Private Delegation and Treasuries

Dan Boneh
Stanford University
Privacy questions in DAOs

- Private voting
- Private delegation
- Private treasuries
- Private membership

today
High level goals:

• Only authorized voters can vote, and vote only once
• A voter cannot be linked to their vote
• End-to-end verifiability:
  voters can check that votes are counted as cast
• Voter cannot prove how they voted (no vote selling / coercion)
Recap: three core techniques

(1) Mix nets

(2) Homomorphic encryption

(3) Blind signatures

Real world systems: VotingWorks and ElectionGuard.
Complications

• If delegate is voting privately, how to hold them accountable?
  
  allow voter to vote multiple times, last vote is the one counted

• Clever forms of coercion are still possible:
  • Require user to turn on camera when voting on a proposal
  • Require user to place their secret key in a TEE (e.g. SGX)

No! but I’ll put it in a TEE

I’ll pay for your key

s_k
voter

defense???
eprint.iacr.org/2023/044

s_k
buyer

vote
Nouns DAO: the proposal

Description

- 3 months, 3 zero-knowledge teams, funded by Nouns to design open source solutions for private voting.
- All outputs are open source, and include detailed designs and proofs of concept.
- 70K USDC per team + 20K USDC marketing budget to appear on zk pods and newsletters. Total: 230K USDC.

Funds are managed in a 3/5 Gnosis Safe managed by Elad, David, Solimander, Vapeape and Will.

Let’s vote on it (not privately):

Mandated Round: Private Voting Research Sprint

Proposed by delegate.el4d.eth at 0x7b1ba

Switch to delegate view

Jan. 31, 2023

<table>
<thead>
<tr>
<th></th>
<th>For</th>
<th>Against</th>
<th>Abstain</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>166</td>
<td>75</td>
<td>19</td>
</tr>
</tbody>
</table>
19 submissions!  Three selected by a vote

Team 1

👑 DeFROST: Poseidon 🫤
We have designed a custom cryptographic scheme we call DeFROST to satisfy all Nouns DAO private voting requirements.

Team 2

👑 Aragon and Aztec join forces to bring private voting to...
State-of-the-art DAO private voting with minimal off-chain dependency via Ethereum storage proofs & timelapse encryption

Team 3

👑 Nouns Vortex
A privacy preserving on-chain voting for Nouns DAO; the proposal by team Mizu
The Time NounsDAO Got Private Voting

Aztec x Aragon bring private on-chain voting to Nouns

Aztec Labs · Follow
Published in Aztec · 4 min read · Mar 8

https://medium.com/aztec-protocol/the-time-nounsdao-got-private-voting-4336fe4a2c29
An encryption-based voting system

(most closely related to blind signature voting)

To set up a vote on a proposal:
• generate a random Proposal ID (PID)
• generate random encryption keys (pk, sk)
• Publish pk; keep sk secret (where? will see in a minute ...)

On chain: Voting Contract (VC) has PID and pk
An encryption-based voting system

A Noun owner: submits to on-chain Voting Contract (VC):

1. an encrypted vote: \( ct \leftarrow E(pk, \text{vote}) \)
2. Nullifier: \( N_{\text{Noun}} \leftarrow \text{Hash}(\text{PID}, s_{k_{\text{Noun}}}) \)
3. a ZK proof that
   (i) they own the Noun and (ii) \( N_{\text{Noun}} \) is computed correctly

VC accepts submission if
(i) ZK proof is valid,  (ii) \( N_{\text{Noun}} \) has not yet appeared

- does not ID voter
- no double voting
An encryption-based voting system

A Noun owner: submits to on-chain Voting Contract (VC):

1. an encrypted vote: $ct \leftarrow E(pk, \text{vote})$

2. Nullifier: $N_{\text{Noun}} \leftarrow \text{Hash}(\text{PID}, sk_{\text{Noun}})$

3. a ZK proof that
   (i) they own the Noun and (ii) $N_{\text{Noun}}$ is computed correctly

If Alice owns four Nouns, she submits four votes.
An encryption-based voting system

Once voting period elapses:

- Secret decryption key $sk$ is revealed
- All votes (in the VC event log) are decrypted and tallied

How to ensure $sk$ revealed at end of vote, and not before?

- The proposal: a trusted time-lapse cryptography service

trustees that only reveal $sk$ at a pre-specified time
Complications

- Voters must send vote to on-chain VC using Tor
  \[ \Rightarrow \] otherwise, voter’s IP address reveals voter’s ID

- If Whale voter owns 145 Nouns and submits all 145 votes at once, the voter is identified

  Proposed solution: delay-relays

  an off-chain service that will submit 145 votes slowly over time
Who pays the gas for casting a vote?

Voter pays ⇒ identifies voter

Proposed solution:

• **delay-relay** will pay for gas,
  and is then reimbursed by the Voting Contract

⇒ Voter must send votes to delay-relay over Tor
A Noun owner: submits to on-chain Voting Contract (VC):

1. an encrypted vote: \( ct \leftarrow E(pk, \text{vote}) \)
2. Nullifier: \( N_{\text{Noun}} \leftarrow \text{Hash}(\text{PID, } sk_{\text{Noun}}) \)
3. a ZK proof that (i) they own the Noun and (ii) \( N_{\text{Noun}} \) is computed correctly

Problem: voter can “open” its encrypted vote \( ct \) to buyer

A possible defense: deniable encryption
Issues: (2) delegation?

- Voters can delegate Nouns publicly to delegate
- Delegate can vote privately

What about accountability for delegate?
Private Voting via Private Payments

A very different approach
Private payment systems

Zcash, Ironfish, Aztec:

1. Buy in: Alice can use non-private tokens to buy private tokens
   \[ \rightarrow \text{a Note with a preset value bound to Alice's signing key} \]

2. A private transaction: Note1, Note2 \[ \rightarrow \text{Note3, Note4, Note5} \]
   - input Notes are nullified
   - output Notes are created bound to recipients' keys

3. Cash out: Alice can exchange her note for non-private tokens
Private payment systems

An observer sees that five Tx took place
- but does not know who paid who or what amounts

Guarantee for every Tx: \( \text{sum(value of inputs)} = \text{sum(value of outputs)} \)
- (in particular, Alice cannot double spend her tokens)
Can we use this for private voting?

At the beginning of election: airdrop tokens to all DAO members (e.g., one token per Noun)

- YES address
- NO address

six Txs

at end of election

Trustees are trusted to not reveal tallies mid-election.
Delegated tokens cannot be further delegated:
can only be sent to YES/NO addresses
Private delegation

Differences from private payment tokens:

• Voters can take yellow delegation tokens back!

• Every voter can track its own delegation tokens to the YES/NO address. Cannot track other voter’s tokens.

  ⇒ voter can learn how its own delegate voted, but not how other delegates voted (or who delegated to them)

This can all be implemented efficiently. Is it what we want???
An alternative

Alternatively: private delegation, but no privacy for delegates
Anyone interested in building a voting contract with private delegation?
Private Treasuries
Private DAO treasury

2021: an auction for a physical copy of the constitution (Sotheby's auction house)

ConstitutionDAO:
- Formed in Nov. 2021 to participate in auction.
- Raised $46.3M from about 20K participants from around the world
- Lost to another bidder who bid $43.2M

bidder knew that ConstitutionDAO could not outbid it

How to participate in an auction when everyone knows your treasury??
Private DAO treasury

[Dunaif, Boneh, 2021]

The design:

• One platform manages many DAOs: a single Ethereum contract (e.g., JuiceBox)

• **DAO manager**: sets up a DAO by publishing a DAO public key (pk)

• **Contributor**: sends funds to platform with a “blinded DAO pk”

• Contract records contribution
  ⇒ an observer learns nothing about which DAO received the funds
  ⇒ only learns total amount stored on the platform as a whole

• DAO manager can later use its secret key to claim funds sent to its DAO
So what happened to Constitution DAO?

Refunds offered: high gas fees ⇒ diluted refunds

... but the PEOPLE token is doing well (the defunct governance token)