Name: Beyond blockchain ballots explainer

Category: Voting protocols

Paper title: '*Beyond Blockchain Ballots: UC-Secure Layer-2 Voting and Governance*'

Authors: Raghav Bhaskar, Pooya Farshim, Matthias Fitzi, and Aggelos Kiayias

Paper: https://eprint.iacr.org/2026/1521

Beyond blockchain ballots explainer

Current on-chain voting processes face severe scalability issues, suffering from high transaction costs and slow settlement times that limit global voter participation.

Research by the Input Output Research (IOR) team proposes a highly scalable, layer-2 electronic voting protocol that solves this. This research introduces a cost-effective protocol architecture where the bulk of the voting lifecycle, including the casting, collection, and tallying of votes, executes off-chain. The main permissionless blockchain (layer-1) steps in only as a secure, minimal-footprint fallback.

This is the first layer-2 blockchain voting protocol backed by a rigorous security analysis within the Universal Composability (UC) framework, which allows a modular, or composable approach to security analysis. The research also introduces a new way to model the voting system that can pinpoint exactly who is responsible when something goes wrong. Any malicious behavior by off-chain bulletin-board managers can be penalized on-chain, including through the slashing of bonded funds.

Why this matters for blockchain users

This research on a layer-2 electronic voting protocol has practical benefits for regular users and stakeholders:

- **Cost-effective participation:** By moving computation and storage off-chain, the protocol drastically lowers the cost of casting a vote, opening participation to millions without pricing anyone out.
- **Seamless system evolution:** Blockchains need to evolve over time to handle quantum computing threats, new regulations, and treasury fund allocations. An affordable, decentralized voting system lets the community agree on these changes without friction.

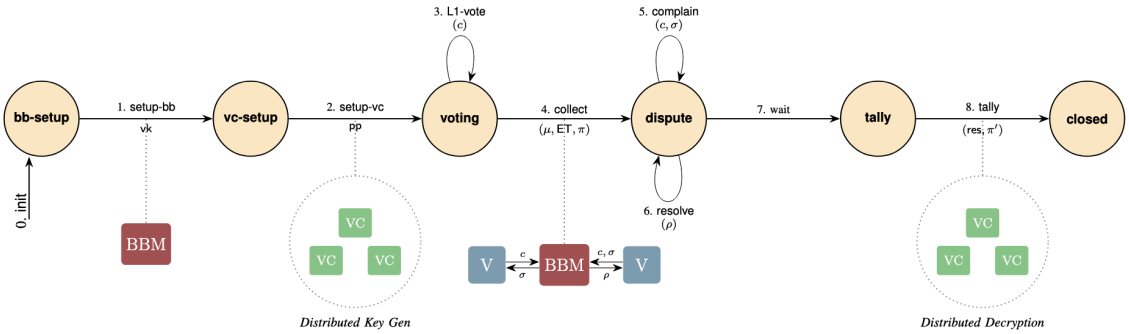
Key components of the protocol

The protocol splits the work of running a decentralized vote across three parts:

- **Bulletin-Board Manager (BBM):** A single server that collects votes submitted off-chain, gives each voter a receipt, and can prove that any given vote was included.
- **Vote-Tallying Committee (VC):** A group of people responsible for generating the election's encryption keys and for jointly decrypting the final vote count, so no single person ever holds the full key.
- **Smart Contract (GovSC):** Lives on the main blockchain. It tracks the overall state of the election, accepts votes submitted directly on-chain if needed, resolves disputes, and publishes the final verified result.

How it works

The protocol moves through various stages, from contract deployment to the final published tally:



Setup

Two parts of the system, a service that manages the digital ballot box (BBM) and a committee that tallies the votes (VC), each generate their own cryptographic setup using a new method for handling encrypted data across multiple parties. They then register that setup on the blockchain using a smart contract, so anyone can verify it's legitimate.

Voting

Voters lock in their choices using a special type of encryption that keeps their vote private while still letting the system check that it's valid, and they sign it to prove their identity. Under the normal process, they submit votes directly to a service called the BBM, which keeps costs low, and they receive a digital confirmation back. If that service acts dishonestly and refuses to confirm a vote, the voter has a backup option: submitting their vote directly to the blockchain itself, which costs more but guarantees it gets counted.

Collection

The BBM service gathers all the valid votes and, using homomorphic features of encryption, combines them into a single encrypted result, without revealing any individual vote. It also generates a compact mathematical proof showing this result was calculated correctly, without having to reveal how it was done. Finally, it posts a short cryptographic summary of everything on the blockchain, so the process can be checked later.

Dispute resolution

Voters can request a proof of inclusion. If a proof is withheld, the voter can file a complaint on the blockchain using the digital confirmation they received earlier. Before the election can move forward, the BBM service must resolve every pending complaint by providing valid proof that each dispute was, in fact, included.

Tallying

The VC then works together, as a group, to decrypt the encrypted tally, so that no single member ever sees the result alone. It posts the final outcome, along with proof that it was calculated honestly, to the blockchain, for anyone to verify.

Rigorous security

The research formalizes a rigorous security definition, called the F-L2Gov ideal functionality, that covers everything a conventional off-chain voting system is expected to guarantee: that votes are counted correctly, that the process doesn't stall, and that no one can tamper with the result undetected, while also keeping individual votes private and letting anyone verify the outcome. On top of this, it introduces a standout feature: fault attribution. If a malicious BBM tries to censor votes or manipulate the ledger, its misbehavior can be provably traced back to it and penalized on-chain, including through the slashing of bonded funds.

The protocol also introduces a new security definition and a novel idealization of smart-contract-enabled blockchain, along with a discussion of the technical challenges that arise when applying the UC framework to layer-2 protocols.

Learn more

For a deep cryptographic dive into the details and design of this protocol, read the '*Beyond Blockchain Ballots: UC-Secure Layer-2 Voting and Governance*' paper by Raghav Bhaskar, Pooya Farshim, Matthias Fitzi, and Aggelos Kiayias.