VTC: Digital Elections

Raymundo Beristain-Barajas, Anton Rotter-Siere, Kevin Tran,
Graciela Valencia, Reed Wirthman

ECS 198: Cryptocurrency Technologies
Spring 2016

Executive Summary

Elections have been used for centuries as a way of organizing government. However, there has been little progress in their voting systems. Essentially, votes are cast and counted on paper, which leaves much room for error and manipulation. This method is still used today, which gives rise to serious concerns. Blockchain technology offers an alternative solution to voting, which resolves many of the shortcomings of paper and pen voting systems. The following paper will describe Votecoin, an alternative voting system inspired by the bitcoin protocol. It will discuss its strengths and weaknesses, as well as its potential to disrupt traditional voting systems.

Introduction

Democratic elections are prone to miscounts and human error, which could change the outcome of an election. American citizens must place trust in the election offices during the election cycle, many who have subtle biases for a particular candidate. This represents a conflict of interest that can easily be resolved with alternative voting systems. Not only that, but running polling booths can be expensive. Given the size of the United States, taxpayers could potentially save a lot of money from not using polling booths in cities. We propose a digital election system, designed to place *trust* in cryptography and not any given individual or organization. Utilizing blockchain technology, it is possible to implement an immutable and transparent voting system, free of the errors and downfalls of traditional voting systems. It could replace polling booths so that all vote verifying is done automatically, without the need for human counters.

Our proposal is a decentralized network of voters and verifiers, incentivized through a cryptocurrency named votecoin (VTC). This cryptocurrency will be awarded to participants of the verifying network of computers, working on adding and maintaining a ledger of votes during an election cycle. Votecoin would also function as a normal cryptocurrency when there is otherwise no elections, so the ledger would also contain transactions.

Background

The 2000 Florida election recount is a prime example of the problems in the current voting system. The level of inefficiency not only cost money to american taxpayers, it also shifted the presidential election in a major way. Traditional voting systems cost too much money, and they

require too many resources (volunteers, traffic, time off work). This atmosphere prompted our group to design a solution that can address many of these problems, and even add more features not possible today. In essence, Votecoin renders recounts obsolete, given the immutable nature of the voting system, and it ensures that events such as the Florida recount are not repeated.

Proposal

Votecoin operates similarly to bitcoin. It utilizes a proof-of-work consensus algorithm, specifically SHA-256 to enable merge mining for VTC and quickly secure the digital election system. The incentive structure is centered around a new cryptocurrency that will be minted and distributed to the network of verifiers. The difficulty of the work required is dependent on how many people are trying to solve a block. Where it differs from bitcoin, is in the block time and currency cap. The block time will be shortened to 1 minute, which will increase the block confirmation quantity required for a “verified voted”. There is no currency cap, or transaction fee in this proposal. The reasons are many, but most importantly, to eliminate tiered and preferential votes. As a democratic election alternative, Votecoin emphasizes the importance of equal priority to all voters, regardless of their backgrounds.

Because of the dual purpose of the votecoin protocol (voting and currency), there will be two main types of transactions, votes (V) and transactions (TX). TX’s will have the ability to contain transaction fees to prioritize certain important transactions, at the discretion of the spending party.

In order to prevent multiple votes, each qualified citizen will receive a voting ID, coupled with a secret and public key, which will be tied to a personal ID (such as SSN, or Driver’s License). This ensures that only the individual with the appropriate secret key can digitally sign their vote once their vote is cast. Verifiers do not require a voting ID, they only require a public key and private key for signing the blocks they solve.

This proposed solution, eliminates the need for recounts, and can track elections in real time. The older the vote, the more confidant the network can be that it is a valid vote, and the voter has not attempted to vote twice.

Potential Problems

There are still the current problems with a typical cryptocurrency. For a starting cryptocurrency, one problem is that the currency has little or no value. Since there is no demand for VTC initially, many vendors would not consider it as a valid form of payment, even with a large quantity. Another problem with conventional cryptocurrencies that is evident in this cryptocurrency is how specialized hardware can make it impossible for other verifiers to solve a block. This creates a computing power race, which is usually solved by people combining their computer power in a group, and distributing the rewards accordingly by how much computing power each person contributed. Having people group together to solve a block defeats the purpose of a decentralized currency.

This cryptocurrency would require the cooperation of any government or organization that wishes to use it. VTC requires a secure connection from the voting program to the organization's ID database, to verify that the voter is unique. Not all organizations will cooperate with this. Maintaining the security of the connection from the program to the organization will require work on the organization's end.

Potential Solutions

There are few solutions to the value of a cryptocurrency, other than merchant adoption and consumer use. The organization could sponsor the currency, and say it is equivalent to some monetary value in their organization, but this will only make the currency valuable to people verifying from that organization. There are potential solutions to the problem of ASICs, or specialized hardware that can limit, and therefore centralize, the network of verifiers. Switching to an alternative mining algorithm (proof-of-stake, or lottery-based) can mitigate this problem, but they also create additional concerns. We could also limit the number of hashes a verifier could do per day, but that would require a unique ID for every verifier, and that would defeat the purpose of it being a decentralized currency.

Conclusion

Votecoin solves the problem of trust in traditional voting systems by creating a cryptographically secured, immutable record of all votes. Additionally, Votecoin is more resilient to attacks, human error, and corrupt actors than the current voting systems, as the network is decentralized and there is no central point of attack. However, there are difficulties which we are currently looking to resolve. That said, votecoin has the potential to disrupt traditional voting methods, which are ridden with problems that could be mitigated through blockchain technology. Placing trust in a decentralized network of voters and verifiers eliminates human manipulation and fraudulent behavior. In addition it saves resources and money, and could eliminate the obstacles to voting that many citizens face during an election.