Vote Buying in DAOs

Iniyan Joseph

01 · Introduction

DAO proposals can move assets through a token-weighted vote. When turnout is low, a small group may pass a proposal despite opposition. We study whether vote payments can mobilize a defense when attackers can also make offers. Related work studies DAO bribery [1], turnout [2] [4], and vote buying [3] [5] [10].

Governance attacks

Compound 289 (2024). The Golden Boys acquired COMP and proposed moving 499,000 COMP to a vault they controlled. The proposal passed, 682,192 to 633,637; it was canceled after negotiations [7].
Indexed 24 (2023). An attacker bought NDX and proposed taking control of the treasury. Holders mobilized 413,036 no votes against 402,219 yes votes. In a later attempt, an attacker received 10,000 DAI to withdraw a proposal [6].
We do not identify vote-contingent payments in these incidents; the Indexed payment was for withdrawal, not a ballot.

02 · Model and timing

There is one weighted, binary vote. Each voter i has:
- Snapshot voting power $w_i > 0$.
- A private value $u_i \sim F_i$ for passage relative to rejection. A **defender** has $u_i < 0$ and prefers rejection; it need not pay.
- Voting cost $k_i \geq 0$ and an offer budget B_i.

Values are independent, their distributions are public, and voters are risk neutral. Abstention is free; ties reject. We impose no quorum.
Offers. A voter may offer payments to other voters for yes or no. We call the offering voter a **payer**. A payer may also vote or receive offers. Payments add and are made only for the specified ballot, regardless of outcome. Each payer reserves funds for its offers within its budget; bribes received cannot fund offers in the same round. Utility is u_i on passage, minus voting cost and bribes paid, plus bribes received.
Timing.
- Voters learn their values and simultaneously commit offers.
- Offers are revealed; voters simultaneously vote or abstain.
- The outcome and payments follow.

A strategy specifies offers and a voting rule after every offer profile, for each type. In a **full-game BNE**, each type's complete strategy is a best response. A **voting-stage BNE** holds offers fixed and requires optimal voting given those offers and the induced beliefs [11]. The three voting actions are yes, no, and abstain.

03 · Voting and crowd-out

Let M_{-i} be other yes weight minus no weight. Conditional on type and observed offers, define

$$p_i^N = \mathbb{P}(0 < M_{-i} \leq w_i), \quad p_i^Y = \mathbb{P}(-w_i < M_{-i} \leq 0).$$

With total no/yes offers d_i, y_i, payoffs relative to abstention are

$$D_i = d_i - k_i - u_i p_i^N, \quad Y_i = y_i - k_i + u_i p_i^Y.$$

Voting-stage BNE uses only maximizers of $0, D_i, Y_i$, with pivotal probabilities induced by the voting strategies.
Crowd-out example. An attacker with weight 1 votes yes at no cost. Defender H has weight 2, loss 3, and voting cost 1. Voter R has weight 1 and cost 1; its loss is 0.75 with probability 0.9, otherwise 0.

Voting-stage BNE	**No offer**	**H: 0.5 for R's no**
H's ballot	No	Abstain
R's ballot	Abstain	No if loss 0.75
Rejection probability	100%	90%
H's expected loss + costs	1	0.75

Under the 0.5 offer, both shown ballot rules are voting-stage BNEs; in the second, H's voting benefit is $0.1 \times 3 < 1$. Offer choice and equilibrium selection remain unspecified.

04 · A sufficient defense

Let j be a defender and S a set of other voters known to oppose passage ($u_i \leq 0$ for every type). Write $W(S) = \sum_{i \in S} w_i$, $W = \sum_i w_i$, and $H_j = \sum_{\ell \neq j} B_\ell$. Assume

$$Q = W(S) - \frac{W}{2} > 0.$$

If

$$B_j > \sum_{i \in S} \max\{k_i, \frac{H_j w_i}{Q}\},$$

the defender can force rejection in every voting-stage BNE despite competing offers: offer each $i \in S$ slightly more than $\max\{k_i, H_j \frac{w_i}{Q}\}$. The recipient prefers no to abstention; passage would require competing offers exceeding H_j.
This does not imply that the defender funds these offers in a full-game BNE.

Necessary BNE condition

In a BNE with certain rejection, let T_i be its bribes paid plus voting cost minus bribes received, and $L_i = -u_i$. Let p_i^0 be the chance of passage if it withdraws offers and abstains, conditional on L_i and holding other strategies fixed. Except on a zero-probability set of types,

$$\mathbb{E}[T_i \mid L_i] \leq L_i p_i^0.$$

Positive net costs require a risk of passage after withdrawal. If $d_i = 0$, voting no also requires $L_i p_i^N \geq k_i$.

Recruitment at given prices

For one payer, fix accepted prices c_i, competing offers, and other ballots. Buying voter i gains $g_i = w_i$ of no margin from nonparticipation, or $g_i = 2w_i$ from switching yes to no. For initial yes lead $D > 0$, minimum-cost recruitment is **minimum knapsack**:

$$\min_{x \in \{0,1\}^n} \sum_i c_i x_i \quad \text{s.t.} \quad \sum_i g_i x_i \geq D.$$

This is a polynomial-time reduction: each voter becomes one item.
Hardness: [9] given SUBSET SUM numbers a_i and target T, set $g_i = c_i = a_i$ and $D = B = T$. A cover within budget B exists iff a subset sums to T. Thus the decision problem is weakly NP-complete for **binary-encoded integers**. A dynamic program uses $O(nD)$ updates. Funding selected payments is a separate flow problem (Section 7).

05 · Competing offers

Market. Every voter may make or receive offers and vote. One attacker has $u_A > 0$; all other voters have $u_i \leq 0$ for every type. These signs are public. Voting weights are unrestricted.
Withdrawal bound. Voter i can cancel its own offers, then choose yes, no, or abstain while others' offers remain available. Lower-bound this deviation by putting all other ballots against i's preferred outcome. Let s_i be its best payoff under those ballots, after seeing offers. Its equilibrium expected utility given its type satisfies $U_i(u_i) \geq \mathbb{E}[s_i | u_i]$.
Candidate BNE test (proof). Fix finite sets of offers used by each voter and voting rules at positive-probability offer profiles. These extend to a full-game BNE **iff**, for each voter and all its types outside a probability-zero set:
- Its expected utility is at least its expected withdrawal bound.
- No type gains by choosing any offer used by that player, then its best voting action, holding others' voting rules fixed.

Votes after zero-probability offer profiles can deter other deviations; those votes need not be optimal there. The test covers arbitrary weights, but does not prove that a defending BNE exists.

06 · Welfare and holdings

Total welfare. Compare strategy profiles with and without payments. Let X_0, X_1 indicate passage without and with payments, K_0, K_1 be voting costs, and $H = -\sum_i u_i$ be net harm from passage, including the attacker's gain. Total welfare increases iff

$$\mathbb{E}[H(X_0 - X_1)] > \mathbb{E}[K_1 - K_0].$$

Transfers cancel when both sides are included. Nash welfare also requires nonnegative utility levels; normalized values may be negative.
Holdings. Consider a feasible transfer $t > 0$ from account j to i, with balances $z_j > z_i$ in one asset. The fixed set of balances, including zeros, becomes strictly more equal in the majorization order iff

$$0 < t < z_j - z_i.$$

Voting power need not equal ownership; defense need not equalize holdings.

07 · Testing the sufficient condition

Are the theorem's offers fundable?
- **Data:** the same 414 snapshots and five DAOs. Whales form the 90%-power prefix [8] habitual whales cast yes/no in at least half their eligible opportunities in 20 earlier completed proposals; require five opportunities. Abstentions do not count.
- **Scenario:** one attacker controls the three largest no-code wallets outside the habitual whale cohort. NO funders are habitual no-code whales. Each side's cap is 10% of its observed wallet ETH/WETH; other funding is not assumed.
- **Targets:** modeled NO-capable accounts outside the attacker. Treat all weight outside S, including omitted accounts, as free YES votes. Require $Q = W(S) - \frac{W}{2} > 0$ and $u_i \leq 0$ for every target type.

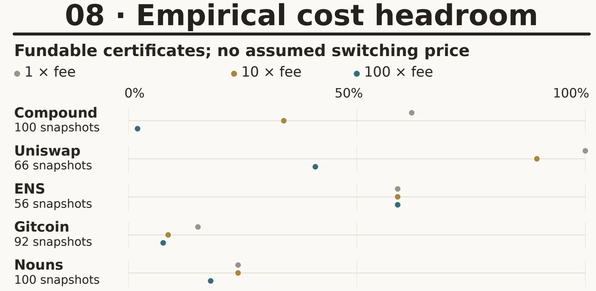
Connection to Section 4. Use NO offers $d_i > \max\{c, H\frac{w_i}{Q}\}$, rounded strictly up in wei, where c bounds voting cost and H caps all YES offers. With NO-funder budgets B_j and $B_D = \sum_j B_j$, these offers are fundable **iff**

$$\sum_{i \in S} d_i \leq B_D, \quad d_i \leq B_D - B_i \quad (i \in S).$$

Take $B_i = 0$ for nonpayers. The second constraint excludes self-payments. Every voting-stage BNE then rejects if $k_i \leq c$. Search a fixed family of opponent sets for the largest feasible c. Proof and funding conditions.

08 · Empirical cost headroom

Fundable certificates; no assumed switching price



Share admitting a fundable theorem certificate at the indicated cost ceiling.

At a cost ceiling of one observed median ballot fee, **199/414** snapshots admit a certificate; at 100 fees, **87/414**. No certificate does not rule out a different defense.
Fees scale hypothetical cost ceilings, not bounds on attention costs. Preference signs, contributions, and YES-budget caps are assumed. This tests financial capacity after offers are committed, **not defending-BNE prevalence**.
Full methods · Data, frontiers, and checks.

Conclusion

DAOs should permit public, verifiable vote payments as a defensive tool. They can fund turnout and make existing opposition more expensive to buy. A ban removes this option while private buying remains possible [1].
The experiment tests affordability against an attacker who also buys votes. It does not establish equilibrium contributions or net welfare gains. Public payments should complement timelocks and vetoes, with auditable offers and contributions.

References

Citations link to sources; see the paper for the full bibliography.

[1] Austgen et al. **DAO Decentralization: Voting-Bloc Entropy, Bribery, and Dark DAOs** (2023). arXiv:2311.03530.
[2] Palfrey & Rosenthal. **Voter Participation and Strategic Uncertainty**. APSR (1985).
[3] Dekel, Jackson & Wolinsky. **Vote Buying: General Elections**. JPE (2008).
[4] Nichter. **Vote Buying or Turnout Buying? Machine Politics and the Secret Ballot**. APSR (2008).
[5] Faliszewski, Hemaspaandra & Hemaspaandra. **How Hard Is Bribery in Elections?** JAIR (2009).
[6] Feichtinger et al. **SoK: Attacks on DAOs**. AFT (2024).
[7] Compound DAO. **Proposal 289**; Colligan, **Stake Compound Product** (2024).
[8] Fritsch, Müller & Wattenhofer. **Analyzing Voting Power in Decentralized Governance: Who controls DAOs?** §5.2.
[9] Karp. **Reducibility Among Combinatorial Problems** (1972).
[10] Louis-Sidois & Musolff. **Buying Voters with Uncertain Instrumental Preferences**. Theoretical Economics (2024).
[11] Milgrom & Weber. **Distributional Strategies for Games with Incomplete Information**. Mathematics of Operations Research (1985).