

# DAOs & Governance

## Pre-Class Discovery Handout

Lesson 09 · Complete before class · 25–30 minutes

### Activity 1: Explore a Live DAO

10 min

Visit a DAO governance portal such as Tally.xyz, Snapshot.org, or Boardroom.io and explore a live DAO (e.g. Uniswap, Aave, or ENS). Answer:

1. How many active proposals does the DAO currently have? What topics do they cover?
2. What is the quorum requirement? What percentage of tokens typically participate in a vote?
3. Look at a recently passed proposal. What did it change? How many votes were cast for vs. against?
4. Is voting conducted on-chain or off-chain (Snapshot)? What are the gas cost implications of each approach?

**Bonus:** Take a screenshot of a proposal page and annotate the key governance parameters (quorum, voting period, vote totals).

### Activity 2: Governance Mechanism Comparison

10 min

Investigate three voting mechanisms and compare their properties. Answer:

1. Simple token voting (1 token = 1 vote): What is the main advantage? What is the primary criticism regarding wealth concentration?
2. Quadratic voting (cost of  $n$  votes =  $n^2$  credits): How does it give smaller holders more proportional influence? What mechanism prevents Sybil attacks?
3. Conviction voting (votes accumulate over time): How does this differ from a single snapshot vote? What problem of last-minute manipulation does it solve?
4. Which mechanism would you choose for a community treasury with 10,000 members of varying token holdings? Justify your answer.

Mechanism	Advantage	Disadvantage	Best For
Token voting	_____	_____	_____
Quadratic voting	_____	_____	_____
Conviction voting	_____	_____	_____

### Activity 3: Treasury Analysis

5 min

Visit DeepDAO.io or a DAO's own treasury dashboard and analyse the treasury of a major DAO (e.g. MakerDAO or Uniswap). Answer:

1. What is the total treasury value? What are the largest asset holdings?
2. How is the treasury diversified across asset classes (ETH, stablecoins, protocol tokens, real-world assets)?
3. Find a recent grant or budget proposal. How much was requested, and what was the stated purpose?
4. If a DAO holds a \$100M treasury earning 5% APY, how much can it spend annually without depleting its capital base?

**Treasury Size:** \$ \_\_\_\_\_ **Largest Asset:** \_\_\_\_\_ **Annual Sustainable Budget:** \$ \_\_\_\_\_

**Activity 4: Governance Attack Scenarios**

5 min

Consider the following attack scenarios and propose a concrete defense for each:

1. An attacker takes a flash loan of 1,000,000 governance tokens, votes to drain the treasury, and repays the loan in the same block. How would you prevent this?
2. A whale holds 40% of governance tokens and consistently votes in their own financial interest against the community. What mechanism could limit their disproportionate power?
3. An adversary creates 100 wallets to accumulate more influence in a quadratic voting system (Sybil attack). How can the protocol detect and prevent this?
4. A malicious proposal passes but is subject to a 48-hour timelock. What emergency mechanism should exist to protect users before execution?

Attack	Defense Mechanism	Tradeoff
Flash loan governance	_____	_____
Whale dominance	_____	_____
Sybil attack	_____	_____
Malicious timelock	_____	_____

**Key Terms**

---

Term	Definition
<b>DAO</b>	Decentralized Autonomous Organization. An organization governed by smart contracts and token holder voting rather than centralized management. Members propose and vote on decisions transparently on-chain.
<b>Governance Token</b>	A token that grants voting rights in a DAO's decision-making process. Holding more tokens typically confers more voting power under simple token-weighted voting schemes.
<b>Proposal</b>	A formal suggestion submitted to a DAO for member voting. Proposals can modify protocol parameters, allocate treasury funds, or change the governance rules themselves.
<b>Quorum</b>	The minimum number of votes (or percentage of total token supply) required for a governance vote to be considered valid. Prevents decisions being made by a tiny minority.
<b>Quadratic Voting</b>	A voting mechanism where the cost of additional votes increases quadratically (1 vote = 1 credit, 2 votes = 4 credits, 3 votes = 9 credits), giving smaller holders more proportional influence relative to whales.
<b>Delegation</b>	The act of assigning one's voting power to another address (a delegate) who votes on the holder's behalf. Enables participation without active involvement in every individual vote.
<b>Timelock</b>	A mandatory delay between when a governance proposal passes and when it is executed on-chain, giving the community time to react to potentially harmful or malicious changes.
<b>Multi-sig</b>	Multi-signature wallet. Requires $M$ -of- $N$ signatures to execute a transaction (e.g., 3-of-5 designated signers must approve). Widely used for DAO treasury management and proposal execution.
<b>Snapshot Voting</b>	Off-chain voting using signed messages instead of on-chain transactions, eliminating gas costs for voters. Results are typically enacted via a trusted multi-sig or guardian contract.
<b>Flash Loan Attack</b>	An attack where an adversary borrows a large amount of governance tokens via a flash loan, votes on a malicious proposal, and repays the loan—all within a single atomic transaction block.
<b>Conviction Voting</b>	A voting mechanism where a voter's influence on a proposal grows continuously over time as they keep their stake committed to it, favoring sustained community support over last-minute flash consensus.
<b>Treasury Diversification</b>	The practice of holding DAO assets across multiple token types (stablecoins, ETH, protocol tokens, real-world assets) to reduce volatility risk and ensure long-term operational sustainability.
<b>Ragequit</b>	A mechanism (popularized by Moloch DAO) allowing dissatisfied members to exit with their proportional share of the treasury before a proposal they oppose is executed, protecting minority rights.
<b>Governance Minimization</b>	A design philosophy advocating for reducing the scope of on-chain governance decisions over time, making protocols more autonomous and less vulnerable to governance capture or coordinated attacks.

---