SoK: Attacks on DAOs

Rainer Feichtinger[1]
ETH Zürich, Switzerland

Robin Fritsch
ETH Zürich, Switzerland

Lioba Heimbach
ETH Zürich, Switzerland

Yann Vonlanthen
ETH Zürich, Switzerland

Roger Wattenhofer
ETH Zürich, Switzerland

Abstract

Decentralized Autonomous Organizations (DAOs) are blockchain-based organizations that facilitate decentralized governance. Today, DAOs not only hold billions of dollars in their treasury but also govern many of the most popular *Decentralized Finance (DeFi)* protocols. This paper systematically analyses security threats to DAOs, focusing on the types of attacks they face. We study attacks on DAOs that took place in the past, attacks that have been theorized to be possible, and potential attacks that were uncovered and prevented in audits. For each of these (potential) attacks, we describe and categorize the attack vectors utilized into four categories. This reveals that while many attacks on DAOs take advantage of the less tangible and more complex human nature involved in governance, audits tend to focus on code and protocol vulnerabilities. Thus, additionally, the paper examines empirical data on DAO vulnerabilities, outlines risk factors contributing to these attacks, and suggests mitigation strategies to safeguard against such vulnerabilities.

2012 ACM Subject Classification Security and privacy → Economics of security and privacy; Human-centered computing → Collaborative and social computing

Keywords and phrases blockchain, DAO, governance, security, measurements, voting systems

Digital Object Identifier 10.4230/LIPIcs.AFT.2024.28

Related Version *Full Version*: `https://arxiv.org/abs/2406.15071` [51]

Supplementary Material *Dataset (Website)*: `https://daoattacks.ethz.ch`

Acknowledgements We thank Hubert Ritzdorf from ChainSecurity for his precious feedback.

1 Introduction

Decentralized Autonomous Organizations (DAO) are organizational structures that facilitate the trustless management of projects that run on a blockchain [11]. In DAOs, governance is typically controlled by the holders of a designated governance token. Those who own these tokens can thus determine the course of the DAO. Today, DAOs govern various blockchain projects, such as ecosystem governance of Layer 2s (e.g., Arbitrum and Optimism) and many of the most-used decentralized applications (e.g., Aave, Compound, ENS, Lido, MakerDAO, and Uniswap). Moreover, DAOs are estimated to hold and control in excess of \$30B in their treasuries [41]. Consequently, they hold significant power and a central position in the blockchain ecosystem.

[1] The authors of this work are listed alphabetically, correspondence through `daoattacks@ethz.ch`.

6th Conference on Advances in Financial Technologies (AFT 2024).
Editors: Rainer Böhme and Lucianna Kiffer; Article No. 28; pp. 28:1–28:27
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

DAOs have been threatened by attacks and hacks ever since their inception. *"The DAO"* on Ethereum was the first attempt at creating a DAO on a blockchain. However, in 2016 an infamous hack stole $50M worth of ETH from the DAO before it even became operational [106]. The event was so severe that it led to a controversial hard fork of the Ethereum blockchain. The original (unforked) blockchain still operates today and is known as Ethereum Classic. Notably, even before the fatal hack, other possible attacks on The DAO had been discussed [86]. The DAO hack highlights the significant threat attacks on DAOs can present not only to the DAOs themselves but also to the broader ecosystem. Additionally, given that DAOs are still in their early days and the ongoing evolution of their design frameworks, DAOs are particularly vulnerable to various novel attack vectors.

In this work, we study real-world incidents and attacks on DAOs, attacks that have been theorized to be possible, and new potential attack vectors. We summarize our main contributions in the following.

- We present and categorize attack vectors on DAOs. To be precise, we categorize attacks on DAOs into four categories: (i) bribing (BR) attacks, (ii) token control (TC) attacks, (iii) human-computer interaction (HCI) attacks, and (iv) code and protocol vulnerability (CP) attacks.
- We examine 28 real-world incidents and attacks across four blockchains and indicate the attack vectors utilized. Our work finds that these attacks exploited vectors from all four introduced categories fairly evenly. Similarly, we categorize attacks described in academic papers or reports as well as those uncovered and prevented through audits. Notably, less tangible attack vectors that take advantage of human and economic aspects involved in governance represent a majority of real-world incidents but are generally not analyzed in audits, which heavily skew toward code and protocol vulnerability attacks.
- Guided by our categorization of real-world incidents, we introduce seven risk factors for DAOs and empirically analyze the susceptibility of 26 DAOs of all shapes and sizes to them.
- Finally, we collect and discuss various mitigations and safeguards for DAOs.

With our work, we aim to enhance the understanding of DAO security challenges and guide the development of more robust governance frameworks.

2 Background

An early definition of DAOs was provided by Vitalik Buterin, who argued that DAOs are entities with internal capital (i.e., *treasuries*), that have automated processing at their core, and human processing at their edges [117].

This definition still holds true today, though DAOs have been continually evolving and are still undergoing substantial efforts to improve. Therefore, countless implementations exist. Nonetheless, some specific designs have reached greater popularity, as new DAOs borrow ideas, pieces of code from the smart contracts implementing the DAOs logic, or entire structures from pre-existing DAOs. Examples thereof are the OpenZeppelin implementations based on the Compound Governor contracts (also used e.g., by Uniswap, ENS, and Gitcoin) and Aragon DAOs (used by e.g., Lido and Curve). Other DAOs might follow a more unique design (e.g., Maker and Optimism) or reuse code only partially. In the following, we aim to distill the main attributes that current DAOs share.

Token Voting. Reaching an agreement between individuals in the decentralized setting of a blockchain is not as simple as in the physical world, where identities are known. On blockchains, only pseudonymous addresses are publicly available. In particular, these addresses could include *sybils*, i.e., multiple addresses created and controlled by a single individual. To address this issue, DAOs typically issue governance tokens. These tokens come with voting rights.[2] Initially, these tokens can be distributed among stakeholders through various methods. The most popular methods include giveaways (*airdrop*) to early users of a protocol, as well as allocating a portion of the tokens to the development team or early investors. After launching, the governance tokens become freely tradable on the open market, enabling individuals to acquire them and thus acquire voting power. In this regard, governance tokens exhibit parallels with shares in companies that grant holders voting rights at shareholder meetings.

Voting Rights and Delegation. While token holders directly vote on each proposal themselves in some DAOs (e.g., Lido), other DAOs introduce an intermediary in the voting process: delegates. In these DAOs, token holders can delegate the voting power associated with their tokens to a delegate they believe represents their views well. Inspiration for this *delegative* approach is taken from *liquid* democracy [54, 10]. Proponents of this approach for DAO voting argue that delegation allows token holders to participate in the governance process passively (i.e., they must not actively keep track of each proposal) and can further help reduce the blockchain transaction fees incurred by DAO members. While delegation is optional in some DAOs (e.g., Aave), many DAOs require delegation (e.g., Compound, ENS, and Uniswap). In DAOs requiring delegation, before tokens can be used for voting, the address holding the tokens must delegate them to a *delegate* address (which may be the same address). Finally, some DAOs require the tokens to be locked in a specified contract to gain the associated voting rights (e.g., Curve and Maker).

Deliberation Phase. Generally, DAO governance processes involve multiple steps, which could include discussions on public governance forums or off-chain *temperature check* votes before a final vote [87] ahead of a proposal being put forward on-chain and voted on. However, these steps are often mere social conventions. The final on-chain vote is often the only obligatory part of the process.

Proposals. Generally, any token holder with a sufficient number of tokens (exceeding a pre-defined proposal threshold) can put forward a proposal. There are some DAOs though that force proposals to be vetted by a committee before being accepted on-chain.

Voting Phase. Once a proposal is submitted on-chain, there is generally a *proposal delay*, i.e., a pre-specified number of blocks before a snapshot is taken of the balances of all token holders (or delegates). The snapshot determines their voting power, and cannot be changed a posteriori. Thereafter, voting starts and generally lasts for a pre-determined number of blocks. During voting, any address with voting rights (token holder or delegate) may submit a vote.

Execution Phase. If a majority votes in favor of a proposal and a pre-determined Quorum is reached, the proposal is accepted. In some DAOs, on-chain proposal execution is automatic, potentially only after a pre-defined *timelock delay*. The execution is scheduled manually by a trusted party in other DAOs.

[2] Generally, each token counts as one vote. Curve is an exception, where the voting power depends not only on the number of tokens held but also the duration the tokens are locked for.

3 Categorization of Attack Vectors

In the following, we provide a categorization and description of attack vectors.

3.1 Bribing

▶ **Definition.** In a *bribing (BR)* attack, an attacker pays to change votes or to acquire voting power without acquiring the underlying governance tokens. The controlled votes and voting power are then utilized to pass a malicious proposal in a governance vote.

Bribing attacks can take the form of paying to obtain voting rights of governance tokens to vote for a certain proposal without acquiring the underlying token, which is often referred to as *vote buying*. Another possibility is directly bribing token holders or delegates.

Given that vote buying has been documented in shareholder governance of traditional companies [76], it is a plausible future concern for DAO governance and was already been a topic of discussion since the early days of DAOs [37, 20].

Bribing Token Holders or Delegates (BR1). Bribing governance participants, i.e. token holders or delegates, can take many forms: it can be done on-chain or off-chain, programmatically using smart contracts or by personal contact. Furthermore, bribes could be fixed sums or a proportion of the proceeds from a successful attack. Note that using proceeds of the attack to bribe leads to a situation similar to an attack by a majority coalition, where the proceeds are split among participants (see TC5).

When voting power is highly centralized, as is the case for many DAOs at the time of writing [52], bribing only a few of them can suffice to change a vote. On the other hand, voting rights being highly distributed can also make it cheaper for an attacker to bribe: holders of small amounts of voting power, besides having little to lose from a successful attack, also have little influence on the outcome of a vote. Hence, it can be economically rational for them to cheaply sell their vote, as described by Buterin [19].

Bribing delegates to vote a certain way could potentially be particularly attractive for an attacker. For governance systems using delegated token voting, a small number of delegates often controls large amounts of voting rights. On the other hand, these delegates do not actually hold the corresponding amount of governance tokens, meaning they are not exposed to the price risk from a successful governance attack. Hence, bribing them could potentially be significantly cheaper for an attacker than bribing governance token holders.

One deterrent against a delegate bribing attack, that is present in most current DAOs, is the fact that most delegates are often publicly (or at least pseudonymously) known. This means that delegates stand to lose their reputation and future earnings based on it, and may even face a risk of criminal charges for accepting bribes.

Vote Buying Protocols (BR2). The act of vote buying or *bribing* can be facilitated by a smart contract protocol. Such protocols allow token holders to deposit their governance tokens into pools, and earn fees from users paying to use the voting rights of the pooled tokens. In particular, this means that vote buyers do not need to deposit collateral, contrary to using traditional lending platforms such as Compound (see Section 3.2). Paladin Lending, as one example of a vote buying protocol, is described in the following.

Case Study Paladin Lending

Paladin Lending [98] lets holders deposit their tokens into pools and in return receive a proportional share of the fees collected in the pool. Users can then borrow the voting power of deposited tokens. A loan contract is automatically created if a user wants to borrow voting power. The borrowed token amount is transferred from the pool to the loan contract, and the votes are delegated to the user. Hence, the user has no direct access to the tokens but can use their voting power. The user pays a fee for borrowing the voting power. At the latest when this fee has been consumed, the tokens in the loan contract will be returned to the pool.

Importantly, with a vote buying protocol such as Paladin Lending, one does not borrow the actual token, but only the voting rights. We also perform an empirical analysis of Paladin Lending (see Appendix of the full version of this paper [51]) to show that low liquidity currently does not allow attacks exclusively using this attack vector.

Daian et al. [37] introduce a particular type of vote buying protocol: *Dark DAOs*. In addition to facilitating vote buying using smart contracts, Dark DAOs are implemented in a privacy-preserving manner. Note that activity on vote buying protocols such as Paladin Lending is publicly recorded on the blockchain. Vote buying activities through Dark DAOs, on the other hand, cannot be detected, meaning that other governance participants cannot react to such an attack. While there are no known cases of active Dark DAOs at the time of writing, they have been theoretically studied by Austgen et al. [5], and proof-of-concept prototypes have been published [4].

3.2 Token Control

▶ **Definition.** With *token control (TC)* attacks, an attacker takes possession or is already in possession of a significant amount of governance tokens. The attacker then uses the voting power associated with these tokens to get their malicious proposal accepted in a governance vote.

This family of attack vectors is of the simplest nature. The attacker merely gains control of a sufficient number of governance tokens to take over the DAO by passing a malicious proposal according to DAO's intended voting process.

Depending on the governance model implemented by the DAO, the required proportion of governance tokens for a successful attack varies. For instance, many DAOs require tokens to be delegated to an address for them to be used in voting and take a snapshot of the current state of delegations at the start of the voting period. For such governance systems, an attacker must only hold a token amount exceeding the amount of previously delegated tokens, and delegate these governance tokens to themselves, thereby securing a majority of the delegated votes. By timing the creation of a proposal accordingly, an attacker can leave very little time (depending on the governance system's parameter choices, see RF4 in Section 5 for more details) for others to react and delegate their tokens. This can almost guarantee the attacker the required voting power to pass their desired proposals. For DAOs that do not require the tokens to be delegated, the attacker would need to hold more than 50% of the circulating token supply for a guaranteed victory of their proposal or hope that not sufficiently many votes are cast, i.e., voter turnout does not increase dramatically in face of a malicious proposal. Short voting windows as well as the absence of reliable communication channels further increase the risk of such attacks for these DAOs.

In the following, we discuss the main possibilities for an attacker to gain possession of the required voting power. Note that in Section 5, we provide an additional empirical analysis of the susceptibility of a set of 26 DAOs to this kind of attack.

Token Purchase (TC1). The attacker buys governance tokens on the open market. This can be done on-chain through decentralized exchanges, or on off-chain centralized exchanges. After using the tokens for voting, the attacker can sell back the tokens to the open market. Importantly, when buying governance tokens, the attacker takes on price risk while holding the tokens. If the attack leads to a decrease in the governance token's market price, the attacker incurs a financial loss. Additionally, the attacker pays trading fees when buying and selling the tokens. Note that the attacker can potentially hedge the price risk using derivatives. However, the availability of such derivatives may be limited depending on the governance token in question.

Attacks through token acquisition have been attempted and have occurred in several DAOs. They are especially attractive and profitable if the value of the treasury (excluding the governance token itself, which is likely to decrease in value in the event of an attack) exceeds the capital required to buy the necessary voting power. In Section 5, we compare the treasury values of DAOs to the value of delegated tokens for a set of 26 DAOs. It is relatively common for the total value of the DAO's treasury to exceed the value of delegated tokens, though this is only rarely the case when excluding the governance tokens from the treasury.

In the following, we present a case study of two consecutive recent governance attacks through token acquisition on the Indexed Finance DAO, a protocol for portfolio management. While interest in the project declined after it was hacked in October 2021 [1], various tokens remained in the project's timelock contract controlled by the DAO.

Case Study Indexed Finance

On 16 November 2023, over ten hours, the attacker bought NDX tokens (i.e., the protocol's governance token) via decentralized exchanges, self-delegated these tokens, initiated a proposal, voted in favor of this proposal, and sold the tokens again [1]. The proposal would allow the attacker to take control of the timelock, mint new NDX tokens, and steal tokens from the timelock (including both NDX and other tokens). A call for action by one of the protocol founders asked users to vote against the proposal. In the end, user votes against the proposal were sufficient to narrowly prevent the attack. Interestingly, the attacker sold his NDX tokens before the end of the proposal and thereby lost his voting power. As a result, the proposer would have been below the proposal threshold and the proposal could have been canceled by anyone. However, this was not done.

Fearing a potential second attack, the community attempted to implement defensive measures. They created a proposal to transfer control of the timelock to a smart contract not be under anyone's control, i.e., the tokens in the timelock would forever be inaccessible if the proposal were executed. Then, on 22 November 2023, another attacker (i.e., a different account than the previous attacker) created a similar proposal that would transfer the admin rights of the timelock to the attacker. This time, the attacker acquired more NDX tokens than the 16 November attacker, and there were not enough votes against this proposal. Thus, the only way to stop the attacker from getting access to the tokens was through passing the proposal that would make the tokens forever inaccessible. Importantly, as this proposal was created a day earlier, it would not only execute first but the attacker also only acquired the tokens after voting had started on the community's proposal and therefore did not have the majority in that vote. What followed, as no one wanted the community's proposal to be executed, was a message exchange between the attacker and the Indexed Finance team using input data of Ethereum transactions. In the end, an agreement was reached, and the attacker received $\approx$ \$10K via an escrow contract after withdrawing his proposal. In conclusion, the two attacks were only mitigated by luck (i.e., the first attacker bought too few tokens) and by unorthodox proposals (i.e., making the tokens forever inaccessible).

In the aftermath of the attacks, the Indexed Finance DAO accepted a proposal that transferred control of the timelock to a multi-signature wallet controlled by former protocol contributors.

Indexed Finance demonstrates the complexities of protecting against this attack vector in the absence of adequate countermeasures. Nevertheless, there exist potential protections that DAOs can put in place. For example, DAOs may opt to restrict proposals from spending the entire treasury or grant veto power to a multi-signature. We provide more detail in Section 6.

Token Loan (TC2). The attacker borrows governance tokens against collateral using lending protocols. Apart from needing to post collateral, the attacker also pays borrowing fees for the period of borrowing the tokens. Importantly, the attacker does not take on price risk when borrowing tokens. After voting for an attacking proposal, the full amount of governance tokens can be returned and the attacker receives back their collateral.

There have been several alleged attempts of DAO attacks through token loans. In early 2022, Justin Sun presumably borrowed large amounts of MKR, the governance token of MakerDAO, to sway a vote. However, he returned the tokens after his actions were detected and did not end up voting [2]. A couple of days later, a similar failed attempt by Justin Sun took place in Compound's governance with borrowed COMP tokens [114].

Flash Loan (TC3). With a flash loan, the attacker only borrows the governance tokens for the duration of a transaction. While the attacker pays a fee to borrow the governance token, the attacker does not need to post any collateral, i.e., does not require access to significant funds. Many protocols protect themselves against flash loan attacks by implementing a delay between the proposal creation and the start of the voting period. Nonetheless, flash loan attacks on DAOs have occurred in the past, the most prominent example is a flash loan attack on the Beanstalk governance described in the following case study.

Case Study Beanstalk

Beanstalk is a stablecoin protocol. On 17 April 2022, Beanstalk suffered an attack that resulted in damages of approximately $182M, netting the attacker a profit of around $76M [44, 50, 13]. The attacker exploited a vulnerability in Beanstalk's governance system, which was not secure against flash loan attacks. The attacker took a flash loan worth approximately $1B. This loan allowed them to achieve a two-thirds majority in Beanstalk's governance. With this majority, they could execute a malicious proposal immediately using an emergency commit function.

Whale Activation (TC4). Inactive token holders with a large number of tokens (often referred to as whales) can suddenly become active in the governance. In DAOs requiring tokens to be delegated, this can be especially problematic. An attacking whale can delegate their tokens and promptly initiate a proposal. Importantly, large entities holding sufficiently many tokens to take over the DAO exist for many DAOs using delegated token voting (see Section 5). Notably, there was one instance in the past where a centralized exchange unexpectedly delegated the UNI governance tokens it held, i.e., the tokens custodied on behalf of its users. They, however, claimed to have accidentally delegated these tokens [85].

Majority Coalition (TC5). In governance systems using majority token voting, it is generally possible for a simple majority of voting tokens to accept any proposal, and effectively, take control of the DAO. In particular, the majority could distribute the entire DAO treasury among themselves. Settings of this type have been modeled in game theory as *coalition games with transferable utility* or *majority games* with *stable sets* describing possible attacking coalitions [17, 70]. Such coalition attacks are specifically attractive when the treasury value of a DAO is high compared to the value of (delegated) governance tokens. We have empirically studied this relation in Section 5 (see RF3) for 26 DAOs.

Of course, a majority of voting tokens can also vote to split the treasury among *all* token holders, or more generally, dissolve the DAO. In this particular case, i.e., if all token holders get a share of the treasury proportional to their voting power, a majority coalition would not pose an attack. An example of this happening in practice is DigixDAO's token holders voting to dissolve the DAO and return all ETH held in the treasury to the token holders (which was worth more than the value of all governance tokens) [120]. However, in all other cases, where a strict subset of token holders come together to take control of a DAO, a majority coalition presents an attack.

3.3 Human-Computer Interaction

▶ **Definition.** *Human-computer interaction (HCI)* attacks aim to manipulate the voting process by exploiting user-facing interfaces and applications or human behaviors involved in the DAO's voting process.

This family of attacks lies at the boundary between the blockchains (computers) and humans. The attack vectors in this family do not exploit vulnerabilities in the underlying governance protocol itself, but rather in the interfaces, applications, or human behaviors surrounding DAO governance.

User Interface Issues (HCI1). Many users participate in the voting process through aggregator websites that provide a convenient *user interface (UI)*. Thus, bugs or malicious code in these UIs can lead to users not voting as they intended or not being able to vote at all. For example, users voting through a UI typically sign a vote transaction prepared by the UI. If this transaction is incorrectly prepared, users will potentially vote differently than they intended by signing the transaction. An incident of this type occurred with Tally, a closed-source and widely-used UI for on-chain governance.

Case Study Tally

On 19 August 2021, a bug, which had persisted from 30 April to 19 August 2021, was discovered on Tally [110]. The bug inadvertently altered the voting process: transactions of users wishing to vote *against* a proposal were erroneously constructed by Tally. This led to these votes being recorded as votes *in favor* on the blockchain. The issue went unnoticed since the transaction arguments were not presented in an easily understandable format, making it challenging for users to notice the discrepancy between their intended vote and the registered vote.

While there is no evidence to suggest that this bug in Tally significantly influenced the outcomes of any votes, it nonetheless highlights a critical vulnerability in centralized, closed-source front-ends for governance systems. Once a vote is cast on-chain for a proposal, it cannot be retracted or altered. This means that if a user realizes their vote has been incorrectly cast due to a platform error, they are powerless to correct it. Thus, bugs in UIs can heavily influence the voting process in DAOs, and the possibility of inserting malicious code into these UIs poses a serious risk for DAOs.

On a similar note, the unavailability of the aforementioned UIs can pose a threat to a functioning DAO governance vote. The unavailability could be caused by technical issues with the UI as well as by deliberate *Denial of Service (DoS)* attacks. If widely-used UIs became unreachable ahead of a vote, users relying on these platforms to cast their votes might be deterred or prevented from voting. To the best of our knowledge, no such attack has taken place or been attempted. Nonetheless, it presents a risk worth considering for DAOs when designing their governance systems.

Proposal Obfuscation (HCI2). Obfuscation of the real intent of a proposal is a further possible attack vector, which presents a risk to DAOs, especially in combination with a weak validation of the proposal – making sure that the proposal description matches its contents. Take as an example a proposal that appears to be a legitimate proposal but, in reality, inserts malicious code that allows the attacker to steal the DAO's funds. Such an attack was successfully performed on the Tornado Cash governance.

Case Study Tornado Cash

On 20 May 2023, an attacker gained control of the governance system of Tornado Cash [44, 9]. The attacker purchased TORN tokens through decentralized exchanges and imitated a previously accepted proposal. Due to the striking resemblance to this earlier proposal, the new, malicious one was also approved by the community. However, there was a critical and deliberate difference in the attacker's proposal: it included a self-destruction feature. After the proposal was approved, the attacker activated this self-destruction functionality, destroyed the existing proposal contract, and replaced it with malicious code. The newly inserted code allowed the attacker to withdraw TORN tokens, i.e., the DAO's governance tokens.

The Tornado Cash incident highlights a general vulnerability in governance mechanisms of decentralized platforms: the lack of a guaranteed match between a proposal's description and its actual code. Proposals might have unintentional errors or, as in the Tornado Cash case, be subject to deliberate manipulation. Notably, the Tornado Cash attack is not the only example of a malicious mismatch between a proposal's description and implementation. The proposal of the flash loan attack on Beanstalk (see Section 3.2) claimed to be donating funds to Ukraine but in reality, stole the DAO's assets [13].

Proposal Spam (HCI3). A further attack vector that can be utilized to hide a malicious proposal is to spam the protocol's governance with many proposals, such that the malicious proposal is hidden in a flood of proposals. One notable example was a governance attack on Synthetify – a protocol on the Solana blockchain whose DAO had been inactive since December 2022. The following case study details the attack, which also involved aspects of token control attacks (see Section 3.2).

Case Study Synthetify

On 17 October 2023, an attacker gained access to the assets controlled by Synthetify's DAO [92, 75, 29]. The attacker first bought sufficient amounts of the protocol's governance token SNY to make a proposal and to hold more tokens than the three biggest holders. Then the attacker used spam to distract from the attack. In particular, the attacker created more than 20 spam proposals over two months and tested whether they would go unnoticed over the seven-day voting period. No one but the attacker voted on any of these proposals, i.e., the attacker was able to pass them without a problem. Knowing that no one was paying attention, the attacker then hid malicious code that allowed them to withdraw the funds controlled by the governance. The proposal passed without any opposition.

Many protocols attempt to protect against such attacks by only allowing one active proposal per account, which must sufficient tokens to exceed the proposal threshold. Nevertheless, workarounds might still pose a threat to DAOs. Consider the following workaround for DAOs utilizing the delegation model. The attacker creates a proposal with one account to which they delegate their tokens. The attacker waits for the votes to come in and cancels the proposal after a significant proportion of votes have been cast. Then, the attacker delegates the tokens to another account. The attacker then creates a new proposal and continues in this fashion in hopes of tiring the DAO's voters who pay fees for every vote.

Social Infiltration (HCI4). Individuals and institutions can take up positions of power in DAOs. For instance, delegates often vote with significantly more tokens than they hold. Moreover, some DAOs grant certain powers in the governance process to *multisignature addresses (multisig)* which are jointly controlled by multiple key holders. The members of the multisig are chosen and voted upon by the DAO. One can imagine that malicious parties can maneuver themselves into these positions of power and then use their position to attack the protocol. The scandal surrounding Wonderland DAO [113] highlights the potential risk that can stem from social infiltration. The treasury manager was found out to be Michael Patryn, a convicted criminal who had hidden his identity.

Behavioral Manipulations (HCI5). Contrary to many voting systems, preliminary results of DAO votes are known to everyone. In a system where voting is associated with high costs, access to interim results could be seen as beneficial, as voters can be mobilized only if needed. However, access to preliminary results also opens up attack vectors. Yaish et al. [119] highlight these attack vectors, which are attested by a large body of work on voting systems and online polls [21, 124, 90, 88, 3].

First, voters might be manipulated not to vote because they observe that their preferred outcome appears to have garnered enough support to win. An attacker can then vote at the last moment, not offering others time to react. This behavioral pattern called *vote sniping* has been reported anecdotally before [93]. Rosello [101] draws parallels to corporate governance and empirically shows the negative effects vote sniping has on token value.

Conversely, attackers voting early might sway uninformed voters to follow their direction. This is commonly referred to as *bandwagon voting*, an effect supported by a large amount of empirical evidence [124, 90, 3]. Yaish et al. [119] analyze this setting theoretically, and show that interim results piled with high voting costs can entice informed voters to follow a mixed strategy of voting either early or late.

3.4 Code & Protocol Vulnerability

▶ **Definition.** *Code and protocol vulnerability (CP)* attacks exploit code or logic vulnerabilities, either in the governance smart contracts or the protocols they are connected to.

Code Vulnerability (CP1). To attack a DAO, an attacker can take advantage of any existing bugs in the governance smart contracts. The arguably most prominent attack on a DAO did exactly that.

Case Study The DAO

The DAO was a crowd-funded investment fund and one of the first DAOs. On 17 June 2016, an attack on The DAO occurred [106]. The attack exploited a loophole in the code, that allowed the attacker to perform a reentrancy attack to repeatedly withdraw ETH from The DAO [99]. Notably, the hack was so severe that it led to a highly controversial hard fork of the Ethereum blockchain. The majority of the Ethereum community decided to fork the chain to undo the hack's damages. The unaltered version of the chain continues to operate as Ethereum Classic.

The DAO hack highlights the complexities of writing secure governance smart contracts. Given these complexities and the ongoing development of DAOs, code vulnerabilities appear infrequently. However, in some cases, these bugs are identified in audits and fixed before they can be exploited. For instance, in two DAOs (MakerDAO and Keep3R Network) vote tallying could be exploited [107, 95]. In the case of Keep3r Network, the contracts permitted users to re-vote on a proposal but failed to properly subtract the user's previous vote.

Based on audits, the most well-known smart contract vulnerabilities apart from reentrancy and re-vote vulnerabilities include insufficient proposal validation and absence of transfer validation [103]. To prevent code vulnerabilities, re-using audited and time-tested code is typically seen as a good practice. However, mixing and matching code from different sources has caused at least two hacks too [63].

Protocol Vulnerability (CP2). Vulnerabilities in the protocols associated with a DAO can extend to the DAO itself given the often intertwined nature of the two. One example of how vulnerabilities in a protocol can affect the DAO is the attack on Mango Markets.

Case Study Mango Markets

In October 2022, Avi Heisenberg performed an attack on Mango Markets and its governance [68]. Heisenberg manipulated the price oracle for MNGO, the protocol's governance token, that allowed him to take out massive loans against the protocol's treasury which the DAO controls. In doing so, Heisenberg effectively drained the treasury. He went on to create a proposal in the DAO promising to return the majority of the funds if the DAO agreed to repay the protocol's bad debt. Further, the attacker's proposal sought to ensure that the token holders could not pursue any legal action against the attacker. The attacker's proposal did not pass, but the DAO later passed an alternative proposal, leading to part of the funds being returned. The attacker, who publicly identified himself [47] and infamously described the hack as a "highly profitable trading strategy", was later charged by the US government for his attack [102].

The previously outlined incident exemplifies how the interconnectedness of a protocol and its DAO can pose a risk to the DAO. When such an intertwined nature is wished for or required, it is especially challenging to fully protect against such attacks, as complexity increases and attack vectors are likely unique to each protocol.

4 Real-World Incidents & Attacks

In the following, we analyze past attacks and incidents, as well as potential attacks described in audits and papers relating to DAOs. The data set in the paper includes all incidents known to us at the time of writing.[3] We further provide an up-to-date data set under the webpage `daoattacks.ethz.ch` and welcome readers to report any additional or new incidents.

Table 1 lists all (theorized) incidents we analyzed. For each incident, we indicate the date and blockchain on which it occurred. Additionally, for real-world incidents, we indicate the purpose of the attack, whether it was successful, and if it was, the financial damage. Finally, we highlight which of the attack vectors introduced in the previous sections are utilized. We provide a summary for all (theorized) attacks in the full version of our paper [51].

Turning to Table 1, we observe a relatively balanced distribution of attack vectors used in real-world incidents across the four previously introduced categories. Specifically, among the 28 attacks analyzed, 4 utilized at least one attack vector from the BR category, 14 employed TC attack vectors, 9 involved HCI attack vectors, and 9 exploit CP attack vectors.

Table 1 further summarizes critical vulnerabilities of DAOs that were uncovered in academic works, reported to the protocols, or discovered as part of audits. While attacks documented in academic papers and reports span multiple categories, those identified through audits almost exclusively belong to the CP category.

[3] We collected the incidents by searching the web for papers, audits, news articles, blog posts, and tweets that discuss them as well as talking to experts in the field.

Table 1 Categorization of past attacks and incidents, as well as possible attacks uncovered in academic papers, reports, or audits. For each attack, we indicate its purpose: $ signifies that the purpose of an attack was to extract funds from the DAO, 🏛 indicates that the goal was a long-term (financial) gain, 🔄 denotes an ongoing attack (possibility), and ? indicates a (potentially) unintentional incident that exemplified vulnerabilities of DAOs. We further indicate whether the attack was successful where appropriate and if so indicate the financial damage of the attack. Finally, we also highlight which attack vector(s) were used. We proceed similarly for (potential) attacks uncovered in academic papers, reports, or audits. Moreover, we provide a brief summary of each (theorized) attack in the full version of this paper [51].

	date	blockchain	attack purpose	successful	attack damages	bribing holders/delegates (BR1)	vote buying protocols (BR2)	token purchase (TC1)	token loan (TC2)	flash loan (TC3)	whale activation (TC4)	majority coalition (TC5)	UI issues (HCI1)	proposal obfuscation (HCI2)	proposal spam (HCI3)	social infiltration (HCI4)	behavioral manipualtion (HCI5)	code vulnerability (CP1)	protocol vulnerability (CP2)
incidents & attacks																			
Audius [112, 30]	Jul 2022	ETH	$	✓	$6.1M													🟦	
Beanstalk [13]	Apr 2022	ETH	$	✓	$182M					🟧				🟩					
BigCap DAO [12]	Sep 2023	ETH	$	✗				🟧						🟩					
Binance [85]	Oct 2022	ETH	?								🟧								
Build Finance [77, 18, 38, 34, 46]	Feb 2022	ETH	$	✓	$470K			🟧						🟩					
Compound [114]	Feb 2022	ETH	🏛	✗					🟧										
Curio [64]	Mar 2024	ETH	$	✓	$16M													🟦	
Curve A [69]	ongoing	ETH	🔄			🟥													🟦
Curve B [8, 122]	Nov 2021	ETH	🏛	✓		🟥													🟦
ForceDAO [63]	Apr 2021	ETH	$	✓	$367K													🟦	
Genesis Alpha [79]	Feb 2019	ETH	$	✓	$90K													🟦	
Indexed Finance [1]	Nov 2023	ETH	$	✗				🟧											
Kleros [73]	Dec 2023	ETH	$	✗										🟩					
Maker DAO B [83]	Oct 2020	ETH	🏛	✓						🟧									
Maker DAO C [2]	Jan 2022	ETH	🏛	✗					🟧										
Mango Markets [68, 102, 47]	Oct 2022	SOL	$	✓	$47M														🟦
Paladin Lending [98]	ongoing	ETH	🔄				🟥												
Steemit [33]	Feb 2020	STEEM	🏛	✓				🟧											
Synthetify [92, 75, 29]	Oct 2023	SOL	$	✓	$230K			🟧							🟩				
Tally [110]	Apr 2021	ETH	?										🟩						
Temple DAO [74, 14, 105]	Oct 2022	ETH	$	✓	$2.4M													🟦	
The DAO [35, 45, 106]	Jun 2016	ETH	$	✓	$50M													🟦	
Tornado Cash [9]	May 2023	ETH	$	✓	$2M			🟧						🟩					
True Seigniorage Dollar [22, 43]	Mar 2021	BSC	$	✓	$16K			🟧											
Wonderland DAO [113]	Jan 2022	ETH	🏛	✓												🟩			
Venus [100]	Sep 2021	BSC	🏛	✗		🟥						🟧							
Yam Finance [108]	Jul 2022	ETH	$	✗										🟩					
Yuan Finance [121, 48]	Sep 2021	ETH	$	✓	$282K			🟧											
academic papers & reports																			
Bandwagon Voting [119]	Feb 2024																🟩		
Dark DAOs [5, 4, 37]	Jul 2018					🟥													
Maker DAO A [60]	Feb 2020	ETH						🟧	🟧	🟧									
Nexus Mutal [39]	Feb 2020	ETH																🟦	
Vote Sniping [101]	Jan 2024																🟩		
audits																			
Agora [94]	May 2023	OP																🟦	🟦
Constitution DAO [62]	Jan 2022	ETH																	🟦
Curve C [115]	Jul 2020	ETH													🟩			🟦	🟦
DAO Maker [61]	Mar 2021	ETH																	🟦
GameDAO [23]	Aug 2021	BSC																🟦	
Hoprnet [27]	Jun 2021	ETH																🟦	
Keep3r Network [107]	Sep 2022	ETH																🟦	
Maker DAO D [95]	May 2019	ETH																🟦	
POA Network [26]	Sep 2018	ETH																🟦	
Snapshot X [28]	Jul 2023	EVM						🟧											

We only found a relatively small set of critical vulnerabilities identified by audits, limiting its representativeness. On the other hand, a closer examination of audits that did not uncover critical vulnerabilities reveals a similar skew towards CP attack vectors [103, 91]. Although most DeFi protocols are primarily susceptible to CP attack vectors [123], the governance aspect introduces an array of exceedingly complex attack vectors. These additional attack vectors are often less tangible to analyze and are typically not accounted for in audit processes.

Additionally, it is worth mentioning that a notable portion of attacks (specifically, 8 out of 28) combine multiple attack vectors. This heterogeneous nature of attacks targeting DAOs can make it challenging for DAOs to anticipate and protect against all potential attacks while, at the same time, striving to innovate and develop.

5 Risk Factors

Guided by our description and analysis of historical precedence cases, we identify seven risk factors that either directly or indirectly correlate with attacks on DAOs. Further, for a set of 26 DAOs on Ethereum and its Layer 2s, we empirically analyze how vulnerable these DAOs are for each of our identified risk factors in Table 2. These DAOs represent both the biggest DAOs in the Ethereum ecosystem in terms of the size of the treasuries or protocols they govern, along with smaller DAOs. This combination allows us to accurately portray the state of DAOs of all shapes and sizes. Note that we provide a brief description of our data collection in the full version of our paper [51] and open-source the data collection code [81].

Voter Apathy (RF1). If token holders do not delegate or vote themselves, it becomes much easier for an attacker to pass malicious proposals. In all but four of the DAOs we empirically analyzed in Table 2, tokens must be delegated before voting. Importantly, when voting takes place, no more delegation is possible. We show the percentage of both delegated tokens voting and the percentage of the total token supply voting on average in the last five votes – a measure of voter apathy. Note that any tokens that are not delegated ahead of the voting period are completely excluded from voting. When regarding the first two columns in Table 2, notice the relatively low participation from the delegated tokens at 34% across the 20 DAOs that require delegation in our data set. While some DAOs have a high participation of more than 81.13% (i.e., Ampleforth), in other DAOs the participation of delegated tokens sits around 1% (i.e., Pooh). Additionally, even more startlingly, of the entire token supply, on average only 5% of tokens participate in the governance across the DAOs we analyzed. We highlight that these low participation rates of (delegated) tokens can be seen as a considerable risk factor, as an attacker can attempt a majority attack, even when holding just a fraction of the tokens.

High Governance Token Liquidity (RF2). High governance token liquidity entails the possibility and comparatively low cost of buying or lending the governance token – making the attack vectors in the token control category we presented in Section 3.2 feasible. Table 2 shows that available liquidity on Uniswap V2 and V3 (the two biggest decentralized exchanges on Ethereum in terms of *total value locked (TVL)* [42]). We show the available liquidity as a percentage of (1) the proposal threshold, i.e., the minimum number of tokens required to create a proposal in the governance, (2) the delegated votes, i.e., the number of tokens required to almost guarantee success in the analyzed DAOs, and (3) the average number of tokens voting in the last five governance votes. We observe that for 17 DAOs the available liquidity exceeds the proposal threshold, whereas only for zero and two DAOs the available liquidity exceeds the delegated votes and the average number of votes respectively. While

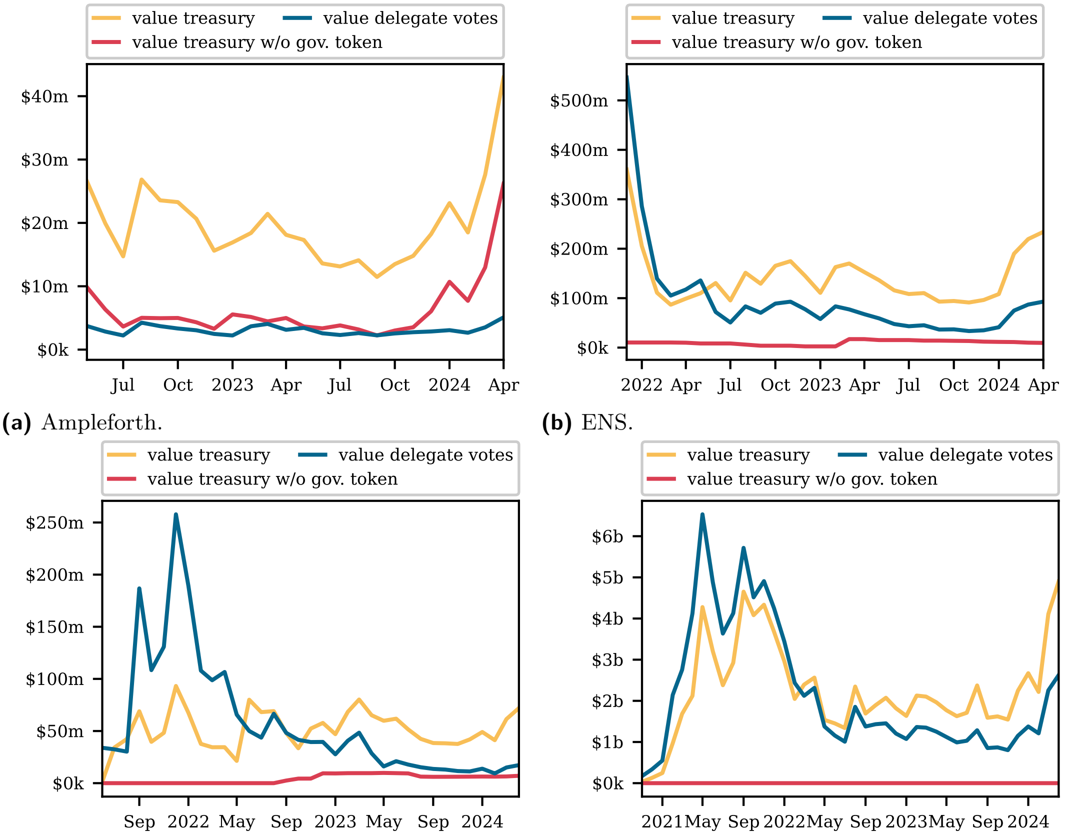
Table 2 An empirical analysis of the susceptibility of a set of 26 DAOs on the Ethereum blockchain as well as Layer 2s Arbitrum and Optimism to the risk factors presented in Section 5. The data is as of the last block of 31 March 2024 on the respective blockchain and block number delays are indicated according to the underlying chain. Any mention of the average votes refers to an average of the previous five executed votes that were not canceled for each DAO. Additionally, the available liquidity refers to the available liquidity of the respective governance token on Uniswap V2 and Uniswap V3 on Ethereum and Uniswap V3 on Arbitrum and Optimism. Finally, missing entries indicate that the respective risk factor measure does not apply to the DAO, e.g., the risk factor measures related to token delegation are only relevant for DAOs that require delegation.

	voter apathy (RF1)		**gov. token liquidity (RF2)**			**large treasury (RF3)**		**configuration (RF4)**			**centralization (RF5)**				**code (RF6)**	
DAO	avg. votes in % of delegated vote	avg. votes in % of token supply	avail. liquidity in % of proposal thresh.	avail. liquidity in % of delegated votes	avail. liquidity in % of avg. votes	treasury value w/ gov. token in % of delegated votes	treasury value w/o gov. token in % of delegated votes	proposal delay in blocks	voting period in blocks	timelock delay in blocks	Nakamoto coefficient of delegated votes	Nakamoto coefficient of token supply	number EOAs holding more gov. token than delegated votes	guardian	ownership renounce [25]	mint function [25]
Aave		3.21	8.74		4.53			7,200	72,000			8		✓	✗	✓
Ampleforth	81.13	4.58	93.55	8.64	10.02	837.18	508.76	13,140	19,710	172,800	3	5	4	✗	✗	✗
ArbitrumCore		0.85	1,595.42		18.68			21,600	100,800			6		✓	✓	✗
ArbitrumTreasury		0.72	1,595.42		22.19			21,600	100,800			6		✓	✓	✗
Babylon	32.07	8.71	52.68	1.80	3.02	0.00	0.00	1	45,818	86,400	4	2	0	✗	✗	✓
Braintrust	75.93	0.10	182,186.84	2.92	381.12	29.83	0.00	1	17,280	604,800	1	15	0	✓	✗	✗
Compound	22.19	5.12	300.00	4.26	14.64	1.21	0.94	13,140	19,710	172,800	12	12	0	✗	✗	✗
Cryptex	48.02	5.79	0.01	0.00	0.00	294.88	1.06	1	17,280	259,200	3	3	0	✓	✗	✗
Curve		47.46			2.35				604,800			2			✗	✗
ENS	33.91	1.47	124.80	3.01	8.49	251.78	10.21	1	45,818	172,800	17	1	0	✗	✗	✓
Fei	18.78	4.83	399.22	9.63	20.67	0.00	0.00	1	13,000	86,400	14	2	0		**?**	**?**
Gas	54.85	1.08	116.82	18.61	10.78	0.00	0.00	1	45,818	0	2	2	4	✗	✗	✗
Gitcoin	34.31	2.92	217.49	4.02	11.17	416.09	40.89	13,140	40,320	172,800	3	3	1	✗	✗	✗
Hifi	51.80	1.98	216.31	2.11	3.87	0.00	0.00	13,140	36,000	172,800	4	2	3	✗	✗	✗
Hop	24.07	0.42	361.06	22.42	85.17	3,396.69	0.00	1	45,818	172,800	7	1	0	✗	✗	✓
Idle	24.82	7.88	365.90	11.61	46.46	0.00	0.00	100	17,280	172,800	2	6	0	✗	✗	✗
InstaDapp	22.25	4.65	440.24	21.04	94.62	0.00	0.00	7,200	14,400	172,800	3	3	0		✓	✗
Lido		4.11			8.41				21,600			10		✗	✓	✗
Maker		15.10			20.94							16		✗	✓	✓
Optimism	35.61	1.11	∞	3.03	5.72				259,200		10	3	1	✗	✗	✓
Pooh	1.38	0.11	4,545.07	68.55	4,203.75	0.00	0.00	1	50,400	259,200	2	35	0	✓	**?**	**?**
Radicle	37.22	3.98	95.61	9.16	24.05	489.50	25.56	1	17,280	172,800	2	2	0	✗	✗	✗
Silo	26.26	2.09	1,183.54	0.97	5.66	161.22	0.00	128	21,000	172,800	3	3	0	✓	✗	✓
Strike	70.15	2.00	39.50	17.00	19.65	0.00	0.00	1	17,280	172,800	1	2	2	✓	✗	✗
Sudoswap	21.50	2.81	425.47	23.51	78.18	274.26	0.00	14,400	21,600		6	2	0	✗	✗	✓
Uniswap	25.14	4.96	325.10	1.60	6.55	186.66	0.00	13,140	40,320	172,800	16	10	0	✗	✗	✗

this appears promising, we underline that the figures presented are a strict lower bound as they for example do not include centralized exchanges where the available liquidity is not easily quantifiable. Even though for the analyzed DAOs liquidity currently appears low, we presented 14 attacks that still attempt to exploit DAOs through token control (see Section 4). Thus, we reiterate that for a DAO's safety, lower liquidity is advantageous.

Large Treasury (RF3). The impact and attractiveness of an attack increase, the more value is stored in the treasury. Since in the aftermath of an attack, token prices are expected to plummet, we wager that the treasury value excluding the governance token itself is the most important driving factor. Our empirical analysis in Table 2 presents the treasury value with respect to the value of all delegated tokens, both with and without the governance token. A considerable chunk of DAOs (i.e., 6) hold less than 10% of their treasury value in tokens other than their governance token and are thus likely less at risk for a governance attack that aims to empty the treasury. Startlingly, for the Ampleforth DAO, the value of the treasury without the governance tokens exceeds the value of all delegated tokens – making it an attractive target for attacks. Additionally, we highlight that if the value of the treasury (without the governance token) exceeds 50% of the delegated votes, 51% attacks of token holders that have delegated their tokens could be rational. A few DAOs are close to reaching this threshold (e.g., Gitcoin) or have been in the past. Note that we are not aware of any precedence for such an attack, but protocols have forked before [65]. In addition to the empirical snapshot of 31 January 2024 presented in Table 2, for a smaller subset of DAOs we also visualize the historical value of the treasury in comparison to the delegated token values (see Figure 1). We observe significant fluctuations over time in the relative value of the delegate tokens in comparison to the treasury for the three DAOs: Ampleforth, ENS, Gitcoin, and Uniswap. While initially for three of the DAOs (i.e., ENS, Gitcoin, and Uniswap) the value of the delegate votes (blue line) exceeded the value of the treasury (yellow line) this is no longer the case for all of them. For these DAOs, except for Uniswap (which does not hold tokens other than its governance token), the difference between the value of the delegate votes and the value of the treasure without the governance token is shrinking over time. Finally, for Ampleforth the value of the delegate votes never exceeded the value of the treasury and also currently does not exceed the value of the treasury without the governance token. We conclude that DAOs need to constantly monitor the value of the treasury to ensure that they are not an attractive target for token control attacks.

Inadequate Configuration (RF4). Inadequate configuration of voting contracts can leave a wide scope of vulnerabilities open. We discuss the most important parameters in the following. First, *proposal delay*, i.e., the delay between proposal creation and the start of the voting period, must be larger than 0 to avoid flash loan attacks. A proposal delay of 1 block, as used by DAOs (see Table 2) is also not without issues though, especially for DAOs that require delegation. Such a small delay does not leave time for non-delegated tokens to be delegated in case of a malicious proposal. For similar reasons, a short *voting window*, might also be dangerous, as delegates might not be reached in time to vote against a malicious proposal. However, all DAOs we analyzed have a voting window that runs for a couple of days (e.g., there are around 7,000 blocks a day on Ethereum). Finally, adjusting the duration a proposal must remain in the timelock can also be beneficial, i.e., *timelock delay*. Extending this period forces an attacker to maintain a number of votes, at least equal to the proposal threshold, for a longer duration. This approach increases the risk for the attacker and makes the potential profits less predictable.



(a) Ampleforth.

(b) ENS.

(c) Gitcoin.

(d) Uniswap.

Figure 1 Comparison of treasury values and the total value of all delegated governance tokens. If the value of the treasury (yellow line) or even the value of the treasury without the governance token (red line) exceeds the value of delegate votes (blue line) this represents an economic risk.

Centralization (RF5). If a large (delegated) token supply is held only by a few addresses or entities, many attack vectors become more likely to succeed (e.g., majority coalition, whale activation). In Table 2, we show the Nakamoto coefficient of the delegate votes and the token supply, i.e., the minimum number of addresses collectively holding more than 50% of the delegate votes and the token supply. The lower the Nakamoto coefficient, the higher the centralization. We find that, startlingly, for three DAOs the Nakamoto coefficient of the delegate tokens is one – one delegate has the majority of delegate votes. Finally, we also consider the number of *externally owned addresses (EOAs)* that hold more governance tokens than are currently delegated. Importantly, more than one holder can hold more votes than delegated governance votes, as not all tokens are delegated. These EOAs could delegate their tokens and would have a majority of the delegate tokens. In combination with a small proposal delay (RF4), they could easily acquire the majority of votes. For six DAOs there was at least one EOA that could perform such a 51% attack on 31 March 2024. Additionally, we also analyze how this figure evolves over time for the five DAOs of these DAOs on the Ethereum blockchain in Figure 2. We observe that for these five DAOs, there was generally at least one EOA that held sufficient tokens for a 51% attack and thereby posed a threat.

Table 2 also shows that some DAOs have a guardian in their governance contract or in their timelock contract. This involves special rights that, for example, enable an EOA or a multi-signature wallet to cancel proposals. On the one hand, this functionality can be abused and lead to a situation where only decisions that aren't canceled by the guardian can be

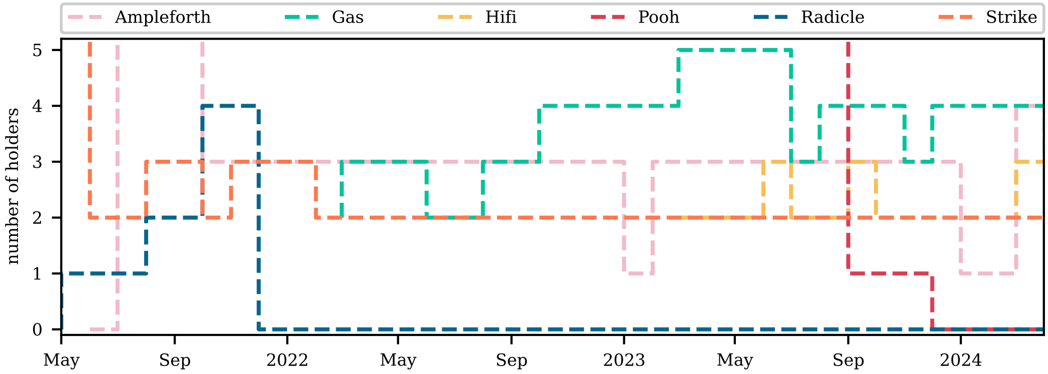


Figure 2 Number of holders, i.e. EAOs, who hold more tokens than delegated governance votes on a monthly basis. These holders would have the majority of the delegated votes after they delegate their tokens.

made, or if not implemented carefully, give the guardian privileged access to the treasury or other critical infrastructure. On the other hand, a trustworthy guardian can mitigate the effect of malicious proposals.

Code Uncertainties (RF6). When smart contracts are created, the contract bytecode that is uploaded on-chain can contain arbitrary logic. As smart contracts may contain various unknown mechanisms, any uncertainty can be viewed as risky. Firstly, the smart contract creators should thus publish the source code, allowing anyone to verify its logic. Additionally, some code functionalities are associated with a higher risk. For instance, the presence of a mint functionality might allow an attacker to create more tokens. The mint function can be a particular risk as it allows attackers to empty the liquidity pools with the governance token (see Build Finance and Curio in the Appendix of the full version [51]). We observe in Table 2 that five of the analyzed DAOs implement such functionality in their smart contract. Risks are also associated when external calls are allowed, and when a proxy contract is used (as the proxy contract may be changed to point to a different contract, bypassing the DAO) [31, 16]. Table 2 shows that only for one DAO the ownership of the contract was renounced. This is considered a good practice, as the contract then cannot be called with elevated owner privilege anymore [24].

Lack of Reliable Communication Channels (RF7). DAO community members mainly communicate through X (formerly Twitter), Telegram, and Discord. These platforms are crucial parts in defending an attack, as seen in the Indexed Finance case study presented in Section 3.2. Still, it is difficult to reach all delegates and token holders, especially if the projects are no longer active, as was the case for Indexed Finance. Thus, better infrastructure to reliably reach holders and inform them about ongoing governance votes would be beneficial. To the best of our knowledge, none of the DAOs we have analyzed have implemented any more reliable communication channels than those mentioned in the beginning.

The described risk factors are diverse and thus preventing against them all simultaneously is a difficult task. Our empirical evaluation of 26 DAOs and their susceptibility to these risk factors also revealed that smaller DAOs tend to be more at risk. For these DAOs, in the absence of the same resources as their larger counterparts, it is likely especially hard to protect against all possible attack vectors. Thus, especially smaller projects should weigh the benefits and disadvantages of a DAO carefully. For those, that choose a DAO as their governance form we continue by describing and discussing safeguards.

6 Mitigation and Safeguards

We present and discuss mitigation strategies to reduce risks. Throughout, we distinguish between mitigations that lower the impact (🚀) of an attack and those that lower the likelihood (❓) of success for an attack. In parentheses, we specify which attack vector categories are targeted.

Conservative Implementation 🚀 ❓ (BR, TC, HCI, CP). Through conservative implementation, DAOs make sure that exogenous factors cannot be exploited to attack a DAO. Examples include *limiting the number of proposals* that can be made by a single proposer at any given time [116] to prevent spamming attacks and having long enough *proposal delays* (see Section 5). This involves trade-offs, as extending the on-chain proposal process can make an attack less appealing, but it also slows down governance in general. Thus, a balance must be struck between a DAO's agility and safeguarding against potential attacks. We further note that a lack of agility for a DAO can pose additional risks depending on the protocols they govern [66, 67].

Limiting the Governance Scope 🚀 (BR, TC, HCI, CP). Another approach to lessening the impact of attacks is for a DAO to add restrictions on its action space that can reduce the attack surface. For instance, if the DAO is only granted control over a few parameters, the extent of potential attacks is much narrower. Additionally, one can imagine only allowing a proposal to spend a fixed maximum amount of the treasury.

Emergency Shutdown 🚀 (BR, TC, HCI, CP). Implementing an emergency shutdown is a very invasive mitigation strategy. Here, a set of holders can halt all transactions. In the case of MakerDAO [84], the emergency shutdown allows token holders to receive a share of the treasury, mitigating potential attacks that were underway.

Governance Forks 🚀 ❓ (BR, TC, HCI, CP). A similar, but less drastic, safeguard could be achieved through forking, a design primitive where a fraction of token holders can vote to create a fork of the DAO. For instance, The DAO allowed token holders to create *child DAOs* and later withdraw their portion of the DAO deposits from there. Another example of the occurrence of a DAO fork is NounsDAO: A large fraction of holders decided to leave the original DAO for a forked DAO taking with them their proportional share of the treasury [53]. The forked DAO then allowed each token holder to *rage-quit* and retrieve their individual share of the treasury. This process is usually not very fast, and thus can typically only prevent foreseeable attacks. Nonetheless, allowing DAOs to fork is a possibility to prevent a majority (coalition) from taking over a DAO (and its treasury). With a fork, a minority would still have the possibility to take their part of the DAO's assets. However, if a DAO governs more than a fungible treasury, e.g., the parameters of a lending protocol, forking may of course not be a viable option.

User Authentication ❓ (BR, TC). Through user authentication, voting power is to be constrained on a per-person basis. This can enable different voting mechanisms, that might be less vulnerable to token control attacks, such as *quadratic voting* (voting power is proportional to the square root of tokens owned) and *democratic voting* (one person one vote). Examples of user authentication include *know-your-customer (KYC)* or decentralized identifiers, like *Proof-of-Personhood* [15]. The Optimism Governance recently implemented a form of user authentication. In particular, they implement a bicameral governance design, with a token house [97] (one token one vote) and a citizen house [96] (one person one vote), only those with citizenship can vote in the citizen house.

Ballot Privacy ❓ (HCI) Ensuring ballot/tally privacy during the voting period can help in mitigating behavioral manipulations (HCI5). Cicada [57] is an existing framework for the EVM which achieves this. While it is costly to implement on Ethereum, the costs are more reasonable on L2s.

Governance Tools ❓ (HCI). The development of novel governance tools reduces the hurdles of participation in governance and can help prevent HCI attacks. For instance, through better communication and notifications on current proposals, voter apathy can be combated. Moreover, they may provide the necessary education for voters to be able to make informed decisions more easily, also mitigating behavioral manipulations (HCI5). We believe it is important that these tools are open-source (i.e., such that bugs as in the Tally [110] case are less likely to happen) and that they cannot easily be spammed or taken down. While these tools can do a great part in reducing the load in governance participation, they can become potential attack victims themselves (see Section 3.3).

Veto Power ❓ (HCI). DAOs may also introduce a veto functionality. Through a veto, a small group of holders can prolong a vote, giving the holders more time to counter malicious proposals. Excessive use of veto power itself leads to issues, but we hypothesize that incentives could deter its misuse (e.g., vetoing could be made expensive).

Objection Phase and Vote Extension ❓ (HCI). A more targeted safeguard consists of the addition of a second round of voting (also called *objection phase*), where voters can only vote against the proposal, or change their vote from in favor to against. This has been introduced by Lido [80], with the goal to protect the DAO from vote sniping (see HCI5). Other proposed remedies to vote sniping include the extension of the voting period after high activity (or sway votes) are observed, as well as randomized voting durations. Both have recently been suggested by Decentraland DAO [40].

Scheduled Voting Windows 🚀 (HCI). Some protocols are experimenting with votes being scheduled on a regular basis (e.g., once a month). This can prevent proposal spam (HCI3) to reduce voter apathy and dampen the effect of behavioral manipulations (HCI5).

Escape Hatches 🚀 (CP). Escape hatches can be added to DAOs to limit the severity of an attack. The *Decentralized Escape Hatch* proposed by Eyal and Sirer [49] for example suggests that outgoing transactions can be buffered (e.g., for 24 hours). Buffered transactions can then be reversed automatically, by specifying programmatic invariants. Such invariants could for example limit the outflow over time, or check whether outflow is consistent with respective inflows. Note that invariants themselves are hard to get right. The authors, thus, also suggest community involvement by crowdsourcing the reversal, for example through a majority involvement.

Bug Bounties 🚀 ❓ (CP). A widespread and important tool to prevent technical attacks is bug bounties. Their extent has been researched in a broader context of cybersecurity and was shown to be a cost-effective instrument [118]. Bug bounties are widespread in the blockchain ecosystem and advertised by several DAOs.

Audits ❓ (CP). Last but not least, audits by external companies can help verify that the DAOs underlying smart contracts are implemented to the state-of-the-art. Audits will make sure that code best practices are respected [32], according to the platform and language used. We observe that audits typically focus on technical vulnerabilities. While we find that they could also consider the more governance-specific attack vectors we present, technical audits also hold immense importance for the security of DAOs.

7 Related Work

Possible attacks on DAOs have been discussed in blog posts almost as long as DAOs have existed [86, 37] including by Ethereum's founder Vitalik Buterin [19, 20]. Among other things, they discuss the risks of low voter participation, centralization, game-theoretic attacks, and vote buying, as well as possible mitigation strategies such as *limited governance*, *non-coin-driven governance*, and *skin in the game*.

An early instance of a DAO governance attack documented in academic literature is a potential attack on the governance of the MakerDAO protocol, the centerpiece of DeFi at the time, by Gudgeon et al. [60]. More recently, Augsten et al. [5] have discussed the potential of hidden vote buying in DAO governance facilitated by smart contracts, i.e., what is referred to as *Dark DAOs*. Related to the attack on DAO governance, the term *Governance Extractable Value (GEV)* has been coined to describe the potential value that can be gained from influencing DAO governance votes [78]. Note that the term is an homage to the widely-studied concept of *Miner/Maximal Extractable Value (MEV)* [36].

Two recent systematizations of knowledge (SoKs) cover topics related to DAO attacks: Zhou et al. [123] survey hacks and incidents in DeFi protocols in general. However, most described attacks are not attacks on the protocol's governance system, which we focus on in this paper. A general overview and systematization of the concept of governance for blockchains and blockchain-based protocols can be found in the SoK by Kiayias and Lazos [71]. It discusses the governance processes of blockchains such as Bitcoin and Ethereum, along with examples of protocols running on blockchains – which are the focus of our SoK. Additionally, Ethereum's governance process, including which actors have how much influence on it, has also been studied in detail by Fracassi et al. [55]. To the best of our knowledge, this paper represents the first SoK to study attack vectors, risks, and possible mitigation of attacks on the governance of DAOs.

Recently, the literature surrounding DAOs has rapidly expanded, including two reports of the WEF on DAOs [58, 59]. This encompasses a flurry of empirical studies on a variety of DAOs covering aspects such as token distributions, voting turnout and voting behavior [56, 7, 52, 6, 109, 44, 104, 72, 89]. In particular, many of the studies (see e.g., Feichtinger et al. [52]) make a number of observations relevant to attacks covered in this paper: They reveal that a majority of voting power is often concentrated in the hands of a very small number of holders and delegates. Additionally, they highlight that participation rates in governance votes are frequently low across many DAOs.

The vast majority of DAOs today, including those covered in the aforementioned studies, use simple token voting (one-token-one-vote). An alternative governance model using *vote escrowed* tokens (governance tokens locked for a fixed time period), which is for instance used by Curve and Balancer, is discussed by Lloyd et al. [82].

Finally, Tan et al. [111] describe open research problems surrounding DAOs in fields ranging from computer science and economics to ethics, law, and politics.

8 Conclusion

In this paper, we systematically analyzed potential attacks on DAOs along with 28 real-world incidents to illustrate the scope of security vulnerabilities. By describing and categorizing the multitude of attack vectors, we provided a comprehensive overview of the threats faced by DAOs. Additionally, we identified and empirically measured risk factors across a set of 26 DAOs, offering insights into the prevalent risks and their impact.

We believe that it is highly advisable for a DAO to engage early with the possibility of such an attack, to monitor parameters closely, and to ensure that an attack does not become economically attractive. Understanding these challenges is critical when designing and operating a DAO, and poses a significant challenge to DAOs. Ultimately, with our systematization of attacks on DAOs, the vulnerabilities of DAOs, and possible safeguards, we seek to arm future DAO designs with the necessary knowledge to anticipate and mitigate these threats.

References

1 Zack Abrams. Indexed dao to distribute remaining treasury after defeating hijack attempts. `https://www.theblock.co/post/264679/indexed-dao-to-distribute-remaining-treasury-after-defeating-hijack-attempts`, 2023.

2 AnnabelTUSD. Open letter to the makerdao community from tusd. `https://forum.makerdao.com/t/open-letter-to-the-makerdao-community-from-tusd/12753/1`, 2022.

3 Victor Araújo and Malu AC Gatto. Casting ballots when knowing results. *British Journal of Political Science*, 52(4):1709–1727, 2022.

4 James Austgen, Andres Fabrega, Sarah Allen, Kushal Babel, Mahimna Kelkar, and Ari Juels. Daos must confront dark daos — or fall under their shadow. `https://initc3org.medium.com/daos-must-confront-dark-daos-or-fall-under-their-shadow-b4c47cb6a1be`, 2024.

5 James Austgen, Andrés Fábrega, Sarah Allen, Kushal Babel, Mahimna Kelkar, and Ari Juels. Dao decentralization: Voting-bloc entropy, bribery, and dark daos, 2023. `arXiv:2311.03530`.

6 Tom Barbereau, Reilly Smethurst, Orestis Papageorgiou, Johannes Sedlmeir, and Gilbert Fridgen. Decentralised finance's timocratic governance: The distribution and exercise of tokenised voting rights. *Technology in Society*, 73:102251, 2023. `doi:10.1016/j.techsoc.2023.102251`.

7 Tom Josua Barbereau, Reilly Smethurst, Orestis Papageorgiou, Alexander Rieger, and Gilbert Fridgen. Defi, not so decentralized: The measured distribution of voting rights. In *Proceedings of the Hawaii International Conference on System Sciences 2022*, page 10, 2022.

8 Rob Behnke. Explained: The mochi inu governance hack (november 2021). `https://www.halborn.com/blog/post/explained-the-mochi-inu-governance-hack-november-2021`, 2021.

9 Rob Behnke. Explained: The Tornado Cash Hack. `https://www.halborn.com/blog/post/explained-the-tornado-cash-hack-may-2023`, May 2023.

10 Jan Behrens. The origins of liquid democracy. *The Liquid Democracy Journal on electronic participation, collective moderation, and voting systems*, 5, May 2017. URL: `https://liquid-democracy-journal.org/issue/5/The_Liquid_Democracy_Journal-Issue005-02-The_Origins_of_Liquid_Democracy.html`.

11 Tom W Bell. Blockchain and authoritarianism: The evolution of decentralized autonomous organizations. In *Blockchain and Public Law*, pages 90–104. Edward Elgar Publishing, 2021.

12 BIGCAP. Community alert! this is scam dao proposal. `https://twitter.com/BIGCAPProject/status/1697958233204490494`, 2023. Twitter post.

13 Everything Blockchain. Beanstalk Exploit - A Simplified Post-Mortem Analysis. `https://medium.com/coinmonks/beanstalk-exploit-a-simplified-post-mortem-analysis-92e6cdb17ace`, 2022.

14 BlockSec. Twitter post on temple dao attack. https://twitter.com/BlockSecTeam/status/1579843881893769222, 2022.

15 Maria Borge, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, and Bryan Ford. Proof-of-personhood: Redemocratizing permissionless cryptocurrencies. In *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 23–26. IEEE, 2017.

16 Boring Security. All About Proxy Contracts. https://boringsecurity.com/articles/all-about-proxy-contracts, 2023.

17 James M. Buchanan. Simple majority voting, game theory, and resource use. *Canadian Journal of Economics and Political Science*, 27(3):337–348, 1961. doi:10.2307/139591.

18 BuildFinance. Twitter post on governance attack. https://twitter.com/finance_build/status/1493223190071554049, 2022.

19 Vitalik Buterin. Notes on blockchain governance. https://vitalik.eth.limo/general/2017/12/17/voting.html, 2017.

20 Vitalik Buterin. Moving beyond coin voting governance. https://vitalik.eth.limo/general/2021/08/16/voting3.html, 2021.

21 Steven Callander. Bandwagons and momentum in sequential voting. *The Review of Economic Studies*, 74(3):653–684, 2007.

22 Certik. Exploiting a smart contract without security vulnerabilities: Analysis of true seigniorage dollar attack event. https://www.certik.com/resources/blog/exploitingasmartcontractwithoutsecurityvulnerabilitiesanalysisoftrueseignioragedollarattackevent, 2021.

23 Certik. Security Assessment GameDAO. https://skynet.certik.com/projects/gamedao, 2021.

24 Certik. Securing The Web3 World. https://www.certik.com/, 2023.

25 Certik. Top DAO Dashboards. https://skynet.certik.com/boards/dao, 2024.

26 ChainSecurity. Security Audit of POA NETWORK's Smart Contracts. https://chainsecurity.com/wp-content/uploads/2019/03/ChainSecurity_PoA.pdf, 2018.

27 ChainSecurity. Code Assessment of the Hoprnet Token Smart Contracts. https://cdn.prod.website-files.com/65d35b01a4034b72499019e8/6644c996df51a11845ac7de3_210629_HOPR-Token_Smart-Contract-Audit-Report_ChainSecurity_compressed.pdf, 2021.

28 ChainSecurity. Code Assessment of the Snapshot X Smart Contracts. https://cdn.prod.website-files.com/65d35b01a4034b72499019e8/6645a5f08d64f89be8ee4856_ChainSecurity_PoA_compressed.pdf, 2023.

29 coinlive. Synthetify suffers $230,000 loss due to governance failure. https://www.coinlive.com/news-flash/298994, 2023.

30 Cointelgraph. Hacker drains $1.08M from Audius following passing of malicious proposal. https://cointelegraph.com/news/hacker-drains-1-08m-from-audius-following-passing-of-malicious-proposal, 2022.

31 Consensys. Ethereum Smart Contract Best Practices. https://consensys.github.io/smart-contract-best-practices/development-recommendations/general/external-calls/, 2023.

32 Consensys. Ethereum smart contract best practices. https://consensys.github.io/smart-contract-best-practices/development-recommendations/, 2023.

33 Tim Copeland. Steem vs tron: The rebellion against a cryptocurrency empire. https://decrypt.co/38050/steem-steemit-tron-justin-sun-cryptocurrency-war, 2020.

34 Tim Copeland. Build finance dao suffers 'hostile governance takeover' loses $470,000. https://www.theblock.co/post/134180/build-finance-dao-suffers-hostile-governance-takeover-loses-470000, 2022.

35 Phil Daian. Analysis of the dao exploit. https://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/, 2016.

36 Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 910–927, 2020. doi:10.1109/SP40000.2020.00040.

37 Philip Daian, Tyler Kell, Ian Miers, and Ari Juels. On-chain vote buying and the rise of dark daos. https://hackingdistributed.com/2018/07/02/on-chain-vote-buying/, 2018.

38 Mike Dalton. Build finance dao suffers governance takeover attack. https://cryptobriefing.com/build-finance-dao-suffers-governance-takeover-attack/, 2022.

39 Roxana Danila. Responsible vulnerability disclosure. https://medium.com/nexus-mutual/responsible-vulnerability-disclosure-ece3fe3bcefa, 2020.

40 Decentraland. Change Gov Mechanism to Mitigate Last-Minute Voting in DAO. https://decentraland.org/governance/proposal/?id=00a79921-2dca-4bde-829e-3a503fc602c2, 2024.

41 DeepDAO. Organizations. https://deepdao.io/organizations, 2023.

42 Defillama. Dexes tvl rankings. https://defillama.com/protocols/dexes/Ethereum, 2023.

43 True Seigniorage Dollar. Twitter post on TSD attack. https://twitter.com/TrueSeigniorage/status/1370956726489415683, 2021.

44 Maya Dotan, Aviv Yaish, Hsin-Chu Yin, Eytan Tsytkin, and Aviv Zohar. The vulnerable nature of decentralized governance in defi. In *Proceedings of the 2023 Workshop on Decentralized Finance and Security*, DeFi '23, pages 25–31, New York, NY, USA, 2023. Association for Computing Machinery. doi:10.1145/3605768.3623539.

45 Quinn DuPont. Experiments in algorithmic governance: A history and ethnography of "the dao," a failed decentralized autonomous organization. In *Bitcoin and beyond*, pages 157–177. Routledge, 2017.

46 Ehterscan. Build Finance. https://etherscan.io/tx/0xf7709b0587d89b9d9b04ca04ce54fdc02a5a30435daf1fb4ba1174486e365c9f, 2022. Ethereum transaction.

47 Avraham Eisenberg. Twitter post on mango markets. https://twitter.com/avi_eisen/status/1581326197241180160, 2022.

48 Etherscan. Yuan Finance. https://etherscan.io/tx/0x4556acce865abe3304eefc7d055112afdcab0d64f838790b46fa0d6dde189c9b, 2021. Ethereum transaction.

49 Ittay Eyal and Emin Gün Sirer. A Decentralized Escape Hatch for DAOs. https://hackingdistributed.com/2016/07/11/decentralized-escape-hatches-for-smart-contracts/, 2016.

50 Corin Faife. How to stole an election: BeanStalk DAO $80million FlashLoan attack study case. https://blog.verichains.io/p/how-to-stole-an-election-beanstalk, 2022.

51 Rainer Feichtinger, Robin Fritsch, Lioba Heimbach, Yann Vonlanthen, and Roger Wattenhofer. SoK: Attacks on DAOs, 2024. arXiv:2310.19201.

52 Rainer Feichtinger, Robin Fritsch, Yann Vonlanthen, and Roger Wattenhofer. The hidden shortcomings of (d)aos – an empirical study of on-chain governance. In *Financial Cryptography and Data Security. FC 2023 International Workshops*, pages 165–185, Cham, 2024. Springer Nature Switzerland.

53 Owen Fernau. Nouns NFT Holders Opt To 'Rage Quit' Through New Fork. https://thedefiant.io/nouns-nft-holders-opt-to-rage-quit-through-new-forky, September 2023.

54 Bryan Alexander Ford. Delegative democracy. Technical report, EPFL scientific publications, May 2002. URL: https://infoscience.epfl.ch/record/265695.

55 Cesare Fracassi, Moazzam Khoja, and Fabian Schär. Decentralized crypto governance? transparency and concentration in ethereum decision-making. *Transparency and Concentration in Ethereum Decision-Making (January 10, 2024)*, 2024.

56 Robin Fritsch, Marino Müller, and Roger Wattenhofer. Analyzing voting power in decentralized governance: Who controls daos?, 2022. arXiv:2204.01176.

57 Noemi Glaeser, István András Seres, Michael Zhu, and Joseph Bonneau. Cicada: A framework for private non-interactive on-chain auctions and voting. *Cryptology ePrint Archive*, 2023.

58 David Gogel, Bianca Kremer, Aiden Slavin, and Kevin Werbach. Decentralized autonomous organizations: Beyond the hype, June 2022. URL: https://www3.weforum.org/docs/WEF_Decentralized_Autonomous_Organizations_Beyond_the_Hype_2022.pdf.

59 David Gogel, Bianca Kremer, Aiden Slavin, and Kevin Werbach. Decentralized autonomous organization toolkit, January 2023. URL: https://www3.weforum.org/docs/WEF_Decentralized_Autonomous_Organization_Toolkit_2023.pdf.

60 Lewis Gudgeon, Daniel Perez, Dominik Harz, Benjamin Livshits, and Arthur Gervais. The decentralized financial crisis. In *2020 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 1–15, 2020. doi:10.1109/CVCBT50464.2020.00005.

61 Hacken. DAO Maker Audit Report. https://hacken.io/audits/dao-maker/, 2021.

62 Hacken. Consitution DAO Smart Contract Code Review and Security Analysis. https://wp.hacken.io/wp-content/uploads/2022/01/%D0%A1onstitution-DAO_11012022Audit_Report.pdf, 2022.

63 Halborn. Explained: The ForceDAO Hack (April 2021). https://www.halborn.com/blog/post/explained-the-forcedao-hack-april-2021, 2021.

64 Halborn. Explained: The Curio Hack (March 2024). https://www.halborn.com/blog/post/explained-the-curio-hack-march-2024, 2024.

65 Andrew Hayward. Nouns Fork: Disgruntled NFT Holders Exit With $27 Million From Treasury. https://decrypt.co/197400/nouns-fork-disgruntled-nft-holders-exit-27-million-from-treasury, 2023.

66 Lioba Heimbach, Eric Schertenleib, and Roger Wattenhofer. DeFi Lending During The Merge. In *5th Conference on Advances in Financial Technologies (AFT), Princeton, NJ, USA*, October 2023.

67 Lioba Heimbach, Eric Schertenleib, and Roger Wattenhofer. Short Squeeze in DeFi Lending Market: Decentralization in Jeopardy? In *3rd Workshop on Decentralized Finance (DeFi), Bol, Brac, Croatia*, May 2023.

68 Louis Husney. Mango markets madness: A case study on the mango markets exploit. https://infotrend.com/mango-markets-madness-a-case-study-on-the-mango-markets-exploit/, 2023.

69 Jimmy Aki. The curve wars. https://www.techopedia.com/definition/the-curve-wars, 2023.

70 James S. Jordan. *Majority rule with dollar voting*, pages 211–220. Springer Berlin Heidelberg, Berlin, Heidelberg, 2003. doi:10.1007/978-3-540-24784-5_13.

71 Aggelos Kiayias and Philip Lazos. Sok: Blockchain governance. In *Proceedings of the 4th ACM Conference on Advances in Financial Technologies*, AFT '22, pages 61–73, New York, NY, USA, 2023. Association for Computing Machinery. doi:10.1145/3558535.3559794.

72 Stefan Kitzler, Stefano Balietti, Pietro Saggese, Bernhard Haslhofer, and Markus Strohmaier. The governance of decentralized autonomous organizations: A study of contributors' influence, networks, and shifts in voting power, 2023. arXiv:2309.14232.

73 Kleros. Kleros Blocks Attack on POH Governor, Saves 46 ETH. https://typefully.com/Kleros_io/5yDM4vb, 2023.

74 Oliver Knight. Defi protocol temple dao struck by $2.3m exploit. https://www.coindesk.com/business/2022/10/11/defi-protocol-temple-dao-struck-by-23m-exploit/, 2022.

75 Jack Kubinec. Dao on solana loses $230k after 'attack proposal' goes unnoticed. https://blockworks.co/news/solana-exploit-dao-hacker, 2023.

76 Luh Luh Lan and Loizos Leracleous. Shareholder votes for sale, July 2005. URL: https://hbr.org/2005/06/shareholder-votes-for-sale.

77 Isabelle Lee. A crypto collective lost $470,000 after one individual amassed enough tokens to take control of the group's treasury. https://markets.businessinsider.com/news/currencies/build-finance-dao-treasury-discord-crypto-build-token-metric-2022-2, 2022.

78 Leland Lee and Ariah Klages-Mundt. Governance extractable value. https://ournetwork.substack.com/p/our-network-deep-dive-2, April 2021.

79 Adam Levi. A technical analysis of the genesis alpha hack. https://medium.com/daostack/a-technical-analysis-of-the-genesis-alpha-hack-f8e34433c14b, 2019.

80 Lido. Moving To Two-Phase Voting. https://blog.lido.fi/moving-to-two-phase-voting/, 2022.

81 Lioba Heimbach. DAO Vulnerability. https://github.com/liobaheimbach/DAOVulnerability, 2024.

82 Thomas Lloyd, Daire O'Broin, and Martin Harrigan. Emergent outcomes of the vetoken model. In *2023 IEEE International Conference on Omni-layer Intelligent Systems (COINS)*, pages 1–6, 2023. doi:10.1109/COINS57856.2023.10189201.

83 LongForWisdom. [Urgent] Flash Loans and securing the Maker Protocol. https://forum.makerdao.com/t/urgent-flash-loans-and-securing-the-maker-protocol/4901, 2020.

84 Maker. Maker Protocol Emergency Shutdown. https://docs.makerdao.com/smart-contract-modules/shutdown, 2023.

85 Shaurya Malwa. 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/, 2022.

86 Dino Mark, Vlad Zamfir, and Emin Gün Sirer. A call for a temporary moratorium on the dao. https://hackingdistributed.com/2016/05/27/dao-call-for-moratorium/, 2016.

87 Matt Hussey. What is Snapshot? The Decentralized Voting System. https://decrypt.co/resources/what-is-snapshot-the-decentralized-voting-system, 2021.

88 Reshef Meir, Kobi Gal, and Maor Tal. Strategic voting in the lab: compromise and leader bias behavior. *Autonomous Agents and Multi-Agent Systems*, 34:1–37, 2020.

89 Johnnatan Messias, Vabuk Pahari, Balakrishnan Chandrasekaran, Krishna P. Gummadi, and Patrick Loiseau. Understanding blockchain governance: Analyzing decentralized voting to amend defi smart contracts, 2024. arXiv:2305.17655.

90 Rebecca B Morton, Daniel Muller, Lionel Page, and Benno Torgler. Exit polls, turnout, and bandwagon voting: Evidence from a natural experiment. *European Economic Review*, 77:65–81, 2015.

91 Konstantin Nekrasov. DAO Voting Vulnerabilities. https://mixbytes.io/blog/dao-voting-vulnerabilities#rec506108657, 2023.

92 Neodyme. Twitter post on synthetify attack. https://twitter.com/Neodyme/status/1715149044794655145?s=20, 2023.

93 Evan Van Ness. Aragon vote shows the perils of onchain governance. https://evanvanness.com/post/184616403861/aragon-vote-shows-the-perils-of-onchain-governance, 2019.

94 Zach Obront. Agora Audit Report. https://github.com/voteagora/optimism-gov/blob/main/audits/23-05-12_zachobront.md, 2023.

95 OpenZeppelin Security. Technical Description of Critical Vulnerability in MakerDAO Governance. https://blog.openzeppelin.com/makerdao-critical-vulnerability, 2019.

96 Optimism. Citizens' house overview. https://community.optimism.io/docs/governance/citizens-house/, 2023.

97 Optimism. Token house history. https://community.optimism.io/docs/governance/token-house-history/, 2023.

98 Paladin. Documentation. https://doc.paladin.vote/, 2023.

99 Zubin Pratap. Reentrancy Attacks and The DAO Hack. https://blog.chain.link/reentrancy-attacks-and-the-dao-hack/, 2022.

100 Rikta Mandal. Venus Protocol Prevented Hostile Takeover Attempt. https://www.cryptotimes.io/2021/09/18/venus-protocol-prevented-hostile-takeover-attempt/, 2021.

101 Romain Rossello. Blockholders and strategic voting in daos' governance. *Available at SSRN 4706759*, 2024.

102 SEC. SEC Charges Avraham Eisenberg with Manipulating Mango Markets' "Governance Token" to Steal $116 Million of Crypto Assets. https://www.sec.gov/news/press-release/2023-13, 2023.

103 Mundus Security. Typical governance vulnerabilities: from DAO building to DAO smart contract audit. https://mundus.dev/blog/typical-dao-and-governance-smart-contracts-vulnerabilities, 2023.

104 Tanusree Sharma, Yujin Kwon, Kornrapat Pongmala, Henry Wang, Andrew Miller, Dawn Song, and Yang Wang. Unpacking how decentralized autonomous organizations (daos) work in practice, 2023. arXiv:2304.09822.

105 Shashank. Temple dao hack analysis. https://blog.solidityscan.com/temple-dao-hack-analysis-c96db856322c, 2022.

106 David Siegel. Understanding The DAO Hack. https://www.coindesk.com/learn/understanding-the-dao-attack/, 2023.

107 Statemind. KP3R Vulnerability Report. https://statemind.io/blog/kp3r-vulnerability-report, 2019.

108 Sujith Somraaj. Yam Finance Safeguards $3.1M Treasury From Governance Attack. https://decrypt.co/104848/yam-finance-safeguards-3-1m-treasury-governance-attack, 2022.

109 Xiaotong Sun, Charalampos Stasinakis, and Georigios Sermpinis. Decentralization illusion in decentralized finance: Evidence from tokenized voting in makerdao polls, 2023. arXiv:2203.16612.

110 Tally. Post mortem and impact summary: Tally voting bug. https://blog.tally.xyz/post-mortem-and-impact-summary-tally-voting-bug-6a12616ce717?gi=3bda9305d9b9, 2023.

111 Joshua Z. Tan, Tara Merk, Sarah Hubbard, Eliza R. Oak, Joni Pirovich, Ellie Rennie, Rolf Hoefer, Michael Zargham, Jason Potts, Chris Berg, Reuben Youngblom, Primavera De Filippi, Seth Frey, Jeff Strnad, Morshed Mannan, Kelsie Nabben, Silke Noa Elrifai, Jake Hartnell, Benjamin Mako Hill, Alexia Maddox, Woojin Lim, Tobin South, Ari Juels, and Dan Boneh. Open problems in daos, 2023. arXiv:2310.19201.

112 Team Audius. Audius Governance Takeover Post-Mortem 7/23/22. https://blog.audius.co/article/audius-governance-takeover-post-mortem-7-23-22, 2022.

113 Andrew Thurman. How did a former quadriga exec end up running a defi protocol? wonderland founder explains. https://www.coindesk.com/tech/2022/01/27/how-did-a-former-quadriga-exec-end-up-running-a-defi-protocol-wonderland-founder-explains/, 2021.

114 Andrew Thurman. 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/, 2022.

115 TrailOfBits. Curve DAO Security Assessment. https://github.com/trailofbits/publications/blob/master/reviews/CurveDAO.pdf, 2020.

116 Uniswap. GovernorBravoDelegate. https://github.com/gettty/uniswap-gov/blob/main/contracts/GovernorBravoDelegate.sol, 2024.

117 Vitalik Buterin. DAOs, DACs, DAs and More: An Incomplete Terminology Guide. https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide, 2014.

118 Thomas Walshe and Andrew Simpson. An empirical study of bug bounty programs. In *2020 IEEE 2nd International Workshop on Intelligent Bug Fixing (IBF)*, pages 35–44. IEEE, 2020.

119 Aviv Yaish, Svetlana Abramova, and Rainer Böhme. Strategic vote timing in online elections with public tallies. *arXiv preprint arXiv:2402.09776*, 2024.

120 Ryan Youngjoon Yi. Digixdao: A divorce story – a case study for voting systems and cryptonative arbitrage. https://blog.coinfund.io/digixdao-divorce-story-6ed74b00e2bd, February 2020.

121 Yuan Finance. Yuan Governance Attack Update and Migration Plan. https://medium.com/yuan-finance/yuan-governance-attack-update-and-migration-plan-3b5d949ab466, 2021.

122 zefram.eth. Twitter post on mochi. https://twitter.com/boredGenius/status/1458732732540854276, 2021.

123 Liyi Zhou, Xihan Xiong, Jens Ernstberger, Stefanos Chaliasos, Zhipeng Wang, Ye Wang, Kaihua Qin, Roger Wattenhofer, Dawn Song, and Arthur Gervais. Sok: Decentralized finance (defi) attacks. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 2444–2461. IEEE, 2023.

124 James Zou, Reshef Meir, and David Parkes. Strategic voting behavior in doodle polls. In *Proceedings of the 18th ACM conference on computer supported cooperative work & social computing*, pages 464–472, 2015.