# #14 DAOs & Governance

Lecture Notes for CS190N: Blockchain Technologies and Security November 17, 2025

This lecture explores Decentralized Autonomous Organizations (DAOs), the final layer of the DeFi stack that governs how protocols evolve. We will demystify the core voting mechanisms that power DAOs, from the simple but flawed "one token, one vote" model to more equitable alternatives. We will also examine how these on-chain democracies can fail, using flash loan attacks as a stark example, and conclude with the Curve Wars as a case study of complex, real-world governance dynamics.

## 1 INTRODUCTION: THE BRAIN OF DEFI

### 1.1 The DeFi Stack: From Money to Management

Over our past few lessons, we've assembled the core building blocks of DeFi, the "money legos." We started with the foundation, **stablecoins**, which provide a reliable unit of value. On top of that, we built the transactional layers: **AMMs** for trading and **lending protocols** for credit. We then explored the sophisticated instruments of **perpetuals** for leverage and the invisible hand of **MEV** that influences transaction ordering.

These legos click together to form powerful, autonomous financial machines. But machines don't run themselves forever. Parameters need tuning, bugs need fixing, and treasuries need managing. This brings us to the final, crucial layer of the stack: who is in charge? In DeFi, the answer is not a CEO or a board of directors, but a new form of collective organization: the **Decentralized Autonomous Organization (DAO)**.

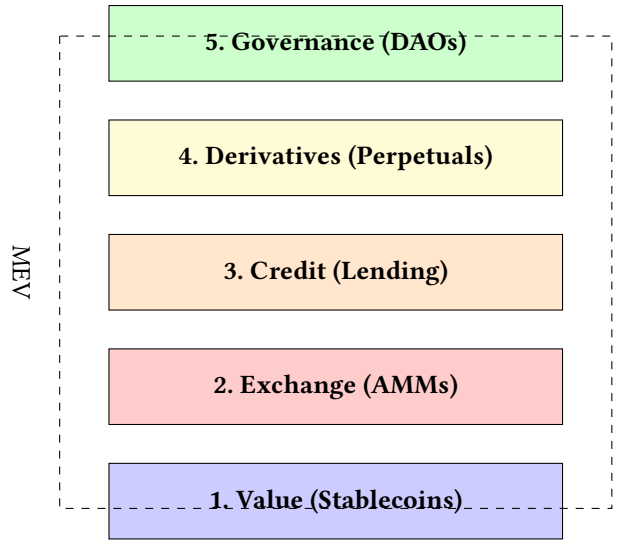


Fig. 1. The DeFi Stack, with DAOs acting as the top-level governance layer that directs and manages the underlying financial primitives.

### 1.2 What is a DAO? A Company Run by Code

A Decentralized Autonomous Organization (DAO) is an organization represented by rules encoded as a computer program that is transparent, controlled by the organization members, and not

influenced by a central government [4]. Think of it as a company where the bylaws are written in smart contracts and all shareholder votes are binding and automatically executed.

The core idea is to replace the opaque, hierarchical structure of a traditional company with a transparent, flat, and democratic system. The DAO is the brain of a DeFi protocol, allowing its community of token holders to collectively steer its future.

## 2 THE MECHANICS OF ON-CHAIN DEMOCRACY

### 2.1 Token-Weighted Voting: One Token, One Vote

The most common form of DAO governance is simple and intuitive: your voting power is directly proportional to the number of governance tokens you hold. If you own 1% of the tokens, you have 1% of the votes.

This model is easy to implement and ensures that those with the largest financial stake in the protocol have the most say. However, it has a significant drawback known as the "**whale problem**." A few large holders, or "whales," can easily outvote hundreds or thousands of smaller holders ("fish"), leading to a concentration of power that undermines the goal of decentralization.

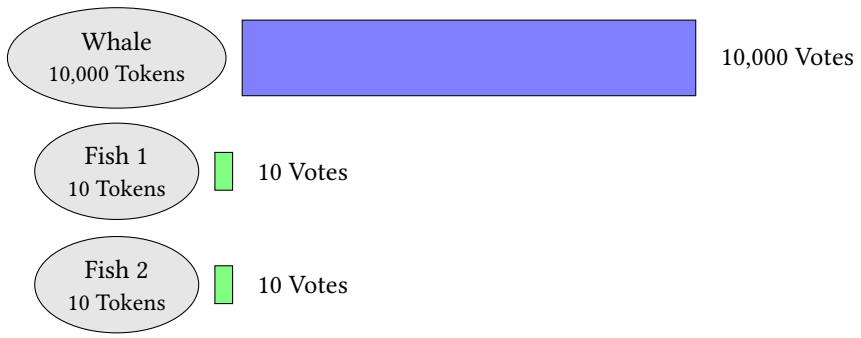


Fig. 2. The "whale problem" in token-weighted voting. The whale's voting power (blue bar) is orders of magnitude larger than that of smaller token holders (green bars), allowing them to dominate decisions.

### 2.2 Quadratic Voting: Power to the Passionate

To counter the whale problem, some DAOs have explored **quadratic voting**. The core principle is simple but powerful: the cost to cast votes increases quadratically. Your first vote costs 1 "credit," your second vote costs 3 more (for a total of 4), your third costs 5 more (for a total of 9), and so on.

$$\text{Cost in Credits} = (\text{Number of Votes})^2 \tag{1}$$

This means casting many votes on a single issue becomes exponentially expensive. It forces voters to allocate their limited resources to the issues they care about most, allowing a passionate minority to have a meaningful voice against an indifferent majority. It measures the *intensity* of preference, not just the amount of capital [3].

**Example:** With a budget of 16 credits, a voter could:

- Cast 1 vote on 16 different issues ($1^2 \times 16 = 16$ credits).
- Or, cast 4 votes on one single, critical issue ($4^2 = 16$ credits).

### 2.3 Governance Failure: The Flash Loan Attack

The on-chain nature of DAOs creates new, unique attack vectors. The most dramatic is the **flash loan governance attack**. Because voting power is just a token balance at a specific block, an attacker can use a flash loan to temporarily acquire a massive number of governance tokens.

The attack unfolds in a single, atomic transaction:

(1) **Borrow:** The attacker takes a flash loan for a huge amount of the protocol's governance token.
(2) **Vote:** The attacker uses this temporary, massive voting power to pass a malicious proposal (e.g., "Transfer all treasury funds to the attacker's address").
(3) **Execute:** If the DAO has no time delay, the proposal is executed immediately, and the funds are transferred.
(4) **Repay:** The attacker repays the flash loan.

The infamous $181 million hack of **Beanstalk Farms** in 2022 was executed this way [1]. It highlights a critical design principle for DAOs: there must be a time delay between when a vote passes and when its code can be executed, to prevent this kind of instant manipulation.

## 3 CASE STUDY: THE CURVE WARS

The "Curve Wars" is a perfect real-world example of how DAO governance is not just about voting on proposals, but is a complex, game-theoretic battle for economic influence.

### 3.1 The Prize: Directing Liquidity

As we know, Curve is the dominant AMM for stablecoins. Its governance token, CRV, can be locked for up to four years to receive **veCRV** (vote-escrowed CRV). This veCRV gives holders the power to vote on which liquidity pools receive the weekly emissions of new CRV tokens.

This is an incredibly valuable power. By directing CRV rewards to a specific pool, a protocol can attract billions of dollars in liquidity, as LPs chase the highest yields. Deep liquidity is the lifeblood of any DeFi protocol, especially for stablecoins that need to maintain their peg.

### 3.2 The Battle: A Flywheel for Power

The Curve Wars is the competition between different protocols (like Convex Finance) to accumulate as much veCRV as possible. This creates a powerful feedback loop, or "flywheel."

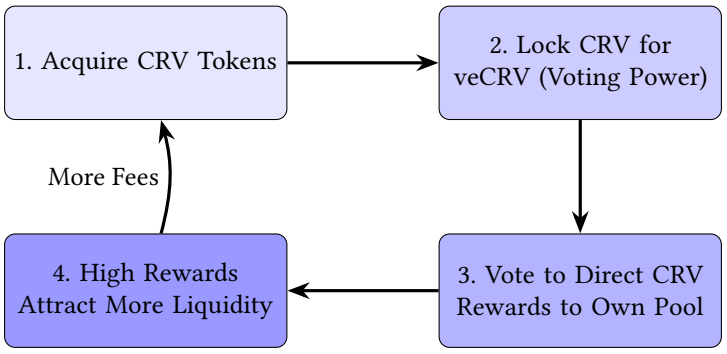


Fig. 3. The Curve Wars Flywheel. Protocols compete to accumulate voting power (veCRV) to direct rewards to their own liquidity pools, which in turn attracts more liquidity, generates more fees, and allows them to acquire even more CRV [2].

This war connects all our previous lessons:

- **AMMs & Stablecoins:** The entire battle is fought over attracting liquidity to specific AMM pools on Curve.
- **MEV:** The competition is so fierce that an entire ecosystem of "bribe" platforms has emerged, where protocols pay veCRV holders directly for their votes, a form of governance MEV.

The Curve Wars demonstrate that DAO governance is not a sterile voting process. It is a dynamic, competitive arena where economic incentives drive complex, emergent strategies.

## REFERENCES

[1] Beanstalk Farms. 2022. Beanstalk Governance Exploit Post-Mortem. https://bean.money/governance-exploit-post-mortem Accessed: 2025-10-01.

[2] Michael Egorov. 2019. StableSwap — Efficient Mechanism for Stablecoin Liquidity. https://curve.fi/files/stableswap-paper.pdf Accessed: 2025-10-01.

[3] Steven P. Lalley and E. Glen Weyl. 2018. Quadratic Voting: How Mechanism Design Can Radicalize Democracy. *American Economic Association Papers and Proceedings* 108 (2018), 33–37. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2003531

[4] Fabian Schär. 2021. Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. *Federal Reserve Bank of St. Louis Review* 103, 2 (2021), 153–174. doi:10.20955/r.103.153-74 Accessed: 2025-10-01.