DAO Decentralization Voting-Bloc Entropy, Bribery, and Dark DAOs **Austgen, Fàbrega, Allen, Babel, Kelkar, and Juels** (2023)[1]

Iniyan Joseph

2026-11-12

Purdue University

iniyanijoseph@gmail.com

[1]CS 592 - Special Topics in Blockchains

The paper

- How can we measure decentralization when voters have aligned interests?
- How do delegation and bribery change this measure?
- Can a private, enforceable vote-buying market be built?

Why measure voting blocs?

A DAO can distribute its tokens across many addresses while decision-making remains concentrated.

- One entity can control multiple addresses.
- Voters may share interests or imitate one another.
- Inactivity can leave decisions to a small set of participants.

Idea: Measure how voting weight is distributed across groups of voters with aligned interests.

Model

Let P be the set of token holders and E the set of binary elections.

- Player i holds w_i tokens; $W = \sum_i w_i$.
- Player i has a vector u_i of utilities across elections.
- A clustering rule groups players with aligned utilities into blocs.
- For a bloc B, let $w(B) = \sum_{i \in B} w_i$.

The paper assumes $u_{i(e,\,\text{yes})} = -u_{i(e,\,\text{no})}$.

Voting-Bloc Entropy

Choose a clustering rule C and an entropy function F. VBE applies F to the distribution of token weight across blocs.

The paper focuses on **min-entropy**:

$$\mathrm{VBE} = -\log_2\left(\max_B \frac{w(B)}{W}\right).$$

The largest bloc determines the metric.

- Largest bloc has 50% of the tokens: VBE $= 1$ bit.
- Largest bloc has 25% of the tokens: VBE $= 2$ bits.

An example

Suppose eight addresses each own $\frac{1}{8}$ of the tokens.

Eight individual addresses

Largest share: $\frac{1}{8}$

Min-entropy: 3 bits

Four aligned pairs

Largest bloc: $\frac{1}{4}$

VBE: 2 bits

Splitting an account cannot increase VBE if the new accounts remain in the same bloc.

The inactivity whale

The authors group sufficiently apathetic voters into an **inactivity whale**.

- A player is ε-apathetic when their utility is close to zero.
- The inactive bloc may contain a large share of all tokens.
- Min-entropy falls when that bloc becomes the largest.

This captures inactivity as a form of concentration, though inactivity and common control need not be the same thing.

Delegation

Delegation can distribute weight from the inactivity whale to several delegates.

Theorem 3.4: VBE weakly increases if each affected delegate's final bloc has no more tokens than the original inactive bloc.

Reason: The inactive bloc shrinks, and no newly enlarged delegate bloc exceeds its original size.

A large delegate can instead concentrate voting weight.

Other changes to the voting process

Herding. Social incentives can move voters into the same bloc as an influential voter.

Proposal bundling. Combining proposals can make previously distinct utility profiles agree on a slate.

Privacy. The authors argue that private voting can reduce herding; this depends on the model of voter behavior.

The bundling result assumes that initially aligned players remain aligned after bundling.

Bribery and decentralization

Bribed voters can become aligned with a buyer's preferred outcomes.

If the resulting bribed bloc is at least as large as the previous largest bloc, VBE cannot increase.

But bribery can also split a large bloc, for example by recruiting only some inactive voters.

Theorem 3.7 states a strict decrease, whereas its proof establishes a weak inequality.

How much corruption is needed?

The paper relates min-entropy to the scale of bribery in two settings:

- **Internal attacker:** its proof subtracts the largest bloc's weight from the target threshold.
- **External attacker:** its proof divides the threshold by the largest bloc's weight.

The argument requires care about **individual control**, indivisible players, and rounding. Aligned preferences alone do not give one player control over a whole bloc.

A closer look at external bribery

Take $q = \frac{1}{2}$, with the same four stakeholders and weights in both cases:

$$0.26, \quad 0.25, \quad 0.25, \quad 0.24.$$

Before: the 0.26 and 0.24 stakeholders form one bloc, of weight 0.50.

After: all four are in separate blocs; the largest has weight 0.26.

VBE rises, but in both cases control of the 0.26 and 0.25 stakeholders guarantees more than half the tokens. Thus the minimum number to control remains two.

This challenges a literal strict equivalence in Theorem 3.9 under indivisible individual control.

Dark DAOs

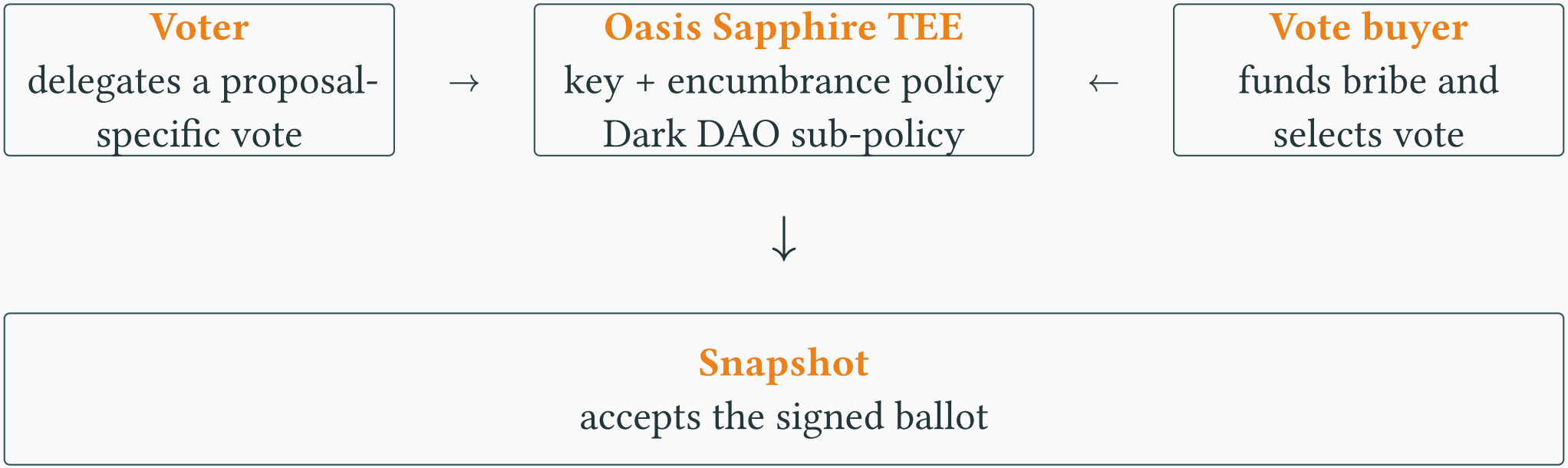
A **Dark DAO** is a mechanism designed to subvert credentials, such as DAO voting rights.

The basic prototype uses a trusted execution environment on Oasis Sapphire:

- A participant's signing key is subject to a policy enforced by confidential computation.
- The policy can sign votes according to a buyer's instructions.
- The design aims to hide participation and enforce the vote-buying agreement.

The prototype targets Ethereum DAO voting through Snapshot. Confidentiality depends on the system's security and metadata assumptions.

Key encumbrance: how a vote is sold



The policy prevents the voter from signing a conflicting vote for the delegated proposal. The voter receives the bribe and can still request permitted signatures for other purposes.

Dark DAO Lite

The Lite design makes participation easier, with weaker confidentiality.

- Participants transfer DAO tokens to accounts controlled by the Dark DAO.
- They receive transferable DD tokens representing deposited value and a share of voting-rights auction revenue.
- Buyers can acquire voting rights while participants retain a liquid financial claim.

The paper implements both variants to study feasibility, not to measure prevalence in existing DAOs.

Can we estimate VBE from votes?

Utilities are latent. Historical votes can provide a proxy, but they do not reveal preferences perfectly.

- Abstention can reflect low stakes, voting costs, or missing information.
- Agreement may reflect shared preferences, social pressure, or coordination.
- A short or selective proposal history can obscure disagreements.

A statistic computed from ballots should be distinguished from latent-utility VBE.

The clustering rule and transitivity

The framework requires its alignment rule to be an equivalence relation. The stated ε-threshold rule does not always satisfy transitivity.

For $\varepsilon = 1$, consider one election with utilities 2, 0.5, and -0.5:

- 2 aligns with 0.5: same sign.
- 0.5 aligns with -0.5: both are within ε of zero.
- 2 does not align with -0.5.

A partition therefore needs an additional convention or a revised rule.

Questions for discussion

- How does delegation affect both concentration and decision quality?
- Can bribery mobilize inactive voters and improve an outcome in equilibrium?
- What information about preferences can we recover from voting records?

Reference

James Austgen, Andrés Fàbrega, Sarah Allen, Kushal Babel, Mahimna Kelkar, and Ari Juels.
DAO Decentralization: Voting-Bloc Entropy, Bribery, and Dark DAOs.
arXiv:2311.03530v1, 2023.

https://arxiv.org/pdf/2311.03530