Blockchain Governance and Liquid Democracy

Quantifying Decentralization in Gitcoin and Internet Computer

Stefan Schmid and Dmitry Shestakov
TU Berlin

Blockchain Governance and Liquid Democracy

Quantifying Decentralization in Gitcoin and Internet Computer

Stefan Schmid and Dmitry Shestakov
TU Berlin

Thanks to Yvonne Anne Pignolet (Dfinity / Internet Computer)!

Decentralization Is „En Vogue“!

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

Cryptocurrencies

Web 3.0

Metaverse

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

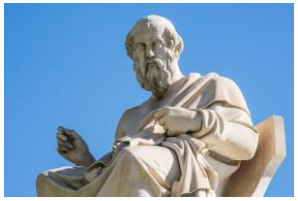
Decentralized Governance

⇢ ***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.

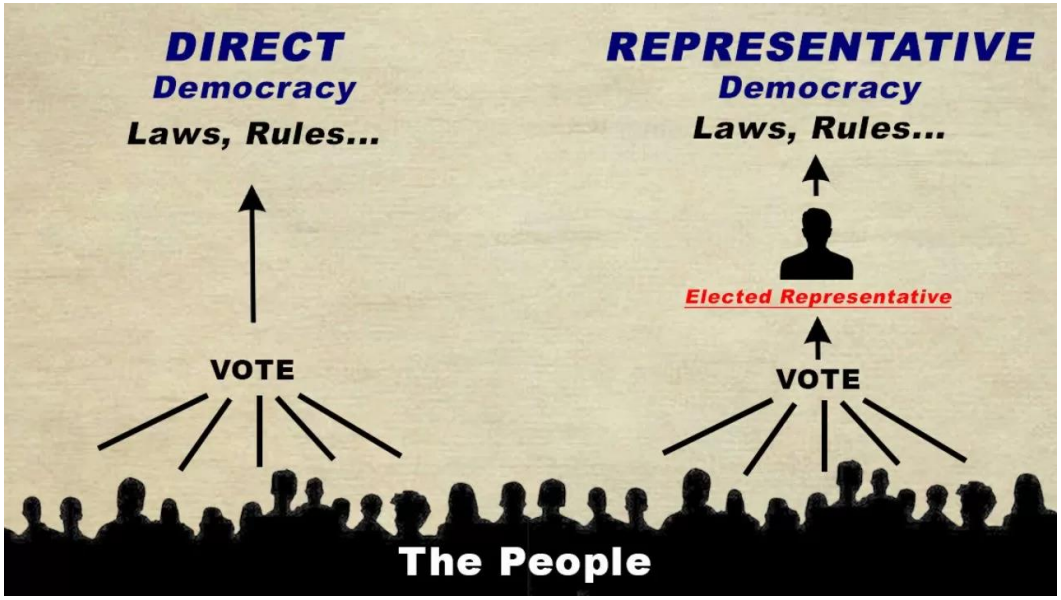
- From Greek kubernaein (“to steer”), first metaphorical use by Plato



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

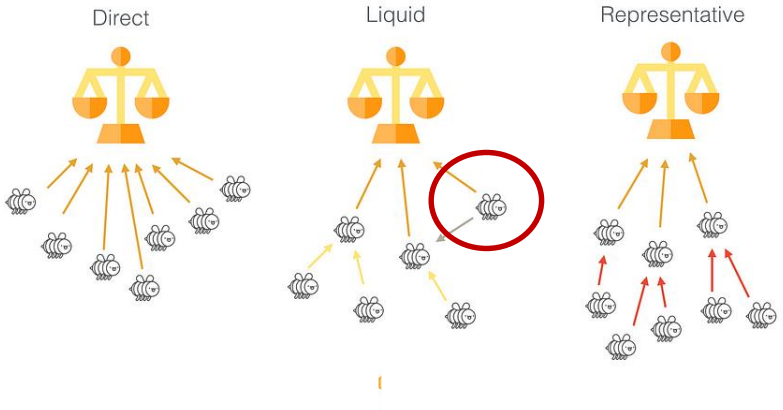
are *incentives* of representatives really aligned with voters?

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***

⇢ Delegation attractive for participants with few governance tokens: no need to research proposal details themselves

⇢ But: does delegation not again lead to ***concentration and centralization***?

⇢ To which extent and how is delegation used in blockchains today?

⇢ In this paper: case study with ***Gitcoin*** and ***Internet Computer***

Internet Computer

⇢ The Internet Computer (ICP): ***general-purpose blockchain*** designed to replace traditional IT and host emerging ***Web 3.0*** services

⇢ Hosts ***canister smart contracts***

⇢ All changes to the ***configuration and behavior*** of are controlled by a governance system called the ***Network Nervous System (NNS)***

⇢ Governance tokens are called ***neurons*** (a staked amount of ICP)

⇢ Neurons 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)

Gitcoin 

⇢ A leading platform in the ***Ethereum*** ecosystem

⇢ Voting used, e.g., to fund public goods or govern the blockchain of the ***GitcoinDAO*** (our focus)

⇢ Distinguishes between ***delegators*** (the delegating node) and ***stewards*** (the delegated node)

⇢ Roles ***not disjoint***: delegator can be a steward for other nodes

Methodology (1)

⇢ Internet Computer (ICP): governance information collectable via their ***public API***

⇢ Gitcoin (GTC): information about on-chain governance collected from the Ethereum network (with ***Dune*** Analytics queries); for off-chain governance, with the ***Snapshot*** GraphQL API

⇢ To obtain ***voting power distribution***: query the number of tokens held by each address, and the number of tokens delegated to each delegate

Methodology (2)

⇢ Actually, ***more complicated*** in practice…

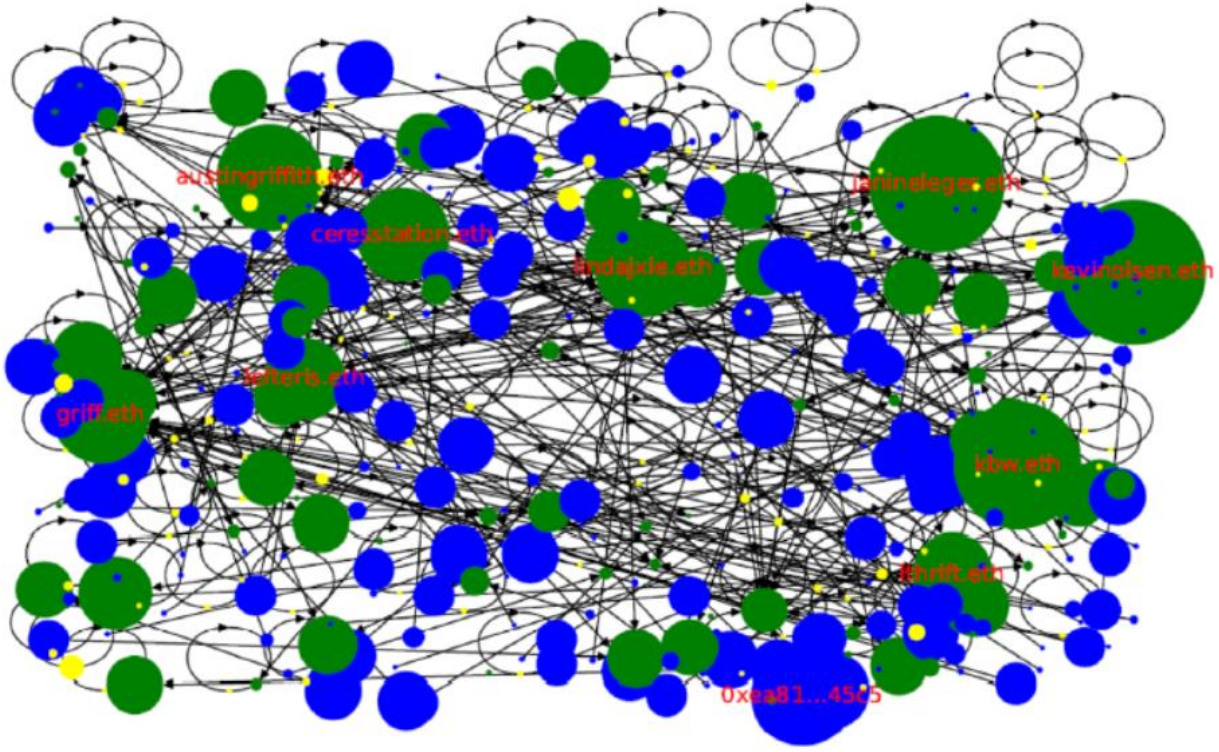
⇢ Large amount of GTC ***locked*** in the GitcoinDAO ***Treasury*** and ***Timelock*** addresses

⇢ These volumes do ***not participate*** in the governance: we deducted them for our analysis

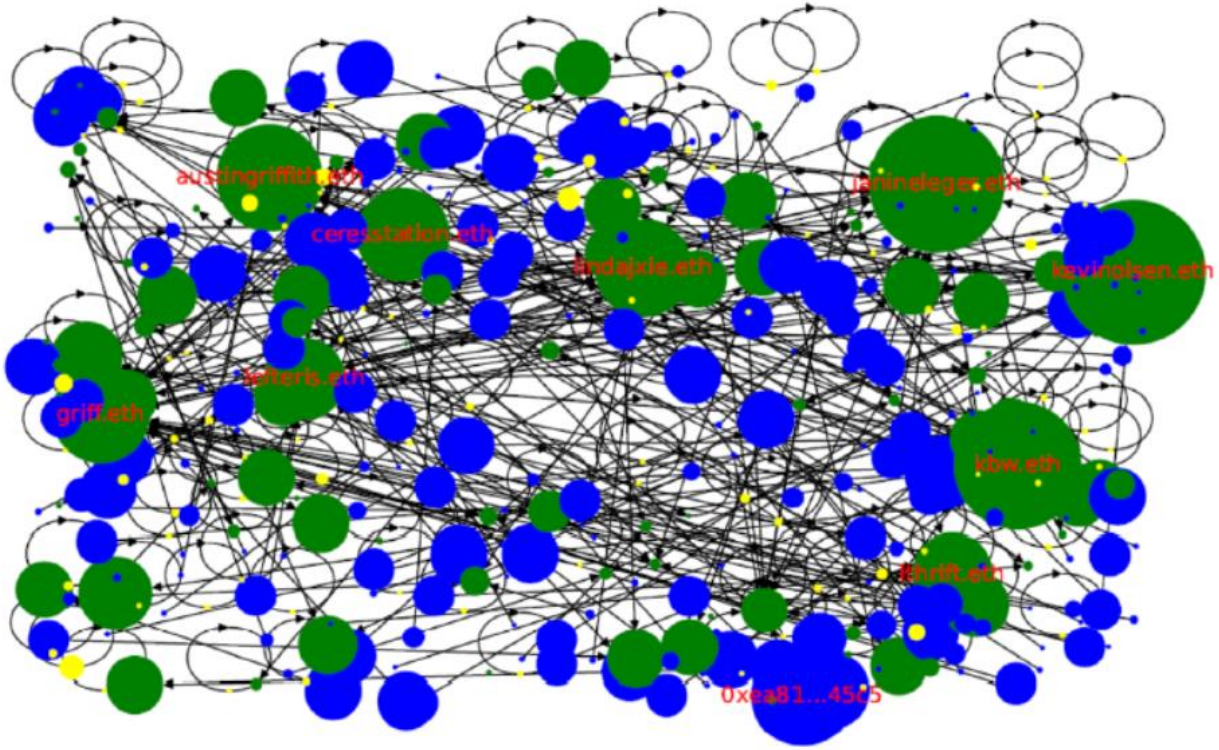
⇢ For ICP, a large part of the neurons is ***not indexed*** and cannot be queried through the API

Take our results with a grain of salt!

Empirical Results (1)



Empirical Results (2)

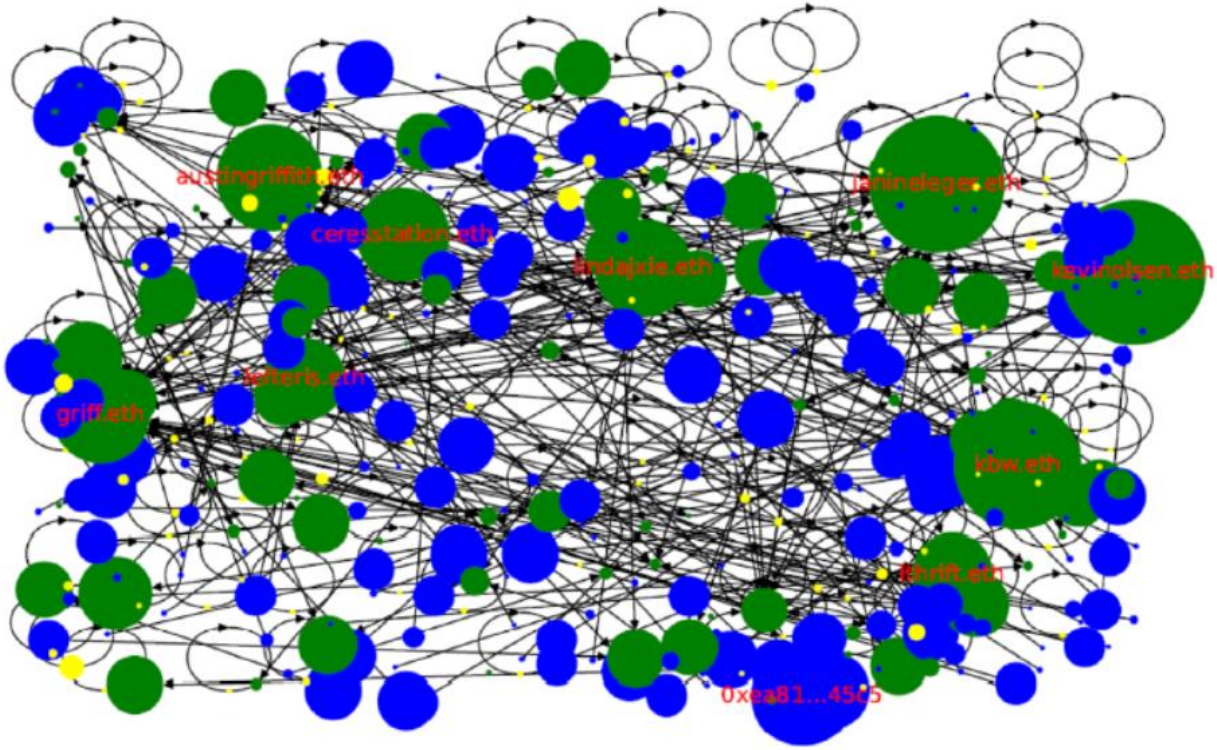


⇢ For ***GitcoinDAO***: node ***size*** = amount of GTC it receives/delegates

⇢ Stewards in ***green***, delegators (who are not also stewards) in ***blue***

⇢ ***Yellow***: node delegates to itself

Empirical Results (3)



⇢ ***Top stewards*** such as kevinolsen.eth, griff.eth and others possess a large amount of ***voting power***

⇢ Some nodes ***delegate*** significant amounts

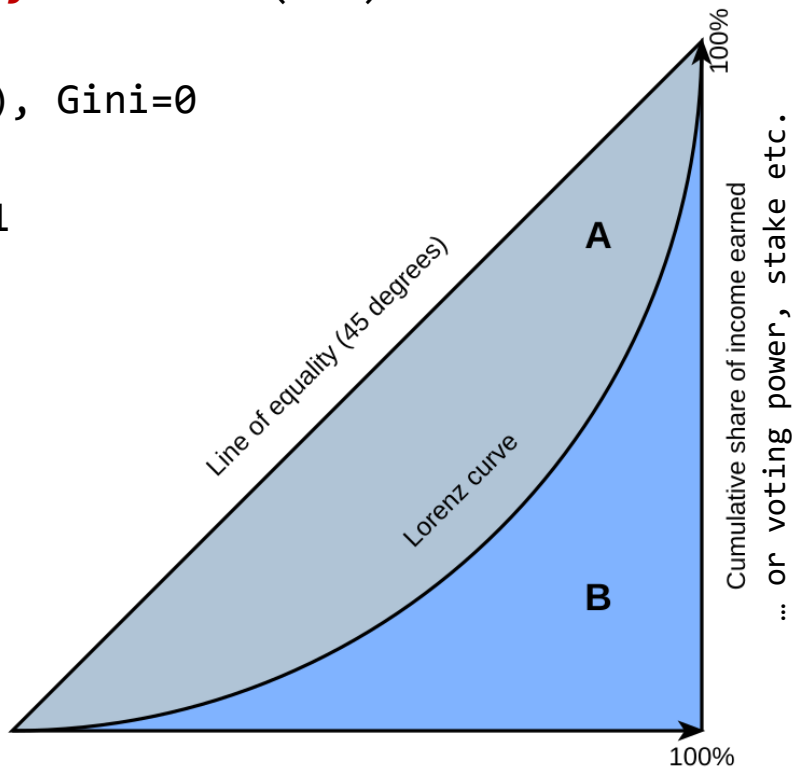
More systematically:

Centralization Metrics (1)

⇢ ***Lorenz curve*** and ***Gini coefficient***: A/(A+B)

⇢ So if perfectly fair (A=0), Gini=0

⇢ So if unfair (B=0), Gini=1



… or voting power, stake etc.

More systematically:

Centralization Metrics (2)

⇢ Alternative: ***Nakamoto coefficient***

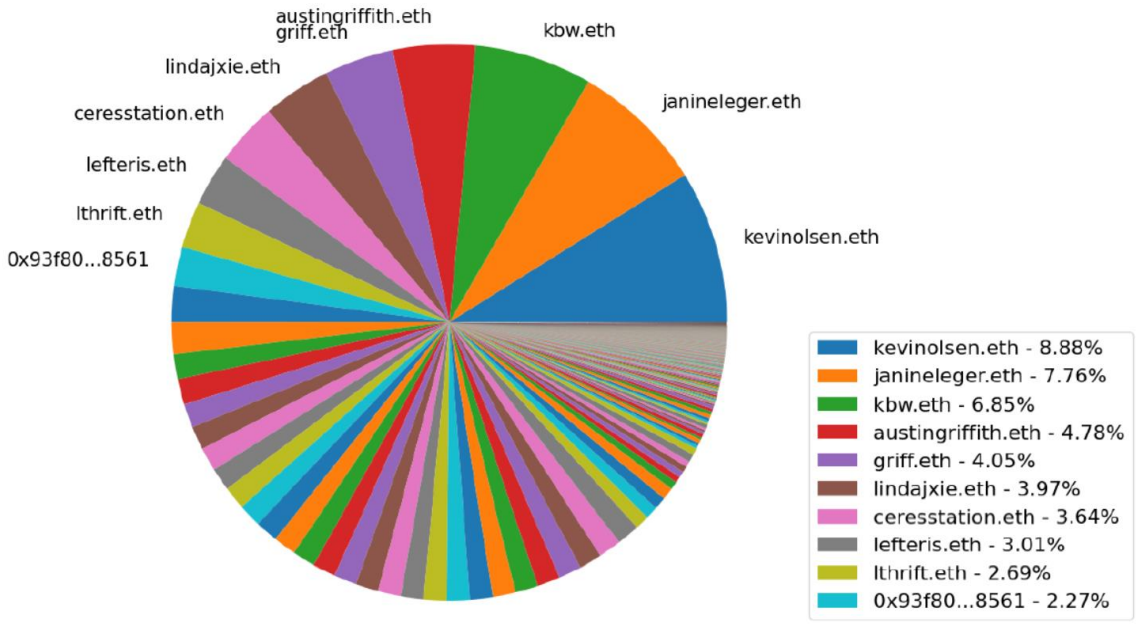
⇢ More critical metric in cryptocurrencies: minimum number of entities required to get to ***51% of the total*** capacity

⇢ Focus more on ***big players***: how many can ***collude*** to get majority

⇢ Remark: for ***Proof-of-Stake***, often ***33%*** is considered

Voting Power in GTC (1)

⇢ GitcoinDAO voting power distribution among Stewards:



⇢ Top-10 stewards control 47.9% of voting power

⇢ Top-50 control 93.8%, top 100 control 96.8%

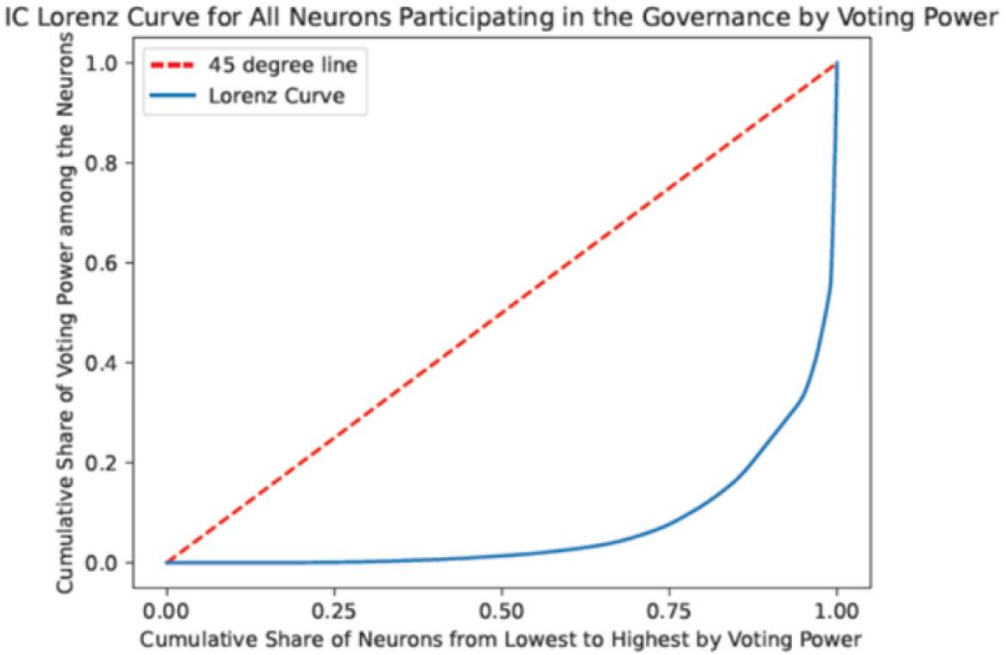
Voting Power in GTC (2)

⇢ Relative and absolute skew:

Steward	Percentage among Stewards	Delegated and Owned Amount (GTC)
kevinolsen.eth	8.88%	1,952,072.97
janineleger.eth	7.76%	1,706,263.00
kbw.eth	6.85%	1,506,050.79
austingriffith.eth	4.78%	1,049,838.39
griff.eth	4.05%	891,141.99
lindajxie.eth	3.97%	872,130.00
ceresstation.eth	3.64%	800,543.00
lefteris.eth	3.01%	662,478.30
lthrift.eth	2.69%	592,244.00
0x93f80...8561	2.27%	500,000.00

Voting Power in ICP

⇢ Also in ICP, voting power is ***skewed***:



⇢ Neurons 27 (DFINITY Foundation) and 28 ("Internet Computer Association“) presumably influence a large part of the voting

Remark: Voting Power

⇢ ***Voting power computation*** in ICP is complicated

⇢ 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

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

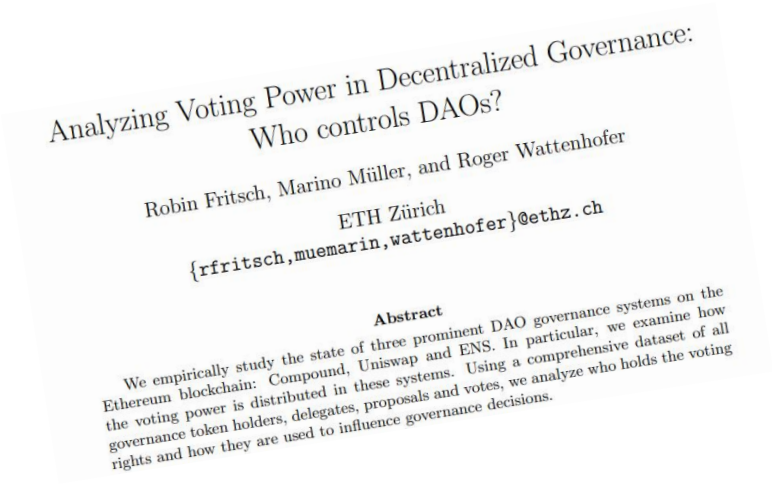
⇢ Blog articles by Vitalik ***Buterin*** show ***drawbacks*** of the current governance models

⇢ 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



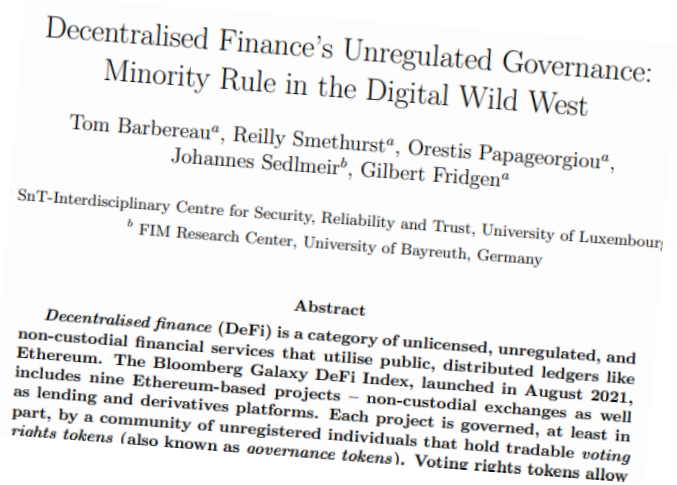
Analyzing Voting Power in Decentralized Governance:
Who controls DAOs?

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]

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

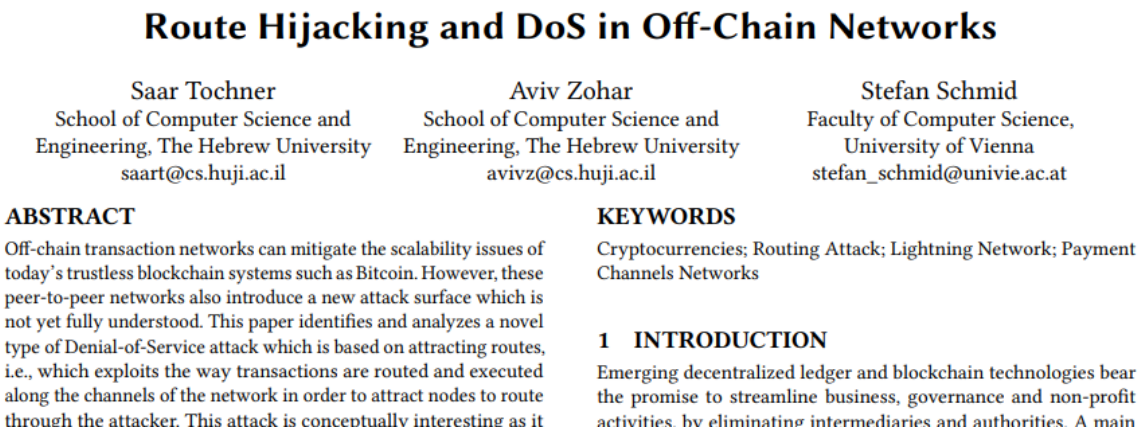
Abstract

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

Centralization in PCNs

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.

Discussion & Ideas

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

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

⇢ ***Delegation*** increases centralization further

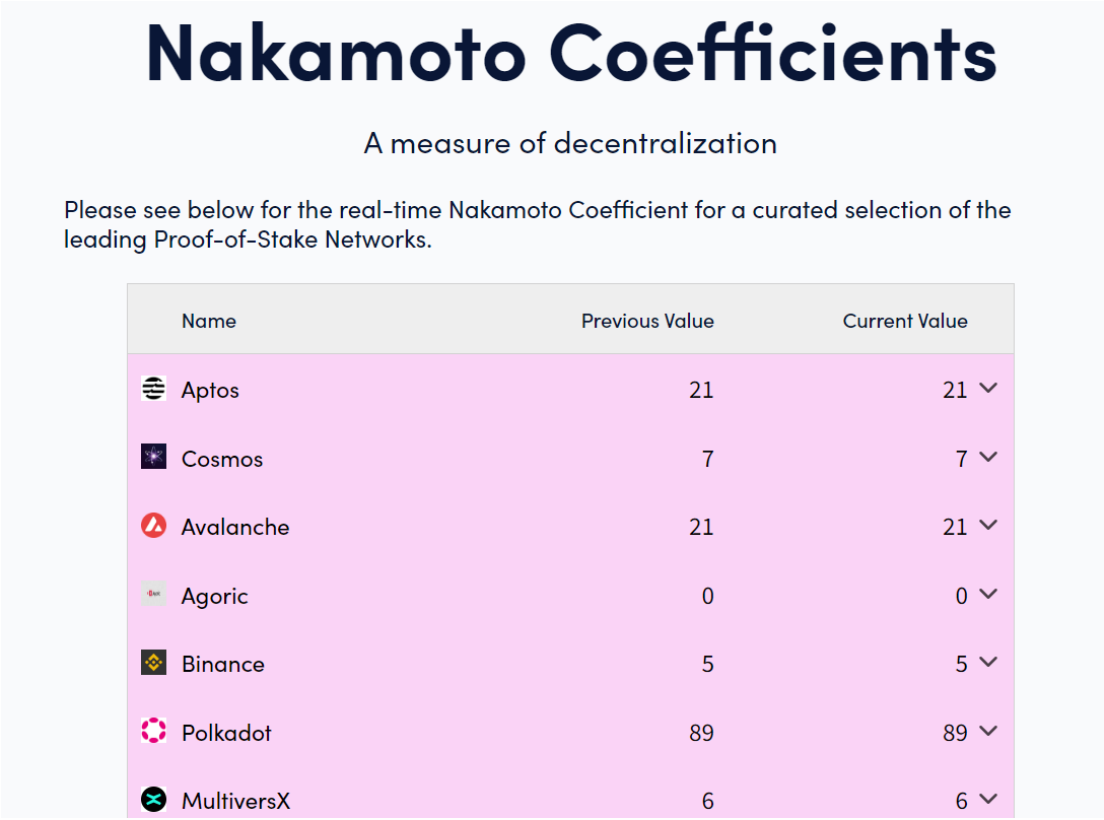
⇢ Really a problem? No evidence so far (e.g., ***communities***)

⇢ But needs further ***attention***…

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

Thank you!

Skew in PoS Systems



Nakamoto Coefficients

A measure of decentralization

Please see below for the real-time Nakamoto Coefficient for a curated selection of the leading Proof-of-Stake Networks.

Name	Previous Value	Current Value
Aptos	21	21
Cosmos	7	7
Avalanche	21	21
Agoric	0	0
Binance	5	5
Polkadot	89	89
MultiversX	6	6

⇢ https://nakaflow.io/