Votechain: Voting by Blockchain

Daniel Cox
Harvard University
Cambridge, MA USA
daniel_cox@g.harvard.edu

Chiara Darnton
Harvard University
Cambridge, MA USA
cdarnton@college.harvard.edu

Christopher Kinyua
Harvard University
Cambridge, MA USA
christopherkinyua@college.harvard.edu

Mahdy Al Majed Yassine
Harvard University
Cambridge, MA USA
myassine@college.harvard.edu

***Abstract*— Trust in the voting process is essential for a democratic government to operate with smooth transitions of power. Recent events suggest the need for a new voting system that engenders more confidence in the accuracy of the finally vote tally. We propose here a new form of blockchain electronic voting that could fulfill this need.**

Keywords—vote, blockchain, election, government

I. INTRODUCTION

As is evident from the recent US presidential election of Nov. 2020, trust in the voting process is essential for a democratic form of government to operate without unrest. We see this in the various claims of fraud by supporters of President Trump, who did not accept the legitimacy of the vote count in swing states. Regardless of the merits of such claims, the situation would be much improved if all vote counting was beyond reproach.

II. PROBLEM TO SOLVE

From the recent events mentioned above, it is clear that public trust is highly desirable for an election system. Moreover, in a democratic country it is also extremely important that an election system minimizes disenfranchisement by making voting easy and widely available to all citizens. With these two primary goals in mind, trust and accessibility, we propose a design for a secure, blockchain-based, electronic voting system. The system will record votes on blocks that are chained into a blockchain "Votechain". Cryptographic techniques including hashing and asymmetric keys will prevent vote tampering and validate and protect voter identities. The chain will be easily queried for vote tabulation by governmental agencies and the public, and a distributed network of both government and private nodes will discourage government-based fraud.

III. PROPOSED APPROACH

The use of blockchain technology for electronic voting is not a novel concept and has been widely criticized as impossible to secure.[1] Our novelty is not in aiming to create a theoretically perfect system, but in prioritizing problems to address in order to improve on the trust and accessibility of the existing system. In particular, we address the problem of top-down government corruption, which is seldom addressed in designs of blockchain voting systems.

A. *The problem of government-based fraud*

The issue of government corruption is of great interest to the general public but is difficult to address. In particular we envision fraud by

1) *an individual, bad-acting government official,*
2) *a government entity that controls the entire election system.*

A typical solution to (1) is to record votes redundantly in multiple places so that a bad actor at any one place will have little influence over the final result. When blockchain technology is used, this typically involves the use of multiple nodes on a distributed computer network. For example, in the Voatz system used by West Virginia for overseas voting in 2018, 32 nodes were used [7]. Such nodes, however, do not address the possibility of top-down fraud (2). Regardless of the number of government nodes, if a single government entity controls all nodes then the system is still amenable to top-down fraud. We address this potential source of fraud with a system that uses a mixture of government and private nodes.

B. *Evaluation metrics*

We have identified several essential requirements of an electronic voting system, which we will use to evaluate our proposed design. The system must be

1) *easy for voters to use,*
2) *confidential,*
3) *secure against vote tampering,*
4) *secure against voter coercion and selling,*
5) *open to public audit,*

6) *scalable to a large population,*
7) *insulated against government corruption. [2]*

IV. Intellectual Points

This project is exciting because it tackles a problem that defines the political landscape of the world. Real and imagined election rigging has made it clear that truly democratic elections are hard to achieve in a centralized system. The advent of blockchain has shown that orderly and trustworthy elections are possible without a centralized system, as long as appropriate mathematical and technical principles are applied.

But how do you conduct an election without a central entity controlling everything? How do you build trust in such a system? How do you ensure the system is more secure than physical ballots, while also improving accessibility?[3] These are some of the key questions that have made researchers question the viability of internet voting, and they are the ones that we tackle in this project.

The work of blockchain pioneers like Satoshi has provided powerful building blocks (trust machine, end-to-end encryption, digital signatures, etc.) that we hope to use to achieve the elusive goal of secure, trustworthy, and accessible democratic elections.

V. Work Performed

After surveying the literature on electronic and blockchain-based voting, we identified strengths and weaknesses of previous systems and used these to outline a system that addresses the most pressing concerns of blockchain-based voting. A prototype for the software that is needed for our proposed system can be found here (Votechain code) The system consists of the following components:

1) *Voter registration*: We consider the process of voter registration beyond the purview of our project. However we imagine voters will register using an existing voter registration system, and upon registration will be given a one-time-use access code to a central server where they will acquire a public/private key pair. The public key will be published as part of an official voter roll.

2) *Vote casting*: To cast their vote, a voter will access a government election server via a secure website, enter their public/private keys and a password of their choice, and then fill out a ballot with their choices of candidates. This information will form a voting transaction block with a signature (made by encrypting the voter's password with their private key), the voter's public key, a timestamp, and an sha256 hash of the data in the block, excluding the public key.

3) *Vote recording*: The central election server will broadcast the voting block to all nodes in the election network, which will each validate the block (as outlined in the next section). Once all nodes have received the block and checked the hash, the voter will receive an receipt from all nodes indicating that their vote block was not tampered with before submission to the nodes. To prevent voter coercion, voters can re-vote at any time before the end of the voting period, and the final tally will only reflect the most recently cast vote blocks. [5]

4) *Vote validation*: Upon receipt of a vote block, each node verifies that (1) the public key is on the official voter-registration roll, (2) the signature is valid (the password is recovered from the signature with the use of the public key), (3) the timestamp is before the end of the voting period, and (4) the hash is valid (rehashing the entire block produces a hash that matches the one on the block) to ensure the data in the block was not tampered with. Once validated, the block will be added to the node's vote-chain.

5) *Vote tallying*: The vote-chain will have built-in methods for vote tallying and the above vote block validations. Vote tallying will be done homomorphically so that no individual vote block will be decrypted. After the election, the vote-chain of the node with the longest valid chain will be declared the official vote-chain and published on a publicly available government website, with the public keys stripped from each block to ensure voter confidentiality. Any voter could then verify the validity of the blocks and the final tally of the official vote-chain.[5]

6) *Node network*: The use of multiple government nodes insulates the system against a single bad actor at a node who might fail to record a vote or alter it before it is placed in the vote-chain, as this would then render that node's chain invalid. For a national election, fifty or more government nodes would be used per state, each run by a local county office. Fewer nodes would be required for smaller elections, but we consider ten physically separated government nodes a minimum requirement, as we consider that many sufficent to guard against collusion between all nodes.

As discussed above, however, a system of solely government nodes does not protect against top-down corruption. To address this, larger elections would require a set of private nodes, equal in number to the government nodes and with the same functionality.

These nodes will be controlled by private citizens selected from a large pool of applicants. The selection process will be random, independently monitored, and won't take place until the election, making it difficult for any central authority to anticipate and control all election nodes.

VI. Results and Discussion

A. Strengths

Our proposed system satisfies our general goals of improving trust (by increasing transparency and accountability of the vote) and accessibility (by creating an electronic voting system available to any registered voter with internet access). The system also fulfills many of our stated requirements at the start of this paper. (1) It is easy to use because voters only need access to their voter registration information and a personal computer with internet access. (2) Confidentiality is ensured because vote blocks don't contain any personally identifiable information, and even if a voter were tied to their vote block, no individual block is decrypted during vote tallying so their ballot would be confidential. (3) Hashing at each stage of the process ensures that votes will not be tampered with. (4) People can only vote with a valid public/private key pair, rendering identity theft difficult. Re-votes allow voters to invalidate any coerced votes and malicious actors cannot verify that voters have voted a specific way, because the published vote-chain doesn't contain information linking a particular voter to their vote. These provisions make the system more secure against voter coercion than the existing system. (5) Anyone can audit the published vote-chain to confirm the validity of votes blocks and the official tally. (6) Provisions for the number of required nodes ensure that the system scales to a large population. Finally, (7) the system is protected against top-down corruption because of public audits and independent nodes.

B. Weaknesses

The main weakness of our Votechain system is the same as is common to all electronic voting systems: the security of the voter's ballot between the point where it is entered into his or her computer and the point where it is broadcast to all nodes. One could imagine malware running on the voter's personal computer that alters the voter's ballot before it is sent to the central server, or malware on the central server that alters the ballot before it is broadcast to all nodes. Such attacks, however, are mitigated in our system through the use of receipts sent back from all nodes to the voter confirming his or her vote was recorded correctly. Any changes would thus be evident in these receipts. Another possibility is that there might be a denial-of-service attack on the central server, such that voters find they cannot cast their vote. The potential for such an attack, however, could be mitigated via a variety of common security measures including: using SSL encryption, having a firewall between the public and the private parts of the server, using intrusion prevention software to monitor login activity, and using multiple servers such that, if one is attacked, traffic can be diverted to the others.

VII. Related Work

We conducted several case studies on previous attempts at internet voting, most notably the Estonian digital elections and the elections conducted by the company Voatz. To date, the Estonian elections are widely accepted to be the only successful large-scale implementation of digital voting. [5] However, the elections are controlled by the government, which develops the software and conducts the elections, requiring a great deal of trust in the government that is not present in all countries. Trust has also been an issue in Voatz's blockchain-based elections, where all nodes are government-controlled [7]. We identified several other flaws in these election systems during our research, all of which we considered when designing our system. [1]

VIII. Conclusion

We have presented here a new design for a blockchain-based voting system. Our system meets the criteria generally deem essential for this type of technology. It is easy to use. It is secure against vote tampering and voter coercion. It is open to public audit. It can be practically implemented at a reasonable cost. It scales well with election size, and importantly, it is resistant to government corruption, more so than previous designs. We believe the use of such a system would increase the confidence voters have in election results, and we hope to see such systems tried more frequently in the near future.

REFERENCES

[1] Park, Sunoo, et al. "Going from bad to worse: from internet voting to blockchain voting." (2020).

[2] “Blockchain Electronic Vote”, Handbook of Digital Currency, pp 453-461

[3] Juels, Ari, Dario Catalano, and Markus Jakobsson. "Coercion-resistant electronic elections." Towards Trustworthy Elections. Springer, Berlin, Heidelberg, 2010. 37-63.

[4] Meter, Christian, et al. "Tor is not enough: Coercion in Remote Electronic Voting Systems." arXiv preprint arXiv:1702.02816 (2017).

[5] Vinkel P. (2012) Internet Voting in Estonia. In: Laud P. (eds) Information Security Technology for Applications. NordSec 2011. Lecture Notes in Computer Science, vol 7161. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-29615-4_2

[6] Furukawa, Jun, Kengo Mori, and Kazue Sako. "An implementation of a mix-net based network voting scheme and its use in a private organization." Towards trustworthy elections. Springer, Berlin, Heidelberg, 2010. 141-15

[7] Moore, Larry, Sawhney, Nimit. "Under the Hood: the West Virginia Voting Pilot”. White paper from Voatz Inc. (2019).