SoK: Attacks on DAOs

Rainer Feichtinger, Robin Fritsch, Lioba Heimbach, Yann Vonlanthen, and Roger Wattenhofer

ETH Zurich
{rainerfe,rfritsch,hlioba,yvonlanthen,wattenhofer}@ethz.ch

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. To reveal 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.

1 Introduction

Decentralized Autonomous Organizations (DAO) are popular organizational structures that facilitate the trustless management of projects, by running atop of a blockchain. 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 many of the most-used decentralized applications on blockchains. They have gained popularity in various sectors, 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, Uniswap, and The Graph). Moreover, DAOs are estimated to hold and control in excess of $30B in their treasuries [17]. Consequently, they hold significant power and a central position in the blockchain ecosystem.

DAOs have been threatened by attacks and hacks ever since their inception. *"The DAO"* on Ethereum in 2016 was the first attempt at creating a DAO on a blockchain. However, an infamous hack stole $50M worth of ETH from the DAO before it even became operational [101]. The event was so severe that it led to a controversial hard fork of the Ethereum blockchain. The original (unforked) blockchain still operates and is known as Ethereum Classic. Notably, even before the fatal hack, other possible attacks on The DAO had been discussed [92]. The DAO hack highlights the significant threat attacks on DAOs 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 summarise 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 and coalition (BC) attacks (ii) token acquisition (TA) attacks, (iii) computer-human interaction (CHI) attacks, and (iv) code and protocol vulnerability (CP) attacks.
- We examine 23 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 historical precedence, we introduce seven risk factors for DAOs and empirically analyze how susceptible a set of 24 DAOs of all shapes and sizes is to them.
- Finally, we collect and discuss various mitigations and safeguards that DAOs can implement.

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

2 Background

While DAOs are in practice primarily utilized for governing blockchain protocols, DAOs can in principle be formed by any group of individuals aiming to collectively pursue a common objective. However, 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 which come with voting rights. 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.

Any token holders with a sufficient amount of tokens (exceeding a threshold) can put forward a proposal, on which all token holders are then able to vote. If a majority of voting tokens votes in favor (each token counts as one vote), the proposal is accepted and, for some DAOs, executed on-chain automatically.

While in principle, each token holder could vote individually on every proposal, executing each voting transaction would incur a fee on the blockchain. To alleviate this burden off token holders, most DAOs employ a form of *delegative* or *liquid* democracy [42, 64] for voting. Generally, 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). These delegate addresses are then able to vote on proposals with the total amount of tokens they received through delegations.

Note that many DAO governance processes involve multiple steps, which could include discussions on public governance forums or off-chain *temperature check* votes before a final vote. However, these other steps are often mere social conventions. The final on-chain vote is the only obligatory part of the process.

3 Categorization of Attack Vectors

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

3.1 Bribing and Coalition

Under *bribing and coalition (BC)* attacks we group attacks in which an attacker makes a payment to change votes. This could take the form of paying to obtain voting rights of governance tokens for a certain proposal vote without acquiring the underlying token, which is often referred to as *vote buying*. Another possibility is directly bribing token holders or delegates. Similarly to bribing, governance voters can form a coalition to push through a governance proposal.

Given that vote buying has been documented in shareholder governance of traditional companies [84], it is a plausible future concern for DAO governance and was already been a topic of discussion since the early days of DAOs [47, 55].

Bribing Token Holders (BC1). Bribing token holders 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 BC4).

When voting power is highly centralized, as is the case for many DAOs at the time of writing [62], 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. This idea has been described by Buterin [46] and, applied to an attack on Bitcoin's PoW by Newman [96].

Vote Buying Protocols (BC2). 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 [24] 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. If a user wants to borrow voting power, a loan contract is automatically created. The borrowed amount of tokens 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 nonetheless. 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.

We perform an empirical analysis of Paladin Lending (see Appendix C) to show that low liquidity currently does not allow attacks exclusively using this attack vector.

Daian et al. [55] introduce a particular type of vote buying protocol: *DarkDAOs*. In addition to facilitating vote buying using smart contracts, DarkDAOs 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 DarkDAOs, 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 DarkDAOs at the time of writing, they have been theoretically studied by Austgen et al. [37], and proof-of-concept prototypes have been published [36].

Bribing Delegates (BC3). Instead of bribing token holders, an attacker could also attempt to bribe delegates to vote a certain way. 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 face the risk of criminal charges for accepting bribes.

Majority Coalition (BC4). 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 [45, 79]. 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 24 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. While not necessarily being an attack, such incentives (e.g., when the value of governance tokens falls below the treasury value) are an important aspect to keep in mind when designing a governance system. 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) [107].

3.2 Token Acquisition

This family of attack vectors is of the simplest nature. In *token acquisition (TA)* 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 take over the DAO, i.e., get their malicious proposal accepted in the absence of sufficient votes against the proposal.

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 more than 20 DAOs to this kind of attack.

Token Purchase (TA1). 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 24 DAOs. We find that it is relatively common for the total value of the treasury of a DAO to exceed the value of delegated tokens, 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 [22], 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 protocols governance token) via decentralized exchanges, self-delegated these tokens, initiated a proposal, voted in favor of this proposal, and sold the tokens again [22]. 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 forever tokens inaccessible. Importantly, as this proposal was created a day early, 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 message exchanges 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 ≈ $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.

The case of 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. At the time of writing, multiple DAOs are susceptible to attacks of this kind (see Section 5).

Token Loan (TA2). 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 [34]. A couple of days later, a similar failed attempt by Justin Sun took place in Compound's governance with borrowed COMP tokens [105].

Flash Loan (TA3). With a flash loan, an attacker can borrow governance tokens only for the duration of a single transaction. While attackers pay a fee to borrow the governance token, they do not need to post any collateral. Hence, flash loan attacks do not require access to significant funds. Many protocols protect against flash loan attacks by implementing a voting delay, i.e., a delay between the proposal creation and the voting period start. This prevents attackers from creating a proposal and voting on it with flash-loaned tokens since they are only controlled for the duration of a single transaction. Nonetheless, flash loan attacks on DAOs have occurred in the past, the most prominent example being a flash loan attack on the Beanstalk governance.

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 [1, 58, 61]. 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.

Inactive Whale (TA4). 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, 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 [91].

3.3 Computer-Human Interaction

The attack vectors compromised in the *computer-human interaction (CHI)* attack family lie 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 (CHI1). 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 [25]. 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 vote registered on the blockchain.

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 (CHI2). 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 [41, 58]. 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. The attacker then 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 [8].

Proposal Spam (CHI3). 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 acquisition attacks (see Section 3.2).

Case Study Synthetify

On 17 October 2023, an attacker gained access to the assets controlled by Synthetify's DAO [27, 28, 83]. 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.

Note that many protocols attempt to protect against such attacks by only allowing at most one active proposal per account, which needs to hold 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 the hope of tiring the DAO's voters who pay fees for every vote.

Social Infiltration (CHI4). 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 [33] 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.

Hacking Governance Participants (CHI5). The final CHI attack vector involves the possibility of an attacker gaining access to the private keys of central governance participants such as large delegates and token holders, or multisig signers. If successfully obtained, e.g., through a social engineering attack, these keys grant the attacker control over the voting power associated with these participants. Consequently, the security of DAO governance systems heavily relies on the security practices of its participants. Specifically, given that numerous DAOs are effectively controlled by a small number of addresses, i.e., prominent token holders and delegates, these individuals' security practices can make or break a governance system's integrity.

3.4 Code & Protocol Vulnerability

The final family of attack vectors, *code and protocol vulnerability (CP)* attacks, exploits code or logic vulnerabilities, either in the governance smart contracts or 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 [101]. 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. A majority of the Ethereum community decided to fork the chain to undo the damages of the hack. 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 do not 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 [2, 3]. 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 [29]. 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 [73].

Protocol Vulnerability (CP2). Vulnerabilities in the protocols associated with a DAO can extend to the DAO itself as a result of 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 [77]. Heisenberg manipulated the price oracle for MNGO, the protocol's native cryptocurrency and governance token, that allowed him to take out massive loans against the protocol's treasury which is controlled by the DAO. In doing so, Heisenberg effectively drained the treasury. He then went on to create a proposal in the DAO of the protocol 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 [13] and infamously described the hack as a "highly profitable trading strategy", was later charged by the US government for his attack [26].

The previously outlined incident exemplifies how the interconnectedness of a protocol and its DAO can pose a risk to the DAO. In case, such an intertwined nature is wished for or required, it is especially hard 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. In particular, we identify which attack vector(s) were used. Table 1 lists all (theorized) incidents we analyzed. For each, 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, for each (theorized) attack, we highlight which attack vectors of those introduced and discussed

	date	blockchain	attack purpose	successful	attack damages	bribing token holders (BC1)	vote buying protocols (BC2)	bribing delegates (BC3)	majority coalition (BC4)	token purchase (TA1)	token loan (TA2)	flash loan (TA3)	inactive whale (TA4)	UI issues (CHI1)	proposal obfuscation (CHI2)	proposal spam (CHI3)	social infiltration (CHI4)	hacking gov. part. (CHI5)	code vulnerability (CP1)	protocol vulnerability (CP2)
incidents & attacks																				
Beanstalk [8]	Apr 2022	ETH	$	✓	$182M							■			■					
BigCap DAO [16]	Sep 2023	ETH	$	✗						■					■					
Binance [91]	Oct 2022	ETH	?										■							
Build Finance [10, 12, 52, 56, 85]	Feb 2022	ETH	$	✓	$470K					■					■					
Compound [105]	Feb 2022	ETH	🏛	✗							■									
Curve A [78]	ongoing	ETH	🔄			■														■
Curve B [6, 40]	Nov 2021	ETH	🏛	✓		■														■
ForceDAO [73]	Apr 2021	ETH	$	✓	$367K															■
Genesis Alpha [87]	Feb 2019	ETH	$	✓	$90K															■
Indexed Finance [22]	Nov 2023	ETH	$	✗						■										
Kleros [82]	Jan 2024	ETH	$	✗											■					
Maker DAO B [89]	Oct 2020	ETH	🏛	✓								■								
Maker DAO C [34]	Jan 2022	ETH	🏛	✗							■									
Mango Markets [13, 26, 77]	Oct 2022	SOL	$	✓	$47M															■
Paladin Lending [24]	ongoing	ETH	🔄				■													
Steemit [4]	Feb 2020	STEEM	🏛	✓						■										
Synthetify [27, 28, 83]	Oct 2023	SOL	$	✓	$230K					■						■				
Tally [25]	Apr 2021	ETH	?											■						
Temple DAO [9, 11, 14]	Oct 2022	ETH	$	✓	$2.4M														■	
The DAO [53, 59, 101]	Jun 2016	ETH	$	✓	$50M														■	
Tornado Cash [21]	May 2023	ETH	$	✓	$2M					■					■					
True Seigniorage Dollar [7, 48]	Mar 2021	BSC	$	✓	$16K					■										
Wonderland DAO [33]	Jan 2022	ETH	🏛	✓													■			
academic papers & reports																				
Dark DAOs [36, 37, 55]	Jul 2018					■														
Maker DAO A [70]	Feb 2020	ETH								■	■	■								
Nexus Mutal [57]	Feb 2020	ETH																	■	
audits																				
Agora [15]	May 2023	OP																	■	■
Constitution DAO [72]	Jan 2022	ETH																		■
DAO Maker [71]	Mar 2021	ETH																		■
GameDAO [5]	Aug 2021	BSC																	■	
Keep3r Network [2]	Sep 2022	ETH																	■	
Maker DAO D [3]	May 2019	ETH																	■	

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 Appendix A.

in the previous sections are utilized. We provide a summary for all (theorized) attacks in Appendix A.

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 23 attacks analyzed, 3 utilized at least one attack vector from the BC category, 12 employed TA attack vectors, 8 involved CHI attack vectors, and 7 involved 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 exclusively belong to the CP category. Note that we only found a relatively small set of critical vulnerabilities that were 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 [29, 95]. Although most DeFi protocols are primarily susceptible to CP attack vectors [108], 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, 7 out of 23) combine attack vectors from multiple categories. This heterogeneous nature of attacks targeting DAOs can make it challenging for these organizations 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 24 DAOs of all shapes and sizes, we empirically analyze how at risk these DAOs are for each of our identified risk factors in Table 2. Note that we provide a brief description of our data collection process in Appendix B.

Voter Apathy (RF1). If token holders do not delegate or vote themselves, it becomes much easier for an attacker to pass malicious proposals. In 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, as well as 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 automatically not voting. When regarding the first two columns in Table 2, notice the relatively low participation from the delegated tokens at 41% across all DAOs. While some DAOs have a high participation of more than 95% (i.e., Braintrust), in other DAOs the participation of delegated tokens sits around 10% (i.e., Pooh and Pooltogether). Additionally, even more startlingly from the entire token supply only 4% of tokens participate in the governance on average 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 acquisition category we presented in Section 3.2 feasible. Table 2 shows that available liquidity on Uniswap (the biggest decentralized exchange on Ethereum in terms of *total value locked (TVL)* [18]) and Aave (the biggest lending platform on Ethereum in terms of TVL [23]). 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 three and four DAOs the available liquidity exceeds the delegated votes and the average number of votes respectively. While 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 twelve attacks that still attempt to exploit DAOs through token acquisition (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 (11/24) hold less than 1% of their

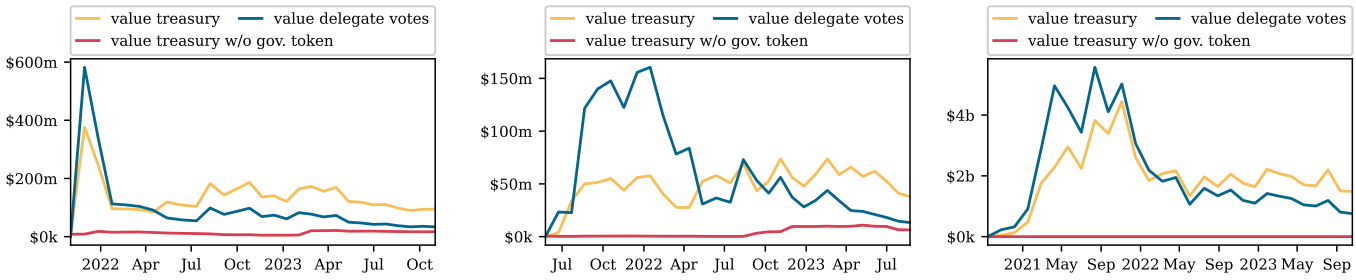
DAO	voter apathy (RF1)		gov. token liquidity (RF2)			large treasury (RF3)		configuration (RF4)			centralization (RF5)				code (RF6)	
	avg. votes in % of delegated vote	avg. votes in % of token supply	avail. liquidity in % of proposal thresh.	avail. liquidity in % of delegated votes	avail. liquidity in % 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	mint function
0xPlasma				401.56		1372.75	0.00	7200	36000	172800	1	4	4	✓	?	?
Ampleforth	80.49	4.63	127.73	11.21	9.58	693.47	287.96	13140	19710	172800	3	5	1	✗	✗	✗
Babylon	31.95	8.71	60.09	2.03	25.09	0.00	0.00	1	45818		4	2	0	✗	✗	✓
Braintrust	96.23	0.12	461328.56	15.30	375.81	55.55	0.00	1	17280	604800	1	15	2	✓	✗	✗
Compound	26.62	5.58	315.81	3.77	13.70	11.36	11.13	13140	19710	172800	10	12	0	✗	✗	✗
Cryptex	55.52	6.46	0.64	0.05	0.10	296.88	0.02	1	17280	259200	3	3	0	✓	✗	✗
ENS	33.97	1.47	1074.69	25.64	46.10	267.59	28.88	1	45818	172800	18	1	1	✗	✗	✓
Euler			104.02	3.03		0.00	0.00	11520	17280	172800	3	3	1	✓	✓	✗
Gas	51.73	1.08	391.71	62.41	59.65	4029.70	0.00	1	45818	0	2	2	4	✗	✗	✗
Gitcoin	33.72	5.23	56.59	3.66	11.44	284.58	47.62	13140	40320	172800	7	3	0	✗	✗	✗
Hifi	49.96	1.72	669.43	7.03	14.72	0.00	0.00	13140	36000	172800	5	1	2	✗	✗	✗
Hop	35.73	0.73	451.68	30.83	50.75	3854.69	40.97	1	45818	172800	10	1	0	✗	✗	✓
Idle	28.85	5.69	234.82	8.14	5.24	0.00	0.00	100	17280	172800	2	6	0	✗	✗	✗
Indexed	27.09	4.78	22.76	2.27	2.69	1294.92	831.75	1	17280	172800	5	2	0	✗	✗	✗
Instadapp	39.59	5.65	347.32	32.16	51.64	0.00	0.00	13140	19710	172800	2	3	0	✗	✗	✗
Inverse	62.45	6.92	11.51	1.16	3.77	374.66	3.53	1	17280	172800	2	2	1	✓	✗	✗
Pooh	11.46	0.89	9253.34	132.01	1170.09	10.64	10.64	1	50400	259200	2	19	0	✓	?	?
Pooltogether	10.04	2.15	7546.34	43.09	337.43	250.26	19.29	1	28800	172810	6	3	0	✗	✗	✗
Radicle	44.67	4.80	121.33	11.84	26.38	472.64	0.02	1	17280	172800	2	9	0	✗	✗	✗
Silo	25.84	2.09	4017.87	4.20	18.35	206.07	0.17	128	21000	172800	3	3	0	✓	✗	✓
Strike	69.15	2.00	33.42	9.29	13.58	0.00	0.00	1	17280	172800	1	2	2	✓	✗	✗
Sudoswap	22.68	2.81	396.75	21.32	97.81	266.80	0.00	14400	21600		7	2	0	✗	✗	✓
Uniswap	26.55	5.12	713.04	3.53	14.55	183.14	0.05	13140	40320	172800	16	9	0	✗	✗	✗
Unslashed	27.71	0.52	3461.34	119.10	623.18	0.00	0.00	1	17280	172800	2	2	1	✓	✗	✗

Table 2: An empirical analysis of the susceptibility of a set of 24 DAOs on Ethereum to the risk factors presented in Section 5. The data is as of the last block of 31 January 2024 (19,129,888) with the exception of four DAOs where the data is taken at the following block (1) Gitcoin (17,969,570), (2) Indexed (18,664,452), (3) Inverse (13,424,209), and (4) Pooltogether (17,984,027). Any mention of the average votes refers to an average of the last five votes that were not canceled for each DAO. Additionally, the available liquidity refers to the available liquidity of the respective governance token on Uniswap and Aave.

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 two DAOs (Ampleforth and Indexed[1]) the value of the treasury without the governance tokens exceeds the value of all delegated tokens – making them an attractive target for attacks. This is underlined by the fact that an attack on Indexed DAO was attempted twice (see Section 3.2). 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 and more DAOs are close to reaching this threshold (e.g., Gitcoin). Note that we are not aware of any precedence for such an attack, but protocols have forked before [74]. In addition, to the empirical snapshot as of 31 January 2024, we present in Table 2, we also visualize the historical value of the treasury for a smaller subset of DAOs in comparison to the delegated token values for a small number of DAOs in Figure 1. We observe significant fluctuations over time in the relative value of the delegate tokens in comparison to the treasure for the three DAOs: ENS, Gitcoin, and Uniswap. While initially for all three 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. Additionally, 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. Thus, DAOs need to constantly monitor the value of the treasury to ensure that they are not an attractive target for token acquisition 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 a majority of DAOs use (see Table 2) is also not without issues though, as this doesn't 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 (there are around 7,000 blocks a day on Ethereum). Finally, adjusting the duration a proposal must remain

[1]The data for Indexed DAO is as of block 18,664,452 (before the attacks described in Section 3.2).



(a) ENS (b) Gitcoin (c) Uniswap

Figure 1: Comparison of treasury values and the total value of all delegated governance tokens. The values of the treasuries were obtained through the Moralis API (https://moralis.io/).

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.

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, inactive whale). 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. Additionally, the governance token liquidity of the analyzed DAOs is often also low. 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 ten DAOs there is at least one EOA that could perform such a 51% attack. Additionally, we also analyze how this figure evolves over time for a subset of six DAOs in Figure 2. We observe that for these six 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

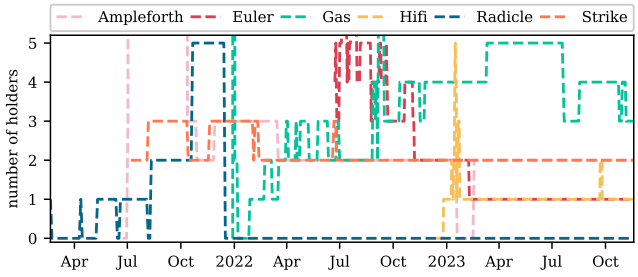


Figure 2: Number of holders, i.e. EAOs, who hold more tokens than delegated governance votes.

to a situation where only decisions that aren't canceled by the guardian can be 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 in Appendix A). 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) [44, 51]. 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 [49].

Lack of Reliable Communication Channels (RF7). DAO community members mainly communicate through X (formerly Twitter), Telegram, and Discord. These media 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 24 DAOs and their susceptibility to these risk factors also revealed that smaller DAOs tend to be more at risk. For these DAOs, in 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.

Escape Hatches 🚀. One can add escape hatches to DAOs to limit the severity of an attack. The *Decentralized Escape Hatch* proposed by Eyal and Sirer [30] 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 crowd-sourcing the reversal for example through a majority involvement.

Veto Power ❓. A slightly different approach would be for a DAO to utilize veto power. Instead of buffering transactions as with escape hatches, 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).

Emergency Shutdown 🚀. Implementing an emergency shutdown is a very invasive mitigation strategy. Here a set of holders can halt all transactions. In the case of MakerDAO [90], the emergency shutdown allows token holders to receive a share of the treasury, mitigating potential attacks that were underway.

User Authentication ❓. 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 acquisition 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 [43]. The Optimism Governance recently implemented a form of user authentication. In particular, they implement a bi-cameral governance design, with a token house [98] (one token one vote) and a citizen house [97] (one person one vote), only those with citizenship can vote in the citizen house.

Governance Forks 🚀 ❓. The design of some governance systems allows for a fraction of token holders to create a fork of a 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 [63]. The forked DAO then allowed each token holder to *rage-quit* and retrieve their individual share of the treasury.

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 simple or viable option.

Governance Tools ❓. The development of novel governance tools reduces the hurdles of participation in governance and can help prevent CHI attacks. For instance, through better communication and notifications on current proposals, voter apathy can be combated.

Additionally, it is important that these tools are open-source (i.e., such that bugs as in the Tally [25] case are less likely to happen) and that they cannot easily be spammed or taken down for instance. While these tools can to a great part in reducing the load in governance participation, they can become potential attack victims themselves (see Section 3.3).

Conservative Implementation 🚀 ❓. 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 to a token holder at any given time [50] 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 [75, 76].

Limiting the Governance Scope 🚀. Another approach to lessening the impact of attacks is for a DAO to add restrictions on its action space 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.

Bug Bounties 🚀 ❓. A widespread and important tool to prevent technical attacks (i.e., CP attacks) is bug bounties. Their extent has been researched in a broader context of cyber security and was shown to be a cost-effective instrument [106]. Bug bounties are widespread in the blockchain ecosystem and advertised by several DAOs.

Audits ❓. 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 [19], 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 [55, 92] including by Ethereum's founder Vitalik Buterin [46, 47]. 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. [70]. More recently, Augsten et al. [37] have discussed the potential of hidden vote buying in DAO governance facilitated by smart contracts, i.e., what is referred to as *DarkDAOs*. 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 [86]. Note that the term is an homage to the widely-studied concept of *Miner/Maximal Extractable Value (MEV)* [54].

Two recent systematizations of knowledge (SoKs) cover topics related to DAO attacks: Zhou et al. [108] 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 [80]. 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. [66]. 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 [68, 69]. This encompasses a flurry of empirical studies on a variety of DAOs covering aspects such as token distributions, voting turnout and voting behavior [38, 39, 58, 62, 67, 81, 93, 100, 102]. In particular, many of the studies, see e.g. Feichtinger et al. [62], 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. [88].

Finally, Tan et al. [103] 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 23 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 facing DAOs. Additionally, we identified and empirically measured risk factors across a set of 24 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 systemization 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] Beanstalk exploit — a simplified post-mortem analysis. https://medium.com/coinmonks/beanstalk-exploit-a-simplified-post-mortem-analysis-92e6cdb17ace.

[2] KP3R Vulnerability Report. https://statemind.io/blog/kp3r-vulnerability-report, 2019.

[3] Technical Description of Critical Vulnerability in MakerDAO Governance. https://blog.openzeppelin.com/makerdao-critical-vulnerability, 2019.

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

[5] Security Assessment GameDAO. https://skynet.certik.com/projects/gamedao, 2021.

[6] Twitter curve b. https://twitter.com/boredGenius/status/1458732732540854276, 2021.

[7] Twitter True Seigniorage Dollar. https://twitter.com/TrueSeigniorage/status/1370956726489415683, 2021.

[8] Beanstalk Exploit — A Simplified Post-Mortem Analysis. https://medium.com/coinmonks/beanstalk-exploit-a-simplified-post-mortem-analysis-92e6cdb17ace, 2022.

[9] 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.

[10] Etherscan build finance. https://etherscan.io/tx/0xf7709b0587d89b9d9b04ca04ce54fdc02a5a30435daf1fb4ba1174486e365c9f, 2022.

[11] Temple dao hack analysis. https://blog.solidityscan.com/temple-dao-hack-analysis-c96db856322c, 2022.

[12] Twitter build finance. https://twitter.com/finance_build/status/1493223190071554049, 2022.

[13] Twitter mango markets. https://twitter.com/avi_eisen/status/1581326197241180160?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1581326197241180160%7Ctwgr%5Ef3657d550fe7845c01ad9cd6592e4764b0a9bbc6%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fblockworks.co%2Fnews%2Favi-eisenberg-committed-fraud, 2022.

[14] Twitter temple dao. https://twitter.com/BlockSecTeam/status/1579843881893769222, 2022.

[15] Agora Audit Report. https://github.com/voteagora/optimism-gov/blob/main/audits/23-05-12_zachobront.md, 2023.

[16] Community alert! this is scam dao proposal. https://twitter.com/BIGCAPProject/status/1697958233204490494, 2023.

[17] Deepdao organizations. https://deepdao.io/organizations, 2023.

[18] Dexes tvl rankings. https://defillama.com/protocols/dexes/Ethereum, 2023.

[19] Ethereum smart contract best practices. https://consensys.github.io/smart-contract-best-practices/development-recommendations/, 2023.

[20] Etherscan bigcap. https://etherscan.io/tx/0x7ce953acd59947f8a63f053f4ce3405e53afd4d9d7ef487e755cb4ebd82dba3a, 2023.

[21] Explained: The Tornado Cash Hack. https://www.halborn.com/blog/post/explained-the-tornado-cash-hack-may-2023, 2023.

[22] 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.

[23] Lending tvl rankings. https://defillama.com/protocols/Lending, 2023.

[24] Paladin documentation. https://doc.paladin.vote/, 2023.

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

[26] 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.

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

[28] Twitter synthetify. https://twitter.com/Neodyme/status/1715149044794655145?s=20, 2023.

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

[30] 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.

[31] Pranav Garimidi and Scott Duke Kominers and Tim Roughgarden. DAO governance attacks, and how to avoid them. https://a16zcrypto.com/posts/article/dao-governance-attacks-and-how-to-avoid-them/, 2023.

[32] Adam Levi. The arc platforms. https://medium.com/daostack/the-arc-platform-2353229a32fc, 2018.

[33] 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.

[34] 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.

[35] Anonymized for double-blind review. Subgraphs. https://anonymous.4open.science/r/sok-attacks-on-daos-140E/README.md, 2023.

[36] 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.

[37] James Austgen, Andrés Fábrega, Sarah Allen, Kushal Babel, Mahimna Kelkar, and Ari Juels. Dao decentralization: Voting-bloc entropy, bribery, and dark daos, 2023.

[38] 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.

[39] 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.

[40] 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.

[41] Rob Behnke. Explained: The tornado cash hack, May 2023.

[42] Jan Behrens. The origins of liquid democracy. *The Liquid Democracy Journal on electronic participation, collective moderation, and voting systems*, 5, 5 2017.

[43] 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.

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

[45] James M. Buchanan. Simple majority voting, game theory, and resource use. *Canadian Journal of Economics and Political Science*, 27(3):337–348, 1961.

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

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

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

[49] Certik. Securing The Web3 World. https://www.certik.com/, 2023.

[50] Consensys. A Consensys Diligence Audit Report: Aave Governance Dao . https://consensys.io/diligence/audits/2020/08/aave-governance-dao/, 2020.

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

[52] 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.

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

[54] 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.

[55] 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.

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

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

[58] 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, page 25–31, New York, NY, USA, 2023. Association for Computing Machinery.

[59] 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.

[60] Etherscan. Ethereum API Provider. https://etherscan.io/apis, 2023.

[61] Corin Faife. How to stole an election: BeanStalk DAO $80million FlashLoan attack study case.

[62] 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.

[63] 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, Sep 2023.

[64] Bryan Alexander Ford. Delegative democracy. Technical report, 2002.

[65] William Foxley. 'flash loans' have made their way to manipulating protocol elections. https://www.coindesk.com/tech/2020/10/29/flash-loans-have-made-their-way-to-manipulating-protocol-elections/?_gl=1*1bq6j4n*_up*MQ..*_ga*MTk5MTAxMjc4Ny4xNzA2MDg3NTk4*_ga_VM3STRYVN8*MTcwNjA4NzU5OC4xLjAuMTcwNjA4NzU5OC4wLjAuMA, 2020.

[66] 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.

[67] Robin Fritsch, Marino Müller, and Roger Wattenhofer. Analyzing voting power in decentralized governance: Who controls daos?, 2022.

[68] David Gogel, Bianca Kremer, Aiden Slavin, and Kevin Werbach. Decentralized autonomous organizations: Beyond the hype, 6 2022.

[69] David Gogel, Bianca Kremer, Aiden Slavin, and Kevin Werbach. Decentralized autonomous organization toolkit, 1 2023.

[70] 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.

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

[72] 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.

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

[74] 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.

[75] 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.

[76] 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.

[77] 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.

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

[79] James S. Jordan. *Majority rule with dollar voting*, pages 211–220. Springer Berlin Heidelberg, Berlin, Heidelberg, 2003.

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

[81] 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.

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

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

[84] Luh Luh Lan and Loizos Leracleous. Shareholder votes for sale, Jul 2005.

[85] 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.

[86] Leland Lee and Ariah Klages-Mundt. Governance extractable value. https://ournetwork.substack.com/p/our-network-deep-dive-2, 4 2021.

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

[88] 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.

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

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

[91] 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.

[92] 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.

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

[94] Moralis Web3. Enterprise-Grade Web3 APIs. https://moralis.io, 2023.

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

[96] Stephen H. Newman. Decentralization Cheapens Corruptive Majority Attacks. In Joseph Bonneau and S. Matthew Weinberg, editors, *5th Conference on Advances in Financial Technologies (AFT 2023)*, volume 282 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 13:1–13:19, Dagstuhl, Germany, 2023. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

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

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

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

[100] 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.

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

[102] Xiaotong Sun, Charalampos Stasinakis, and Georgios Sermpinis. Decentralization illusion in decentralized finance: Evidence from tokenized voting in makerdao polls, 2023.

[103] 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.

[104] The Graph. Access the world's blockchain data. https://thegraph.com/explorer, 2023.

[105] 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.

[106] 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.

[107] Ryan Youngjoon Yi. Digixdao: A divorce story – a case study for voting systems and cryptonative arbitrage. https://blog.coinfund.io/digixdao-divorce-story-6ed74b00e2bd, 2 2020.

[108] 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.

A Analyzed Incidents, Attacks & Audits

In the following, we provide a brief description of each of the attacks and incidents analyzed in Table 1. Note that we present the incidents and attacks in alphabetical order. Additionally, for those already discussed in case studies, we refer to the section where the case study can be found.

Agora Audit (May 2023) [15] The audit by an independent security researcher brought to light that certain proposals could be passed irrespective of whether votes in favor of the proposal were more numerous than votes against it. Instead, the contract only checked that a given quorum of yes votes was reached (As is customary in DAOs, the required quorum was set much lower than 50% of voting power).

Beanstalk (Apr 2022) See Section 3.2.

BigCap DAO (Sep 2023) [16] A malicious proposal on the BigCap DAO, which was ultimately rejected, tried to steal the treasury. The proposal copied a previous proposal and the attacker had previously acquired the BIGCAP tokens, i.e., the DAO's governance tokens, through a decentralized exchange [20].

Binance (Oct 2022) [91] UNI tokens (Uniswap governance token) deposited with Binance were delegated even though the cryptocurrency exchange says that it does not vote with its users' tokens. Binance later commented on the incident and said that it was an accident.

Build Finance (Feb 2022) [12, 52, 56, 85] A first attempt at a takeover of the DAO was made on 9 February 2022 with a proposal that would allow the attacker to mint the DAO's governance token – BUILD. This attempt was picked up in the DAO's Discord channel, where voters were urged to vote against the proposal and subsequently failed. On the next day, the attacker tried their luck again, transferred the tokens to a different wallet, and created a second proposal. This proposal went undiscovered, passed in favor of the attacker, and gave the attacker control of the DAO. The attacker went on to mint BUILD tokens and emptied the liquidity pools that held BUILD on various decentralized exchanges [10]. The attacker received the equivalent of $470,000. Note that some of the BUILD tokens were bought on decentralized exchanges.

Constitution DAO (Jan 2022) [72] An audit found that the project owners (that control a multisig), can replace the management contract, allowing them to move funds, and change the project logic arbitrarily.

Compound (Feb 2022) [105] An address proposed to add TUSD as a collateral asset on Compound, the address had previously received COMP (Compound's governance token) tokens worth $9M from Binance. As Justin Sun had previously borrowed COMP tokens and sent them to Binance, it is alleged that he is behind this governance attack which ultimately failed.

Curve A (ongoing) [78] The Curve Wars is an ongoing competition between various DeFi projects to attract rewards to their respective liquidity pools. Protocols bribe veCRV, i.e., Curve's governance token, token holders to vote to distribute rewards towards their pools on Curve.

Curve B (Nov 2021) [6, 40] Mochi Inu set up a pool on Curve pool that attracted significant liquidity, they were able to push up the rewards of the Mochi Inu pool and gain an outsized influence in the Curve governance. Even though such practices are constantly ongoing on Curve (see Curve A), this particular attack was stopped by Curve's Emergency DAO, which cut off the pool's rewards.

DAO Maker (Mar 2021) [71] An audit found that contract owners have elevated privilege access to certain functionality, allowing them for example to drain user funds.

Force DAO (Apr 2021) [73] The decentralized Hedge fund was built on smart contracts that were written using code from two different sources. Due to their mismatch in error handling, by performing transfers that failed, attackers were able to obtain tokens that granted them access to shares of the vault for free.

GameDAO (Aug 2021) [5] An audit by Certik uncovers that an address has privileged ownership over many contract functionalities, giving it control over the minting and burning of NFTs to and from any account.

Genesis Alpha DAO (Feb 2019) [87] The Genesis Alpha DAO was an experimental project led by the DAOstack initiative (shutdown in late 2022), that proposed a suite of governance solutions. The Genesis Alpha contract was a DAO built on top of the Arc platform. Arc was capable of supporting multiple DAOs through the same voting contracts, which DAOstack argued made created DAOs more secure, as all the individual pieces of the platform could be audited

separately [32]. On 5 February 2019 however, attackers showed that the lack of separation of code was exploitable, as they were able to drain the Genensis Alpha treasury, through another DAO. More precisely, due to a bug in the code, the attackers were able to assign themselves voting rights for the Genesis Alpha DAO. In the same atomic transaction, the attacker then created, voted for, and passed a proposal that transferred the contents of the Genesis Alpha DAO treasury (around $15,000 in ETH and GEN tokens) to himself. The Arc Platform had previously been audited. Speculation arose that the attack might have happened since a bounty for a newer DAO contract had recently been put up. DAOstack wrote that this showed that *community bug bounties* work [87].

Indexed Finance (Nov 2023) [22] See Section 3.2.

Kleros (Jan 2024) [82] Kleros is a decentralized arbitration protocol whose DAO was attacked in January 2024. In this DAO, voting happens off-chain, and only proposals that are to be implemented are submitted on-chain. The attacker deployed a custom smart contract to submit the proposal list to the Governor smart contract. Most likely, a custom smart contract was used to evade the notification systems. The attacker's proposal would have transferred 46 ETH out of the DAO if it had been successful. However, the attack was discovered and stopped by issuing a counter-proposal, which was selected instead of the malicious proposal by Kleros' Court system.

KP3R Network (Sep 2022) [2] An audit discovered that the contracts permitted users to re-vote on a proposal but failed to properly subtract the user's previous vote. The vulnerability went unnoticed for two years.

MakerDAO A (Feb 2020) [70] A prevented attack on the MakerDAO stablecoin protocol was disclosed to MakerDAO by the researchers who discovered it. If successful, the attack would have potentially allowed an attacker to steal $0.5b worth of MKR and DAI collateral, as well as minting an unlimited supply of DAI tokens. The attacker simply needed to obtain a sufficient amount of MKR tokens to win a vote (see *Token Purchase*, *Token Loan*, *Flash Loan* in Section 3.2). In particular, using flashloaned tokens to vote was possible at the time.

MakerDAO B (Oct 2020) [65] In an effort pass and speed up the passing of a proposal, BProtocol first took out a flashloan on dYdX of ETH which they deposited on Aave to borrow MKR tokens, i.e., MakerDAO's governance token. These MKR tokens were then used to vote in favor of the proposal and schedule the execution of the proposal. In the aftermath, additional safeguards were implemented by the DAO [89].

MakerDAO C (Jan 2022) [34] Justin Sun allegedly borrowed large amounts of MKR, the governance token for the MakerDAO, to vote in a poll to create a TUSD-DAI peg stability module. He, however, returned the tokens after his actions were noticed and did not end up waiting.

MakerDAO D (May 2019) [3] An audit discovered that the contract logic permitted an attacker to remove votes of other users from proposals, as well as indefinitely lock other users' tokens on any given proposal.

Mango Markets (Oct 2022) See Section 3.4.

Nexus Mutal (Feb 2020) [57] The Nexus Mutal team was informed that the DAO's advisory board could whitelist a proposal but that a different proposal would be executed in practice. In more detail, a proposal to upgrade the protocol would be whitelisted and then replaced with a malicious proposal that would execute.

Paladin Lending (ongoing) See Section 3.1.

Steemit (Feb 2020) [4, 31] Steemit is a protocol whose on-chain governance is controlled by 20 witnesses selected by the STEEM token holders, i.e., the protocol's native and governance token. Justin Sun acquired 30% of the STEEM token supply, which was noticed by the protocol's witnesses. The witnesses went on to freeze the tokens bought by Justin Sun. A back and forth between Justin Sun and the protocol followed, in a quest to install their preferred 20 witnesses to control the protocol. Eventually, Justin Sun came out victorious and gained control of the protocol.

Synthetify (Oct 2023) See Section 3.3.

The DAO (Jun 2016) See Section 3.4.

Tally (Apr 2021) See Section 3.3.

Temple DAO (Oct 2022) [9, 11, 14] An attacker took advantage of insufficient access control to the migrateStake function in the Temple DAO smart contract. In more detail, anyone was able to call the migrateStake functions and there was no validation on the oldStaking parameter. This allowed the attacker to insert a malicious contract as the oldStaking

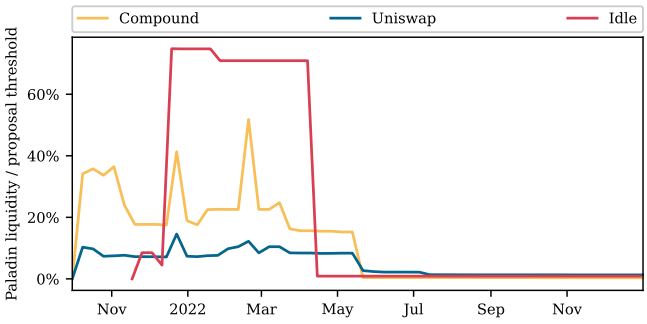


Figure 3: Amount of liquidity available on Paladin in relation to the proposal threshold of the respective protocol.

parameter and insert an arbitrary amount, which was then withdrawn from the DAO and received by the attacker. The attacker drained around $2.4M from the DAO.

Tornado Cash (May 2023) See Section 3.3.

True Seigniorage Dollar (Mar 2021) [7, 48] The attacker first acquired a large amount of TSD tokens, i.e., the protocol's governance tokens. With these tokens, the attacker went on to propose and vote on a proposal that would replace the token contract with malicious code. The attacker then minted TSD tokens and swapped these for BUSD (a stablecoin pegged to the $) on decentralized exchanges.

Wonderland DAO (Jan 2022) [33] Wonderland DAO discovered that Michael Patryn was their treasury manager. He had hidden his identity behind the pseudonym 0xSifu. Possibly he hid his identity as he is the co-founder of the failed cryptocurrency exchange QuadrigaCX and a convicted criminal.

B Data Collection

Our empirical measurements are based on data collected using The Graph [104]. For each DAO we index its governance data including token transfers, votes, proposals, and delegations by creating a tailored subgraph. The established graph database can then be queried using GraphQL. The code used to generate the subgraphs is provided and will be made open source [35]. Furthermore, we measure liquidity available on Uniswap and Aave, the biggest DEX and lending protocol respectively. Finally, to obtain the treasury value, we queried each DAO's timelock contract through the Etherscan API [60]. The timelock value is then obtained through the Moralis API [94].

C Paladin Lending

Figure 3 shows the liquidity available on Paladin compared to the proposal threshold for Compound, Uniswap, and Idle over time. Currently, there is nearly no liquidity available on Paladin.