Strengthening DAO Governance: Vulnerabilities and Solutions

Lori Qian

Received February 12, 2025
Accepted September 11, 2025
Electronic access September 30, 2025

Decentralized Autonomous Organizations (DAOs) are blockchain technologies that collectively manage billions of dollars without a centralized organization. While they promise transparency and democratic governance, recent exploits have revealed security vulnerabilities that undermine trust and legitimacy. This study investigates the systemic flaws of DAO governance systems and proposes countermeasures. It focuses on three major DAOs: Uniswap, GnosisDAO, and ArbitrumDAO, chosen for their treasury size and accessible governance data. Additionally, to contextualize the governance risks, we examine real world exploits involving Cream Finance, Tornado Cash, Build Finance, and Beanstalk which suffered a combined loss surpassing $300 million due to weak governance, allowing voting manipulation and malicious proposals. Using a comparative case study with the three major DAOs supported by official website records and academic sources, three core governance vulnerabilities were identified: flash loan exploitation, off-chain voting manipulation, and token-based coercion. This paper proposes solutions aimed at reinforcing security while maintaining decentralization: (1) implementing fully off-chain voting to enhance transparency, (2) using cryptographic techniques such as zero-knowledge proofs to ensure vote privacy and coercion resistance, and (3) integrating decentralized identity tools like Proof of Humanity and Soulbound Tokens to support fair voting. Each solution is evaluated for feasibility, technical readiness, and scalability. This research provides a structured framework for analyzing and mitigating governance vulnerabilities in DAOs, helping developers and users protect security, privacy, decentralization, and billions of dollars in web3 governance.
Keywords: DAO governance, decentralized finance (DeFi), flash loan attacks, on-chain voting, token-based voting, blockchain

Introduction

Decentralized Autonomous Organizations (DAOs) are online organizations built on Distributed Ledger Technologies (DLT), that enable a collective to pursue a common goal and decide upon proposals and projects. Holding billions in their treasuries, these financial systems are managed not by banks or governmentbut by groups of individuals. These entities offer a revolutionary approach to governance and financial control. By operating on blockchain technology, DAOs allow members to vote on proposals and manage treasuries without a central authority, using smart contracts to enforce decisions transparently and autonomously.[1]

Uniswap, GnosisDAO, and Arbitrum are three major DAOs that control treasuries worth billions of dollars[2]. Decisions regarding these treasuries are made through member voting and governance tokens. These votes determine everything from software updates to funding allocations. However, the promise of secure decentralization is frequently damaged by weak governance systems, exposing DAOs to manipulation and outright theft.

Recent examples of DAO governance failures demonstrate what is at stake. Table 1 summarizes a series of exploits that drained millions of dollars from DAO treasuries.

The implications of these exploits extend beyond financial losses they destroy trust among DAO participants and undermine the credibility of decentralized systems. Governance vulnerabilities are existential threats. A DAOs ability to operate fairly and securely depends on strong voting structures and resistance to manipulation. Without satisfying these requirements, decentralization is simply an empty promise[7]. This paper investigates three central research questions using case studies of Uniswap, GnosisDAO, and ArbitrumDAO:

1 Identify significant governance vulnerabilities that affect the major DAOs.

2 Identify technical and structural flaws responsible for governance vulnerabilities

3 Identify mitigation strategies that preserve decentralization while addressing vulnerabilities and assess their feasibility.

By recognizing root causes and proposing strategies, this study aims to strengthen DAO governance systems, creating a future where decentralized autonomous organizations can thrive without fear of exploitation.

Related Work

The study of secure voting and decentralized governance systems has produced a variety of literature relevant to DAO governance vulnerabilities. Work by Bernhard et al. (2017) outlined

Table 1 Selected DAO governance exploits, showing amounts lost, causes, and dates.

DAO	Amount Lost	Cause of Exploit	Date
Cream Finance	$130 million	Manipulated price calculation and exploited vulnerabilities in the system managing loan funds [3]	27-Oct-21
Tornado Cash	Unspecified	Control of governance through malicious voting proposals that enabled the attacker to siphon funds. [4]	May-23
Build Finance DAO	$470,000	An attacker exploited a flaw in DAOs voting mechanism to assume control of the treasury. [5]	Feb-22
Beanstalk DAO	$182 million	Flash loan attack manipulated governance to approve draining of treasury funds. [6]	17-Apr-22

requirements for secure voting systems, including trust, verifiability, privacy, and coercion resistance [8]. Although their focus was on traditional pollsite and online voting, these criteria translate into challenges DAOs face, particularly regarding privacy and voter influence.

One way to enhance the privacy and security of voting systems is to protect voter anonymity. DAOs aim to provide anonymity in their voting systems, but they operate on blockchain technology, which inherently limits the extent of true anonymity. With wallet addresses publicly exposed on-chain, voters are at risk of coercion or influence, particularly in high-stakes proposals. However, DAOs can achieve pseudonymity, where a users interactions are connected with a pseudonym: a cryptographic wallet address identity rather than their real-world identity [9]. Below are reasons why full anonymity is impossible for DAOs:

1. Blockchain Transparency: Blockchain networks keep an immutable, transparent ledger where all transactions are recorded. While identities are not directly stored, wallet addresses and their activities can be studied. Wallet interactions can be traced and analyzed, revealing behavioral patterns or linking them to off-chain identities, like IP addresses. Repeated interactions between wallets can unintentionally reveal relationships, making it possible to associate specific wallets with individuals. Additionally, companies and researchers frequently use machine learning and clustering techniques to identify and map wallets to real-world identities based on transaction patterns and metadata.

2. Legal and Regulatory Constraints: The case of Tornado Cash demonstrates how legal and regulatory challenges prevent full anonymity in blockchain systems [10](. Tornado Cash faced sanctions from U.S. authorities for allegedly facilitating illegal activities such as money laundering, including transactions linked to cybercrime groups like the North Korean Lazarus Group, which reportedly used the platform to hide stolen cryptocurrency. These activities were possible because the platforms design prioritized full anonymity, preventing identity verification and allowing malicious attackers to exploit it.

   Anti-money laundering (AML) and know-your-customer (KYC) regulations require identity verification for many blockchain users, especially when interacting with centralized exchanges or services [11]. This legal requirement undermines efforts to maintain anonymity. Because of the criminal implications, these legal pressures discourage the usage of systems that prioritize absolute anonymity, leaving DAOs to settle for pseudonymity.

3. Balancing Privacy and Accountability Governance Transparency: DAOs often prioritize transparency for voting outcomes and processes in governance to build trust and encourage participation, which can conflict with efforts to protect voter identities.

In the end, pseudonymity is the compromise. By associating actions with wallet addresses rather than real identities, DAOs achieve a balance between privacy and accountability.

Another way to strengthen privacy and authenticity are advanced cryptographic methods such as homomorphic encryption and zero-knowledge proofs, as introduced by Ologunde (2023) [12]. The study also mentions auditing methods and legal regulations that address electronic voting vulnerabilities. These tools, in theory, could make DAO voting more secure. However, the complexity and inefficiency of these protocols make them difficult to adopt in fast-moving and community-governed systems, and their acceptance among DAO participants remains uncertain.

While DAOs inherit many vulnerabilities from traditional e-voting, they also face challenges unique to blockchain systems. Lee (2019) examines 78 cyberattacks across blockchain systems, categorizing common methods of exploitation [13]. Building on this, Feichtinger et al. (2024), shift the focus specifically to DAOs by compiling real-world incidents. They identify attack

methods like bribery and token control that threaten governance integrity, providing a broad overview of how DAOs have been exploited [14].

To further investigate the bribery attack vector, Austgen et al. (2023) mathematically demonstrate that bribing many small token holders is more feasible than targeting a few large holders [8]. They introduce the concept of Voting-Bloc Entropy (VBE) to measure decentralization and explain how low VBE makes DAOs more vulnerable to bribery and vote manipulation. This finding highlights the fragility of token-based voting systems, where economic incentives can be easily exploited. Another reason token-based voting struggles lies in its broader economic issues. Tan et al. (2023) identify challenges such as unclear benchmarks, a lack of standardized datasets for analyzing vulnerabilities, and tokenomics problems like centralization, speculative behavior, and inefficiencies in governance [15]. Together, these studies show that token-based voting is vulnerable both from bribery manipulation and deeper structural economic flaws. For these reasons, DAOs must look toward alternative governance models and stronger anti-coercion measures to preserve integrity.

While prior research has laid important groundwork by outlining the requirements of secure voting, documenting DAO exploits, and analyzing weaknesses in token-based systems, it often stops short of offering fixes for DAOs. Much of the literature emphasizes vulnerabilities, such as privacy, centralization, and bribery, without suggesting governance improvements to implement. This paper addresses that gap by analyzing both traditional e-voting research and blockchain case studies to identify actionable solutions in DAO governance. It proposes stronger anti-coercion practices, improved privacy protections, and alternative governance models in order to move decentralized finance communities closer to secure, trustworthy decision-making.

Methodology

This study analyzed vulnerabilities in the governance systems of three major DAOs: Uniswap, GnosisDAO, and Arbitrum. These DAOs were selected based on their large treasury sizes, $7.3 billion, $2.9 billion, and $3.9 billion, respectively at time of writing, which makes them high-value targets for potential attacks [2]. A comparative case study method was used to examine each DAOs governance structure, using both qualitative and quantitative data.

Official governance documentation of DAOs provided information on voting processes, quorum thresholds, voting platforms, proposal creation procedures, etc. Community discussion forums were analyzed to gather insights into participant concerns and informal practices. Smart contract code and technical records from Github were examined to uncover potential vulnerabilities or design limitations. Market tracking platforms were used to determine token price, while tools like DeepDAO provided information on voter participation rates and treasury allocations.

Collected data was then organized by DAO and systematically categorized to highlight issues in governance structures. It was organized into categories such as voting design, participation, centralization risks, and attack vectors. Key patterns across cases showed where vulnerabilities overlapped and where they differed. These findings were then synthesized to identify the most significant issues that impact the integrity, security, and decentralization of DAO governance. Finally, these results were used to propose potential solutions that address the identified vulnerabilities. When developing solutions, existing methods were researched and compared against alternative ideas. Tradeoffs were considered, but the proposed approaches were shown to better address the identified vulnerabilities.

However, this study relies on publicly available documentation, which may be incomplete or outdated, and does not account for private DAO communications, so these limitations should be taken into consideration.

Results

Uniswap Governance

Uniswaps governance protocol operates in three main phases [16];

1 Request for Comment (RFC): Community members propose and discuss ideas on the governance forum. This phase is informal and focuses on gathering feedback and refining the proposal.

2 Temperature Check (Phase 2): An off-chain Snapshot poll determines whether the community supports moving the proposal forward. It requires at least 10 million UNI votes to pass.

3 Governance Proposal (Phase 3): The final proposal is submitted for on-chain voting. To pass, it must meet a quorum of 40 million* UNI votes and receive majority approval. Additionally, proposers need at least 1M* UNI tokens delegated to their address to initiate on-chain voting.

*Note on Discrepancies in Uniswaps Documentation Uniswaps governance documentation contains inconsistencies that undermine the reliability and trustworthiness of the DAO. For instance, the Governance Process page on the official documentation specifically states a delegated token threshold of 1 million UNI and a quorum requirement of 40M UNI for Phase 3 voting. However, the Governance Reference page contradicts this by listing the delegated threshold as 2.5M UNI and the quorum as 4M UNI [17]. Reviewing other pages on websites about Uniswap governance, most reported 40 million and 1 million UNI as the threshold, so these figures were used.

Such discrepancies are highly problematic for several reasons. Undoubtedly, inaccurate or conflicting information creates uncertainty and confusion among users about the rules governing the DAO. Members are not able to fully understand or confidently participate in the governance process when the requirements are unclear. Errors like these reflect poorly on the DAOs ability to self-manage, undermining trust. While no known incidents or exploits have arisen from these discrepancies so far, the existence of contradictory documentation poses a significant risk that could lead to manipulation in the future. Uniswap must address these discrepancies urgently. Establishing clear, unified documentation that is regularly updated and well-maintained is critical to boosting user confidence in the DAO system.

To successfully advance a malicious proposal through the Uniswap DAOs governance process, a malicious actor would need to overcome specific token and voting thresholds during the last two phases of governance. They would first need to control at least 1 million UNI tokens delegated to their address in order to initiate the on-chain proposal. At the current market price of approximately $10 USD per UNI token[18], this would require $10 million if the actor does not already hold sufficient delegated tokens. In Phase 2, the Temperature Check, the proposal must then receive a minimum of 10 million UNI yes votes and a majority in favor to proceed, which would cost about $100 million. Finally, in Phase 3, the Governance Proposal, the quorum rises to 40 million UNI yes votes and majority during the on-chain vote, requiring an additional $400 million in tokens. Altogether, the cumulative cost to execute such a malicious proposal would amount to a minimum of 0$510 million.

The cost barriers are high and engaged Uniswap voters are likely to recognize and vote against a malicious proposal during both the Temperature Check and Governance Proposal phases; therefore, it would be difficult to acquire a majority. To circumvent this, an attacker could apply for a flash loan and obtain 10 or 40 million UNI tokens, or more if necessary, then strategically submit the required yes votes at the last possible moment before the voting period ends, leaving the Uniswap community with insufficient time to counteract the move. This strategy highlights a vulnerability in Uniswaps voting system: the absence of protections against instantaneous, large-scale token transactions. While this financial requirement of at least $510 million is significant, it represents a fraction of Uniswaps $7.3 billion treasury, potentially incentivizing malicious actors. A successful attack could result in the misallocation of treasury funds, directly harming the users who have invested in the DAO and rely on the protocols stability.

Since flash loans involve borrowing large amounts of money, some doubt the feasibility of such an attack because there might not be enough tokens available, and it could cause major price changes in the market. However, flash loan attacks are very much real and have been carried out many times. Between February 2020 and May 2024, about 100 flash loan attacks have taken place on various blockchain systems. These exploits range in scale from mere thousands to as much as $196 million, with an average loss of about $6.2 million. Attackers often use techniques like oracle manipulation, liquidity pool draining, and reentrancy attacks, proving that flash loans are a practical and dangerous tool for manipulating blockchain systems[19].

As part of its governance, the system includes a waiting period of 2 days before the start of the 7-day Phase 3 voting and an additional 2-day timelock period after a proposal passes, which theoretically gives the community time to review and respond to malicious proposals[17]. However, the timelock contract is described as operating in a time-delayed, opt-out upgrade pattern, and does not explicitly state that it can be used to reject or veto a proposal that has successfully passed the governance process. Its primary purpose appears to be enforcing a delay to provide preparation time, rather than acting as a governance override.

If the timelock contract could indeed block or cancel a passed proposal, it would fundamentally contradict the decentralized principles of DAOs. Such action would undermine the community driven governance model and raise questions about whether central entities could intervene in the governance process.

While safeguards like the timelock and voting thresholds exist to slow down or expose malicious actions, these mechanisms alone do not guarantee protection against last moment exploits, such as flash loan attacks. Still, the absence of veto powers demonstrates Uniswap DAOs commitment to decentralization, even if it means potential vulnerabilities remain exploitable by attacks with incentive for financial gain.

GnosisDAO Governance

GnosisDAOs governance protocol also operates in three main phases[20]

1 Proposal Creation (Phase 1): Community members draft and post proposals on the Gnosis forum. This phase allows for open discussion, refinement, and feedback from the community. While optional, it is highly recommended as it provides a preliminary indicator of the proposals potential success.

2 Specification (Phase 2): Proposals come to this phase as formal Gnosis Improvement Proposals (GIPs), which are detailed documents including specifications, milestones, and funding requests. The community votes on these proposals in a forum poll, and although a positive majority is recommended, proposals can still advance to the next phase without full consensus.

3 Consensus (Phase 3): A Snapshot poll determines the final decision. This requires a minimum quorum of 4% of the circulating $GNO token supply of for-votes. The poll must achieve a majority in favor of the proposal for it to pass.

Advancing a malicious proposal through GnosisDAOs governance process at Phase 3 requires a quorum of 4% of the circulating GNO supplyequivalent to approximately 120,000 tokens costing $34 million at the current price of approximately $280 per token[18]. But, the difficulty lies in securing a majority of votes, which makes it hard to ascertain the exact amount of tokens required to pass a malicious proposal. However, the strategy of using a flash loan to acquire the necessary tokens and cast the needed votes at the last second could still exploit the system, leaving the community without enough time to react.

The most significant issue in GnosisDAOs governance structure is its reliance on off-chain Snapshot polls for the final voting phase[21]. Unlike on-chain votes, which are permanently recorded on the public ledger and are immutable, off-chain votes lack binding enforcement and depend on external entities to enact the results on-chain[22].This reliance introduces a potential issue: the agents responsible for reporting the voting outcome may simply refuse to do so or manipulate the result, since the result is not bound on-chain.

This problem is not hypothetical it mirrors the Bitcoin New York Agreement in 2017[23].The New York Agreement was an off-chain consensus attempt among Bitcoin stakeholders, including miners, exchangers, and developers, to implement a protocol upgrade known as Segregated Witness (SegWit2x). While the agreement initially appeared to gain broad support, it failed due to discrepancies between the off-chain agreements and the on-chain documentation, demonstrating off-chain polls are unreliable. Despite not being a DAO example, Bitcoin is similarly built on Distributed Ledger Technology, which makes it a reasonable comparison as both are based on the same architecture. This case illustrates that informal, unenforceable governance agreements can fall apart. DAO communities face a similar risk when relying on Snapshot. Without automated, immutable enforcement on the blockchain, outcomes depend on intermediaries that may or may not be trusted.

For a DAO designed to be transparent and on-chain, using off-chain voting systems like Snapshot contradicts its foundational principles. By depending on external entities to report results, GnosisDAOs governance risks becoming exploitable because key decisions rely on trusting an agent to correctly bring results on chain. The entire governance model loses legitimacy when outcomes are not automatically enforced on chain, leaving participants to rely on intermediaries and question whether results were truthfully implemented.

While the cost and requirements to advance a malicious proposal are substantial, the most pressing concern is that the reliance on off-chain snapshot polls undermines the integrity of GnosisDAOs governance process. Without binding, transparent, and immutable enforcement on-chain, the system is susceptible to manipulation. Over time, this could potentially lead to fewer users participating in governance and decreased community engagement.

ArbitrumDAO Governance

ArbitrumDAOs governance protocol for voting on Arbitrum Improvement Proposals (AIPs) consists of seven phases[24]:

1. Temperature Check (Optional but Recommended): AIP proposals are introduced in the forum for a 1-week discussion and Snapshot poll.

2. Formal Submission (3 Days): Proposals must be formally submitted through governance contracts on Tally, Arbitrum Ones user interface. Submissions must meet a minimum threshold of 1 million delegated tokens. This 3-day period is intended to give interested parties time to discuss the AIP and gather votes before the formal vote.

3. On-Chain Voting (14-16 days): Voting occurs directly on Arbitrum One. For an AIP to pass, it must meet two conditions:
   a. Simple Majority: More votes in favor than against.
   b. Participation Thresholds:
   i. Constitutional AIPs (software updates, changes to Arbitrum Constitution, etc.): At least 5% of votable tokens must vote in favor or abstain.
   ii. Non-Constitutional AIPs (funding requests): At least 3% of votable tokens must vote in favor or abstain. If the threshold is met within the last 2 days, the 14-day voting period is extended by 2 days.

4. L2 Waiting Period: allows users to withdraw funds or take other actions if they disagree with the decision.

5. L2-to-L1 Message Finalization*: confirms the proposals passage on L1. This ensures that the different chains are synchronized.

6. L1 Waiting Period*: An additional 3-day waiting period provides time for further L1 user actions before execution.

7. Implementation: AIP is executed on L1, a transaction from L1, or on another Governance Chain. *Note: Phases 5 and 6 are bypassed for Non-Constitutional AIPs.

The Arbitrum DAO governance process has specific token requirements for proposals. To submit an On-Chain Proposal via Tally, the proposer must be delegated at least 1 million $ARB tokens, equivalent to $750,000 at a price of approximately 0.75 per token[18]. For non-Constitutional AIPs for fund allocation to pass, 3% of the circulating supply of 4.2 billion $ARB tokens, or 126 million tokens, must participate by voting in favor or abstain. In total, this would cost about $95.25 million. The proposal needs to secure a simple majority, where the last second flash loan strategy can once again be employed. While a malicious proposal could potentially pass the first three phases, the Security Council[25] would likely catch and block such

attempts using their authority to intervene and safeguard the DAO against harmful proposals.

While it might be difficult to pass a malicious proposal, the main vulnerability lies with the Security Council, an entity tasked with making final decisions in the governance process. Members of the Security Council[26] are not anonymous; their Ethereum wallet addresses and affiliations are publicly available. This transparency, while useful for accountability, causes complications about privacy and coercion, as publicly identifiable members may be pressured or influenced by external entities. Additionally, several members of the Security Council are closely tied to Arbitrum's maintenance and development teams, such as Zellic and fred. This overlap compromises the councils impartiality, as members may inherently prioritize Arbitrums interests over neutral oversight, creating a conflict of interest. Another potential issue arises from Dennison Bertram, the CEO of Tally, the voting system used for Arbitrums on-chain proposals. His position on the Security Council presents a direct conflict of interest, as he oversees the very platform that governs Arbitrums decision-making processes. With centralized bodies, the key method to prevent issues is a proper system of checks and balances. However, in Arbitrums case, these checks are undermined by overlapping roles, creating a false sense of accountability. From the outside, decentralization may appear to be preserved through the presence of a Security Council, but in reality, the council is composed of individuals closely tied to the protocols development team. Although there is no public evidence of Bertram misusing this dual role, the overlap raises concerns about bias within the supposedly impartial Security Council.

To illustrate the risks of centralized decision making, the case of Aragon is important to consider, although specific circumstances differ. Aragon is a platform designed to help developers and communities build and manage DAOs[27]. The Aragon Association decided to dissolve the DAOs governing body, shut down its ANT token, and distribute most of its treasury, which included around $155 million in digital assets, without consulting the community. Angered members claimed it disproportionately benefited the founding team, leading the DAO community to vote to allocate funds towards legal action against its founding team. This decision made by the governing council explicitly violated the principles of decentralized governance associated with DAOs. This case highlights a larger problem: centralized entities, even within organizations that support decentralization, do not always reflect the desires of their communities. This case serves as evidence for how centralized groups, like the Security Council in Arbitrum, face potential conflicts of interest and are capable of overriding the will of the community they are supposed to represent.

Overall, Arbitrums centralized nature and lack of a wholly third-party composition undermine the decentralized ethos of the DAO. Centralized authorities introduce potential conflicts of interest and expose the final decision makers to external coercion due to their public identities. These vulnerabilities pose significant challenges to the trustworthiness of Arbitrum's governance model.

Comparative Analysis

Each DAOs governance model exhibits vulnerabilities that risk stability within the organization, treasury security, and member trust. As shown in Table 2, all three DAOs face shared challenges like coercion risk but differ in other significant vulnerabilities due to governance structure, highlighting the need for specific reforms.

Discussion

The vulnerabilities in DAO governance identified range from off-chain voting systems to coercion risks and flash loan exploits. Addressing solutions to these issues is necessary for ensuring trust and decentralization in DAO governance systems.

Transition from Off-Chain to On-Chain Voting

Off-chain voting mechanisms for final decision making, such as the protocol used in GnosisDAO, lack transparency and immutability. Adopting fully on-chain voting systems addresses these issues, as on-chain voting ensures results are binding and recorded in an immutable blockchain. Most DAOs already use blockchain voting, so clearly, this transition is feasible.

However, it is important to recognize that on-chain voting is not without its own set of issues. Problems with on-chain voting include the cost of participation, as voters must pay transaction fees on the blockchain to cast their votes. These fees can vary, leading to potential discrimination among voters because some individuals may face higher barriers to participation. Also, votes in on-chain systems are typically public, which could expose members to external pressure.[28] These issues highlight challenges associated with on-chain voting that have yet to be fully addressed.

Nevertheless, the transition to on-chain voting is essential for DAOs to adhere to their principles of immutability. While current shortcomings require attention, implementing blockchain based voting must be prioritized in order to ensure the foundational ethos of DAOs.

Another critical issue that affects the reliability of DAOs is the conflicting documentation, as in the case of Uniswap. A practical solution is for the community to vote to implement an automated cross-verification dashboard. This tool would continuously compare important governance parameters across official documentation, on chain data, and other sources and flagging discrepancies. This approach would detect and resolve

Table 2 Key vulnerabilities, causes, and trade-offs in the governance structures of major DAOs.

DAO	Primary Vulnerability	Effect on DAO	Root Cause / Trade-Off
Uniswap	Susceptibility to flash loan attacks	Risk of malicious proposals passing via temporary token control	Financially incentivized token system
GnosisDAO	Off-chain voting via Snapshot	Votes are not enforced on-chain; possible manipulation or inaction	Off-chain voting is cheaper and faster but lacks legitimacy
ArbitrumDAO	Centralized decision making by the Security Council	Decision-making potentially biased and susceptible to coercion due to power in the hands of a few	Central oversight is meant to act as a safeguard but undermines decentralization

inconsistencies quickly, ensuring that DAOs are committed to maintaining accurate information.

Enhancing Coercion Resistance through ZKPs and Homomorphic Encryption

Coercion resistance is the ability of a voting system to ensure that voters cannot be forced or bribed to vote in a specific way. In order to prevent coercion and outside manipulation, ideally, the voters are anonymous and the votes are secret[29]. This way, it is difficult to identify the voters to coerce outside of the blockchain network and impossible to determine how they voted. However, at best, voters in on-chain systems can only achieve pseudonymous status while currently, most DAOs have limited vote secrecy.

In order to make votes secret, DAOs could implement zero-knowledge proofs (ZKPs) and homomorphic encryption. If voter behavior is public, it becomes possible for external parties to coerce or manipulate voters based on their choices.

1. Zero-knowledge proofs (ZKPs) are cryptographic protocols that allow one party to prove to another party that a statement is true without revealing any additional information beyond the fact that the statement is true[30]. This concept is valuable in scenarios where sensitive information must remain private, like during voting. By keeping voter choices and proof of valid identity private, ZKPs help address coercion risks through ensuring that the vote is valid while the actual choice remains anonymous. This anonymity prevents external actors from knowing how a voter cast their vote, making coercion ineffective.

2. Homomorphic Encryption is a cryptographic technique that allows computations to be performed directly on encrypted data without the need to decrypt it first[31]. This means that sensitive information like voter behavior can remain hidden while still being added to determine the final outcome of the vote. The result of computations on the encrypted data, when decrypted, matches the output of the same computations performed on the unencrypted data.

   Zama, a cryptographic project, has developed solutions for implementing fully homomorphic encryption (FHE) in smart contracts[32]. These advancements bring encrypted voting directly to blockchain based DAOs, offering on-chain computations that preserve privacy and transparent voting mechanisms without compromising security. However, Zama is only one implementation, there are other well established schemes such as Paillier, ElGamal, and GSW, allowing DAOs to select the most suitable method for their governance. By using FHE, only the final aggregated tally is decrypted and shared, preserving voter anonymity and preventing real-time tampering.

In contrast, current off-chain voting systems like Snapshot often use Aztecs shielded voting[33,34]. This method encrypts votes during submissions but decrypts before tallying, which exposes the intermediate results and creates a privacy concern. While Aztecs approach is more common today, it does not provide the same level of end-to-end privacy during voting as FHE. However, FHE faces challenges, including high computational demands that limit its current scalability and adoption in blockchain environments. Despite these obstacles, FHE offers a stronger privacy guarantee, making it a promising technology for future DAO governance.

The combination of ZKPs and FHE offers a powerful solution to enhance privacy, security, and coercion resistance in DAO voting systems. By integrating both technologies, DAOs can create valid but hidden aggregated vote results, upholding voter privacy and strengthening trust in decentralized governance.

Token-based to One-Person-One-Vote

While token-based voting systems are widely used in DAOs today due to their financial incentives, encouraging active participation from investors and members, this system is vulnerable to exploitation. Flash loans exploit token-based voting systems by allowing attackers to temporarily buy large voting power and manipulate outcomes. A transition to a one-person-one-vote mechanism can completely eradicate this vulnerability, as it eliminates reliance on tokens and ensures a fair distribution of power among participants. This proposed system prevents gov-

ernance from being influenced by temporary token ownership and ensures that every member of the DAO has an equal voice in voting. It creates a more democratic participation and protects against coercion and economic manipulation with the right tools. Despite one-person-one-vote possibly encountering low user adoption and reducing incentive as participants don't need to hold a stake to vote, it strengthens the legitimacy and inclusivity of decision making, crucial to decentralization.

To guarantee that each account is tied to a real person and that individuals cannot create multiple accounts to gain additional voting power, identity verification mechanisms are needed:

1. The Proof of Humanity protocol provides a decentralized identity verification system that guarantees unique participation without compromising privacy [35]. Participants register by first creating a profile and submitting evidence of their humanity such as a video submission, claiming their unique online identity. Then, verified participants already in the registry vouch for new registrants and confirm the new users existence and validate that they are not a bot or duplicate account. Also, any suspicious profiles of pending submissions can be challenged and sent to a decentralized review court. This model ensures a fair and transparent way to link governance participation to unique individuals while minimizing risks of exploitation.

2. Soulbound Tokens (SBTs) are a theoretical solution under development that offers a promising method for enforcing one-person-one-vote governance [36]. SBTs are non-transferable tokens permanently linked to an individuals blockchain identity. Once issued, they cannot be sold, traded, or transferred, ensuring that governance rights remain with the original recipient. By replacing traditional governance tokens that can be bought with money with SBTs, DAOs can prevent flash loan exploits. SBTs ensure that each individual has a unique and immutable vote, eliminating vulnerabilities related to token borrowing.

Compared to existing BrightID Sybil Resistance, which relies on social graphs and community validation, SBTs provide a more scalable and tamper-resistant solution. BrightID relies on social verification, which is susceptible to manipulation through coordinated efforts and requires members to be consistently active [37]. On the other hand, SBTs cryptographically bind voting rights to a real identity on the immutable blockchain, allowing automated enforcement of one-person-one-vote systems without needing ongoing human intervention.

While SBTs have not yet been practically implemented, they are a fundamentally stronger and more reliable method for long-term identity and voting in DAO governance. Their development is a step toward guaranteeing secure and fair DAO governance.

By adopting a one-person-one-vote mechanism supported by tools like the Proof of Humanity and possibly Soulbound Tokens in the future, DAOs effectively end flash loan attacks. These measures are necessary to improve decentralized decision-making by preserving trust and fairness in blockchain systems.

Conclusion

The vulnerabilities in DAO governance ranging from off-chain voting mechanisms and coercion risks to flash loan attacks pose challenges to the security and trustworthiness of decentralized systems. Addressing these vulnerabilities requires a diverse approach combining governance-based, technical, and organizational improvements. Transitioning from off-chain to on-chain voting brings transparency and immutability.

Incorporating cryptographic techniques like ZKPs and homomorphic encryption can strengthen voter privacy and coercion resistance. Shifting from token-based voting to identity-based systems like one-person-one-vote eliminates flash loan threats and plutocracy, while tools such as Proof of Humanity and Soulbound Tokens support these systems by verifying unique identities in a decentralised manner. Strengthening DAO governance is essential for building trust and ensuring the success of decentralized systems in the growing blockchain and DeFi space.

However, it should be noted that this study focuses on a limited set of DAOs, specifically those with the highest treasury sizes at time of writing (e.g., GnosisDAO, Uniswap, and Arbitrum). While the analysis is relevant to high-stakes governance systems, it may not fully capture vulnerabilities related to smaller or newer DAOs. Additionally, some proposed solutions, such as Soulbound Tokens, remain theoretical and untested in real DAO environments, while others are very new and, like FHE, making them slower and less time efficient due to complexity. Some practical problems, such as legal regulations and acceptance by users remain uncertain.

Future studies should analyze a wider scope of DAOs, including those operating on different blockchain networks and governance models. This would provide a more broad understanding of vulnerabilities. Also, the proposed solutions would need to be implemented and tested. The practical evaluation of ZKPs, FHE, and one-person-one-vote mechanisms in real DAO environments is required to improve upon DAO vulnerabilities. This includes evaluating their usability and impact on governance outcomes. Since DAOs and blockchain are relatively new technologies, legal frameworks around them will continue to evolve, so future work must consider how DAOs can abide by rules and regulations while maintaining decentralization and privacy. Also, in order to persuade DAOs and their members to adopt these solutions, the social and economic incentives of widespread implementation must be understood by the readers.

By addressing these limitations and pursuing the future work, DAOs can evolve into more secure and fair governance systems, paving the way for the growth of decentralized finance in

blockchain.

Acknowledgements

The author would like to express sincere gratitude to Dr. Aida Manzano of Imperial College London for her guidance and support on this paper.

References

1 S. U. W. S. of Management, *In the News and Trending: Decentralized Autonomous Organizations (DAOs): What Are They and Why Are They Potentially Changing the Way Businesses Are Governed?*, https://whitman.syracuse.edu/about/newsroom/whitman-news/news-detail/2023/02/03/in-the-news-and-trending-decentralized-autonomous-organizations-%28daos%29-what-are-they-and-why-are-they-potentially-changing-the-way-businesses-are-governed, 2023.

2 DeepDAO, *DeepDAO Discovery Engine for DAO Ecosystem*, https://deepdao.io/organizations, 2024, Accessed: 2024-12-15.

3 Medium, *Hack Analysis: Cream Finance Oct 2021*, 2022, Medium, Published: 2022-11-09.

4 *Explained: The Tornado Cash Hack (May 2023)*, https://www.halborn.com/blog/post/explained-the-tornado-cash-hack-may-2023, 2023, Published: 2023-05-23.

5 M. Dalton, *Build Finance DAO Suffers Governance Takeover Attack*, https://cryptobriefing.com/build-finance-dao-suffers-governance-takeover-attack/, 2022, Published: 2022-02-15.

6 Immunefi, *Hack Analysis: Beanstalk Governance Attack, April 2022*, https://medium.com/immunefi/hack-analysis-beanstalk-governance-attack-april-2022-f42788fc821e, 2023, Medium, Published: 2023-01-09.

7 A. M. Kharman and B. Symth, *arXiv preprint arXiv:2406.08605*, 2024.

8 M. Bernhard *et al.*, Electronic Voting: Second International Joint Conference, E-Vote-ID 2017, Bregenz, Austria, October 24-27, 2017, Proceedings 2, 2017.

9 *Anonymity vs. Pseudonymity In Crypto*, https://www.gemini.com/cryptopedia/anonymity-vs-pseudonymity-basic-differences#section-what-does-a-pseudonym-mean-in-crypto, 2024.

10 U.S. Department of the Treasury, *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash*, https://home.treasury.gov/news/press-releases/jy0916, 2022.

11 Chainalysis, *What is AML and KYC for Crypto?*, https://www.chainalysis.com/blog/what-is-aml-and-kyc-for-crypto/, 2021.

12 E. Ologunde, *SSRN Electronic Journal*, 2023.

13 J. H. Lee, *PhD thesis*, Massachusetts Institute of Technology, 2019.

14 R. Feichtinger *et al.*, *arXiv preprint arXiv:2406.15071*, 2024.

15 J. Tan *et al.*, *arXiv preprint arXiv:2310.19201*, 2023.

16 Uniswap Labs, *Uniswap Governance Reference*, https://docs.uniswap.org/contracts/v2/reference/Governance/governance-reference, 2024.

17 Uniswap Labs, *Governance Process*, https://docs.uniswap.org/concepts/governance/process#, 2024, Uniswap Docs.

18 *CoinMarketCap: Cryptocurrency Prices, Charts And Market Capitalizations*, https://coinmarketcap.com/, 2024, Accessed: 2024-12-12.

19 *List of Flash Loan Attacks in Crypto*, https://immunebytes.com/blog/list-of-flash-loan-attacks-in-crypto/, 2024, ImmuneBytes, Published: 2024-05-30.

20 Gnosis DAO, *GnosisDAO Governance Documentation*, https://www.gnosis.io/dao, 2023.

21 *Welcome to Snapshot docs — snapshot*, https://docs.snapshot.box/, 2024, Accessed: 2024-12-12.

22 Akshata, *On-Chain and Off-Chain Voting in Blockchain*, https://metaschool.so/articles/on-chain-voting-in-blockchain, 2024, Published: 2024-03-21.

23 Bitcoin Calendar, *What Was the New York Agreement?*, https://calendar.bitbo.io/ny-agreement/, 2024.

24 *The Amended Constitution of the Arbitrum DAO*, https://docs.arbitrum.foundation/dao-constitution, 2024, Accessed: 2024-12-12.

25 *Security Council Members*, https://docs.arbitrum.foundation/security-council-members, 2024, Arbitrum DAO - Governance docs.

26 *Security Council: A conceptual overview*, https://docs.arbitrum.foundation/concepts/security-council, 2024, Arbitrum DAO - Governance docs.

27 E. Reguerra, *Aragon DAO votes to fund legal action against its founders*, https://cointelegraph.com/news/aragon-dao-lawsuit-founders-patagon-management, 2023, CoinTelegraph, Published: 2023-11-21.

28 S. Park *et al.*, *Journal of Cybersecurity*, 2021, **7**, tyaa025.

29 H. Jonker and W. Pieters, *Anonymity in voting revisited*, https://www.researchgate.net/publication/221156726_Anonymity_in_Voting_Revisited, 2010, ResearchGate.

30 Chainlink, *Zero-Knowledge Proof (ZKP) Explained*, https://chain.link/education/zero-knowledge-proof-zkp, 2024.

31 K. Yuan *et al.*, *National Institutes of Health*, 2023.

32 R. Hindi, *Private Smart Contracts Using Homomorphic Encryption*, https://www.zama.ai/post/private-smart-contracts-using-homomorphic-encryption, 2023, Zama, Published: 2023-05-23.

33 Aztec Protocol Team, *Aztec Network Documentation*, https://docs.aztec.network/aztec, 2024, Accessed: 2024-12-12.

34 *Shielded Voting*, https://www.shutter.network/shielded-voting, 2024, Shutter.

35 *Proof of Humanity*, https://proofofhumanity.id/, 2024, Accessed: 2024-12-12.

36 Coinbase, *What are Soulbound Tokens (SBT)?*, https://www.coinbase.com/zh-cn/learn/crypto-glossary/what-are-soulbound-tokens-sbt, 2024.

37 BrightID Foundation, *BrightID Whitepaper*, https://www.brightid.org/whitepaper, 2020.