L09 — Voting Systems & DAO Governance

Cheatsheet

Token-Weighted Voting

Rule: 1 Token

`votingPower(user) = tokenBalance[user]`

Each token holder votes proportional to holdings. Simplest mechanism; most common in early DAO governance (MakerDAO, Compound, Uniswap).

Characteristics:

- **Plutocratic** — wealth equals power; 1000 tokens = 10× power of 100 tokens.
- **Whale dominance** — top holders can pass/block any proposal.
- **Low participation** from small holders who feel votes are inconsequential.
- Aligns voting with economic stake.

Flashloan attack — borrow tokens, vote, repay in single transaction. Defeated by snapshot-based voting (balance fixed at prior block) or time-locks.

Quadratic Voting

Key Formula

$$c(v) = v^2$$

Cost c in voice credits to cast v votes on a single issue. Equivalently, voting power from a budget B is $\sqrt{B}$.

Mechanism: Each voter receives a budget of *voice credits* (not tokens directly). Spending more credits on one issue is quadratically expensive, incentivising broad rather than concentrated preference expression.

Example (100 voice credits):

- Cast 10 votes on one issue: costs $10^2 = 100$
- Cast 5 votes on each of 4 issues: costs $4 \times 25 = 100$

Real-world use:

- **Gitcoin Grants:** \$60M+ distributed; number of contributors weights matching more than individual donation size.
- **Colorado Legislature** (2019): budget prioritisation pilot.

Limitation: Requires Sybil resistance — identity verification needed or one person creates many wallets to get multiple budgets.

Conviction Voting

Formula: Conviction Accumulation

$$C(t) = C(t-1) \cdot \alpha + \text{tokens} \cdot (1 - \alpha)$$

where $\alpha \in (0, 1)$ is the decay factor (e.g. $\alpha = 0.9$).
Conviction approaches token amount asymptotically; switching proposal resets accumulated conviction.

Key properties:

- **Continuous** — no fixed voting periods; votes accumulate over time until threshold is met.
- **Sustained support wins** — a flash vote from a whale cannot instantly pass a proposal.
- **Manipulation resistant** — last-minute reversals lose accumulated conviction.
- **Slow** — deliberate; best for funding allocation, not emergency decisions.

Used by: 1Hive Gardens, Giveth.

veToken Voting (Time-Lock)

Voting Power Formula

$$P = \text{tokens} \times \frac{t_{\text{remaining}}}{t_{\max}}$$

Longer lock ⇒ higher voting power; power decays linearly to zero at lock expiry.

Example (100 tokens, $t_{\max} = 4$ years):

- Lock 4 yr: $100 \times \frac{4}{4} = 100$ vp
- Lock 2 yr: $100 \times \frac{2}{4} = 50$ vp
- Lock 1 yr: $100 \times \frac{1}{4} = 25$ vp

Additional benefits for lockers: protocol revenue sharing, boosted liquidity-provision rewards, proposal rights.

Trade-off: Capital locked, illiquid during lock period. Still plutocratic (more tokens = more power).

Pioneered by: Curve Finance (veCRV, \$2.2B TVL); adopted by Balancer, Frax, many DeFi protocols.

Reputation-Based Voting

Formula

$$\text{Voting Power} = \sqrt{\text{Reputation}}$$

Reputation is **non-transferable** (soulbound) and accumulated through contributions: attendance, code commits, proposals, engagement.

Properties:

- **Strong Sybil resistance** — reputation must be earned; cannot be purchased or transferred.
- **Non-plutocratic** — wealth alone confers no voting power.
- **Centralization risk** — requires trusted oracle or committee to assign reputation scores.
- **Late-joiner disadvantage** — early participants accumulate compounding advantages.

Best for: contributor-centric communities where merit matters more than token holdings.

Snapshot vs. On-Chain Voting

	Snapshot (off-chain)	On-chain
Gas cost	Free (signed messages)	Paid by voter
Binding?	Signalling only	Directly executes
Security	Centralised server risk	Smart-contract enforced
Speed	Instant	Block confirmation
Used by	Uniswap, Aave, ENS	Compound Governor, MakerDAO

Best practice: off-chain Snapshot for signalling + on-chain execution via timelock for binding decisions.

Snapshot facts: 33,000+ spaces; signed messages; balances verified at snapshot block to prevent flashloan manipulation.

DAO Structure & Governance Lifecycle

Typical Governance Flow

1. **Proposal** submitted (meet threshold: e.g. 0.25% of supply)
2. **Discussion** period (off-chain forum, e.g. 5 days)
3. **Vote** on-chain or Snapshot (3–7 days)
4. **Quorum check** (e.g. 4% of tokens must participate)
5. **Timelock** delay (48 h) — allows users to exit before execution
6. **Execution** by governor contract or multisig

Multisig safeguards: emergency pause capabilities; operational decisions by core team within limits set by governance.

Quorum problem: typical DAO turnout is 5–15% of token supply; low participation enables minority capture.

Delegation (Liquid Democracy)

Mechanism: Token holders call `delegate(address)` to transfer voting rights (not token ownership) to a representative. Delegatee's power equals own tokens plus all delegated tokens.

Liquid democracy: delegation is transitive (A delegates to B who delegates to C) and revocable at any time. No fixed representatives.

Re-delegation: voter can reclaim and directly vote on any specific proposal even while generally delegated.

Concentration risk: large delegates in Uniswap and Compound control enough votes to pass proposals unilaterally; top 10 delegates often >50% of participating votes.

Used by: ENS, Uniswap, Compound.

Sybil Resistance

Sybil Attack

Attacker creates many fake identities (wallets) to multiply voting power or quadratic-voting budget. Named after the book about multiple personality disorder.

Resistance mechanisms:

- **Proof of Humanity** — biometric or social verification (Worldcoin iris scan, Proof of Humanity via video).
- **Quadratic costs** — each extra identity must build reputation or buy tokens; diminishing marginal returns.
- **Non-transferable reputation** — soulbound tokens (SBTs) cannot be sold; must be earned per identity.
- **Social graph** — Gitcoin Passport scores social media and on-chain activity; anomaly detection for bot wallets.

Privacy trade-off: stronger identity verification ⇒ lower privacy; many users resist KYC-style identity schemes.

Voter Participation

Typical DAO statistics:

- Average participation: 5–15% of token supply
- Unique voters per proposal: often <200 in large DAOs
- Voting power: top 10 addresses control 40–80% in most DAOs

Solutions to low participation:

- **Delegation** — reduces burden; one expert votes for many
- **Incentivised voting** — rewards for casting votes (risk: uninformed voting for rewards)
- **Rage-quit / exit rights** — guaranteed exit if outvoted (Moloch DAO model) increases participation confidence
- **Conviction voting** — continuous; no need to monitor windows

Gini Coefficient of voting power:

$$G = \frac{2\sum_{i=1}^{n} i \cdot VP_i}{n\sum_{i=1}^{n} VP_i} - \frac{n+1}{n}$$

Scale: $G = 0$ (perfect equality) to $G = 1$ (one entity holds all power).

Key Formulas

Mechanism	Formula
Token voting	$VP = \text{tokens}$
Quadratic cost	$c(v) = v^2; \quad VP = \sqrt{B}$
veToken power	$P = \text{tokens} \times t_{\text{rem}}/t_{\max}$
Reputation VP	$VP = \sqrt{\text{rep}}$
Conviction	$C(t) = \alpha\, C(t-1) + (1-\alpha)\,\text{tokens}$
Gini coeff.	$G = \frac{2\sum i \cdot VP_i}{n\sum VP_i} - \frac{n+1}{n}$

Voting Mechanisms: Comparison Table

System	Plutocracy?	Sybil resist.	Speed	Best For
Token	High	Low	Fast	Quick decisions
Quadratic	Low	Needed	Med	Public goods
veToken	Med	Med	Med	Protocol gov.
Reputation	Low	High	Med	Communities
Conviction	Med	Med	Slow	Ongoing fund.

Hybrid approaches: many DAOs combine systems — token voting for protocol upgrades + quadratic funding for grants (e.g. Uniswap); veToken for emissions + snapshot signalling for meta-governance.