

Blockchain Voting Systems

Lesson 9: Decentralized Governance Mechanisms

Prof. Joerg Osterrieder

Spring 2026

Learning Objectives

After this lesson, you will be able to:

- Explain five blockchain voting mechanisms and their trade-offs
- Calculate voting power under different systems
- Analyze Sybil resistance and fairness properties
- Design appropriate voting systems for specific use cases

Prerequisites: L07 (Game Theory), L05 (Tokenomics)

This lesson applies mechanism design principles to real governance problems

- 1 Introduction to Blockchain Voting
- 2 Simple Token Voting
- 3 Quadratic Voting
- 4 veToken Locking
- 5 Reputation-Based Voting
- 6 Conviction Voting
- 7 System Comparison
- 8 Practical Implementation

Introduction to Blockchain Voting

Why Blockchain Voting?

Traditional voting problems:

- Centralized control: Single entity can manipulate results
- Lack of transparency: Voters cannot verify their vote was counted
- High costs: Physical infrastructure, personnel, time

Blockchain solutions:

- Immutable records on distributed ledger
- Cryptographic verification of votes
- Smart contract automation

DAOs collectively manage billions in assets and governance decisions using on-chain voting

The voting trilemma—hard to achieve all three:

- **Sybil Resistance:** One person, one vote (prevent fake identities)
- **Fairness:** Equal opportunity to influence outcomes
- **Simplicity:** Easy for users to understand and participate

Additional considerations:

- Manipulation resistance (vote buying, flashloan attacks)
- Gas costs and scalability
- Voter engagement and participation rates

Flashloan attack: Attacker borrows tokens, votes, repays in single transaction—defeated by snapshot-based voting or time-locks.

No perfect system exists—each makes different trade-offs

Simple Token Voting

Simple Token Voting: Mechanism

Rule: 1 Token = 1 Vote

- Each token holder votes proportional to their holdings
- Most common in early DAO governance (MakerDAO, Compound)
- Simple to implement and understand

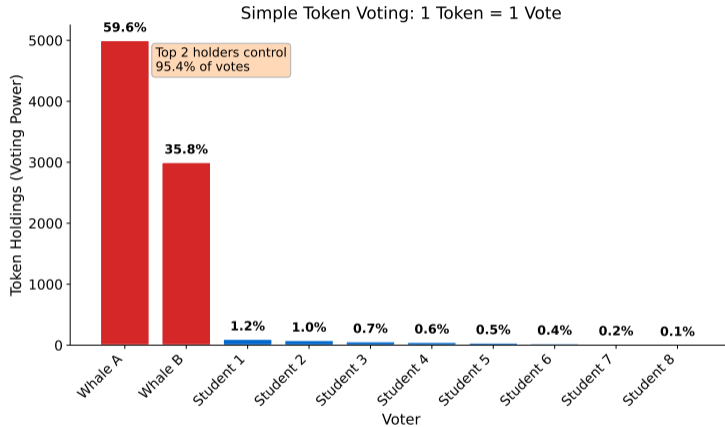
Smart Contract Logic:

```
votingPower(user) = tokenBalance[user]
```

Example: Alice has 1000 tokens, Bob has 100 tokens
Alice has 10x the voting power of Bob

Simple but plutocratic—wealth equals power

Token Voting: Vote Distribution



Whale dominance is the primary concern with simple token voting

Advantages:

- Extremely simple to implement
- Easy for users to understand
- Aligns voting with economic stake
- Low gas costs

Best for: Quick decisions where stakeholder alignment matters

Disadvantages:

- Plutocratic: wealth = power
- Vulnerable to whale manipulation
- No Sybil resistance
- Low participation from small holders

Used by MakerDAO, Compound, Uniswap governance

Quadratic Voting

Quadratic Voting: Mechanism

Core Idea: Make concentrated voting expensive

Formula:

$$\text{Cost} = n^2 \quad \text{where } n = \text{number of votes}$$

Voice credits: The budget each voter receives for expressing preferences. In quadratic voting, voters spend voice credits (not tokens directly) to cast votes.

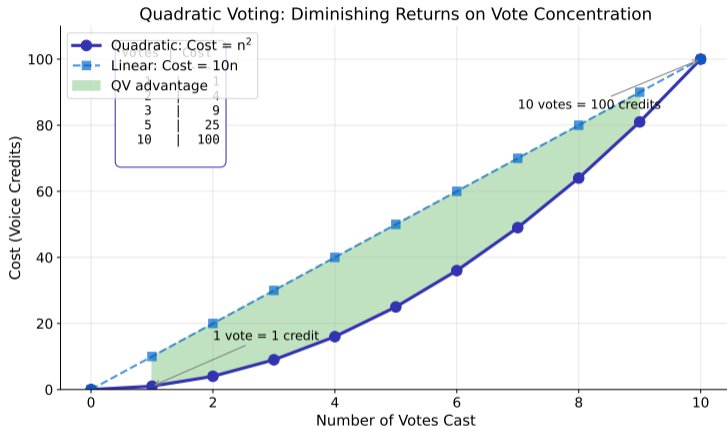
Example with 100 voice credits:

- Option A: Cast 10 votes (cost: $10^2 = 100$)
- Option B: Cast 5 votes each on 4 issues (cost: $4 \times 25 = 100$)

Key Insight: Expressing strong preference is costly

Proposed by Posner & Weyl in "Radical Markets" (Princeton, 2018): press.princeton.edu

Quadratic Voting: Cost Curve



Diminishing returns prevent vote concentration

Quadratic Voting: Real-World Example

Bitcoin Grants: \$60M+ distributed using quadratic funding

How it works:

- Number of contributors matters more than amount
- $\sqrt{\text{donation}}$ determines matching weight
- Prevents single whale from dominating allocation

Result: Broad community support signals importance

Colorado Legislature: Used QV for budget prioritization in 2019

QV is increasingly used for public goods funding. See: gitcoin.co/results

Advantages:

- Reduces plutocracy
- Rewards broad support
- Mathematically elegant
- Proven in practice

Best for: Public goods funding, preference aggregation

Disadvantages:

- Requires Sybil resistance
- More complex UX
- Collusion still possible
- Identity verification needed

Sybil attacks can circumvent QV—identity verification is essential

veToken Locking

veToken: Time-Weighted Voting Power

Core Idea: Lock tokens longer = more voting power

Formula:

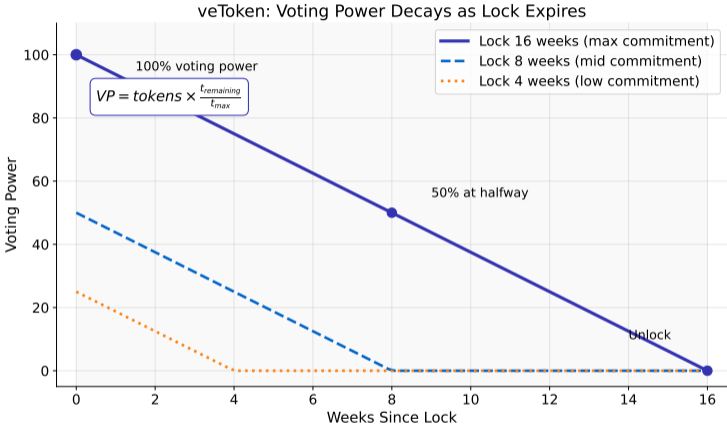
$$\text{Voting Power} = \text{tokens} \times \frac{t_{\text{remaining}}}{t_{\text{max}}}$$

Example (100 tokens, max lock 4 years):

- Lock 4 years: $100 \times \frac{4}{4} = 100$ voting power
- Lock 2 years: $100 \times \frac{2}{4} = 50$ voting power
- Lock 1 year: $100 \times \frac{1}{4} = 25$ voting power

Pioneered by Curve Finance (veCRV)—TVL \$2.2B (Jan 2026). See: defillama.com

veToken: Voting Power Decay



Voting power decays linearly as lock expiration approaches

What behaviors does veToken reward?

- Long-term commitment to the protocol
- Reduced token circulation (supply squeeze)
- Aligned incentives with protocol success

Additional benefits for lockers:

- Protocol revenue sharing (Curve, Balancer)
- Boosted rewards for liquidity provision
- Governance proposal rights

Trade-off: Illiquidity during lock period

veToken creates strong alignment between voters and protocol health. See: docs.curve.fi

Advantages:

- Rewards long-term thinking
- Prevents vote manipulation
- Reduces mercenary capital (short-term holders seeking quick profits who may destabilize governance)
- Proven at scale

Best for: Protocol governance with long-term focus

Disadvantages:

- Complex for new users
- Capital inefficiency
- Lock-in risk
- Still plutocratic

Used by Curve, Balancer, Frax, and many DeFi protocols

Alternative: Delegated Voting

Problem: Many token holders lack time or expertise to vote

Solution: Delegate your voting power to a trusted representative

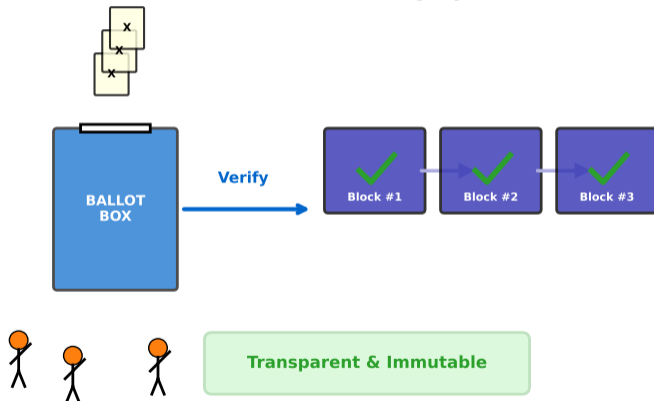
- Keep token ownership, transfer voting rights
- Delegatee votes on your behalf
- Revocable at any time

How it works:

- Call `delegate(address)` on governance contract
- Delegatee's voting power = own tokens + delegated tokens
- Popular in ENS, Uniswap, Compound governance

Delegation increases participation without requiring active voting

Blockchain Voting System



Reputation-Based Voting

Reputation Voting: Earned Voting Power

Core Idea: Earn voting power through participation

Reputation sources:

- Attendance, contributions, engagement
- Non-transferable (soulbound—cannot be sold or transferred to another address, like a gaming item bound to your character)
- Accumulated over time

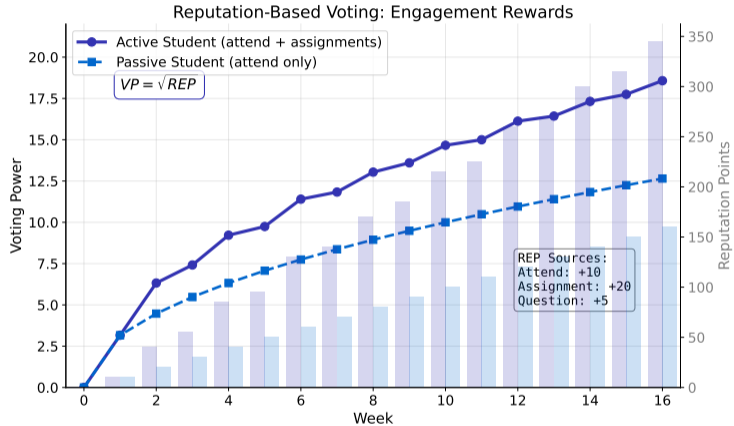
Formula:

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

Why square root? Prevents runaway inequality while rewarding engagement

Reputation is Sybil-resistant because it must be earned

Reputation: Engagement Rewards



Active participants gain significant voting power advantage

Advantages:

- Strong Sybil resistance
- Rewards active participation
- Aligns with contribution
- Non-plutocratic

Best for: Community governance where engagement matters

Disadvantages:

- Requires trusted oracle
- Centralization risk
- Late joiners disadvantaged
- Gaming possible

Emerging in DAOs focused on contributor recognition

Conviction Voting

Conviction Voting: Time-Weighted Preference

Core Idea: Votes accumulate weight over time

Formula:

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

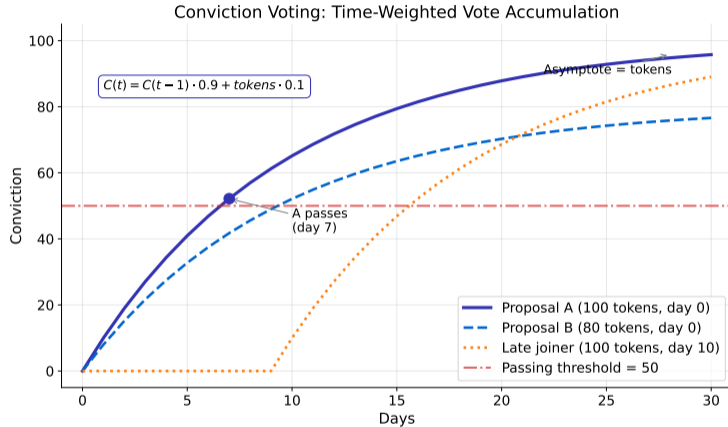
where $\alpha = 0.9$ (decay factor)

Key properties:

- Continuous voting (no fixed periods)
- Sustained support wins over flash votes
- Conviction approaches token amount asymptotically

Used by 1Hive Gardens, Giveth. See: wiki.1hive.org

Conviction: Time-Weighted Accumulation



Sustained support is required to pass proposals

Advantages:

- Prevents last-minute attacks
- Continuous, not periodic
- Rewards sustained conviction
- Manipulation resistant

Best for: Continuous improvement, funding allocation

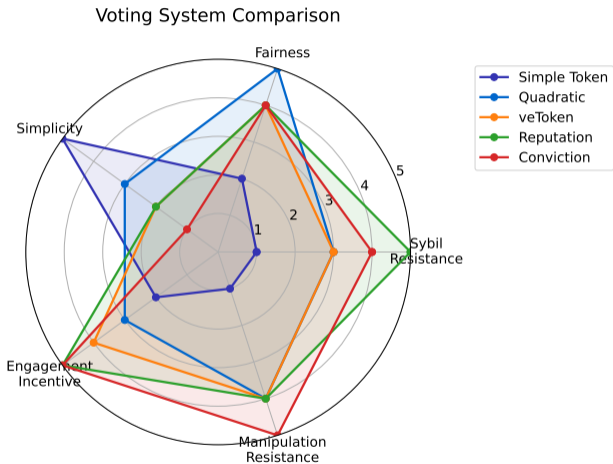
Disadvantages:

- Complex to understand
- Slow decision-making
- Favors early voters
- Requires ongoing attention

Ideal for ongoing community governance

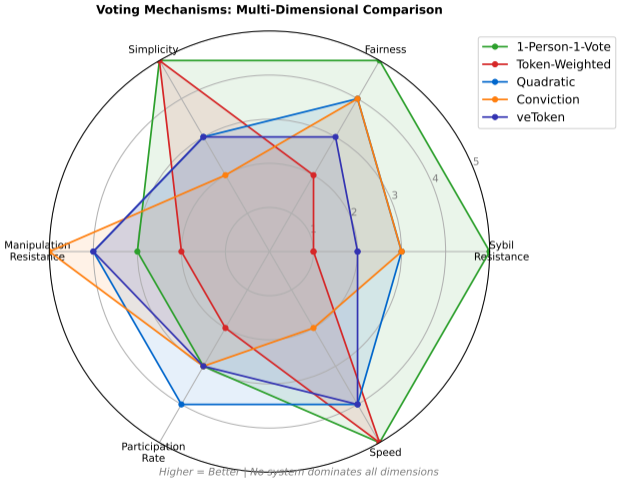
System Comparison

Voting Systems: Multi-Dimensional Comparison



No system dominates on all dimensions—choose based on priorities

Voting Mechanisms: Radar Comparison

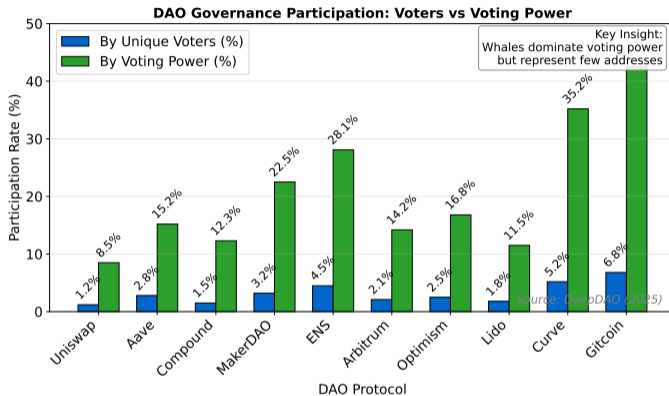


Each mechanism excels on different dimensions—no universal winner

Measuring Voting Power Inequality: Gini Coefficient

- **Gini Coefficient:** Measures inequality in voting power distribution
- Scale: 0 = perfect equality, 1 = total inequality (one entity has all power)
- Formula: $G = \frac{2 \sum_{i=1}^n i \cdot VP_i}{n \sum_{i=1}^n VP_i} - \frac{n+1}{n}$
 - Where VP_i = voting power of i -th participant (sorted ascending)
 - Equivalent to: $G = 1 - 2 \times (\text{area under Lorenz curve})$
- Example: 4 voters with [10, 20, 30, 40] tokens $\rightarrow G \approx 0.25$
- Use case: Compare fairness across voting systems

Lower Gini = more equal voting power distribution



Few unique voters, but whales concentrate voting power — Source: DeepDAO

When to Use Which System

System	Best For	Avoid When
Token	Quick decisions	Fairness matters
Quadratic	Public goods	No identity system
veToken	Protocol governance	Users need liquidity
Reputation	Communities	No trusted oracle
Conviction	Ongoing funding	Fast decisions needed

Hybrid approaches: Many DAOs combine systems

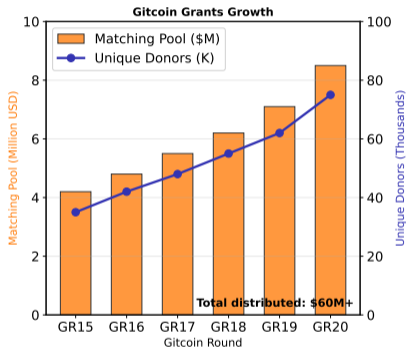
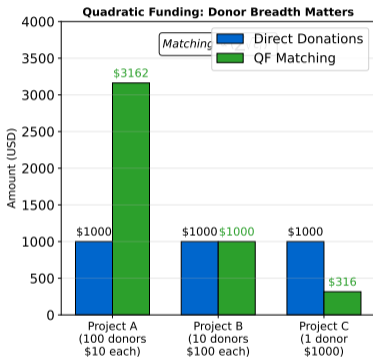
- Token + veToken for different proposal types
- Quadratic for grants, token for protocol changes
- Example: Uniswap uses token voting for protocol + quadratic for grants program

Match the voting system to the governance need

Practical Implementation

Quadratic Funding in Practice

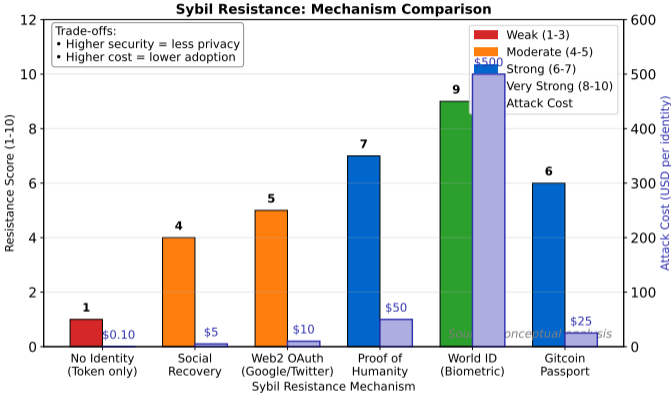
Quadratic Funding in Action



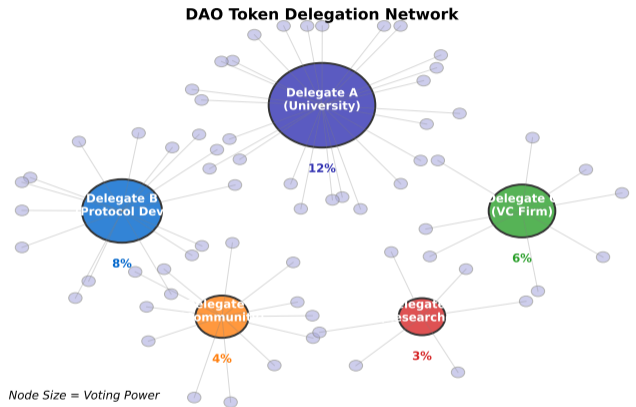
Source: gitcoin.co/results (Historical: GR15-GR20)

Donor breadth matters more than donation size — Source: Gitcoin

Sybil Resistance Mechanisms



Higher security often means lower privacy—design trade-offs



Delegation Statistics:

- Top 5 delegates: 33% of votes
- Top 20 delegates: 65% of votes
- Active delegators: ~2,000

Note: Most tokens are not delegated (~70%)

Source: Tally, Agora (conceptual)

Why Snapshot?

- Free to vote (no gas costs)
- Easy setup for any token
- Supports multiple voting strategies

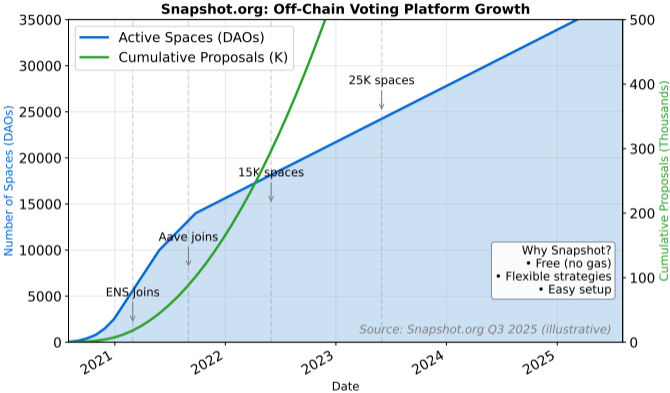
How it works:

- Votes are signed messages (off-chain)
- Token balances verified at snapshot block
- Results are verifiable but not on-chain

Used by: Uniswap, Aave, ENS, 33,000+ spaces (snapshot.org)

Snapshot enables gasless governance for any ERC-20 token

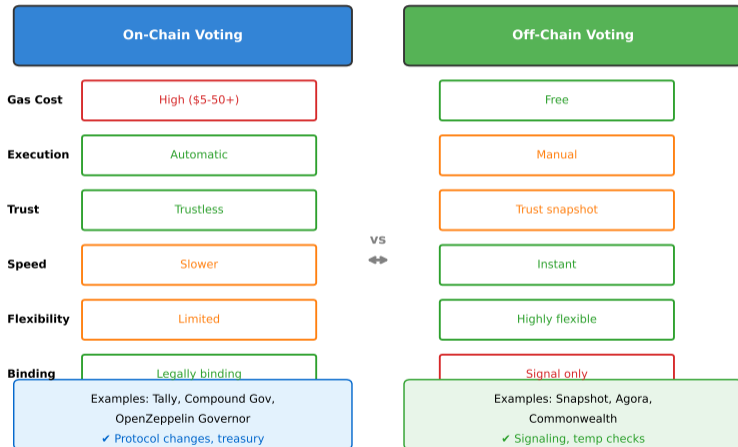
Snapshot Platform Growth



33,000+ spaces and growing — Source: Snapshot.org

On-Chain vs Off-Chain Voting

On-Chain vs Off-Chain Voting: Tradeoffs



Best Practice: Hybrid approach - off-chain discussion, on-chain execution

Best practice: off-chain signaling, on-chain execution

Setting Up Governance: Steps

1. **Choose platform:** Snapshot (off-chain) or Tally (on-chain)
2. **Deploy token:** ERC-20 on Ethereum/Polygon/other
3. **Configure voting:**
 - Strategy: token balance, quadratic, delegation
 - Quorum: minimum participation required
 - Duration: voting period length
4. **Create proposal:** Title, description, options
5. **Execute result:** Manual or via smart contract

Cost: \$6 on Polygon (illustrative, varies with gas prices)

Five voting systems, five trade-offs:

- **Token:** Simple but plutocratic
- **Quadratic:** Fair but needs identity
- **veToken:** Long-term aligned but illiquid
- **Reputation:** Earned but centralized oracle
- **Conviction:** Resistant but slow

Design principles:

- Match system to governance needs
- Consider hybrid approaches
- Prioritize participation over perfection

Good governance design is iterative—start simple, improve based on feedback

Academic:

- Posner & Weyl (2018): “Radical Markets” – Princeton UP
- Buterin, Hitzig & Weyl (2018): “Liberal Radicalism” – arXiv:1809.06421

Technical:

- Curve Finance: docs.curve.fi/curve_dao/vecrv
- 1Hive: wiki.1hive.org
- Snapshot: docs.snapshot.org

Tools:

- Snapshot.org (off-chain voting)
- Tally.xyz (on-chain governance)
- OpenZeppelin Governor

Next lesson: Hands-on governance exercise with Snapshot