Democracy for DAOs: Decentralized Governance in Theory and Practice

Stefan Schmid
TU Berlin

Decentralization Is „En Vogue“!

Blockchain-based applications receive much attention, e.g.,

Web 3.0

Metaverse

Cryptocurrencies

But also

Decentralized Governance

⇢ ***Governance****: defines process how a society ***makes decisions***

⇢ In blockchain: enables participants in a ***blockchain project*** to ***vote on proposals*** for the future development

⇢ E.g. questions related to: forks, ***code changes***, addition or removal of nodes, etc.

But also

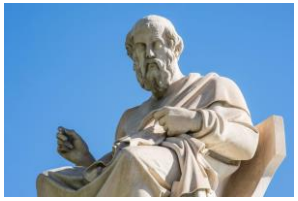
Decentralized Governance

⇢ ***Governance****: defines process how a society ***makes decisions***

⇢ In blockchain: enables participants in a ***blockchain project*** to ***vote on proposals*** for the future development

⇢ E.g. questions related to: forks, ***code changes***, addition or removal of nodes, etc.

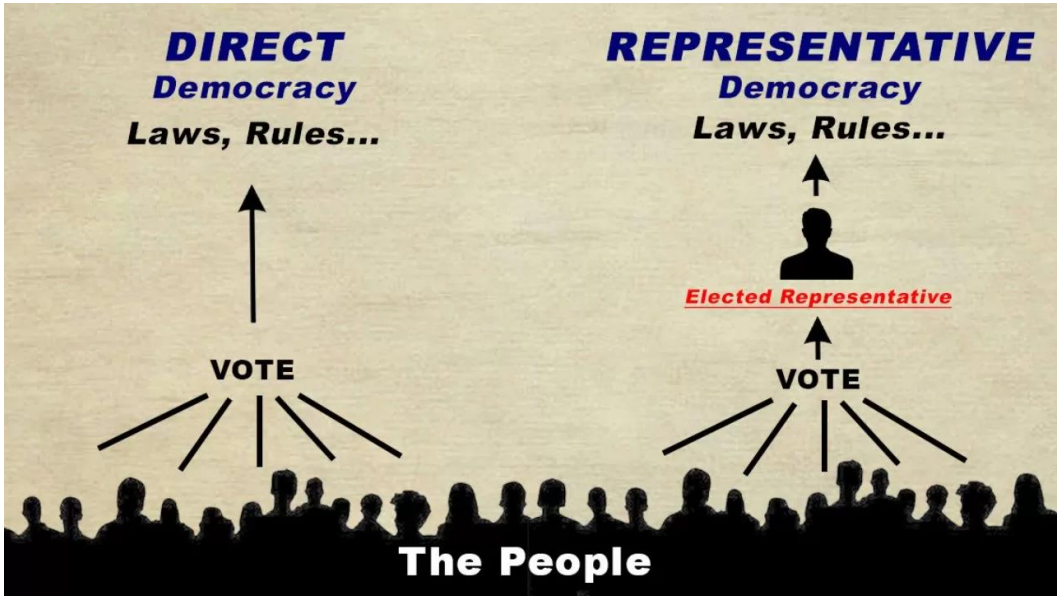
- From Greek kubernaein (“to steer”), first metaphorical use by Plato



kubernetes

Governance Models

⇢ Classic basic forms: ***direct voting*** vs ***representative democracy***



Pro and Cons

Direct Voting

good when relatively *few but important* issues to decide on

inefficient when many issues (*does not scale*) or for issues which *require expertise*

Representative Democracy

voting for *experts* in the domain allows voters to focus on other things

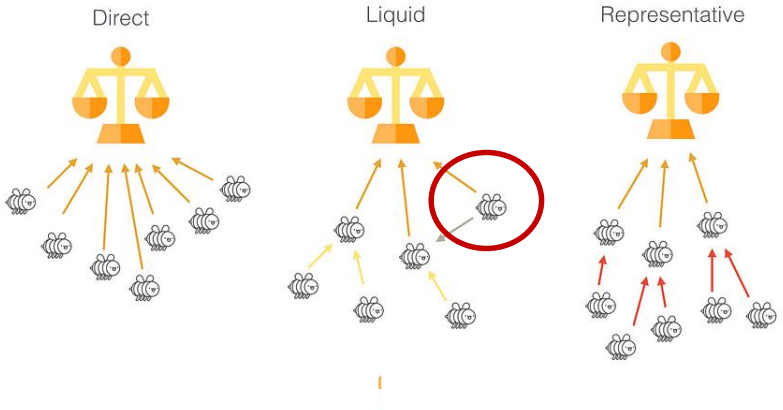
are *incentives* of representatives really aligned with voters?

Liquid Democracy

⇢ Instead of always voting directly or electing representatives: *"best of both worlds"* with a *hybrid and flexible* approach

⇢ Enables voters to *fluidly delegate their vote* or override their delegates position as they see fit

⇢ Sometimes can even delegate vote *to multiple people* based on the type of issue in question



Credits: Luke Duncan, Medium.com

Not a new concept!

⇢ In Carroll's book about ***Alice's Adventures in Wonderland*** candidates can transfer received votes to other candidates

⇢ But historically ***hard to implement***

⇢ Now possible: ***ubiquitous access to the Internet*** and modern cryptography enable functional liquid democracy

⇢ Real-world example: ***Germany's Pirate Party*** applied delegations for internal voting

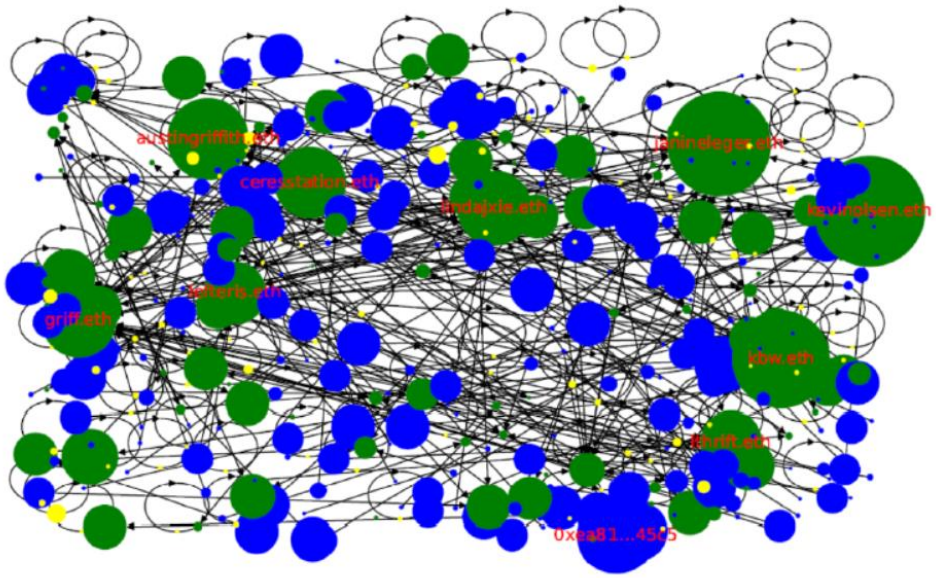
Realization in Blockchain

⇢ Can delegate my vote via ***token delegation***

⇢ For example in Internet Computer:
Neurons (=governance tokens)
can either vote themselves or
follow the decision of one…

⇢ … or ***even multiple other neurons***
(e.g., be represented by the
majority of the followed neurons)

Example: Gitcoin DAO



- Stewards in ***green***, delegators (who are not also stewards) in ***blue***
- Node ***size*** = amount of GTC it receives/delegates
- ***Top stewards*** such as kevinolsen.eth, griff.eth and others possess a large amount of ***voting power***
- Some nodes ***delegate*** significant amounts

Over 30 days: some highly

Active DAOs

Name	Proposals	Successful Proposals	Proposals in last 30 days	Successful Proposals in last 30 days
1 WaterNeuron	3391	3182	318	284
2 Network Nervous S...	13443	12607	311	281
3 BOOM DAO	675	604	165	135
4 OpenChat	1902	1733	64	55
5 Dragginz	374	312	58	57
6 CLever	1106	582	46	36
7 AladdinDAO	1161	137	45	0
8 Concentrator	601	280	34	0
9 ICPSwap	680	629	30	25
10 PokedBots	169	130	22	18

DefiLlama

Online Governance Raises Many

Interesting Questions

⇢ How can users be ***incentivized*** to vote?

⇢ What is the ***voting behavior*** of users today?

⇢ Does vote delegation lead to risk of ***power concentration***?

⇢ Is delegation compatible with ***privacy***: e.g. certain votes in German Parliament are private?

⇢ Fundamentally, when is ***liquid democracy "better"*** than other forms of democracy?

Remark: Voting Power

⇢ ***Voting power computation*** can be complicated: example ***ICP***

⇢ The total voting power of a neuron is the ***product*** of the `Neuron Stake', the ` Dissolve Delay Bonus' and the `Age Bonus'

⇢ ***Neuron Stake***: Amount of ICP utility tokens staked in neuron

⇢ ***Dissolve Delay Bonus***: Bonus if you commit to wait before you can unlock your original ICP utility token

⇢ ***Age Bonus***: Older neurons receive an age bonus

Practical Perspective

Empirical Study ICP

⇢ Data set: 14 SNS DAOs, 3000 proposals

⇢ Metrics: participation rates, voting power in favor/against, frequency of proposals

Name	Age months	Category	Treasury USD	Neurons
OpenChat	20	Chat	$ 26,453,292	29,497
ICLighthouse	7	DeFi	$ 41,721,648	7,108
ICPSwap	6	DeFi	$ 11,748,411	10,220
SONIC	12	DeFi	$ 7,236,326	5,132
Nuance	12	Publishing	$ 2,071,079	2,435
TRAX	10	Publishing	$ 6,509,400	4,433
Yral	16	Social Media	$ 7,540,204	16,452
Seers	13	Social Media	$ 5,371,027	2,315
Catalyze	14	Social Media	$ 5,027,497	4,250
BOOM	14	Gaming	$ 2,490,307	5,411
ICGhost	15	Meme Coin	$ 17	2,614
ICPanda	6	Meme Coin	$ 40,525	1,531
Kinic	16	AI	$ 9,025,317	4,918
ELNA	7	AI	$ 6,134,524	5,089

Proposal Types

- **Harmless proposals:** mainly “***Motion***” proposals, a means for community ***discussions*** (e.g., to get ***opinions***) and placing ***suggestions***

- **Critical proposals:** have a ***great impact*** on the ecosystem, e.g., control their ***treasury*** and transferring of funds, require ***complex*** calculations

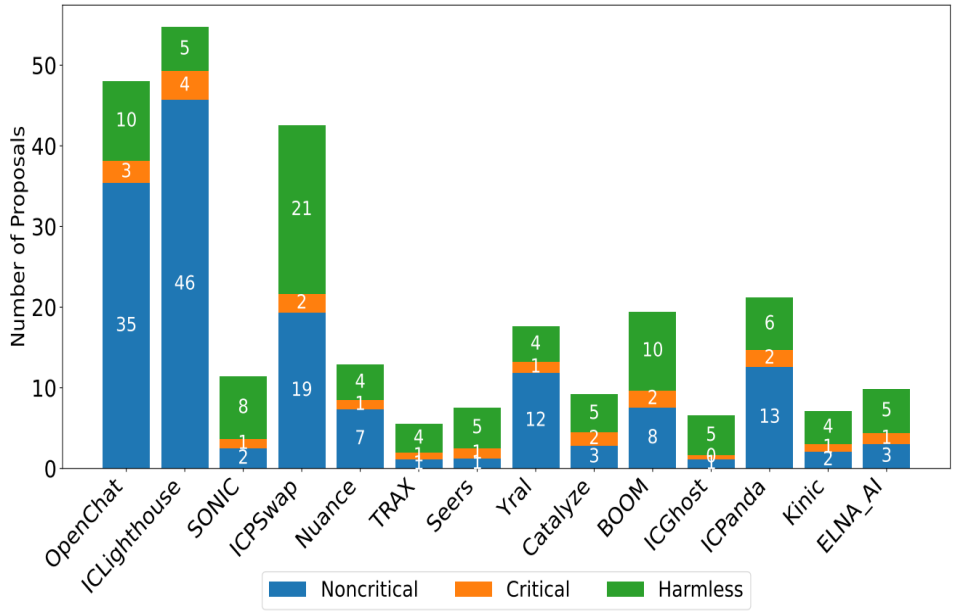
- **Non-critical proposals:** e.g., simpler ***feature*** extensions

Frequency of Proposals

⇢ Quite ***active*** but ***critical proposals*** are minority

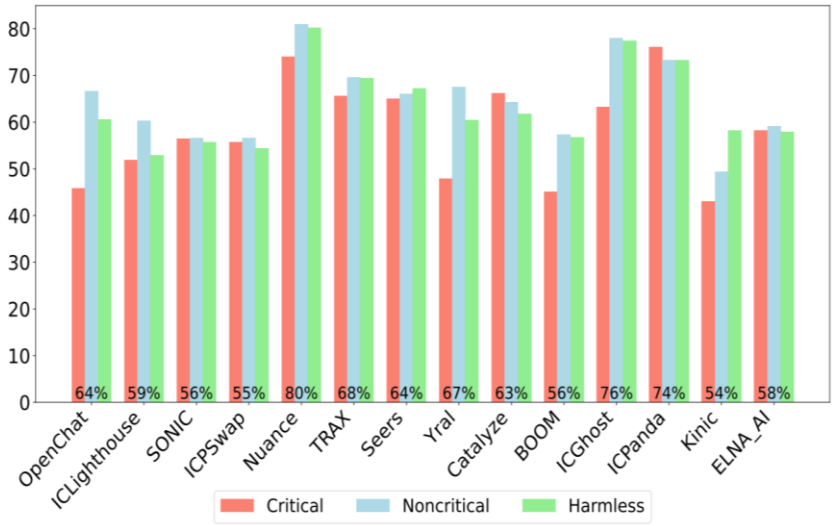
⇢ Only a ***small number of neurons*** actually proposes: submitting a proposal requires ***substantial effort***

⇢ Would be ***nice to have*** a larger set of proposers: more ***diverse opinions*** but too many could also ***hinder*** the governance engagement



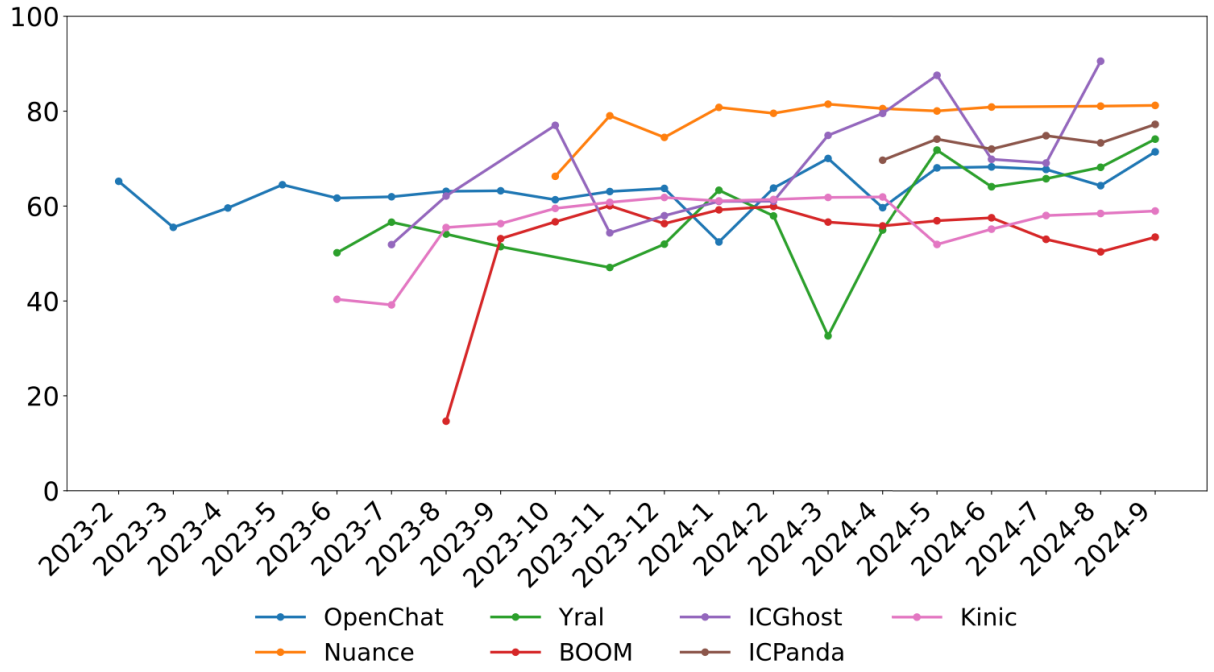
User Engagement

- ***Engagement***: % of voting power participating in proposal
- High on average: approximately 64%
- Higher for ***smaller DAOs*** (like Nuance), members feel a stronger ***responsibility***?
- ***Older*** DAOs like OpenChat shows moderate participation
- Interestingly, participation for ***critical proposals*** lower: require more effort from the neurons to follow?



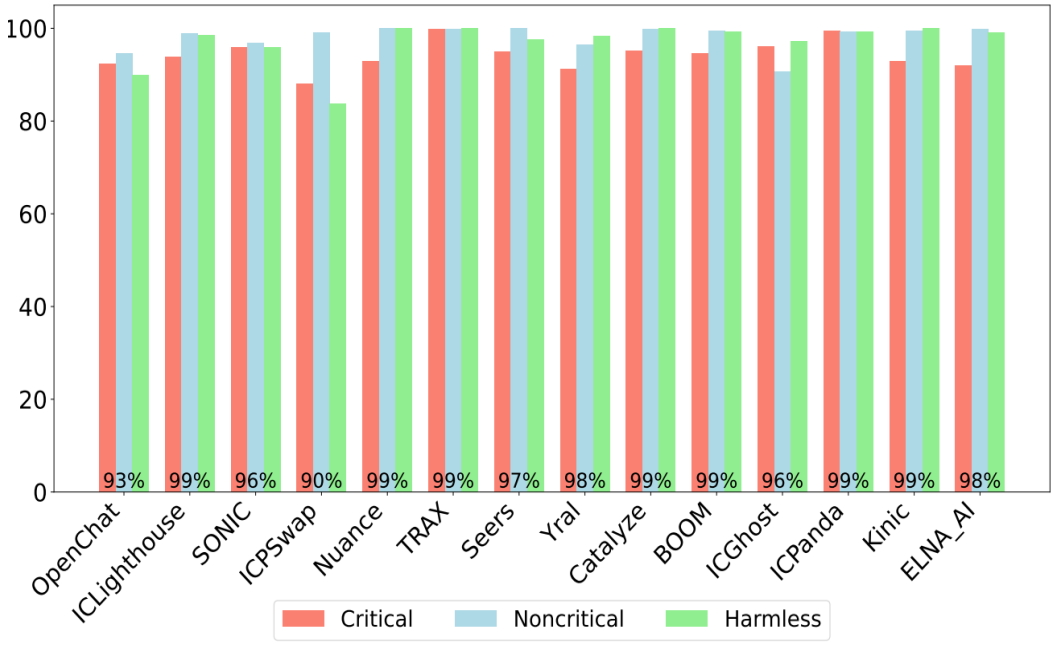
Engagement Over Time

⇢ ***Fluctuations*** but overall ***upward trend***



Approval Rates

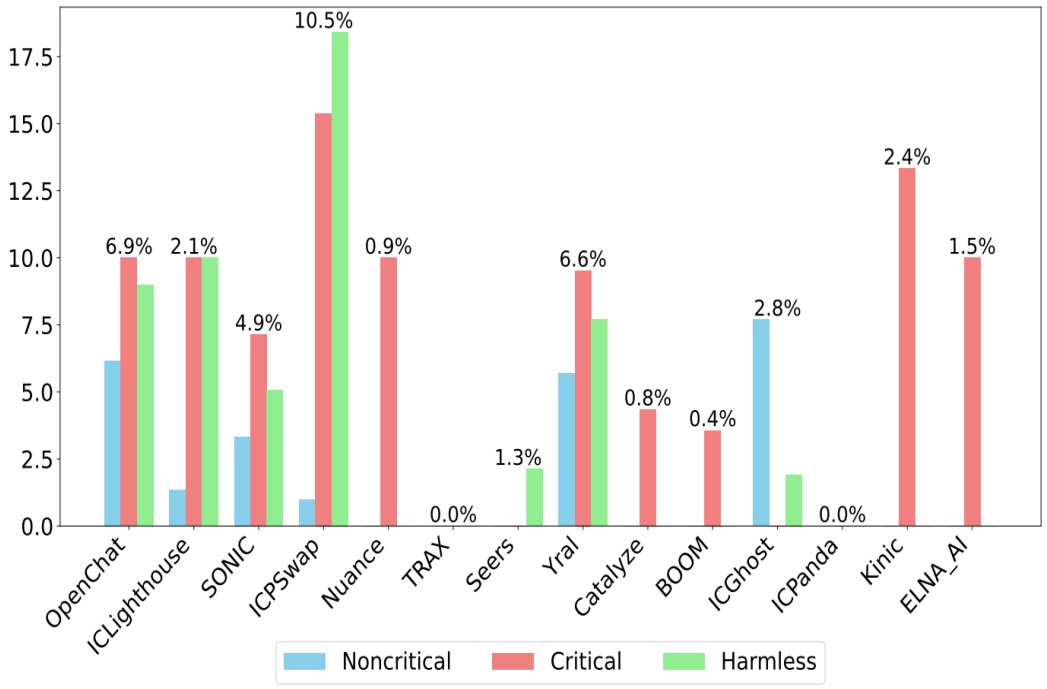
- ***Approval rates***: % of voting power in favor of proposal
- ***Strong consensus*** among the participants!
- May imply ***close alignment*** between proposers and community



Rejected Proposals

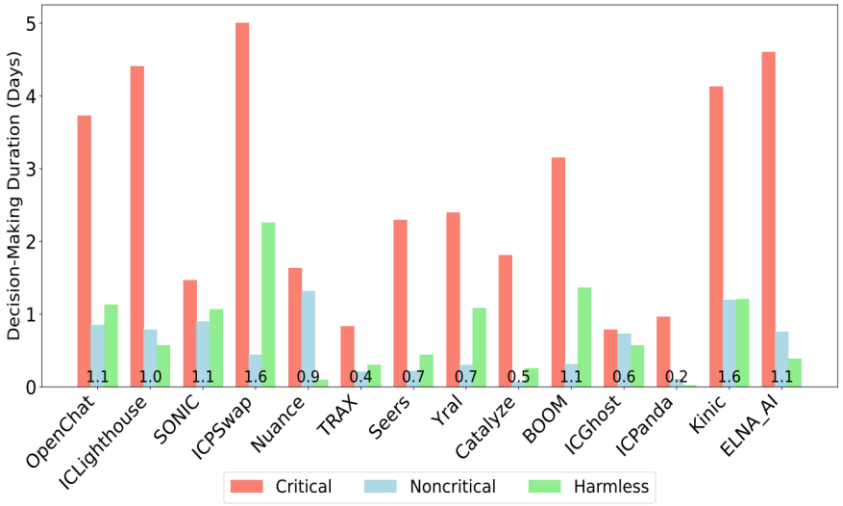
⇢ Lower approval for ***critical proposals***: indicates more varied opinions that could ***impact the future*** of the project

⇢ More rejections for ***harmless***: because they are specifically submitted gather ***diverse opinions***?



Proposal Durations

- Average time between proposal submission and decision
- Generally ***fast***: indicates community ***responsiveness and efficiency***
- ICPanda and ICGhost: ***short*** (3.84 h and 14.8 h), possibly due to their category as a ***meme coin***
- ***Critical proposals*** require significantly longer: due to longer voting period and require ***more attention***
- H***armless*** proposals also exhibited a higher duration that non-critical: ***encourage discussions***



Theoretical Perspective

When is liquid democracy

Possible/Efficient?

A simple model:

⇢ Binary voting with ground truth

⇢ Players only know which other players have at least ***+α*** more competence

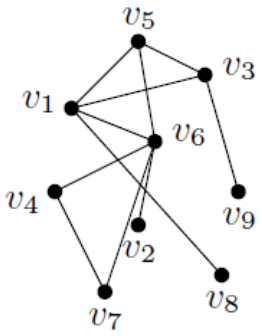
⇢ If ***at least t*** many, delegate to a ***random one*** of them

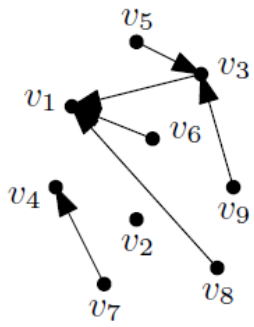
⇢ Results in ***delegation graph***

⇢ Compare to ***direct voting***?

Competencies:

$p_1 = 0.8$
$p_2 = 0.6$
$p_3 = 0.5$
$p_4 = 0.4$
$p_5 = 0.3$
$p_6 = 0.3$
$p_7 = 0.2$
$p_8 = 0.2$
$p_9 = 0.1$





Desiderata

- **Positive gain:** there exists some instances where delegation performs better
- **Do no harm:** for all instances, the loss asymptotically goes to 0 (with more players)
- **Strong positive gain:** for all instances, delegation performs better

Liquid democracy can lead to

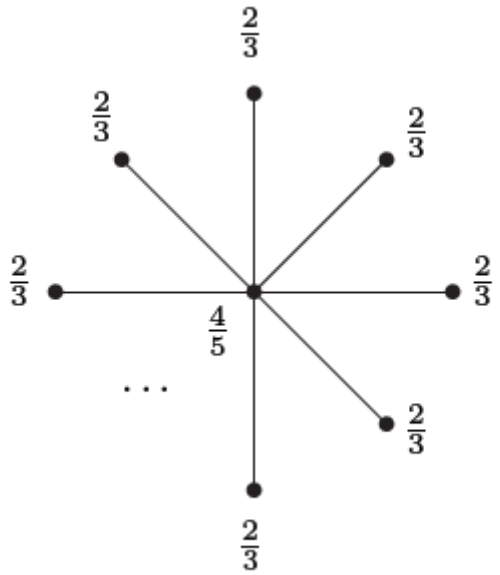
Worse Outcomes in Theory

⇢ ***Direct majority*** converges to ***1***
(for large networks)

⇢ Delegation good? All delegate to ***more competent*** node!

⇢ However, delegation concentrates all voting power to the central node.
Thus, the probability of voting correctly in the delegation setting is 4/5 leading to a ***negative gain*** of 1/5.

.



But often it performs

Better in Practice

⇢ On the positive side: delegation better for many ***realistic graphs***!

⇢ Complete graph, random d-***regular graphs***, and bounded degree and bounded minimal degree graphs

Discussion

⇢ Governance plays ***important role*** in decentralized applications

⇢ But voting power distributed is currently fairly ***skewed***

⇢ Really a problem? In practice: no evidence so far (e.g., ***communities***). What about additional delegation skew?

⇢ And/or is there a way to make ***direct democracy*** more ***efficient***? E.g., using ***random sampling***? At least for ***reviewing*** votes of stewards?

⇢ How can users be ***incentivized*** to vote? And should they?

⇢ Is delegation compatible with ***privacy***: e.g. certain votes in German Parliament are private?

Further Reading

Democracy for DAOs: An Empirical Study of Decentralized Governance and Dynamics (Best Student Paper Award)
Burak Arda Okutan, Stefan Schmid, and Yvonne-Anne Pignolet.
IEEE International Conference on Blockchain and Cryptocurrency (**ICBC**), Pisa, Italy, June 2025.

When Is Liquid Democracy Possible? On the Manipulation of Variance
Krishnendu Chatterjee, Seth Gilbert, Stefan Schmid, Jakub Svoboda, and Michelle Yeo.
ACM Symposium on Principles of Distributed Computing (**PODC**), Huatulco, Mexico, June 2025.

Invited Paper: Blockchain Governance and Liquid Democracy – Quantifying Decentralization in Gitcoin and Internet Computer
Stefan Schmid and Dmitry Shestakov.
ApPLIED Workshop at ACM PODC, Nantes, France, June 2024.

Thank you!

Backup Slides

Related Work (1)

⇢ Innovative governance structures often discussed in the context of ***decentralized autonomous organizations (DAO)*** and member-owned communities

⇢ Early blockchain example: ***stablecoin*** protocol MakerDAO

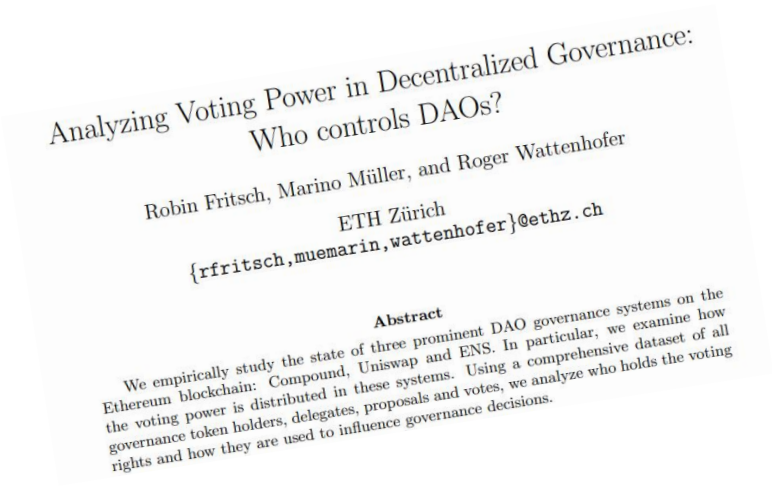
⇢ Blog articles by Vitalik ***Buterin*** show ***drawbacks*** of the current governance models

⇢ First studies on centralization aspects e.g., by Gochhayat et al. who discuss additional metrics like ***entropy, Kullback-Leibler divergence***

Related Work (2)

⇢ ***Fritsch et al.*** study DAO governance of three Ethereum systems (Compound, Uniswap, ENS). Also find very ***high skew*** (comparable to ***shareholder meetings***). However, large delegates often do not use their power but decide in the same way as the larger ***community***, i.e. smaller delegates.

⇢ ***Barbereau et al.*** study also Aave, SushiSwap, Synthetix, Yearn Finance, 0x, and UMA



Analyzing Voting Power in Decentralized Governance: Who controls DAOs?

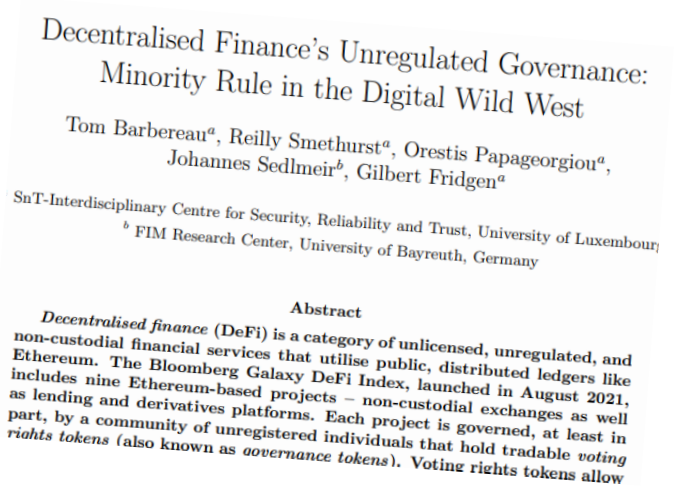
Robin Fritsch, Marino Müller, and Roger Wattenhofer

ETH Zürich

{rfritsch,muemarin,wattenhofer}@ethz.ch

Abstract

We empirically study the state of three prominent DAO governance systems on the Ethereum blockchain: Compound, Uniswap and ENS. In particular, we examine how the voting power is distributed in these systems. Using a comprehensive dataset of all governance token holders, delegates, proposals and votes, we analyze who holds the voting rights and how they are used to influence governance decisions.



Decentralised Finance's Unregulated Governance: Minority Rule in the Digital Wild West

Tom Barbereau[a], Reilly Smethurst[a], Orestis Papageorgiou[a], Johannes Sedlmeir[b], Gilbert Fridgen[a]

[a] SnT-Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembour
[b] FIM Research Center, University of Bayreuth, Germany

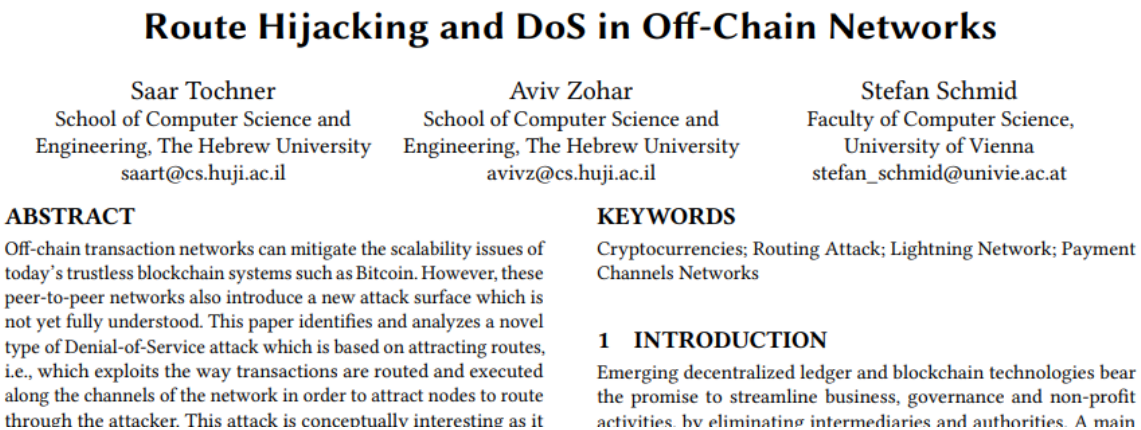
Abstract

Decentralised finance (DeFi) is a category of unlicensed, unregulated, and non-custodial financial services that utilise public, distributed ledgers like Ethereum. The Bloomberg Galaxy DeFi Index, launched in August 2021, includes nine Ethereum-based projects – non-custodial exchanges as well as lending and derivatives platforms. Each project is governed, at least in part, by a community of unregistered individuals that hold tradable *voting rights tokens* (also known as *governance tokens*). Voting rights tokens allow

Related Work (3)

⇢ Centralization may also be an issue in off-chain networks and ***Payment Channel Networks (PCNs)*** like Lightning: most transactions may be ***routes*** through a small set of nodes

⇢ Can also lead to ***denial-of-service*** attacks:



Route Hijacking and DoS in Off-Chain Networks

Saar Tochner
School of Computer Science and Engineering, The Hebrew University
saart@cs.huji.ac.il

Aviv Zohar
School of Computer Science and Engineering, The Hebrew University
avivz@cs.huji.ac.il

Stefan Schmid
Faculty of Computer Science, University of Vienna
stefan_schmid@univie.ac.at

ABSTRACT

Off-chain transaction networks can mitigate the scalability issues of today's trustless blockchain systems such as Bitcoin. However, these peer-to-peer networks also introduce a new attack surface which is not yet fully understood. This paper identifies and analyzes a novel type of Denial-of-Service attack which is based on attracting routes, i.e., which exploits the way transactions are routed and executed along the channels of the network in order to attract nodes to route through the attacker. This attack is conceptually interesting as it

KEYWORDS

Cryptocurrencies; Routing Attack; Lightning Network; Payment Channels Networks

1 INTRODUCTION

Emerging decentralized ledger and blockchain technologies bear the promise to streamline business, governance and non-profit activities, by eliminating intermediaries and authorities. A main

ACM Conference on Advances in Financial Technologies (AFT), 2020

Related Work (4)

Short Paper: A Centrality Analysis of the Lightning Network

Philipp Zabka[1], Klaus-T. Foerster[2], Christian Decker[5], and Stefan Schmid[3,1,4]

[1] Faculty of Computer Science, University of Vienna, Austria
[2] Faculty of Computer Science, Technical University of Dortmund, Germany
[3] Faculty of Computer Science, Technical University of Berlin, Germany
[4] Fraunhofer SIT, Germany
[5] Blockstream, Zurich, Switzerland

Abstract. Payment channel networks (PCNs) such as the Lightning Network offer an appealing solution to the scalability problem faced by many cryptocurrencies operating on a blockchain such as Bitcoin. However, PCNs also inherit the stringent dependability requirements of blockchain. In particular, in order to mitigate liquidity bottlenecks as well as on-path attacks, it is important that payment channel networks maintain a high degree of decentralization. Motivated by this require-

Financial Cryptography and Data Security (FC), 2022.