Coin-Vote

Version 0.1
Sunday, 21 June, Year 7
funkenstein the dwarf

Abstract:

Coin-vote is a voting system for establishing opinion and resolving disputes amongst willing participants. Rather than using a traditional method of trying to tally one vote per person, it relies on a one vote per coin tally. This enables votes to be counted with provable security, as there are no longer the usual issues of identity fraud, counting fraud, or polling bias, which have plagued traditional polling systems. This document is meant to explain our platform and database for conducting coin-votes. We outline here security procedures and motivation for using the coin-vote system.

Introduction

Attempts to tally public opinion date at least as far back as 2500 year old Athens, but doubtless further. We won't review here the history of voting, polling, and opinion gathering, other than to note that we are seeing today a remarkable change in some of our technical abilities to conduct polls. The communications revolution ushered in by Claude Shannon and electronic computer networks have enabled new weapons in this theater. The proof of work network of a public coin is itself is a voting system of sorts, in which the ledger is decided by a plurality of hashing power.

Online polls are familiar to most internet subscribers today. These polls attempt to determine public opinion by requesting interested parties to perform some action (such as a following a link, performing a captcha, or otherwise registering their vote). The system we describe here is no different in that regard. The action required of the voter in our case requires using bitcoin. It is vastly different in one important regard: it is not falsifiable.

Procedure

A poll question and answer selection is initiated in the coin-vote system and established in our database. Now anyone can submit their opinion on the poll question. No login or identification is required: only that a certain amount of coin is selected as the coin which “votes” on the poll in question. A would-be voter selects the question to vote upon, and sees the current status of the vote.

Then, the voter selects their choice. The voter is given a string unique to the question and the vote choice, which they must the sign using their key which controls one or more unspent outputs (UTXOs). The signature, performed with the digital signature algorithm of the coin just as a transaction is signed, is another string. The signature is submitted to the database, where the validity is checked, and if it passes the checks – the vote is registered and the tally altered to reflect it's weight. The weight is the amount of coin. Votes can be made using the sum of all UTXOs present in a single bitcoin address, or with a single UTXO. The reason for allowing this freedom to the voter will be made apparent in the discussion of security concerns. In no case is any coin spent in the voting procedure; all vote submissions are free of charge.

Traditional security concerns

One common way that online polls are compromised is that a voter can return and place a bet again, using another identity. This is the *Sybil attack*. With coin-vote, every vote must have a fresh coin. Without real limited bitcoin, a voter is provably unable to vote, just as a person without bitcoin is provably unable to spend. Voting identity is in this case cannot be counterfeit in exactly the same way as the units of bitcoin annot be counterfeit.

Another common way that online polls are compromised is that they are *adjusted* by their purveyors. There are many reasons a poll purveyor might adjust the results; the imagination of the reader is likely sufficient to determine them. For the case of coin-vote, the total list of all votes is available to the public and every vote can be verified. Therefore, the list cannot be compromised. There is no way to add votes to a poll, because every vote must be from a unique bitcoin. Removing votes could be accomplished, however if this were done the voter who's vote had been removed could easily divulge their vote and demonstrate to the public that the poll had been compromised. With coin-vote, there can be no hidden inside job.

Yet another common security concern in conducting a poll is *intimidation*. For this reason, all legitimate voting procedures allow the vote to be cast in secrecy. Otherwise, a voter might feel threatened or pressured into a particular action regarding the poll. For the case of coin-vote, a coin holder is able to hold coin pseudonymously, and so is able to vote in relative secrecy. In some cases however, this will not be the case. Holders of very large or infamous fortunes of bitcoin might be readily identifiable, including for example well known businesses that have made their addresses public. Secrecy is never a perfect affair. However in this case, the built in pseudonymous nature of bitcoin provides a good solution.

Yet another traditional security concern with polling is that votes can be *bought*. In this scenario, a wealthy individual might wish for a certain outcome and would pay voters to cast their vote in his favor. This is still in theory possible with the coin-vote system, but is much alleviated. A large coin holder might, or example, have no opinion on a certain poll. One who cares about this poll could then solicit the large coin holder to place one vote or another with their coin.   A provable obfuscation of the vote in the record which nonetheless allows validation of the fact that it came from real coin could be used to thwart this kind of attack. However, this “poor man pays the rich man” scenario is less likely than in many traditional voting systems. Whether it becomes an issue in the coin-vote system as currently implemented remains to be seen.

Coin-vote specific security concerns

When a vote is submitted to the system, two checks are performed on it to make sure of its validity:

1) That the signature is a valid one and is made with a key controlling at least one unspent output
2) That the unspent output is not tainted by coin previously used to vote in this question.

The first of these two is readily apparent from our description, that the vote must have demonstrated currently valid bitcoin at the time (block height) of submission. The amount of confirmations which an unspent output has received may be important, at the moment we are running with a single confirmation as enough to make a vote. There is always the possibility that a chain reorganization or double-spend could allow our system to be compromised. However we are generally protected from this by the fact that the coin itself is more valuable than the vote. The security of the vote tally is thus precisely the same nature as the security of the coin ownership.

The second validation is more subtle. It is necessary to prevent a voter from *double voting*, which is moving their coin to another address and voting with it once again. We must in the case of every individual vote check the history of all previously submitted votes to ascertain the cleanliness of the new vote. If any of the previously submitted and tallied votes have been spent in such a way that they wind up as value in the submitted UTXO, the vote is rejected.

There is a further concern which become apparent when considering our vote checking procedure above. A nefarious user might imagine that they could send some of their coin used for a vote to a third party, thus “tainting” the coin of the third party and preventing them from voting. Such a concept of taint is in fact does not exist. This is readily apparent when we realize that the fundamental spendable (and votable) coin is not the amount of coin controlled by an address but individual unspent outputs. Therefore, receipt of previously voted coin at an address does nothing to taint the existing UTXOs controlled by that address. All of them are still clean. However, the user who controls this address will be forced to vote with their existing UTXOs individually. A vote attempt made with the entire contents of the address will be rejected.

Other than verification of votes, there is very little operational security required in the operation of coin-vote. No funds are stored by the coin-vote server, and no account information exists to be stolen. The primary concern from a data security standpoint is to ensure the integrity of the database. It is important that the entire database of votes be available for confirmation by any party. A database dump in JSON format is the current method of distribution, and regular backups are made to ensure no voting information is lost.

General Utility

At first glance, the coin-vote system might seem somewhat unfair when compared to a traditional one-person-one-vote system. In the coin-vote system, a voter's say in the poll is directly proportional to their wealth. While one might complain about this, there is nothing one could do to change the fact. It could be argued that coin-vote's weighting of votes is actually a more fair reflection of the power structures of society. We will refrain from such philosophical arguments here. The system is dictated not by appeal to fairness or social concerns, but by the security and the architecture of the coin cryptography. A coin-vote is a coin-vote, it will not always be the proper poll to make in a given situation. However, we believe it will be of great utility in saving great time and energy going down paths which are not desired by the powerful. A coin-vote allows us to “follow the money”.

It is also the case that coin-votes represent another way that one can put their coin to work in exercising political power. It has always been the case that in spending one's money, one chooses to support one or another institution, and thus exercises political power. With coin-vote, it is possible to wield some piece of this power without diminishing one's holdings.

Further Considerations

It is to be noted that most all operational and business concerns are purposely not addressed in this paper. Being very new, the utility and security of coin-vote is still uncertain. We expect to levy a tax on those who wish to submit new questions, both to support the operation and to eliminate spam. Advertisement banners are also an option we explore. It is expected that use cases will emerge which were not planned, and that some use-cases will wind up being inappropriate for such a poll. The patience and assistance of the community of coin users, voters, and pollers, is greatly appreciated while the bugs are slowly removed from the system and the interface continues to improve.