DeFi Attacks and the Role of DAOs*

Bianca Kremer and Kanye Ye Wang

Abstract Decentralized Finance (DeFi) represents an innovative alternative to the traditional financial system and is driven by blockchain technology. While it has witnessed significant growth, it has also been plagued by a range of security breaches, including hacks and other malicious attacks, leading to significant financial losses. By 2022, such attacks within the DeFi ecosystem amounted to an alarming $3.8 billion. Within this landscape, Decentralized Autonomous Organizations (DAOs), a pioneering model of bottom-up coordination, have emerged as both potential mitigators of risk and, paradoxically, potential attack vectors. In this paper, we explore the multifunctional role of DAOs within DeFi attacks. We examine their proactive involvement in preventing, mitigating, and responding to such attacks, while also being susceptible targets. Through case studies involving DAOs, we provide insights into how DAOs operate in DeFi.

I. Introduction

Decentralized Finance (DeFi) is an alternative to the traditional financial system and offers a rich array of services.[1] It is built using blockchain technology and supported by smart contracts. Ethereum, a leading programmable blockchain, hosts both DeFi incarnations of traditional financial services, such as exchanges, trading, lending, derivatives, banking, and a plethora of novel and innovative financial products, including stablecoins, flash loans, and more.[2]

* Thanks to Ding Feng for valuable research assistance. We thank Professor Kevin Werbach for valuable feedback on the initial draft. We are grateful to the organizers of the Lisbon DAO Regulation Conference for inviting us to share and test our preliminary ideas. This article is based on our presentation at the Lisbon DAO Observatory's DAO Regulation Conference held in April 2023. This article was made possible due to the support of the Wharton Blockchain and Digital Asset Project and the grant from the University of Macau (File no. APAEM/SG/0005/2023).

[1] See e.g., *Coelho-Prabhu*, A Beginner's Guide to Decentralized Finance (DeFi), Coinbase, 2020, https://www.coinbase.com/de/blog/a-beginners-guide-to-decentralized-finance-defi (26.07.2023) ("Imagine a global, open alternative to *every* financial service you use today – savings, loans, trading, insurance and more – accessible to anyone in the world with a smartphone and internet connection."). See also *Zetzsche et al.*, Decentralized Finance, Journal of Financial Regulation, 2020, 6, 183.

[2] See https://ethereum.org/en/defi (13.07.2023) ("DeFi is a collective term for financial products and services that are accessible to anyone who can use Ethereum – anyone with an

The DeFi ecosystem has seen substantial growth, especially during 2020 and 2021. DeFi projects now hold a total value of close to 50 billion USD (total value locked, TVL), reaching its peak of close to 180 billion USD in mid-2022 before entering a bear market.[3] However, it is impossible to ignore the significant number of hacking incidents that occurred during this period. Indeed, 2022 was the worst year for DeFi in terms of hacks, with losses totaling 3.8 billion USD according to Chainalysis reports.[4] These attacks often exploit vulnerabilities in the code or the governance system of DeFi protocols, in a way that harms the protocol or its users. Additionally, numerous risk events shook the market in 2022, such as the Terra Luna crash.[5] The wider crypto ecosystem, especially centralized finance (CeFi) saw the collapse of Three Arrows Capital,[6] the bankruptcy of the crypto exchange FTX,[7] and the financial failure of Silvergate and Silicon Valley Bank (SVB), which were banks that supported crypto startups.[8]

In face of potential malicious attacks and various risks, a robust governance system is vital for DeFi projects to be successful. One of the fastest growing bottom-up governance models in DeFi are so-called Decentralized Autonomous Organizations (DAOs). While the concept of DAOs was initially theorized in the 1990s, it gained significant attention when Ethereum co-founder Vitalik Buterin wrote a blog post about it on ethereum.org.[9] Though early experiments

---

internet connection. With DeFi, the markets are always open and there are no centralized authorities who can block payments or deny you access to anything.", "There's a booming crypto economy out there, where you can lend, borrow, long/short, earn interest, and more. Crypto-savvy Argentinians have used DeFi to escape crippling inflation.").

[3] See https://defillama.com/ (13.07.2023).

[4] See https://blog.chainalysis.com/reports/2022-biggest-year-ever-for-crypto-hacking (13.07.2023).

[5] See e.g., *Liu et al.*, Anatomy of a Run: The Terra Luna Crash, National Bureau of Economic Research, Working Paper 31160, 2023, https://www.nber.org/papers/w31160 (13.07.2023) (explaining that a variety of factors led to the collapse and incentivizing market participants to stay vigilant and actively monitor the system, "The complexity of the system made it difficult even for insiders to understand the buildup of risk. Finally, we draw broader lessons about financial fragility in an environment where a regulatory safety net does not exist, pseudonymous transactions are publicly observable, and market participants are incentivized to monitor the financial health of the system.")

[6] See *Lee et al.*, How Three Arrows Capital Blew Up and Set Off a Crypto Contagion, Bloomberg, 2022, https://www.bloomberg.com/news/features/2022-07-13/how-crypto-hedge-fund-three-arrows-capital-fell-apart-3ac (13.07.2023).

[7] See *Reif*, The Collapse of FTX: What Went Wrong with the Crypto Exchange?, Investopedia, 2023, https://www.investopedia.com/what-went-wrong-with-ftx-6828447 (25.08.2023). See also Chaturvedi, Crypto's Horrible, No Good, Very Bad Year, Investopedia, 2022, https://www.investopedia.com/cryptos-horrible-no-good-very-bad-year-6835076 (13.07.2023).

[8] See *Morris*, A Tale of 2 Banks: Why Silvergate and Silicon Valley Bank Collapsed, Yahoo Finance via CoinDesk, 2023, https://finance.yahoo.com/news/tale-2-banks-why-silvergate-174002150.html (13.07.2023).

[9] See *Buterin*, Ethereum Blog 2014, https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide (13.07.2023).

like "The DAO" in 2016 were pivotal,[10] it was not until the DeFi boom of 2020 that DAOs truly began to proliferate.[11] DAOs are essentially self-governing entities that operate on a set of rules encoded in smart contracts, without the need for traditional intermediaries or centralized authorities. DAOs can have various purposes and goals, such as investing in start-ups, managing a stablecoin, or buying digital art.

Most major DeFi platforms employ DAOs, and if they do not, DAOs are often seen as a promising direction for the evolution of DeFi, as they embody the ethos of decentralization and empower users to have a voice and a stake in the protocols they use. Indeed, DAOs are highly popular within the DeFi ecosystem. According to Chainalysis reports, among various Web3 sectors, DeFi boasts the highest concentration of DAOs.[12] Noteworthy examples include Uniswap DAO, Lido DAO, MakerDAO, and CurveDAO, some of the largest entities in this space. This is no surprise as DAOs emerged as a way to manage resources and coordinate activities when DeFi skyrocketed in 2020, a period often referred to as "DeFi summer".[13]

DAOs play an important role in the DeFi ecosystem. They serve as entities managing governance systems for DeFi protocols, enabling collective decision-making and coordination among participants. However, the functionalities and operations of DAOs can also be susceptible to various attacks, with consequences potentially reverberating throughout the DeFi ecosystem.

Governance attacks are typically aimed at exploiting the decision-making processes of DAOs. Bad actors might manipulate votes to make decisions favorable to them, oftentimes utilizing flash loans to acquire substantial voting power temporarily. This form of attack focuses primarily on the governance structure and procedures, rather than on the underlying smart contract vulnerabilities.

Direct vulnerabilities in the smart contracts of DeFi services could lead to loss of funds or other exploitable scenarios independent of DAO governance attacks. Hackers may take advantage of flaws in the code and drain funds or manipulate contract interactions for their benefit. Other types of attacks are, e. g., bridge attacks, which involve exploiting vulnerabilities in the bridges con-

---

[10] See e. g., *Morris*, The DAO Hack: How a $60M Ethereum Attack Shaped Crypto History, 2023, https://www.coindesk.com/consensus-magazine/2023/05/09/coindesk-turns-10-how-the-dao-hack-changed-ethereum-and-crypto (13.07.2023).

[11] *Gogel et al.*, Decentralized Autonomous Organization Toolkit Insight Report, World Economic Forum in Collaboration with the Wharton Blockchain and Digital Asset Project, 2023, 4, https://www3.weforum.org/docs/WEF_Decentralized_Autonomous_Organization_Toolkit_2023.pdf (13.07.2023).

[12] See https://www.chainalysis.com (13.07.2023).

[13] *Gogel et al.*, Decentralized Autonomous Organization Toolkit Insight Report, World Economic Forum in Collaboration with the Wharton Blockchain and Digital Asset Project, 2023, 4, https://www3.weforum.org/docs/WEF_Decentralized_Autonomous_Organization_Toolkit_2023.pdf (25.08.2023).

necting different blockchains or layer 2 solutions, affecting the interoperability and functionality of DeFi services, potentially leading to loss of funds and data integrity issues.

DAOs can actively work to prevent, mitigate, and respond to the various forms of attacks mentioned above by enforcing rigorous code audits, implementing robust governance mechanisms, and establishing responsive frameworks to detect and handle vulnerabilities and breaches.

Given the rising prominence and economic influence of DAOs in the DeFi ecosystem, there is an increasing need to understand these entities better. DAOs have become critical players in shaping the economic landscape of decentralized finance, affecting how value is created, distributed, and exchanged. Therefore, our research aims to investigate what role DAOs play in DeFi attacks. Understanding the interplay between DeFi and DAOs can give valuable insights into the stability and governance of the DeFi ecosystem, offering actionable strategies to bolster its security and resilience. These findings can inform subsequent research questions aimed at addressing the challenges of regulating DeFi and DAOs.

To address our research question about the role of DAOs in DeFi attacks, we conduct empirical studies, beginning with an examination of projects in the attack dataset provided by Zhou et al.,[14] which consists of 181 DeFi attacks that occurred on Ethereum and Binance Smart Chain between April 30, 2018, and April 30, 2022. Excluding duplicate attacks, we find 169 unique instances. Among these, 92 projects featured a DAO or voting mechanism, 72 did not, and 5 were inconclusive. We then examine the response measures adopted by DAOs against attacks, along with specific instances of governance attacks targeting DAOs.

This paper is structured as follows. Part I introduces DeFi and DAOs and offers some background information. Part II delves into the risks of the DeFi ecosystem and the role DAOs play in this complex landscape. Part III delivers the findings of our empirical analysis and interprets the results in the context of our present discussion. Part IV brings our discussion to a close with concluding remarks.

II. DeFi, its Risk Landscape and The Role of DAOs

This Part introduces the phenomena of DeFi, DeFi risks and DAOs. Section 1 outlines the features of DeFi. Section 2 explores DeFi risks, highlighting risk categories and real-world examples. Section 3 defines DAOs, while Section 4 examines their role within the DeFi landscape.

[14] *Zhou et al.*, SoK: Decentralized Finance (DeFi) Attacks, Cryptology EPrint Archive, 2022.

1. Features of DeFi

DeFi protocols represent a noteworthy innovation in financial systems, challenging traditional financial models by utilizing smart contracts, and offering decentralized alternatives to traditional financial services.[15] Some even suggests that the convergence of DeFi and web3 could potentially lead to notable changes in future financial infrastructures.[16] Web3 is a term used to describe the evolution of applications on the internet, aiming for decentralized architectures built on technologies such as blockchain and smart contracts. While the original internet was designed for peer-to-peer communication, web3 aims to extend this decentralization to include user data ownership, financial transactions, and more. DeFi can be considered a significant application of the web3 vision, seeking to create more open, transparent, fair, and inclusive financial systems that empower users and communities over traditional intermediaries.[17]

DeFi platforms enable users to access and exchange financial assets without relying on intermediaries, which increases the efficiency of transactions and potentially reduces costs.[18] One key feature of DeFi protocols is their non-custodial nature; unlike traditional financial institutions, these platforms do not hold or manage users' funds. Instead, users retain complete control over their assets, stored in their own digital wallets, which interact directly with the smart contracts.

Typically, users do not need to provide any personal information or credentials to access or use DeFi protocols. Furthermore, the open source and permissionless nature of DeFi protocols allow anyone to audit the code and join or leave the network at will, increasing financial inclusion and offering opportunities to a more diverse range of participants.

DeFi platforms are often championed as catalysts for financial democratization, aspiring to extend financial services to the unbanked or underbanked, thus allowing more inclusive participation in financial activities beyond the confines of traditional banking infrastructures. This inclusivity potentially empowers

---

[15] *Schär*, Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets, Federal Reserve Bank of St. Louis Review 103 no. 2, 2021, 153-74.

[16] See *Gapusan*, DeFi: Who Will Build The Future of Finance?, Forbes 2021, https://www.forbes.com/sites/jeffgapusan/2021/11/02/defi-who-will-build-the-future-of-finance/ (25.08.2023).

[17] See e.g., *Zetzsche et al.*, Decentralized Finance, Journal of Financial Regulation, 2020, 6, 183 ("Despite technological limitations of the Bitcoin design, particularly in terms of speed and scalability, DeFi enthusiasts argue that the cryptoanarchist vision which was part of the motivation for Bitcoin is now attainable: the democratization of finance.", "DeFi enthusiasts go beyond technical decentralization. For them, DeFi offers governance structures they perceive as the 'democratization' of finance, while incuments might well view such structures as 'anarchy'.")

[18] *Deshmukh et al.*, Decentralized Finance (DeFi) Policy-Maker Toolkit, World Economic Forum in Collaboration with the Wharton Blockchain and Digital Asset Project, 2021, 6, https://www3.weforum.org/docs/WEF_DeFi_Policy_Maker_Toolkit_2021.pdf (25.08.2023).

individuals in developing regions, or those marginalized from mainstream financial systems to access savings, lending, and investment opportunities previously unavailable to them. However, despite its potential and the advocacies for its democratizing role, the discourse around DeFi's actual effectiveness in making finance more inclusive is ongoing, with varying perspectives on DeFi's capacity to deliver on its promises. While DeFi may reduce the risk of fund misuse or mismanagement by eliminating central authorities, there are numerous other risks inherent in DeFi.

2. DeFi Risks

Despite its many promised advantages, it's crucial to acknowledge that DeFi also presents its own set of challenges and risks, many of which are not yet fully understood. Researchers like Carter and Jeng,[19] point out that these risks are understudied, [20] making the mitigation of these challenges a pressing issue. They also argue that as DeFi becomes mainstream, it will be paramount for regulators and industry to understand the risks that DeFi poses for society and the economy.[21]

Various organizations and researchers have proposed classifications for these risks, providing a framework to comprehend and address them. We will introduce some DeFi risk categories and offer examples of real-life incidents in the DeFi space.

a) DeFi Risk Categories

In a report published in February 2023, the Financial Stability Board (FSB), an intergovernmental body responsible for monitoring and making recommendations about the global financial system, outlined key vulnerabilities associated with DeFi.[22] These vulnerabilities include operational fragilities, liquidity and maturity mismatches, leverage, interconnectedness, concentration, and complexity, as well as other risks like market integrity issues and cross-border regulatory arbitrage. Given the FSB's role in assessing global financial risks, these findings serve as a crucial point of reference for understanding the challenges posed by DeFi's rapid evolution.

Other models and risk categorization offer valuable insight. In Zhou et al.'s threat model taxonomy, DeFi incidents are described as "a series of actions that

[19] *Carter/Jeng*, DeFi Protocol Risks: The Paradox of DeFi, Regtech, Suptech and Beyond: Innovation and Technology in Financial Services, RiskBooks 2021, 36.

[20] *Carter/Jeng*, DeFi Protocol Risks: The Paradox of DeFi, Regtech, Suptech and Beyond: Innovation and Technology in Financial Services, RiskBooks 2021, 1.

[21] *Carter/Jeng*, DeFi Protocol Risks: The Paradox of DeFi, Regtech, Suptech and Beyond: Innovation and Technology in Financial Services, RiskBooks 2021, 1.

[22] Financial Stability Board, The Financial Stability Risks of Decentralized Finance, 2023, https://www.fsb.org/2023/02/the-financial-stability-risks-of-decentralised-finance/(25.08.2023).

result in an unexpected financial loss to one or more of the following entities: (i) users; (ii) liquidity providers; (iii) speculators; or (iv) operators".[23] Further subcategories for DeFi incidents distinguish between "attacks" and "accidents", whereby in the former an "attacker" may take advantage of vulnerabilities in either the smart contract, the DeFi protocol design or auxiliary service layers and in the latter proactive adversaries may "not explicitly [be] involved".[24] The lines dividing "attacks" and "accidents" may not always be clear cut.

WEF's and Wharton BDAP's DeFi Policy-Maker Toolkit[25] presents five DeFi risk categories: financial,[26] technical,[27] operational,[28] legal compliance,[29] and emergent.[30] The report distinguishes several related risks in each of these five broader risk categories. Some risks, like liquidity risk, are analogous to those encountered in conventional finance, whereas others are entirely new such as smart contract failures, MEV[31] or flash loans.[32]

---

[23] *Zhou et al.*, SoK: Decentralized Finance (DeFi) Attacks, Cryptology EPrint Archive, 2022, 4.

[24] *Zhou et al.*, SoK: Decentralized Finance (DeFi) Attacks, Cryptology EPrint Archive, 2022, 4 ("For example, a user's fund may become permanently locked in a contract due to unintentional coding mistakes.").

[25] WEF/Wharton BDAP, Decentralized Finance (DeFi) Policy-Maker Toolkit, Whitepaper 2021, https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/06/DeFi-Policy-Maker-Toolkit-Final.pdf (25.08.2023).

[26] See WEF/Wharton BDAP, Decentralized Finance (DeFi) Policy-Maker Toolkit, Whitepaper 2021, 14. Financial risks involve potential fund loss due to market volatility, counterparty defaults, liquidity crunches, or market manipulation.

[27] See WEF/Wharton BDAP, Decentralized Finance (DeFi) Policy-Maker Toolkit, Whitepaper 2021, 15 et seq. Technical risks pertain to software failures or attacks, such as those affecting smart contracts or miners, which may result in DeFi service disruptions or significant financial losses like the 2016 DAO exploit.

[28] See WEF/Wharton BDAP, Decentralized Finance (DeFi) Policy-Maker Toolkit, Whitepaper 2021, 16 et seq. Operational risks are human-system failures or challenges, including maintenance, upgrades, or governance issues, that can cause difficulties in implementing changes or make DeFi services vulnerable to malicious attacks.

[29] See WEF/Wharton BDAP, Decentralized Finance (DeFi) Policy-Maker Toolkit, Whitepaper 2021, 18. Legal compliance risks are associated with illicit activities or regulatory evasion through DeFi, potentially involving money laundering or market manipulation via pseudonymous identities, challenging regulatory enforcement.

[30] See WEF/Wharton BDAP, Decentralized Finance (DeFi) Policy-Maker Toolkit, Whitepaper 2021, 18 et seq. Emergent risks represent systemic instability due to the interaction and scaling of DeFi components, creating potentially complex financial instruments that may cause widespread impacts like a flash loan attack.

[31] MEV, or Miner/Maximal Extractable Value, refers to the measure of the profit a miner (or validator etc.) can make through their ability to arbitrarily include, exclude, or re-order transactions within the blocks they produce. In blockchain ecosystems, especially in Ethereum, MEV has become a prominent issue as it can lead to various forms of exploitation or unfair advantage, impacting the fairness and security of the network. For more on MEV, see https://ethereum.org/en/developers/docs/mev (25.08.2023).

[32] See Knowledge at Wharton, The Opportunities and Dangers of Decentralizing Finance, 2021, https://knowledge.wharton.upenn.edu/article/opportunities-dangers-decentralizing-finance/ (25.08.2023). Flash loans are uncollateralized loans that are borrowed and repaid

Carter and Jeng[33] categorize DeFi risks in five broad risk factors. The first is the risk arising from DeFi's interconnections with the traditional financial system, including bank failures, regulatory actions, and market illiquidity that could impact associated stablecoins or fiat currencies. Additionally, the operational risks deriving from the underlying blockchains are considered, with potential pitfalls such as consensus failures, protocol interventions, and miner or validator manipulation, all of which could compromise the security or functionality of DeFi systems.

The study further highlights the vulnerabilities tied to the usage of smart contracts in DeFi. These encompass technical glitches, oracle attacks, and excessive leverage which can affect the contracts' code or logic. Moreover, governance and regulatory risks pose threats of administrative key abuse, governance attacks, tainted liquidity, or pseudo-equities that might weaken the control mechanisms or legitimacy of DeFi protocols. Lastly, scalability challenges in the form of high transaction fees, low throughput, or network congestion are recognized, which could negatively impact the overall performance and accessibility of DeFi platforms.

These are just some among several risk categorization efforts undertaken across various groups. Multiple models like Zhou et al.'s threat model taxonomy, the WEF's and Wharton BDAP's DeFi Policy-Maker Toolkit, the model presented by Carter and Jeng, and the Financial Stability Board's report have sought to categorize and shed light on these potential pitfalls. These encompass both familiar risks as well as newer, technology-specific risks.

Understanding risks associated with smart contracts and governance mechanisms is important due to their central role in the functioning of DeFi platforms, and any glitches or malicious attacks can have serious consequences. The operational risks deriving from the underlying blockchains such as consensus failures and protocol interventions are equally important, as they can compromise the security or functionality of DeFi systems.

In conclusion, while all the models presented offer valuable insights, FSB's taxonomy provides a comprehensive framework that is globally attuned, making it particularly relevant. However, assimilating insights from the various taxonomies will allow for a more nuanced and holistic understanding of the risks in the DeFi landscape, enabling the development of robust solutions and informed policymaking.

---

within the same transaction, allowing users to execute complex arbitrage or manipulation strategies without upfront capital.

[33] *Carter/Jeng*, DeFi Protocol Risks: The Paradox of DeFi, Regtech, Suptech and Beyond: Innovation and Technology in Financial Services, RiskBooks 2021, 6 et seq.

b) Examples of Real-World DeFi Incidents

One of the most prominent and controversial incidents in the history of DAOs and DeFi protocols was the hack of The DAO in 2016, arguably not only the first DAO but also the first attempt at creating a DeFi mechanism. The DAO developers wanted to leverage the technology for a new way of funding and governing decentralized applications (DApps) on the Ethereum blockchain. Additionally, this was also a first attempt to realize Vitalik's concept of a DAO. The DAO was powered by smart contracts, which are self-executing agreements encoded in computer code. It raised over 150 million USD worth of ether (ETH), the native cryptocurrency of Ethereum, in a crowdfunding campaign, considered as one of the largest crowdfunding campaigns of its time,[34] and it attracted thousands of investors from around the world.

However, things took a dark turn when an unknown attacker exploited a re-entrancy bug in The DAO's smart contract code and drained over 50 million USD worth of ether from the fund. This was a devastating blow for The DAO and its investors, and it sparked a heated debate in the Ethereum community about how to deal with the situation. Some argued that code is law, and that the attacker should be allowed to keep the stolen funds, as they were acting within the rules of the smart contract. Others argued that code is not law, and that the funds should be returned to investors. This led to a proposal to conduct a hard fork[35] on Ethereum to undo the attack.

The hard fork proposal was put to a vote by the Ethereum community, and it received majority support. However, not everyone agreed with the hard fork, and some decided to stick with the original version of Ethereum that did not reverse the attack. This resulted in two separate blockchains: Ethereum and Ethereum Classic. Ethereum Classic maintained the original history of transactions, while Ethereum created a new history that erased the attack.

This was a significant event that had major implications for DeFi and Ethereum. It exposed some of the risks and challenges of building decentralized applications on smart contracts, such as security vulnerabilities, governance issues, ethical dilemmas, and community conflicts. It also raised questions about the immutability and censorship-resistance of blockchains.

---

[34] However, it's important to note that despite its initial fundraising success, The DAO did not manage to successfully fund projects that reached fruition. Additionally, while it attracted thousands of investors from around the world, subsequent crowdfunding efforts, have since surpassed it in scale.

[35] A hard fork is a radical change to a blockchain protocol that creates a permanent divergence from the previous version of the protocol. A hard fork requires all nodes or users to upgrade to the latest version of the protocol software. Those who do not upgrade will be left behind on an incompatible network.

After the DAO hack of 2016, the landscape of DeFi has continued to evolve and expand. Along with this growth, unfortunately, have come several notable instances of security breaches and attacks.

For instance, in 2017, an attacker exploited a vulnerability in the smart contract code of Parity, a popular Ethereum wallet, and stole 32 million USD worth of ether from several DeFi projects that used Parity as their wallet provider.[36] Another example is the 2018 attack on Bancor, a decentralized exchange, where an attacker compromised a wallet used by the platform and stole 23.5 million USD worth of ether, Bancor's BNT, and Pundi X's NPXS tokens from the platform.[37]

Some of these attacks also involve the use of flash loans, which are loans that are borrowed and repaid within the same transaction. Flash loans allow users to access large amounts of liquidity without collateral, but they also enable attackers to manipulate prices and exploit arbitrage opportunities. For example, in 2022, an attacker used flash loans to exploit Cream Finance, a lending protocol, and stole 130 million USD worth of cryptocurrency from the platform.[38]

In May 2023 the Tornado Cash DAO[39] was attacked by an unknown entity that managed to gain full control over its governance state via a malicious proposal granting it more than a million votes.[40] The attacker then submitted a proposal to undo their attack and return governance control back to the community.[41] The attacker's motives were unclear, but some speculated that they were trying to manipulate the price of TORN or test the security of the protocol.

Each highlighted incident reveals distinct vulnerabilities and challenges within DeFi, contributing uniquely to the evolution of this space. The DAO Hack in 2016 triggered philosophical debates and led to structural changes in Ethereum. The 2017 Parity and 2018 Bancor attacks illuminated critical security vulnerabilities in wallet software and decentralized exchanges, emphasizing the need for robust security protocols across diverse applications and platforms. Cream Finance's 2022 exploit unveiled the risks associated with innovative

[36] See *Zhao*, $30 Million: Ether Reported Stolen Due to Parity Wallet Breach, Coindesk, 2017, https://www.coindesk.com/markets/2017/07/19/30-million-ether-reported-stolen-due-to-parity-wallet-breach/ (25.08.2023).

[37] See *Russell*, The crypto world's latest hack sees Bancor lose $23.5M, TechCrunch, 2018, https://techcrunch.com/2018/07/10/bancor-loses-23-5m breach (25.08.2023).

[38] See *Copeland*, Ethereum DeFi protocol Cream Finance hacked for more than $130 million, The Block 2022, https://www.theblock.co/post/122241/ethereum-defi-protocol-cream-finance-hacked-for-115-million (25.08.2023).

[39] Tornado Cash is a privacy-preserving protocol that allows users to send anonymous transactions on Ethereum. The Tornado Cash DAO is distinct from the Tornado Cash mixer. In 2022, the Tornado Cash mixer was sanctioned by OFAC.

[40] See *Sarkar*, Attacker hijacks Tornado Cash governance via malicious proposal, Coindesk, 2023, https://cointelegraph.com/news/attacker-hijacks-tornado-cash-governance-via-malicious-proposal (25.08.2023).

[41] See *Nwaokocha*, Tornado Cash governance control set to be restored as voters approve proposal, Coindesk 2023, https://cointelegraph.com/news/tornado-cash-governance-control-set-to-be-restored-as-token-votes-approve-proposal (25.08.2023).

DeFi instruments like flash loans, stressing the substantial financial repercussions of such vulnerabilities. Finally, the 2023 Tornado Cash DAO incident spotlighted the complexities and potential frailties in decentralized governance, emphasizing the diverse motivations behind such attacks. Each incident can serve as a lesson to refine governance and security frameworks in DeFi and their DAO ecosystems.

3. What are DAOs?

DeFi and DAOs are not just new technologies. They are new modes of organizing and governing economic activity. They challenge the existing legal and regulatory frameworks that have been designed for a different world – a world of centralized intermediaries, custodial services, and jurisdictional boundaries.

DAOs and DeFi protocols are new dynamic phenomena that do not always correspond to traditional notions of corporations, legal contracts, assets, or financial services. Moreover, DAOs and DeFi protocols may change over time, as they evolve through governance decisions, code updates or forks.

There is no universally accepted or standardized definition of DAOs and DeFi protocols, as various stakeholders may have different perspectives. For example, developers may focus on the technical features and functionalities, while regulators may be more interested in the legal implications and consequences of DeFi and DAOs.

A possible definition for DAOs is that they are a new form of internet-native organization represented by rules and decision processes encoded via blockchain technology using smart contracts. DAOs, in essence, can be seen as blockchain-based, open-source systems that operate through smart contracts and are governed by token holders' consensus, primarily to achieve a democratic governance structure that guides the developmental trajectory of the platform.

In a DAO, the process typically consists of a set of programmed rules or protocols allowing members to propose, discuss, and vote on decisions and changes related to the project.[42] Users typically become members by purchasing or earning tokens related to the DAO. These tokens usually represent voting power within the organization. DAO members can submit proposals for changes, new features, developments, or any other modifications to the organization or its governing protocols. Any submitted proposals are subject to discussion and scrutiny by the community, allowing for a thorough examination of their merits and disadvantages. This can occur on various platforms such as forums, chat groups, or other communication channels associated with the DAO.

Finally, members vote on proposals using their tokens, where one token may represent one vote. However, different models and voting structures exist. Some

[42] See e.g., snapshot, which is a popular voting service, https://snapshot.org (25.08.2023).

DAOs may have a quorum requirement, meaning a minimum number of votes is needed for the proposal to go through. If a proposal receives enough support (meets the required quorum and receives more affirmative than negative votes), the proposed changes are either automatically executed by the smart contract or are taken forward for implementation. The specifics of how a proposal is executed can vary depending on the rules encoded in the DAO's smart contracts.

4. DAOs in the DeFi Ecosystem

As new internet-native modes of organization, DAOs can be seen as a new form of organizational structure that challenges traditional models.[43] DAOs are designed to enable collective decision-making and coordination among participants. They thus enable communities to coordinate their activities in a more open and transparent way, minimizing trust. DAOs in the DeFi space play three key roles. First, they decentralize decision-making, allowing participants to shape the direction of DeFi protocols directly, without traditional intermediaries. Second, they promote innovation, providing a platform for creating and testing new DeFi products and services. They facilitate resource sharing and foster partnerships across different DAOs and protocols. Lastly, DAOs may encourage inclusivity by allowing anyone with internet access and a compatible digital wallet to join, thereby giving interested users the opportunity to benefit from and contribute to DeFi protocols. Nevertheless, the realization of these key benefits is not always guaranteed. Issues can arise when governance becomes concentrated in the hands of a select few, undermining the principle of decentralized decision-making. Similarly, if DAOs and DeFi protocols do not offer genuine opportunities for user involvement, the potential for inclusivity can be significantly diminished.

By transitioning control and ownership to the broader community, developers may wish to distance themselves from the purview of regulatory scrutiny and legal responsibility, not only in the U.S. but across various jurisdictions worldwide. For example, bZx Protocol developers stated that the creation of a DAO would insulate the Protocol "from regulatory oversight and accountability for compliance with U.S. law,"[44]. However, this may not always be the case, as some DAOs have faced legal challenges and lawsuits from users and/or regulators.

---

[43] See e.g., Ethereum Foundation, Decentralized autonomous organizations (DAOs), https://ethereum.org/en/dao (25.08.2023).

[44] See *Drylewski et al.*, Court Ruling Could Affect the Future Direction of DAOs, Insights, Skadden, Arps, Slate, Meagher & Flom LLP 2023, https://www.skadden.com/insights/publications/2023/04/court-ruling-could-affect-the-future-direction-of-daos (25.08.2023).

III. Empirical Analysis

We investigate real-world DeFi attacks to examine the involvement of DAOs. The dataset[45] consists of 181 DeFi attacks that happened on Ethereum and Binance Smart Chain (BSC) between April 30, 2018, and April 30, 2022 (four years). These attacks were reported on internet websites, predominantly Rekt News,[46] SlowMist,[47] PeckShield,[48] and Medium.[49]

1. Method

This Section describes the method and findings of the empirical analysis conducted in this study.

a) Data Collection

To examine the involvement of DAOs in DeFi attacks, we analyzed whether the 169 projects in the attack event dataset[50] (totaling 181 attack events, with some projects attacked multiple times) used DAOs or similar voting mechanisms for governance. We used three information channels to make this determination:

1. We looked for information or subpages related to "Governance", "Vote", or "DAO" on the official project website.
2. We used Twitter's advanced search function to find tweets of exploited projects containing the keywords: "Governance," "vote," or "DAO" within a timeframe from one month before the attack event to one month after.
3. We searched Google for content containing the keywords "project name" + "Governance," "vote," or "DAO".

After uncovering attacked projects with DAOs, we selected the ten most recent ones from the dataset for case studies, in order to examine the way in which DAOs are involved in attacks.

b) Findings

Ultimately, we found that out of the 169 attacked projects, 92 had a DAO or a similar voting governance mechanism, 72 did not adopt a DAO, and 5 projects were inconclusive due to broken official website links and deactivation of Twitter accounts.

---

[45] *Zhou et al.*, Sok: Decentralized finance (defi) attacks, Cryptology ePrint Archive 2022.
[46] rekt. https://rekt.news/ (25.08.2023).
[47] SlowMist Hacked, https://hacked.slowmist.io/en/ (25.08.2023).
[48] PeckShield, https://peckshield.medium.com (25.08.2023).
[49] Medium, https://medium.com (25.08.2023).
[50] *Zhou et al.*, Sok: Decentralized finance (defi) attacks, Cryptology ePrint Archive 2022.

More than half of the attacked projects have DAOs or some form of voting and governance mechanism, a fact that underscores the widespread acceptance and adoption of DAOs within the DeFi ecosystem. However, it's important to note that the existence of a DAO within an attacked project does not necessarily imply that the DAO directly participated in handling and responding to the attack.

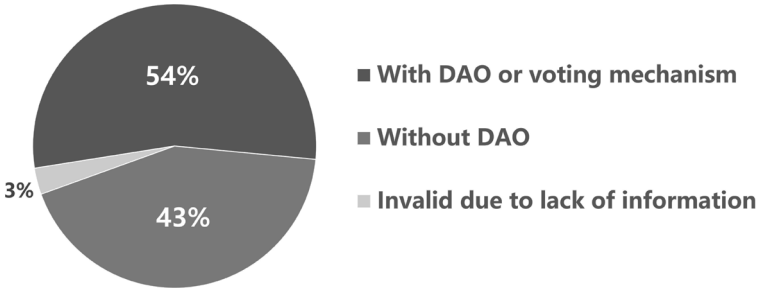

Figure 1. Breakdown of attacked DeFi projects based on the presence of DAOs or voting mechanisms

2. Systematizing DAO Involvement in DeFi Attacks

In DeFi, DAOs shape the dynamics of community-driven governance mechanisms and protocols. The governance vote is indeed the overt function of DAOs, as it permits participants to propose, discuss, and implement changes; however, the scope of DAOs extends beyond governance. They inherently encapsulate functions related to the management, organization, and security of DeFi platforms, rendering them pivotal in sustaining the platform's integrity and operational flow.

This Section delineates the involvement of DAOs in DeFi attacks, with a focus on their roles and responses either before, during, or after the attack, providing a systematic analysis on how the characteristics and functionality of DAOs are intertwined with the attack vectors and mitigation measures of DeFi platforms. A nuanced understanding of DAO participation is indispensable, as it sheds light on the implications of their decisions and interventions on the security and resilience of DeFi ecosystems.

We selected the six most recently attacked projects within the data set that had a DAO governance system, which are:

1. Yearn Finance[51]
2. Beanstalk Farms[52]

[51] YearnFinance, https://yearn.finance (25.08.2023).
[52] Beanstalk Farm, https://beanstalk.farm (25.08.2023).

3. Badger-DAO[53]
4. Bancor DAO[54]
5. Value DeFi[55]
6. PiDAO[56].

For each project, we visited its corresponding governance page, looked at all proposal themes from the inception of the DAO organization to March 2023, and summarized and organized these themes.

Organizational Level
Personnel Management Governance Mechanism Updates Treasury Pool Management
Project Level
Modifying Protocol Parameters Version Updates
Community Level
Event Organization Inter-project Collaboration

Table 1: Types of Proposals in DAOs

We have summarized the recurring proposal themes in DAOs into three levels: Organization Level, Project Level, and Community Level (see Table 1).

The Organization Level refers to adjustments in the governance mechanisms and personnel structure of the DAO organization itself. For example, Yearn Finance's YIP-61[57] and YIP-62[58] proposals aim to address governance enhancements within the DAO, while BeanStalk Farms Proposal BFP-65[59] focuses on making hiring decisions and is thus concerned with personnel management. The Project Level primarily involves the management of protocol parameters

[53] Badger DAO, https://badger.com (25.08.2023).
[54] BancorDAO, https://forum.badger.finance (25.08.2023).
[55] ValueDeFi, https://valuedefi.io (25.08.2023).
[56] PiDAO, https://www.pidao.finance (25.08.2023).
[57] YearnFinance, YIP-61: Governance 2.0 – Proposals, https://gov.yearn.fi/t/yip-61-governance-2-0/10460 (25.08.2023).
[58] YearnFinance, YIP 62 Contribute to the nomic foundation, https://gov.yearn.fi/t/yip-62-change-two-multisig-signers/10758 (25.08.2023).
[59] Beanstalk Farm, Proposal: BFP-65: Hire Beasley and Pay Retroactively (snapshot.org), https://snapshot.org/#/beanstalkfarms.eth/proposal/0xe8564cb73e098193fcc6470a1216a7192b9edce093422864f48e1ffc2b01f78a (25.08.2023).

and version updates, which are essential for the smooth operation of the DeFi protocol. The Community Level involves collaboration and communication between different protocols, such as Bancor DAO's whitelist updates,[60] as well as the organization of activities within the user community, as seen in BancorDAO's BIP 34.[61]

When confronting attack incidents, the resolutions put forth by DAOs in the form of e.g., emergency responses and post-incident rectifications, may focus on any of the proposal levels, from Organizational, to Project and Community Levels.

Proposals emerging at the Community Level are chiefly characterized by user compensation and the institution or allocation of White Hat bounties. BadgerDAO, for example, created an ambitious restitution plan.[62] In contrast, the proposals at the Project Level are designed to mend and enhance the protocol coding subsequent to an attack. For instance, BeanStalk initiated a proposal for a thorough re-audit of its smart contracts.[63]

A hybrid Community and Organizational level proposal took place after Inverse Finance suffered an attack in April 2022. A proposal was put to the vote to form a risk working group.[64] Shortly after the execution of this proposal, another proposal was put to the vote to fully compensate users affected by the April attack.[65]

These varied responses show the adaptive nature of DAOs in steering through crises and in assuring the sustained progression of the project, thereby accentuating their resilient attributes.

---

[60] See BancorDAO, https://gov.bancor.network/t/proposal-to-determine-whitelisting-status-of-sbtc-on-bancor-v3/3680, see also https://vote.bancor.network/#/proposal/0xf68058a221c25f02c1438680b9c9174176ed4c472113bb869ac30139c1191327 (25.08.2023).

[61] BancorDAO, BIP 34: Meme Competition for WenDIGG – BIP, Badger Improvement Proposals, https://forum.badger.finance/t/bip-34-meme-competition-for-wendigg/2728 (25.08.2023).

[62] See *Thurman*, After $130M Hack, Badger's Restitution Plan Tests Limits of DAO Governance, Coindesk 2021, https://www.coindesk.com/tech/2021/12/16/after-130m-hack-badgers-restitution-plan-tests-limits-of-dao-governance/ (25.08.2023).

[63] See BFP-66: Hire Halborn to Perform Audit, April 22, 2022, https://snapshot.org/#/beanstalkfarms.eth/proposal/0x54fad9c756daa38bb4bafadbee2cea6cb98f380fe2d6a62fdf723d0b15430d42 (25.08.2023). The Beanstalk DAO also wanted to strengthen the governance structure by switching to a community-run multisig wallet custodied by nine Beanstalk community members until a more resilient governance mechanism was developed, audited and implemented. See Brandy Betz, Beanstalk Stablecoin Protocol "Barn Raise" aims to restore $77M in lost funds, Coindesk 2022, https://www.coindesk.com/business/2022/06/02/beanstalk-stablecoin-protocol-barn-raise-aims-to-restore-77m-in-lost-funds/ (25.08.2023).

[64] See Inverse Finance, Proposal To Form a Risk Working Group, 2022, https://www.inverse.finance/governance/proposals/mills/22; see also https://forum.inverse.finance/t/proposal-to-form-a-risk-working-group/119/1 (25.08.2023).

[65] See Inverse Finance, Proposed Make-Good For Users Affected by April 2, 2022 Price Manipulation Incident, 2022 https://www.inverse.finance/governance/proposals/mills/28 (25.08.2023).

Table 2 beneath shows the different forms of involvement throughout distinct phases of an attack, each illustrated with pertinent incidents.

Category	Time	DAO's Role	Example
DeFi Attack Response Mechanism	Before an Attack	Preventive measures	Fei FIP82[66]
	During an Attack	Emergency DAOs	Curve Emergency DAO[67]
	After an Attack	Rescue Plans, Future Risk Proofing	InverseFinance Proposal 28[68]
DAO Attack	N/A	DAO as Target	Beanstalk BIP18/19[69]

Table 2: Involvement of Decentralized Autonomous Organizations (DAOs) in DeFi Attacks

This section analyzes how DAOs engage with DeFi security incidents, exploring their strategies to impact, mitigate, or resolve breaches. It highlights DAOs' critical roles in shaping security frameworks within the DeFi ecosystem.

a) Before an Attack

DAOs within DeFi platforms allow for a collective approach towards risk management and security. DAOs, as part of their governance functionality, regularly propose Improvement Proposals (IPs) to preventively address potential security breaches and bolster the platform's defenses. These IPs are pivotal as they act as a collective resolution mechanism that aims to identify and mitigate risks related to security vulnerabilities, thus serving as an integral component in safeguarding the DeFi ecosystem from prospective attacks.

In our case studies, the emphasis on IPs is not just tangential; rather, it holds significance in fortifying platforms through diverse strategies such as establishing Bug Bounty programs, procuring services of audit firms, and refining governance structures. These Improvement Proposals are strategic initiatives that exemplify the proactive stance of DAOs in enhancing the resilience and security robustness of DeFi platforms.

[66] Fei, FIP-82: Governance Enhancements, https://snapshot.fei.money/#/proposal/0x463fd1be98d9e86c83eb845ca7e2a5555387e3c86ca0b756aada17a11df87f2b (25.08.2023).

[67] Curve Emergency DAO, https://dao.curve.fi/emergencymembers (25.08.2023).

[68] See Inverse Finance Governance Proposals, https://www.inverse.finance/governance/proposals (25.08.2023).

[69] BIP18: Beanstalk Exploit – A Simplified Post-Mortem Analysis, https://medium.com/coinmonks/beanstalk-exploit-a-simplified-post-mortem-analysis-92e6cdb17ace (25.08.2023).

A notable example is the Fei Protocol's "Governance Enhancement" initiative, proposed on March 9, 2022.[70] This initiative was not a simple amendment; it represented a paradigmatic shift aiming to overhaul the existing Optimistic Approval process by adopting a Council approach. In essence, the proposition involved the establishment of a Tribal Council entrusted with proposing and approving governance actions. This alteration was not trivial; it was designed to mitigate prevalent issues such as voter apathy, lack of community context, and barriers to participation like gas fees by ensuring a streamlined and inclusive governance process. The significance of shifting to a Council approach composed of Tribe DAO community members lies in its ability to provide a structured, organized, and transparent governance model. Unlike non-DAO DeFi or traditional financial (TradFi) protocols, which often are centralized and lack community-driven governance mechanisms, the Tribe DAO community Council approach enables a collective, consensus-driven governance model. This is instrumental in addressing and resolving potential discrepancies, conflicts, and risks, allowing for a more agile and responsive decision-making process. In the Tribal Council model, a collective body has the responsibility to thoroughly deliberate upon, scrutinize, and assess the proposed actions, ensuring that every decision is well-informed, balanced, and reflective of the community's interests and needs. This approach follows the Liquid Representative Democracy model, which aims to be more democratic and inclusive, allowing for a diverse range of perspectives and inputs to be considered.

Regrettably, a conspicuous absence of comprehensive emergency plans was observed across the studied projects. This lack of preemptive planning to address potential losses and impacts on the project's ecosystem due to hacker attacks underscores a critical vulnerability. It highlights the necessity for DAOs to not only concentrate on enhancing governance structures but also to develop robust contingency plans to effectively navigate and mitigate the repercussions of unanticipated security breaches.

The initiation of Improvement Proposals by DAOs and the shift towards more structured governance models, like the Tribal Council approach, signify the proactive and strategic efforts made within the DeFi sector to curb potential threats and vulnerabilities. However, the general lack of emergency plans reveals a critical gap that needs careful attention and calls for a holistic approach to security and risk management that combines proactive risk mitigation with strategic response mechanisms.

---

[70] Fei, FIP-82: Governance Enhancements, https://snapshot.fei.money/#/proposal/0x463fd1be98d9e86c83eb845ca7e2a5555387e3c86ca0b756aada17a11df87f2b (25.08.2023).

b) During an Attack

DAOs facilitate community-driven governance within DeFi ecosystems. While their decentralized nature offers an avenue for collective decision-making, the challenges associated with this decentralization become palpable during security breaches or attacks, where the urgency and immediacy of responses are imperative to mitigate losses. Thus, an important aspect to examine is how DAOs, traditionally reliant on community consensus, reconcile the need for swift actions during emergencies with the principles of decentralized governance.

An example that illustrates such a reconciliation is Curve's Emergency DAO.[71] Structured as a specialized arm within the project's overall DAO, the Emergency DAO is configured with nine members who are democratically elected by CurveDAO. This entity is vested with unparalleled authority during crisis scenarios where the risk of losing funds is imminent. In such instances, the Emergency DAO holds the prerogative to suspend all project functionalities, sparing only the withdrawal feature.

The embodiment of such an emergency mechanism is emblematic of a strategic resolution to counterbalance the inherent limitations of DAOs in terms of response agility. Given that DAOs necessitate public voting for decision-making, this often becomes a bottleneck during crisis scenarios, impeding the immediate execution of countermeasures. Curve's Emergency DAO, by circumventing the prolonged deliberations associated with public voting, ensures a timely intervention, thereby mitigating the potential escalations of the attack's impacts.

However, the inception of such an emergency mechanism also beckons a slew of controversies and debates surrounding the ethos of decentralization intrinsic to DAOs. The empowerment of a select group with elevated privileges during emergencies sparks discussions on the paradox of centralization within decentralized entities. This duality brings forth crucial questions about the sanctity of decentralization in DeFi projects and opens dialogues on the extent to which concessions on decentralization are justifiable in the pursuit of security and operational stability.

This mechanism reflects a tradeoff between decentralized governance and the necessity for instantaneous decisions during crises. Addressing this point, it is imperative to understand that the incorporation of mechanisms like the Emergency DAO doesn't inherently negate the principles of decentralization. Rather, it acts as a pragmatic adaptation to the operational exigencies that demand immediate resolutions.

In essence, the deployment of such mechanisms is an acknowledgment of the varying demands of different operational scenarios within DeFi platforms. It is a nuanced approach aimed at preserving the foundational ethos of decentraliza-

[71] Curve Emergency DAO, https://dao.curve.fi/emergencymembers (25.08.2023).

tion while ensuring the adaptability and responsiveness of the system in the face of unforeseen security breaches. The quest here is about fostering a harmonious coexistence between decentralization and the imperative for swift, decisive actions in critical situations.

The implementation of emergency response mechanisms like Curve's Emergency DAO encapsulates the ongoing endeavors to refine and optimize the governance structures within DeFi ecosystems, addressing the intrinsic tensions between decentralized governance and the necessity for quick, effective responses during security incidents. This dialectic between centralization and decentralization in DeFi DAO governance models is reflective of their pursuit to reconcile operational efficiency with foundational principles.

c) After an Attack

The aftermath of an attack on DeFi platforms involves a meticulous response management to contain and rectify the damages incurred. It is within this critical juncture that DAOs play an important role in orchestrating comprehensive response strategies. These strategies span across multiple facets including devising immediate rescue plans, formulating equitable user compensation frameworks, implementing security rectifications, and conceptualizing long-term enhancements for bolstering the project's security. All these elements are integral to re-establishing operational normalcy and rebuilding user trust post-attack.

Illustrative of such post-attack management is the approach adopted by Inverse Finance following a price manipulation attack on its oracle.[72] The community-led governance system was swift in proposing a series of counteractive measures aimed at restoring stability and mitigating further damages. On April 3rd, 2022, Inverse Finance's governance community introduced Proposal 19, suggesting a substantial reduction of INV rewards for several assets to re-establish DOLA DEX liquidity, followed by a sequence of additional proposals targeting different aspects of the platform's recovery and user compensation.[73]

Proposal 19 articulated a specific strategy focusing on restoring liquidity by altering the reward dynamics for various assets, showcasing a precise and targeted approach to liquidity management post-attack. Subsequently, Proposal 20, introduced on April 4th, was aimed at curtailing the burgeoning bad debt by temporarily setting the rates for several assets to zero, a necessary measure to arrest the daily increment of $20,000 in bad debt.[74] The unanimous approval of

[72] Inverse Finance, https://www.inverse.finance (25.08.2023).

[73] See Inverse Finance, Proposal 19, https://www.inverse.finance/governance/proposals/mills/19 (25.08.2023).

[74] See Inverse Finance, Proposal 20, https://www.inverse.finance/governance/proposals/mills/20 (25.08.2023).

this proposal underscores the community's consensus on the urgency and importance of such immediate interventions.

Beyond immediate interventions, Inverse Finance also emphasized addressing the impacts on its user base. Proposal 28, unveiled on May 8th, delineated a comprehensive compensation plan, signifying the DAO's commitment to uphold user interests and ensure equitable redressal for those affected by the attack.[75] This proposal manifested the holistic approach of Inverse Finance, combining immediate mitigative actions with long-term user-centric solutions, portraying a balanced and responsible post-attack management strategy.

Moreover, the series of proposals tabled by Inverse Finance also highlighted the importance of fortifying the project's security framework to preclude future incidents. This included considerations for conducting fresh audits and establishing more robust bug bounty programs, reflecting a forward-looking approach that seeks to intertwine immediate recovery with sustained resilience.[76] The integration of such measures is indicative of the DAO's resolve to continually refine and enhance the platform's security posture, emphasizing a progressive and proactive stance in aftermath management.

The involvement of DAOs in the aftermath of an attack can serve as the nexus for initiating multifaceted response strategies based on the communities' wishes. Inverse Finance exemplifies the diverse and comprehensive approach necessitated post-attack, balancing immediate interventions with user compensation and long-term security enhancements. The unanimous and swift adoption of multiple proposals shows the collective resolve of the community to restore operational stability and fortify the platform against future vulnerabilities. It underscores the inherent strength of decentralized governance in merging diverse insights to forge cohesive recovery and enhancement pathways, essential for sustaining trust in the evolving DeFi landscape.

d) Special Case of DAO Attacks

While DAOs play an important role in defining and implementing the governance structures of various DeFi platforms, their inherent design mechanisms are not immune to exploitation. The DAOs' public and transparent nature, coupled with the possibility of flaws in their governance structures or smart contract implementations, can render them susceptible to malevolent attacks. Intruders, exploiting price manipulations of governance tokens or leveraging logical vulnerabilities, can ingeniously pass and execute malicious proposals, potentially

[75] See Inverse Finance, Proposal 28, https://www.inverse.finance/governance/proposals/mills/28 (25.08.2023).

[76] See e.g., Inverse Finance, Proposal 32 on additional funding for security related services, https://www.inverse.finance/governance/proposals/mills/32 (25.08.2023).

leading to severe financial ramifications and undermining the treasury governed by the DAO.

A glaring instance of such vulnerabilities being exploited occurred in the attack on the yield farming protocol, Beanstalk Farms, in April 2022.[77] The attacker manipulated the protocol's democratic governance mechanism by creating two deceptive proposals, BIP18 and BIP19, under the guise of philanthropic intents. BIP18, disguised with the humanitarian cause of "donating to Ukraine," was a mere empty shell, harboring no content or real intention to donate. In contrast, BIP19 was a more intricate deceptive proposal, designed with a contract that benefited the attacker while maintaining the façade of contributing to Ukraine. This incident unraveled the potential of exploiting the DAO's transparent and open mechanism for malevolent gains and emphasized the need for meticulous scrutiny and verification of proposals.

Similarly, the incident involving Tornado Cash[78] underscored the critical vulnerabilities in DAO governance, where a malicious actor, through a meticulously crafted governance proposal, seized control over both the DAO and the protocol.[79] This unscrupulous control enabled the malefactor to withdraw tokens from the governance contract and even launder money through the protocol.[80] Although control was subsequently relinquished, the exploitation highlighted some methods by which attackers could manipulate decentralized governance mechanisms to their advantage.

These incidents serve as stark reminders of the potential exploitations that can permeate through DAOs. The subversion of governance mechanisms by leveraging manipulative and deceptive proposals emphasizes the need for robust validation mechanisms and heightened vigilance within the community. The adaptability and resilience of DAOs are contingent on the continuous refinement of their governance structures, aiming to strike a balance between openness and security. The assimilation of multi-layered validation processes, rigorous auditing of smart contracts, and the integration of advanced security protocols are imperative to bolster the resilience of DAOs. Enhanced community awareness and participation in governance mechanisms can act as additional safeguards against deceptive proposals, ensuring the integrity and credibility of

---

[77] BIP18: Beanstalk Exploit – A Simplified Post-Mortem Analysis, https://medium.com/coinmonks/beanstalk-exploit-a-simplified-post-mortem-analysis-92e6cdb17ace (25.08.2023).

[78] Tornado Cash has reportedly been used by North Korean hacking group Lazarus Group to launder at least 450 million USD. The mixing service has been sanctioned by OFAC and some of its smart contract addresses were put on the OFAC list.

[79] See *Malwa*, Tornado Cash DAO Attacker Starts to Move Ether, TORN Tokens, Coindesk 2023, https://www.coindesk.com/tech/2023/05/25/tornado-cash-dao-attacker-starts-to-move-ether-torn-tokens/ (25.08.2023).

[80] See *Mutunkei*, Hacker drops control over Tornado Cash as they use it to wash stolen funds, Crypto News 2023, https://crypto.news/hacker-drops-control-over-tornado-cash-as-they-use-it-to-wash-stolen-funds (20.06.2023)

the decentralized governance model. These combined efforts will be instrumental in preserving the ethos of decentralization while mitigating the risks associated with potential exploitations and vulnerabilities in DAOs.

IV. Conclusion

Our research aimed to investigate the roles of DAOs in the Decentralized Finance ecosystem, focusing on their roles in an illustrative data set of attacks that plagued the ecosystem and DAOs' responses to such exploits. DeFi, a disruptive innovation in the financial world, reached considerable growth with a Total Value Locked (TVL) peaking at around 180 billion USD in 2022, despite suffering a series of significant setbacks, including relentless hacking incidents and other financial risks.

We find that of 169 attacked DeFi projects in our data set, 92 had a DAO or voting mechanism, highlighting the critical presence and influence of DAOs in the DeFi space. DAOs are not just a concept but are practical components in the management and governance of DeFi projects. Our empirical analysis revealed vulnerabilities both in the direct functionalities of DeFi services and the governance systems managed by DAOs. Attackers exploited these vulnerabilities to manipulate outcomes or drain funds, proving that the underlying smart contract and governance mechanisms are critical points of concern.

Bad actors often exploit governance systems by manipulating votes to pass favorable decisions, revealing the need for stronger, more secure governance structures that can resist malicious actors and ensure the integrity of collective decision-making processes. DAOs, despite being susceptible to attacks, have actively worked on enforcing rigorous code audits and implementing robust governance mechanisms. They are the frontline defense in preventing and mitigating various forms of attacks and are pivotal in establishing responsive frameworks for detected vulnerabilities and breaches.

The interrelation between DeFi and DAOs is intricate, with DAOs shaping the economic landscape of decentralized finance. Understanding this interplay gives valuable insights into the stability, governance, and future developments of the DeFi ecosystem.

Our findings underscore the importance of strong, resilient DAOs for the security, stability, and growth of the DeFi ecosystem. DAOs must focus on enhancing their governance structures and decision-making processes to counteract attacks effectively. Rigorous and frequent code audits, robust governance models, and proactive vulnerability detection and management are crucial to maintaining integrity and user trust.

Enhanced security measures and continuous improvements in governance systems will not only prevent the exploitation of vulnerabilities but will also

ensure the sustainable development of DeFi projects, helping them to realize their full potential in revolutionizing the financial sector.

Furthermore, the evolving nature of DAOs and their increasing economic influence necessitate further research. Subsequent studies should address the regulatory challenges surrounding DeFi and DAOs, aiming to create a more resilient and inclusive financial ecosystem.

In conclusion, DAOs, with their decentralized and transparent nature, are integral components in the realization of the promises of DeFi, acting as the guardians of decentralization and user participation. While they are vulnerable to attacks and exploitations, their continuous improvement and adaptation are essential in overcoming these challenges and ensuring the development of a secure and stable DeFi ecosystem.