Topic 5.3: DAO Governance

Decentralized Autonomous Organizations

Joerg Osterrieder

Digital Finance

2025

Learning Objectives

By the end of this topic, you will be able to:

1. Explain DAO governance mechanisms and their tradeoffs
2. Identify governance attack vectors and defenses
3. Evaluate tradeoffs between on-chain and off-chain governance
4. Understand why "code is law" is insufficient
5. Analyze token distribution's impact on voting power

Core Question

Can decentralized organizations achieve effective governance without central authority?

Key Insight:
Governance IS the attack surface. Secure code means nothing if governance can change it.

Prerequisites and Background

What You Should Already Know:

- Basic blockchain concepts (from Days 1–3)
- Smart contract fundamentals (from T5.1)
- DeFi protocol basics (from T5.2)

No Prior Knowledge Needed For:

- Voting systems — we explain everything from scratch
- Game theory — we introduce concepts as we go
- Square root calculations — we walk through every example

Conceptual Foundations:

- Traditional corporate governance (boards, shareholders)
- Democratic voting systems (elections, referendums)
- The challenge of making sure the people who manage an organization actually serve the members' interests, not their own

Important Context

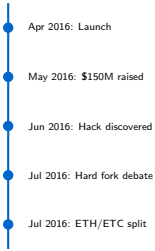
DAOs attempt to solve the coordination problem: How can groups make collective decisions without trusted intermediaries?

Historical Context: The DAO

The Original DAO (2016):

- First major DAO experiment on Ethereum
- Raised $150M in crowdfunding
- Hacker exploited reentrancy vulnerability
  (Recall from T5.1: reentrancy = the bug where a contract can be tricked into sending money multiple times before updating its records)
- Drained $60M from the fund
- Led to Ethereum/Ethereum Classic split

Key Lesson:
The "code is law" philosophy was tested—and the community chose human intervention over code finality.



What is a DAO?

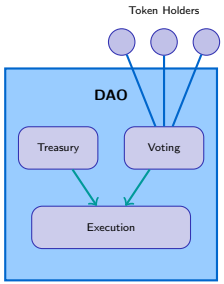
Decentralized Autonomous Organization:

- Rules encoded in smart contracts
- Decisions via token holder voting
- Treasury managed on-chain
- No traditional legal structure
- "Code is law" philosophy

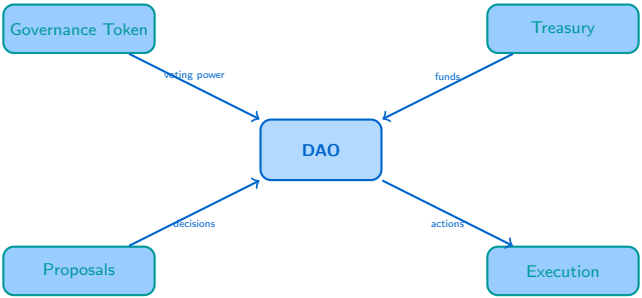
Analogy: Imagine a club where:

1. The rules are written in a contract that nobody can secretly change
2. Every member votes on decisions using tokens instead of raised hands
3. The treasury is managed by code, not a treasurer who could run away with the money

That's a DAO.



Core DAO Components



Governance Token: Represents voting power and economic stake in the protocol

Treasury: Pooled funds controlled by governance votes, often billions in value

Token-Based Voting (1 Token = 1 Vote)

How It Works:

- Each token equals one vote
- Simple and transparent
- Aligns voting with economic stake
- Most common mechanism

Analogy: Token voting works like corporate shareholder voting: 1 share = 1 vote. If you own more shares (tokens), you have more say. Simple, but this creates a problem...

Example:
If you hold 100 tokens out of 1,000,000 total, you have 0.01% voting power.

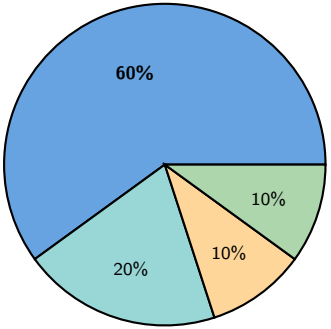
Advantage:
Economic skin in the game—those most invested have most say.

Disadvantage:
Wealth equals power—by design. This is the **plutocracy problem**, and it is the central challenge of DAO governance.

Critical Issue

If 10 wallets hold 60% of tokens, democracy becomes oligarchy. The majority of token holders have no meaningful voice.

The Plutocracy Problem



Top 10 wallets: 60%

Next 100: 20%

Next 1000: 10%

Everyone else: 10%

Reality: Most DAOs have highly concentrated token distributions.
Result: A few whales control most decisions. “Decentralized” in name only.

Real-World Token Concentration

Top 10 Holders' Share of Governance Tokens

DAO	Top 10 Share	Implication
MakerDAO (MKR)	48.2%	Near majority control
Uniswap (UNI)	52.1%	Majority control
Compound (COMP)	57.8%	Strong majority
Aave (AAVE)	42.3%	Significant influence
Curve (CRV)	61.5%	Dominant control

Key Insight

In most "decentralized" protocols, fewer than 10 entities can pass any proposal they want. This is not a bug—it reflects how token distributions naturally evolve.

Why So Many Voting Systems?

The Core Problem:
Simple token voting (1 token = 1 vote) has a fatal flaw: it turns "decentralized governance" into rule by the wealthiest token holders.

So researchers and developers have proposed alternatives. Each tries to fix plutocracy in a different way:

Basic (next two slides)

- **Quadratic Voting** — make extra votes increasingly expensive
- **Conviction Voting** — reward long-term commitment

Advanced (later slides)

- **Delegation** — let experts vote on your behalf
- **Optimistic Governance** — approve unless someone objects
- **Multi-Sig** — require multiple keyholders
- **Futarchy** — use prediction markets to decide

No Silver Bullet

Every mechanism trades one problem for another. The art of DAO design is choosing the right combination.

Quadratic Voting

Core Concept:

$$\text{Voting Power} = \sqrt{\text{Tokens Held}}$$

Why the square root? It makes each additional vote on the same issue increasingly expensive. Your 1st vote costs 1 token. Your 2nd vote costs 4 tokens total. Your 3rd costs 9. This means a passionate minority can express strong preferences, but cannot simply buy dominance.

Example Calculations:

- 100 tokens $\rightarrow \sqrt{100} = 10$ votes
- 10,000 tokens $\rightarrow \sqrt{10{,}000} = 100$ votes
- 1,000,000 tokens $\rightarrow \sqrt{1{,}000{,}000} = 1{,}000$ votes

Impact:
A whale with 10,000x more tokens only gets 100x more votes (not 10,000x).

Advantages:

- Reduces whale dominance
- Gives small holders more voice
- Encourages broader participation

Critical Vulnerability:

Sybil Attack

A **Sybil attack** is when one person creates many fake identities to gain disproportionate influence (named after a book about multiple personalities).

Under regular voting: 1 person, 100 tokens = 100 votes. Split into 10 wallets of 10 each = still 100 votes.

Under quadratic voting: 1 person, 100 tokens = $\sqrt{100} = 10$ votes. Split into 10 wallets: $10 \times \sqrt{10} \approx 31.6$ votes.

Splitting INCREASES power! Quadratic voting requires identity verification.

Conviction Voting

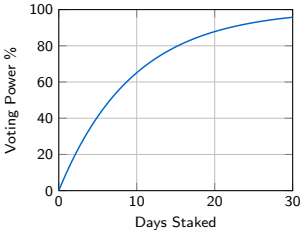
How It Works:

- Votes accumulate over time
- Longer stake = more voting power
- Rewards long-term alignment
- Prevents flash loan attacks

Worked Example (decay factor = 0.9):
Alice stakes 100 tokens on Proposal A:

- Day 1: conviction = 100
- Day 2: conviction = 190 (100 + 90)
- Day 3: conviction = 271 (190 + 81)
- Day 4: conviction = 344 (271 + 73)

Her conviction grows over time but at a decreasing rate. When total conviction crosses the threshold, the proposal passes.



Tradeoff:
Slower decision-making. Emergencies require alternative mechanisms.

Difficulty: *Intermediate* — requires understanding how time affects voting power.

Vote Delegation (Liquid Democracy)

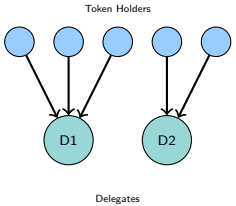
What Is Liquid Democracy?
In liquid democracy, you can either vote yourself OR delegate your vote to someone you trust—and take it back anytime. Think of it as a "flexible proxy" system.

How Delegation Works:

- Delegate votes to trusted experts
- Retain token ownership
- Can revoke delegation anytime
- Addresses voter apathy

Popular Implementations:

- Compound Finance delegates
- Uniswap governance
- ENS DAO delegation



Risk

Delegation can further concentrate power among a few prominent delegates.

Multi-Signature (Multi-Sig) Governance

Analogy: Like a bank vault that needs 3 out of 5 keyholders to open. An N-of-M signature means N people (out of M total) must approve before a transaction goes through.

N-of-M Signing:

- N signers must approve out of M total
- Example: 3-of-5 multi-sig
- Fast execution for routine decisions
- Common for treasury management

Popular Tools:

- Gnosis Safe (most common)
- Aragon multi-sig
- Custom implementations

Tradeoffs:

Aspect	Rating
Speed	High
Decentralization	Low
Security	Medium
Transparency	Medium

Common Pattern

Many DAOs combine multi-sig for day-to-day operations with token voting for major decisions.

Optimistic Governance

Analogy: Like expense approvals at work: submit your receipt, and it is automatically approved UNLESS someone objects within 3 days. Most proposals pass without drama—only controversial ones get challenged.

How It Works:

1. Proposal submitted
2. Short challenge period begins
3. If no veto $\rightarrow$ auto-execute
4. If vetoed $\rightarrow$ standard vote

Advantages:

- Dramatically increases speed
- Reduces voter fatigue
- People only engage when they disagree

Requirements:

- Active community monitoring
- Fast response capability
- Clear veto thresholds

Best For

Low-risk parameter changes, not major protocol upgrades.

Voting Mechanism Comparison

Mechanism	Whale-Proof?	Speed	Complexity	Identity Needed?
Token Voting	No	Fast	Low	No
Quadratic	Partially	Fast	Medium	Yes
Conviction	Yes	Slow	Medium	No
Delegation	No	Fast	Low	No
Multi-Sig	N/A	Very Fast	Low	Yes
Optimistic	No	Very Fast	Low	No

Key Takeaway

No single mechanism solves all problems. Most successful DAOs combine multiple mechanisms for different types of decisions.

Real-World Pattern

Routine changes: optimistic or multi-sig.
Major upgrades: token voting with timelock.
Treasury grants: conviction or quadratic.

Governance Attack Vectors

Flash Loan Governance Attack:

(Remember flash loans from T5.1: borrow millions instantly, use them, return them—all in one transaction.)

1. Borrow millions in governance tokens
2. Vote on malicious proposal
3. Execute immediately
4. Repay loan, keep profits

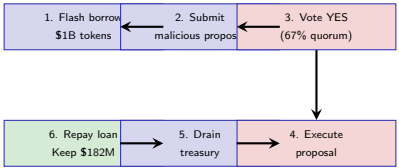
Beanstalk Attack (2022):

- Flash borrowed $1B in tokens
- Passed proposal in one block
- Drained $182M from treasury
- All in a single transaction

Other Attack Vectors (ranked by prevalence):

1. **Whale dominance** (every major DAO)—large holders outvote everyone else
2. **Voter apathy** (widespread)—too few people vote, making attacks easier
3. **Flash loan attacks** (rare but devastating)—borrow tokens, vote, return them
4. **Dark DAOs** (theoretical)—secret organizations that pay voters to vote a certain way, like a hidden lobby that bribes shareholders
5. **Governance capture** (emerging)—slowly accumulating enough power to control the protocol

Case Study: Beanstalk Governance Attack



Critical flaw: No time delay between vote and execution.
Fix: Timelocks, snapshot voting, flash loan protection.

Governance Defense: Timelocks

Analogy: A timelock is a mandatory "cooling-off period" — like the waiting period when you buy a house, giving you time to reconsider before the deal is final.

How Timelocks Work:

- Delay between approval and execution
- Typically 24–72 hours minimum
- Gives community time to react
- Critical security mechanism

Real Examples:

- Uniswap: 7-day timelock
- Compound: 48-hour timelock
- MakerDAO: Variable by risk

What Happens During Timelock:

1. Community reviews approved proposal
2. Users can exit protocol if they disagree
3. Guardians can cancel malicious proposals
4. Security researchers can alert issues

Tradeoff

Longer timelock = more security but slower operations. Emergency situations require special mechanisms.

Vote Escrow: The veToken Model

Intuition: veTokens are a "commitment multiplier." Lock your tokens for longer, get more voting power. Lock for 1 year = 1x votes. Lock for 4 years = 4x votes. This rewards long-term commitment over short-term speculation.

How veTokens Work:

- Lock tokens to gain voting power
- Longer lock = more voting power
- Maximum lock often 4 years
- Pioneered by Curve Finance

Voting Power Formula:

$$\text{vePower} = \text{Tokens} \times \frac{\text{Lock Time}}{\text{Max Lock}}$$

Example: 100 CRV locked 2 years
$= 100 \times \frac{2}{4} = 50$ veCRV

Why It Prevents Flash Loans:

- Tokens must be locked to vote
- Flash loans require same-block return
- Cannot lock and unlock instantly
- Attacker would need real capital

Additional Benefits:

- Aligns long-term incentives
- Reduces token velocity (how quickly tokens change hands)
- Committed stakeholders decide

Snapshot Voting as Defense

How Snapshot Defense Works:

- Record token balances at specific block
- Block chosen BEFORE proposal created
- Voting power based on historical balance
- Flash loan has no effect

Timeline:

1. Block 100: Snapshot taken
2. Block 105: Proposal created
3. Block 150: Flash loan attempted
4. Result: Flash loan ignored—balance was 0 at block 100

Implementation:

- Snapshot.org (off-chain)
- OpenZeppelin Governor (on-chain)
- Custom snapshot contracts

Key Insight

Snapshot voting elegantly solves flash loan attacks without restricting token liquidity. Users can still trade freely—only historical balance matters for votes.

Quorum Requirements

What is Quorum?
Analogy: Like needing a minimum number of people at a meeting before you can take a valid vote. If too few show up, any decision is invalid.

- Minimum participation threshold
- Vote invalid if quorum not met
- Prevents minority rule
- Typical range: 4–10%

Example:
If quorum = 4% and total supply = 1B tokens:
At least 40M tokens must vote for the result to be valid.

Higher Quorum for Critical Decisions:

Decision Type	Quorum
Parameter change	4%
Treasury grant	5%
Protocol upgrade	10%
Emergency action	15%

The Quorum Dilemma

Too low: Small group can pass anything
Too high: Nothing ever passes due to voter apathy

Guardian and Veto Powers

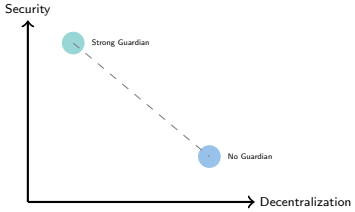
Guardian Multi-Sig:

- Small trusted group (5–9 members)
- Can veto malicious proposals
- “Emergency brake” function
- Used during timelock period

When Guardians Act:

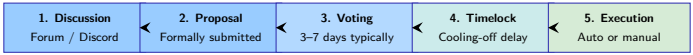
- Clear governance attack detected
- Proposal would harm protocol
- Bug discovered in approved code
- Legal/regulatory emergency

The Centralization Tradeoff:



Best Practice:
Sunset guardians over time as protocol matures and governance proves robust.

How a DAO Proposal Actually Works



Typical Timeline:

- Discussion: 1–2 weeks on forums
- Proposal: snapshot or on-chain submission
- Voting: 3–7 day window
- Timelock: 24 hours to 7 days
- Execution: immediate (on-chain) or manual (off-chain)

Where Attacks Can Happen:

- Step 2: Flash loan to create + vote instantly
- Step 3: Vote buying during voting period
- Step 4: This is where timelocks protect us
- Step 5: Malicious code in proposal payload

Key Point

Each step is a potential point of failure—and a potential point of defense.

On-Chain vs. Off-Chain Governance

Aspect	On-Chain	Off-Chain
Binding	Automatic execution	Requires implementation
Transparency	Fully verifiable	Forum/snapshot
Cost	Gas fees	Usually free
Speed	Blockchain constrained	Faster iteration
Flexibility	Rigid (code)	Adaptable
Attacks	Flash loans, 51%	Social, coordination
Examples	Compound, Uniswap	Bitcoin, Ethereum L1

Hybrid Approaches

Most successful DAOs use both: off-chain discussion/signaling, on-chain execution with safeguards.

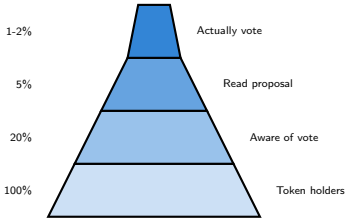
The Voter Apathy Problem

Reality of DAO Participation:

- Typical turnout: 1–5% of tokens
- Most token holders never vote
- Few wallets dominate decisions
- Governance fatigue is real

Why People Don't Vote:

- Gas costs (on-chain)
- Time to understand proposals
- Rational ignorance—when the cost of learning about an issue exceeds the impact your single vote can have, it is "rational" to stay uninformed
- Token holders $\neq$ users



"Code is Law" vs. Rule of Law

"Code is Law" Philosophy:

- Smart contract IS the agreement
- No external intervention
- Predictable, immutable
- "If the code allows it, it's allowed"

The DAO Hack Challenge (see slide 4):

- Hacker used code as designed
- Was it theft or legitimate use?
- Ethereum community chose to fork
- "Code is law" violated by humans

Traditional Rule of Law:

- Intent matters—*mens rea* (Latin: "guilty mind," the legal concept that you must intend to do wrong to be criminally liable)
- Fairness considerations
- Courts interpret disputes
- Law evolves with society

The Tension

Code cannot encode intent, fairness, or context. Pure "code is law" may be unjust. But human intervention undermines decentralization.

Model How Token Distribution Affects Governance

In the Colab notebook, we will:

1. Create token distributions with varying concentration and simulate voting on proposals (∼8 min)
2. Test attack scenarios: whale dominance and flash loans (∼7 min)
3. Explore defense mechanisms: quadratic voting, delegation (∼7 min)

Access the Notebook

`day_05/notebooks/NB12_dao_governance_simulation.ipynb`

See how 1 whale with 51% can override 10,000 small holders.

Time: 20–25 minutes for guided exploration

NB12: Key Simulation Exercises

Exercise 1: Distribution & Voting

- Generate realistic Pareto distributions
- Visualize wealth concentration
- Calculate Gini coefficient
- Simulate proposal voting
- Model whale vs. community outcomes

Exercise 2: Attack Scenarios

- Model flash loan attack
- Test vote buying economics
- Simulate 51% accumulation
- Measure attack costs

Exercise 3: Defense Mechanisms

- Implement quadratic voting
- Test conviction voting
- Model delegation effects
- Compare outcomes across mechanisms

Key Question to Answer

How does changing from 1-token-1-vote to quadratic voting affect a whale's ability to pass self-serving proposals?

Discussion: Governance Tradeoffs

Questions to Consider:

1. Is plutocracy inherent to token voting?
2. Should DAOs have constitutions?
3. When is centralization acceptable?
4. Can code ever fully replace human judgment?

Key Takeaways:

- Governance IS the attack surface
- Token distribution = power distribution
- "Decentralized" often isn't
- Hybrid models emerging

The Governance Trilemma

You can optimize for two of three: **Decentralization**, **Efficiency**, **Security**. Pick which one to sacrifice.

Examples:

- **Company board** = efficient + secure, but centralized
- **Bitcoin governance** = decentralized + secure, but slow (years to change)
- **Small DAO with optimistic voting** = decentralized + efficient, but vulnerable to attacks

Application: Real DAO Governance Examples (1/2)

MakerDAO:

- Governs DAI stablecoin
- MKR token for voting
- Complex risk parameters
- Executive votes for changes

Uniswap:

- UNI token governance
- 7-day timelock
- 4% quorum requirement
- Treasury grants program

Compound:

- COMP token governance
- On-chain proposals
- 48-hour timelock
- Delegation system

Aave:

- AAVE token governance
- Two-tier proposal system
- Progressive decentralization
- Cross-chain governance emerging

Application: Real DAO Governance Examples (2/2)

Curve Finance:

- veCRV model pioneer (lock tokens for votes)
- Up to 4-year locks
- **Gauge voting for emissions:** token holders vote on which liquidity pools receive newly minted CRV rewards each week — controlling where incentives flow
- **"Curve Wars":** DAOs competing to accumulate veCRV so they can direct CRV rewards to their own pools — a battle for governance power over the largest stablecoin exchange

Why Curve Wars Matter:
The Curve Wars illustrate a key governance insight: when governance tokens control real economic flows (like reward emissions worth millions per week), governance power itself becomes a valuable asset that other protocols will fight to acquire.

Pattern

Governance power $\rightarrow$ economic control $\rightarrow$ arms race for governance tokens $\rightarrow$ further concentration.

Application: Designing DAO Governance

Key Design Questions:

1. Who can submit proposals?
2. What is the voting period?
3. What quorum is required?
4. How long is the timelock?
5. Who has veto power?

Progressive Decentralization:

- Start with strong team control
- Gradually add community power
- Remove training wheels over time
- Earn trust through track record

Common Governance Stack:

1. **Forum:** Discussion (Discourse)
2. **Signaling:** Temperature check (Snapshot)
3. **Voting:** Binding vote (Governor)
4. **Execution:** Timelock controller
5. **Safety:** Guardian multi-sig

OpenZeppelin Governor

Standard, audited implementation covering the full governance lifecycle.

Application: The Future of DAO Governance

Emerging Innovations:

- **Reputation-based voting:** Non-transferable credentials
- **Soulbound tokens:** Identity-linked voting power (named after non-transferable items in video games — once earned, they cannot be sold or given away)
- **Futarchy:** Governance by prediction markets — bet on outcomes to decide policy. If the market predicts Policy A leads to better results, Policy A wins
- **AI governance:** Automated analysis of proposals

Legal Developments:

- Wyoming DAO LLC law (USA)
- Marshall Islands DAO recognition
- EU MiCA framework (Europe)
- Switzerland's "DLT Act" (enables tokenized securities and DAO-like structures)
- Regulatory clarity emerging globally

Open Question

Can DAOs become the dominant organizational form of the 21st century, or are they limited to niche applications where trust minimization is paramount?

Executive Summary

Core Concepts:

1. DAOs encode governance in smart contracts
2. Token-based voting creates plutocracy
3. Quadratic voting reduces but doesn't eliminate whale power
4. Flash loans can exploit instant-execution governance
5. Timelocks and snapshots are essential defenses

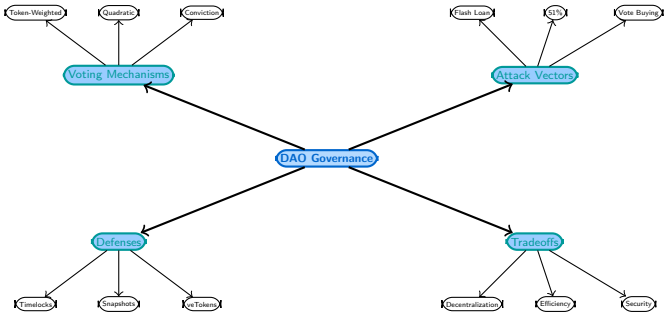
Key Insights:

1. Governance IS the attack surface
2. "Decentralized" is often a spectrum
3. Voter apathy is rational behavior
4. Code cannot encode fairness
5. Hybrid models work best

One-Sentence Summary

DAO governance attempts to solve collective decision-making without trusted intermediaries, but faces fundamental tradeoffs between decentralization, efficiency, and security that make true "decentralization" elusive in practice.

Concept Map: DAO Governance



Key Terms (1/2)

DAO: Decentralized Autonomous Organization—rules encoded in smart contracts, decisions via token voting.

Governance Token: Token representing voting power in organizational decisions.

Token-Weighted Voting: 1 token = 1 vote system; simple but plutocratic.

Quadratic Voting: Voting power = $\sqrt{\text{tokens}}$; reduces whale influence.

Conviction Voting: Voting power accumulates over time; rewards long-term alignment.

Delegation: Lending voting power to trusted representatives while retaining token ownership.

Quorum: Minimum participation threshold for valid vote.

Timelock: Delay between proposal approval and execution; security mechanism.

Snapshot Voting: Using historical token balance for voting power; prevents flash loan attacks.

veToken: Vote-escrowed token; locked tokens for increased voting power.

Key Terms (2/2)

Flash Loan Attack: Borrowing tokens temporarily to vote on malicious proposals.

51% Attack: Accumulating majority tokens to control all governance decisions.

Vote Buying: Paying token holders (directly or via protocols) to vote a certain way.

Plutocracy: Rule by the wealthy; inherent risk in token-weighted voting.

Voter Apathy: Low participation due to costs, complexity, or rational ignorance.

Multi-Sig: N-of-M signature requirement; used for treasury management.

Guardian: Trusted entity with veto power for emergency situations.

Sybil Attack: One person creating many fake identities to gain disproportionate influence.

On-Chain Governance: Voting and execution happen on blockchain; automatic but costly.

Off-Chain Governance: Voting off-chain (e.g., Snapshot); free but requires manual execution.

Code is Law: Philosophy that smart contract code defines all valid behavior.

Common Misconceptions

Misconception 1:
"DAOs are truly decentralized"
Reality: Token concentration means a few wallets often control outcomes. Most DAOs are plutocracies in practice.

Misconception 2:
"1 token = 1 vote is fair"
Reality: It's fair by one definition (stake-weighted), but it gives wealthy holders disproportionate control over protocol direction.

Misconception 3:
"Quadratic voting solves whale dominance"
Reality: Without identity systems, whales simply split tokens across wallets to game quadratic voting (Sybil attack).

Misconception 4:
"Code is law provides certainty"
Reality: Code cannot encode intent, context, or fairness. Communities regularly intervene when code produces unjust outcomes.

Misconception 5:
"High quorum prevents attacks"
Reality: High quorum can make governance non-functional. Attackers with sufficient tokens can still reach quorum.

Misconception 6:
"Token holders = users"
Reality: Many token holders are speculators; actual protocol users may have no governance voice.

Self-Assessment Questions (1/2)

Question 1: What does DAO stand for in blockchain governance?

A. Distributed Autonomous Operation
B. Decentralized Autonomous Organization
C. Digital Asset Organization
D. Delegated Authority Operation

Question 2: What happens when you delegate your governance tokens?

A. You permanently transfer ownership
B. The delegate can vote with your voting power on your behalf
C. Your tokens are locked and cannot be moved
D. You lose all rights until delegation is revoked

Answers: 1-B, 2-B

Self-Assessment Questions (2/2)

Question 3: What is the most effective defense against flash loan governance attacks?

A. Requiring voters to stake tokens for the entire voting period
B. Increasing gas costs for voting transactions
C. Using snapshot voting power from before proposal creation
D. Limiting tokens that can participate in any proposal

Reflection Questions:

- Can true decentralization exist with token-weighted voting?
- How would you design governance that balances efficiency and security?
- What role should human judgment play in "code is law" systems?

Answer: 3-C (Snapshot voting captures historical balance, making flash loans ineffective since attacker had 0 balance at snapshot)

What's Next: Topic 5.4 – Privacy and Financial Inclusion

Preview of T5.4:

- Blockchain transparency vs. privacy
- Surveillance capabilities and risks
- Privacy-preserving technologies
- Zero-knowledge proofs basics
- Financial inclusion opportunities

Connection to DAO Governance:
Privacy tools could enable anonymous voting, reducing vote buying and social pressure.

Key Questions for T5.4:

1. Is blockchain transparency a feature or bug?
2. How do privacy coins work?
3. Can DeFi serve the unbanked?
4. What are ZK-proofs and why do they matter?

Prepare

Consider: How does the public nature of blockchain transactions affect governance participation? Would you vote differently if your vote was anonymous?

Resources for Further Learning

Academic Papers:

- Buterin et al., "Liberal Radicalism" (Quadratic Voting)
- Weyl & Posner, "Radical Markets"
- Catalini & Gans, "Initial Coin Offerings"

Technical Documentation:

- OpenZeppelin Governor docs
- Compound Governance whitepaper
- Snapshot documentation
- Curve veToken mechanics

Case Studies:

- The DAO hack (2016)
- Beanstalk attack (2022)
- MakerDAO governance evolution
- Curve Wars analysis

Tools to Explore:

- Tally (governance aggregator)
- DeepDAO (DAO analytics)
- Boardroom (governance dashboards)
- Snapshot.org (off-chain voting)

Hands-On Practice

`day_05/notebooks/NB12_dao_governance_simulation.ipynb`

Questions?

Topic 5.3: DAO Governance
Decentralized Autonomous Organizations

"Governance is the attack surface."

Joerg Osterrieder
Digital Finance
2025