Proficiency Evaluation

Computational Methods for Analyzing Decentralized Finance Ecosystems

---

Advisor: Univ.-Prof. Matteo Maffei,
Co-Advisor: Dr. Bernhard Haslhofer,
Student: DI Stefan Kitzler (01127884)

Sept 03rd, 2024

TECHNISCHE
UNIVERSITÄT
WIEN

Presentation Overview

Problem Statement

Research Directions

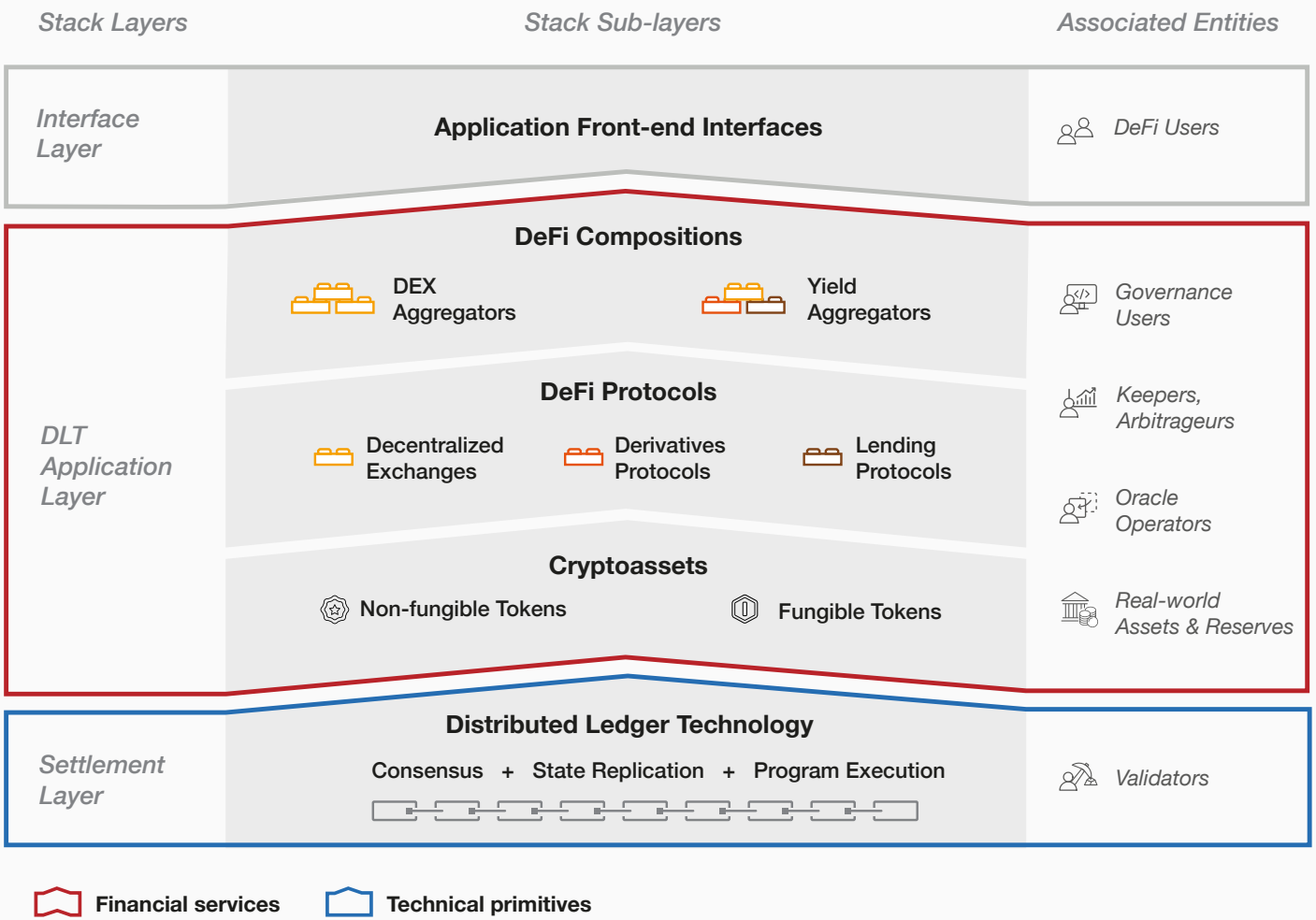
- DeFi Complexity
- DeFi Governance
- DeFi Crime

Publications

Introduction

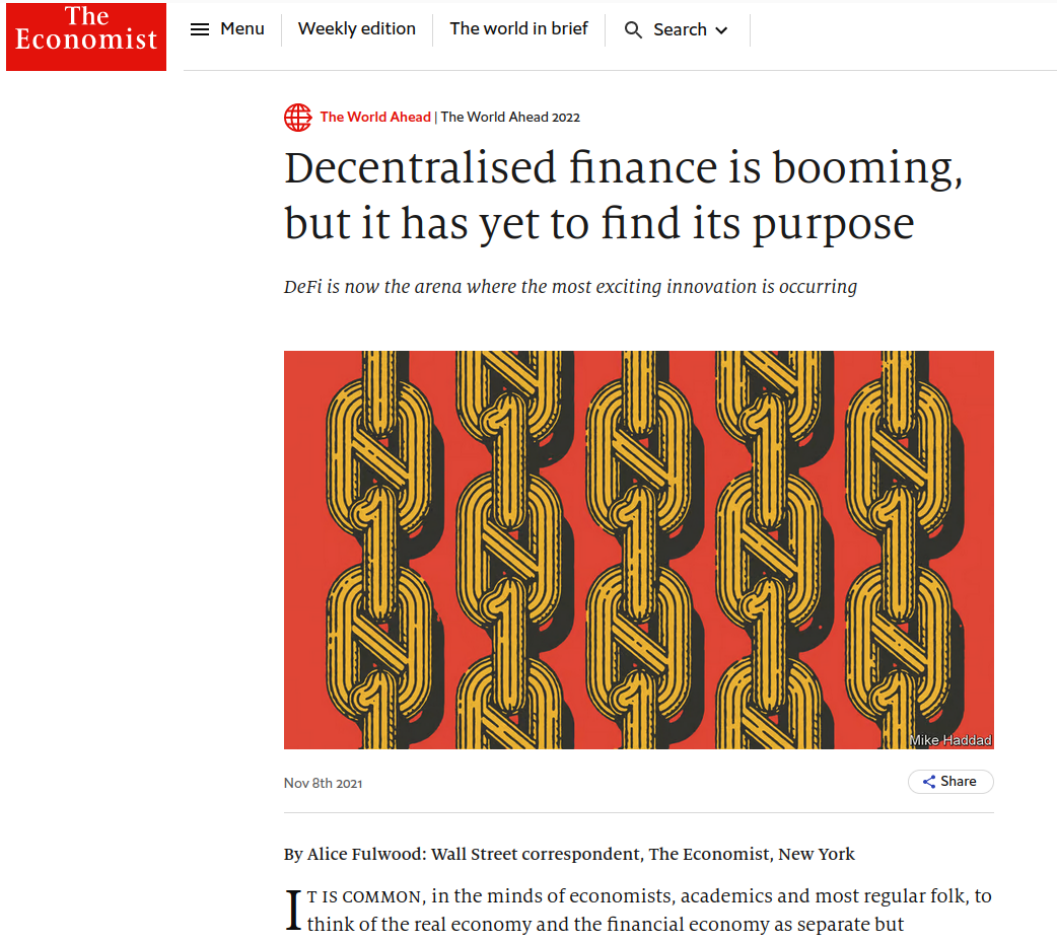
- In 2014, the **account-based model** of Ethereum introduced a new era of blockchain-based financial services.
- The architecture distinguishes between **user accounts** (externally owned accounts, EOA) and **contract accounts** (CA, or smart contracts), i.e., programmable software programs.
- Smart contracts constitute an additional application layer, facilitating innovations such as **cryptoassets**.
- Cryptoassets serve as the cornerstone for **decentralized finance** (DeFi), providing financial services such as asset management services, decentralized exchanges (DEXs) or lending.

DeFi Stack



Auer, R., Haslhofer, B., **Kitzler, S.**, Saggese, P., & Victor, F. (2024). The technology of decentralized finance (DeFi). Digital Finance, 6(1), 55-95.

DeFi | Media Coverage



The Economist ≡ Menu | Weekly edition | The world in brief | Search

The World Ahead | The World Ahead 2022

Decentralised finance is booming, but it has yet to find its purpose

DeFi is now the arena where the most exciting innovation is occurring

Mike Haddad

Nov 8th 2021 Share

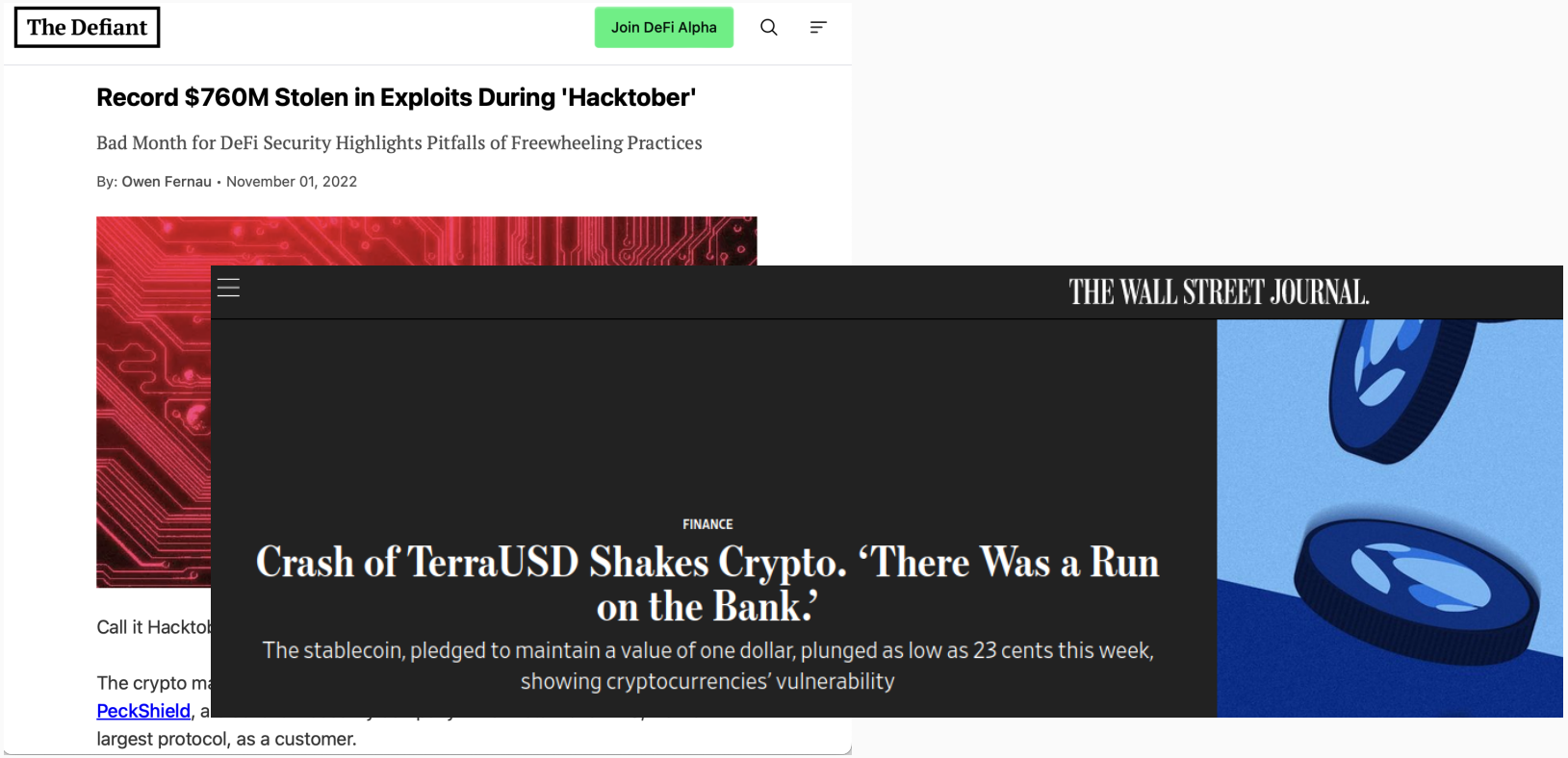
By Alice Fulwood: Wall Street correspondent, The Economist, New York

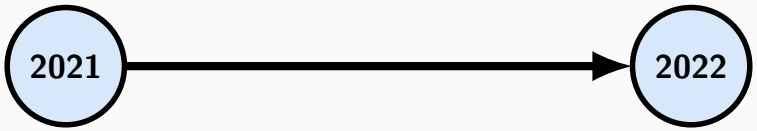
IT IS COMMON, in the minds of economists, academics and most regular folk, to think of the real economy and the financial economy as separate but

2021

Source: https://www.economist.com/the-world-ahead/2021/11/08/decentralised-finance-is-booming-but-it-has-yet-to-find-its-purpose

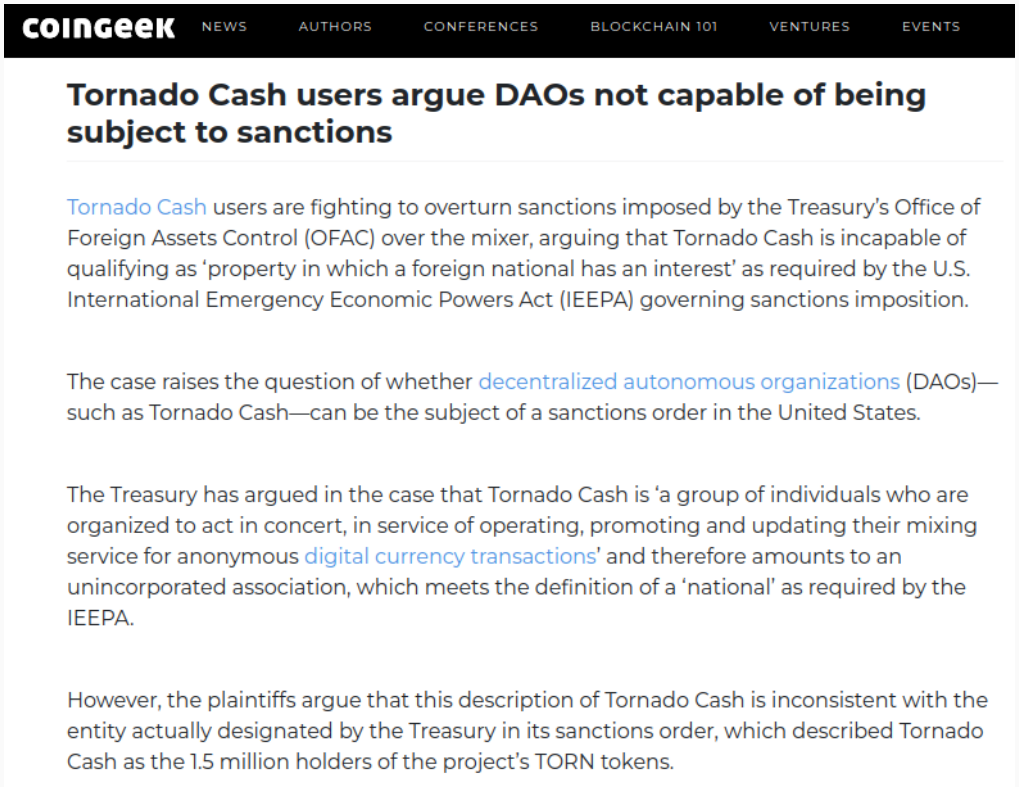
DeFi | Media Coverage





Sources: https://thedefiant.io/news/defi/exploits-double-to-3b-2022, https://www.wsj.com/articles/crash-of-terrausd-shakes-crypto-there-was-a-run-on-the-bank-11652371839

DeFi | Media Coverage



coingeek NEWS AUTHORS CONFERENCES BLOCKCHAIN 101 VENTURES EVENTS

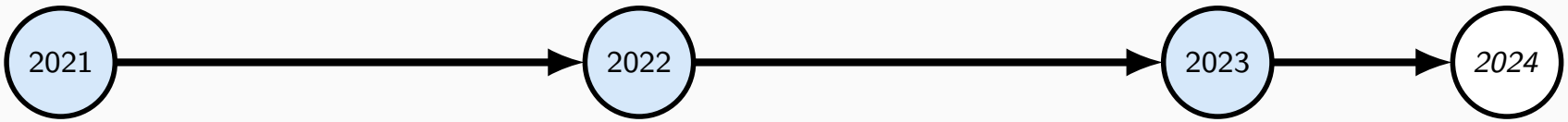
Tornado Cash users argue DAOs not capable of being subject to sanctions

Tornado Cash users are fighting to overturn sanctions imposed by the Treasury's Office of Foreign Assets Control (OFAC) over the mixer, arguing that Tornado Cash is incapable of qualifying as 'property in which a foreign national has an interest' as required by the U.S. International Emergency Economic Powers Act (IEEPA) governing sanctions imposition.

The case raises the question of whether decentralized autonomous organizations (DAOs)—such as Tornado Cash—can be the subject of a sanctions order in the United States.

The Treasury has argued in the case that Tornado Cash is 'a group of individuals who are organized to act in concert, in service of operating, promoting and updating their mixing service for anonymous digital currency transactions' and therefore amounts to an unincorporated association, which meets the definition of a 'national' as required by the IEEPA.

However, the plaintiffs argue that this description of Tornado Cash is inconsistent with the entity actually designated by the Treasury in its sanctions order, which described Tornado Cash as the 1.5 million holders of the project's TORN tokens.



Source: https://coingeek.com/tornado-cash-users-argue-daos-not-capable-of-being-subject-to-sanctions/

Problem Statement

Problem Statement — DeFi

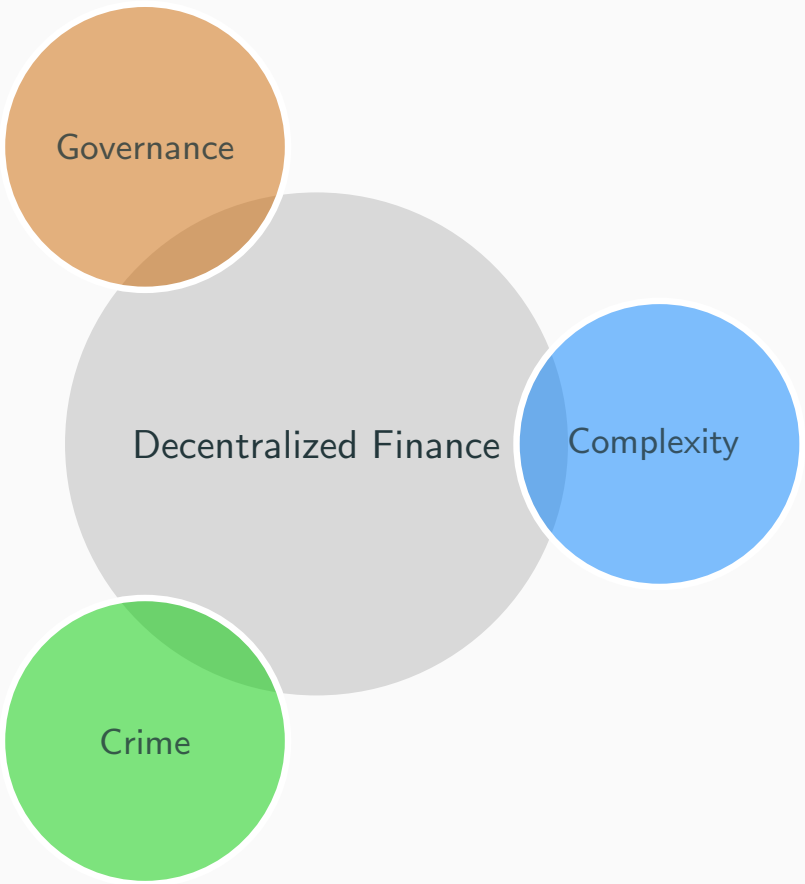
Decentralized Finance (DeFi) leverages **cryptography and blockchain technology** to provide **financial services**.

Unlike conventional financial systems, DeFi offers:

- automation and composability of financial services,
- decentralized decision-making on future developments, and
- unregulated, pseudonymous access to distributed ledgers, which introduces the possibility of abuse.

Problem Statements — Computational Challenges

2.5k DAOs
3.2M voters &
proposal makers [1]



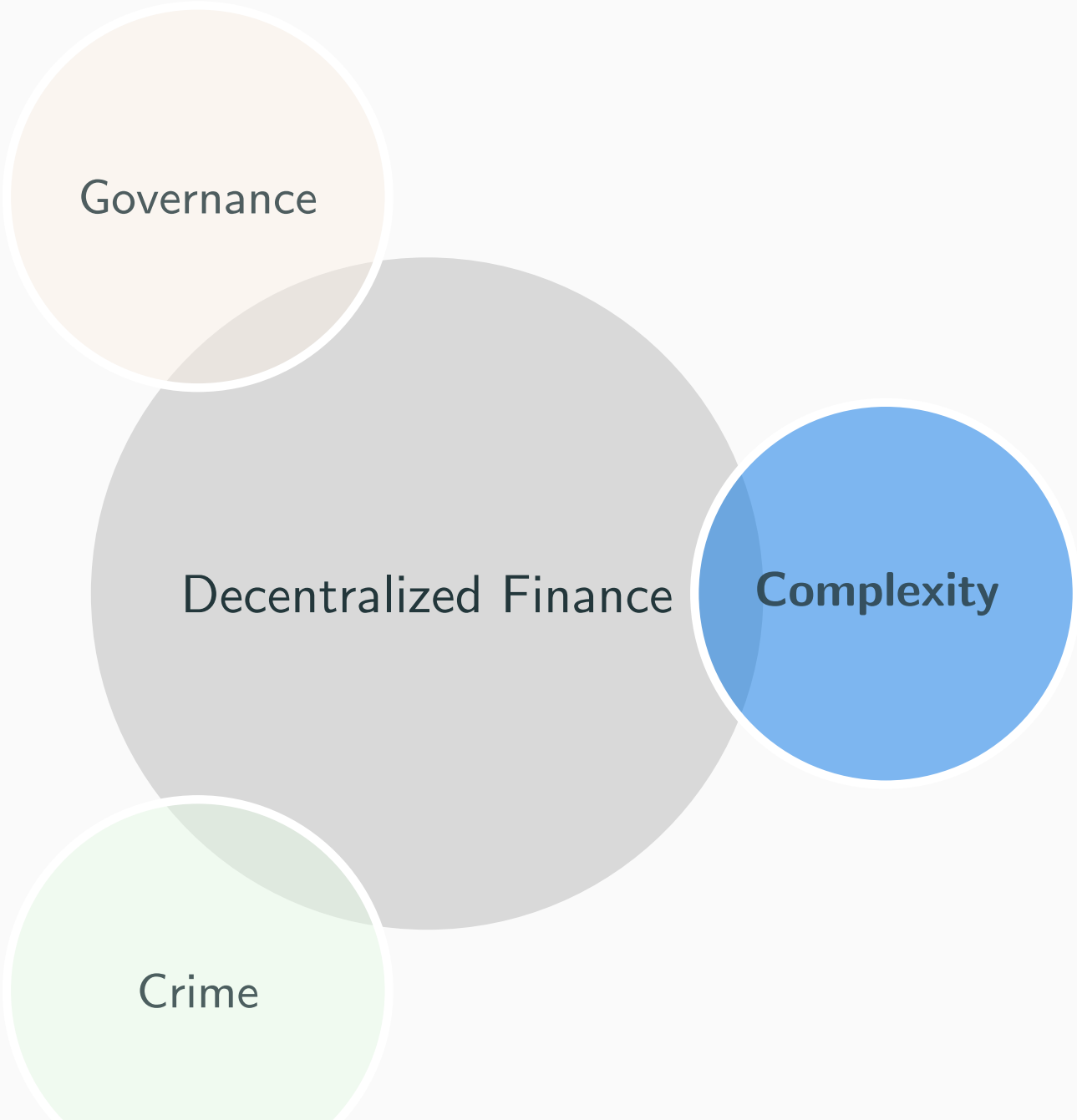
2.5B transactions,
310M addresses [2],
1.4M ERC20 transfers [3]

2.9k incidents
\$80B lost funds
33% on ETH [4]

[1] `deepdao.io/`, [2] `app.ikna.io/stats`, [3] `etherscan.io/charts` on 2024-08-29
[4] `https://de.fi/rekt-database` on 2024-09-01

Research Directions

DeFi Complexity

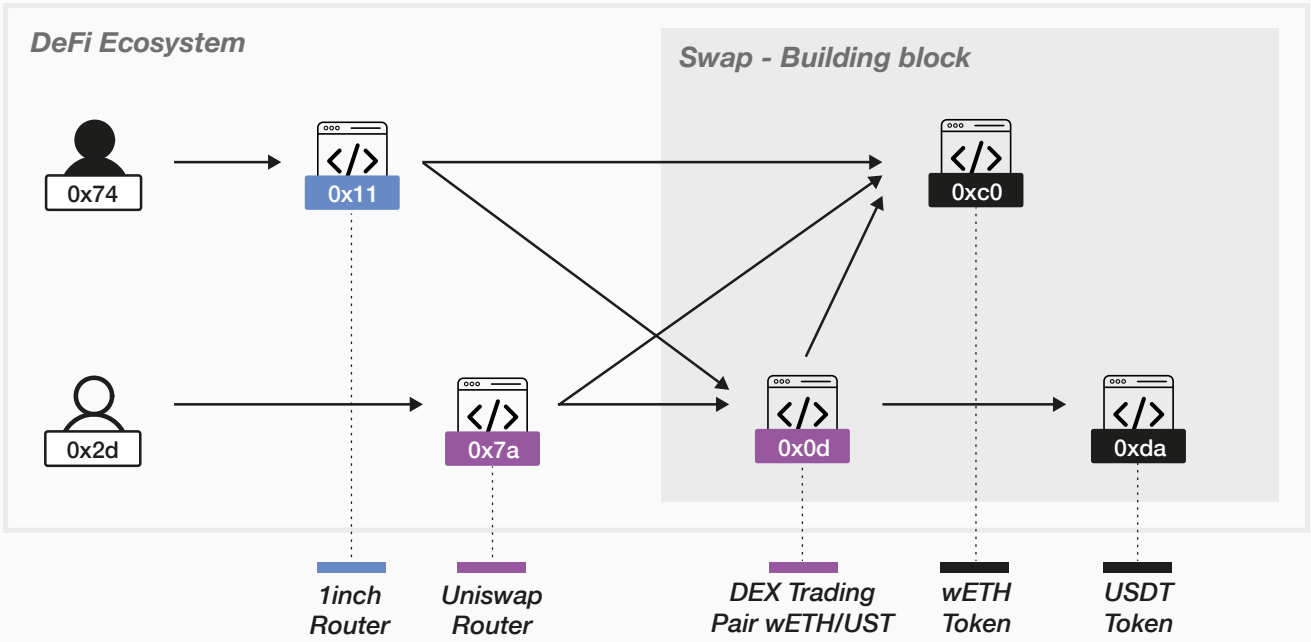


DeFi Compositions — Definition

Definition

A DeFi composition provides novel financial services by utilizing a combination of multiple DeFi protocol-specific smart contracts within a single transaction.

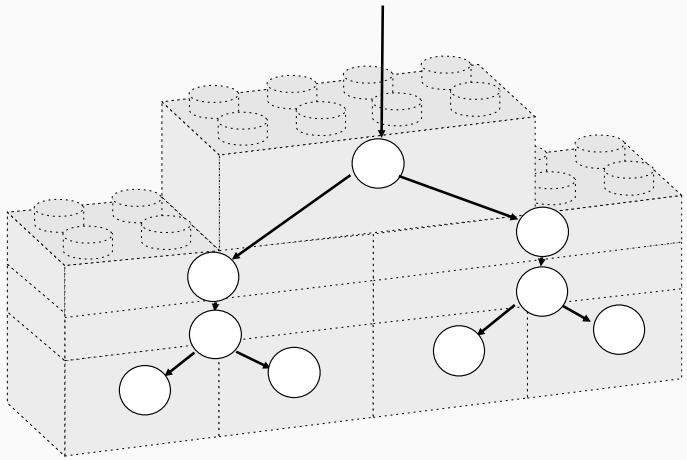
Example



Auer, R., Haslhofer, B., **Kitzler, S.**, Saggese, P., & Victor, F. (2024). The technology of decentralized finance (DeFi). Digital Finance, 6(1), 55-95.

Research Question

Previous studies have focused on understanding single DeFi protocols and how their intended design could be subverted [8, 6]. Up to now, potential risks of compositions have been discussed [13, 9, 14, 10] but not well investigated.



DeFi Complexity

RQ1: How can we decompose DeFi protocols and measure their nestedness?

Data

We gathered data:

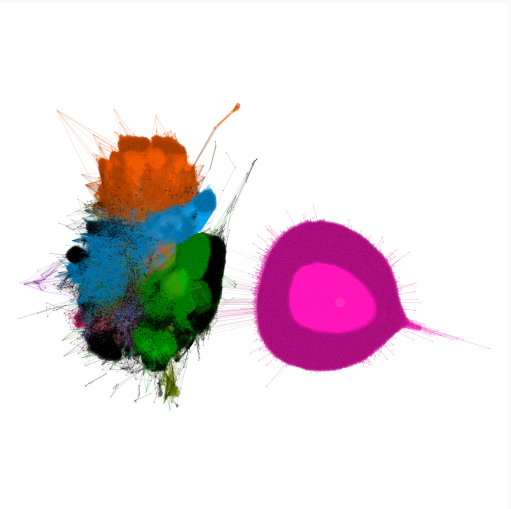
- Manually collected seed addresses of *23* DeFi protocols for categories:

  DEXs, *Lending*, *Derivatives*, and *Assets*.

- We extraced Ethereum transaction and associate internal traces of over $10M$ contract addresses of the DeFi protocols from January 2021 to August 2021.

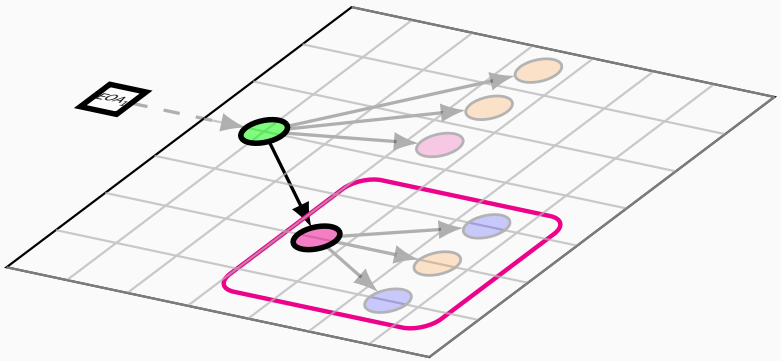
Network Analysis

- Dimension: $\sim 2.5M$ nodes, $\sim 3.5M$ links.
- The vast majority of protocol interactions are in the 2^{nd} **largest component**.
- Common **community detection** algorithms cannot disentangle DeFi protocols from the contract address networks.



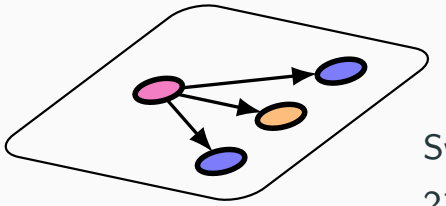
Computational Method

We propose an **algorithm to decompose** a protocol call into a nested set of recurring patterns (building blocks) that may be part of another DeFi protocol. This allows us to untangle and study protocol compositions.



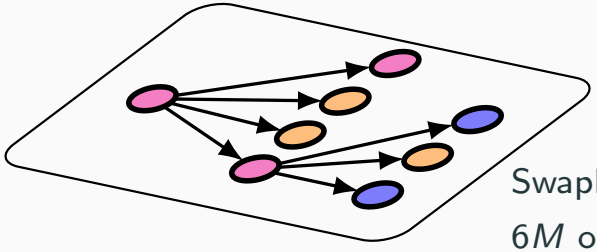
Building Block — Insights

Most Frequent Appearances



Swap

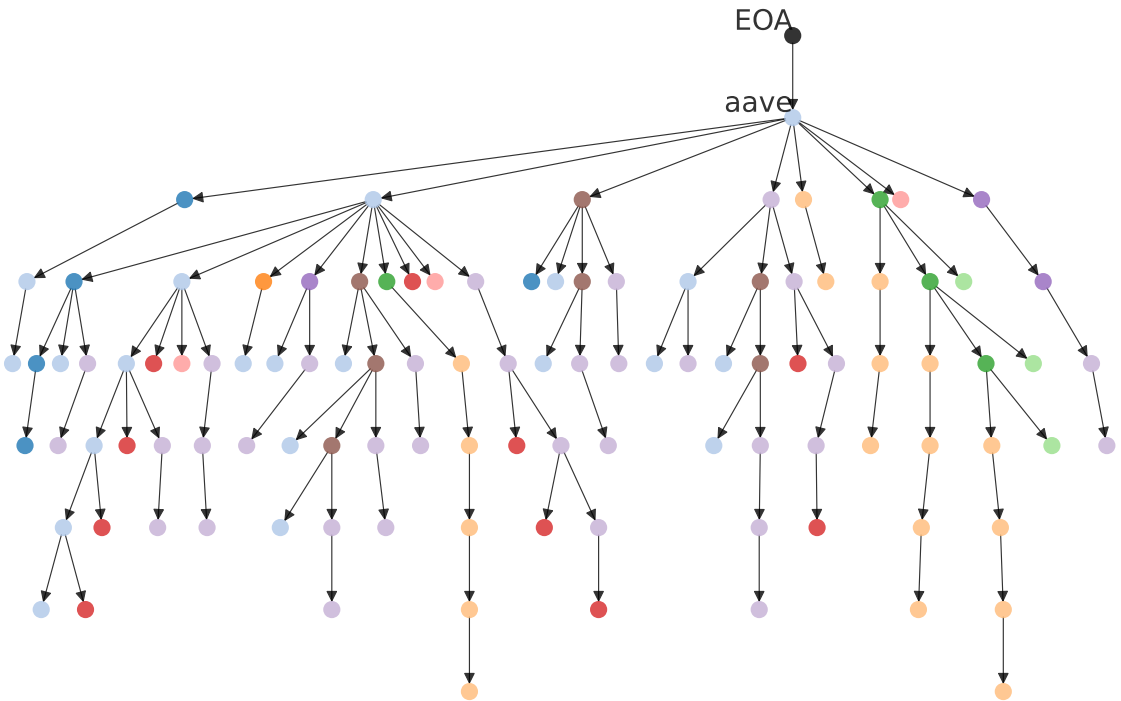
21*M* occurrences



SwapExactETHForTokens

6*M* occurrences

Nested structures *for the example of Aave*



Main Findings

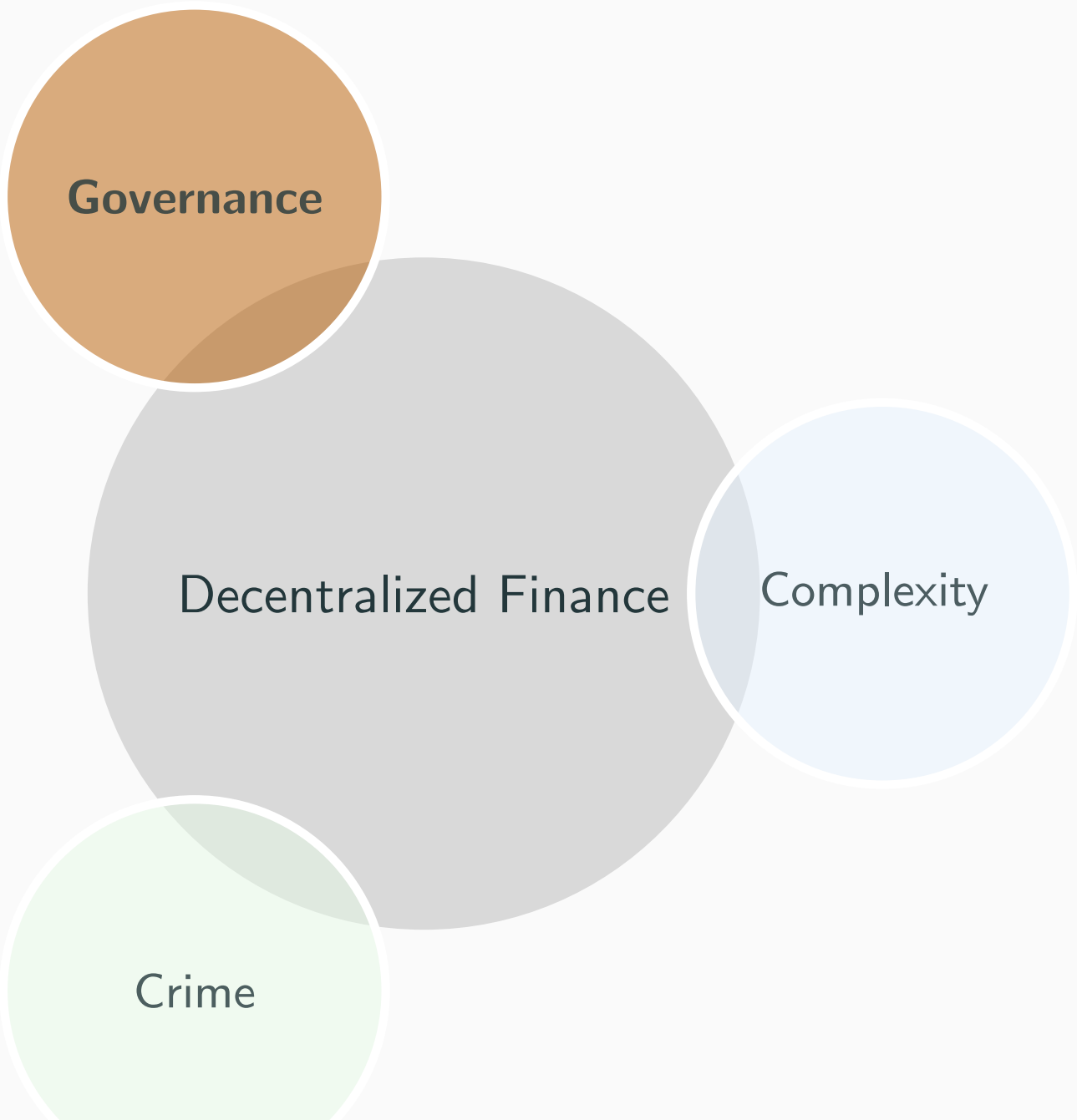
We analyze the complexity of DeFi compositions:

- The network topology reveals strongly connected components, and known community detection methods cannot disentangle DeFi protocols.
- We propose an algorithm that extracts building blocks from individual transactions.
- The swap building blocks of Uniswap are the most common building blocks with over 21M occurrences.
- We present a case study showing the extent to which DeFi service building blocks depend on Tether.

Impact:

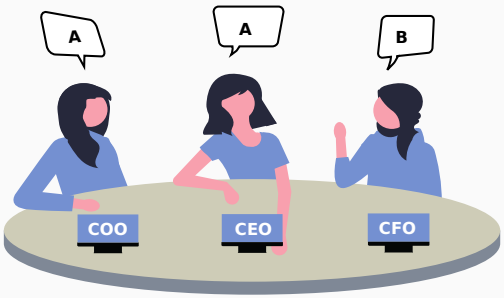
- DeFi building block extraction reveals unexpectedly high levels of compositions.
- Our **computational method** can be used to **decompose the nested structure** of DeFi services within a single transaction.

DeFi Governance



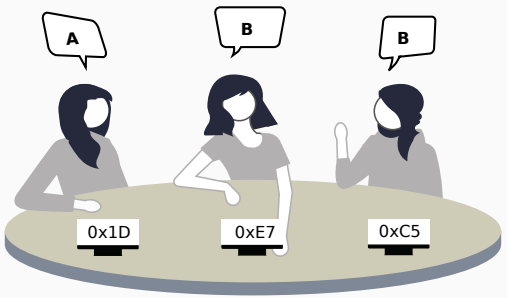
Decentralized Autonomous Organization

Decentralized Autonomous Organizations **(DAOs)** represent a novel organizational and governance model, particularly in Decentralized Finance (DeFi) ecosystems.



Centralized
e.g., traditional company

Decision-makers are known and have defined roles.



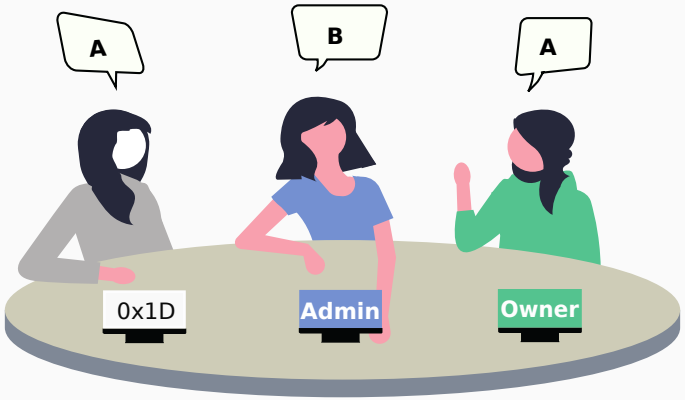
Decentralized
e.g., DAO

The pseudo-anonymous nature of accounts makes voting opaque.

Research Question

Previous studies have extensively documented the high concentration of governance token ownership, which affects voting rights.

In the recent legal case of *Tornado Cash DAO*, the suspected founder and developer faced arrest, and sanctions were imposed.



DeFi Governance

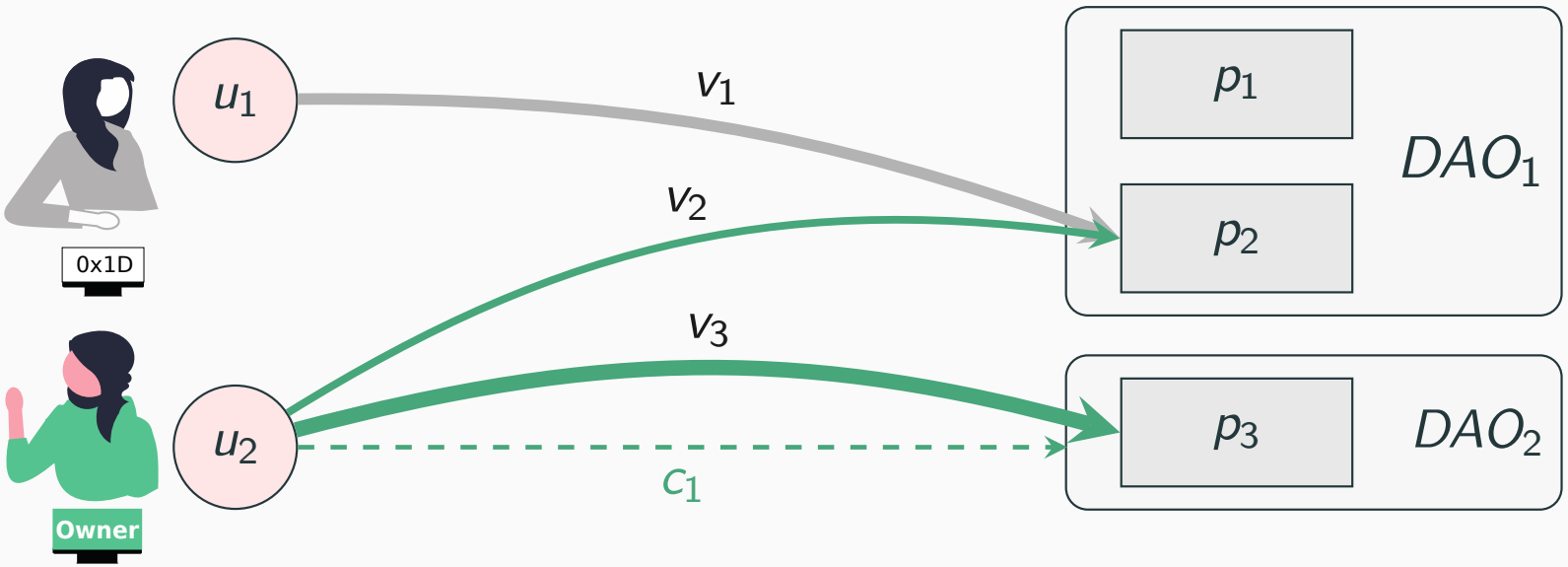
RQ2: What is the role of contributors in DAO voting?

Data and Method

We gathered data from the following sources:

- **Snapshot** voting data from Nov 2020 to Dec 2022; We derived 872 DAOs with $35k$ improvement proposals p and $5M$ votes v.
- **Ethereum** full archive node to acquire additional information.

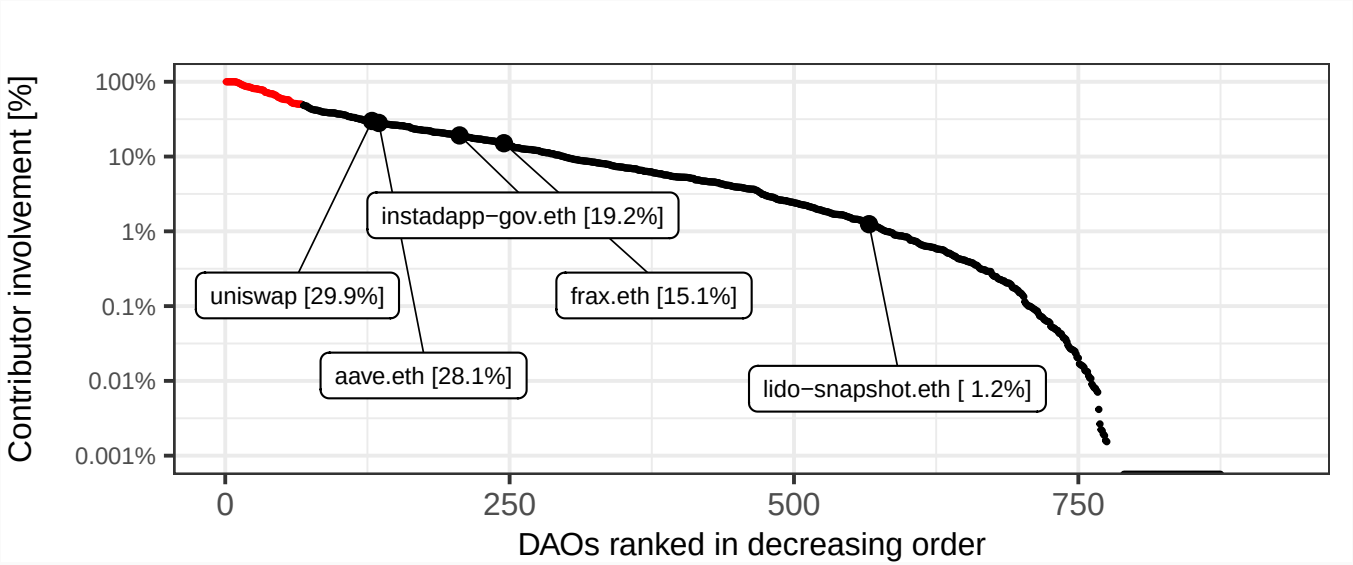
We identify $7k$ voters' **contributions** c to DAOs, by **owner**, **administrator** or **Developers**.



Results — Influence of Contributors on DAO Governance

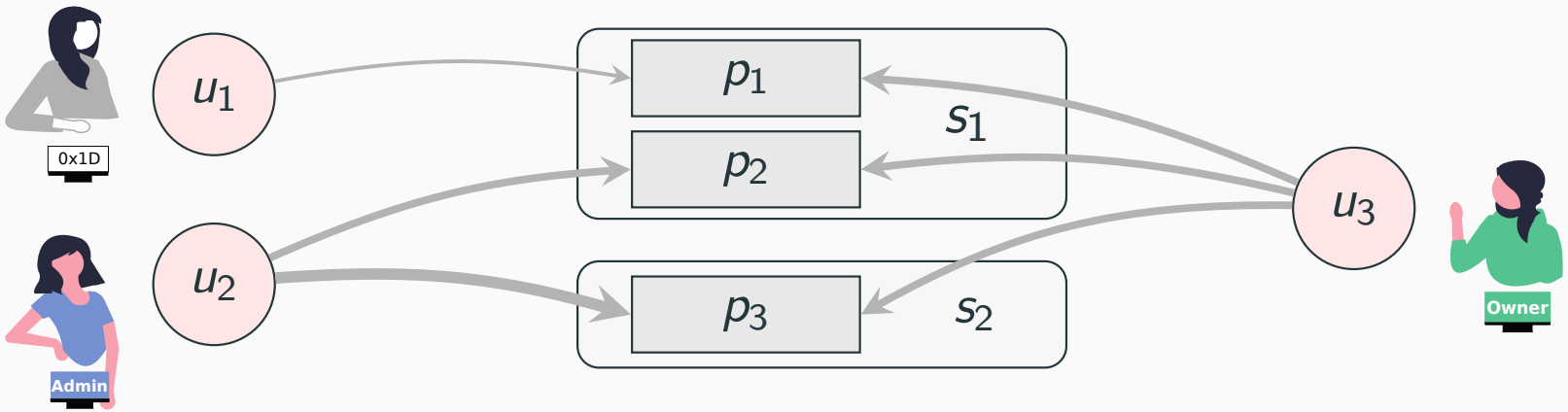
We analyze *contributor involvement* as the average share of voting power held by contributors in a given DAO space:

→ In 66 DAOs (•), contributors hold more than 50% of the voting power . These DAOs show a majority of voting power among contributors. Notably, some high-TVL dApps are highlighted (●).

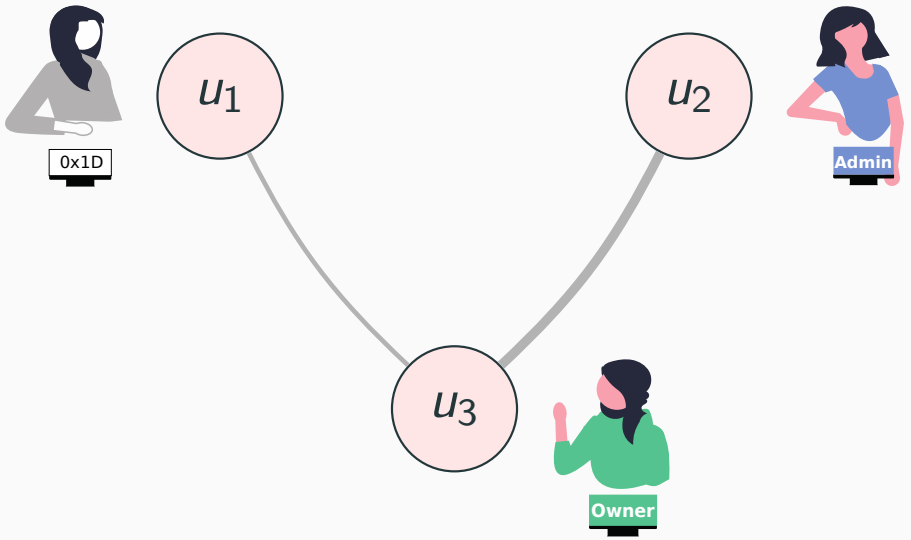


Illustrative example

DAO Governance Voting

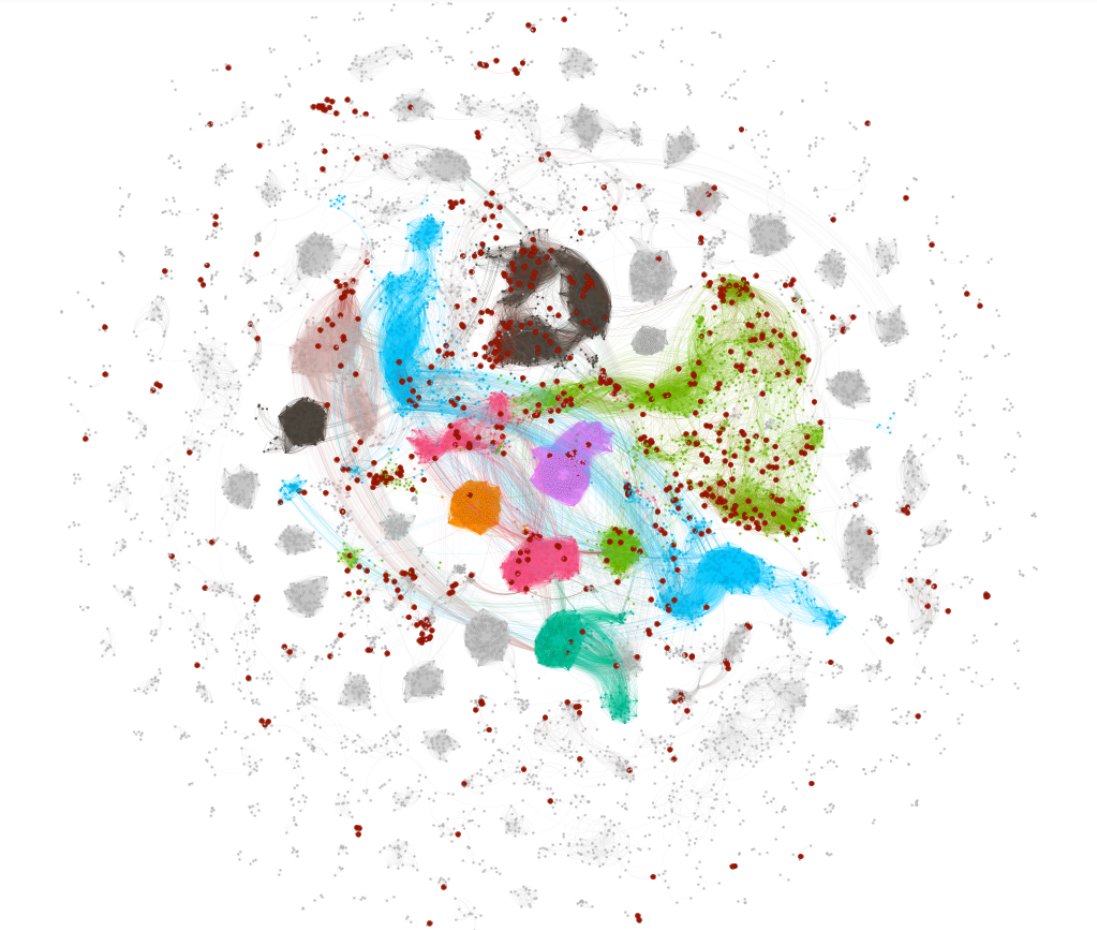


Co-voting Network



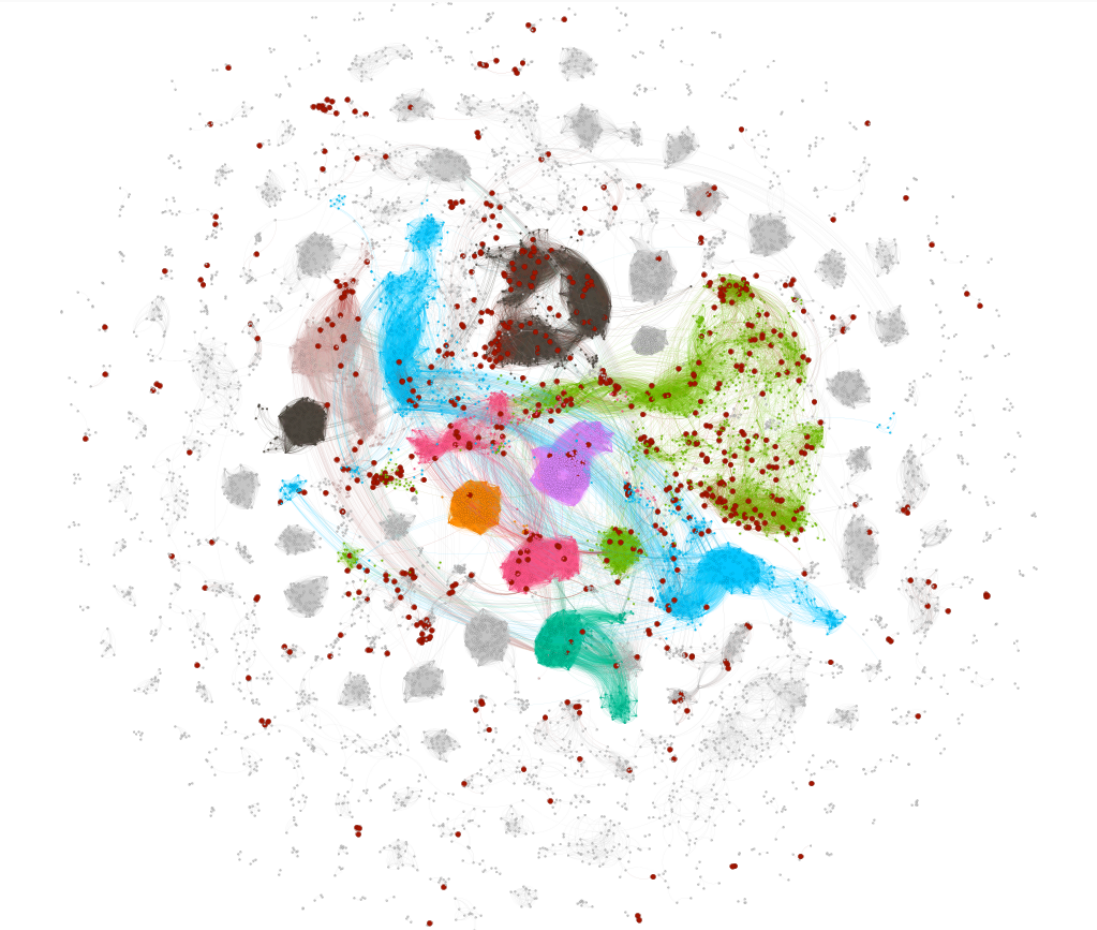
Network Communities

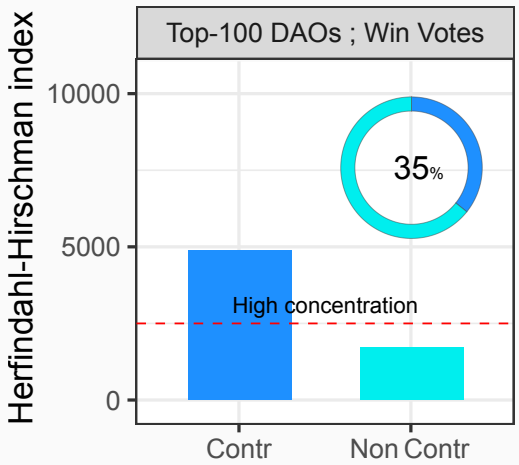
Analysis Focus: Sub-networks of winning votes in top-100 DAOs.



Network Communities

Analysis Focus: Sub-networks of winning votes in top-100 DAOs.





Main Findings

We analyze the role of contributors in governance structure of DeFi protocols:

- Contributors have, on average, a majority in voting power for 66 (7.54%) DAOs. In 178 (20.41%) DAO spaces, contributors of the same DAO decided on at least one proposal on their own.
- Contributors are highly concentrated in a few communities formed by co-voting patterns.
- We observed *majority shifts* in governance token ownership in 1202 (14.81%) out of 8116 proposals in the days preceding the votes.

Implications:

- Contributors have a high presence in the decision-making of DAOs: **evidence for inner power circles**.
- It **challenges the notion of decentralization**: relevant for regulatory discussions because it raises the questions of accountability of vested users.

Publications

Publications — Core

Core publications:

Complexity

Kitzler, S., Victor, F., Saggese, P., & Haslhofer, B. (2023). Disentangling decentralized finance (DeFi) compositions. ACM Transactions on the Web, 17(2), 1-26.

Governance

Kitzler, S., Balietti, S., Saggese, P., Haslhofer, B., & Strohmaier, M. (2024). The Governance of Decentralized Autonomous Organizations: A Study of Contributors' Influence, Networks, and Shifts in Voting Power. In Financial Cryptography and Data Security 2024.

Publications — Others

Other work within the thematic context:

Auer, R., Haslhofer, B., **Kitzler, S.**, Saggese, P., & Victor, F. (2024). The technology of decentralized finance (DeFi). Digital Finance, 6(1), 55-95.

Kitzler, S., Victor, F., Saggese, P., & Haslhofer, B. (2022, May). A systematic investigation of DeFi compositions in ethereum. In International Conference on Financial Cryptography and Data Security (pp. 272-279). Cham: Springer International Publishing.

Kitzler, S., Saggese, P., Diem, C., Bernhard, H., & Thurner, S. (2022, November). Systemic risk in decentralized finance (defi)-an investigation of smart contract interdependencies. In 11th International Conference on Complex Networks and Their Applications (pp. 233-235).

Carpentier-Desjardins, C., Paquet-Clouston, M., **Kitzler, S.**, & Haslhofer, B. (2023). Mapping the DeFi Crime Landscape: An Evidence-based Picture. *Accepted at Journal of Cybersecurity*

Luo, J., **Kitzler, S.**, & Saggese, P. (2024). Investigating Similarities Across Decentralized Financial (DeFi) Services. arXiv preprint arXiv:2404.00034.

Presenter:

Stefan Kitzler

kitzler@csh.ac.at

Thank you for your attention

References i


Ross Anderson, Chris Barton, Rainer Bölme, Richard Clayton, Carlos Ganán, Tom Grasso, Michael Levi, Tyler Moore, and Marie Vasek.
Measuring the changing cost of cybercrime.
2019.


Ata Assaf, Mehmet Huseyin Bilgin, and Ender Demir.
Using transfer entropy to measure information flows between cryptocurrencies.
Physica A: Statistical Mechanics and its Applications, 586:126484, January 2022.


Nguyen Phuc Canh, Udomsak Wongchoti, Su Dinh Thanh, and Nguyen Trung Thong.
Systematic risk in cryptocurrency market: Evidence from DCC-MGARCH model.
Finance Research Letters, 29:90–100, June 2019.


Yu-Lun Chen, Yung Ting Chang, and J. Jimmy Yang.
Cryptocurrency hacking incidents and the price dynamics of Bitcoin spot and futures.
Finance Research Letters, 55:103955, July 2023.


Shaen Corbet, Douglas J. Cumming, Brian M. Lucey, Maurice Peat, and Samuel A. Vigne.
The destabilising effects of cryptocurrency cybercriminality.
Economics Letters, 191:108741, June 2020.


Maya Dotan, Aviv Yaish, Hsin-Chu Yin, Eytan Tsytkin, and Aviv Zohar.
The Vulnerable Nature of Decentralized Governance in DeFi.
Technical report, The Hebrew University, August 2023.
arXiv:2308.04267 [cs] type: article.


ÖGET Emrah.
The effect of positive and negative events on cryptocurrency prices.
Ekonomi Politika ve Finans Araştırmaları Dergisi, 7(1):16–31, 2022.


L. Gudgeon, D. Perez, D. Harz, B. Livshits, and A. Gervais.
The decentralized financial crisis.
In *2020 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 1–15, 2020.


Campbell R Harvey, Ashwin Ramachandran, and Joey Santoro.
DeFi and the Future of Finance.
John Wiley & Sons, 2021.


Johannes Rude Jensen and Omri Ross.
Managing risk in defi.
In *5th Workshop on Managed Complexity*, 2020.


Seung Ah Lee.
Investigating the impact of cyber security attacks on cryptocurrency markets.
PhD Thesis, Macquarie University, 2022.


Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage.
A fistful of Bitcoins: characterizing payments among men with no names.
Communications of the ACM, 59(4):86–93, March 2016.


Fabian Schär.
Decentralized finance: On blockchain- and smart contract-based financial markets.
Federal Reserve Bank of St. Louis Review, 2:153–74, 2021.


Sam M. Werner, Daniel Perez, Lewis Gudgeon, Ariah Klages-Mundt, Dominik Harz, and William J. Knottenbelt.
Sok: Decentralized finance (defi), 2021.