arXiv:2305.17655v3 [cs.CR] 21 Apr 2024

Understanding Blockchain Governance: Analyzing Decentralized Voting to Amend DeFi Smart Contracts

JOHNNATAN MESSIAS*, MPI-SWS, Matter Labs, Germany
VABUK PAHARI, MPI-SWS, Germany
BALAKRISHNAN CHANDRASEKARAN, Vrije Universiteit Amsterdam, Netherlands
KRISHNA P. GUMMADI, MPI-SWS, Germany
PATRICK LOISEAU, Inria, FairPlay team, France

Smart contracts are contractual agreements between participants of a blockchain, who cannot implicitly trust one another. They are software programs that run on top of a blockchain, and we may need to change them from time to time (e.g., to fix bugs or address new use cases). Governance protocols define the means for amending or changing these smart contracts without any centralized authority. They distribute the decision-making power to every user of the smart contract: Users vote on accepting or rejecting every change.

In this work, we review and characterize decentralized governance in practice, using Compound and Uniswap—two widely used governance protocols—as a case study. We reveal a high concentration of voting power in both Compound and Uniswap: 10 voters hold together 57.86% and 44.72% of the voting power, respectively. Although proposals to change or amend the protocol receive, on average, a substantial number of votes (i.e., 89.39%) in favor within the Compound protocol, they require fewer than three voters to obtain 50% or more votes. We show that voting on Compound proposals can be unfairly expensive for small token holders, and we discover voting coalitions that can further marginalize these users.

1 INTRODUCTION

Blockchains transformed traditional and centralized sectors of great societal importance, such as banking and finance [3, 28, 67, 69], by providing a secure means of ensuring compliance via contracts, i.e., established agreements, in situations where participants cannot trust each other [63, 75, 86, 89]. Many prior work studied different types of security vulnerabilities that arise from incorrect implementations or unintended (or undesired) executions of smart contracts, particularly in the context of Decentralized Finance (DeFi) such as exchanges [3, 28], loans [67, 69], and auctions [33]. Few studies, if any, focused, however, on vulnerabilities that may originate in the design of the procedures to *amend*, i.e., change, smart contracts, and/or stem from the execution of these procedures in practice. In this paper, we focus on the *governance protocols* of smart contracts, which define the procedures and mechanisms by which smart contracts—which users have previously agreed upon—can be amended.

An appealing feature of the governance protocols is their decentralization, i.e., their independence from any central trusted authorities [3, 6, 8, 19, 55]. The power to propose and approve amendments to a smart contract in governance protocols rests with stakeholders of the smart contract. Users vote on the amendments, and the voting power of each voter is proportional to their stake in the protocol. The majority vote decides whether that amendment is approved or rejected. The protocols, furthermore, enhance transparency in voting by eschewing trusted election monitors and relying on, instead, on on-chain voting mechanisms [87].

The transparent decentralized governance of DeFi smart contracts stands in sharp contrast to opaque, centralized governance of crypto exchanges such as FTX [43, 64]. In the case of FTX, opaque decision-making by a small group of individuals resulted in a collapse in trust. This debacle,

*Main author: https://johnnatan-messias.github.io – Twitter: @johnnatan_me

Authors' addresses: Johnnatan Messias, MPI-SWS, Matter Labs, Germany; Vabuk Pahari, MPI-SWS, Germany; Balakrishnan Chandrasekaran, Vrije Universiteit Amsterdam, Netherlands; Krishna P. Gummadi, MPI-SWS, Germany; Patrick Loiseau, Inria, FairPlay team, France.

among others such as the crashes of Silicon Valley Bank [32] and Luna [47, 68], highlights the need for a mechanism that will allow *every* stakeholder to participate in critical decisions and engage in discussions in a *transparent* manner. The use of governance mechanisms by themselves does not guarantee, nevertheless, that all the potentially diverse interests of stakeholders are taken into account in deciding whether to approve any given amendment. Of crucial importance are how governance tokens (i.e., voting power) are distributed among the stakeholders, whether the token holders actively participate in the voting on amendments in practice, how controversial the amendment proposals are, and whether stakeholders form voting coalitions that result in marginalizing some voters. In practice, unequal or unfair distribution of governance tokens undermine the core objective of decentralization, potentially compromising the security of the governance protocol [40, 61, 74].

This work provides an in-depth analysis of the voting patterns, delegation practices, and outcomes of proposals in two widely used governance protocols: Compound [55] and Uniswap [3]. Since they record the votes cast transparently on a blockchain (i.e., uses on-chain voting), we conducted measurements studies to analyze the extent to which this voting is decentralized, i.e., how small or large are the set of voters that determine the outcomes for the amendments. Our goal is to thoroughly examine these protocols to better understand how their governance mechanism operates and identify potential areas for improvement.

1.1 Research questions

The challenge of achieving true decentralization in governance protocols is exacerbated by the concentration of voting power. When a minority of participants controls a significant majority of tokens, they can make decisions that primarily serve their interests, often to the detriment of others. Therefore, ensuring an equitable distribution of tokens becomes key in achieving decentralization within these protocols.

Below, we discuss the research questions addressed in this paper.

► **RQ 1**: *How frequently are amendments proposed and voted on in these protocols?*

This research question aims to investigate the activity level of the these protocols and its community engagement. Specifically, we seek to understand how frequently amendments are proposed and voted on in the protocol. Examining these aspects allows us to assess the level of participation and the extent to which the community actively contributes to improving the protocol.

► **RQ 2**: *What is the distribution of tokens among its participants?*

This research question aims to investigate the distribution of tokens among its participants. We aim to understand the size of the set of voters who determine outcomes for amendments and assess the decentralization of their tokens. This is crucial for proposing fairness in these protocols based on their token distribution.

► **RQ 3**: *What is the cost associated with casting a vote in these protocols?*

Voting in on-chain governance protocols involves transaction fees that vary based on network congestion. This research question explores the impact of voting costs on voter participation in these protocols. Understanding these costs provides insights into the fairness of the decision-making process and identifies potential barriers that may discourage certain participants from exercising their voting rights. For instance, if the voting cost is too high and voting power is concentrated among a few powerful voters, users may be reluctant to participate in voting. This can be explained from the perception that a handful of powerful voters can easily pass a proposal, making individual less-powerful voter seem less impactful.

► **RQ 4**: *What are the voting patterns of delegates, and do voters form coalitions?*

This research question analyzes the voting patterns of delegates in these protocols and investigates whether voters form coalitions. Coalition formation may lead to the marginalization of

certain voters, compromising the core principle of decentralization. Understanding the presence and impact of coalition formation provides valuable insights into decision-making dynamics among voters and helps mitigate the concentration of tokens or voting power within these protocols.

1.2 Contributions

More specifically, we summarize our contributions as follows

► ***Users actively vote on proposals:*** We characterize the Compound and Uniswap protocols' on-chain voting process, showing that they are active and regularly used, with a steady flow of proposals. For example, the majority of the proposals receive significant support in Compound: on average, 89.39% of votes are in favor.

► ***Casting a vote might be expensive to small players:*** We reveal a substantial variation in voting costs, from \$0.03 to \$294.02, with an average of \$7.88.[1] If we normalize the costs per vote by the count of tokens held by users, we obtain an average cost per vote unit of \$358.54. Voting costs can, hence, be *unfairly* expensive for small token holders, which has fairness implications for the decision-making process.

► ***Voting power is highly concentrated:*** We show that a small group of 10 voters holds a significant amount of voting power (57.86% and 44.72% of all tokens for Compound and Uniswap, respectively) and that proposals only required an average of 2.84 voters to obtain at least 50% of the votes. These observations strongly suggest that the voting outcomes may not reflect the preferences of the broader community.

► ***Powerful voters form coalitions:*** We discover potential voting coalitions among the top voters, which could further exacerbate concerns of voting concentration.

► ***Scientific reproducibility:*** To foster reproducible research and inspire research into other aspects of governance protocols, we plan to share our scripts and data sets via a GitHub repository.

2 DECENTRALIZED GOVERNANCE

Smart contracts underpin many DeFi applications today [3, 28, 33, 67, 69], and it is only natural to have a mechanism for updating these (software) contracts to fix bugs or evolve them over time to cater for new use cases [30, 56, 94]. If decisions concerning such updates are made in a centralized manner, e.g., by a regulatory body, or a cabal of developers or miners, it undermines users' trust in the applications that these contracts support. The updates could, for instance, be tailored to benefit the centralized regulatory body at the expense of others. Governance protocols address this issue by distributing the decision-making power among all the users of the application or smart contract being updated.

A governance protocol establishes rules and (transparent) mechanisms for changing smart contracts. It defines the required procedures for creating, voting on, and executing proposals to amend smart contracts. It facilitates users of a protocol (or, more aptly, *token holders* who hold one or more tokens of the protocol) to propose changes. The changes are then vetted by and voted by other users, and implemented only if the proposals receive the majority of favorable votes. The protocols also grant voting power to a user based on the number of tokens held by them (i.e., one token equals one vote), essentially capturing the user's stake and/or participation in the protocol. Some protocols such as Compound [55] and Uniswap [3] allow token holders who do not wish to exercise their voting power to delegate their voting power (i.e., tokens) to others. This delegation is a form of *liquid democracy*, where voters can participate in decision-making either directly by voting or indirectly by delegating their voting rights to others [12, 14, 17]. Governance protocols

[1] All costs are in US dollars, taking into account the exchange rate at the time of casting the vote.

Table 1. A comparison of voting mechanisms in decentralized governance protocols. *SC* stands for smart contract.

Protocol	*Type*	*Voting*	*Who can vote?*	*Delegation*	*Voting Aggregation*	*How proposals are implemented?*
AAVE [2]	Lending	on-chain	addresses with delegated tokens	yes	on-chain	on-chain via an SC call.
Balancer [10]	DEX	off-chain	stakers with locked tokens	yes (off-chain)	off-chain	via 6-of-11 multisig.
Compound [55]	Lending	on-chain	addresses with delegated tokens	yes	on-chain	on-chain via an SC call.
Convex Finance [25]	Yield Farming	off-chain	stakers with locked tokens	yes (off-chain)	off-chain	via 3-of-5 multisig.
Curve [27]	DEX	on-chain	stakers with locked tokens	yes	on-chain	on-chain through an SC call.
Maker Executive [59]	Stablecoin	on-chain	holders	no	on-chain	New Governance Contract requires more MKR staked than previous.
Maker Polling [59]	Stablecoin	on-chain	addresses with delegated tokens	yes	off-chain	Engineers at Maker create the governance contract based on the voting outcome.
Uniswap [3]	DEX	on-chain	addresses with delegated tokens	yes	on-chain	on-chain via an SC call.
1Inch [1]	DEX Aggregator	off-chain	stakers with locked tokens	yes	off-chain	via 7-of-12 multisig.
Ampleforth [5]	Stablecoin	on-chain	addresses with delegated tokens	yes	on-chain	on-chain via an SC call.
Rarible [70]	NFT	on-chain	stakers with locked tokens	yes	on-chain	on-chain via an SC call. However, a 3-seat security council has veto power over proposals that they deem malicious.

give every participant the right to propose, support, or oppose any proposal. They are, hence, crucial for ensuring absolute decentralization of applications running atop blockchains.

2.1 Types of Existing Governance Protocols

There are various smart contract applications that utilize decentralized governance protocols for decision-making, including those for lending, decentralized exchanges (DEXes), and stablecoins, among others. An example of such protocols can be found on the Ethereum blockchain, where a number of these applications are available. We have selected some of the most protocols that use decentralized governance for decision-making. Table 1 presents 11 protocols, including Maker Executive and Maker Pooling, which are part of the MakerDAO [59] stablecoin protocol responsible for the DAI token. These protocols use decentralized governance mechanisms, and we characterize them based on whether their votes are cast on- or off-chain, the delegation methods they use, how they aggregate the votes, and how the proposal outcome take effect.

In our work we focus on two established protocols providing decentralized governance: Compound [55] and Uniswap [3]. These are two leading governance protocols.

2.2 Voting Modalities

Proposals to change a governance protocol takes birth in the protocol's community forum. Community members suggest and discuss potential changes to the protocol in the forum and may even conduct an informal poll to gauge the community's support for a proposal. The proposer then either amends the proposal to incorporate the community's feedback and submit it for a formal vote, or simply abandon it. The formal voting on the proposal has two modes: *on-chain* and *off-chain* voting.

On-chain voting In this voting system, participants make all governance decisions via smart contracts on a blockchain. Under this system, participants cast a vote by issuing a transaction (and paying a fee for committing it) to the blockchain. The system allows only participants with at least a threshold amount of (governance) tokens to create a proposal, albeit any token holding participant can vote on that proposal. It executes the proposal on the blockchain only if it receives a significant number of votes in favor and reaches a *quorum*. This voting system thus facilitates making transparent and tamper-proof changes to the protocol. Decentralized governance protocols such as AAVE [2], Compound [23], and Uniswap [85] use on-chain voting.

Off-Chain Voting This system conducts voting on an off-chain third-party platform and, as a consequence, also establishes the rules for voting, aggregating votes, and determining the results off-chain. Protocols such as Balancer [10] and Convex Finance [25], for instance, use Snapshot [52] for off-chain voting. Snapshot stores the voting data on a P2P network called InterPlanetary File System (IPFS) [51]. The voting process does not require voters to pay any fees and (unlike on-chain voting) promotes participation across all participants, regardless of their level of participation or investment in the protocol. After the voting, this system uses a *multi-signature* contract to enact the off-chain voting outcome on the blockchain. Typically, an *n-of-m multisig* contract requires the transaction to be signed by at least n out of the m "admins" to be executed on-chain. The system trusts the multisig "admins", who are well-known in the community, to implement the voting outcome on the blockchain truthfully. The admins can also, however, refuse the proposal. In Convex Finance, for instance, the admins can choose not to execute a proposal if they deem it harmful, even if it had received the majority of votes and reached a quorum [26]. On-chain voting systems, in contrast, prevent such manipulation of voting outcomes by one or more individuals (after the voting process), since all governance decisions (e.g., voting and execution) happen on the chain.

Token delegations Some governance protocols (e.g., Compound, Uniswap, and AAVE) require a user to own a certain amount of governance tokens for casting a vote. These tokens can be obtained through airdrops (i.e., given away by the protocol) [61], purchased or traded on exchange. Users must delegate their tokens either to themselves or, if they do not wish to vote, delegate them to others. The ability to delegate voting power to others facilitates a form of liquid democracy; the token holder who delegates or sells their tokens to another loses their voting power. Delegations allow anyone to buy (or sell) tokens and gain (or lose) voting power instantly. Justin Sun, the founder of (stablecoin) TrueUSD [84], for instance, allegedly borrowed COMP tokens to create and vote for Compound proposal #84, resulting in a *governance attack* [83]; this proposal was, however, defeated. We discuss attacks on governance in details in §2.4.

Token "locking" Protocols such as Balancer and Curve [27] mandate that a user "lock" their tokens into a smart contract for a specified period of time to gain their right to vote. The user cannot withdraw the locked tokens until the lock-up period expires. The voting power of a user in this system is proportional to the amount of tokens locked as well as the lock-up period. In Balancer, for instance, a user receives 1 unit of voting power if they lock 1 token into the contract for 1 year, and only half when locking it for 6 months.

Continuous voting A few protocols (e.g., MakerDAO [59]) allow voters to change their votes at any time during the voting period. Users propose a protocol change by developing a new implementation via a smart contract. The new implementation is accepted if it receives more votes than the current one, i.e., the winning implementation must always receive the majority of the votes (or tokens). MakerDAO requires a user to deposit their (MKR) tokens into the (Maker) governance contract for casting a vote. The more tokens they deposit, the more voting power they obtain, and they vote for their desired implementation by specifying it as a protocol parameter in the smart contract. Since the voting process is continuous, if a user withdraws their MKR tokens from the

governance contract, their vote will no longer count towards the implementations for which they previously voted.

2.3 Real-world decision-making using Decentralized Governance

Interestingly, there are cases where decentralized governance has been applied to real-world decisions. For example, Compound has been utilized for real-world decision-making purposes, such as allocating grants to contributors or hiring an audit company to review the governance protocol through the Compound code [79]. For instance, on September 29, a bug was introduced in the Comptroller of the Compound Protocol through proposal #62 that allowed users to claim more COMP tokens than they were entitled to, resulting in a loss of $50 million worth of COMP tokens [58, 65]. The Compound community sought to hire, through the Compound governance protocol, a smart contract auditor to audit the protocol [79]. Three companies, ChainSecurity, OpenZeppelin, and Trail of Bits, posted their business plans for discussion and then created proposals via the Compound Governor. Voters were able to vote for their preferred proposal, and the winning proposal was eventually implemented. The losing proposals would have been cancelled by the community's multi-signature mechanism after the voting period ended, ensuring only one could pass.

OpenZeppelin was the only proposal to reach quorum and get the majority of votes to be implemented. They audited the Compound code, assisted proposers, participated in community discussions, and reviewed any new proposals formally created by the Compound community [66].

2.4 Attacks on Governance

A potential issue in the governance of blockchain networks is the concentration of governance tokens in the hands of a few participants, which can pose a threat to the protocol [62]. This issue manifested in Balancer [10], a decentralized exchange (DEX) running on top of Ethereum, where a user with large amount of governance tokens voted for decisions that were beneficial for the user but detrimental for the protocol [40]. When a minority holds a large portion of the tokens, decision-making power can become centralized, which conflicts with the goal of decentralization of governance protocols.

Yet another issue concerns many centralized exchanges that *hold* their users' tokens; they could potentially use these tokens for voting *without* their users' knowledge, compromising the integrity of the voting process [37, 74]. Alameda Research, a former cryptocurrency trading firm, which was affiliated with FTX, for example, voted on 8 proposals and even initiated three proposals (#13, #14, and #16) on Compound. Eventually, one of the proposals was executed. Their goal was to raise the collateral of WBTC from 0% to 40%, which allowed WBTC to be utilized for borrowing other assets [92]. This change may have been beneficial to Alameda Research as they were one of the biggest WBTC minters and held highly leveraged positions (i.e., borrowed money to invest even more) [45, 93]. To alleviate these concerns, centralized exchanges typically promise that they will not use their users' tokens to vote on their behalf [78]. While there is no guarantee that they will keep their promise, we can monitor their public wallet addresses to check if the exchange has delegated these governance tokens to another address, or whether they used the tokens for voting while they were stored on that exchange.

Governance protocols intend to eliminate (or at least minimize) centralized decision-making in blockchains. Their effectiveness in achieving that goal can, however, be compromised depending on how the tokens (i.e., voting power) are distributed. Our work evaluates whether governance protocols uphold their promise of decentralized governance of smart contracts, and, if they do not, investigates exactly how they renege on that promise.

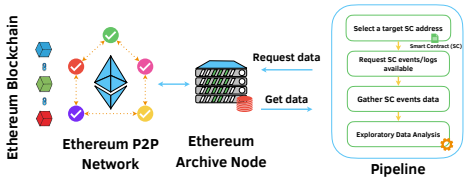


Fig. 1. *Overview of the data collection methodology and analysis.*

Table 2. Summary of events related to the Compound (COMP) and Uniswap (UNI) tokens that we gathered from the Ethereum blockchain.

Event name	*# of events*		*Description*
	Compound	*Uniswap*	
Approval	213,220	645,538	Standard ERC-20 approval event.
DelegateChanged	12,095	25,492	Emitted when an account changes its delegate. This means that the delegatee will receive voting power from the sender. Users can only delegate to one address at a time, and the number of votes added to the delegatee's vote count is equal to the user's token balance. The delegation of votes will take effect from the current block until the sender either delegates to a different address or transfers their tokens.
DelegateVotesChanged	75,820	118,096	Emitted when a delegate account's vote balance changes.
Transfer	1,886,618	3,715,442	Emitted when users/holders transfer their tokens to another address.

Table 3. Summary of events related to the Compound and Uniswap Governor contracts recorded on the Ethereum blockchain.

Event name	*# of events*		*Description*
	Compound	*Uniswap*	
ProposalCanceled	17	6	Emitted when a proposal is canceled.
ProposalCreated	133	29	Emitted when a new proposal is created.
ProposalExecuted	101	14	Emitted when a proposal is executed in the Time-Lock.
ProposalQueued	105	14	Emitted when a proposal is added to the queue in the TimeLock.
VoteCast	9500	18,084	Emitted when a vote is cast on a proposal: 0 for against, 1 for in-favor, and 2 for abstain.

3 DATA COLLECTION

To gather the data, we deployed an Ethereum *archive* node on a server with 64 cores (with a base clock frequency of 2.25GHz that can be boosted to 3.4 GHz), 256 MB L3 cache, 252 GB of RAM, and 21 TB of NVMe-based storage. The archive node took about 4 weeks—a relatively long time, though not unexpected—to fully synchronize with the Ethereum blockchain.

We used Web3.py [88], a Python library for interacting with Ethereum nodes, to query and retrieve the information that we need from the archive node (Fig. 1).

Smart-contract events Smart contracts in Ethereum can generate and dispatch *events* (or "logs") for signaling various types of activity (e.g., ERC-20 token transfers or state changes) within the contract. We used these logs to filter transactions that triggered specific events, e.g., sending, receiving, or swapping tokens. We also filtered and analyzed transactions that triggered events related to governance protocols tokens to track the evolution of each proposal, including when it was created, when users started voting, and when it was executed or canceled. We refer the reader to §B for low-level implementation details on how we filter and gather transactions that trigger events of interest.

Data set We gathered various details on tokens and governance contracts for both Compound and Uniswap since their inception. Our data collection consists of Compound data since Mar. 3, 2020 (block #9,600,000) and of Uniswap data since May 31st, 2021 (block #12,543,659) until Nov. 7, 2022 (block #15,917,000). We illustrate our methodology and data-analysis pipeline in Fig. 1. For Compound (Uniswap), we obtained 213,220 (645,538) *Approval* events, 12,095 (25,492) *DelegateChanged* events, 75,820 (118,096) *DelegateVotesChanged* events, and 1,886,618 (3,715,442) *Transfer* events (Table 2). We also collected various events (Table 3) related to their governance contracts for analyzing various aspects of the proposal creation and voting processes.

Inferring wallet address ownership Since an entity can control multiple wallet addresses in the blockchain (also known as Sybils [44]), identifying the ownership of these wallets helps in grouping together the accounts that are owned by the same entity. This task is complicated as owners are only identifiable if they choose to voluntarily make their identities public. To address this challenge, we combine wallet ownership information from two widely used data sources: Etherscan [35] and Sybil-List [81]. The former is a blockchain explorer that helps in identifying the top holders of various cryptocurrencies, and the latter, a Uniswap governance tool for discovering delegates addresses [80]. It uses cryptographic proofs for verifying wallet addresses voluntarily disclosed by the wallet owner. From these two data sources, we gathered the owners of 3191 public wallet addresses (refer §C). We used these addresses to infer the owners of 17 (51.52%) of the 33 unique addresses associated with proposal creation, 114 (3.42%) out of 3335 proposal voters, and 265 (0.13%) out of 210,598 token holders in Compound. By analyzing the top 10 most influential voters for each proposal, determined by the number of delegated tokens they possessed when casting their vote, we were able to infer the ownership of 67 (50.37%) of these 133 unique addresses. Finally, as an entity can control more than one address, we grouped the addresses we identified belonging to the same entity together to conduct our analysis.

4 AN ANALYSIS OF COMPOUND'S GOVERNANCE

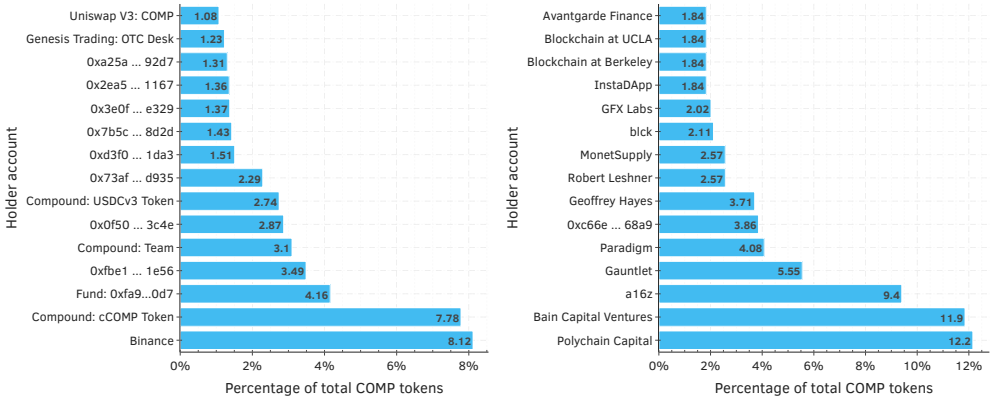
Compound [55] is a decentralized lending protocol that allows users to lend and borrow tokens or assets via smart contracts. Lenders earn interest (*yield*) by supplying liquidity to the protocol, while borrowers obtain tokens from the protocol and pay interest on the borrowed tokens.

Compound protocol has two versions of its governance contract: *Alpha*[2] and *Bravo*.[3] *Compound Governor Alpha*, the first version of the governance contract, was deployed on Mar. 4, 2020 (block #9,601,459) and was active until Mar. 28, 2021 (block #12,126,254). The improved version, *Compound Governor Bravo*, was deployed on Mar. 9, 2021 (block #12,006,099) and has been active since Apr. 14, 2021 (block #12,235,671). Brave introduced several improvements such as smart-contract upgradability (through proxies), a new option for voters to abstain from voting, and the ability for voters to state the reasons behind their voting choices through text comments attached to on-chain votes. The Bravo contract was proposed in proposal #42, and it received 1,438,679.86 votes from 59 voters—all but one vote were in favor of its implementation [50].

4.1 Control of Governance Tokens

The voting power of a user in Compound and Uniswap is proportional to the amount of (delegated) tokens held by that user—one token equals one vote. Below, we examine how these tokens are distributed over time among Compound and Uniswap participants.

[2]The Compound Governor Alpha was deployed at the Ethereum smart contract address 0xc0dA01a04C3f3E0be433606045bB7017A7323E38.
[3]The Compound Governor Bravo was deployed at the Ethereum smart contract address 0xc0Da02939E1441F497fd74F78cE7Decb17B66529.



(a) COMP tokens in circulation (b) COMP tokens delegated

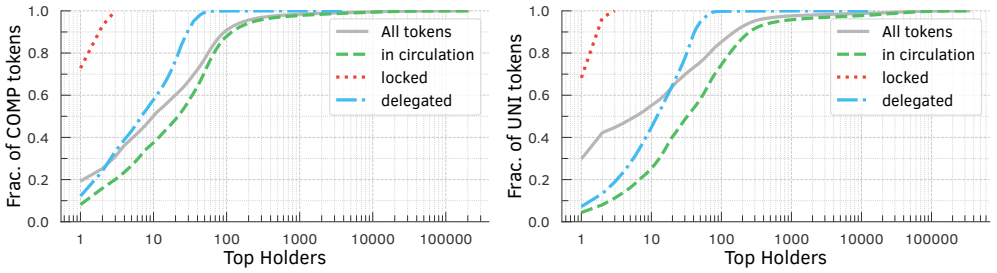
Fig. 2. Distribution of the top 15 COMP tokens per accounts on Nov. 7, 2022: (a) These accounts hold 43.83% (3.2 million) out of 7.3 million COMP tokens in circulation; (b) These addresses have 63.56% of all 2.7 million delegated tokens.

Distribution of token holding Initially, 42.15% of the total Compound supply (10 million COMP tokens) was allocated to liquidity mining, 23.95% to shareholders, 22.46% to the founders and the Compound team, 7.73% to the community, and 3.71% to future team members [21]. The public release of COMP tokens started only after proposal #7 was executed on June 15, 2020 [49]. This proposal enabled the continued distribution of COMP tokens to the protocol users over time. At the time of our analysis (Nov. 7, 2022), the 10 million COMP tokens were distributed among 210,573 accounts. The largest holder is *Compound Reservoir* with 19.24% (1,924,344.52) of the tokens followed by Binance (5.97% or 397,289.78 tokens) and cComp (5.73% or 572,723.77 tokens). The Compound Team holds 2.28% (228,061.62) and Compound Timelock 1.84% (184,258.39) of the tokens. We discuss further details of Uniswap in §5.

However, only 7.3 million COMP tokens are in circulation, and we characterize their distribution among a few top token holders in Fig. 2a. In calculating the tokens in circulation, we only included tokens that can be traded or exchanged between users. We excluded *locked* tokens from the Compound Reservoir, Comptroller, and Timelock contracts from our analysis [23, 48], which are *not* in circulation. These locked tokens require a governance proposal to be released, although some of them are released daily through the Comptroller as an incentive for users to use the protocol, by lending or borrowing these tokens.

We plot the cumulative distributions of all available COMP and UNI tokens along with the locked, delegated, and in-circulation tokens, i.e., the tokens available for users to buy, trade, or sell, in Fig. 3a and Fig. 3b, respectively. The top-15 accounts (in terms of the amount of tokens held) together account for 43.83% of all tokens in circulation in Compound (Fig. 2a) and for 33.27% in Uniswap (Fig. 15a). Binance [13], a popular centralized cryptocurrency exchange, leads this ranking in Compound with 8.12% of the available tokens. It is technically feasible for them to delegate these tokens to themselves to vote or propose changes to the protocol (refer §2.4), but Binance stated that it will not use these tokens to vote on behalf of its users [78].

4.1.1 Distribution of token delegation. Delegation is a prerequisite for voting (refer §2.2), and Compound and Uniswap allows its participants to delegate their voting rights to others. This ability enables users to delegate their voting power to individuals who share their interests, and allows participants with less voting power to pool their votes together and have a significant



(a) Compound (b) Uniswap

Fig. 3. CDF of the fraction of COMP (UNI) tokens held per account. The 10 million (1 billion) tokens available are shared among 210,573 (358,238) accounts, in grey. The dashed green line shows the distribution of the fraction of 7.3 million (563.9 million) accounting for 73.57% (56.38%) of the tokens in circulation held by 210,570 (358,235) accounts. The remaining tokens are locked and held by 3 accounts (in dotted red). The dash-dotted blue line shows the delegated tokens' distribution where 10 out of 4186 (14,922) accounts have 57.86% (44.72%) of all delegated tokens available.

voting impact. Users, however, can only delegate *all*, not a fraction, of their tokens. The protocol, nevertheless, enforces this limitation at the wallet address level. Users can own multiple wallet addresses and divide their tokens into them, thereby allowing them to delegate a subset of their tokens to others [4, 38]. To determine if delegated tokens are held by a few voters, we group together all inferred addresses (as discussed in §3) that belong to the same entity and then count the total number of delegated tokens held by each group. We observe, per Fig. 3, that delegated tokens are concentrated among few voters, and we show the distribution of delegated tokens across several top token holder accounts in Fig. 2b and in Fig. 15b. Out of 4186 COMP delegatee accounts (or accounts with voting rights), the top 50 (1.19%) hold 99.23% of all delegated tokens, giving them significant decision-making power when voting on proposals. Similarly, in Uniswap, the top 50 (0.34%) hold 94.73% of all UNI delegated tokens. On Nov. 7, 2022, Polychain Capital held the most COMP delegated tokens, with 12.15% (330,986.09) followed by Bain Capital Ventures with 11.85% (322,763.87) and a16z with 9.40% (256,046.13). These three addresses together held 33.41% (909,796.10) of all the 2,723,123.73 delegated tokens in our analysis.

We note that only approximately half of the tokens in circulation are delegated. If we investigate token delegation among the top token holders in Fig. 2a, we observe that many of them are crypto exchanges (e.g., Binance and Uniswap V3:COMP) that do *not* delegate their tokens. This assuages concerns that crypto exchanges that hold their users token could abuse their users' trust (§2.4).

4.2 Voting on Governance Proposals

To propose changes to the Compound protocol, an address must have at least 25,000 COMP tokens delegated to it to create a proposal.[4] However, as of Sept. 18, 2021, proposal #60 introduced an exception to this rule, allowing also whitelisted-addresses to create proposals even if they do not have 25,000 delegated tokens [16].

Per Fig. 4, when a proposal is created in Compound, there is an approximately 2-day voting delay period (or 13,140 blocks) that is used to allow the community to discuss the proposal before the voting period begins. During the approximately 3-day voting period (or 19,710 blocks), voters can cast their votes. In order for a proposal to be executed, it needs to meet two requirements. Firstly, it must receive a minimum of 400,000 votes in favor of the proposal. This number corresponds to 4% of the total supply and is known as the *quorum*. Secondly, the majority of the votes cast must

[4]Prior proposal 89, an address should have at least 65,000 delegated tokens to create proposals [7].

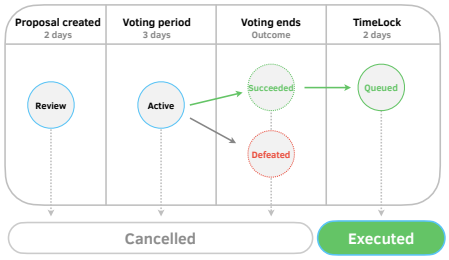


Fig. 4. *The lifecycle of a Compound proposal until it gets executed lasts 7 days.*

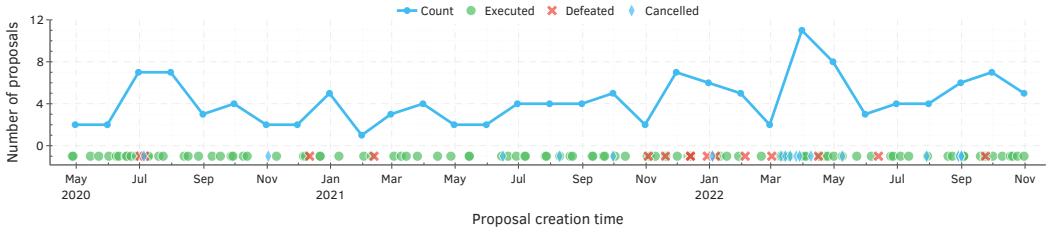


Fig. 5. *Monthly number of Compound proposals created and their final outcome.*

be in favor of the proposal. The number of votes each voter has is determined by the number of delegated tokens they held in the block before the voting period began. This prevents voters from changing their delegated tokens after the voting has begun, which could potentially lead to sudden changes in the outcome of the election. After a proposal is approved, it is placed in the *TimeLock* for a minimum period of 2 days before it can be implemented (or executed) [23]. A proposal can be cancelled at any time by the proposer prior to its execution, or by anyone if the proposer fails to maintain at least 25,000 delegated tokens.

In total, 3335 Compound voters cast their votes through 9500 transactions with 8769 (92.31%) for in-favor votes, 644 (6.78%) for against votes, and finally 87 (0.91%) for abstained votes. Most of the voters (51.36%) only voted for 1 proposal. 1% of participants voted for at least 26.66 proposals. On average, participants voted on 2.85 proposals with a *standard deviation (std.)* of 5.23. The address *0x84e3*$\cdots$*5a95* voted on the maximum number of proposals (100), followed by *MonetSupply* and *blck* who voted on 96 and 88 proposals, respectively.

4.2.1 Creation of proposals. In total, 33 Compound proposers created the 133 proposals. Of these proposers, 16 (48.48%) created one proposal, while 10% of them created at least 8 proposals. The average number of proposals created per proposer is 4.03 proposals, with a std. of 5.27 and a median of 2. The highest number of proposals was created by *Gauntlet*, who created 24 proposals, followed by *blck*, who created 20 proposals.

The maximum number of proposals were created in Mar. 2022, 11 proposals created (from #86 to #96). However, of those, only 5 were executed, as 1 was defeated and 5 were cancelled (see Fig. 5). Proposals were submitted, on average, every 6.95 days (std. of 6.41), with a median of 5.08 days. The shortest and longest interval between proposals was 0 and 31.14 days, respectively. Proposals typically take 1.64 days (std. of 0.72) to reach the quorum (Fig. 19 in §E).

Compound is actively and regularly used, continually receiving a steady flow of proposals. We believe that governance protocols gain more traction in the future for transparent decision-making in real-world applications (refer §2.3).

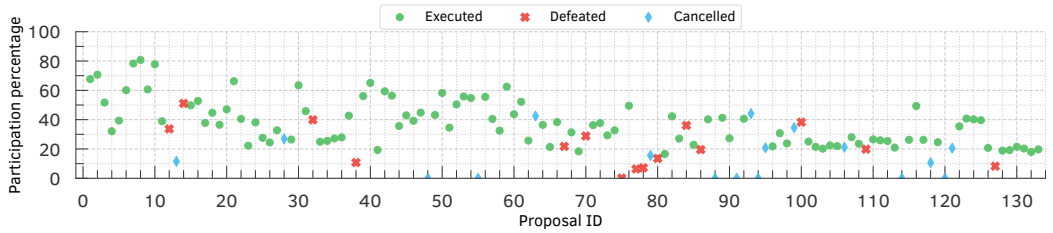


Fig. 6. *Compound's voting participation per proposal in terms of delegated tokens used from all delegated tokens available.*

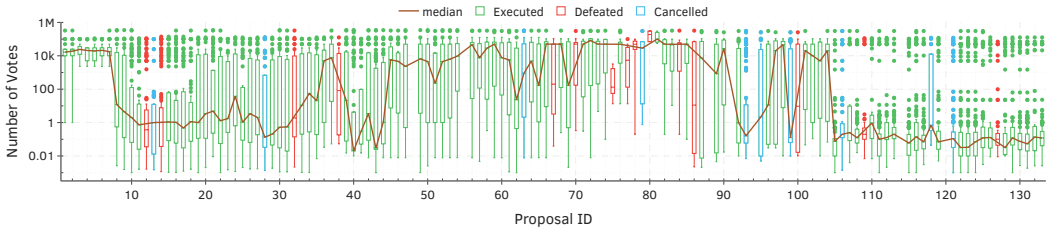


Fig. 7. *Compound's distribution of voting power by voter per proposal. We consider a cutoff of 0.001 votes.*

4.2.2 Participation in voting. Next, we computed the voting participation per proposal (see Fig. 6). This metric is calculated by dividing the number of votes (or delegated tokens) cast on a proposal by the total number of delegated tokens eligible to vote on that proposal at the start of the voting period. This is a crucial measurement as it shows the proportion of all delegated tokens that are used in the governance election process by the voters on proposals. Also, protocols with low voter turnout are more susceptible to vote-buying, as non-voting users may sell their voting rights to others [29]. Our results show that the average voter turnout is 33.25% (std. of 17.61%), the median is 32.10%, and the maximum 80.80%. Based on Fig. 6, we observe higher voting participation for early proposals compared to recent ones, likely due to the limited availability of tokens to a select few in the beginning.

On average, the 133 proposals had 71.43 voters participating in their election, with a std. of 98.97 voters. 50% of the proposals received votes from 38 voters, while the numbers of voters varied between 0 (when proposals are cancelled before the voting period begins) and a maximum of 619, as seen in proposal #111. This particular proposal received a total of 686,289.04 votes from 615 voters in favor, 3 against, and 1 abstention. The next proposals with higher number of voters are proposals #115 and #105 that received votes from 579 and 404 voters, respectively.

Next, we analyze the 9500 events triggered by voters during the voting process. Of these events, 1732 (18.23%) were votes cast by voters who did not have any delegated tokens available, resulting in zero voting power or *useless vote*. Although this is allowed by the protocol, it does not count for or against a proposal. However, it shows support for the proposal, as these voters still participate in the election despite not having any delegated tokens available. The average number of votes cast (or tokens used to vote) was 10,961.73, with a std. of 39,212.17 and a median of 0.1, ranging from 0 to 345,067.49 as shown in Fig. 7.

Additionally, there is a financial cost involved when casting a vote due to the on-chain transactions required to cast votes. To determine these costs, we collected the relevant transactions from the Ethereum blockchain and analyzed the fees paid by voters to issue the transactions and cast their votes. We report the voting cost in US dollars, using the ETH-USD Yahoo Finance data feed [91] exchange rate at the time the transaction was included in a block. In total, voting for the 133 Compound proposals, voters paid $74,865.74. The average voting cost per proposal is $7.88 with a

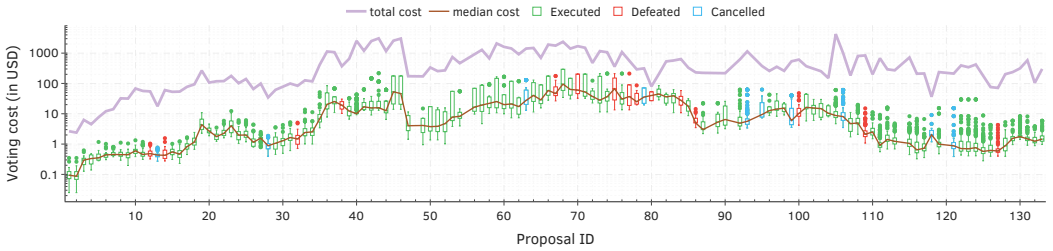


Fig. 8. *Compound's voting cost distribution per proposal. On average, casting a vote costs $7.88 with a std. of $22.29.*

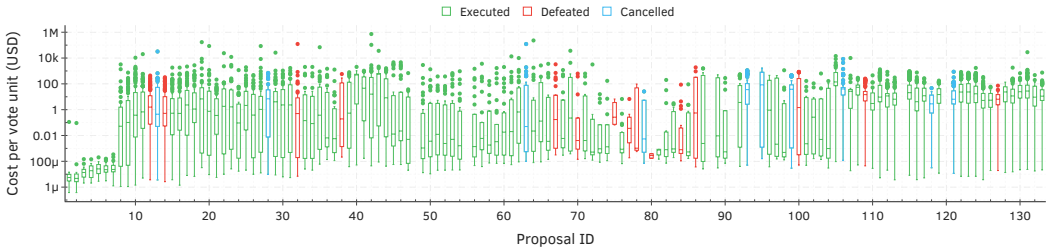


Fig. 9. *Voting cost distribution normalized per the voting power in Compound. We consider a cutoff of* 10^{-6} *votes.*

std. of $22.29. The median voting cost is $1.48 with a range from $0.03 to $294.02. Fig. 8 shows the voting cost distribution per proposal. We also computed these metrics at proposal level, on average, each proposal costed $594.17 with a std. of $745.62 and a median of $291.92. The cost ranges from $2.39 to $4247.25.

Voting on proposals can, hence, present a significant cost barrier, especially for voters with relatively few tokens. In such cases, the cost per token vote (or vote unit) may be too high compared to those with a higher number of delegated tokens. To better understand this, we normalized the cost of casting a vote by the number of votes cast (measured by the total number of delegated tokens available to voters' addresses). For this analysis, we focused on voters who cast at least 10^{-6} votes in any proposal. As shown in Fig. 9, some voters faced prohibitively high costs per vote unit. For example, the cost per vote unit has a mean of $358.54 and a std. of $9334.73, indicating a highly skewed distribution. However, half of the voters faced a cost per vote unit of only $6.69.

Our results also show that, for 99 executed proposals, the average number of voters required for a proposal to reach the quorum and pass was 3.25, with a std. of 1.65. The median number of voters required was 2, and the range of voters required varied from 2 to 8. This sheds light on how centralized these delegated tokens are distributed among a few participants, where for half of the proposals only 2 voter casting their votes would be enough to pass (or execute) a proposal.

Furthermore, we analyzed the number of voters needed for proposals to reach 50% of the total votes cast. Out of 133 proposals, we excluded 7 proposals that were cancelled before the voting period, leaving us with 126 (94.74%) proposals for analysis. On average, those proposals required 2.84 voters with a std. of 0.97 and a median of 3 voters. The minimum and maximum number of voters were 1 and 5, respectively. This again suggests that the token distribution is concentrated among few voters who hold a high voting power. Fig. 20 in §D shows the cumulative voting power for the top 10 most powerful voters for each of these 126 proposals in our data set.

4.2.3 Margin of victory/defeat. During the analyzed period, 133 proposals have been created. Of these, 17 were cancelled and 15 defeated, leaving 101 (75.94%) executed proposals. Fig. 10 shows the percentage of in-favor, against, and abstain votes for Compound each proposal. The majority of the

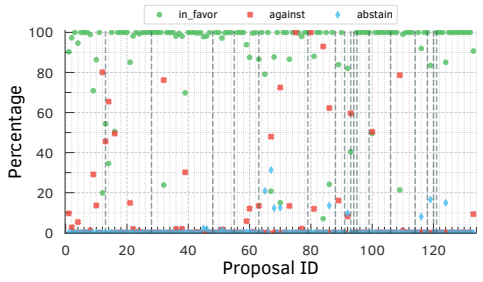


Fig. 10. *Percentage of in-favor (in green), against (in red), and abstain (in blue) votes for each Compound proposal, 15 (11.28%) proposals were defeated, and vertical lines represent 17 (12.78%) cancelled proposals.*

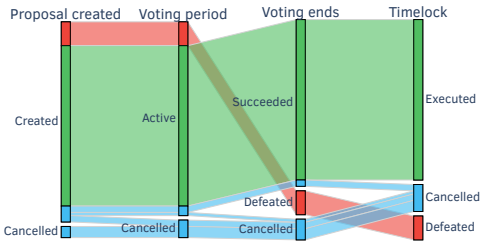


Fig. 11. *Summary of the outcome of 133 Compound proposals at each stage of their lifecycle. There are 101 proposals executed (in green), 15 defeated (in red), and 17 cancelled (in blue).*

proposals received significant support from the voters. On average, proposals received 89.39% of the votes in favor, with a std. of 23.98% votes and a median of 99.99%. We highlight the proposals' outcome at each stage of their lifecycle in Fig. 11. Our analyses show that 7 (5.26%) out of 133 proposals were cancelled right after they were created and, therefore, they had not reached the *Voting Period* meaning they were not available for voting. Next, 4 proposals were cancelled before the *Voting Ends* stage, meaning they were pulled out before the election finished. 2 were also cancelled after they succeeded in the election (after the *Voting Ends* stage) but before they were queued in the *Timelock*. Further, 4 proposals were cancelled when in the *Timelock*. These proposals account for 6 cancelled proposals after they successfully passed, which could indicate a lack of community consensus [77]. Finally, 101 (75.94)% proposals were successfully executed. We report the results for Uniswap in Fig. 17 in §5. Further, we gathered data from Messari [60] to categorize the executed Compound proposals and report their importance level in §4.3. In §A we also discuss the temporal dynamics of voting.

4.3 Proposals Categorization

In this section, we explore the importance of each type of proposal that have been implemented, examining their impact on the Compound protocol. Specifically, we explore whether these proposals mainly focus on adjusting parameters or addressing security concerns.

To this end, we gathered data from Messari [60] to determine the categories, subcategories, and the level of importance associated with each Compound proposal. Fig. 12 shows the distribution of 101 executed Compound proposals across different categories and subcategories. We show the degree of importance for each proposal according to Messari divided into "low", "medium", "high", and "very high". As a result, a few proposals categorized as "Parameter Change" and "Security" demonstrate a high level of importance. Furthermore, proposals with the highest level of importance are found within the "Security" category, specifically within the "Mining and Validation" subcategory. This refers to the proposal 64 that was created to fix a bug introduced by proposal #62.

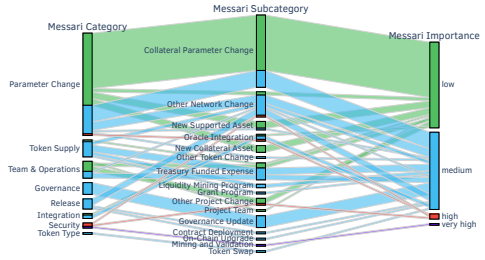


Fig. 12. Categorization of executed Compound proposals. Most of the proposals (60.4%) are related to "Parameter Change". We also show the importance level (low in green, medium in blue, high in red, and very high in purple color) for each proposal according to Messari [60].

The majority of the proposals (61 proposals, accounting for 60.4%) are related to "Parameter Change" followed by "Team and Operations" and "Token Supply" accounting for 10 (9.9%) each, and "Governance" with 7 (6.93%) proposals. According to the level of importance reported by Messari, out of the total of 101 executed proposals, 51 proposals (50.5%) are classified as low importance, 46 proposals (45.54%) as medium importance, 3 proposals as high importance, and 1 proposal as very high importance.

4.4 Voting patterns of delegates

In this section, we analyze the formation of coalitions among voters, where they cast their votes as a group. This analysis is crucial because such behavior may compromise the security of the governance protocol. Specifically, instead of expressing their individual opinions on a proposal, voters may choose to mimic the votes of their peers. The transparency of the Ethereum blockchain used for voting in Compound allows anyone to view the addresses of voters and their corresponding votes (e.g., their voting power and voting preference) during the election process, potentially facilitating this behavior. As a result, exploring the possibility of coalition formation could provide valuable insights into the decision-making patterns of voters. Fig. 13 shows a heatmap of how each of the top 15 voters cast their votes across all 133 proposals in our data set.

We use cosine similarity to quantify how similar the voting patterns of different voters are. Cosine similarity calculates the similarity between two vectors by determining the cosine of the angle between them [76, 90]. It is useful in the context of voting because it allows us to compare voting patterns and determine whether and which voters vote for the same proposals. The cosine similarity value ranges from -1 to 1, with a value of 1 indicating a high degree of similarity.

Our analysis shows that the top 3 voters (i.e., 0x84e3$\cdots$5a95, MonetSupply, and blck) have a strong cosine similarity in their voting behavior when casting a vote in favor of a proposal, meaning that they cast their votes similarly (see Fig. 14). Moreover, Gauntlet, Dakeshi, Robert Leshner, and Arr00 also show a strong similarity with 0x84e3$\cdots$5a95. We also analyzed the voting similarity when voters cast a vote against a proposal. Blockchain at Michigan and Blockchain at Berkeley have the highest cosine similarity with 0.73 followed by blck and Dakeshi with 0.67. These results suggest that these voters have similar voting patterns when indicating their opposition to a proposal. On the other hand, we could not make definitive conclusions regarding abstained votes as they are infrequent: only 87 (0.91%) out of 9500 votes.

5 AN ANALYSIS OF UNISWAP'S GOVERNANCE

In this section, we provide more details into the Uniswap and its governance protocol. Uniswap [3] is a decentralized exchange (DEX) platform that enables users to trade one token for another. In addition, users can add liquidity to Uniswap and earn interest based on the amount they provide.

Fig. 13. *Votes cast by the top-15 Compound voters. In-favor votes are in green, against in red, and abstain in blue color.*

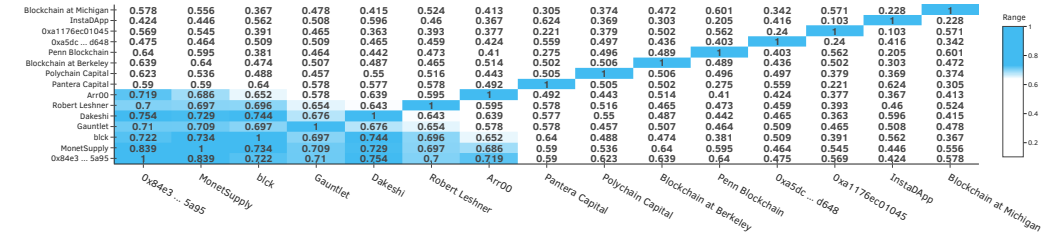


Fig. 14. *Cosine similarity of the top-15 Compound voters voting in-favor a proposal.*

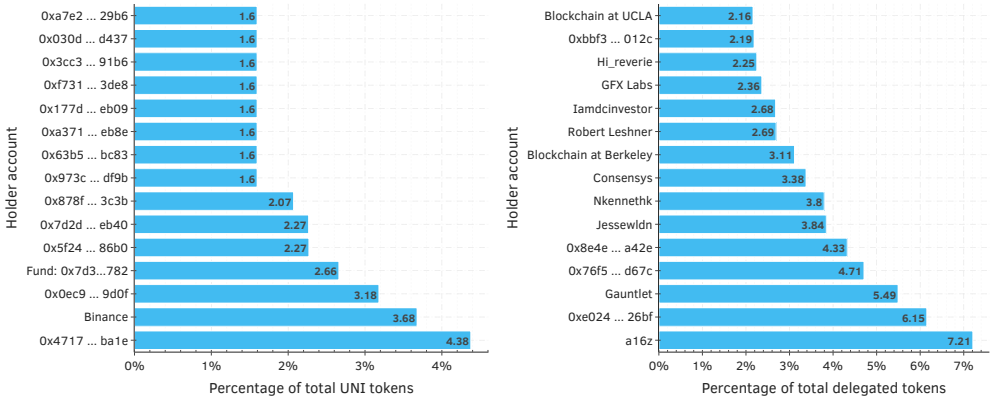
The Uniswap token (UNI) is an ERC-20 token that allows its holders to transfer UNI between addresses. Similarly to Compound, with Uniswap, holders can also participate in the Uniswap Governance Protocol by proposing changes and voting on proposals. Uniswap Governance is derived from Compound Governance Alpha and Bravo (refer to §4), and therefore shares similar features. For example, token holders must delegate their tokens to themselves or other addresses in order to vote. Each delegated token counts as one vote. Similar to Compound, participants can increase their voting power by holding multiple tokens.

The Uniswap protocol also has two versions of its governance contract. Alpha[5] and Bravo.[6] Uniswap Governor Alpha was deployed on May 31st, 2021 (#12,543,659) and is the first version of the governance contract, and it was active until March 20th, 2022 (#14,422,934). Uniswap Governor Bravo was deployed on August 20th, 2021 (#13,059,157) and is an improved version of the Alpha contract, and it is active since August 30th, 2021 (#13,129,516).

We gathered transaction and events data from our Ethereum archive node regarding Uniswap since its conception. Table 2 and Table 3 show the data set description we gathered from our node that was used in the analysis for the Uniswap (UNI) token and the Uniswap Governance protocol, respectively.

Uni tokens distribution Uniswap's initial token distribution consisted of 1 billion UNI tokens. 60% of these tokens were allocated to the community, 21.27% were given to Uniswap's team, 18.04% were allocated to investors, and 0.69% were set aside for advisors [22]. At the time of our analysis, however, there are 1 billion UNI tokens held by 358,238 accounts (see Fig. 3b). The largest holder is *Uniswap V2: Uni Timelock* with 29.8% (29,756,767.79) of the tokens followed by Uniswap Treasure Vester (12.5% or 124,945,829.21 tokens). Per Fig. 15a, Binance [13], is the second-largest holder of Uniswap tokens in circulation. Similar to Compound, we also observed, per Fig. 3b, that the

[5]The Uniswap Governor Alpha was deployed at the Ethereum smart contract address 0xC4e172459f1E7939D522503B81AFAaC1014CE6F6.
[6]The Uniswap Governor Bravo was deployed at the Ethereum smart contract address 0x408ED6354d4973f66138C91495F2f2FCbd8724C3.



(a) UNI tokens in circulation (b) UNI tokens delegated

Fig. 15. Distribution of the top 15 UNI tokens per accounts on Nov. 7, 2022: (a) These accounts hold 33.27% (187.61 million) out of 563.92 million UNI tokens in circulation; (b) These addresses have 56.37% (117.27 million) of all delegated tokens.

Uniswap delegated tokens are concentrated among few voters. We also show the distribution of delegated tokens across several top token holder accounts in Fig. 15b.

Proposal Creation and voting cast Uniswap proposals were submitted, on average, every 16.81 days (std. of 22.62), with a median of 5.52 days, as seen in Fig. 16a. The shortest and longest interval between proposals was 0 and 80.98 days, respectively. During August and September 2021, the largest number of proposals, totaling 10, were generated. It is noteworthy that a significant proportion of these proposals were initiated by the Uniswap Governor as initial proposals, with support levels ranging from 2.1 to 2.8. These proposals did not receive any votes and, are also not documented on the Uniswap webpage [53]. Upon conducting a further analysis, it was observed that the "target" field within their proposals has an Ethereum *null address* (i.e., 0x0). This means that, even in the event of these proposals passing, no modifications would be introduced to any contracts. The inclusion of these proposals seems to be a preemptive measure, possibly aimed at preventing conflicts with proposal numbers in the Governor Alpha contract. However, we could not verify that.

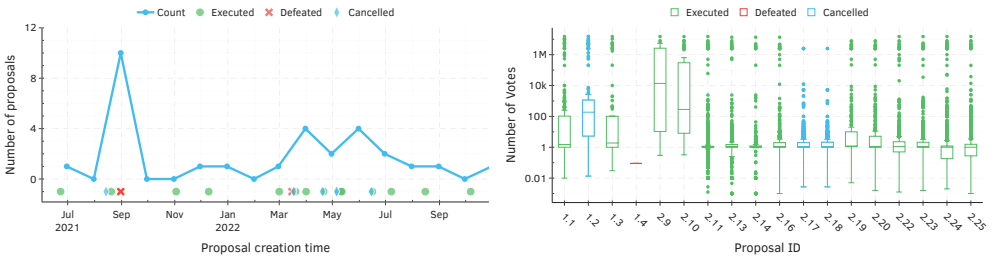
At the time of our analysis, from the total of 29 proposals, 14 (48.28%) were executed, 9 (31.03%) were defeated, and 6 (20.69%) cancelled, as show in Fig. 17. The executed proposals were approved with high percentage of votes supporting the proposal.

Finally, we also report the Uniswap's distribution of voting power by voter per proposal in Fig. 16b. The average number of votes cast (or tokens used to vote) was 56,923.91, with a std. of 614,598.36 and a median of 1, ranging from 0 to 15,000,491.54.

6 RELATED WORK

There is rich literature on decentralized governance and social contracts, and on decentralized autonomous organizations (DAOs). We review prior efforts that are most relevant to our work below.

Decentralized Governance and Social Contracts Prior work have studied the potential of blockchain-based (decentralized) governance for replacing centralization in traditional applications and services. Atzori *et al.* discussed, for instance, the extent to which blockchain-based governance can mitigate or replace the centralized and hierarchical societal structures and authorities [8]. Reijers *et al.* examined the relationship between blockchain governance and social contract



(a) (b)

Fig. 16. (a) Monthly number of Uniswap proposals created overtime. (b) Uniswap's distribution of voting power by voter per proposal. For better illustration, we consider only votes that are bigger than 0.001 votes.

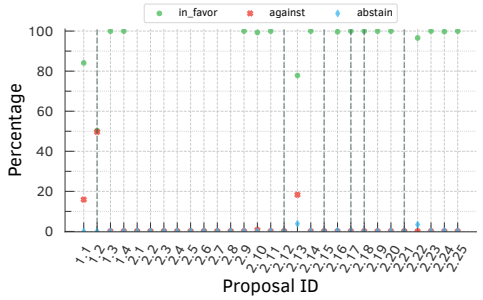


Fig. 17. *Percentage of in-favor (in green), against (in red), and abstain (in blue) votes for each Uniswap proposal, 9 (31.03%) proposals were defeated, and vertical lines represent 6 (20.69%) cancelled proposals.*

theory [71]. They analyzed the political implications of the blockchain technology and how it follows or deviates from the governance principles established by philosophers such as Thomas Hobbes [42], Jean-Jacques Rousseau [73], and John Rawls [18]. Chen *et al.* presented the trade-offs between decentralization and performance [19]. Arruñada and Garicano suggested new forms of "soft" decentralized governance to surpass traditional centralized governance structures [6]. Zwitter and Hazenberg conducted a comprehensive review of governance theory and proposed a re-conceptualization of the term governance that is tailored to DAOs [95]. These prior work provide valuable insights into decentralized governance structures, albeit they neither confirm the extent to which their (theoretical) observations hold in real-world implementations nor characterize the behavior of governance protocols deployed today.

Decentralized Autonomous Organizations (DAOs) Several prior studies analyzed the governance structures of DAOs [9, 11, 31, 41, 72, 82]. Hassan and De Filippi analyzed what DAOs constitute and discuss their key traits [41]. Rikken *et al.* identified various political challenges in governance of blockchains [72]. Beck *et al.* [11] presented a case study of a DAO in Swarm City [20], a decentralized commerce platform. A recent work categorized the governance of several blockchains such as Bitcoin, Ethereum, Tezos, Polkadot, and some governance protocols like Uniswap [3], MakerDAO [59] and Compound [55] into different types [46]. These invaluable prior work do not, nevertheless, empirically examine the data on existing DAOs to characterize how users interact with on-chain governance smart contracts.

There are three works closely related to ours [36, 38, 77]. Their findings agree with our own, e.g., they too found a high concentration of token delegation among a small number of users. Similarly, they also showed that the largest token holders are more active in voting, further exacerbating the centralization problem. However, while they analyzed voting participation and the cost of voting on

the blockchain for more than 10 DAOs, our study presents a comprehensive and in-depth analysis focused on Compound and Uniswap. Specifically, our analysis reveals the complete life cycles of proposals, highlighting how voting behavior evolves over time for different proposals. We also examine token ownership in detail revealing among which entities the tokens held are concentrated as well as how delegations (by individual entities) affect the concentration of tokens. Finally, we discover a vast inequality in voting costs among the token holders and present its implications for decentralized governance.

7 CONCLUDING DISCUSSION

In this work, we analyzed data from the Ethereum blockchain related to Compound and Uniswap, two widely used smart contracts. Our analysis centers on their decentralized governance protocols, with a particular focus on amendments to their contract. We found that the Compound contract is being actively amended—token holders continuously propose amendments that are then voted on by other token holders. We observed a striking concentration of tokens (be it in terms of their ownership or their delegation or their voting participation) in the hands of a few participants for both Compound and Uniswap, which raises serious concerns about the extent to which governance is decentralized in practice. For instance, our analysis showed that, on average, only 3.25 voters were needed for the proposals to reach quorum and pass in Compound, and only 2.84 voters were needed to reach 50% of the total votes. Our analysis also highlights issues with the Compound use of on-chain voting – in particular, the transaction fees voters must pay to cast an on-chain vote can make it prohibitively expensive for voters with fewer tokens. These costs have implications for voting participation and can affect how voters, proposers, and other stakeholders interact with these protocols.

Our findings motivate new research directions; for example, we find empirical evidence in support of recent proposals to redefine voting power based on social rewards, such as a voter's reputation or a voter's contributions to the protocol [39, 57, 77] or the use of a quadratic voting scheme, where voting power is calculated as the square root of the number of tokens held by the voters [15, 54]. We acknowledge that collecting data from smart contracts and determining wallet ownership can be a challenging task that requires the use of an Ethereum archive node. Therefore, we intend to make our data sets publicly available to enable scientific reproducibility of our results.

In conclusion, our research adds to the recent and growing body of knowledge on governance protocols and demonstrates the importance of measuring and auditing such systems to ensure they are working as expected. We hope that our study will be useful to future researchers in this field.

ACKNOWLEDGMENTS

This research was supported in part by a European Research Council (ERC) Advanced Grant "Foundations for Fair Social Computing", funded under the European Union's Horizon 2020 Framework Programme (grant agreement no. 789373). It has also been supported by MIAI @ Grenoble Alpes (ANR-19-P3IA-0003) and by the French National Research Agency under grant ANR-20-CE23-0007.

The first author is a researcher at Matter Labs. This research article is a work of scholarship and reflects the authors' own views and opinions. It does not necessarily reflect the views or opinions of any other person or organization, including the authors' employer. Readers should not rely on this article for making strategic or commercial decisions, and the authors are not responsible for any losses that may result from such use.

REFERENCES

[1] 1inch. 2024. Overview. https://docs.1inch.io/docs/governance/overview/. Accessed on January 28, 2024.

[2] AAVE. 2023. AAVE Economics – Governance. https://docs.aave.com/aavenomics/governance. Accessed on May 25, 2023.

[3] Hayden Adams, Noah Zinsmeister, Moody Salem, River Keefer, and Dan Robinson. 2021. Uniswap v3 core.

[4] Jeff Amico. 2023. On Crypto Governance. https://a16z.com/2021/02/05/on-crypto-governance. Accessed on February 8, 2023.

[5] Ampleforth. 2024. About FORTH Governance. https://docs.ampleforth.org/learn/about-forth-governance. Accessed on January 28, 2024.

[6] Benito Arruñada and Luis Garicano. 2018. Blockchain: The birth of decentralized governance. *Pompeu Fabra University, Economics and Business Working Paper Series* 1608 (2018).

[7] Blockchain at Berkeley. 2021. Compound Proposal 89 - Lower Proposal Threshold to 25K COMP. https://compound.finance/governance/proposals/89. Accessed on May 22, 2023.

[8] Marcella Atzori. 2017. Blockchain technology and decentralized governance: Is the state still necessary? *Journal of Governance and Regulation/Volume* 6, 1 (2017).

[9] James Austgen, Andrés Fábrega, Sarah Allen, Kushal Babel, Mahimna Kelkar, and Ari Juels. 2023. DAO Decentralization: Voting-Bloc Entropy, Bribery, and Dark DAOs. *arXiv preprint arXiv:2311.03530* (2023).

[10] Balancer.fi. 2023. Governance – Balancer. https://docs.balancer.fi/ecosystem/governance. Accessed on May 25, 2023.

[11] Roman Beck, Christoph Müller-Bloch, and John Leslie King. 2018. Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information Systems* 19, 10 (2018).

[12] Jan Behrens. 2017. The origins of liquid democracy. *The Liquid Democracy Journal* 5, 2 (2017).

[13] Binance. 2023. https://www.binance.com. Accessed on May 25, 2023.

[14] Christian Blum and Christina Isabel Zuber. 2016. Liquid democracy: Potentials, problems, and perspectives. *Journal of political philosophy* 24, 2 (2016).

[15] Vitalik Buterin, Zoë Hitzig, and E. Glen Weyl. 2019. A Flexible Design for Funding Public Goods. *Management Science* 65, 11 (2019).

[16] Polychain Capital. 2021. Compound Proposal 60 - Address Whitelist for Submitting Proposals. https://compound.finance/governance/proposals/60. Accessed on May 22, 2023.

[17] Lewis Carroll. 1884. Principles of Parliamentary Representation. (1884).

[18] John W. Chapman. 1971. Rawls's Theory of Justice. (1971).

[19] Yan Chen, Jack I Richter, and Pankaj C Patel. 2021. Decentralized governance of digital platforms. *Journal of Management* 47, 5 (2021).

[20] Swarm City. 2023. Swarm City. https://swarm.city. Accessed on February 2, 2023.

[21] CoinGecko. 2023. Compound Tokenomics. https://www.coingecko.com/en/coins/compound/tokenomics. Accessed on February 2, 2023.

[22] CoinGecko. 2023. Uniswap Tokenomics. https://www.coingecko.com/en/coins/uniswap/tokenomics. Accessed on February 2, 2023.

[23] Compound Labs, Inc. 2022. Compound Governance. https://docs.compound.finance/governance. Accessed on Dec 10, 2022.

[24] Compound Labs, Inc. 2022. Compound Leaderboard. https://compound.finance/governance/leaderboard. Accessed on Dec 2, 2022.

[25] Convex. 2023. Convex Finance Proposals. https://vote.convexfinance.com/. Accessed on May 25, 2023.

[26] Convex. 2023. Voting and Gauge Weights. https://docs.convexfinance.com/convexfinance/general-information/why-convex/voting-and-gauge-weights. Accessed on May 25, 2023.

[27] Curve. 2023. Curve.fi Governance. https://gov.curve.fi. Accessed on April 2, 2023.

[28] Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. 2020. Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability. In *2020 IEEE Symposium on Security and Privacy (SP)*.

[29] Philip Daian, Tyler Kell, Ian Miers, and Ari Juels. 2018. On-Chain Vote Buying and the Rise of Dark DAOs. https://hackingdistributed.com/2018/07/02/on-chain-vote-buying. Accessed on December 15, 2022.

[30] David Siegel. 2013. Understanding The DAO Attack. https://www.coindesk.com/learn/understanding-the-dao-attack. Accessed on February 16, 2023.

[31] Maya Dotan, Aviv Yaish, Hsin-Chu Yin, Eytan Tsytkin, and Aviv Zohar. 2023. The Vulnerable Nature of Decentralized Governance in DeFi. In *Proceedings of the 2023 Workshop on Decentralized Finance and Security (DeFi '23)*. 25–31.

[32] Edward Helmore. 2023. Why did the $212bn tech-lender Silicon Valley bank abruptly collapse? https://www.theguardian.com/business/2023/mar/17/why-silicon-valley-bank-collapsed-svb-fail. Accessed on April 10, 2023.

[33] Ethereum Foundation. 2023. Non-fungible tokens (NFT). https://ethereum.org/en/nft. Accessed on May 25, 2023.

[34] Etherscan. 2023. Etherscan APIs Documentation – Contracts. https://docs.etherscan.io/api-endpoints/contracts. Accessed on May 25, 2023.

[35] Etherscan. 2023. Etherscan (ETH) Blockchain Explorer. https://etherscan.io. Accessed on May 25, 2023.

[36] Rainer Feichtinger, Robin Fritsch, Yann Vonlanthen, and Roger Wattenhofer. 2023. The Hidden Shortcomings of (D)AOs – An Empirical Study of On-Chain Governance. arXiv:2302.12125 [cs.CY]

[37] Francisco Rodrigues. 2022. Maintaining decentralization: Are custody services a threat to DeFi protocols? https://cointelegraph.com/news/maintaining-decentralization-are-custody-services-a-threat-to-defi-protocols. Accessed on April 2, 2023.

[38] Robin Fritsch, Marino Müller, and Roger Wattenhofer. 2022. Analyzing Voting Power in Decentralized Governance: Who controls DAOs? arXiv:2204.01176 [cs.CY]

[39] Barbara Guidi, Andrea Michienzi, and Laura Ricci. 2021. A Graph-Based Socioeconomic Analysis of Steemit. *IEEE Transactions on Computational Social Systems* 8, 2 (2021).

[40] Samuel Haig. 2022. Balancer Ends Long Governance Battle With Whale. https://thedefiant.io/balancer-ve-tokenomics-whale. Accessed on April 28, 2023.

[41] Samer Hassan and Primavera De Filippi. 2021. Decentralized autonomous organization. *Internet Policy Review* 10, 2 (2021).

[42] Thomas Hobbes. 1651. Leviathan. *Project Gutenberg* (1651).

[43] Ian Allison. 2022. Divisions in Sam Bankman-Fried's Crypto Empire Blur on His Trading Titan Alameda's Balance Sheet. https://www.coindesk.com/business/2022/11/02/divisions-in-sam-bankman-frieds-crypto-empire-blur-on-his-trading-titan-alamedas-balance-sheet/. Accessed on Dec 10, 2022.

[44] Mubashar Iqbal and Raimundas Matulevičius. 2021. Exploring sybil and double-spending risks in blockchain systems. *IEEE Access* 9 (2021), 76153–76177.

[45] Jeff Kauflin and Emily Mason. 2022. How Did Sam Bankman-Fried's Alameda Research Lose So Much Money? https://www.forbes.com/sites/jeffkauflin/2022/11/19/how-did-sam-bankman-frieds-alameda-research-lose-so-much-money. Accessed on December 2, 2022.

[46] Aggelos Kiayias and Philip Lazos. 2023. SoK: Blockchain Governance. arXiv:2201.07188 [cs.CR]

[47] Krisztian Sandor and Ekin Genç. 2022. The Fall of Terra: A Timeline of the Meteoric Rise and Crash of UST and LUNA. https://www.coindesk.com/learn/the-fall-of-terra-a-timeline-of-the-meteoric-rise-and-crash-of-ust-and-luna/. Accessed on February 2, 2023.

[48] kybx86. 2020. Compensation Proposal: Distribute COMP to Affected Users in the DAI Liquidations. https://www.comp.xyz/t/compensation-proposal-distribute-comp-to-affected-users-in-the-dai-liquidations. Accessed on February 9, 2023.

[49] Compound Labs. 2020. Compound Proposal 7 - Distribute COMP to Users. https://compound.finance/governance/proposals/7. Accessed on May 22, 2023.

[50] Compound Labs. 2021. Compound Proposal 42 - Migration to Governor Bravo. https://compound.finance/governance/proposals/42. Accessed on May 22, 2023.

[51] Protocol Labs. 2023. IPFS Powers the Distributed Web. https://ipfs.tech. Accessed on February 2, 2023.

[52] Snapshot Labs. 2023. Snapshot. https://snapshot.org. Accessed on February 2, 2023.

[53] Uniswap Labs. 2023. Uniswp Proposals. https://app.uniswap.org/vote. Accessed on September 20, 2023.

[54] Steven P. Lalley and E. Glen Weyl. 2018. Quadratic Voting: How Mechanism Design Can Radicalize Democracy. *AEA Papers and Proceedings* 108 (May 2018).

[55] Robert Leshner and Geoffrey Hayes. 2019. Compound: The money market protocol.

[56] Chao Liu, Han Liu, Zhao Cao, Zhong Chen, Bangdao Chen, and Bill Roscoe. 2018. ReGuard: Finding Reentrancy Bugs in Smart Contracts. In *Proceedings of the 40th International Conference on Software Engineering: Companion Proceeedings (ICSE '18)*.

[57] Zhiyong Liu, Yueping Li, Qingfei Min, and Mengting Chang. 2022. User incentive mechanism in blockchain-based online community: An empirical study of steemit. *Information & Management* 59, 7 (2022).

[58] Tyler Loewen. 2021. Compound Proposal 62 - Split COMP rewards distribution and bug fixes. https://compound.finance/governance/proposals/62. Accessed on May 16, 2023.

[59] MakerDAO. 2023. Governance Module – Maker Protocol Technical Docs. https://docs.makerdao.com/smart-contract-modules/governance-module. Accessed on April 2, 2023.

[60] Messari. 2023. Messati: Crypto Research, Data, and Tools. https://messari.io. Accessed on May 16, 2023.

[61] Johnnatan Messias, Aviv Yaish, and Benjamin Livshits. 2023. Airdrops: Giving Money Away Is Harder Than It Seems. *arXiv preprint arXiv:2312.02752* (2023).

[62] Mike Dalton. 2022. Build Finance DAO Suffers Governance Takeover Attack. https://cryptobriefing.com/build-finance-dao-suffers-governance-takeover-attack/. Accessed on February 2, 2023.

[63] Satoshi Nakamoto. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System.

[64] Nathan Reiff. 2023. The Collapse of FTX: What Went Wrong with the Crypto Exchange? https://www.investopedia.com/what-went-wrong-with-ftx-6828447. Accessed on April 2, 2023.

[65] Nick Martitsch. 2021. Compound Treasury Updates, COMP Bug Fix, Dynamic Risk Parameters. https://compound.substack.com/p/compound-treasury-updates-comp-bug. Accessed on April 10, 2023.

[66] OpenZeppelin. 2023. Security Audits - Compound. https://blog.openzeppelin.com/?s=compound. Accessed on May 22, 2023.

[67] Daniel Perez, Sam M Werner, Jiahua Xu, and Benjamin Livshits. 2021. Liquidations: DeFi on a Knife-edge. In *Financial Cryptography and Data Security (FC '21)*.

[68] Q.ai. 2022. What Really Happened To LUNA Crypto? https://www.forbes.com/sites/qai/2022/09/20/what-really-happened-to-luna-crypto/?sh=62332b664ff1. Accessed on December 10, 2022.

[69] Kaihua Qin, Liyi Zhou, Benjamin Livshits, and Arthur Gervais. 2021. Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit. In *Financial Cryptography and Data Security (FC '21)*.

[70] Rarible. 2024. Governance. https://rari-foundation.gitbook.io/rari-dao-knowledge-base/governance. Accessed on January 28, 2024.

[71] Wessel Reijers, Fiachra O'Brolcháin, and Paul Haynes. 2016. Governance in blockchain technologies & social contract theories. *Ledger* 1 (2016).

[72] Olivier Rikken, Marijn Janssen, and Zenlin Kwee. 2019. Governance challenges of blockchain and decentralized autonomous organizations. *Information Polity* 24, 4 (2019).

[73] Jean-Jacques Rousseau. 1920. *The social contract: & discourses.* Number 660. JM Dent & Sons.

[74] Sam Kessler. 2022. Binance Becomes Second-Largest Voting Entity on Uniswap DAO. https://www.coindesk.com/tech/2022/10/19/binance-becomes-second-largest-voting-entity-on-uniswap-dao. Accessed on April 2, 2023.

[75] Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. 2014. Zerocash: Decentralized anonymous payments from bitcoin. In *2014 IEEE symposium on security and privacy*. IEEE.

[76] Scikit Learn. 2023. Cosine Similarity. https://scikit-learn.org/stable/modules/generated/sklearn.metrics.pairwise.cosine_similarity.html. Accessed on April 10, 2023.

[77] Tanusree Sharma, Yujin Kwon, Kornrapat Pongmala, Henry Wang, Andrew Miller, Dawn Song, and Yang Wang. 2023. Unpacking How Decentralized Autonomous Organizations (DAOs) Work in Practice. arXiv:2304.09822 [cs.CY]

[78] Shaurya Malwa. 2022. Binance Denies Allegations It Intends to Use Users' Uniswap Tokens for Voting. https://www.coindesk.com/tech/2022/10/20/binance-denies-allegations-that-it-intends-to-use-users-uniswap-tokens-for-voting/.

[79] Sukernik. 2021. Auditing Compound Protocol. https://www.comp.xyz/t/auditing-compound-protocol/2543. Accessed on April 10, 2023.

[80] Sybil. 2023. Introducing Sybil. https://blog.uniswap.org/sybil. Accessed on May 19, 2023.

[81] Sybil. 2023. Sybil – Top delegated addresses. https://sybil.org/. Accessed on February 2, 2023.

[82] Joshua Z Tan, Tara Merk, Sarah Hubbard, Eliza R Oak, Joni Pirovich, Ellie Rennie, Rolf Hoefer, Michael Zargham, Jason Potts, Chris Berg, et al. 2023. Open Problems in DAOs. *arXiv preprint arXiv:2310.19201* (2023).

[83] Andrew Thurman. 2022. Tron's Justin Sun Accused of 'Governance Attack' on DeFi Lender Compound. https://www.coindesk.com/tech/2022/02/04/trons-justin-sun-accused-of-governance-attack-on-defi-lender-compound. Accessed on February 2, 2023.

[84] TrueUSD. 2023. TrueUSD. https://www.trueusd.com. Accessed on February 2, 2023.

[85] Uniswap Labs. 2023. Governance – Uniswap Protocol. https://uniswap.org/governance. Accessed on April 2, 2023.

[86] Nicolas Van Saberhagen. 2013. CryptoNote v2.0. (2013).

[87] Vitalik Buterin. 2021. Blockchain voting is overrated among uninformed people but underrated among informed people. https://vitalik.ca/general/2021/05/25/voting2.html. Accessed on March 16, 2023.

[88] The web3.py team. 2022. Web3.py documentation. https://web3py.readthedocs.io/en/v5/. Accessed on December 12, 2022.

[89] Gavin Wood. 2014. Ethereum: A secure decentralised generalised transaction ledger.

[90] Peipei Xia, Li Zhang, and Fanzhang Li. 2015. Learning similarity with cosine similarity ensemble. *Information sciences* 307 (2015).

[91] Yahoo Finance. 2023. Ethereum USD (ETH-USD), Price, Value, News, and History. https://finance.yahoo.com/quote/ETH-USD/history?p=ETH-USD. Accessed on January 17, 2023.

[92] Zack Voell and William Foxley. 2020. https://www.coindesk.com/markets/2020/09/04/alameda-research-claimed-nearly-70-of-wrapped-bitcoin-minted-in-august. Accessed on April 10, 2023.

[93] Zack Voell and William Foxley. 2020. Alameda Research Claimed Nearly 70% of Wrapped Bitcoin Minted in August. https://www.coindesk.com/markets/2020/09/04/alameda-research-claimed-nearly-70-of-wrapped-bitcoin-minted-in-august.

[94] Liyi Zhou, Xihan Xiong, Jens Ernstberger, Stefanos Chaliasos, Zhipeng Wang, Ye Wang, Kaihua Qin, Roger Wattenhofer, Dawn Song, and Arthur Gervais. 2023. SoK: Decentralized Finance (DeFi) Attacks. In *2023 IEEE Symposium on Security*

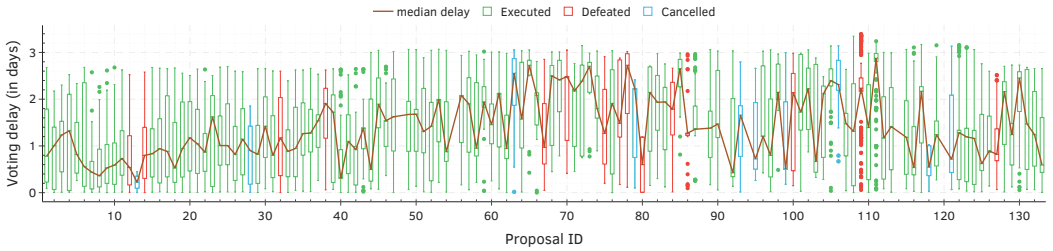


Fig. 18. *Distribution of the number of days it takes Compound voters to cast their votes.*

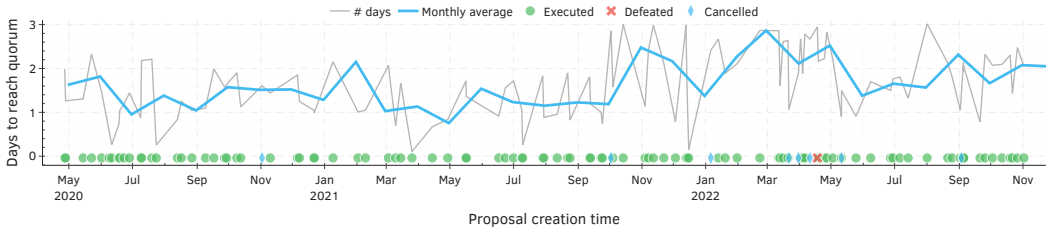


Fig. 19. Compound proposals typically reach the quorum after 1.64 days on average.

and Privacy (SP).

[95] Andrej Zwitter and Jilles Hazenberg. 2020. Decentralized network governance: blockchain technology and the future of regulation. *Frontiers in Blockchain* 3 (2020).

A TEMPORAL DYNAMICS OF VOTING

Compound Governor does not allow voters to change their votes once they have been cast. This means that voters can only vote once on each proposal. Nevertheless, voters can view all votes that have been cast on-chain in real-time. Thus, understanding how long it takes voters to cast their votes is interesting because it can shed light on whether they want to wait until the last minute to cast their votes.

According to our analysis, voters take an average of 1.4 days (with a std. of 0.95 and a median of 1.34 days) to cast their votes after the voting period began. The shortest and longest recorded delays in our data set are 0 and 3.39 days, respectively. Fig. 18 shows the distribution of the time it takes voters to cast their votes for each proposal. We also highlight the voting delays for all votes cast per proposal in Fig. 21 in §D.

B FILTERING EVENTS TO CONSTRUCT OUR COMPOUND DATA SET

This section describes the details required to filter and collect transactions data that triggered events of interest from any smart contract on the Ethereum blockchain. Before creating a filter, we need the address of our target contract and its Application Binary Interface (ABI). The ABI is a JSON file that specifies the functions available in the contract, their signatures, and the available events. We can retrieve this information by calling the Etherscan API [34]. Once we have the contract address and ABI, we can create a filter to track the contract's activity on the Ethereum blockchain using an important Python library for interacting with Ethereum nodes called Web3.py [88] to facilitate the communication with our node's API.

The Web3.py library provides a filtering function called *createFilter*. This function can be used to filter transactions that triggered events of interest from a specific contract within a range of block numbers. We use this function to efficiently collect all transactions that triggered these events from the Compound [55] smart contract.

C INFERRING WALLET ADDRESSES OWNERSHIP

We aim to identify the ownership of public wallet addresses on the Ethereum blockchain. Due to the inherent anonymity of blockchain addresses, this proves to be a challenging task as we can only know the owners of an address if the owner chooses to disclose it. However, popular blockchain explorers such as Etherscan [35] often provide information on the top holders of specific cryptocurrencies, which allows us to partially overcome this obstacle.

Then, we first obtained the lists of the top 10,000 Ether holders from which there are 290 (2.9%) identified addresses and the top 1000 COMP holders from which there are 82 (8.2%) identified addresses from Etherscan. By comparing these lists to our data set, we were able to identify most of the top COMP holder addresses in our sample. However, this method did not work for the top delegated accounts, as most of them were not included in the list of top COMP holders on Etherscan. This means that most of the delegated accounts does not hold many tokens. Further, we also used the list of top 100 delegated Compound addresses by voting weight available on the Compound website [24] from which there are 66 identified addresses.

Furthermore, to extend the available identified addresses in our analysis, we obtained the addresses of 2783 identified users from the Sybil-List [81], a project maintained by Uniswap that uses cryptographic proofs to verify wallet addresses ownership. By combining the identified addresses from both sources, we were able to obtain the ownership of 3191 inferred public wallet addresses to use in our analysis. We were able to infer 114 (3.41%) out of the 3341 unique addresses in our data set. Considering the top 10 most powerful voters for each proposal (refer to Fig. 20 in §D), we were able to infer 67 (50.37%) of the 133 unique addresses. Overall, our methodology allowed us to partially overcome the anonymity of public wallet addresses on the Ethereum blockchain and shed light on the ownership of these addresses in our data set. Finally, as an entity can control more than one address, we grouped the addresses we identified belonging to the same entity together to conduct our analysis.

D HOW VOTERS CAST THEIR VOTES

This section examines how each of the top-10 voters of Compound and Uniswap cast their votes. Some proposals may not have received any votes if they were cancelled before the voting period began. See §4.2.3 for details. Fig. 20 shows how each of the top-10 voters cast their votes in each of the 126 (94.74%) out of 133 Compound proposals.

E TIME UNTIL REACHING THE QUORUM IN COMPOUND

For a proposal to pass, it must receive a majority of in favor votes and at least 400,000 (4%) votes in favor from the total supply of Compound tokens. This minimum number of in favor votes is referred to as the *quorum* and is defined by the Compound Governor Bravo contract.

We analyzed how long it takes for these proposals to reach the required quorum. Fig. 19 shows the number of days it took each of the evaluated Compound proposals to reach the quorum. On average, it takes 1.64 days with a standard deviation of 0.72 days for the proposals to reach the quorum. The cumulative distribution function of our results, where 32% take more than 2 days to reach the quorum. The shortest and longest time it took was 0.11 and 3 days, respectively.

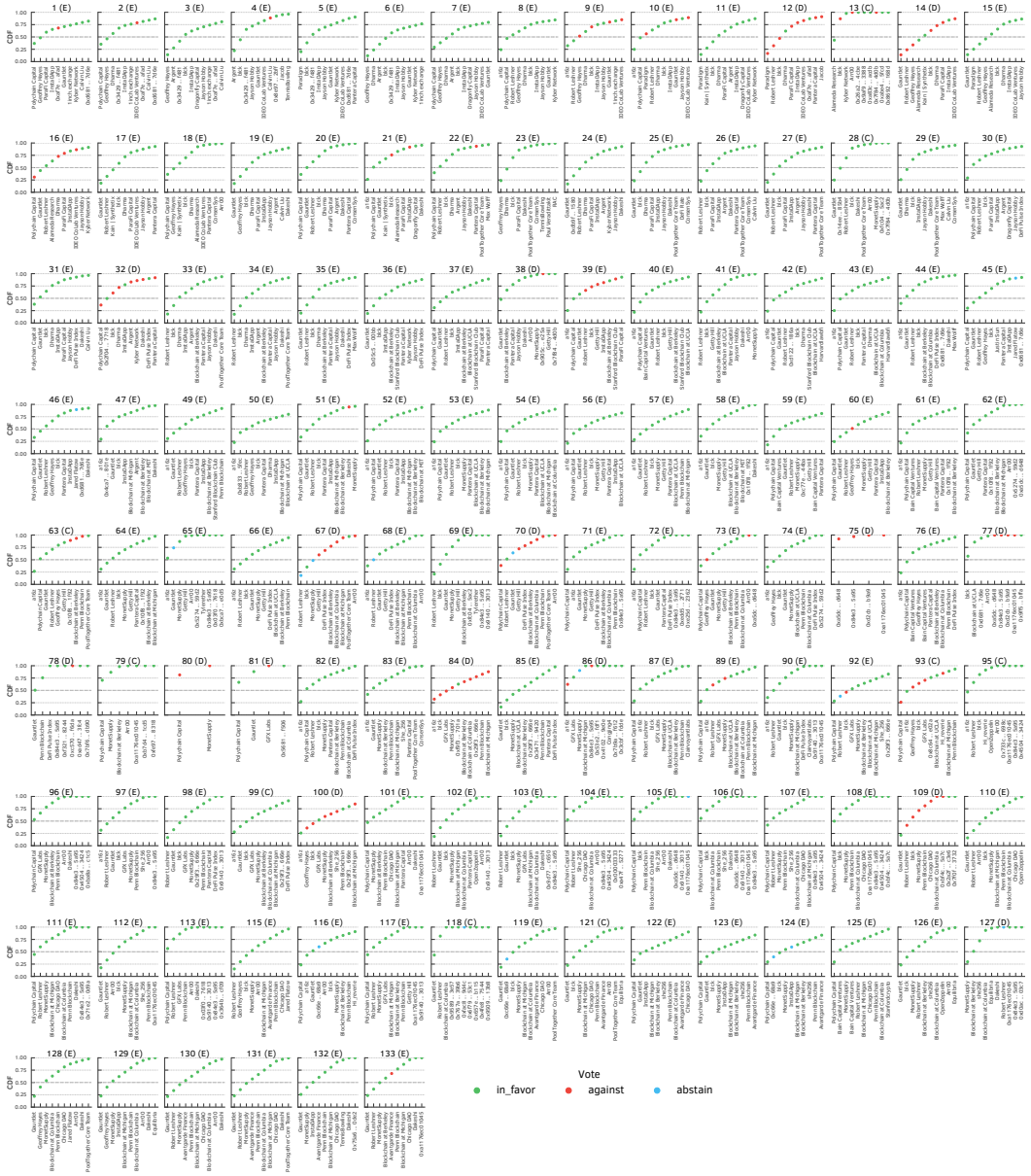


Fig. 20. Cumulative voting power distribution of the top-10 Compound voters per proposal. On average, proposals required 2.84 voters (std. of 0.97) to reach at least 50% of their total votes. The median was 3 voters, with a range of 1 to 5 votes. This indicates a concentrated amount of voting power. The subtitles indicate the proposal ID and outcome ("E" for executed, "D" for defeated, and "C" for cancelled).

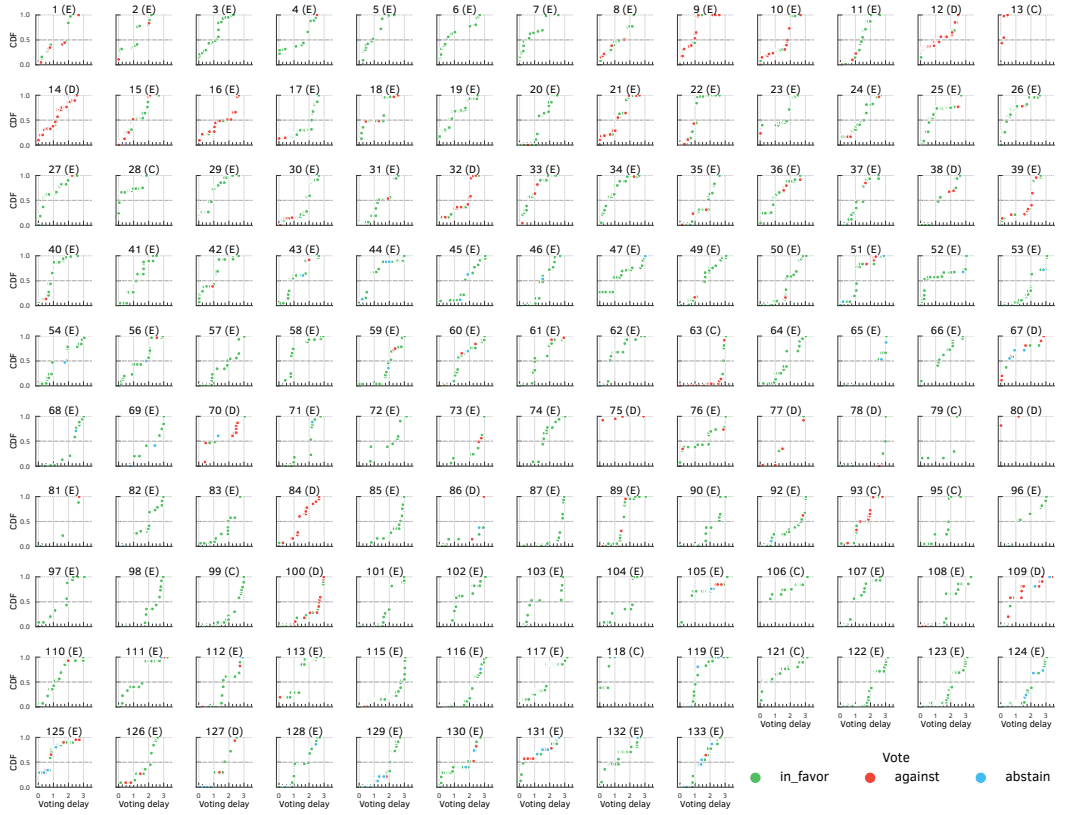


Fig. 21. Voting delays for all votes cast per Compound proposal in chronological order of vote. On average, voters took 1.4 days (with a standard deviation of 0.95 and a median of 1.34 days) to cast their votes after the voting period began. The subtitles indicate the proposal ID and outcome ("E" for executed, "D" for defeated, and "C" for cancelled).