of Iowa
This Version is Intended for Public Distribution

5/15/2020

1 Introduction

Electronic voting has been a hot topic for many years now with people constantly proposing new methods to approach the societal shift towards personal electronics use. Research shows that 81% of Americans own a smartphone and 90% use the internet [1,2]. There are over 9000 public libraries in the US meaning that access to computers and the internet are now a very interlocked part of daily life [3]. With many Americans working 9-5 jobs it can be difficult to fit voting into their busy schedules even with poll locations being open for long hours. Polling location distance matched with a lack of time/desire to travel to voting means that votership often is much lower than we would expect. For the last 100 years we have not seen higher than a 65% voter turnout for the presidential election and a shockingly low 55% for midterm elections [4]. The recent failures of electronic vote tallying and reporting systems seen in the Iowa Democratic Caucus and subsequent usage of paper backups proves that there is still no clear system that fits the rigorous needs of an large scale electronic voting system. The impact of failures such as this result a lack of confidence in the system which can drastically worsen trust in the outcome of an election. For the sake of modern Democracy, it is should be a priority to find a solution that both fits the needs of the American public as well as the legitimate concerns regarding electronic voting. The goal of this paper will be look at Smart Contracts and Blockchain as potential implementation strategies for secure electronic voting.

2 Background

To start, it is important that I begin by addressing "What is blockchain?" Blockchain is a type of distributed data ledger system in which digital events are recorded as blocks, which connect to form a history from a Genesis block. Each block contains two main components, the list of events and the Block Header. The Block Header contains: the cryptographic hash of the previous block, a timestamp of when the current block was hashed, the difficulty of the

block and a nonce. The difficulty is scaled as a function of speed at which blocks are being added to the network to try and fit the goal of adding six blocks per hour. The nonce is the number that when plugged into the SHA256 hash function, results in a hash with a certain amount of leading 0's [5]. This is important to note as once the block has been broadcasted, everyone can take the nonce and verify that the hash is correct. The intention of the system is to have a mutual trust between many distrusting peers. It should be noted that the most well known implementation of blockchain is in the form of cryptocurrency financial systems like Bitcoin or Ethereum. These are both examples of public, open source, distributed computing platforms that act on a multi-owner chain. A multi-owner chain is characterized by management by a peer-to-peer network that collectively adheres to a protocol for communication and block validation. In the context of financial systems, individuals are incentivized to validate blocks by having a validation fee distributed to them as a function of the compute power that they provide. This works to provide flow in the system, fees fluctuate with the current hash rate available and how high others are willing to pay to get their transactions verified first.

For the purposes of this paper, I will assume the usage of a single-owner or private chain which is a simplified form of the discussed implementation above which in the context of this paper would be operated by the Election Agency or a contractor. In the case of a private blockchain contractors and the Election Agency can work as a checks and balance system that a regular single-owner chain fails to answer. Of course this implementation has concerns of its own which will be discussed. I also make the assumption that the tally occurs and all votes are released after polling places have closed as to not influence differing time zones given a federal election as well as waiting until poll places close in state elections. This is to recognize the fact that disenfranchisement of West coast and Hawaii voters that have other regions results released before they have finished voting.

3 Critiques of Blockchain Voting

Blockchain usage for the purposes of electronic voting has a large amount of critique as a hyped up system that is an attempt at being a catch all solution to security issues. I will attempt to address the most commonly mentioned points of contention but there are bound to be others that I have missed. It should be noted that voting itself is a rather complex system and for it to be fully successful, the lack of in person verification adds levels of complexity that would be inherent in most electronic voting systems.

The first point I will introduce and functionally one of the most important in terms of skewing elections is the difficulty in verifying voter identification. To ensure that fraud does not occur, each individual must only have access to their own vote. Most common proposed solutions to identification have their own issues from drivers license to SSN, both predictable number schemes and have been abused previously [6]. Databases of personal information are limited on a federal level and things like finger prints are not filled in for most individuals. The notion that authentication of identity is uncertain makes electronic voting a difficult task given the status quo. Blockchain does not provide a unique solution to this problem that

exists for all forms of electronic voting. The second major point to the failures of electronic voting that blockchain fails to solve is that there exists no paper ballot for auditing. Paper ballots are the current system that acts as backup and as mentioned in the introduction, are key in the case where things go wrong infrastructure of otherwise. Although a receipt of vote can be generated, the same concerns of spoofing votes applies to spoofing receipts.

In this next section I will discuss the vectors of attack specifically for a permissioned blockchain. Specter, Kopper, and Weitzner wrote a fantastic paper discussing the security standpoints of Voatz which was the first internet voting application used in US federal elections [7]. It should be noted that Voatz mentions they use a permissioned chain but there is a distinct lack of public knowledge about how their system actually works, they seemingly use a serious of buzzwords to describe the security of their model. Regardless, Specter et al makes a fantastic point about the risk of API server being compromised. Given that the interaction required for voting by the public, the process would need to be wrapped in a simple non-tech savvy approach. This means that there will more than likely be an API server handling all requests from the app to the blockchain meaning that if a bad actor had access to said server, fraudulent votes could be published to the chain without the need of a 51% attack or anything related to the blockchain. Additionally they bring up the point of a potential malware attack controlling users devices and posting votes directly through their devices. Considering the infrastructure of how devices would need to communicate with the API server or a man in the middle attack could potentially rewrite packets or even simple sniff the packets and publish results for an election early, thus influencing the outcome.

A short note that should be included on a lesser technical level is a question of stake and potential opponents. Park et al raises an interesting point that often these two parties overlap in voting systems [8]. If we look to the example of voting systems created by an outside contractor, the one that led to failure in Iowa had received funds from various politicians. Even if they are not bad actors, the question of potential fraudulent action brings down the confidence of the voter. A very resounding point is that a voting system has to convince supporters of the losing candidate that the system is honest.

4 Proponents of Blockchain Voting

I would like to note that many of the people offering critiques of blockchain voting were also proponents and still defend parts of the technology but conclude that it is not an end all be all solution to electronic voting. It is interesting that many defenses of blockchain voting discuss the technology of blockchain but sort of fail to answer the indicts of electronic voting systems as a whole.

To start with, Voatz themselves released a blog post that responds to Specter, et al indicts of their system [9]. They list a few points but I will summarize them, first the paper is based on a review of an old version of the app itself which was not used in an election. Voatz offers a public bug bounty program to increase the quality and security of their product. They note that the researchers were unable to spoof a legitimate voter or receive a ballot through

the real Voatz servers. They have ran nine pilot elections with less than 600 voters which were conducted securely.

One of the commonly touted points in support of blockchain technology is the immutability of data. A 51% attack is not possible given a permissioned or single chain system. Dan Wallach notes that "Blockchains do turn out to be incredibly helpful for verifying a "counted as cast" property, because they force everybody to agree on the exact set of ballots being tabulated. If an election official needs to disqualify a ballot for whatever reason, that fact needs to be public and everybody needs to know that specific ballot, ..., otherwise the cryptographic math won't add up." [10] It should be noted that Wallach is also a critique of blockchain voting and this quote is taken from an article that concludes that although blockchain is useful for building voting systems, it does not satisfy the multiple other properties he mentions.

A proposal by Lopes, et al goes through some of the critiques that are mentioned above [11]. In terms of authenticity "every user of the network is identified by a public key, which can only be accessed by its own private key. Assuming that every voter will keep its own private key secret, then the authenticity requirement is fulfilled". They note that in terms of anonymity since every user has a public key and the stored vote is encrypted its impossible to associate a vote with a voter. In terms of auditing, every node in the network can audit the blockchain and verify that the hashes match. It should be noted that within their proposed solution, they include an API layer that communicates with a cryptographic server and the blockchain, "For each request made in the interface, it will interact with the encryption server by server calls to encrypt, decrypt or add votes." They also mention that in their implementation, the user must have ether in order to form contract and vote.

5 Conclusions

My original intention when reading through the literature was to write a paper about smart contracts and their implementation as a solution to electronic voting. After reading through the critiques and seeing the subsequent responses, couple with the fact that many critics were originally proponents signals that blockchain is not the solution I was looking for. The Lopes, et al paper in particular uses smart contracts in a similar way that I was originally thinking of writing it but fails to address simple critiques like attacks on the API layer in addition to the requirement of needing ether to vote. Many blockchain proponents either spend the majority of their paper talking up the technology and spending little time addressing the primary concerns of electronic voting principles or they simply don't recognize the failures of layers that need to be built on top of blockchain for it to succeed. I think Wallach summarizes it best in that it is a useful tool, but it is not a solution that address all of the concerns.

I would like to note some of the limitations to the Lopes, et al paper as they spent little time working out the details of the fundamental electronic voting concerns. Namely, in the section on anonymity they discuss a public and private key but thinking about how to distribute

those keys that are also verifiable is nearly impossible. While researching this subject, nearly all data the government has on all of its voting individuals are unsecure, predictable, and have been used fraudulently before.

The common notion of immutability of data only matters when the data entered originally is verified and guaranteed non-fraudulent. The case of a public peer-to-peer blockchain opens up the possibility of interactions by bad actors that have proven themselves to engage in elections. Notably, Russia is currently repurposing an old city to mine bitcoin right now, meaning that they would have the compute power available to reasonably attempt a 51% attack. That coupled with the lack of validation fees that would be presented to the public, the chain most realistically would have to be private or permissioned. With that assumption, look to the previously mentioned point that operators of said network have the potential to influence elections and the resulting destruction in confidence.

Ultimately, I have changed my opinion on the feasibility of blockchain technologies to solve electronic voting. The failure to address fundamental problems does not make the solution bad, but rather incomplete. I imagine in the future if a solution ever occurs, there will be a reminiscent ledger/verification system similar to blockchain technology but for now, it fails to solve.

6 References

1. "Demographics of Mobile Device Ownership and Adoption in the United States." Pew Research Center: Internet, Science and Tech, Pew Research Center, 12 June 2019, www.pewresearch.org/internet/fact-sheet/mobile/.

2. Anderson, Monica, et al. "10% Of Americans Don't Use the Internet. Who Are They?" Pew Research Center, 22 Apr. 2019, www.pewresearch.org/fact-tank/2019/04/22/some-americans-dont-use-the-internet-who-are-they/.

3. "LibGuides: Number of Libraries in the United States: Home." Number of Libraries in the United States, American Library Association, 14 June 2019, libguides.ala.org/numberoflibraries.

4. FairVote.org. Voter Turnout. FairVote, www.fairvote.org/`voter_turnout#voter_turnout_101.`

5. Marshall, Blair. "How Are Transactions Validated?" Medium, Medium, 4 June 2018, medium.com/@blairlmarshall/how-do-miners-validate-transactions-c01b05f36231.

6. Jefferson, David. "David Jefferson: The Myth of 'Secure' Blockchain Voting." Verified Voting, 3 Oct. 2018, www.verifiedvoting.org/`jefferson_themythof_secure_blockchainvoting`

7. Specter, Michael A. et al. "The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections." (2020).

8. Park, Sunoo et al. "Going from Bad to Worse: From Internet Voting to Blockchain Voting." (2020).

9. Voatz. “Voatz Response to Researchers’ Flawed Report.” Blog @ Voatz, Voatz, 13 Feb. 2020, blog.voatz.com/?p=1209.

10. Wallach, Dan. “Blockchains and Voting.” Freedom to Tinker, 12 Sept. 2017, freedom-to-tinker.com/2017/09/12/blockchains-and-voting/.

11. Lopes, Jorge et al. “Blockchain Based E-voting System: A Proposal.” AMCIS (2019).