BUIP129: Finish and Productize the BU Voting System

Submitted by: Andrew Stone
Date: 2019/8/11

Summary

Currently the BU voting process simply requires that every user sign a vote. This BUIP allocates resources to evolve this process into a fully-fledged voting system that could be easily adopted by external organizations, integrated with or closely related to the Bitcoin Cash blockchain. This BUIP requests a person-year of work in funding to allow us to bring a developer on for a longer time frame than is normally possible via small projects. This should make this effort attractive to a larger set of possible candidates.

End Goal, User Perspective

A website allowing an external entity to register and manage a vote. This website will be open source and easily cloned and customized by institutions that want a dedicated site.

A mobile “Activity” (embeddable in any mobile app) that handles voting, connecting to any registered entity. Embed this activity into an app that integrates with the website described above.

Voting System Requirements

Hjálmarsson, et. al provides a summary of voting requirements:

(i) An election system should not enable coerced voting.

(ii) An election system should not enable traceability of a vote to a voters identifying credentials.

(iii) An election system should ensure and proof to a voter, that the voters vote, was counted, and counted correctly.

(iv) An election system should not enable control to a third party to tamper with any vote.

(v) An election system should not enable a single entity control over tallying votes and determining an elections result.

(vi) An election system should only allow eligible individuals to vote in an election

In a digital era, additional requirements and modifications to these requirements may be needed.
A weaker form of requirement (v) may be acceptable:

(v.1) A single tallying entity must be able to prove inclusion of individuals’ votes, and the non-existence of fake votes.

A stronger (or perhaps simply a clearer) form of i is needed to discourage selling of votes -- in traditional voting, someone can pay a voter to vote a certain way, but cannot verify what vote is actually cast. This inability to verify discourages direct vote purchases:

(i.2) An election system should not enable coerced voting. Even with the cooperation of the voter, a dishonest voter should be able to plausibly claim different vote choices (unless vote delegation is explicitly desired within the voting system).

Technology

This section discusses an approach with the purpose of showing that a robust voting system can be achieved. The technologies are here. But the final system may change based on careful reading of prior work.

1. Identity: An external entity is assumed to validate identity and associate a public key with a voter in a manner beyond the scope of this document.

2. Creating a vote & registering: A UTXO (OP_RETURN annotated for public blockchains, or a first class token) is sent to every voter per vote. The UTXO is optionally sent to every voter or a prospective voter needs to ask for one.

3. Anonymity: Before voting opens, these UTXOs are mixed (automatically via user's apps) via cash shuffle ideally with Schnorr input aggregation (which may be coming soon in bitcoin cash).

4. Opening a vote: After a period of time voting opens. Votes are cast using cash shuffle, by sending the shuffled UTXO to an output address that corresponds to the vote choice. Even if a user skips step 3, at least one cash shuffle round offers some anonymity, so long as the outputs go to multiple choices.

5. Votes are tallied using a merkle tree. Voting apps can query the tallying entity and receive a merkle proof that a vote was part of the tally. Requesting the merkle proof could deanonymize the requester to the contents of the final cash shuffle voting transaction. To further preserve anonymity, request multiple proofs for random voting transactions. Doing so also probabilistically checks the honesty of the tally.

6. On a public blockchain, anyone can create a full tally, fully verifying any "official" tally.

Observations

These protocols could be run on a public blockchain, private blockchain or no blockchain at all (just a sequence of dependent transactions). The disadvantage of a public blockchain is in data management. For major elections, this generates lots of data, potentially wasting blockchain space. For small votes, the opposite may be a problem -- requiring that tally machines sift through a huge amount of blockchain data for a few votes.

But in the no blockchain case, a set of attackers could claim their votes were not included by not publishing a voting transaction and then presenting the transaction after the fact. This is avoided by requiring cash shuffle, since a single few input few output vote would be suspicious, but would be fixed by committing all voting transaction hashes to an (unrelated) public blockchain to prove existence.

The private blockchain solution presumes that the entities that assemble blocks won't censor transactions.

Another issue is that an attacker could refuse to sign a cashshuffle operation in which any output tx votes differently, but this would simply isolate votes into different transactions. It may be useful to commit to a vote and then reveal it later, but this may also just defer

censorship to the reveal stage.

Prior Work

There is a medium amount. Some of this effort will be culling interesting ideas from prior work. However, much of the prior work expects a Ethereum style smart contract system or a custom blockchain, whereas this BUIP proposes the creation of a solution that uses Bitcoin Cash technologies.

Blockchain-Based E-Voting System, Friðrik Þ. Hjálmarsson et.al:
https://skemman.is/bitstream/1946/31161/1/Research-Paper-BBEVS.pdf

Secure Digital Voting System based on Blockchain Technology, Khan et. al.:
https://pdfs.semanticscholar.org/c1f0/b096f9ce1b17bea2d39ee760aaede9829d29.pdf

ELECTRONIC VOTING SYSTEMUSING BLOCKCHAIN Ganji, et. al.:
https://pdfs.semanticscholar.org/84c7/c5b9df300d5d282038684654e2d47998b3dd.pdf

(but incomplete IMHO since it “solves” voter anonymity in a trusted centralized manner)