Concave is the New Linear: The Impossibility of Anti-Plutocratic DAO Governance

Austin Bennett
Circle Research, USA

Preston Vander Vos
Circle Research, USA

Duc V. Le
Circle Research, USA

Mira Belenkiy
Circle Research, USA

Abstract

Decentralized Autonomous Organizations (DAOs) run protocol governance by letting token holders vote on proposals. The dominant rule, voting power proportional to wallet balance, concentrates control among a small number of large holders, fueling the *token-control* governance attacks that have already compromised real protocols. To counter this concentration, the community has turned to *anti-plutocratic voting mechanisms* such as Quadratic Voting (QV), which assign sublinear voting power per token with the goal of dampening the influence of large holders.

In this work, we prove that no voting rule that derives power solely from wallet balance can succeed on a permissionless blockchain. Through a costed model of on-chain voting that captures realistic blockchain frictions, including per-wallet splitting and voting costs, fixed setup costs, and minimum-balance requirements, we show that whenever a wallet of any size yields nonzero voting power, a Sybil attacker who splits tokens across many wallets achieves total voting power that grows at least linearly in their token holdings. For concave rules that are actually proposed to dampen governance power—those that are positive, increasing, and finite—we show that the optimal strategy yields power that is *asymptotically linear* in token holdings, *regardless* of the cost scheme.

Instantiating the model on real DAOs reveals attack costs orders of magnitude below the value at stake. Replaying the ten most recent finalized proposals of five major DAOs (ENS, Compound, Uniswap, Arbitrum, and ZKsync) under linear, quadratic, logarithmic, and power-($\beta = 0.25$) voting, we measure Sybil amplification factors between 1,172× and 4,039× under Quadratic Voting, and exceeding 229,000× under steeper power rules. On Uniswap specifically, a Sybil-optimal attacker captures a \$300M vote for roughly \$75K in token and gas costs; a single-wallet attacker with the same budget achieves only $\approx 1/259$ of the voting power needed to win.

2012 ACM Subject Classification Security and privacy → Distributed systems security

Keywords and phrases Sybil Attack, DAO Governance, Decentralized Finance

1 Introduction

Decentralized Autonomous Organizations (DAOs) have become the dominant governance structure for on-chain protocols. Collectively, they direct the evolution of many of the most widely used decentralized-finance (DeFi) protocols including ENS [15], Compound [9], Uniswap [30], Aave [2], Lido [21], and MakerDAO [22] as well as the ecosystem governance of Layer-2 rollups such as Arbitrum [5], ZKsync [33] and Optimism [25]. Billions of dollars sit in these protocols, but they are not controlled by a single entity. Instead, they're protected by the governance decisions of token-holding communities. The legitimacy of a DAO therefore rests on a simple premise: its voting process faithfully aggregates the preferences of participants and resists manipulation by an adversary. When this premise fails, the consequences are immediate and severe.

Securing DAO governance is hard. Real-world incidents make this danger concrete. On 20 May 2023, an attacker imitated a previously accepted proposal on the *Tornado Cash* DAO, slipping in a self-destruct modification that, once passed, replaced the governance contract with malicious code and drained TORN tokens from the treasury [6, 13]. Six months later, in November 2023, the *Indexed Finance* DAO was targeted by two consecutive governance attacks in which the adversary purchased NDX tokens on decentralized exchanges, self-delegated the voting power, and submitted a proposal intended to seize the protocol's timelock. The community narrowly averted the attack, but was forced to pass a defensive proposal that would render its own treasury permanently inaccessible [3]. These are not isolated events. A recent systematization by Feichtinger et al. [18] discovered 28 real-world attacks across four blockchains, roughly corresponding to four evenly distributed attack vectors—*bribing*, *token control*, *human-computer interaction*, and *code/protocol vulnerability*. Securing DAO governance is a multi-faceted problem with often subtle exploits.

The plutocracy problem. One potential enabler of these attacks is the *concentration of voting power*. Most DAO governance systems follow a one token, one vote mechanism. In principle, this includes every participant's share equally; but in practice, it is dominated by a small number of large holders. Compounding this issue, empirical data shows that proposals only receive about 5% of the total token supply on average [17]. This concentration directly fuels the entire *token control* (TC) family of attack vectors in the SoK taxonomy: an adversary can buy tokens on the open market (TC1), borrow them against collateral (TC2) or via flash loans (TC3), rely on a previously inactive whale suddenly delegating its balance ("whale activation", TC4), or coordinate a majority coalition (TC5) [18]. The common denominator is that voting power in canonical DAO designs is *linear* in token holdings, so whoever holds (or can temporarily acquire) more tokens wins.

Quadratic Voting as a proposed defense. To dampen this plutocratic dynamic, the blockchain community has turned to anti-plutocratic mechanisms like *Quadratic Voting* (QV), introduced by Lalley and Weyl [20]. Under QV, a participant committing w tokens receives only $\sqrt{w}$ votes, so the marginal additional influence decreases with holdings. In a single-identity setting, this provably leads to socially optimal collective decisions and shifts the balance of governance away from the largest holders. Motivated by this property, QV has been proposed as a defense against token-concentration attacks on DAOs [12]. Crucially, however, QV was designed for settings in which each voter has a *single*, *stable* identity. Lalley and Weyl themselves caution that high-stakes applications "remain far more speculative and are not advisable without further experimentation" [20]. In securing billions of dollars without a centralized backstop, permissionless blockchains provide the exact environment that the authors warn against.

Sybil Attacks. The main danger is a Sybil Attack [14], where an adversary artificially inflates its power in a decentralized system by creating fake identities. Since permissionless blockchains cannot reliably tie wallets to identity, the single-identity assumption underlying QV and many other anti-plutocratic mechanisms does not hold. We show that an attacker can split their tokens across multiple wallets to obtain disproportionate voting power that the blockchain cannot trace back to a single identity. For this reason, large-scale implementations of QV-style mechanisms have primarily been in non-governance applications (e.g. Gitcoin's Quadratic Funding [31]). Still, many proponents of anti-plutocratic governance mechanisms believe that modifications to Quadratic Voting could be viable. Commonly proposed solutions include less severe concave mechanisms or anti-Sybil features such as high wallet minimum balances or increased voting and wallet generation costs.

Our contributions. In this paper, we ask whether Quadratic Voting or any other anti-plutocratic mechanism can withstand a Sybil adversary on a permissionless chain, and answer in the negative. We find that *no* wallet-level voting rule can avoid plutocracy under a rational Sybil attacker. Whenever a wallet of any size yields nonzero voting power, the attacker's Sybil-adjusted voting power grows at least linearly in their token holdings, regardless of the per-wallet splitting cost, voting cost, fixed setup cost, or minimum-balance requirement. For the concave rules actually proposed for anti-plutocratic governance (i.e. those that are increasing, finite, and positive), we sharpen this result to show optimal voting power is asymptotically linear in token holdings with a closed-form expression. Concretely, we make five contributions:

1. **A unified, costed model of wallet-based voting (Section 3).** We introduce a model that captures realistic blockchain frictions—per-wallet splitting costs, voting gas costs, fixed setup costs, and a minimum balance required to vote—for an *arbitrary* wallet-level voting rule f. We formalize the notion of a *plutocratic* voting rule via the asymptotic slope of the attacker's Sybil-adjusted voting power, providing a single definition that applies uniformly across linear, concave, and other rules.
2. **A universal impossibility result (Section 4).** We prove that *every* nontrivial wallet-based voting rule is plutocratic under unrestricted Sybil splitting, and that this conclusion is robust to any linear cost scheme. That is: as long as some wallet size yields nonzero voting power, an attacker holding a tokens achieves Sybil-adjusted voting power $V^*(a) = \Omega(a)$. The result rules out the entire wallet-based design space of anti-plutocratic mechanisms in one stroke, independent of the specific shape of f or the cost scheme imposed on top.
3. **A tight asymptotic slope for concave rules (Section 5).** For the concave rules actually proposed for anti-plutocratic governance, we sharpen the universal lower bound to a tight asymptotic slope: as the attacker's budget grows, their per-token amplification converges to an explicit constant determined entirely by the voting rule and the per-wallet cost. We give closed-form expressions for this constant under the three concave rules — power, quadratic, and logarithmic voting.
4. **Empirical impact across major DAOs (Section 6).** We instantiate our model with on-chain voting data from the ten most recent finalized proposals of five governance-heavy DAOs—ENS, Compound, and Uniswap (on Ethereum), together with Arbitrum and ZKsync—and per-proposal gas prices on each chain. Under Quadratic Voting, we measure Sybil amplification factors between 1,172× and 4,039× across these protocols; under a steeper power rule ($\beta = 0.25$) the amplification exceeds 229,000×. Concretely, the Sybil-optimal attacker captures a \$300M Uniswap vote under QV for roughly \$75K in token and gas costs, while a single-wallet attacker with the same budget achieves only $\approx 1/259$ of the voting power needed to win.
5. **Mitigation discussion (Section 7).** We survey candidate defenses—wallet minimum balances, increased per-wallet fees, Proof-of-Personhood, and compositions of multiple mechanisms—and show that no per-wallet economic friction can avoid asymptotic plutocracy: per-wallet costs only reduce the slope κ, they do not change its order. Anti-plutocratic governance on a permissionless chain therefore requires an identity-based Sybil-resistance layer that limits *wallet count* rather than per-wallet behavior. Concave voting must be deployed only as one component of such a composite mechanism, never as the primary line of defense.

2 Preliminaries

Before developing our model and main result, we review the two pieces of background a reader needs to follow the rest of the paper: the lifecycle of on-chain DAO governance, and the Quadratic Voting mechanism that motivates our generalization.

2.1 Decentralized Autonomous Organizations

A *Decentralized Autonomous Organization (DAO)* is an organizational structure that facilitates trustless, on-chain governance of blockchain-based projects. Today, DAOs govern major blockchain protocols, including Aave, Compound, ENS, Lido, MakerDAO, and Uniswap, and collectively control treasuries estimated to hold $8B [11]. Instead of being vested in a centralized board or executive, DAOs distribute decision-making authority among holders of a designated *governance token*.

Governance Tokens. Governance tokens confer voting rights on their holders. These tokens are initially distributed through various means, such as airdrops to early users or allocations to founding teams and investors. Once launched, governance tokens are freely tradable on both centralized and decentralized exchanges, allowing anyone to acquire voting power. Most DAOs follow a token voting model similar to Governor Bravo [10], which allows for three vote categories —*for*, *against*, or *abstain* — in addition to other governance features, such as time locks. Under this system, each token counts as one vote, making voting power directly proportional to token holdings.

Delegation. Many DAOs allow token holders to *delegate* their voting power to a representative who votes on their behalf. In some DAOs (e.g., Compound, ENS, Uniswap), delegation is mandatory: tokens must be delegated to an address (possibly the holder's own) before they can be used to vote. This design reduces the transaction costs of governance participation. Organizations like a16z's token delegate program [4] use delegation to decentralize power; but in other cases, delegation can concentrate voting power in a small set of delegates.

Proposals. In many Governor Bravo-style governance systems, token holders whose balance exceeds a predefined *proposal threshold* may submit a governance proposal. A proposal specifies a set of on-chain actions (e.g., transferring treasury funds, updating protocol parameters) along with a human-readable description. Some DAOs additionally require off-chain deliberation, such as discussion on governance forums or temperature-check votes on platforms like Snapshot [28], before a proposal can be submitted on-chain.

Voting and Execution. Once a proposal is submitted on-chain, a *proposal delay* (measured in blocks) elapses before a snapshot of token balances (or delegations) is taken. This snapshot fixes each participant's voting power for the duration of the vote. A *voting period* then opens, during which eligible addresses cast their votes. The voting period typically lasts several days. A proposal passes if it receives a majority of votes in favor and meets a predefined *quorum* requirement. Accepted proposals may be executed automatically or, in some DAOs, only after a *timelock delay* that gives stakeholders additional time to react (e.g., exit the protocol) before changes take effect.

Security Concerns. Despite the democratic aspirations of DAO governance, the one-token-one-vote model leads to significant concentration of power. Empirical studies such as Falk et. al [17] show that voter participation is low: on average, only about 5% of the total token supply participates in governance votes. This voter apathy, combined with large token holdings by whales and exchanges, makes DAOs susceptible to governance attacks

including vote buying, flash-loan attacks, and majority coalitions. These concerns motivate the exploration of alternative voting mechanisms that dampen the influence of large token holders.

2.2 Quadratic Voting

Quadratic Voting (QV) draws on a long line of mechanism-design work on truthful preference revelation, most notably the Vickrey–Clarke–Groves (VCG) tradition, and was popularized in its modern form by Lalley and Weyl [20], who coined the name and gave the formal academic treatment. It addresses two well-known failure modes of ballot-box democracy: *one-person-one-vote* cannot express how strongly a voter prefers one outcome over another, while unconstrained weighted voting degenerates to plutocracy when participants hold vastly different weights. QV sits between them by charging a *quadratic* price for influence: committing more lets a voter express more intensity, but at a sharply rising marginal cost.

What QV is. Concretely, a participant committing w tokens receives $\sqrt{w}$ votes; equivalently, purchasing V votes costs V^2 tokens. The rule $f(w) = \sqrt{w}$ is concave, so a wallet's voting power grows with its balance at a diminishing rate. A whale who doubles their stake gains only $\sqrt{2} \approx 1.41\times$ more votes, while a small holder with w tokens wields $1/\sqrt{w}$ votes per token — disproportionately more than a whale.

Why it was proposed. Lalley and Weyl prove that quadratic cost is the *unique* pricing rule achieving robust welfare optimality under a price-taking assumption: a voter equating marginal cost to marginal benefit casts votes proportional to their true valuation of the proposal. Beyond this theoretical benefit, Lalley and Weyl claim that the mechanism provides a good balance between voter intensity and decentralizing power.

Where it is deployed. Gitcoin implemented a QV-style system with Quadratic Funding [31]. Citing issues of plutocracy, they use quadratic scaling in order to allocate funding for different projects. Proponents of QV often herald this as a solution to the overcentralization seen with linear voting, but concerns about collusion and sybil-vulnerability persist. For this reason, Gitcoin uses anti-Sybil mechanisms to prevent an attacker from arbitrarily splitting their tokens into many wallets to gain a disproportionate advantage over the system [26]. Collusion, however, remains a threat.

3 DAO Governance Model

We present a mathematical model for analyzing DAO governance. We define the concept of a voting rule that assigns votes to a wallet based on its wealth and give a precise mathematical definition of a plutocratic voting rule. We show how to measure Sybil-adjusted voting power.

We then introduce our model of a cost scheme that captures the frictions a real Sybil attacker faces on a permissionless blockchain. An adversary can create additional wallets freely, but each wallet incurs gas to receive tokens and to cast a vote. In addition, some DAOs impose a threshold below which a wallet cannot vote at all to deter spam. Building on the model in Bennett [7], our model exposes these frictions as a cost scheme alongside the voting rule function. The attacker's optimization problem becomes a function of on-chain costs and protocol design choices.

We intentionally omit any extraneous utility function. As previous attacks have shown, the attacker's ultimate utility is measured outside the system through extraneous effects. We are concerned with a worst-case analysis for governance safety. An attacker seeking to

destroy a system does not care about the nominal value of tokens. Therefore, we evaluate using a simple question: how much voting power can an attacker extract from a wallet?

3.1 Parameters

A DAO governance instance and a would-be attacker are described by the following parameters, all denominated in the DAO's governance token.

- $a \in \mathbb{R}^+$: the total number of governance tokens controlled by the participant (the *adversary's budget*).
- $W = \{w_1, \ldots, w_n\} \in \mathbb{R}^{n+}$: the balances of the n wallets into which the adversary splits the tokens.
- $f : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$: the wallet-level vote valuation function defining the voting mechanism. Linear voting corresponds to $f(w) = w$; quadratic voting to $f(w) = \sqrt{w}$; power voting to $f(w) = w^\beta$ with $\beta \in (0, 1)$; logarithmic voting to $f(w) = \ln(w + 1)$.
- $m \in \mathbb{R}_{\geq 0}$: the minimum token balance a wallet must hold in order to vote (the *voting threshold*). Some DAOs set $m = 0$; others require a dust amount to discourage spam.
- $v \in \mathbb{R}_{\geq 0}$: the average per-wallet cost of casting a vote, converted into tokens. Empirically this is the gas for a `delegate`, if applicable, and a `castVote` transaction.
- $p \in \mathbb{R}_{\geq 0}$: the *fixed* (one-shot) cost of preparing the Sybil split. This covers, *e.g.* the gas for deploying a batch-transfer helper contract, off-chain key generation, or any per-attack infrastructure that does not scale with n.
- $s \in \mathbb{R}_{\geq 0}$: the average *per-wallet* cost of splitting tokens, *i.e.* the gas to transfer tokens from the adversary's main wallet into each new wallet (one ERC-20 `transfer` per wallet).
- $C \in \mathbb{R}^4$: a cost scheme $C = (m, v, p, s)$ imposed on top of a voting rule. Intuitively, the rule f defines how many votes a wallet w has, while the cost scheme imposes costs to splitting a wallet a into multiple wallets w.

We assume that there is no other external source of friction (e.g. KYC, proof-of-personhood, rate-limits) outside of the above parameters. We also enforce that one of $m, v, s > 0$. Our model precisely captures the scenario of an on-chain permissionless DAO.

3.2 Voting Schemes

We define a voting scheme and how to measure the voting power of a wallet holder.

▶ **Definition 1** (Voting Rule). *A voting rule is a function*

$$f : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$$

that assigns $f(x)$ votes to a wallet holding x tokens. We assume the rule is nontrivial, i.e., there exists some $k > 0$ such that $f(k) > 0$.

The voting rule simply assigns votes to each wallet. Since a wallet holder can split a larger wallet into multiple wallets, we need to consider the actual voting power based on all the possible splits.

▶ **Definition 2** (Sybil-Adjusted Voting Power). *Given total wealth $a \geq 0$, define the Sybil-adjusted voting power as*

$$V^*(a) = \sup_{\substack{w_1,\ldots,w_n \geq m \\ w_1+\cdots+w_n+n(s+v)+p \leq a}} \sum_{i=1}^{n} f(w_i).$$

In a plutocratic system, the number of votes increases at least linearly with total wealth. We use Sybil-adjusted voting power rather the voting rule itself to measure the advantage.

▶ **Definition 3** (Plutocratic Voting Rule). *A voting rule is said to be* plutocratic *if there exist constants $\alpha > 0$ and a_0 such that for all $a \geq a_0$,*

$$V^*(a) \geq \alpha \cdot a.$$

We call α the ***vote-yield per coin****.*

The constant α helps us measure how many votes a plutocrat can extract from a wallet a. However, it does not accurately measure the plutocratic advantage. Consider two voting schemes $f(a) = a$ and $f'(a) = a/3$. Both schemes give plutocrats the same fraction of the total votes but result in different ratios $\alpha_f = 1$ and $\alpha_{f'} = 1/3$. We use the vote-yield to measure the asymptotic advantage.

3.3 Cost Scheme

A cost scheme $C = (m, v, p, s)$ is imposed on top of a voting rule f. As mentioned earlier, m is the minimum wallet balance allowed, p is the initial setup cost for splitting into multiple wallets, s is the splitting cost of creating a wallet, and v is the cost of a single wallet casting a ballot. The cost p is paid once, while $s + v$ are paid for each wallet that votes. So, a voter with n wallets pays $C(n) = p + n(s + v)$ to vote.

▶ **Definition 4** (Linear Voting Cost). *Let $W = \{w_1, w_2, \ldots, w_n\}$ be a set of n wallets. We say that C is a linear cost scheme if the cost $C(W) = \Omega(n)$. A cost scheme $C = (m, v, p, s)$ with fixed values is by definition linear.*

For standard ERC-20 tokens, splitting a balance across multiple wallets incurs linear cost. However, there are some tokens which implement non-linear fees for transfers, such as charging a percentage of the transferred value [27]. To the best of our knowledge, we do not know of any DAO governance token that charges non-fixed voting fees.

4 Plutocracy is Robust to Splitting Costs

To help motivate the optimal Sybil strategy for our class of concave functions, we first show that all non-trivial wallet-based voting rules are plutocratic. We note that increasing linear rules such as $f(w) = w$ and increasing convex rules such as $f(w) = w^2$ are obviously plutocratic because larger wallets get a natural advantage. A more interesting case is concave rules that give voters an incentive to gain voting power by splitting their wealth into smaller wallets.

We outline the proof:

1. We begin with the Sybil Voting Power Lemma that computes a lower-bound on the voting power of a large wallet split into equal m-size chunks.

2. This leads us to the Sybil-Induced Plutocracy Theorem that shows that the minimum vote-yield of this even split strategy is a constant, which means wallet-based voting is plutocratic.

3. Finally, the Robustness of Plutocracy to Cost Theorem shows that all linear cost schemes reduce to an instance of the Sybil-Induced Plutocracy Theorem.

▶ **Lemma 5** (Sybil Voting Power Lemma). *Let f be a non-trivial voting rule for which there exists $m > 0$ such that $f(m) > 0$. Then for all wallets $a \geq m$,*

$$V^*(a) \geq \left\lfloor \frac{a}{m} \right\rfloor f(m).$$

▶ **Theorem 6** (Sybil-Induced Plutocracy). *Every nontrivial voting rule is plutocratic under unrestricted Sybil wallet splitting. Specifically, if $\exists m > 0 : f(m) > 0$, then for all $a \geq 2m$, there exists a constant $\alpha > 0$ such that $V^*(a) \geq \alpha \cdot a$.*

▶ **Theorem 7** (Robustness of Plutocracy to Costs). *Suppose there is a non-trivial voting scheme combined with a cost scheme $C = (m, v, p, s)$ where there are fixed costs of additional wallet creation $p \geq 0$, a wallet splitting cost $s \geq 0$ per wallet, a voting cost $v \geq 0$ per wallet, and a minimum wallet size m. The Sybil-adjusted voting power is still plutocratic and satisfies:*

$$V_C^*(a) = \Omega(a).$$

Due to space constraints, all proofs are deferred to Section A.

5 Turning Concave Mechanisms Linear

In the previous section, we proved that all non-trivial voting rules are plutocratic under a Sybil attack, even if accounting for a linear cost function. This proves a loose lower bound on available power. In this section, we demonstrate that a simple attack—splitting wallets into equal parts—is optimal for most useful concave voting rules (i.e. those that are finite, positive, and increasing in token size). We then prove an optimal attacker's power is asymptotically linear, reversing the intended anti-plutocratic effect beyond a lower bound.

Notice that convex and linear rules like $f(w) = w^2$ and $f(w) = w$, respectively, are already plutocratic. Therefore, a wallet holder gains no benefit from Sybil splitting under those regimes. Beyond this, virtually all on-chain voting rules are finite, positive, and increasing to reward governance participation as well as prevent trivial exploitation. We ignore non-concave and non-convex, disjoint, and other non-standard rules as those require custom attacks to achieve optimal results. This leaves our set of concave functions for analysis.

Main result. *Every finite, positive, increasing, concave wallet-level voting rule f collapses to asymptotically linear voting power under a Sybil attack.*

5.1 High-Level Description

Concretely, Theorem 10 below shows that the attacker's optimal aggregate voting power $V^*(W)$ satisfies $V^*(W) \leq \kappa\,(a - p)$, with matching asymptotic tightness as $a \to \infty$. The constant κ depends only on f and the per-wallet cost $v + s$. Concavity, therefore, buys a constant-factor dampening, but *no* sublinear dampening. A sufficiently wealthy attacker can effectively convert any concave rule back into linear voting power. The argument decomposes into three steps, mirroring the attack stages of Figure 1:

Step 1 (Lemma 8). For a fixed number of wallets n, the sum $\sum_i f(w_i)$ is maximized by an even split $w_i = a/n$. This is a direct consequence of Jensen's inequality and rules out any "clever" unequal allocation.

Step 2 (Lemma 9). Given the even-split structure and the costed budget constraint $p + n(v + s) + \sum_i w_i \leq a$, the optimal per-wallet balance is $w^* = \frac{a-p}{n} - v - s$ when the minimum bound holds with slack. This reduces the attacker's problem to choosing the *number* of wallets n, which we optimize over to find maximum power.

Step 3 (Theorem 10). Optimizing over n yields $V^*(W) \leq \kappa\,(a-p)$ with $\kappa = \sup_{x \geq m} f(x)/(x + v + s)$, and this bound is asymptotically tight as $a \to \infty$. The concave rule is thus *asymptotically linear* in the attacker's token holdings; concavity buys a constant factor, not a sublinear dampening.

The three subsections below execute these steps in order. A reader interested only in the final result can skip to Theorem 10 after reading the "Takeaway" paragraph of each subsection.

5.2 The Sybil Attack, Step by Step

Figure 1 traces the Sybil attacker's strategy under the cost scheme $C = (m, v, p, s)$ from Section 3.1. Starting from a single wallet holding a tokens, the attacker:

1. Pays the fixed setup cost p;
2. Divides the remaining $a - p$ tokens evenly across n new wallets;
3. Pays s per wallet to fund each new wallet;
4. Pays v per wallet to cast a vote;
5. Casts one vote per wallet, for n votes total.

After all costs, each wallet holds $w^* = \frac{a-p}{n} - v - s$ tokens at vote time and contributes $f(w^*)$ votes, so the attacker's aggregate voting power is

$$V^*(W) \;=\; n\, f\!\left(\frac{a-p}{n} - v - s\right).$$

Theorem 6 (Sybil-Induced Plutocracy) already establishes that for some choice of n, this strategy achieves a vote-yield $\alpha > 0$ for any nontrivial f. What is left open — and what we sharpen below for concave f — is the *tight* asymptotic slope κ: the maximum amplification an optimizing attacker actually attains in the limit. The lemmas in the next three subsections close this gap by, in order, showing that the even split assumed in step (ii) is optimal (Lemma 8), that the per-wallet balance w^* above is optimal once n is fixed (Lemma 9), and that optimizing over n yields $V^*(W) \leq \kappa\,(a - p)$ with matching asymptotic tightness (Theorem 10).

5.3 Even Wallet Splits Are Optimal

The intuition is purely economic: a concave f gives *diminishing marginal returns* in voting power per token, so any wallet holding more than the group average is wasting its marginal tokens. The excess tokens would earn strictly more voting power if moved to a wallet below the average. Jensen's inequality converts this intuition into a mathematical relation.

▶ **Lemma 8** (Even-split optimality). *Let $f : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ be concave. Fix a total token amount $a > 0$ and an integer $n \geq 1$. Among all allocations $(w_1, \ldots, w_n)$ satisfying $w_i \geq 0$ and $\sum_{i=1}^n w_i = a$, the sum of voting power $\sum_{i=1}^n f(w_i)$ is maximized by an even split: $w_i = \frac{a}{n}, \forall i$.*

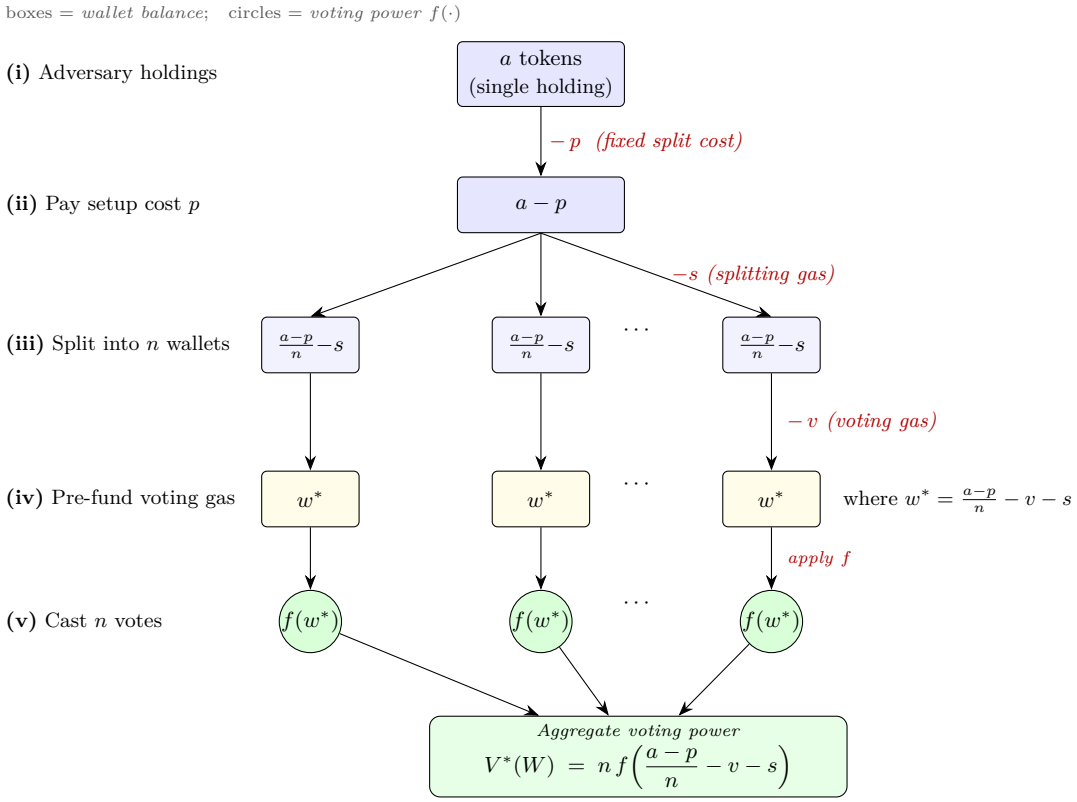

Figure 1 Sybil attack accounting under a concave wallet-level voting rule f. Rows (i)–(iv) track each wallet's *token balance*; row (v) is the resulting *voting power*, obtained by applying f to the balance. An adversary with a tokens pays a fixed setup cost p (*e.g.* deploying a splitter contract), and divides the remainder *evenly* across n wallets (optimal by Lemma 8). The splitting cost s is paid at step (iii) as it is the gas for the ERC-20 transfer into each new wallet. So the post-split wallet balance is $\frac{a-p}{n} - s$. The voting cost v is *physically* paid at step (v) when `castVote` is called; however, because gas is funded by pre-selling governance tokens at attack-start, each wallet's snapshot-time balance already reflects this pre-deduction, giving $w^* = \frac{a-p}{n} - s - v$ at step (iv). Every wallet that satisfies the voting threshold $w^* \geq m$ casts one vote of weight $f(w^*)$, yielding aggregate voting power $V^*(W) = n\, f\!\left(\frac{a-p}{n} - v - s\right)$. The adversary chooses n to maximize this quantity.

Proof. Because f is concave, Jensen's inequality yields

$$f\left(\frac{1}{n}\sum_{i=1}^{n} w_i\right) \geq \frac{1}{n}\sum_{i=1}^{n} f(w_i).$$

Substituting the average wallet balance $\frac{a}{n} = \frac{1}{n}\sum_{i=1}^{n} w_i$ on the left and multiplying both sides by n gives

$$n\, f\left(\frac{a}{n}\right) \geq \sum_{i=1}^{n} f(w_i).$$

Thus, for every feasible allocation $(w_1, \ldots, w_n)$, the total voting power is upper-bounded by $n\, f(a/n)$, and this upper bound is achieved by the equal allocation $w_i = a/n$ for all i. ◀

> **Takeaway.** Given a fixed token budget and a concave voting scheme, the attacker's best strategy is to distribute tokens *equally* across wallets. Any uneven allocation strictly lowers total voting power. This simplifies the attacker's problem to deciding how many wallets to use.

5.4 Optimal Token Amount

Now that we know an even token split is optimal, we use Lemma 8 to determine the optimal amount of tokens per wallet given a fixed number of wallets. For simplicity, we restrict to the case where the minimum wallet bound is not enforced.

▶ **Lemma 9** (Unrestricted Optimal Token Amount per Wallet). *Let $f : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ be positive, concave, and increasing. Fix a total token amount $a > 0$ and an integer $n \geq 1$. Further, assume $\frac{a-p}{n} - v - s \geq m$. Among all allocations $(w_1, \ldots, w_n)$ satisfying $w_i \geq m$ and $p + n(v+s) + \sum_{i=1}^{n} w_i \leq a$, then the optimal voting power will be:*

$$w^* = \frac{a-p}{n} - v - s$$

Proof. We set up the constrained optimization problem representing the maximum voting power available to a user:

$$V^*(W) = \max_{w_i} \sum_{i=1}^{n} f(w_i),$$

subject to (i) $p + n(v+s) + \sum_{i=1}^{n} w_i \leq a$ and (ii) $w_i \geq m$, $\forall i$. By Lemma 8, an even split of tokens among the wallets yields optimal voting power. Moreover, since f is increasing, the budget constraint must bind at the optimum; otherwise, we could increase some w_i while remaining feasible and strictly increase $\sum_{i=1}^{n} f(w_i)$. Hence, under an even split,

$$p + n(v+s) + nw^* = a$$
$$w^* = \frac{a-p}{n} - v - s.$$

Since $\frac{a-p}{n} - v - s \geq m$ by assumption, $w_i \geq m$ for all i as well as the budget constraint are satisfied. ◀

5.5 The Optimal Voting Power

First, we discuss the case where the minimum wallet bound is enforced and provide an intuitive understanding of how that leads to asymptotically linear voting power as $a \to \infty$. This case has the unconstrained optimal wallet size satisfying $w^* < m$. Because f is concave and increasing, an attacker maximizes voting power by splitting tokens into as many wallets of size approximately m as the budget allows. The problem therefore reduces to dividing the budget into portions of size $m + v + s$, each contributing approximately $f(m)$ voting power, yielding $V^*(W) \approx \frac{a-p}{m+v+s} f(m)$, which is linear in a.

Next, we consider the more significant case: when the minimum balance holds with slack (i.e. $\frac{a-p}{n} - v - s \geq m$). We combine the two preceding results into the main theorem of this section. For any fixed number of wallets n, Lemma 8 tells us to distribute tokens evenly and Lemma 9 tells us each wallet must hold $w^* = \frac{a-p}{n} - v - s$; the only choice left to the attacker is the integer n itself.

A single-wallet honest participant, by contrast, receives only $f(a)$ — a quantity that grows *sublinearly* in a whenever f curves. What makes the theorem below striking is that, no matter which concave rule in our class f that we began with, the attacker's optimal aggregate voting power $V^*(W)$ grows *linearly* in the total budget a asymptotically. Concavity earns the mechanism only a constant-factor reduction in the attacker's effective growth rate — captured by a single number κ depending only on f and the per-wallet cost $v + s$ — but provides no sublinear dampening whatsoever. The next few lines fix notation and derive the closed form before stating the theorem.

Fix an integer $n \geq 1$ satisfying $m \leq \frac{a-p}{n} - v - s$. An optimal split into n wallets is an even split, yielding the following values of w_i:

$$w_i^* = \frac{a-p}{n} - v - s \qquad (i = 1, \ldots, n)$$

Aggregating across our n wallets, this achieves a total voting power:

$$V(W) = nf\left(\frac{a-p}{n} - v - s\right)$$

A naive participant holds all tokens in one wallet. This yields a voting power of $f(a)$. The attacker, however, optimizes the number of wallets into which they split their tokens. This yields the optimal voting power:

$$V^*(W) = \max_{n \in \mathbb{N}_{\geq 1}:\ m \leq \frac{a-p}{n} - v - s} nf\left(\frac{a-p}{n} - v - s\right)$$

We now show that this allows an attacker to obtain asymptotically linear voting power in their number of tokens, a, despite the concave mechanism.

▶ **Theorem 10** (Concave Mechanisms Are Asymptotically Linear-Exploitable in Token Amount)**.** *Let $A = a - p$ and $c = v + s$. Assume that there exists at least one integer $n \geq 1$ such that*

$$m \leq \frac{A}{n} - c$$

Define the values:

$$g(x) = \frac{f(x)}{x + c} \qquad \text{and} \qquad \kappa = \sup_{x \geq m} g(x) < \infty$$

Then, we have that:

1. *(Linear upper bound) The optimal voting power satisfies*

$$V^*(W) \le \kappa A$$

2. *(Asymptotic tightness) If g attains its supremum on $[m, \infty)$ at some $x^* \ge m$, then*

$$\lim_{a\to\infty} \frac{V^*(W)}{A} = \kappa$$

The proof of the theorem is deferred to Section A.

> **Takeaway.** No matter which concave rule f is chosen, the attacker's optimal voting power grows *linearly* in their token budget: $V^*(W) \le \kappa\,(a-p)$, with equality in the limit $a \to \infty$. The constant $\kappa = \sup_{x\ge m} f(x)/(x+v+s)$ depends only on the mechanism and the gas-denominated per-wallet cost. Geometrically it is the slope of the steepest line through the origin that lies above the attacker-return curve. In other words, concavity provides a finite dampening factor but *no sublinear dampening*: an attacker with enough tokens faces the same linear-in-a cost–benefit as under one-token-one-vote, recovering plutocracy up to a constant.

5.6 Closed forms for common concave rules

Having established our main result, we now specialize the optimization to the three concave rules most often proposed for DAO governance — quadratic, power, and logarithmic — and obtain closed forms for $V^*(W)$. In order to do this, we consider a relaxation n to be positive real numbers. Assuming the minimum-wallet-balance constraint is nonbinding at the relaxed optimum, Theorem 10 implies that the integer optimum is asymptotically equal to the relaxed optimum as $a \to \infty$. Table 1 collects the resulting expressions, and Corollary 11 states them formally.

Voting Function	**Traditional Form**	**Worst-Case Sybil Form**
Linear Voting	$V(W) = a$	$V^*(W) = a$
Quadratic Voting	$V(W) = \sqrt{a}$	$V^*(W) = \frac{a-p}{2\sqrt{v+s}}$
Power Voting ($\beta \in (0,1)$)	$V(W) = a^\beta$	$V^*(W) = \frac{(a-p)(\beta^\beta)(1-\beta)^{(1-\beta)}}{(v+s)^{1-\beta}}$
Logarithmic Voting	$V(W) = \ln(a+1)$	$V^*(W) = \frac{(a-p)\,W_0\left(\frac{v+s-1}{e}\right)}{v+s-1}$

Table 1 Traditional vote power compared to Sybil-optimal voting power for the linear baseline and standard concave functions

▶ **Corollary 11** (Closed forms for common concave rules). *Let $A = a - p$ and $c = v + s$ and assume the minimum wallet bound is a slack condition. Under the conditions of Theorem 10, the attacker's optimal voting power admits the following closed forms.*

1. ***Power voting.*** *If $f(x) = x^\beta$ with $\beta \in (0,1)$, then*

$$V^*(W) \;=\; \frac{A\,\beta^\beta(1-\beta)^{1-\beta}}{c^{1-\beta}}.$$

As a special case, quadratic voting *($\beta = 1/2$, $f(x) = \sqrt{x}$) yields $V^*(W) = A/(2\sqrt{c})$.*

2. ***Logarithmic voting.*** *If* $f(x) = \ln(x+1)$*, then*

$$V^*(W) \;=\; \frac{A\,W_0((c-1)/e)}{c-1},$$

where W_0 *denotes the principal branch of the Lambert W function.*[1]

The derivations of the closed forms are deferred to Section A.

6 Estimating the Impact on Modern DAOs

In this section, we instantiate our model with on-chain data from five major DAOs — ENS, Compound, ZKsync, Arbitrum, and Uniswap — and replay their ten most recent finalized proposals under linear, quadratic, power, and logarithmic voting. The goal is to quantify how much cheaper a Sybil attacker's vote is than an honest voter's on real protocols, and to test whether economic frictions (gas, minimum balances) meaningfully deter the attack.

Getting data. We pull address-level voting data from Tally [29][2] for the ten most recent finalized proposals for five well-known DAOs: *ENS* (naming service), *Compound* (lending), *ZKsync* (zero-knowledge rollup), *Arbitrum* (optimistic rollup), and *Uniswap* (decentralized exchange) The DAOs were chosen for their size and active governance as each had at least one proposal finalized within the three months preceding our data collection on April 20, 2026. We exclude active, canceled, and draft proposals so that every entry in our dataset has a stable tally. Our query is governor agnostic which matters for ZKsync and Arbitrum who have multiple governors that control different aspects of the protocol.

We also pull USD spot prices for ETH and the governance tokens (ENS, COMP, ZK, ARB, UNI) from CoinGecko [8] on the days proposals were created.

Gas accounting. We compute each of the splitting cost s and voting cost v as the product of the number of gas units the corresponding action consumes and the per-unit gas price paid on the proposal's chain. ENS, Compound, and Uniswap run governance on Ethereum, where we use 65,000 gas for splitting (ERC-20 `transfer` to a new address) and 175,000 gas for voting (approximate combined amount for `delegate` and `castVote` transactions on Uniswap). ZKsync and Arbitrum are rollups on top of Ethereum and run their governance on the rollup, where a transaction pays for its own execution plus its share of the cost of posting that execution back to Ethereum. Since both rollups batch transactions and fold that share into each transaction's reported gas, we set their budgets conservatively at 500,000 gas for both splitting and voting.

Per-unit gas prices can vary depending on chain conditions, so we calculate them for each proposal rather than holding them constant. For Ethereum and Arbitrum we query Etherscan [16] for `baseFeePerGas` and average it across blocks sampled from the day the proposal was created. For ZKsync we fetch the base fee directly from ZKsync's public API [23] using the block the proposal was created on. Ethereum's base fee has lots of variation, Arbitrum's is relatively stable, and ZKsync's is constant because it is set by a

[1] The *Lambert W function* is the inverse of $z \mapsto z\,e^z$: by definition, $W(z)\,e^{W(z)} = z$. The *principal branch* W_0 is the (unique) real-valued branch on $[-1/e, \infty)$, satisfying $W_0(0) = 0$ and $W_0(z) \to \infty$ as $z \to \infty$. A useful identity, applied in the proof, is $e^{W_0(z)} = z/W_0(z)$ for $z \neq 0$, which follows directly from the defining equation.

[2] The authors are aware that Tally announced it is shutting down (`https://newsletter.tally.xyz/p/tally-is-shutting-down`). We do not believe the announcement affects the quality of the raw vote data our evaluation relies on.

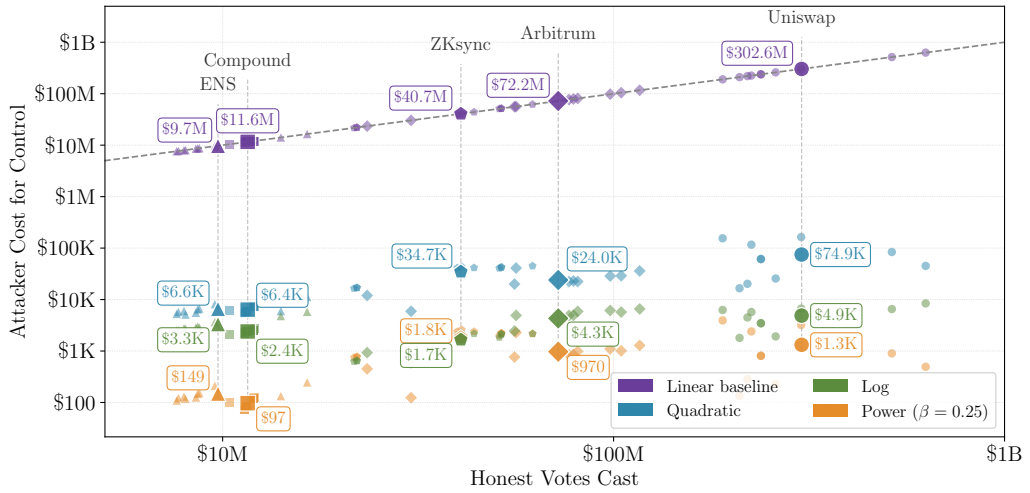

Figure 2 An attacker's cost to achieve voting control across five DAOs under four voting functions. Large dots are per-protocol means over the ten most recent finalized proposals and are annotated with their value while background dots are individual proposals. The dashed $y = x$ line is the linear-equivalent baseline, so distance below it is the amplification factor gained by an attacker performing our attack. Axes are in USD and are on a log scale while color encodes the voting function and shape encodes the protocol.

protocol-defined rule rather than chain conditions. We set $p = 0$ throughout, treating any one-time attack setup cost as negligible.

Analysis. We are now able to replay all 50 proposals to analyze the benefit an attacker would have from splitting their votes. We run the analysis with linear (baseline), quadratic, power ($\beta = 0.25$), and logarithmic voting functions.

For each proposal we begin by computing the total voting power of all participants as $\sum_i f(w_i)$ where f is the voting function. We aggregate every recorded voter, regardless of whether they voted for, against, or abstain, because we do not know which side of the proposal the attacker would take and the worst case for the attacker is to face every honest voter aligned against them.

The attacker's budget to match the voting power of all honest voters is the value of a that solves $V^*(W) = \sum_i f(w_i)$. We obtain a for each proposal by plugging its s and v (recall $p = 0$) into the closed form equation from Section 5.6. We report the result in USD so that all protocols are directly comparable.

Attack cost by DAO. Figure 2 plots the attacker's cost to achieve voting control for every (DAO, voting function) pair. The averages per protocol are bolded and labeled with their value which can also be seen in Table 2. Linear voting is immune to the attack, so every dot is on the $y = x$ diagonal and the attacker must have USD equal to the amount voted by all honest participants. However, every concave function collapses the cost for the attacker by three to five orders of magnitude with exact amplification factors listed in Table 2.

Isolating the role of splitting. The amplification factors in Table 2 conflate two effects: the concavity of the voting rule and the attacker's freedom to split wallets. To isolate the second, we hold the attacker's USD budget fixed at the Sybil-optimal control cost and ask how much voting power the *same* budget delivers under quadratic voting with and

Table 2 Mean attacker cost to achieve voting control across the ten proposals sampled from each DAO, for each voting function. Linear voting is Sybil-immune (splitting does not help), so its column is the capital cost of acquiring the tokens outright and serves as the worst case any Sybil-resistant rule should demand. The parenthesized multiplier is the *Sybil amplification factor* — i.e., how many times cheaper the attack becomes under the concave rule than under the Sybil-immune linear baseline. Amplification above 1× means the concave "improvement" is *worse* than linear against an optimal Sybil attacker.

Protocol	Linear	Quadratic	Log	Power ($\beta = 0.25$)
ENS	\$9.7M	\$6.6K (1,472×)	\$3.3K (2,912×)	\$149 (65,290×)
Compound	\$11.6M	\$6.4K (1,820×)	\$2.4K (4,835×)	\$97 (119,328×)
ZKsync	\$40.7M	\$34.7K (1,172×)	\$1.7K (24,539×)	\$1.8K (22,247×)
Arbitrum	\$72.2M	\$24.0K (3,006×)	\$4.3K (16,763×)	\$970 (74,392×)
Uniswap	\$302.6M	\$74.9K (4,039×)	\$4.9K (62,041×)	\$1.3K (229,175×)

without splitting. Figure 3 plots this comparison. Blue dots sit on the control-threshold line $V_{\text{attacker}} = V_h$: at the Sybil-optimal budget, a splitting attacker matches the honest total by construction. Red dots, at the same x and the same dollar spend, plot $\sqrt{a_{\text{tokens}}}/V_h$ — the fraction of V_h a single-wallet attacker achieves with that same budget. The upward arrow per protocol, annotated with the amplification factor, is the share of voting power the attacker gains purely by splitting, with no additional capital. For Uniswap, the same \$74.9K delivers full control when split across many wallets and only roughly $\frac{1}{259}$ of V_h when held in a single wallet; every other DAO in our sample shows a similarly large gap.

Voting power per dollar. Beyond total cost, another way to see the attacker's advantage is to compare voting power per dollar: how many votes each dollar of budget delivers for an honest voter versus for the attacker. This is calculated as $V(a)/a$ for an honest voter and $V^*(a)/a$ for the attacker. Figure 4 plots these results for quadratic voting on Uniswap while Section B plots the results for logarithmic and power voting.

The linear baseline maintains one-token-one-vote, so the voting power per dollar is constant at 1. The honest curve is strictly decreasing because concave voting functions discount marginal tokens — each additional dollar contributes less than the previous one.

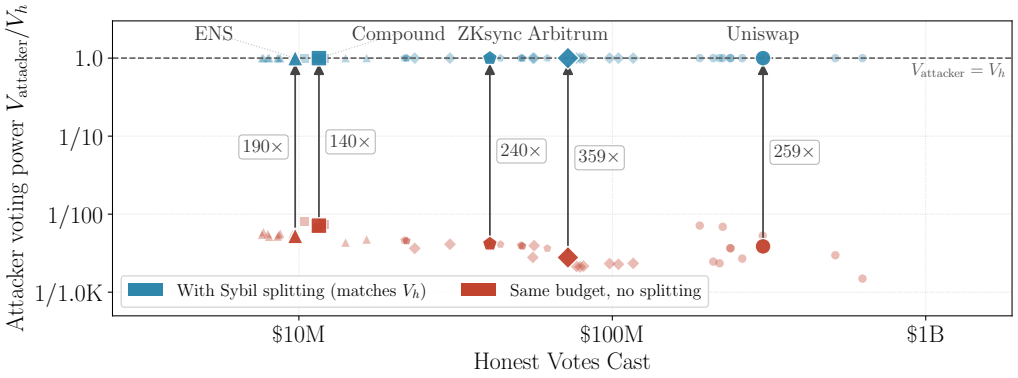

Figure 3 Attacker voting power as a fraction of the honest total V_h under quadratic voting, at the Sybil-optimal control budget from Table 2. Blue dots: Sybil-optimal splitting (sits on $y = 1$ by construction). Red dots: the same budget held in a single wallet. Upward arrows, labeled with the amplification factor, visualize the voting power gained purely from splitting.

The attacker's curves asymptotically plateau at κ as proven in Theorem 10.

Unlike in the previous section, $V^*(a)$ here is the integer-optimal value, not the relaxed value, and consequently the curves have a wavy shape. To see why, follow the attacker's decisions as the budget a grows. Right after the attacker opens a new wallet, the extra budget is spread evenly across every wallet. Because the gas cost c of each wallet is already paid while voting tokens keep accumulating in every wallet, each extra dollar buys more voting power than the dollar before it, and the votes-per-dollar ratio climbs. Eventually the concavity of the voting rule takes over and each new token buys less voting power than the token before it. The ratio peaks (at κ) and starts to slide back down. It keeps sliding until opening another wallet — paying a fresh c in gas but then distributing tokens across more wallets — becomes the better move. At that moment the attacker splits, the budget is redistributed evenly across the now-larger pool of wallets, and the cycle begins again: rise, peak, fall, split.

Every new wallet brings with it an additional c of gas cost that has to be taken from budget that the attacker previously voted with. All of the existing wallets evenly share this additional cost. So the per-wallet share shrinks with every new wallet, and the dips grow shallower with each cycle, drawing the curve ever closer to the asymptote κ from below.

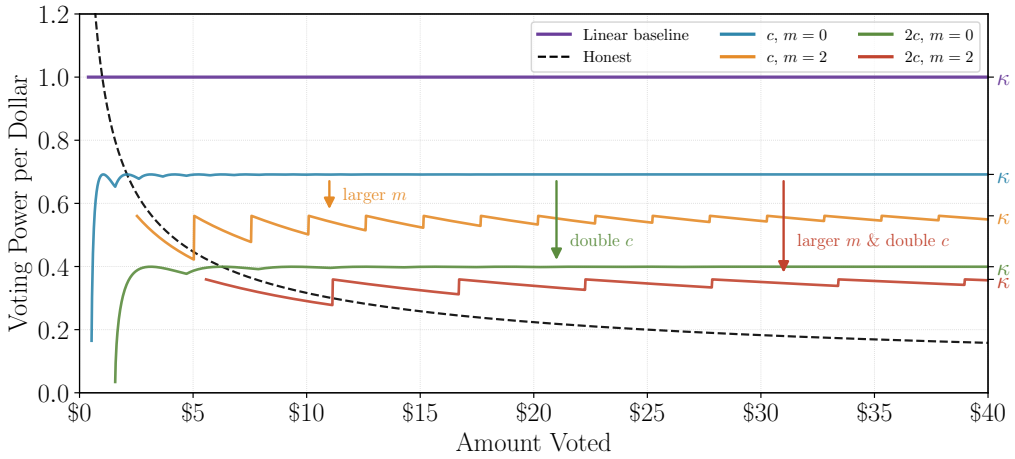

Figure 4 Voting power per dollar for Uniswap in our model under quadratic voting. The dashed curve shows $V(a)/a$, an honest participant's voting power per dollar. The solid curves show $V^*(a)/a$, the attacker's Sybil-optimal voting power per dollar. While honest voters see their power per dollar decline with every increasing dollar, the attacker's power per dollar eventually plateaus at κ (shown on the right axis). The orange, green, and red curves illustrate the effect of increasing m and doubling c to try and defend against the attack. While the curves are below the blue, which has $m = 0$ and regular c, the attacker's power per dollar still plateaus, just at a lower level.

Voting Power with Frictions. Figure 4 also shows what happens to the attacker's voting-power-per-dollar curve on Uniswap under quadratic voting when c or m is changed. Section B show the same for logarithmic and power voting. Raising c means each wallet costs more in gas, so the attacker's budget is consumed faster by new wallets. Raising m forces each wallet to hold more tokens than the attacker would naturally choose, concentrating power in fewer, over-funded wallets. Each effect lowers the plateau κ: the orange line (with $m = 2$) sits below the baseline blue, the green line (with c doubled) sits lower still, and the red line (both $m = 2$ and c doubled) sits lowest of all. Crucially, every curve still flattens into a

plateau, just at a different height. This illustrates how the asymptotic linearity guaranteed by Theorem 10 still holds in spite of additional frictions. Raising c or m can lower the slope of that linear growth and push out when the attack first becomes profitable, but it cannot turn the concave rule's response into anything sublinear in the attacker's budget.

Caveats. It is alarming that an attacker can control proposals from some of the largest DAOs with 1,100-4,000× less cost than all honest voters combined when Quadratic Voting is in place and 2,900-62,000× less cost when logarithmic voting is in place. That said, there are some caveats to consider.

The analysis assumes that honest voters behave the exact same way under all voting functions. In reality, voters may behave differently depending on the voting function used, making the attack less effective.

Further, attackers may be more interested in creating and passing a malicious proposal (i.e. stealing a DAO's treasury) than swaying the vote on proposals from honest participants. In this scenario, honest voters would fight to thwart the attack, and the participation rate and amounts of votes cast would likely be higher making the attack more expensive.

7 Mitigation Discussion

Our result relies on a single assumption: an attacker can create wallets at a cost-per-wallet that does not depend on the attacker's identity. Every mitigation in this section either attacks that assumption (by binding wallets to identities) or accepts it and composes concave voting with a second mechanism layer. No defense we are aware of preserves the assumption *and* breaks asymptotic linearity against a patient, well-capitalized adversary. We group candidate defenses into three families and assess each.

Breaking Sybil Capacity: Proof-of-Personhood Layers. One simple defense is to enforce one entity one vote. *Proof-of-Personhood* (PoP) systems — Worldcoin's iris biometrics, BrightID's social-graph analysis, and Gitcoin Passport's aggregated-stamp scoring, among others — each attempt to issue at most one voting credential per human without a central registry. Gated by such a credential, a concave rule f really does move voting power away from whales because the number of credentials a single adversary can obtain is bounded. The catch is that every PoP design today makes a trade along one of three axes: (i) *privacy*, by requiring biometric or off-chain enrollment; (ii) *inclusivity*, by excluding participants who cannot or will not enroll; or (iii) *adversarial robustness*, since stamp-based and social-graph designs can be farmed at a cost much lower than their economic weight. Of these, stamp farming is the most relevant to DAO governance: a sufficiently wealthy attacker can purchase or synthesize stamps at a price that is still small compared to the governance value at stake, effectively reintroducing a costed-per-identity version of our attack. PoP is thus best framed as a *necessary but not sufficient* substrate — the only known defense that formally breaks our theorem, provided the specific PoP instantiation's stamp price exceeds the governance-capture payoff. This same bound applies to a network of colluders who temporarily redistribute tokens for a vote to equalize their wallet holdings.

Raising the Cost of Sybils: Economic Friction. A second way of defense is to make Sybil splitting expensive enough to deter attacks in practice. The natural solutions are per-wallet bonds, long snapshot look-backs, and conviction- or age-weighted voting. Each raises one of the cost terms in our model (i.e., p, s, or the opportunity cost of capital) but none changes the *functional form* of the attacker's problem. Our theorem still applies and $V^*(W)$ remains asymptotically linear in the attacker's budget with a (possibly reduced)

slope κ. Snapshot voting with a short look-back denies opportunistic attacks mounted after a proposal is seen, but a patient attacker pre-splits in anticipation and recovers full power. Longer look-backs and conviction voting (in which voting weight grows with token age in a single wallet, as in 1Hive [1]) extend the attack's preparation window from hours to months. This is a real deterrent against opportunistic adversaries but a patient attacker — precisely the adversary a permissionless protocol must assume — is willing to pre-fund Sybil wallets at token-generation time. Refundable per-wallet bonds increase s, but because the bond is returned after honest behavior they do not raise the attacker's *capital* cost, only their opportunity cost. Moreover, bonds presuppose an adjudication mechanism that can slash them, which itself typically requires the identity layer the scheme was designed to avoid. In conclusion, economic friction buys larger attack windows and smaller κ, not Sybil resistance.

Compositional Defenses: Stacking Mechanisms. The most pragmatic defenses accept that concave voting alone is insufficient and combine it with a second mechanism whose failure modes are disjoint. *Bicameral governance* is one instance: a proposal must pass through two chambers with different rules, typically one concave and one linear. Then an attacker who neutralizes the concave chamber via Sybil splitting still faces the linear chamber's full whale-visible cost. Alternatively, a concave vote can be gated by an *identity quorum*. Here a proposal passes only if $V^*(W)$ clears a weighted threshold and at least k distinct PoP-verified participants vote in favor. This decouples vote weighting from gatekeeping and ensures a single Sybil cluster cannot meet the quorum no matter how many wallets it fabricates.

> **Mitigation summary.** No standalone defense preserves the permissionless blockchain assumption of our model and simultaneously restores sublinear dampening against a patient adversary. Proof-of-Personhood is the only family that breaks our theorem, and it does so by replacing the assumption rather than the voting rule. Economic friction raises attack cost linearly but does not change the asymptotic scaling. Compositional designs accept the attack on the concave layer and contain it at an outer layer. We therefore recommend that concave voting be deployed only as one component of a composite governance mechanism whose outermost Sybil-resistance layer is identity-based — never as the primary line of defense.

8 Related Work

Two prior works analyze the Sybil vulnerability of QV specifically. Dimitri [12] raises the conceptual concern that permissionless QV deployments cannot enforce the single-identity assumption underlying Lalley and Weyl's optimality guarantee. Bennett [7] formalized this concern for the square-root rule $f(w) = \sqrt{w}$, proving that the Sybil-optimal attacker achieves asymptotically linear voting power, both when the wallet minimum is enforced and when the condition holds with slack. We generalize this result to the entire class of finite, increasing, positive, concave wallet-level rules and instantiate it empirically across five major DAOs. In doing so, we show that parameter modifications to the mechanism (e.g. increased voting costs) are ineffective.

Bennett [7] notes that this Sybil strategy is also available to rational voters, which they may choose to execute as long as the utility they obtain from additional voting power outweighs the cost of the split. Still, Kaplow and Kominers [19] suggest it's unlikely an honest voter would take advantage of it. They claim that the actual number of votes cast under Quadratic Voting would likely significantly deviate from pure, rational QV equilibrium play. This is because voting behavior would more likely be driven by social and psychological factors. Interestingly, they discuss a similar exploit of QV that mirrors our proposed Sybil

attack involving affinity groups, wherein a group encourages voters to contribute small amounts as they have disproportionate impact.

Zhou *et al.* [32] concurrently propose *QV-net*, a decentralized self-tallying QV scheme providing maximal ballot secrecy via new zero-knowledge argument protocols. Their focus is voter privacy [24], preventing the plaintext ballot leakage inherent in current on-chain QV deployments. Their work is orthogonal and complementary to ours. Since QV-net preserves the wallet-level structure of QV, our attack (Theorem 10) still applies, and a privacy-enhanced QV remains asymptotically linear under a rational Sybil adversary.

The broader landscape of DAO governance attacks was recently systematized by Feichtinger *et al.* [18], cataloguing 28 real-world incidents across bribing, token control, human-computer interaction, and code/protocol vulnerability categories. The attack we formalize sits within the token-control family, but exploits a mechanism-design flaw rather than acquiring additional tokens outright: an attacker who cannot afford to buy control under one-token-one-vote can still achieve it under any concave rule by splitting a smaller budget across many wallets.

9 Conclusion

There's nothing inherently bad about using a concave mechanisms, nor a linear one; but system designers need to be aware of how introducing inequalities can have adverse effects. When we design governance, there's an instinct to be inclusive. Blockchains were created for decentralization, so it is reasonable to want to empower small holders through concave voting rules. The issue is that mechanisms aimed at leveling the playing field can inadvertently destabilize it when implemented without guardrails. The people most harmed by governance failure are not the whales with hedges and lawyers. They are the small holders, the newcomers, the communities that cannot afford to be wrong even once. For our most vulnerable participants to reap the benefits, it is imperative that the most powerful cannot exploit them. Otherwise, we perpetuate the structural injustices that the mechanism was supposed to solve.

Concave mechanisms can provide a decentralizing force. But as our analysis demonstrates, they are too dangerous to implement alone when wallet splitting is unlimited. The path forward is to combine concave mechanisms with complementary approaches to ensure their integrity. Proof of Personhood and other anti-Sybil mechanisms can help mitigate the effects on concave mechanisms, while bicameral voting systems can provide an additional backstop. Perhaps the optimal DAO governance system is not a single voting function, but a composition of multiple mechanisms, each resistant to different attack vectors.

Future work should examine compositional mechanism defenses. Additionally, privacy-preserving Proof of Personhood could make anti-Sybil mechanisms more feasible for on-chain governance, reducing such attacks in the first place. If we study these further, we may converge upon a governance system that is more inclusive and fundamentally fair for all of its participants. Decentralization is not merely a slogan. It is a property we have to secure.

References

1 1Hive. Dao proposals. `https://about.1hive.org/docs/dao/Participation/proposals/`, 2026.

2 Aave. Aave Governance. `https://governance.aave.com/`, 2026.

3 Zack Abrams. Indexed DAO to distribute remaining treasury after defeating hijack attempts. The Block, `https://www.theblock.co/post/264679/indexed-dao-to-distribute-remaining-treasury-after-defeating-hijack-attempts`, 2023.

4 Jeff Amico. Open sourcing our token delegate program, August 2021. URL: https://a16z.com/open-sourcing-our-token-delegate-program/.

5 Arbitrum. Arbitrum Governance. https://forum.arbitrum.foundation/, 2026.

6 Rob Behnke. Explained: The Tornado Cash hack. Halborn Blog, https://www.halborn.com/blog/post/explained-the-tornado-cash-hack-may-2023, May 2023.

7 A. Bennett. Going parabolic: Analyzing sybil resistance in quadratic voting mechanisms for blockchain-based daos. Version 1, Stanford Digital Repository, 2025. Version 1. URL: https://purl.stanford.edu/hj860vc2584/version/1, doi:10.25740/hj860vc2584.

8 CoinGecko. CoinGecko API. https://docs.coingecko.com/, 2026. Accessed April 20, 2026.

9 Compound. Compound Governance. https://compound.finance/governance, 2026.

10 Compound Labs. Governance, 2026. Describes Governor Bravo. URL: https://docs.compound.finance/v2/governance/.

11 Defi Llama. DeFi Treasury Ranking. https://defillama.com/treasuries, 2026. Accessed May 15, 2026.

12 N. Dimitri. Quadratic voting in blockchain governance. *Information*, 13(6), 305, June 2022.

13 Maya Dotan, Aviv Yaish, Hsin-Chu Yin, Eytan Tsytkin, and Aviv Zohar. The vulnerable nature of decentralized governance in DeFi. In *Proceedings of the 2023 Workshop on Decentralized Finance and Security (DeFi '23)*, pages 25–31, New York, NY, USA, 2023. Association for Computing Machinery. doi:10.1145/3605768.3623539.

14 J. Douceur. The sybil attack. *IPTPS 2002, Lecture Notes in Computer Science*, 2429, March 2002.

15 ENS. ENS Governance. https://ens.domains/governance, 2026.

16 Etherscan. Etherscan API V2. https://docs.etherscan.io/, 2026. Accessed April 20, 2026.

17 Brett Falk, Tasneem Pathan, Andrew Rigas, and Gerry Tsoukalas. Blockchain governance: An empirical analysis of user engagement on daos. *arXiv preprint arXiv:2407.10945*, 2024. URL: https://arxiv.org/abs/2407.10945, doi:10.48550/arXiv.2407.10945.

18 Rainer Feichtinger, Robin Fritsch, Lioba Heimbach, Yann Vonlanthen, and Roger Wattenhofer. SoK: Attacks on DAOs. In *6th Conference on Advances in Financial Technologies (AFT 2024)*, LIPIcs. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2024. Dataset: https://daoattacks.ethz.ch.

19 Louis Kaplow and Scott Duke Kominers. Who will vote quadratically? voter turnout and votes cast under quadratic voting. *Public Choice*, 172(1–2):125–149, 2017. doi:10.1007/s11127-017-0412-5.

20 S. Lalley and E.G. Weyl. Quadratic voting: How mechanism design can radicalize democracy. *AEA Papers and Proceedings*, 108:33–37, May 2018.

21 Lido. Lido DAO Governance. https://lido.fi/governance, 2026.

22 MakerDAO. MakerDAO Governance. https://vote.makerdao.com/, 2026.

23 Matter Labs. ZKsync JSON-RPC API. https://docs.zksync.io/zksync-protocol/api, 2026. Accessed April 20, 2026.

24 Mohsen Minaei, Pedro Moreno-Sanchez, Zhiyong Fang, Srinivasan Raghuraman, Navid Alamati, Panagiotis Chatzigiannis, Ranjit Kumaresan, and Duc V. Le. DTL: Data tumbling layer — a composable unlinkability for smart contracts. In *Proceedings of the 20th ACM Asia Conference on Computer and Communications Security*, ASIA CCS '25, pages 971–984, New York, NY, USA, 2025. Association for Computing Machinery. doi:10.1145/3708821.3736221.

25 Optimism. Optimism Governance. https://gov.optimism.io/, 2026.

26 Kevin Owocki. Sybil resistance in quadratic funding: 2024 approaches, December 2024. URL: https://gitcoin.co/research/quadratic-funding-sybil-resistance.

27 Reflect Finance. Reflect finance (rfi). https://reflect.finance/, 2026.

28 Snapshot. Snapshot. https://snapshot.box/, 2026.

29 Tally. Tally GraphQL API. https://apidocs.tally.xyz/, 2026. Accessed April 20, 2026.

30 Uniswap. Uniswap Governance. https://gov.uniswap.org/, 2026.

31 K. Weiss. Gitcoin grants — quadratic funding for the world. https://www.gitcoin.co/blog, August 2022.

32 Zibo Zhou, Zongyang Zhang, Feng Hao, Bowen Zheng, and Zulkarnaim Masyhur. Qv-net: Decentralized self-tallying quadratic voting with maximal ballot secrecy. In *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security*, CCS '25, pages 453–467, New York, NY, USA, 2025. Association for Computing Machinery. doi:10.1145/3719027.3744810.

33 ZKsync. ZKsync Governance. https://docs.zknation.io/zksync-governance-procedures, 2026.

A Missing Proofs

For completeness, we collect here the proofs of the statements deferred from the main body. Proofs of Lemma 8 and Lemma 9 appear inline with their statements in Section 5.

▶ **Lemma 5** (Sybil Voting Power Lemma). *Let f be a non-trivial voting rule for which there exists $m > 0$ such that $f(m) > 0$. Then for all wallets $a \geq m$,*

$$V^*(a) \geq \left\lfloor \frac{a}{m} \right\rfloor f(m).$$

Proof. Given total wealth a, divide it into $\lfloor a/m \rfloor$ wallets of size m, and one remaining wallet smaller than m (which we ignore since it cannot vote). The voting power is then lower-bounded as

$$V^*(a) \geq \left\lfloor \frac{a}{m} \right\rfloor f(m). \qquad \blacktriangleleft$$

▶ **Theorem 6** (Sybil-Induced Plutocracy). *Every nontrivial voting rule is plutocratic under unrestricted Sybil wallet splitting. Specifically, if $\exists m > 0 : f(m) > 0$, then for all $a \geq 2m$, there exists a constant $\alpha > 0$ such that $V^*(a) \geq \alpha \cdot a$.*

Proof. For $a \geq 2m$, we have

$$\left\lfloor \frac{a}{m} \right\rfloor \geq \frac{a}{2m}.$$

Combining with the Sybil Voting Power Lemma (Lemma 5),

$$V^*(a) \geq \left\lfloor \frac{a}{m} \right\rfloor f(m) \geq \frac{a \cdot f(m)}{2m}.$$

Setting $\alpha = \frac{f(m)}{2m}$ proves the result. $\blacktriangleleft$

▶ **Theorem 7** (Robustness of Plutocracy to Costs). *Suppose there is a non-trivial voting scheme combined with a cost scheme $C = (m, v, p, s)$ where there are fixed costs of additional wallet creation $p \geq 0$, a wallet splitting cost $s \geq 0$ per wallet, a voting cost $v \geq 0$ per wallet, and a minimum wallet size m. The Sybil-adjusted voting power is still plutocratic and satisfies:*

$$V_C^*(a) = \Omega(a).$$

Proof. Assuming an attacker elects to split their budget, the fixed cost of wallet creation reduces the attacker's usable wealth from a to

$$a' = a - p.$$

Adding in the wallet splitting cost and voting cost are equivalent to increasing the minimum wallet size:

$$m' = m + s + v.$$

Thus any split of the post-entry wealth a' into gross wallets is an instance of Theorem 6 applied to the shifted rule $g(x) = f(x - (s + v))$ with minimum wallet size m'. Therefore,

$$V_C^*(a) = \Omega(a')$$

Since p is a constant independent of a, we have $a - p = \Omega(a)$, and hence $V_C^*(a) = \Omega(a)$. ◀

▶ **Theorem 10** (Concave Mechanisms Are Asymptotically Linear-Exploitable in Token Amount)**.** *Let $A = a - p$ and $c = v + s$. Assume that there exists at least one integer $n \geq 1$ such that*

$$m \leq \frac{A}{n} - c$$

Define the values:

$$g(x) = \frac{f(x)}{x + c} \qquad \textit{and} \qquad \kappa = \sup_{x \geq m} g(x) < \infty$$

Then, we have that:

1. *(Linear upper bound) The optimal voting power satisfies*

$$V^*(W) \leq \kappa A$$

2. *(Asymptotic tightness) If g attains its supremum on $[m, \infty)$ at some $x^* \geq m$, then*

$$\lim_{a \to \infty} \frac{V^*(W)}{A} = \kappa$$

Proof. We prove the statement by showing each component is true.

Step 1: Linear upper bound. For any feasible integer n, let $x = \frac{A}{n} - c$ so that $x \geq m$ and $n = \frac{A}{x+c}$. By substituting $g(x)$,

$$n\, f\left(\frac{A}{n} - c\right) = \frac{A}{x + c}\, f(x) = A \cdot \frac{f(x)}{x + c} = A\, g(x) \leq A\, \kappa.$$

Taking the maximum over feasible n yields the upper bound:

$$V^*(W) \leq A\, \kappa.$$

Step 2: Asymptotic tightness. Assume $g(x)$ attains its supremum at some $x^* \geq m$. Thus $\kappa = g(x^*)$.

For all sufficiently large A such that $A \geq x^* + c$, define the following variables to conform to our integer-bounded number of wallets:

$$n_A = \left\lfloor \frac{A}{x^* + c} \right\rfloor, \qquad x_A = \frac{A}{n_A} - c.$$

This satisfies our lower wallet-bound condition as

$$\frac{A}{n_A} \geq \frac{A}{A/(x^* + c)} = x^* + c,$$

and therefore

$$x_A = \frac{A}{n_A} - c \geq (x^* + c) - c = x^* \geq m.$$

Next, define $t_A = \frac{A}{x^*+c}$. By definition of the floor function, $n_A \leq t_A < n_A+1$. Substituting in t_A, we can define upper and lower bounds, U_A and L_A respectively, for $x^* + c$:

$$L_A = \frac{A}{n_A + 1} < \frac{A}{t_A} = x^* + c \leq \frac{A}{n_A} = U_A.$$

We now show that the difference between these bounds vanishes as $A \to \infty$:

$$U_A - L_A = \frac{A}{n_A} - \frac{A}{n_A + 1} = A \cdot \frac{1}{n_A^2 + n_A}.$$

Since $n_A = \left\lfloor \frac{A}{x^*+c} \right\rfloor \geq \frac{A}{x^*+c} - 1$, for large enough A (specifically $\frac{A}{x^*+c} \geq 2$) we have $n_A \geq \frac{A}{2(x^*+c)}$. Thus,

$$\frac{A}{n_A^2 + n_A} \leq \frac{A}{n_A^2} \leq \frac{A}{\big(A/(2(x^* + c))\big)^2} = \frac{4(x^* + c)^2}{A} \longrightarrow 0 \quad \text{as } A \to \infty.$$

Since $L_A < x^* + c \leq U_A$ and $U_A - L_A \to 0$, $U_A = A/n_A \to x^* + c$, and hence $x_A = A/n_A - c \to x^*$.

Because f is concave it is continuous on $(0, \infty)$ (and right-continuous at 0). Since $x + c \geq c > 0$ for all $x \geq m$, $g(x) = f(x)/(x + c)$ is continuous at x^*. Choose any $\varepsilon > 0$. By continuity, there exists $\delta > 0$ such that

$$|x - x^*| < \delta \;\Rightarrow\; |g(x) - g(x^*)| < \varepsilon.$$

Since $x_A \to x^*$, there exists A_0 such that for all $A \geq A_0$, $|x_A - x^*| < \delta$, and hence $|g(x_A) - g(x^*)| < \varepsilon$. This gives $\kappa - \varepsilon = g(x^*) - \varepsilon < g(x_A)$ for large A, and so

$$\kappa - \varepsilon < g(x_A) = \frac{f(x_A)}{x_A + c} = \frac{n_A\, f(x_A)}{A} = \frac{n_A\, f\big(\frac{A}{n_A} - c\big)}{A} \leq \frac{V^*(W)}{A}.$$

Combining with $V^*(W)/A \leq \kappa$ from Step 1,

$$\kappa - \varepsilon < \frac{V^*(W)}{A} \leq \kappa.$$

Letting $\varepsilon \to 0$, the squeeze theorem gives $\lim_{a\to\infty} V^*(W)/A = \kappa$. ◀

▶ **Corollary 11** (Closed forms for common concave rules)**.** *Let $A = a - p$ and $c = v + s$ and assume the minimum wallet bound is a slack condition. Under the conditions of Theorem 10, the attacker's optimal voting power admits the following closed forms.*

1. ***Power voting.*** *If $f(x) = x^\beta$ with $\beta \in (0, 1)$, then*

$$V^*(W) \;=\; \frac{A\,\beta^\beta(1-\beta)^{1-\beta}}{c^{1-\beta}}.$$

As a special case, quadratic voting *($\beta = 1/2$, $f(x) = \sqrt{x}$) yields $V^*(W) = A/(2\sqrt{c})$.*

2. ***Logarithmic voting.*** *If* $f(x) = \ln(x+1)$*, then*

$$V^*(W) \;=\; \frac{A\,W_0((c-1)/e)}{c-1},$$

where W_0 *denotes the principal branch of the Lambert W function.*[3]

Proof. In each case, we reduce the relaxed objective $h(n) = n\,f\big(\frac{A}{n} - c\big)$ to a single-variable problem in the per-wallet amount. Let $g(w) = f(w)/(w+c)$ denote the attacker's voting power per dollar at per-wallet amount w. Substituting $w = A/n - c$ (so that $n = A/(w+c)$ is a bijection from $n \in (0, A/c)$ onto $w \in (0,\infty)$) gives

$$h(n) = n\,f(w) = A \cdot \frac{f(w)}{w+c} = A \cdot g(w).$$

The relaxed optimum is therefore $V^*(W) = A \cdot \sup_{w>0} g(w)$. When the supremum is attained at an interior point w^*, that point satisfies the first-order condition $g'(w^*) = 0$. By the quotient rule,

$$g'(w) = \frac{f'(w)\,(w+c) - f(w)}{(w+c)^2},$$

and since $(w+c)^2 > 0$ on the interior, $g'(w^*) = 0$ is equivalent to

$$f'(w^*)\,(w^*+c) = f(w^*). \qquad (\star)$$

Each case below solves $(\star)$ for w^* and then evaluates $V^*(W) = A \cdot g(w^*)$.

Case 1: Power voting, $f(x) = x^\beta$ with $\beta \in (0,1)$. Here $f'(w) = \beta\,w^{\beta-1}$, so $(\star)$ becomes $\beta\,w^{\beta-1}(w+c) = w^\beta$. Dividing through by $w^{\beta-1}$ yields $\beta(w+c) = w$, i.e., $(1-\beta)\,w = \beta\,c$. This gives the unique interior critical point

$$w^* = \frac{\beta\,c}{1-\beta}, \qquad w^* + c = \frac{c}{1-\beta}.$$

On the boundary, $g(w) = w^\beta/(w+c) \to 0$ as $w \to 0^+$ and as $w \to \infty$ (since $\beta < 1$), while $g(w^*) > 0$, so w^* is the global maximum. Substituting,

$$g(w^*) = \frac{(w^*)^\beta}{w^*+c} = \frac{(\beta\,c/(1-\beta))^\beta}{c/(1-\beta)} = \frac{\beta^\beta\,(1-\beta)^{1-\beta}}{c^{1-\beta}},$$

and multiplying by A yields the stated formula. The quadratic specialization is $\beta = 1/2$, which collapses $\beta^\beta(1-\beta)^{1-\beta}$ to $1/2$ and yields $V^*(W) = A/(2\sqrt{c})$.

Case 2: Logarithmic voting, $f(x) = \ln(x+1)$. Here $f'(w) = 1/(w+1)$, so $(\star)$ becomes $(w+c)/(w+1) = \ln(w+1)$. Substituting $x = w+1$ (so $w + c = x + (c-1)$) reduces the first-order condition to

$$x\,(\ln x - 1) = c - 1.$$

---

[3] The *Lambert W function* is the inverse of $z \mapsto z\,e^z$: by definition, $W(z)\,e^{W(z)} = z$. The *principal branch* W_0 is the (unique) real-valued branch on $[-1/e, \infty)$, satisfying $W_0(0) = 0$ and $W_0(z) \to \infty$ as $z \to \infty$. A useful identity, applied in the proof, is $e^{W_0(z)} = z/W_0(z)$ for $z \neq 0$, which follows directly from the defining equation.

Let $y = \ln x - 1$, so that $x = e^{y+1} = e \cdot e^y$. The first-order condition becomes

$$e \cdot y \cdot e^y = c - 1 \qquad \Longleftrightarrow \qquad y\, e^y = \frac{c-1}{e}.$$

By definition of the principal Lambert branch, this equation has a unique solution, which we denote

$$y^* = W_0\left(\frac{c-1}{e}\right).$$

Reversing the substitutions $y = \ln x - 1$ and $x = w + 1$ recovers the optimal per-wallet balance. From $x = e \cdot e^y$ and the identity $e^{W_0(z)} = z/W_0(z)$ (with $z = (c-1)/e$),

$$x^* = e \cdot e^{y^*} = \frac{c-1}{y^*},$$

so

$$w^* = x^* - 1 = \frac{c-1}{y^*} - 1, \qquad w^* + c = \frac{(c-1)(1+y^*)}{y^*}.$$

Since $\ln(x^*) = y^* + 1$ (directly from $y^* = \ln x^* - 1$), the voting power per dollar simplifies by cancellation of the $(1 + y^*)$ factor:

$$g(w^*) = \frac{f(w^*)}{w^* + c} = \frac{\ln(x^*)}{w^* + c} = \frac{1 + y^*}{(c-1)(1+y^*)/y^*} = \frac{y^*}{c-1} = \frac{W_0((c-1)/e)}{c-1}.$$

On the boundary, $g(w) = \ln(w+1)/(w+c) \to 0$ as $w \to 0^+$ (since $c > 0$) and as $w \to \infty$, while $g(w^*) > 0$, so w^* is the global maximum. Multiplying by A yields

$$V^*(W) = \frac{A\, W_0((c-1)/e)}{c-1}.$$ ◀

B Honest vs Attacker Voting Power per Dollar

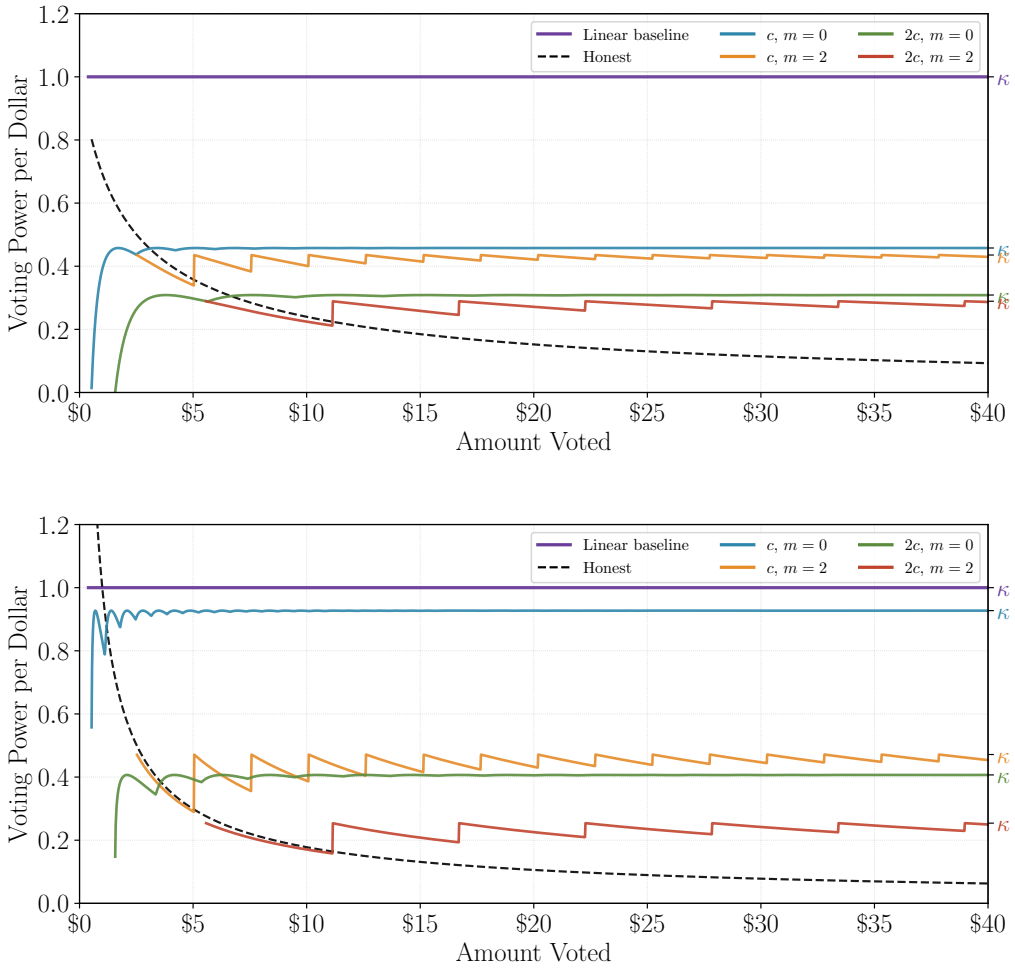

Figure 5 Top: Voting power per dollar for Uniswap proposals in our model under logarithmic voting. The dashed black line shows how an honest voter has less power with each additional dollar they vote with. This is true for all concave voting functions. The blue line represents an attacker under realistic conditions. The costs $c = v + s$ are taken from the analyzed proposals and current Ethereum assumptions, and there is no minimum wallet balance to vote ($m = 0$). As seen, the blue curve flattens out and approaches its κ value. This is because the attacker achieves linear voting with enough budget. The orange, green, and red lines indicate how either doubling c or increasing m to 2 does not impede the attacker from achieving linear voting power, instead it just reduces the asymptotic κ values. **Bottom:** The same as the top for power ($\beta = 0.25$) voting. Identical patterns are observed.