DAOs & Governance: Decentralized Decision-Making

Standalone Technical Lecture

Prof. Dr. Joerg Osterrieder

University Lecture Series

March 5, 2026

Lecture Roadmap

Learning Objectives

- Understand DAO architecture and smart contract governance
- Analyse voting mechanisms from simple to advanced
- Evaluate treasury management and tokenomics
- Identify governance attack vectors and defences
- Assess real-world DAO case studies and future trends

Prerequisites

- Lessons 1–5: Blockchain fundamentals, smart contracts, DeFi
- Basic familiarity with ERC-20 tokens and Ethereum

Durat

90 minutes — 5 sections — ˜55 frames — Prerequisite: Lessons 1–5

Table of Contents

Navig

through 5 sections covering DAO fundamentals to real-world governance and the future

Learning Objectives

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

1. **Explain** DAO architecture and compare governance models (token, reputation, multisig)
2. **Analyze** voting mechanisms (quadratic voting, conviction voting, holographic consensus)
3. **Evaluate** treasury management strategies and token economic sustainability
4. **Identify** governance attack vectors (flash loan attacks, vote buying, Sybil attacks)
5. **Assess** real-world DAO governance through MakerDAO, Uniswap, and Aave case studies

Bloom

taxonomy levels: Remember → Understand → Apply → Analyze → Evaluate → Create

Section 1: DAO Fundamentals & Architecture

Understanding decentralized organizations and their smart contract foundations

What You Will Learn

- What DAOs are and how they differ from traditional organizations
- Smart contract architecture for DAOs
- Membership models: token-based, share-based, reputation-based
- DAO creation frameworks and legal wrappers

Frames in This Section

Secti

1 of 5 — Frames 4–14

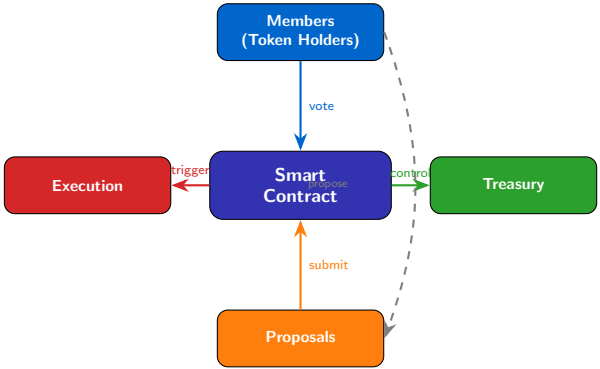
What is a DAO?

Decentralized Autonomous Organization

- **Organization encoded in smart contracts** – rules are code, not documents
- **No central authority** – no CEO, no board with unilateral power
- **Transparent and permissionless** – anyone can read the code and participate
- **Governed by token holders** – voting rights proportional to stake
- **Treasury on-chain** – funds held collectively, disbursed by vote

First DAO

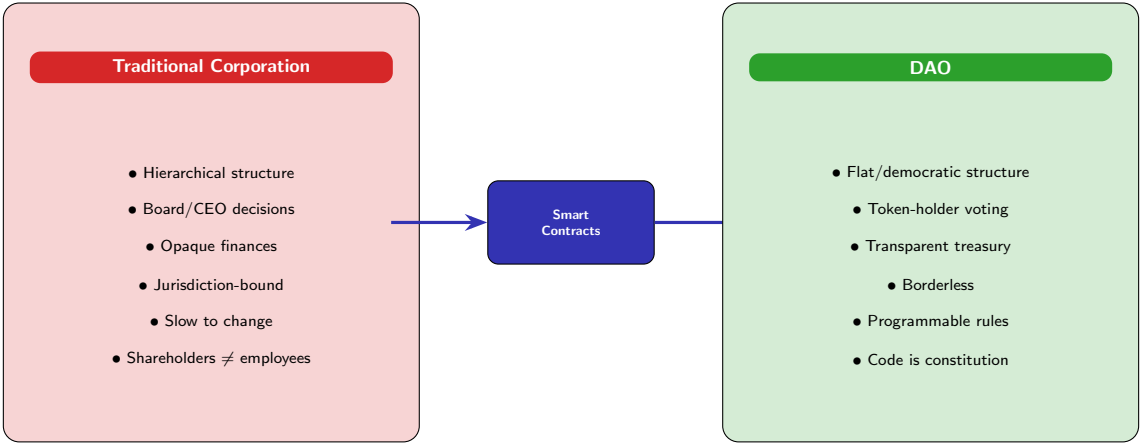
"The DAO" (2016) raised $150M in ETH before being hacked via a reentrancy vulnerability – leading to the Ethereum hard fork.



DAOs

replace legal contracts and corporate hierarchy with immutable code and token-based consensus

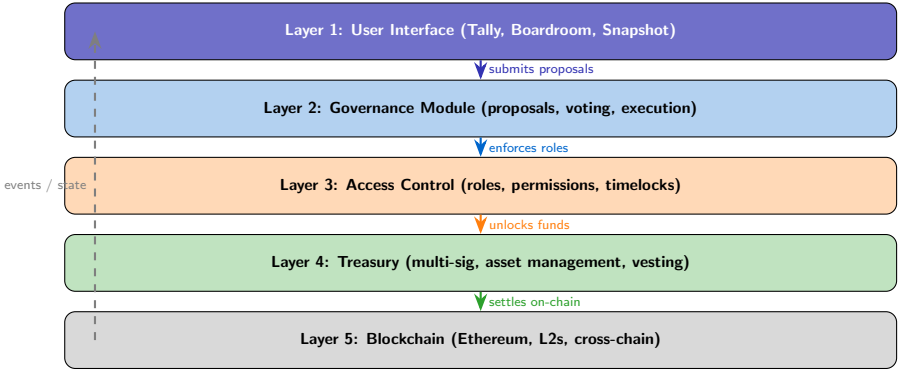
Traditional Organizations vs DAOs



DAOs

aim to replace trust in people with trust in code – but code has its own risks

DAO Architecture Overview



Open

Governor is the dominant Layer 2 implementation; Gnosis Safe dominates Layer 4 treasury management

Governor Contract Architecture

Listing 1: Simplified Governor Contract

```
// Simplified Governor Contract
contract DAOGovernor {
    uint256 public proposalCount;
    uint256 public quorumVotes;
    uint256 public votingPeriod;

    struct Proposal {
        address proposer;
        uint256 forVotes;
        uint256 againstVotes;
        uint256 endBlock;
        bool executed;
    }

    mapping(uint256 => Proposal)
        public proposals;

    function propose(
        string memory description
    ) external returns (uint256) {
        proposalCount++;
        proposals[proposalCount] =
            Proposal(msg.sender,
                0, 0,
                block.number + votingPeriod,
                false);
        return proposalCount;
    }
}
```

Governor Architecture

- **Proposal struct** stores proposer, vote tallies, deadline block, and execution status
- **proposalCount** acts as auto-incrementing ID and prevents hash collisions
- **votingPeriod** is measured in blocks (≈12s on mainnet), typically 40,320 blocks = 7 days
- **quorumVotes** sets minimum participation threshold to prevent low-turnout attacks

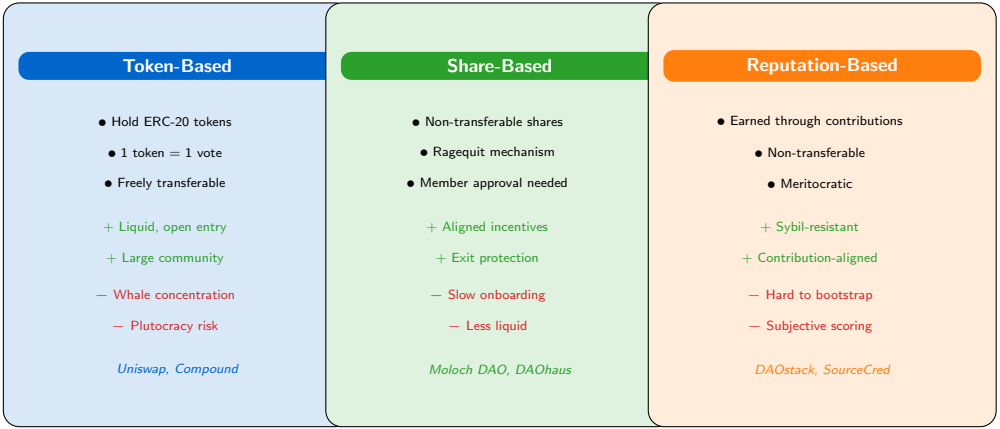
Production Standard

OpenZeppelin Governor (OZ) extends this pattern with:

- ERC20Votes checkpointing for snapshot-based voting power
- Timelock controller for delayed execution
- Modular extensions (Bravo-compatible, fractional voting)

Governor is used by Compound, Uniswap, and most major DAOs – always audit before deployment

Membership Models



Most real-world DAOs use token-based governance due to simplicity, but share-based models offer stronger alignment

Mechanics of Token Governance

- **Token distribution** determines governance power from day one – initial allocation is a political act
- **Delegation**: holders can delegate voting power to active participants without transferring tokens (ERC20Votes)
- **Whale concentration**: top 10 addresses in many DAOs control >50% of votes
- **Governance Extractable Value (GEV)**: large holders can profit by passing self-serving proposals
- **Voter apathy**: typical participation rates are 5–15% of circulating supply

Typical Governance Token Distribution

Token distribution = governance power

Plutocracy Problem

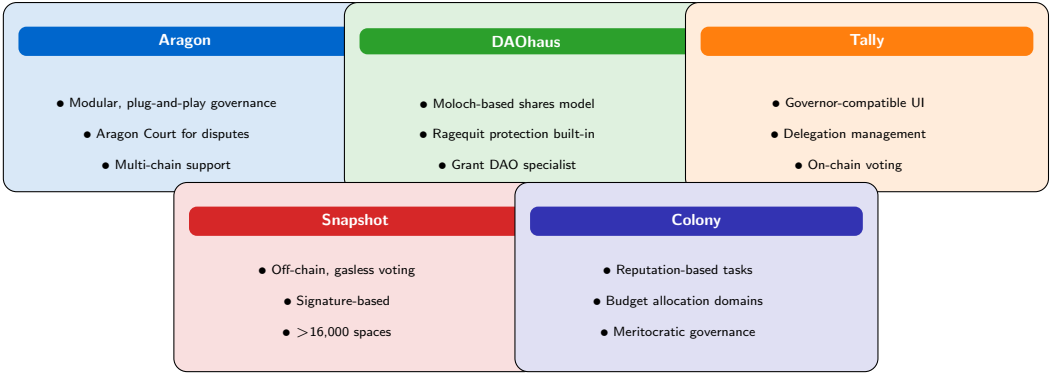
1 token = 1 vote ⇒ wealthiest wallets dominate. Quadratic voting and conviction voting (Section 2) address this.

distribution

Unisv

top 10 delegates control ˜70% of votes; voter participation peaked at ˜40M UNI in early proposals

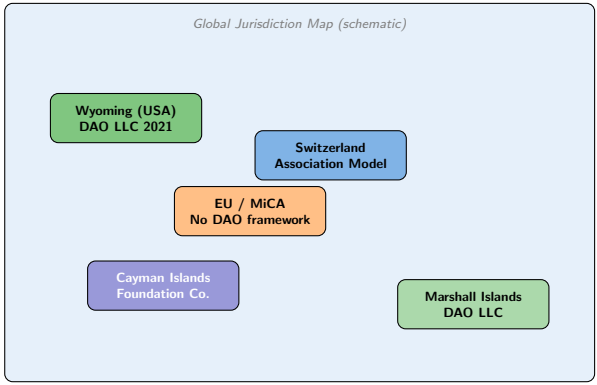
DAO Creation Frameworks



Snaps

+ Tally is the most common hybrid: gasless signalling on Snapshot, binding execution via on-chain Governor

Legal Status of DAOs



Legal Wrapper Concept

DAO + Legal Entity =

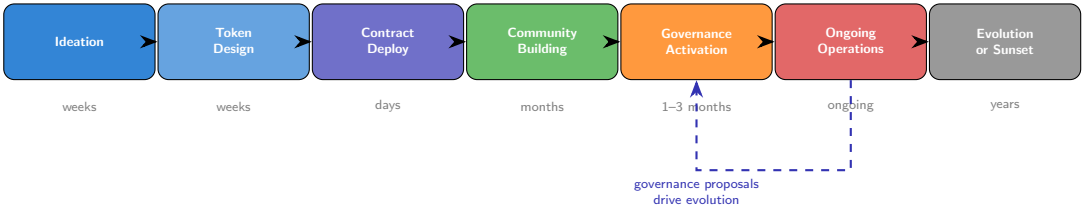
- Limited liability for members
- Ability to sign contracts
- Bank accounts and payroll
- Regulatory compliance
- IP ownership

Unresolved Issues

- Who is liable when a DAO is hacked?
- Are token holders employees or partners?
- Tax treatment varies by jurisdiction
- Securities law: is a governance token a security?

Legal wrapping is essential for DAOs interacting with the traditional world – contracts, bank accounts, and liability protection

DAO Lifecycle



Launch Risks

- Unaudited contracts
- Uneven token distribution
- Premature decentralization

Growth Challenges

- Voter apathy
- Contributor retention
- Treasury runway

Exit Scenarios

- Protocol ossification
- Acquisition by another DAO
- Graceful wind-down

Most DAOs fail within 2 years due to voter apathy and treasury mismanagement – lifecycle planning is critical

Section 1 Summary: DAO Fundamentals

1. DAOs are organizations governed by smart contracts and token-holder consensus – code replaces trust

2. Three membership models: token-based (liquid), share-based (ragequit), reputation-based (earned)

3. Governor contracts (OpenZeppelin) are the on-chain governance standard with timelocks and quorum

4. Framework tools (Aragon, Tally, Snapshot, DAOhaus) simplify DAO creation and operation

5. Legal wrappers (Wyoming LLC, Swiss Association, Cayman Foundation) bridge DAOs to traditional law

Next: Section 2 – Voting Mechanisms & Token Governance

Secti

1 complete — Key insight: DAOs encode organizational rules as immutable (or upgradeable) smart contracts

Section 2: Voting Mechanisms & Token Governance

How decentralized decisions get made – from simple voting to advanced mechanisms

What You Will Learn

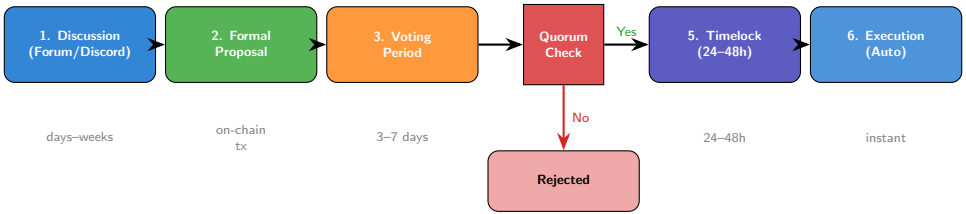
- On-chain vs off-chain voting tradeoffs
- Token-weighted voting and its plutocracy problem
- Advanced mechanisms: quadratic, conviction, holographic consensus
- Delegation, timelocks, and proposal lifecycle

Frames in This Section

Secti

2 of 5 — Frames 15–26

Proposal Lifecycle



Stage Details

- **Discussion**: Governance forums (Discourse, Commonwealth), temperature checks
- **Proposal**: Proposer must hold minimum tokens (e.g., 1M UNI to propose on Uniswap)

Voting Details

- For/Against/Abstain votes accumulated over block range
- Snapshot of voting power taken at proposal block
- Prevents last-minute token purchases for votes

Execution

- TimelockController queues transactions
- Anyone can trigger execution after delay
- On-chain atomicity: all-or-nothing

The full lifecycle from idea to on-chain execution typically takes 2–4 weeks – deliberate slowness is a security feature

On-Chain vs Off-Chain Voting

	On-Chain Voting	Off-Chain (Snapshot)	Hybrid Approach
Binding?	Yes – auto-executes	No – signalling only	Yes – executed on-chain
Cost	$5–$100 gas/vote	Free (gasless)	Gas only at execution
Trust Model	Trustless	Trust Snapshot & multisig	Vote off-chain
Speed	Slow (blocks)	Fast	Fast vote, safe exec
Tamper-proof?	Yes	Signature-based	Yes (on execution)
Used For	Critical changes	Signalling, sentiment	Best of both worlds
Examples	Compound, Uniswap	Most DAOs use Snapshot	Optimistic Governance

Most large DAOs use off-chain Snapshot for signalling and on-chain Governor for binding execution

Gas cost is the primary barrier to on-chain participation – a single governance vote on Ethereum mainnet costs $20–$150 in gas

Listing 2: Simplified Governor Contract

```
// Simplified Governor Contract
contract DAOGovernor {
    uint256 public proposalCount;
    uint256 public quorumVotes;
    uint256 public votingPeriod;

    struct Proposal {
        address proposer;
        uint256 forVotes;
        uint256 againstVotes;
        uint256 endBlock;
        bool executed;
    }

    mapping(uint256 => Proposal)
        public proposals;

    function propose(
        string memory description
    ) external returns (uint256) {
        proposalCount++;
        proposals[proposalCount] =
            Proposal(msg.sender,
                0, 0,
                block.number + votingPeriod,
                false);
        return proposalCount;
    }
}
```

Governor Architecture

- **Proposal struct** stores proposer, vote tallies, deadline block, and execution status
- **proposalCount** acts as auto-incrementing ID and prevents hash collisions
- **votingPeriod** is measured in blocks (≈12s on mainnet), typically 40,320 blocks = 7 days
- **quorumVotes** sets minimum participation threshold to prevent low-turnout attacks

Production Standard

OpenZeppelin Governor (OZ) extends this pattern with:

- ERC20Votes checkpointing for snapshot-based voting power
- Timelock controller for delayed execution
- Modular extensions (Bravo-compatible, fractional voting)

Open

Governor is used by Compound, Uniswap, and most major DAOs – always audit before deployment

Simple Token Voting

Mechanics

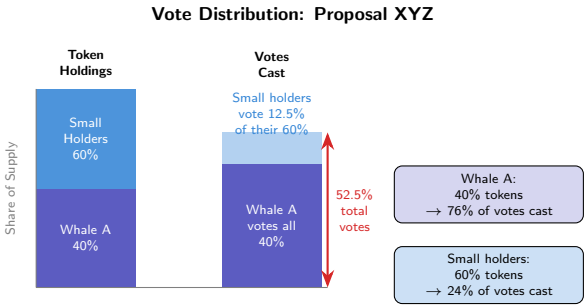
- **1 token = 1 vote** – voting power proportional to holdings
- **Majority wins**: For votes > Against votes (simple) or >50% of total (absolute)
- **Quorum threshold**: minimum participation required (e.g., 4% of supply)
- **Participation**: typically 5–15% of circulating supply votes

The Plutocracy Problem

- Wealth ≡ governance power
- Top 10 wallets in Uniswap control ˜70% of votes
- Whale can single-handedly pass proposals
- Retail holders face high gas costs with negligible voting impact

Voter Apathy

Typical DAO turnout: <10% of eligible tokens. Compound governance: many proposals pass with <2% participation.



token voting is simple to implement but systematically amplifies whale power relative to their token share due to voter apathy

Quadratic Voting

Formula & Mechanics

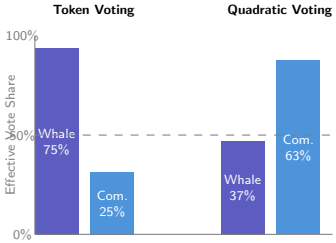
Cost to cast n votes:

$$\text{Cost} = n^2 \text{ credits} \iff n = \sqrt{\text{credits}}$$

Votes (n)	Credits Used	Marginal Cost
1	1	1
2	4	3
3	9	5
5	25	7
10	100	15

Each additional vote costs more – expensive to dominate.

Token Voting vs Quadratic Voting



Token Voting:
Whale wins
(75% control)

Quadratic:
Community wins
(63% influence)

Scenario: 1 whale (1000 tokens) vs 100 community members (10 tokens each)

Sybil Vulnerability

Splitting tokens across many wallets cheaply obtains more quadratic votes. Requires robust identity or anti-Sybil mechanism (e.g., Gitcoin Passport, Proof of Humanity).

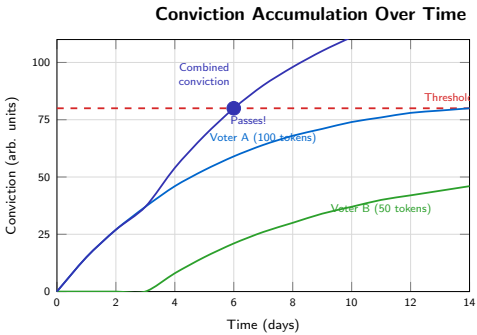
Quad

voting used in Gitcoin Grants ($50M+ distributed); radical markets theory shows it achieves Pareto-efficient collective decisions

Conviction Voting

Core Concept

- Conviction **accumulates** the longer tokens are staked on a proposal
- No fixed voting deadline – proposals pass when accumulated conviction crosses a threshold
- Removing stake resets conviction quickly
- Rewards **sustained commitment** over last-minute voting



Advantages

- **Attack resistance**: attacker must sustain large stake for extended period
- **Continuous governance**: proposals always open, no discrete voting windows
- **Signal clarity**: conviction reflects genuine long-term preference
- **Voter apathy mitigation**: passive staking counts as implicit approval

Used By

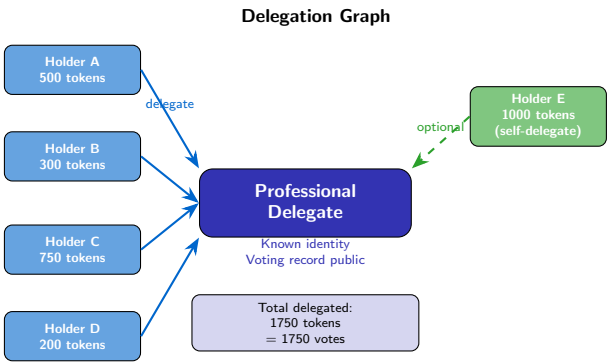
Vote Delegation

Why Delegate?

- **Gas costs**: voting on-chain costs $20–$100; delegation is one-time
- **Expertise**: delegates specialize in protocol governance
- **Time**: retail holders lack time to analyse proposals
- **Participation**: delegation improves effective participation rates

Liquid Democracy

- Delegation can be changed or revoked at any time
- Transitive delegation: A delegates to B who delegates to C
- Override: delegator can still vote directly if they choose
- Delegation platforms: Tally, Agora, Karma

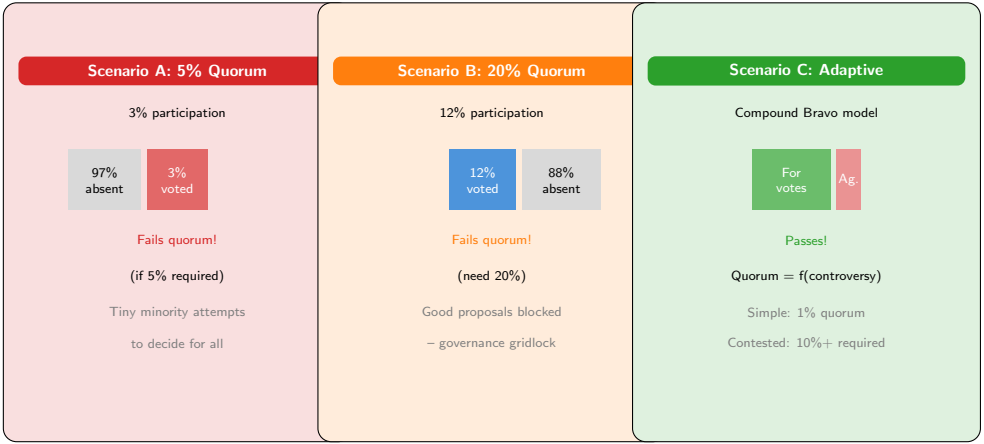


Delegation Risks

Delegates can become new whales. Inactive delegates drain participation. Misaligned delegates may vote against holders' interests.

has ˜3000 active delegates; top 10 control majority – delegation solves participation but can recreate plutocracy

Quorum and Thresholds



Real thresholds: Uniswap 4% (˜40M UNI) Compound 1% Aave 2% Maker 3%

Quor

design is critical: too low enables minority capture, too high creates gridlock – adaptive quorum is the emerging best practice

Holographic Consensus

The Scalability Problem

- Every proposal needs **full quorum** – impractical at scale
- Large DAOs may have hundreds of active proposals
- Voter fatigue: members cannot evaluate all proposals
- Low-quality proposals waste voter attention

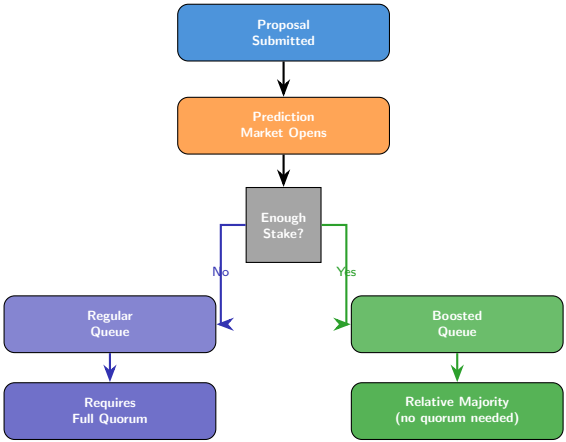
Holographic Solution (DAOstack)

- **Prediction market** layer: GEN token stakers bet on proposal outcomes
- **Boosted proposals**: sufficient stake $\Rightarrow$ proposal enters boosted queue
- **Relaxed threshold**: boosted proposals pass with simple relative majority (no quorum)
- **Incentive alignment**: correct stakers earn rewards; incorrect lose stake

Key Property

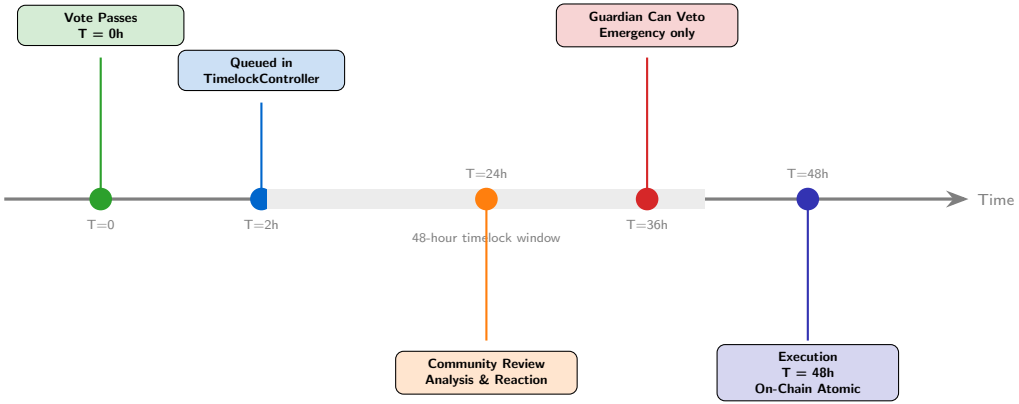
A small, informed minority can surface important proposals to the full

Holographic Consensus Flow



Correct sta
earn GEN re

Timelocks and Execution



Why Timelocks Matter

- Time to detect and react to malicious proposals
- Allows users to exit protocol before harmful changes apply
- Emergency guardian veto as last resort (multisig)

OZ TimelockController

- Standard: 24h or 48h delay
- Cancellation: Proposer can cancel queued tx
- Grace period: tx expires if not executed within 14 days

Real Incidents

- Beanstalk (2022): No timelock $\Rightarrow$ **$**182M flash-loan governance attack in one block
- Compound: 2-day timelock saved treasury from a misconfigured proposal

Section 2 Summary: Voting Mechanisms & Token Governance

1. Proposal lifecycle: discussion → formal proposal → vote → quorum check → timelock → execution

2. On-chain voting is binding but costly; off-chain (Snapshot) is free but requires trust for execution

3. Quadratic voting reduces plutocracy (cost = n^2); conviction voting rewards sustained long-term support

4. Delegation enables participation without active voting – liquid democracy; delegates can become new power centres

5. Timelocks provide critical safety buffer between vote passage and execution – Beanstalk proved their necessity

Next: Section 3 – Treasury Management & Token Economics

Secti

2 complete — Key insight: voting mechanism design determines whether a DAO is democratic or plutocratic in practice

Section 3: Treasury Management & Economics

How DAOs manage billions in assets and design sustainable token economies

In this section you will learn:

- Multi-sig treasury architecture (Gnosis Safe)
- Treasury diversification and risk management
- Grant programs and budget allocation
- Token economics: inflation, buybacks, and sustainability

Secti

3 of 5 — Treasury & Token Economics – the financial engine of decentralised governance

DAO Treasury Overview

What is a DAO Treasury?

A DAO treasury is a collectively owned pool of digital assets controlled exclusively by on-chain governance.

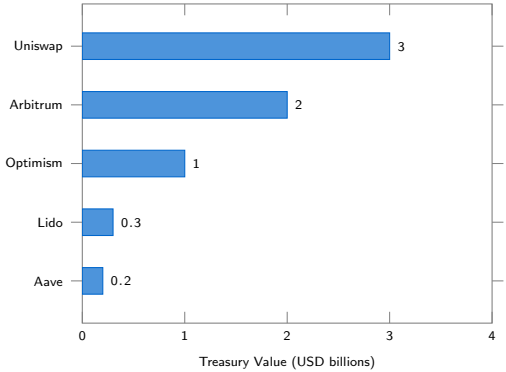
Core Functions

- Fund protocol development
- Incentivise liquidity and contributors
- Cover operational expenses
- Build protocol-owned liquidity

Key Risk

Most treasuries hold 60–90% of their value in their *own* governance token.
A 90% token price drop ⇒ 90% treasury drop.

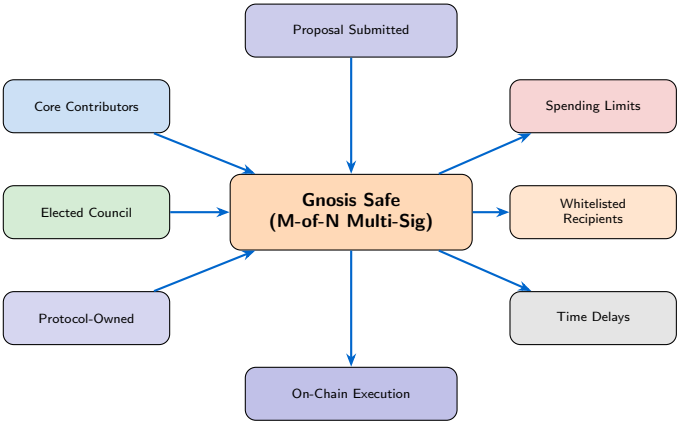
Top DAO Treasuries (approximate, 2024):



Sourc

DeepDAO, Messari (2024) – values fluctuate significantly with token prices; concentration risk is a systemic concern

Multi-Sig Treasury Architecture



Common Configurations:

- **3-of-5**: Small DAOs, fast decisions
- **5-of-9**: Large protocols, higher security
- **7-of-12**: Flagship treasuries

Guard Modules

- Spending caps per address/period
- Recipient whitelists prevent draining
- Time delays allow community veto

Transaction Flow

Proposal → Multi-sig approval → Guard checks → Execution

Gnosi

Safe manages over $50B in digital assets across the ecosystem – the de-facto standard for DAO treasury management

Governor Contract Architecture

Listing 3: Simplified Governor Contract

```
// Simplified Governor Contract
contract DAOGovernor {
    uint256 public proposalCount;
    uint256 public quorumVotes;
    uint256 public votingPeriod;

    struct Proposal {
        address proposer;
        uint256 forVotes;
        uint256 againstVotes;
        uint256 endBlock;
        bool executed;
    }

    mapping(uint256 => Proposal)
        public proposals;

    function propose(
        string memory description
    ) external returns (uint256) {
        proposalCount++;
        proposals[proposalCount] =
            Proposal(msg.sender,
                0, 0,
                block.number + votingPeriod,
                false);
        return proposalCount;
    }
}
```

Governor Architecture

- **Proposal struct** stores proposer, vote tallies, deadline block, and execution status
- **proposalCount** acts as auto-incrementing ID and prevents hash collisions
- **votingPeriod** is measured in blocks (≈12s on mainnet), typically 40,320 blocks = 7 days
- **quorumVotes** sets minimum participation threshold to prevent low-turnout attacks

Production Standard

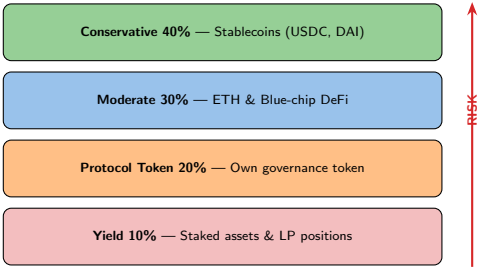
OpenZeppelin Governor (OZ) extends this pattern with:

- ERC20Votes checkpointing for snapshot-based voting power
- Timelock controller for delayed execution
- Modular extensions (Bravo-compatible, fractional voting)

Governor is used by Compound, Uniswap, and most major DAOs – always audit before deployment

Treasury Diversification

Risk-Tiered Portfolio Allocation:



Why Each Tier?

- **Stablecoins**: 12–18 months of runway regardless of market conditions; pay contributors and service providers
- **ETH / Blue-chip**: Store of value with growth potential; widely accepted collateral
- **Protocol token**: Retain alignment; required for incentive programs
- **Yield positions**: Generate passive income to extend runway without selling

Concentration Risk

If the protocol token drops 90%, a 60%-concentrated treasury loses $540M on a $1B treasury. Diversification is existential.

Rebalancing Triggers

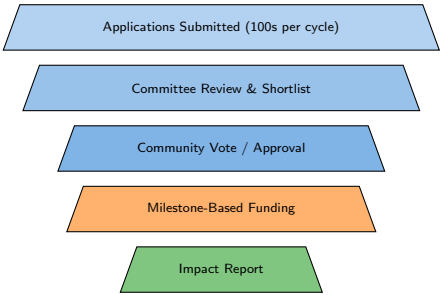
Quarterly review, or immediately if any tier moves ±15pp from target.

Make

"Endgame" plan shifted $500M+ from MKR to stablecoins and real-world assets to reduce concentration risk

Grant Programs

Funnel: Applications to Impact



Real-World Examples:

- **Uniswap Grants**: $75M allocated; development, research, and community building
- **Aave Grants**: Quarterly cohorts; focus on integrations and tooling
- **Optimism RetroPGF**: Retroactive rewards for *past* public goods contributions

Grant Categories

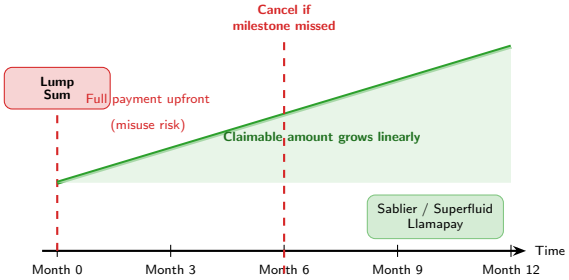
Development	Protocol features, integrations
Research	Security, economics, governance
Community	Education, events, translation
Marketing	Awareness, partnerships

Miles

based disbursement reduces risk of grant misuse – funds released only upon verified delivery of agreed outputs

Streaming Payments

Traditional vs. Streaming Payment:



Why Streaming?

- **Reduced trust**: Recipient earns per second of work delivered
- **Automatic payroll**: No monthly proposal needed; contributors claim anytime
- **Revocable**: DAO can cancel the stream if deliverables are not met
- **Composable**: Streams can be used as collateral in DeFi

Leading Protocols

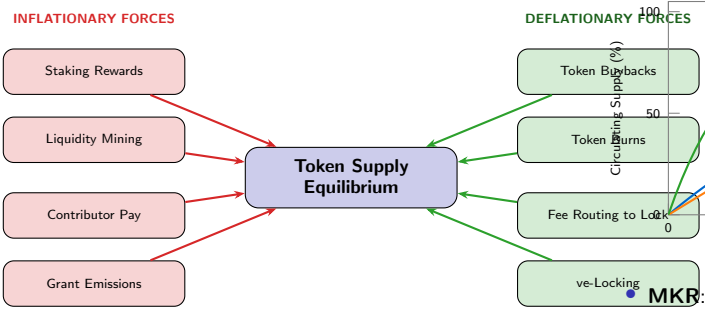
- **Sablier**: Fixed-term streams
- **Superfluid**: Real-time streams with DeFi composability
- **Llamapay**: Simple, gas-efficient payroll

Strea

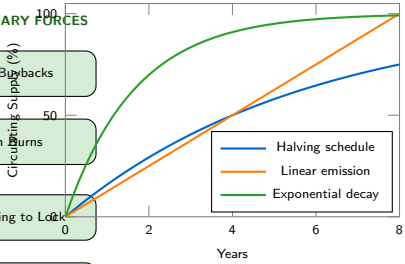
replaces the "pay and pray" model – every second of non-delivery means zero incremental cost to the DAO treasury

Token Economics: Supply Side

Supply Dynamics:



Emission Schedules Over Time:

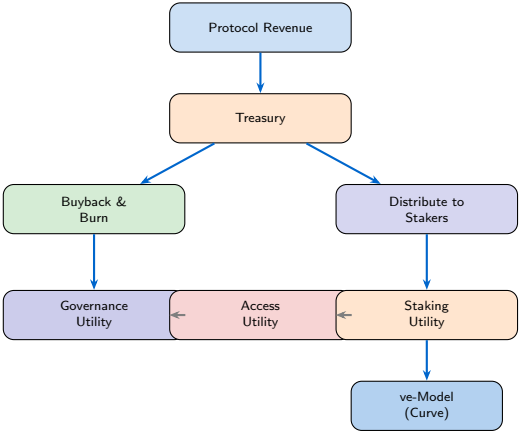


- **MKR**: Burned from stability fees (deflationary)
- **UNI**: 2% perpetual inflation after year 4
- **CRV**: Decaying emission schedule over 6 years

Sustainable tokenomics require inflationary emissions to be offset by real protocol revenue – "print and hope" fails long-term

Token Economics: Demand Side

Value Accrual Flowchart:



Utility Dimensions:

- **Governance**: Voting rights, proposal power, veto capability
- **Access**: Fee discounts, premium features, whitelist access
- **Staking**: Security bonds, yield, ve-locking multiplier

The ve-Model (Curve Finance)

Lock tokens for 1–4 years to receive **veCRV**:

- More voting power for gauge weights
- Boosted liquidity rewards (up to 2.5×)
- Share of protocol fees (3CRV)

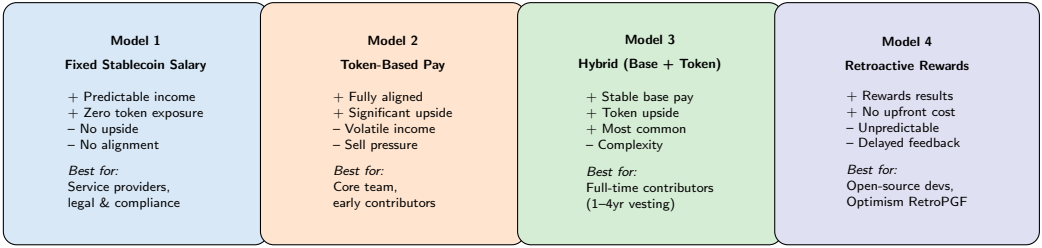
Creates **long-term alignment**: only committed holders influence the protocol.

Toker

value ultimately depends on the protocol's ability to generate sustainable revenue and direct it to token holders

Compensation Models

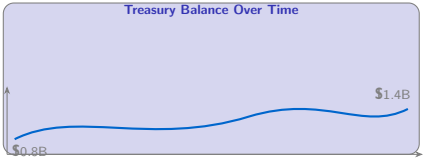
Four Approaches to DAO Contributor Compensation:

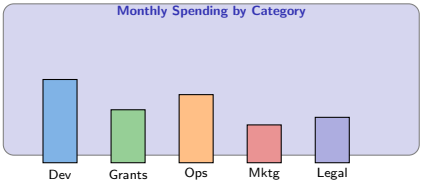


Most mature DAOs use Model 3 with 4-year vesting and 1-year cliff – mirroring traditional startup equity compensation structures

Financial Reporting & Transparency

On-Chain Dashboard Mockup:





The Transparency Advantage:

- Every transaction is on-chain and publicly auditable – no hidden spending
- Real-time balance visible to all token holders globally
- Automated reporting via Dune Analytics dashboards

Reporting Tools

- **DeBank**: Portfolio tracking across chains
- **Zerion**: Multi-wallet treasury view
- **Dune Analytics**: Custom SQL dashboards
- **Karma**: Contributor accountability

Best Practice

Monthly treasurer reports with on-chain proof; quarterly audits by independent firms.

Unisv

Aave and Compound all publish monthly treasury reports – setting the standard for DAO financial transparency.

Section 3 Summary: Treasury Management & Economics

1. DAO treasuries hold billions but face concentration risk – most value is in the protocol's own governance token

2. Multi-sig wallets (Gnosis Safe) provide secure, multi-party treasury management with guard modules and spending limits

3. Grant programs and streaming payments enable accountable, milestone-driven resource allocation without upfront trust

4. Token economics must balance inflationary incentives (staking, liquidity mining) with deflationary sustainability (burns, buybacks)

5. On-chain transparency is a unique advantage – every transaction is publicly auditable, enabling trustless financial reporting

Next: Section 4 – Security, Attacks & Governance Failures

Secti

3 complete — Key insight: treasury diversification and on-chain transparency are the foundations of long-term DAO sustainability

Section 4: Governance Attacks & Security

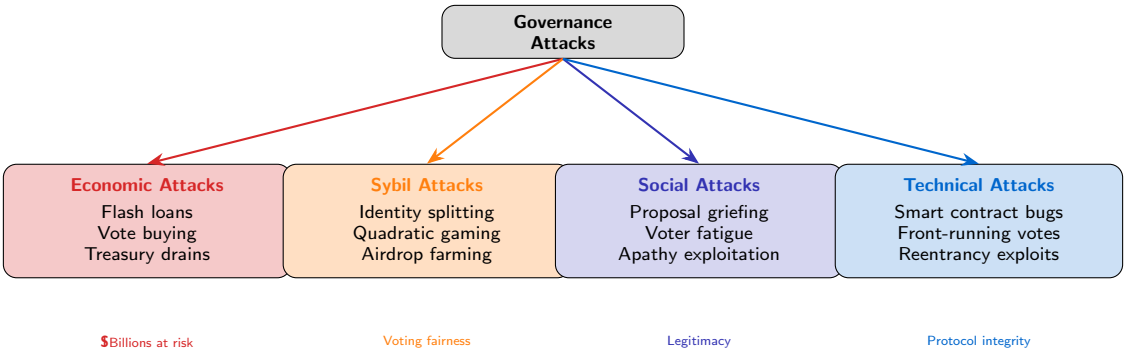
Understanding and defending against threats to decentralized governance

What You Will Learn

- Flash loan governance attacks and prevention
- Vote buying, bribery, and dark markets
- Sybil attacks on governance systems
- Defensive mechanisms: timelocks, guardians, veto power

4 of 5 — Governance security is not optional — billions of dollars depend on getting it right

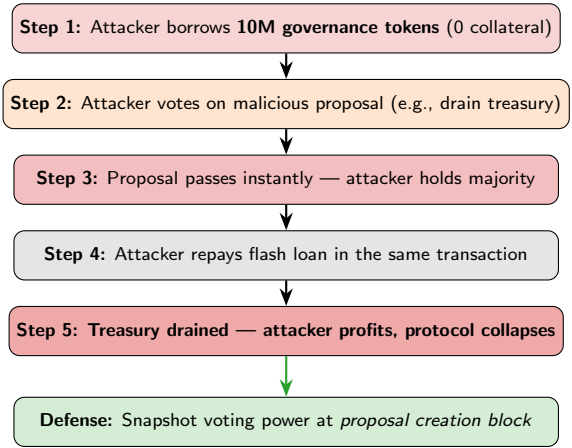
Governance Attack Taxonomy



Attac

surface grows with protocol value — No single defense covers all attack types — layered security is mandatory

Flash Loan Governance Attacks



Real Example

Beanstalk Farms
April 2022

- Attacker borrowed $1B in flash loan
- Passed emergency BIP-18 proposal
- Drained $182M from protocol
- All in a **single transaction**

Key Insight

Flash loans make anyone temporarily the largest token holder — voting power must be measured *before* the loan is taken.

Flash loan attacks exploit the atomic nature of blockchain transactions — Prevention: ERC20Votes with block-number checkpoints

Listing 4: Simplified Governor Contract

```
// Simplified Governor Contract
contract DAOGovernor {
    uint256 public proposalCount;
    uint256 public quorumVotes;
    uint256 public votingPeriod;

    struct Proposal {
        address proposer;
        uint256 forVotes;
        uint256 againstVotes;
        uint256 endBlock;
        bool executed;
    }

    mapping(uint256 => Proposal)
        public proposals;

    function propose(
        string memory description
    ) external returns (uint256) {
        proposalCount++;
        proposals[proposalCount] =
            Proposal(msg.sender,
                0, 0,
                block.number + votingPeriod,
                false);
        return proposalCount;
    }
}
```

Governor Architecture

- **Proposal struct** stores proposer, vote tallies, deadline block, and execution status
- **proposalCount** acts as auto-incrementing ID and prevents hash collisions
- **votingPeriod** is measured in blocks (≈12s on mainnet), typically 40,320 blocks = 7 days
- **quorumVotes** sets minimum participation threshold to prevent low-turnout attacks

Production Standard

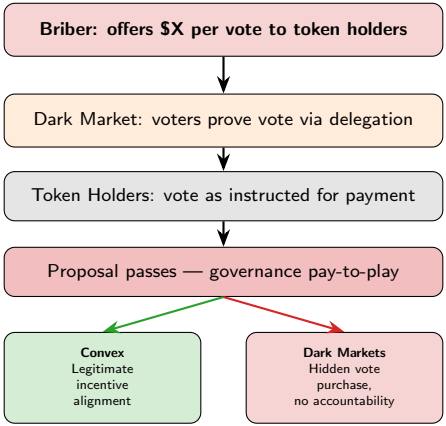
OpenZeppelin Governor (OZ) extends this pattern with:

- ERC20Votes checkpointing for snapshot-based voting power
- Timelock controller for delayed execution
- Modular extensions (Bravo-compatible, fractional voting)

Open

Governor is used by Compound, Uniswap, and most major DAOs – always audit before deployment

Vote Buying & Bribery



The "Governance is a Market" Thesis

Governance votes have financial value. If a protocol controls $1B in assets, voting rights are worth significant money — creating natural bribery incentives.

Defenses

- **Vote Privacy (MACI)**: Minimum Anti-Collusion Infrastructure — voters can change votes privately, making bribes unverifiable
- **Shielded Voting**: votes hidden until voting period closes
- **Commit-Reveal**: two-phase voting to prevent last-minute coordination

Vote buying is rational if the governance asset is worth more than the bribe cost — MACI offers cryptographic bribery resistance

Sybil Attacks on Governance

Voting Type	1 Person, 1 Wallet	1 Person, 100 Wallets
Token Voting	100 tokens = 100 votes	1 token each = 100 votes
Quadratic Voting	$\sqrt{100}$ = 10 votes	$100 \times \sqrt{1}$ = 100 votes
Airdrop Governance	1 claim	100 claims

Sybil Resistance Methods: Gitcoin Passport (Web2 verification) · Worldcoin / Proof-of-Per
Social graph analysis · Minimum token holding period · KYC (sacrifices privacy)

The Core Tradeoff

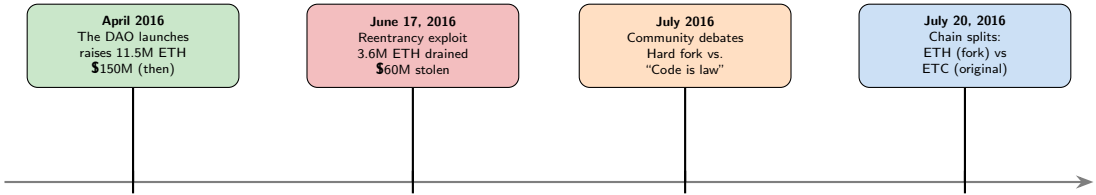
Sybil resistance requires identifying unique humans — which conflicts with the **pseudonymity** that blockchain users value.

No Perfect Solution

- KYC: effective but centralizing
- Proof-of-personhood: promising but experimental (Worldcoin controversy)
- Social graphs: gameable over time
- Holding periods: reduce but don't eliminate Sybil advantage

Sybil attacks are especially dangerous for quadratic voting systems — Privacy vs. Sybil-resistance remains an open research problem

The DAO Hack (2016): A Watershed Moment

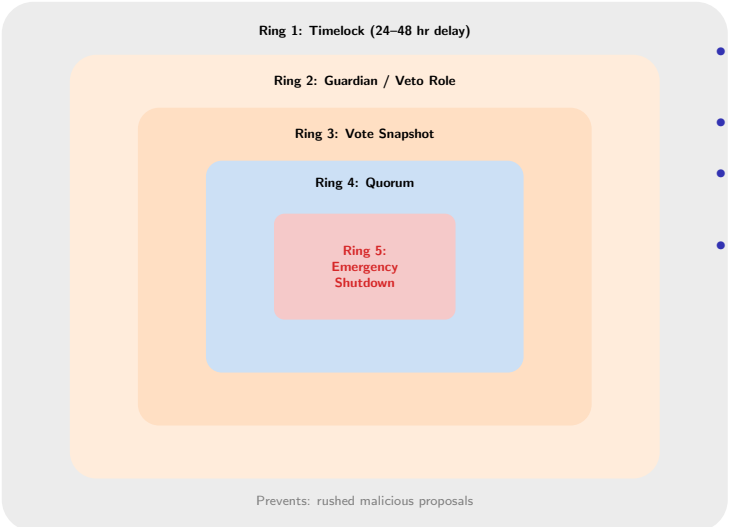


Vulnerability: Reentrancy — `withdraw()` sent ETH *before* updating balance ⇒ attacker called `withdraw()` recursively in fallback function

Legacy: Sparked "Code is law" debate · Led to mandatory security audits · Created Ethereum Classic (ETC) · Shaped DAO legal thinking

The DAO hack was the first major test of blockchain governance under crisis — The fork proved that human consensus can override "immutable" code

Defensive Mechanisms: Defense-in-Depth



- **Ring 1 — Timelock:** 24–48 hour delay between vote passing and execution; users can exit before harmful change takes effect
- **Ring 2 — Guardian:** Multisig committee can cancel proposals during timelock; sacrifices some decentralization for safety
- **Ring 3 — Snapshot:** Voting power measured at proposal creation block; defeats flash loan attacks
- **Ring 4 — Quorum:** Minimum participation required; prevents minority capture with abstaining majority
- **Ring 5 — Emergency Shutdown:** Circuit breaker pauses protocol; last resort against active exploits

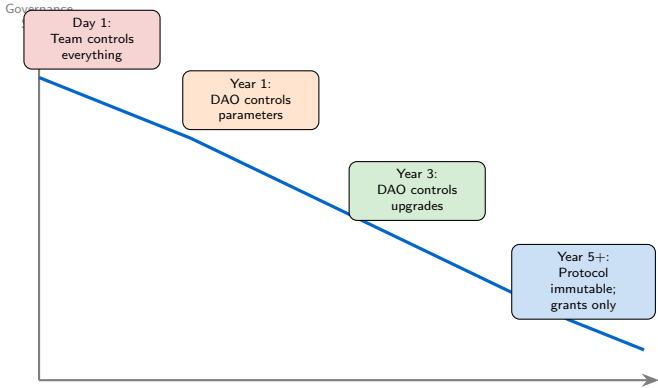
No

Governance Minimization

Philosophy

Reduce the attack surface by reducing what governance can control. The safest governance decision is one that **does not need to be made**.

- **Immutable code** cannot be governance-attacked
- **Progressive decentralization**: gradually hand control to the DAO as trust is established
- **Uniswap v3**: minimal governance — only fee switch and grant programs
- **MakerDAO**: extensive governance — hundreds of decisions per year, higher risk surface



The safest governance decision is one that doesn't need to be made — immutable code can't be attacked via governance

Section 4 Summary: Governance Security

1. Flash loan attacks exploit instant token borrowing for vote manipulation — **snapshot voting** (at proposal block) is the primary defense

2. Vote buying and bribery create pay-to-play governance — **vote privacy (MACI)** is an emerging cryptographic solution

3. Sybil attacks undermine quadratic and identity-based voting — **proof-of-personhood** is an active open problem

4. The 2016 DAO hack ($60M) was a watershed moment — it split Ethereum and catalyzed professional security auditing

5. Defense-in-depth (timelocks, guardians, snapshots, emergency shutdown) is essential for robust governance security

Next: Section 5 — Real-World DAOs & Future of Governance

Secti

4 complete — Key insight: layered defenses and governance minimization are the two most powerful security strategies

Section 5: Real-World DAOs & Future of Governance

Case studies, participation challenges, and the road ahead

What You Will Learn

- MakerDAO, Uniswap, and Aave governance case studies
- Governance participation rates and voter apathy
- Legal frameworks for DAOs by jurisdiction
- The future of decentralized governance

5 of 5 — Real-world DAOs prove both the promise and the hard problems of decentralized governance

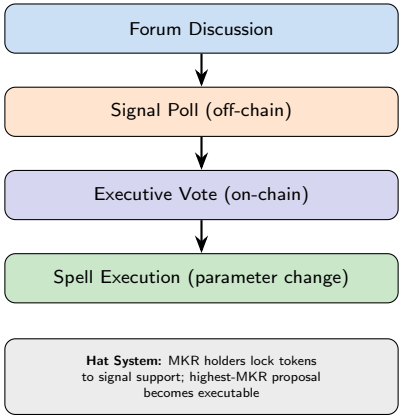
MakerDAO Governance

Structure

- **MKR token** holders govern the **DAI** stablecoin system
- Key parameters: stability fees, collateral ratios, DSR (DAI Savings Rate)
- **Hat system**: continuous approval voting — proposal with most MKR locked becomes the "hat" and is executable
- Hundreds of governance decisions per year

Endgame Plan

SubDAOs, MetaDAOs, real-world asset integration — MakerDAO evolving toward modular governance with specialized sub-units each managing a vertical.



governs the $5B+ DAI ecosystem — Complexity concern: high governance overhead risks voter fatigue and plutocratic capture

Uniswap & Aave Governance

Uniswap Governance

- **Token:** UNI (1B total supply)
- **System:** Governor Bravo (OpenZeppelin)
- **Quorum:** 4% of supply (≈40M UNI)
- **Voting period:** 7 days
- **Timelock:** 2-day delay
- **Key debates:** Fee switch (protocol revenue), BSL license exceptions, deployment on new chains
- **Challenge:** Large holders dominate; retail rarely reaches proposal threshold (2.5M UNI to propose)

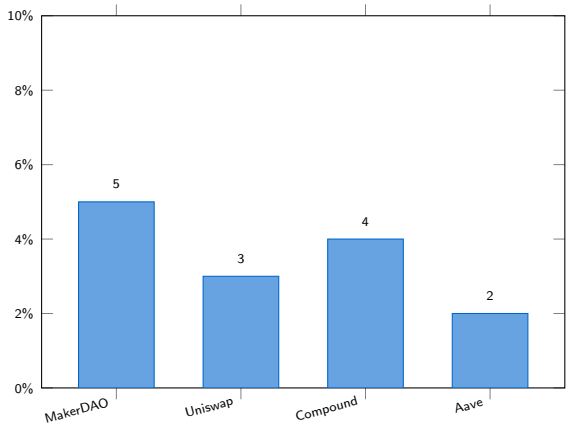
Aave Governance

- **Token:** AAVE + stkAAVE (staked)
- **System:** Governance v3 (cross-chain)
- **Safety Module:** stkAAVE holders backstop protocol losses
- **Risk DAO:** Specialized committee for risk parameter updates
- **Cross-chain:** Governance on Ethereum controls deployments on Polygon, Avalanche, Optimism
- **Key decisions:** New asset listings, interest rate models, protocol upgrades

Participation rates: Uniswap ≈3% of UNI · Aave ≈2% of AAVE · Both rely heavily on delegated voting from large holders

Both protocols show: good governance tooling exists, but participation remains the unsolved challenge

Governance Participation Crisis



Root Causes

- **Voter fatigue:** too many proposals, too little time
- **Gas costs:** voting on-chain costs $5–$50 per vote
- **Complexity:** proposals require deep protocol knowledge
- **Rational ignorance:** small token holders' votes rarely decisive

Solutions

- Delegation to active representatives
- Gasless voting (Snapshot off-chain)
- Governance mining (rewards for voting)
- Simplified proposal summaries

Avg. turnout below 5% means a motivated minority can dominate governance — Low participation is a systemic vulnerability, not just inconvenience

DAO Legal Frameworks

Jurisdiction	Structure	Key Feature
Wyoming, USA	DAO LLC (since 2021)	Smart contract as operating agreement; limited liability
Marshall Islands	DAO LLC (flexible)	More flexible than Wyoming; first sovereign DAO LLC law
Switzerland	Association / Foundation	Ethereum Foundation model; nonprofit, crypto-friendly
Singapore	Foundation Company	Common for DeFi protocols; MAS oversight
EU / MiCA	No DAO-specific law	Token regulation applies; DAO = general partnership risk
Cayman Islands	Foundation Company	Exempted limited partnership; widely used by DeFi funds

Key risk: Without a legal wrapper, a DAO may be a general partnership — Ooki DAO case (CFTC) held token voters liable as partners

The Future of DAO Governance

Governance Evolution

AI-assisted governance decision support

Automated parameter tuning (protocol AI)

Cross-chain voting with unified identity

2025–2027

Participation Innovation

Gasless voting everywhere

Governance rewards (mining 2.0)

Delegation marketplaces with track records

2025–2028

Legal Integration

Global DAO standards (ISO / IOSCO)

Regulatory clarity in G20 jurisdictions

DAO-to-DAO contracts legally enforceable

2026–2030

The future of governance is hybrid: human wisdom + algorithmic efficiency + legal legitimacy — No single solution wins alone

Key Takeaways and Course Summary

DAO Fundamentals: Smart contracts replace hierarchies; membership can be token-based, share-based, or reputation-based

Voting Mechanisms: From simple token voting to quadratic and conviction voting; delegation enables scalable participation

Treasury Management: Multi-sig wallets, diversification, and streaming payments enable accountable resource allocation

Security: Flash loan attacks, vote buying, and Sybil attacks are real threats; defense-in-depth is essential for protocol safety

Real-World DAOs: MakerDAO, Uniswap, and Aave demonstrate both the promise and the hard challenges of decentralized governance

Next: Advanced topics in decentralized identity, cross-chain governance, and DAO-to-DAO coordination

Cours

complete — DAOs are the organizational frontier of Web3 — participation, security, and legitimacy remain the defining open challenges