A Comprehensive Study of Governance Issues in Decentralized Finance Applications

WEI MA, Nanyang Technological University, Singapore, Singapore
CHENGUANG ZHU, The University of Texas at Austin, Austin, Texas, USA
YE LIU, Nanyang Technological University, Singapore, Singapore
XIAOFEI XIE, School of Computing and Information Systems, Singapore Management University, Singapore, Singapore
YI LI, Nanyang Technological University, Singapore, Singapore

Decentralized Finance (DeFi) is a prominent application of smart contracts, representing a novel financial paradigm in contrast to centralized finance. While DeFi applications are rapidly emerging on mainstream blockchain platforms, their quality varies greatly, presenting numerous challenges, particularly in terms of their governance mechanisms. In this article, we present a comprehensive study of governance issues in DeFi applications. Initially, we collected 3,165 academic papers and numerous industry reports. After thorough screening, we selected 44 academic papers and 11 industry reports for detailed analysis. Drawing upon insights from industry reports and academic research articles, we develop a taxonomy to categorize these governance issues. We collect and build a dataset of 4,446 audit reports from 17 Web3 security companies, categorizing their governance issues according to our constructed taxonomy. We conducted a thorough analysis of governance issues and identified vulnerabilities in the governance design and implementation, e.g., voting sybil attack and proposal front-running. Our statistical analysis indicates that a significant portion (35.48%) of governance-related issues is classified as severe. Within these, ownership-related problems constitute the largest share (65.38%). Despite DeFi governance being essential for the long-term success of DeFi projects, our data shows that both auditors and development teams have not fully grasped its significance. Based on audit reports, we also analyzed common vulnerabilities and issues in the governance domain. Our research identifies two primary categories of DeFi governance issues: technology-centric and human-centric. Technology-centric issues can be addressed through technology updates and iterations, whereas human-centric issues are influenced not only by the development team's technical skills but also by their understanding of DeFi governance. Data analysis reveals that design and implementation issues are frequently overlooked; although not directly associated with vulnerabilities, these issues can impact the equitable distribution of project benefits. Furthermore, our analysis of 104 projects' tokenomics configurations, including 15 collected from DeFi platforms, uncovered 27 inconsistent configurations, with only two projects exhibiting no issues. This suggests that such issues are relatively common. We therefore advise project teams to ensure consistency between their tokenomics design and the actual code. Our study culminates in providing several key practical implications for various DeFi

This work was supported by the Nanyang Technological University Centre for Computational Technologies in Finance (NTU-CCTF). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of NTU-CCTF.
Authors' Contact Information: Wei Ma, Nanyang Technological University, Singapore, Singapore; e-mail: ma_wei@ntu.edu.sg; Chenguang Zhu, The University of Texas at Austin, Austin, Texas, USA; e-mail: cgzhu@utexas.edu; Ye Liu (corresponding author), Nanyang Technological University, Singapore, Singapore; e-mail: yeliu@smu.edu.sg; Xiaofei Xie, School of Computing and Information Systems, Singapore Management University, Singapore, Singapore; e-mail: xiaofei.xfxie@gmail.com; Yi Li, Nanyang Technological University, Singapore, Singapore; e-mail: yi_li@ntu.edu.sg.

ACM 1557-7392/2025/8-ART208
https://doi.org/10.1145/3717062

stakeholders, including developers, users, researchers, and regulators, aiming to deepen the understanding of DeFi governance issues and contribute to the robust growth of DeFi systems.

CCS Concepts: • **Software and its engineering** → *Software creation and management*; • **Security and privacy** → **Trust frameworks**; **Security requirements**; **Logic and verification**; • **Computer systems organization** → **Distributed architectures**; • **Social and professional topics** → **Financial crime**; **Social engineering attacks**; • **Information systems** → **Decision support systems**; **Enterprise information systems**;

Additional Key Words and Phrases: Decentralized Finance (DeFi), DeFi Security, DeFi Governance, Governance Tokenomics, DeFi Economic Model Security, Software Governance, Blockchain Governance

ACM Reference format:
Wei Ma, Chenguang Zhu, Ye Liu, Xiaofei Xie, and Yi Li. 2025. A Comprehensive Study of Governance Issues in Decentralized Finance Applications. *ACM Trans. Softw. Eng. Methodol.* 34, 7, Article 208 (August 2025), 31 pages.
https://doi.org/10.1145/3717062

1 Introduction

Decentralized Finance (DeFi) [122] has rapidly emerged as a transformative force in the financial world, challenging traditional paradigms with its blockchain-based, intermediary-free model. The appeal of DeFi lies in its foundational principles: *transparency*, *immutability*, and *openness*, coupled with the *anonymity* it offers to users. At its core, DeFi contrasts starkly with centralized finance by empowering users with direct control over their transactions. This autonomy, facilitated by blockchain technology and smart contracts, marks a significant shift towards a more accessible and inclusive financial ecosystem. DeFi has sparked innovation, which is evident in its expanding landscape of services like lending, trading, and asset management. A testament to its growing influence is the substantial capital influx, with billions of dollars currently locked in various DeFi protocols. A notable example is Uniswap, a decentralized cryptocurrency exchange boasting over 30 million active users and a **Total Value Locked (TVL)** of approximately $48.65 billion [106]. However, in addition to its immense opportunities, DeFi also faces a myriad of challenges [76, 119], such as money laundering [68].

One of the most important challenges in the DeFi space is governance [11, 18, 21, 42, 66]. Governance plays a central role in DeFi applications and serves as the foundation of the DeFi ecosystem. Effective governance in DeFi is vital for collective decision-making, management of business models, and the distribution of rewards within the ecosystem. However, DeFi governance faces many challenges. First, some DeFi applications, such as Uniswap V1 [114], operate without specific governance mechanisms, resulting in difficulties in maintaining and updating these applications. This issue was addressed in its later versions, namely V2 and V3 [115]. Second, vulnerable governance mechanisms expose an entire DeFi system to malicious attacks which could result in massive financial losses. Examples include the Beanstalk governance attack [97] and the Build Finance **Decentralized Autonomous Organization (DAO)** incident [38], which demonstrate vulnerabilities not just in code, but also in governance designs. Third, another serious issue that may harm DeFi users and investors is opaque or fraudulent governance strategies. It is a common practice for DeFi development teams to publish whitepapers about their projects in advance, which document the particular governance mechanisms to be adopted. Nonetheless, there are instances where the actual implementations deviate from these plans. For example, CodeInc developers can issue tokens in excess of their declared amount and also have the ability to destroy them to gain additional benefits, all without making any payment [105]. These discrepancies, while often subtle,

can have a profound impact on the healthy growth of DeFi systems. They raise questions regarding transparency and ethical practices in DeFi governance, potentially resulting in diminished public trust. A notable instance of such is the phenomenon of rug pulls [102], where certain DeFi teams (e.g., ARBIX FINANCE [94]) exploit hidden governance loopholes to rapidly deplete funds from the pool.

To mitigate these problems, robust and transparent governance mechanisms are essential. They play a vital role in establishing trust among users and investors, which is key to encouraging long-term investment and ensuring the sustainable development of the ecosystem. However, there is a noticeable research gap in this area, particularly regarding the standardization of governance practices. To address this, our article embarks on a thorough examination of governance issues in DeFi applications, mainly by analyzing audit reports of DeFi applications. Specifically, we delve into both academic research papers and high-quality industry reports to develop a comprehensive understanding of the DeFi governance taxonomy. This taxonomy categorizes governance issues as well as assesses the issues based on their nature and severity, offering a detailed perspective on the present challenges in DeFi governance. We observe that about 38.11% of the high-severity issues identified pertain to governance, which is substantial.

Building on this taxonomy, our analysis of audit reports of various DeFi applications reveals several key insights. While previous research has highlighted the importance and challenges of DeFi governance, it has only focused on a small number of DeFi projects as case studies [15, 49, 80, 85]. In contrast, we gathered 4,446 published audit reports documenting detailed analyses conducted by domain experts, providing a broader view of the problem based on more reliable data. To highlight a few interesting findings not mentioned in previous studies, we found that (1) ownership issues (e.g., lack of owner identity verification and incorrect owner rights) account for most of the severe governance issues, (2) the severity of many governance issues remains uncertain, which indicates the difficulty of issue triage and the need for better guidelines, and (3) governance issues do not receive adequate attention from DeFi project teams, likely due to the lack of strong incentives. We revealed that the main governance issues center around the ownership structures and incentive schemes. For example, a recurring concern is the degree of centralization, especially in areas such as token distribution and protocol management, where a high degree of centralization may endanger the application's credibility. Critical privileges such as changing fee rates or transferring ownership are usually not expected to be centrally controlled. Despite the high proportion of governance-related issues and their potential to trigger systemic risks, we found that these issues have not received enough attention from auditors and project teams. Many governance issues are marked as pending decisions, and high-risk governance issues are not fixed at a higher rate either. In addition, our analysis also revealed that some serious governance issues in DeFi are rooted at the mismatch between the governance design in whitepapers and their actual implementations. For instance, there are cases [35] where DeFi owners reserve the right to mint any number of tokens with hidden mint functions, which is never specified in the published governance design. These discrepancies indicate potential loopholes which may be exploited to bypass intended governance mechanisms. To investigate the DeFi design-implementation issue, we collected 15 real-world DeFi projects and found that only two of them have the consistent tokenomics configurations between the design and the implementation.

Building on our data analysis, our findings offer several significant insights for multiple DeFi stakeholders. For researchers in software engineering, there is a need to study and develop governance frameworks and theories [78, 79, 109] for DeFi, as well as methods for validating these governance systems [32]. As an important application of blockchain, DeFi applications should have a standardized governance system development process. Unlike centralized software systems, the lifecycle management of DeFi diverges from traditional software approaches [77]. In the traditional

software development, user feedback drives continuous modifications and improvements [41]. However, DeFi projects deviate from this model; their evolution is governed by their distinct governance systems. Stakeholders in DeFi should possess the authority to guide its evolution. Hence, it is imperative for software engineers to address challenges within DeFi governance and contribute towards establishing a comprehensive framework for its governance. For developers, it is essential to be aware of governance issues and to design transparent, ethical, and robust governance systems [77]. One key recommendation is to address DeFi governance issues at the design level, which are often overlooked by the developers. To effectively reduce governance risks, it is crucial for project teams to incorporate governance considerations from the earliest stages of the project. This includes defining the scope of governance, clarifying ownership rights and user rights, and establishing processes for monitoring and addressing potential governance issues. Furthermore, DeFi designers should proactively consider and prevent potential attacks, such as key leaks and front-running of governance proposals. DeFi teams should also consider whether the initial allocation of governance tokens is reasonable. This is to prevent the whale account from attacking the project after it obtains a large number of governance tokens. Besides ensuring a good design at the architectural level, DeFi teams must pay special attention during the implementation process to the protection mechanisms of governance-related functions. This involves ensuring the accuracy of caller authentication and conducting thorough error checks and vulnerability scans to mitigate risks. For users and investors, they should investigate the governance structure of DeFi projects [95], such as the project ownership, user privileges, and token power distribution. For regulators, it is crucial to both oversee governance structures and examine whitepapers of DeFi projects [47, 84], as they are key to identify fraudulent activities.

These insights are instrumental in understanding and addressing the governance challenges within the DeFi sector, such as how to design and manage the ownership and voting mechanism. We aim to contribute to the development of robust and secure DeFi governance frameworks, foster a better understanding of governance issues, promote best practices, and facilitate the sustainable growth of the DeFi ecosystem. In summary, we make the following contributions:

— *A Taxonomy of DeFi Governance*: We created a detailed taxonomy for DeFi governance based on an extensive review of academic literature and industry reports. This taxonomy offers a structured approach to understanding and categorizing governance challenges in DeFi.
— *A Comprehensive Analysis of DeFi Governance Issues*: Our article provides a thorough examination of governance issues in DeFi applications. Through our analysis of the audit reports using our governance taxonomy, we shed light on the present situations, challenges, and unaddressed needs in DeFi governance. Our research highlights important issues that urgently need to be addressed in DeFi governance-related research.
— *Recommendations for DeFi Governance in Practice*: Our research provides valuable guidance for DeFi governance practices. Researchers should focus on developing DeFi governance frameworks, and establishing standards and verification methods. Developers need to understand DeFi governance concepts deeply, recognize potential risks, and formulate corresponding strategies during the design phase. Users and investors should thoroughly assess the governance of DeFi projects, including their defence measures against common attacks and whether there are any privileged functions. Regulatory bodies should consider the governance of DeFi projects as a key criterion in project evaluation.

The article is organized as follows. Section 2 introduces three **Research Questions (RQs)** under investigation, delineates our methodology, and details our data sources. Section 3 presents the results corresponding to each RQ and discusses the implications of our study. Related studies to our work are reviewed in Section 4. Finally, Section 5 identifies potential threats and the corresponding

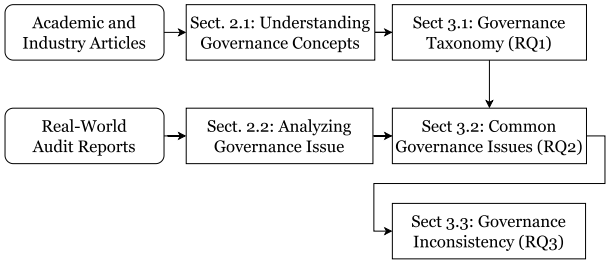


Fig. 1. Overview of our study methodology.

mitigation strategies used. Our concluding remarks and a summary of the work are encapsulated in Section 6.

2 Methodology

Figure 1 depicts the process that illustrates our analytical methodology and our three RQs in the different stages:

—RQ1: What governance taxonomy can we use to analyze the governance issue?
—RQ2: What are the common governance issues in DeFi applications?
—RQ3: How closely do DeFi developers follow governance designs in whitepapers during the development?

At the initial phase, we delve into the concept of DeFi governance as it is elucidated in academic literature and industry blogs. Our aim here is to develop a comprehensive governance taxonomy, a crucial framework that will underpin our entire analysis that guides us review the governance issues (RQ1). Moving forward, we collect and scrutinize audit reports, employing our newly established governance taxonomy to dissect and understand governance issues in DeFi applications (RQ2). A significant aspect of our study revolves around the role of DeFi development teams in designing and implementing governance mechanisms. We analyze the issues related to DeFi governance designs described in the whitepapers. Additionally, we build an assistant tool and analyze 15 real-world DeFi projects and find that only two of them faithfully implement the designs outlined in the whitepapers (RQ3).

The manual analysis in this study was led by one of the authors, who is also a senior Web3 security researcher, having over 3 years' experience in the Web3 security company. We employed a collaborative approach during the analysis process. All contributing authors established standards through discussion before the analysis began. After the preliminary review, the research team held regular meetings to discuss identified issues and refine the analysis, ensuring consensus on all key issues.

2.1 Understanding DeFi Governance Concepts

Governance, a pivotal concept in DeFi, lacks a universally accepted definition that encompasses its principles, scope, and role. This ambiguity poses a significant challenge in understanding and analyzing governance within DeFi. To address this crucial gap, we adopt the mapping study [89]. We aimed at establishing a comprehensive taxonomy of DeFi governance. This taxonomy is a classification system and a tool to dissect and categorize the multifaceted governance issues prevalent in DeFi applications. Through this endeavor, we aim to paint a clear picture of the current governance landscape in DeFi, highlighting key concerns and areas demanding further research attention.

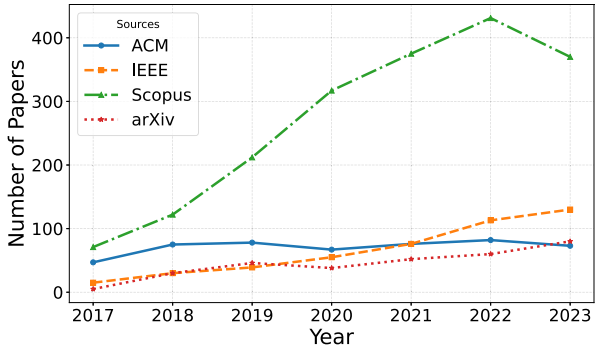


Fig. 2. Conference paper count by year (2017–2023).

We commenced our literature search with a systematic exploration of prominent databases, namely IEEE Xplore [7], ACM Digital Library [2], Scopus [8] and arXiv [3]. We first defined the keywords that are directly related to the domain we were going to study, "blockchain governance," "smart contract governance," and "DeFi governance." These predefined keywords were used to search the related articles. This initial phase yielded a substantial corpus of articles: 458 from IEEE Xplore, 498 from ACM Digital Library, 1,898 from Scopus, and 311 from arXiv between 2017 and 2023 as shown in Figure 2. It is evident that there is a growing emphasis on governance. Recently, researchers have studied how GPT4 can be used to analyze documents [80, 103]. To distill this vast collection, we also employed GPT4 as a query assistant, focusing specifically on the titles and abstracts to identify the 100 most relevant articles from each database, with an emphasis on governance in DeFi applications. We used the GPT Academic project[1] with 62.9k stars and uploaded the files that contain the title and abstracts to GPT4. If one file was too large, we splitted them to smaller ones and later we manually merged the results. Then, we instructed GPT4 to return the most related items using this prompt, "according to the title and abstract, please use the topic model to extract the top 100 items from the file that related to the topic 'Decentralization Finance Application Governance' in a concise way." Expanding our search horizon, we also utilized Google Scholar and Connected Papers [4], reviewing the first five pages of the search results to identify articles closely aligned with our research theme. We checked their titles and abstracts to see if they are related to DeFi and governance. To filter the collected papers, we have an inclusion principle that the articles must focus on studying the DeFi governance framework or claim to research key components of DeFi governance (governance mechanisms, tokenomics, governance security, and implementation). We also have an exclusion principle where we do not consider articles discussing the usage of blockchain or DeFi to manage real-world systems, such as using blockchain to govern a smart city. In the end, this comprehensive approach led to the selection of 44 academic articles.

In our quest for a holistic understanding of DeFi governance, we extended our exploration beyond academic literature to also cover industry perspectives. Recognizing the critical insights that Web3 entities offer, we expanded our dataset to encompass 11 blog articles about DeFi governance from leading companies [13] in this field, like OpenZeppelin. This inclusion of diverse, industry-specific perspectives ensures a more comprehensive understanding of DeFi governance. Notably, during searching articles, we discovered that several esteemed international organizations have published reports on decentralization finance from EUROFI [47], WIFPR [120], OECD [84], BIS [25], and Dutch Blockchain Coalition [43]. We used Google search engine and the aforementioned keywords to search for these reports. We considered only the international organization or the national

[1] https://github.com/binary-husky/gpt_academic

institute, and chose the results that are directly related to DeFi governance. This led us to include five such reports into our dataset, enriching our analysis with practical viewpoints. We used Google to collect industry blogs and organization reports, employing DeFi governance as a keyword search, and checked the first 10 pages. We have published the list of search results online [13].

As we strive to understand the specific aspects of governance emphasized in the literature, we find that the widely accepted definition of DeFi governance is still evolving [18, 19, 20, 40, 60, 66, 79, 88, 104, 120]. Capponi et al. [26] explore the DeFi ecosystem, analyzing its key components and emphasizing their operational mechanisms and governance structures. Key components identified in these studies include decision-making processes [15, 18, 40, 42, 52, 79, 99, 108], incentives for participation [18, 21, 60, 66], and issues related to ownership and decentralization [21, 98, 108]. A central aspect of governance in DeFi systems is the use of governance tokens [59], which often determine voting power in decision-making processes [18, 21, 60, 69, 108]. The distribution of these tokens and the mechanism by which they are used in governance, including both off-chain and on-chain methods [30, 40, 45, 48, 79, 121], are crucial aspects that shape the governance structure. Furthermore, participants in the governance process are often influenced by incentive models, which can include utility tokens, incentive models, and revenue models [18, 21, 33, 60, 66, 88] that are collectively called tokenomics.

An examination of governance from an industry perspective reveals notable congruences with academic viewpoints, especially in conceptualizing it as a rule-based framework for decision-making. While academic literature often delves into broad topics, such as the governance of foundational platforms like Ethereum, industry blogs [22–24, 29, 30, 44, 45, 81] tend to diverge, placing a greater emphasis on the practical aspects of DeFi governance at the application layer. This includes a focus on the technical details, design strategies, and monitoring mechanisms of smart contract governance. These industry discussions typically revolve around several key themes, such as determining the scope of governance, identifying stakeholders, exploring different governance models, and conducting comparative analyses of their pros and cons. For instance, the industries often discuss how governance mechanisms are integrated into the codebase, offering insights into real-world implementation challenges and successes. This practical orientation provides a complementary perspective to the theoretical frameworks discussed in academic circles. As a summary, the academy focuses on the nature of DeFi and its governance systems with these aspects: decision-making processes, incentive for participation, ownership, and decentralization, while the industry emphasizes the mechanisms of implementation and the scenarios of real-world applications with the following views, design strategies, monitoring mechanisms, and implementation choice.

2.2 Analyzing DeFi Governance in Audit Reports

Audit reports, as products of expert scrutiny, are invaluable for studying the complex issues and challenges in DeFi governance. These reports, rich in high-quality data, provide detailed insights into smart contract issues that are critical to understanding DeFi governance. To harness this wealth of information, we gathered audit reports from a diverse range of reputable online sources, available in formats such as PDF and HTML. This varied collection ensured a comprehensive data pool. Our analysis of these reports involved extracting and categorizing governance-related issues, thereby creating a detailed picture of the challenges and intricacies involved in DeFi governance.

2.2.1 Data Resource. To get the high-quality audit reports, we prioritized security companies known for their expertise and reliability, particularly focusing on Certik and OpenZeppelin, whose comprehensive reports are readily accessible on their Web sites. Recognizing that many security companies also publish their findings on GitHub, we employed a targeted search using the following keywords “audit,” “audit report,” and “smart contract audit” to gather more reports. To ensure the

Table 1. Commercial Security Company List as the Resource of Audit Reports

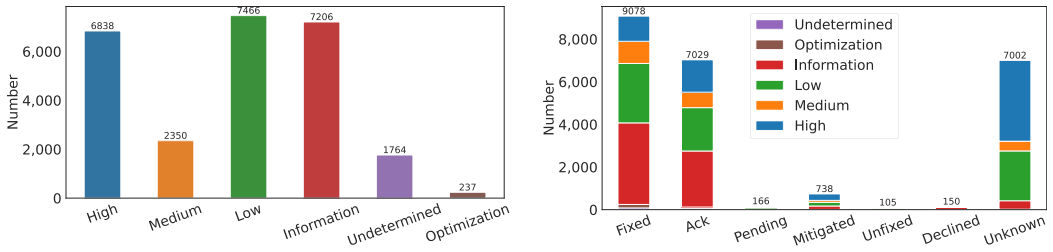
Company	Official Web site	#X Followers	Etherscan	#Reports	#Issues
Certik	https://www.certik.com	288,957	✓	1,133	12,461
Openzeppelin	https://www.openzeppelin.com	53,327	✓	92	1,133
Immune Bytes	https://www.immunebytes.com	738	✓	83	673
Oak Security	https://www.oaksecurity.io	1,544		92	950
Cyberscope	https://www.cyberscope.io	12,703		336	2,364
Coinscope	https://www.coinscope.co	15,851		184	1,124
Solidified	https://www.solidified.io	2,546	✓	142	289
HASHEX	https://hashex.org	10,472	✓	30	280
Zellic	https://www.zellic.io	6,676		28	143
QuillAudits	https://www.quillaudits.com	12,563	✓	85	512
CyStack	https://cystack.net	4,643	✓	11	48
TechRate	https://techrate.org	12,466	✓	1,745	3,049
Decentraland	https://decentraland.org	631,806		1	3
Chainsulting	https://chainsulting.de	39,894	✓	74	329
Somish	https://www.somish.com	349	✓	9	113
PeckShield	https://peckshield.com	76,204	✓	277	1,227
Quantstamp	https://quantstamp.com	79,148	✓	124	1,339
Total	-	-	-	4,446	26,037

credibility of these sources, we established a set of criteria: We examine an audit report only if the auditing company has over 1,000 X (formerly known as Twitter) followers or is recognized on the Etherscan directory of smart contract auditors [9]. The Web site [9] includes recognizable security companies, and audit reports from these companies have a higher chance of being good. We also use the tool FollowerAudit [5] to check if the X accounts are reliable. Table 1 lists 17 security companies, collectively contributing to a dataset of 4,446 audit reports.

2.2.2 Data Processing. An audit report contains the issues found by experts in one project, and we need to extract each issue. We implemented a PDF parser and an HTML parser to convert raw audit reports into text format. Furthermore, we remove invalid text characters and then parse these texts into JSON format according to the different audit sections, *title*, *severity*, *recommendation*, *status*, and *description* of each issue. The extraction leads to a total of 26,037 issues, as shown in the last column of Table 1. Our dataset is publicly available.[2] Figure 3(a) illustrates the severity distribution of all issues (notice some issues do not have status and severity records). The x-axis shows the different severity labels, such as "high" and "low." Among all the issues, 35.53% are labeled as *high* and *medium* by the auditing teams. Figure 3(b) shows the resolution status distribution of all issues. We color code the bars to also show the distribution of different severity levels for each resolution status. Except the ones classified as unknown, most of the high-severity issues are fixed and acknowledged. One interesting observation is that the high-severity labels account for the most unknown issues. Based on this result, we conclude that most of the raised issues have been fixed (37.41%) or acknowledged (28.96%) by the developers. However, acknowledgment may not always translate to issues being fixed. According to Figure 3(b), many high-severity issues remain unfixed even if they are acknowledged.

Next, we filter out non-governance issues with keywords extracted from the reviewed articles, and then group the remaining governance issues based on a governance taxonomy. To build the governance taxonomy, we manually reviewed the collected literature to identify keywords and

[2] https://doi.org/10.5281/zenodo.13825219



(a) Distribution of Issue Severity (b) Distribution of Issue Status

Fig. 3. Issue severity and issue status in our dataset.

precisely pinpoint the relevant paragraphs according to our classification system. We then focused on analyzing the subjects and associated nouns and verbs in each paragraph. Finally, we integrated and summarized these keywords for each category in the taxonomy.

We also collect statistics on governance issues in terms of the status and severity of the issue. This can reflect what impact governance issues have and how developers handle them. First, we perform a comprehensive statistical analysis of the severity and resolution status of governance issues. Following that, we systematically classify these issues based on our established taxonomy. We pay particular attention to those governance issues with high-severity levels and conducted an in-depth study of their resolution status. Additionally, we examine the governance issues that the project teams refused to solve. Beyond the statistical analysis based on our taxonomy, we also investigate the governance vulnerabilities exposed by these issues. Finally, we summarize governance issues based on our governance taxonomy. Owing to the substantial amount of data acquired, manual analysis poses a significant workload. Consequently, we leverage **Natural Language Processing (NLP)** techniques for initial data processing. We employ BERTopic [57] as an assistant to group the data, and help us find and summarize common governance topics. We examine the clusters generated by BERTopic and determine the three most significant topics (top-3) by the frequency for each governance category.

3 Findings and Implications

In this section, we delve into a detailed analysis of our three RQs based on our data and the analytical framework. We present our findings for each RQ and, in the end, illustrate the implications.

3.1 Taxonomy of DeFi Governance (RQ1)

We identified the *governance definitions* and *what aspect they focus on DeFi governance* in our collected articles. After carefully reviewing these resources, we formulate a governance taxonomy specifically tailored to the domain of DeFi. This taxonomy served as an analytical lens for our subsequent scrutiny of governance issues.

3.1.1 Developing a Taxonomy for DeFi Governance. The governance of one DeFi project should follow the typical software development pattern and is usually developed in a top-down manner, proceeding through three stages: *governance design*, *governance content*, and *governance implementation* as shown in Figure 4:

(1) *Governance Design*. First, the DeFi team must establish a clear vision and principles guiding their governance approach to navigate the complexities of DeFi effectively. This fundamental step is crucial, as it shapes the subsequent decisions and strategies.
(2) *Governance Content*. Next, the DeFi team should delve into the scope and specifics of the governance structure. This involves selecting a suitable governance mechanism and justifying

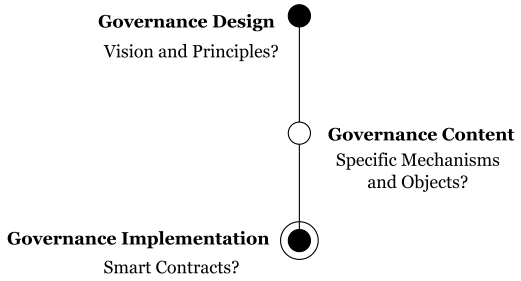


Fig. 4. Three-stage development process of DeFi governance.

its appropriateness for their unique context. This step details the governance process's "what" and "why," ensuring all stakeholders understand the rationale behind the choices.

(3) *Governance Implementation.* As the last step, the DeFi team implements the governance design. For a DeFi project to be deemed reliable, it should, at a minimum, detail its governance design in its whitepaper. An exemplary DeFi project not only makes claims in its whitepaper but also shows how these claims are realized in practical applications.

Figure 4 illustrates the three steps to develop governance in practice. A good whitepaper should record the three steps and make sure that the governance is transparent to users and investors from the design to the end. Based on our understanding of the extracted information of the collected articles as described in Section 2.1, we developed our taxonomy to study governance issues. For each document, we summarized the governance topics it explored and identified the scope of governance it addressed, integrating this information with reference to Figure 4. We approach DeFi governance as shown in Figure 5 from two perspectives: *mechanisms* and *subjects*. According to the common contents that we found from the collected articles, blogs, and reports, we used the six labels of governance issues with several related keywords that were highlighted in orange as shown in Figure 5. The leaf nodes list the common content of each category. *Mechanism* (how to govern) is decided by the vision and objective of DeFi applications. Different types of DeFi applications have different usages and goals, so their governance designs and the corresponding implementations are also different. For example, Uniswap 3 is a decentralized exchange platform and assigns voting power to users through liquidity mining.[3] Aave[4] is a lending platform and claims to be a decentralized non-custodial liquidity market protocol, so it uses DAO to govern. Both are based on the on-chain governance but the latter also need to communicate in the forum. *Subjects* (what to govern) describes the scope of DeFi governance. It consists of two parts, namely system mechanisms and underlying code. The DeFi project constructs an economic system that includes financial models, and all on-chain governance is conducted through code.

Mechanisms (How to Govern). In the design phase, the developers decide which governance approach will be adopted based on their vision. There are two types of governance mechanisms [30, 45, 48, 79]: off-chain and on-chain governance. Off-chain governance typically employs social approaches to reach a consensus for governance. On the other hand, on-chain governance utilizes coded mechanisms within the platform to achieve consensus. First, since our focus is on governance issues related to DeFi projects implemented in smart contracts, our taxonomy is based primarily on on-chain governance (specifically, governance tokens) [16, 22, 29, 30, 81]. The *governance token* is used for decision-making and is regarded as the power to propose and vote [20, 40, 66]. Usually, the

[3] https://uniswap.org/governance
[4] https://aave.com/#governance

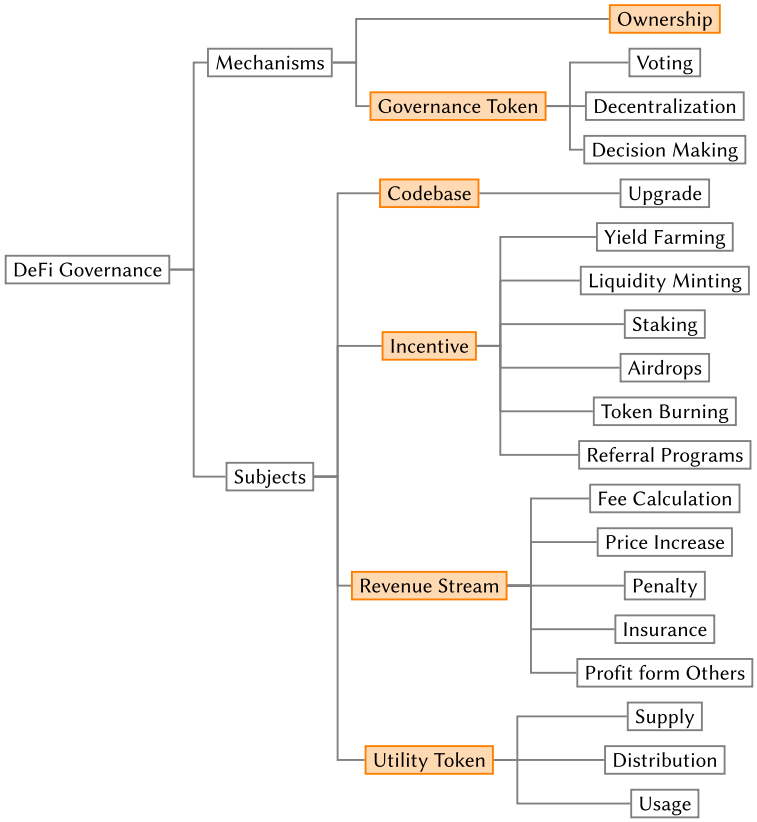


Fig. 5. The overview of DeFi governance taxonomy.

governance token should be decentralized. Second, since the owner of a DeFi project often has certain privileges to govern smart contracts, *ownership* [30, 53] significantly influences the governance of DeFi projects and plays an important role in the governance mechanism. The right of belonging is a controversial topic, and centralization does not comply with the Web3 manifesto, decentralization, but the actual situation may be more complicated. In the initial phase of the DeFi app, the team usually maintains ownership for convenience of updating. Although excessive rights are considered risky, when analyzing data, we have observed that the presence of the owner role is needed in emergency situations, e.g., stopping an attacking transaction. The developer team should justify why they keep ownership, what power the owner role has, and how they manage the owner role.

Subjects (What to Govern). We identified two key areas: tokenomics [18, 21, 23, 24, 33, 53, 60, 66, 88, 118] and codebase [118]. *Tokenomics* refers to the ecosystem defined by DeFi projects and comprises three essential components: (1) Utility tokens [23], which serve as proof of access to DeFi services such as payments, staking, and lending. The supply of utility token usually has the maximum limitation. The initial distribution of tokens greatly affects the interest allocation, the security, and reliability of the project. (2) Revenue streams [24, 53], which outlines how DeFi projects generate profits. The revenue mechanism directly affects the survival time of the project and is a key issue to focus on in the DeFi governance. Revenue streams involve charging fees from users, increasing token prices, insurance, and the profits from other projects. (3) Incentive mechanisms [23, 53], which detail how participants are incentivized to ensure long-term sustainability of the DeFi project. Depending on the target of DeFi applications, there are various incentive mechanisms that reward

Table 2. Raw Keywords for Issue Classification

Category	Subcategory	Keywords	Citations
Governance Mechanism	Governance Token	Governance token, vote, proposal, decision-making, tally, abstention, quorum, veto	[18, 40, 42, 79, 99, 108] [15, 21, 59, 98, 108]
	Ownership	Owner, ownership, privilege	
Tokenomics	Utility Token	Supply, token distribution, token name, token usage, asset token, token utility	[18, 21, 33, 60, 66, 88] [14, 18, 51, 58, 63]
	Revenue Stream	Transaction fee, trading fee, marketplace fee, borrow rate, protocol fee, premium fee, performance fee, token issuance, generic fee, interest rate, charge a fee	
	Incentive Mechanism	Lock up, TVL, yield, borrow, airdrop, burn, stake, liquidity, lend, loan, referral, mint, incentive	
Codebase	Code	Update contract, upgradable	[1, 6, 43, 46, 56, 90]

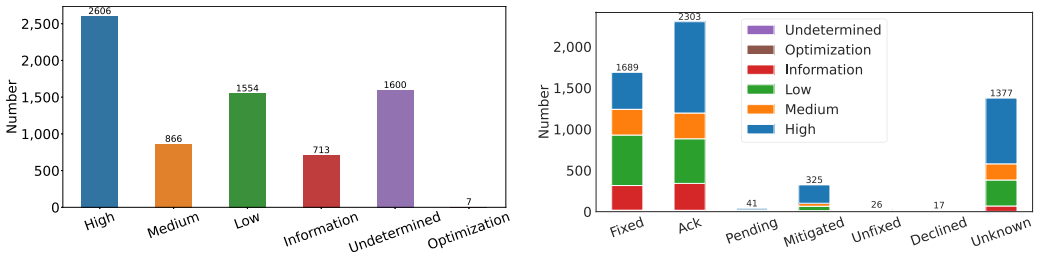
participants. Yield farming is to earn the rewards by locking the token. Liquidity mining rewards the liquidity providers. Other incentive mechanisms include staking, airdrops, token burning, and referral programs.

Codebase pertains to the implementation of DeFi applications. Governance of the codebase involves determining how to update the implementation and address code-related issues, e.g., fixing vulnerabilities or code optimization. These modifications directly influence the DeFi project's functionality, impacting every user. Hence, regulating changes in the code is a crucial aspect of contract governance. In this study, we focus on the issues of code updating, that is, how DeFi applications maintain their code.

3.2 Common Governance Issues (RQ2)

3.2.1 Distribution of Governance Issues. Initially, we must filter out non-government issues. Table 2 presents the raw keywords we originally used for issue classification, aimed at extracting governance issues based on our established governance taxonomy. The first and second columns list the categories and the subcategories from our taxonomy. The third column list the keywords extracted from the papers. Our taxonomy contains six class labels, as depicted in the subcategory column. These labels are grouped into three categories: governance mechanism, tokenomics, and codebase. These keywords were derived from the papers and blogs we collected. We identified the relevant paragraphs using the category words in the collected articles. Then, we read these paragraphs to pinpoint the corresponding keywords closely related to our topic. We eliminated the issues that did not include these keywords, yielding a total of 7,346 governance issues.

Overall Distribution of Governance Issues for Severity and Resolution Status. Regarding governance issues, we conducted a similar statistical analysis to Figure 3, detailed in Figure 6 (notice some issues do not have status and severity records). Figure 6(a) reveals a different data distribution from Figure 3(a), indicating that high-severity governance issues are the most prevalent (35.48%). However, the second most common category is "Undetermined" (21.78%), which implies that auditors have difficulty in determining the severity of governance issues. This may be due to a lack of triage guidelines and an insufficient understanding of governance impacts. Regarding resolution status, the distribution in Figure 6(b) is similar to that in Figure 3(b), suggesting that DeFi development teams do not adopt specific strategies for addressing governance issues. Additionally, Figure 6(b)



(a) Distribution of Severity about Governance Issues (b) Distribution of Status about Governance Issues

Fig. 6. Severity and status of governance issues in our dataset.

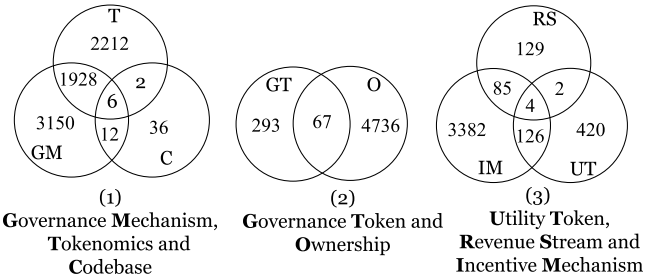


Fig. 7. Overlapping of different categories about governance issues.

Table 3. Status of Governance Issues

Category	Fixed	Ack.	Mitigated	Pending	Unfixed	Declined	Unknown	All
Gov. Token	**175**	**118**	19	1	3	1	43	360
Ownership	**688**	**1,372**	214	23	9	8	2,489	4,803
Utility Token	**115**	**273**	40	6	3	2	113	552
Revenue	**88**	**80**	8	1	2	3	38	220
Incentive	**879**	**986**	130	16	12	9	1,565	3,597
Codebase	**20**	**14**	7	0	1	0	14	56
Total	**1,689**	**2,303**	325	41	26	17	2,945	*7,346*

The number in the last row is counted by excluding the overlapping. The numbers of fixed issues and acknowledged issues are marked in bold font. The italics is the total number of issues.

shows that more governance issues are acknowledged than fixed by the development team, which slightly differs from the pattern shown in Figure 3(b).

Distribution of Governance Issues in Each Category. The status and severity of the governance issues for each category are demonstrated, respectively, in Tables 3 and 4 (notice that if the issues do not have their corresponding records, we label them as unknown or undetermined). We also collected statistics on the overlap of governance issues among different categories, and the results are shown in Figure 7. The last columns in Tables 3 and 4 reveal that most of the governance issues are related to ownership and incentive mechanisms. Discounting the status-unknown issues, it is evident that almost all governance issues with known status are fixed or acknowledged by the development team, as seen in Table 3. Table 4 indicates that most governance issues are labeled with high or medium severity. Compared with Figure 3(a) (26.4%), it is clear that a significant number of high-severity issues are governance related (about 35.48%). Figure 7 illustrates the extent of overlap among different categories of governance issues. It is evident from Figure 7 that the majority of these issues are unique to their respective categories and do not overlap.

Table 4. Severity of Governance Issues

Category	High	Medium	Low	Information	Optim.	Undet.	All
Gov. Token	101	77	**130**	44	0	8	360
Ownership	**1,814**	447	637	327	3	1,575	4,803
Utility Token	**279**	98	118	48	0	9	552
Revenue	46	43	**82**	41	0	8	220
Incentive	**972**	421	832	356	3	1,013	3,597
Codebase	**21**	14	14	5	1	1	56
Total	**2,606**	866	1,554	713	7	1,600	*7,346*

The number in the last row is counted by excluding the overlapping. Governance issues with the highest issue severity are marked in bold font at each row. The italics is the total number of issues.

Table 5. Status of High-Severity Governance Issues

	Fixed	Ack.	Mitigated	Pending	Unfixed	Declined	Unknown	All
Gov. Token	**54**	34	8	0	0	0	5	101
Ownership	208	**789**	161	16	0	5	635	1,814
Utility Token	40	**156**	31	1	2	0	49	279
Revenue	**18**	15	5	0	0	1	7	46
Incentive	201	**403**	81	5	5	4	273	972
Codebase	7	7	6	0	0	0	1	21
Total	528	1,404	292	22	7	10	970	3,233

The highest numbers in the issue resolution status are marked in bold font.

How High-Severity Issues Are Handled. Tables 3 and 4 have showed the status and severity of governance issues. It is interesting to see if there is any connection between the two tables. Therefore, we study the high-severity issues to see how DeFi teams handle them. Given that high-severity governance issues often pose significant vulnerability risks, it stands to reason that these issues should be prioritized for resolution. To understand the actual status of these high-severity issues, we compiled their status distribution, as shown in Table 5. Excluding issues with unknown status, only 23.33% of high-severity issues have been resolved. Issues related to governance tokens have the highest resolution rate (53.47%, 54/101), while those related to ownership and utility token have the lowest resolution rate, at approximately 17.5%. Statistical data shows that current DeFi projects do not place enough emphasis on the importance of governance mechanisms, failing to prioritize the resolution of governance issues. Although ownership issues with high severity are the most prevalent, DeFi project teams prefer to postpone these issues rather than address them immediately. The reasons behind this are worth considering. As developers and primary maintainers, DeFi project teams have the reason to retain certain ownership and special privileges in the project framework. Acknowledging the fact that it is unrealistic for DeFi project teams to forgo all ownership and privileges completely is essential. Hence, users must consider this aspect when evaluating DeFi projects and making investment decisions.

Reasons for Declined Issues. We conduct an in-depth analysis on the 17 governance issues that the project team refused to acknowledge or resolve. These issues can be classified into four categories:

(1) Centralization: The contract owner holds extensive permissions, enabling them to modify key contract parameters or controls without community consensus.

(2) Security Vulnerabilities and Access Control Issues: Governance-related functions lack necessary validation or have incorrect validation mechanisms.
(3) Incorrect Price Update and Operation Mechanisms: Some functions or privileges may allow manipulation of token prices through mechanisms such as flash loans.
(4) Governance Design Flaws: The project teams do not fully consider all business scenarios during design, which results in an inability to handle certain edge cases properly.

We also count the number of responses from the project team to these issues and analyze why they refused to address them. We find that nine issues received responses from the project team, highlighting the reasons for refusals:

(1) Design Decisions: Some designs are based on specific business logic or market strategies.
(2) Retention of Privileges and Control: The project team chose to retain more control for operational convenience and management flexibility.
(3) Misunderstanding of Auditors: Some issues have been reported due to auditors' misunderstanding of the functionality or design intention of the project.

Regarding these reasons, we would like to highlight that retaining excessive control may go against the core principles of decentralization in DeFi. For example, some project teams have absolute control over parameter settings during the token pre-sale period and claim it is part of their business plan. The various parameter settings of the token sales undoubtedly have profound impacts on all users and the project team's interests. From the moment a DeFi project operates publicly, all its actions should be conducted within the governance framework to ensure that every decision undergoes transparent review and receives wide recognition from the community. Such governance flaws not only affect the project's credibility but may also erode the entire ecosystem's trust and adherence to the principles of decentralization.

We conclude *the following points*: (1) auditors do not fully understand the importance of governance, and lack triage guidelines to determine the severity of governance issues; (2) DeFi teams do not recognize the importance of DeFi governance and do not handle the governance issues differently from other issues; (3) ownership and incentive mechanisms are two of the most common governance issues; (4) the number of high-severity issues is the highest among all severity levels of governance issues; (5) there is a small overlap among these governance categories; (6) most of high-severity governance issues are not fixed; (7) in analyzing the reasons behind DeFi project teams' refusal to address governance issues, it was discovered that these teams do not fully understand the importance or adhere to the scope of DeFi governance.

3.2.2 Hierarchy of Governance Vulnerability. To delve deeper into governance issues and their related vulnerability, we have categorized these issues based on the design and implementation process of governance, as depicted in Figure 8. The first column in the figure outlines the governance issues at each developmental stage, while the second column identifies the corresponding vulnerabilities. For each stage, we summarized vulnerabilities by identifying key security-related terms, such as "attack," and then conducted a manual review of the filtered issues. Initially, in the governance design stage, ownership is determined based on the vision and principles of the DeFi project. Ownership is the core of DeFi governance. It decides which governance mechanism will be applied. For example, if ownership is decided to belong to all participants, it should use the DAO governance model. During this stage, the owner rights should be carefully designed. Flaws in ownership design can lead to risks like rug-pull [107]. Owners, typically vested with extensive rights to manipulate contracts and maintain privileged functions, can easily misappropriate funds from users. The special rights associated with governance roles can, if compromised, pose a threat to the entire DeFi application.

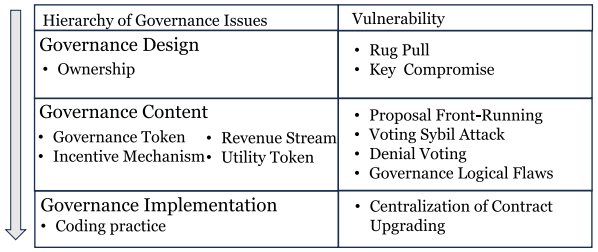


Fig. 8. Hierarchy of governance issue.

In the subsequent stage, issues concerning governance tokens, revenue streams, incentive mechanisms, and utility tokens emerge, all of which contribute to the formation of governance content. This stage often brings to light governance functionality issues, such as proposal front-running, Sybil attacks in voting, denial voting, and inconsistencies in the governance process relative to its design. For instance, in proposal front-running, attackers can prematurely reach a consensus on a malicious proposal [86]. In voting Sybil attacks [87], an attacker might rapidly acquire substantial voting weight through flash loans. Denial voting often results from the depletion of gas fees [91]. We also notice that some issues are caused by the implementation pattern of tokenomics and governance mechanisms. Some of them can result in logical flaws in governance rules. Logical flaws in governance can significantly increase the susceptibility to attacks. For example, DerivaDEX's governance structure and its use of the Diamond proxy pattern are vulnerable to exploitation by malicious actors [91]. The implementation of governance may be different from the designed documents, introducing some risks such as phishing attacks [100] or causing the fairness problem [27] to the DeFi projects.

In the final stage, the governance implementation involves addressing issues related to coding practices. The way governance roles manage and update the DeFi system is crucial. Incorrect initialization [31] or inappropriate upgrades can precipitate the failure of a DeFi project [28].

Mitigation. A sound governance mechanism can effectively mitigate the security vulnerability risks faced by DeFi governance. Firstly, such a mechanism will manage ownership and privileged functions safely and efficiently. This includes clearly defining the design intent of ownership and privileged functions, clarifying ownership relationships, and establishing a clear permissions management system to ensure that each asset and resource has well-defined ownership and responsibility. In this way, we can effectively prevent unauthorized access and use, and promptly track and resolve issues when they arise. Moreover, a clear permissions management system helps optimize the allocation and use of resources, thereby enhancing overall efficiency and security. For instance, implementing a multi-signature mechanism can not only effectively prevent the theft of contract ownership or malicious invocation of privileged functions due to individual key leaks but also significantly reduce user concerns about "rug pulls" (sudden withdrawals by project teams). At the same time, a good governance mechanism should balance the interests of all stakeholders, ensure an equitable distribution of rights, and prevent potential threats posed by large accounts to the project.

3.2.3 Common Topics on Governance Issues. We use BERTopic [57] to cluster governance issues for each category. Table 6 demonstrates the top-3 frequent topic words, respectively. More importantly, to gain a deeper understanding of the critical governance issues, we thoroughly reviewed various high-severity issues. Based on Table 6 and the review of high-severity governance issues, we make the following summary.

Table 6. Top-3 Topic Words in All Governance Issues

Category	Top 1	Top 2	Top 3
Gov. Token	Proposal, contract, token	Voting power, power moved	Governance, malicious, lack event
Ownership	Centralization risk	Trust issue admin, keys	Blacklisted contract
Utility Token	Token distribution initial	Total supply, wrong total, supply restriction	Rewards, price, users, duplicate, liquidity
Incentive	Owner privileges, centralization risk	Mint token	Trust issue admin, keys
Revenue	Protocol fee, transaction	Interest rate, borrow, manipulate	Incompatibility deflationary tokens
Codebase	Upgradeable contracts, storage	Centralized control contract, contract upgrade	-

Governance Token. The primary concerns include proposal management, notably the expiration and unexpected cancellations of proposals, and issues with non-unique identifiers for voting topics. The second cluster addresses the voting process, focusing on the transfer, burning, or minting of voting power. The third highlights decision-making and governance vulnerabilities, such as delays in executing decisions and the risk of malicious proposals. When we review the high severity of governance tokens, we identify three primary issues: token management errors, voting mechanism defects, and proposal management. Token management errors, such as incorrect token amounts, often stem from faulty implementations or logical mistakes. Additionally, we discover that voting rights do not transfer with token transfers, potentially causing governance inconsistencies. In the voting mechanism, repeated delegation can unduly amplify voting power, and some contracts lack proper condition validation before executing voting functions. Governance and proposal management issues include repeated actions or transaction processing errors during proposal execution, disproportionately impacting governance.

Ownership. The most important issue is the centralization risk, where owners may have excessive or insufficient authority, such as the ability to halt transactions or a lack of emergency management rights. The second topic relates to administration key management, emphasizing the risk of significant losses due to leaked admin keys. The third topic discusses blacklist management issues. After we reviewed ownership issues with high severity, we found three frequent problems related to lack of input validation, unauthorized operations, and improper ownership settings. Concerns about outdated ownership information during migration could lead to unauthorized proxy control. Privileged functions lacked proper restrictions, enabling unauthorized users to manipulate sensitive contract states or withdraw funds arbitrarily. The potential for excessive control granted to a single owner or privileged role could result in unauthorized token minting, fund extraction, and modification of key contract parameters.

Utility Token. The first concern is the initial distribution, where tokens are often distributed without community consensus, leading to concentration in whale accounts. The second issue pertains to discrepancies in the total token supply compared to what is stated in the whitepaper, along with unregulated adjustments to the supply. The third focuses on utility token usage problems, including price setting, liquidity issues, and reward calculation. When we check the high-severity issues related to utility token, we find two main problems. First, utility tokens exhibited discrepancies between the specified fixed total supply and the actual initial supply, as well as supply changes resulting from certain operations. This could lead to potential errors in token supply update

calculations under specific circumstances. Second, contract deployers could unilaterally allocate tokens without community consensus, leading to centralized distribution and potential abuse.

Incentive Mechanism and Revenue Stream. The primary issue is the risk of centralization and privileged functions, which allows owners to manipulate incentive-related functions such as fee rates. The second concern involves the minting process, including restrictions, authority, and access control. The third points to potential manipulation of the incentive mechanism due to improper key management. For Revenue Stream, the first issue is the fee configuration problem, including calculation errors and manipulation of transaction fees. The second issue covers the design of borrowing and loaning processes, and interest rate settings. The third raises concerns about the compatibility between non-deflationary and deflationary tokens. After we review the revenue and incentive issues with high severity, revenue and incentives had three risks of excessive token minting, exceeding expected supply: First, the management and transaction fee functions run incorrectly, affecting liquidity and user interests; second, there are logical problems with the system pricing mechanism, leading to possible price manipulation; third, centralization vulnerabilities allowed attackers to extract significant value from pools with minimal input, breaking pool sustainability.

Codebase. This first concern highlights technical concerns such as improper initialization or incorrect implementations during upgrades, which may cause catastrophic failures or expose vulnerabilities. The second major concern is the risk of centralization in contract upgradeability, where an attacker controlling the owner role could introduce malicious updates, leading to significant losses. When we review the high-severity issues related to codebase, we find that code issues included that design incompatibilities with upgrade and storage mode implementation or initial value settings in field declarations caused problems post-upgrade.

3.2.4 Technical and Human-Centric Issues in DeFi Governance. In most DeFi projects, the governance process still requires human participation. We discuss the differences between technical governance issues and human-centered governance issues. The main distinction lies in whether the human role is that of an active participant or a passive influencer. *Technical governance issues* mainly involve the implementation of DeFi governance, including logical vulnerabilities in governance contracts and specific implementation problems such as contract updates and code optimization. These issues can lead to vulnerabilities being exploited by hackers or contracts not functioning as intended. Common examples include insufficient input validation, contract update issues, and reentrancy attacks. Problems related to the codebase fall into this category and can typically be addressed through improvements in code and system architecture, with traditional smart contract auditing tools capable of detecting these issues. However, these tools have limitations in dealing with complex attacks. *Human-centered governance* issues pertain to the design of DeFi governance and usually require human intervention, decision-making, and oversight. Governance design issues can be broadly categorized into two types: flawed designs and the improper implementation of what should have been a reasonable design. Flawed designs encompass centralized structures, retention of privileged functions, unfair economic models, and opaque governance mechanisms. Notably, issues related to centralization and privileged functions constitute at least 65% of all cases (4,803/7,346). Current detection tools have some capacity to identify these problems, e.g., privileged functions. To address centralization risks, solutions include limiting the powers of privileged roles, implementing transparent governance voting processes, and encouraging extensive community involvement. However, the detection of flaws in economic models and governance mechanisms remains largely reliant on manual review. Addressing these issues may involve providing technical guidance to development teams and enhancing their understanding of governance principles. The flawed governance design issues can lead to serious vulnerabilities and have gotten more attention.

Moreover, the improper implementation of sound designs typically arises when development teams fail to adhere to governance design during development. From the users' perspective, this is a significant injustice—they expect to interact with a well-designed system but instead encounter a different mechanism. In Section 3.3, we further investigate this issue by analyzing 15 real-world projects in the market.

3.3 DeFi Design-Implementation Inconsistency Issues (RQ3)

3.3.1 Governance Design-Implementation Inconsistencies. Our analysis indicates that almost all issues related to human factors are closely tied to governance design. We delved into the issues about the governance design. First, we screened governance issues containing the keywords "whitepaper" and "document," ultimately identifying 136 issues directly related to governance design in our collected audit reports. The whitepaper or documentation of a project typically details its DeFi governance design, while the audit of smart contracts is based on the contract code. The resulting 136 issues are related to governance design and come with the corresponding implementations. After manual review, we found that these issues are almost all about tokenomics, concerning discrepancies between the code implementation and the documented design. For instance, in the audit report for **Abstract Syntax Tree (AST)**-Finance,[5] the auditors noted that although the whitepaper claimed there were no fees, the project charged a deposit fee. Such discrepancies, even if they do not lead to vulnerabilities, can profoundly affect the credibility and success of a DeFi project. For users and investors alike, it is both interesting and vital to assess how faithfully developers adhere to their claims made in the whitepapers. This adherence is not just a matter of technical accuracy but also one of maintaining trust and transparency in the emerging world of DeFi. Second, to investigate the design-implementation issues regarding governance in the real world, we collected and checked 15 DeFi projects on the DeFi platform, including 104 tokenomics configurations. Our selection criteria were: (1) the project must be related to DeFi, and we chose projects with the tag DeFi; (2) both the whitepaper and code must be accessible; (3) the whitepaper should have a section describing its tokenomics. During data collection, we leveraged the Internet Archive[6] to gather the required information. Our collection process revealed the often-overlooked challenge of accessing reliable sources; many projects, despite claims of openness, had invalid links to their whitepapers and code due to various reasons, such as project discontinuation or poor maintenance. We explored various DeFi websites, including Code4Rena,[7] ICODrops,[8] and ICOmarks,[9] to collect these projects implemented in Solidity. We discovered that only a few projects had valid links to the whitepaper and the code despite claiming to be open to all users.

3.3.2 Investigation of DeFi Design-Implementation Inconsistency Issues. We leverage **Large Language Model (LLM)'s** capability of extracting key information from long textual inputs to assist in analyzing the inconsistencies between whitepapers and code of these 15 projects. Current smart contract detection tools primarily focus on identifying vulnerabilities rather than verifying compliance with governance design. They only work with code, but in our case, we need to work with both the document and the code together. Figure 9 demonstrates the analysis process and the code is publicly available.[10] An expert first reads the whitepaper and locates the tokenomics configurations. We then ask an LLM to find the possible variable names that can appear in the code

[5] https://certik-public-assets.s3.amazonaws.com/REP-AST.Finance-2021-08-05.pdf
[6] https://wayback-api.archive.org/
[7] https://code4rena.com/
[8] https://icodrops.com/
[9] https://icomarks.com/icos/defi
[10] https://github.com/Marvinmw/consistency_checker

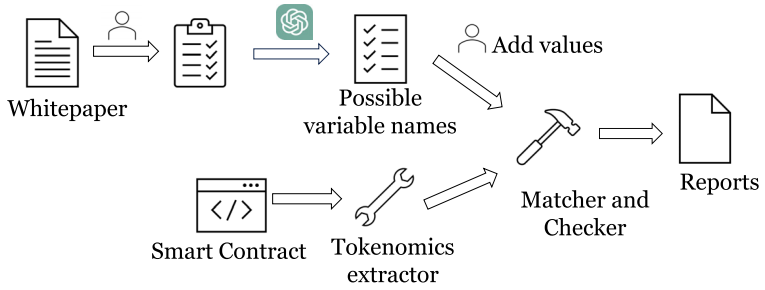


Fig. 9. Analysis process about tokenomics.

for these tokenomics descriptions. Then, we extract the corresponding variables and the expressions from the smart contract. For the extraction, we parse the source code into an AST, and then we visit the AST and extract nodes if their types match the variable or expression type. We employ the embedding model to obtain embeddings for the token economics variable names from the previous steps. We compute the cosine similarity and match the variables predicated by the LLM and the variables from code based on the top-5 similarity. Based on the variables matching, we check if they make sense and add the values to them according to tokenomics descriptions. We also report all fee items we find in the code, and find that some projects have the charge fees but never discussed in the whitepaper.

We first used auxiliary analysis tools to analyze the data (see Table 7) and manually verified the output results. Among the 104 tokenomics configurations analyzed, we found that 27 configurations had inconsistencies between design and implementation, while 77 were consistent. Out of the 15 projects inspected, only 2 were completely consistent. The reasons for the inconsistencies between design and implementation mainly fall into two categories: First, the total amount of tokens initialized did not match the description in the documentation; second, the fee ratio related to the transaction was higher than stated in the whitepaper, resulting in greater benefits for the project team. Before collecting this data, we did not anticipate these design and implementation issues. This suggests that inconsistencies between design and implementation might be a common phenomenon in the industry, which could be due to deliberate actions by the project team or changes during development that were not promptly reflected in the documentation updates. Although such issues may not directly lead to security vulnerabilities, they can affect the distribution of benefits in DeFi projects. Therefore, we urge project teams to emphasize consistency between design documents and code, as this is crucial for enhancing the overall reputation of the project.

3.4 Implications

Our findings from this study derive multiple implications for various stakeholders in the DeFi ecosystem, including researchers, DeFi developers, investors, users, policymakers, and regulatory bodies. The stakeholders have varying concerns about governance issues identified in our taxonomy study based on Figure 5. Researchers should focus on the issues about the overall framework of governance mechanisms and strengthen research on their transparency and credibility. DeFi developers need to address the management of privileged functions within governance to prevent financial losses due to privilege leaks. Users should scrutinize the transparency of a project's governance mechanisms, ensuring there are no unmonitored privileged functions, particularly those issues related to tokenomics and financial models. Regulators should prioritize governance design issues to identify scam projects more effectively. Additionally, our research has revealed which governance aspects should be prioritized in DeFi applications. This not only helps to optimize the

Table 7. DeFi Tokenomics Configuration Inconsistency Checking (F1 = 53.00%, Recall = 81.48%)

Project ID	No. of Params	Predicted P/N	FP	FN
1	5	0/5	0	0
2	6	4/2	2	1
3	6	5/1	3	0
4	8	3/5	3	2
5	6	4/2	3	0
6	7	7/0	1	0
7	7	6/1	1	1
8	9	8/1	8	0
9	19	11/8	7	1
10	10	0/10	0	0
11	3	2/1	2	0
12	3	1/2	2	0
13	2	2/0	1	0
14	6	1/5	1	0
15	7	2/5	1	0
Total	104	56/48	34	5

governance structure of DeFi applications but also enhances the system's security and transparency, thereby better meeting the needs of users.

For Researchers. First, in the realm of software engineering research, our analysis shows that about 28% of audit issues are about the governance and therefore, there is a pressing need to delve into DeFi governance frameworks. Governance challenges form a substantial part of the hurdles DeFi applications face, necessitating thorough research and solutions. Our taxonomy serves as a foundation for this exploration. Yet, numerous challenges remain unaddressed. For instance, the absence of a governance development model akin to software development frameworks hampers the design and implementation of effective governance strategies. Furthermore, the fairness in tokenomics and the balancing act in centralization demand in-depth study. For example, determining the extent of control for owners and establishing ownership criteria are critical. The ideal model for DeFi governance is the DAO model [116], which is a fully decentralized governance model. However, this ideal model faces significant challenges and issues in practice. The first hinder is cost. We have found that developers often prioritize the implementation of the project's business aspects, including fixing business-related vulnerabilities. In current DeFi projects, adopting a DAO governance model would significantly increase design and development costs. This is especially true given that many DeFi project teams do not place a high emphasis on DeFi governance. As a result, many project teams opt for easier-to-implement governance methods. Additionally, there are recent studies proposing new, more complex voting mechanisms, such as hybrid models [42] combining on-chain voting with off-chain discussions. However, from a user perspective, a complex DeFi governance participation process may reduce user engagement. This needs to be particularly considered when designing DeFi governance models, as active user participation is crucial for the success of any governance model. Especially in the field of DeFi, user engagement is not only the foundation of governance but also a vital indicator of the ecosystem's healthy development. Therefore, designing a governance model that is both efficient and easy for users to participate in is one of the key challenges that DeFi governance needs to address. *Second*, a robust verification

methodology is vital for scrutinizing the governance system design prior to implementation as indicated by Singh and Chopra [104]. Our analysis shows that about 65% of governance issues are about the ownership design. Given that smart contracts are immutable post-deployment, rectifying defects is not as straightforward as in traditional software systems. From proposal initiation to final execution, each state transition within the governance process warrants careful verification. Overlooking flaws in governance design can have dire consequences, such as losing control to hackers. Addressing potential flaws proactively is crucial, as fixing high-level issues post-deployment in DeFi systems can be exceedingly costly. *Third*, ensuring consistency between DeFi whitepapers and their implementation is paramount. This alignment is crucial for transparent and accurate communication with investors and users. Developing semi- or fully automatic approaches to verify this consistency is an essential step forward. The prototype assistant tool developed in our research could pave the way for more advanced systems capable of automating the verification process, thereby upholding the integrity of DeFi projects.

For DeFi Developers. DeFi governance design is a complex and multi-layered process. Developers can refer to our governance taxonomy framework and clearly articulate the fundamental principles behind the chosen design. Developers should fully consider the degree of decentralization, including the distribution of governance tokens and the ownership/privileges of contracts. Among these, the distribution of governance tokens is an important aspect of DeFi governance design. The distribution of governance tokens is usually concentrated between internal participants (such as the founding team and investors) and external users (such as early adopters and ecosystem developers). The distribution of governance tokens determines the governance voice. The issues regarding incentive mechanisms are very common, accounting for up to 49% in our dataset. Developers should also recognize that fair incentive mechanisms play a crucial role in DeFi governance. Incentive mechanisms can consider both short-term and long-term rewards. Short-term reward mechanisms can compensate early participants for their contributions. Long-term rewards can help DeFi projects sustain for a longer period. By implementing reasonable incentive mechanisms, the interests of all parties can be aligned, promoting system stability and development. Additionally, developers need to implement a transparent decision-making process to build trust. For the management of privileged functions, a corresponding decision-change mechanism should be established. This can prevent black-box decision-making. Developers should strive to communicate transparently and accurately with investors and users. Maintaining consistency between the governance design and the actual implementation is important to reduce misinformation and mitigate risks. This approach not only builds trust but also consolidates the project's credibility within the DeFi ecosystem. Developers must stay informed about common governance issues and vulnerabilities. Particular attention should be paid to ownership protection mechanisms and logical vulnerabilities in governance contracts, such as preventing unauthorized access to owner keys by team members or external threats.

For Investors and Users. This study can provide important references for investors and users when investing in the DeFi sector. By understanding the governance issues outlined in our taxonomy, investors and users can grasp the risks involved in the investment process. Investors should carefully examine the governance framework, ownership structure, and tokenomics of DeFi projects to understand indicators of robustness and fairness. Crucial steps include:

— Evaluating how a DeFi program manages ownership and the rationale behind these strategies.
— Investigating the rights granted by governance tokens within the project's structure.
— Assessing token distribution and privileged functions for potential unfair practices or inconsistencies with the design.
— Understanding who holds the power to alter the DeFi code.

By comprehensively analyzing these elements, investors and users can discern the value and legitimacy of a DeFi application, thereby steering clear of scams. For example, the ability of a DeFi program to mint unlimited tokens or withdraw liquidity unrestrainedly may signal fraudulent intent. While there are inherent risks and cost, a well-governed DeFi project can also present significant opportunities. Thus, a balanced approach in evaluation is crucial.

For Regulators and Policymakers. Regulators and policymakers can gain valuable insights from this work, particularly in understanding the nuanced governance challenges and potential solutions within DeFi. This study underscores the necessity of a regulatory framework that goes beyond assessing code vulnerabilities to encompass the entire governance structure of DeFi projects. A key area for future policy development is the role of whitepapers; it is time to discuss their legal significance within the DeFi ecosystem. For instance, considering the role of whitepapers in outlining the fundamental principles of a project, it is crucial to consider whether they should be subject to regulatory oversight to prevent fraudulent projects. Additionally, governance issues often revolve around ownership and incentive mechanisms. Therefore, regulators should closely monitor privileged functions that significantly impact the DeFi economy to ensure investors are not deceived.

Priority of DeFi Governance Design and Implementation. In the design and implementation of DeFi, the following points should be prioritized: (1) transparency and consistency, (2) voting mechanism, (3) incentive mechanism, and (4) risk management and security audits. *First*, for transparency and consistency, governance design must clearly define ownership structures and the allocation of permissions to prevent any single entity from having excessive control, especially over critical decisions and functions (such as minting and rate adjustments), thereby effectively reducing centralization risks. Additionally, ownership structures and permission allocations should be documented for easy reference by security personnel and users. DeFi projects must also ensure that their whitepapers are consistent with actual implementation, which not only helps build trust among investors and users but also prevents potentially fraudulent activities. In terms of transparency, projects should disclose the processes and results of all key decisions, ensuring that community members can clearly understand the operation of the project, further enhancing trust. *Second*, for voting mechanism, design fair and transparent voting mechanisms to ensure that all stakeholders have the opportunity to participate in the decision-making process. The voting mechanism should encompass broad participation to avoid decision-making being monopolized by a few individuals. Establish detailed voting rules and procedures so that all participants can understand and comply. Additionally, voting results should be transparent and open to ensure there is no behind-the-scenes manipulation, increasing the credibility of the governance mechanism. Utilizing on-chain voting technology can improve the transparency and efficiency of the voting process. *Third*, for incentive mechanism, establish reasonable incentive mechanisms to balance short-term and long-term interests. Short-term incentives can attract early participants, while long-term incentives help ensure the sustainable development of the project. Ensuring the transparency and fairness of incentive mechanisms can enhance community cohesion and the stability of the project. The incentive mechanism should consider the needs of different types of participants, including developers, users, and investors, and formulate corresponding reward measures to promote active participation from all parties. The incentive mechanism should also be flexible, capable of being adjusted according to the project's development stage and market changes. *Fourth*, for risk management and security audits, conduct comprehensive risk assessments and security audits during the governance design and implementation phases, especially targeting vulnerabilities in smart contracts and logical flaws in governance mechanisms. Regularly perform security audits and promptly fix any identified issues to ensure the system's safety and stability. Establish robust

risk management mechanisms, including emergency plans and risk mitigation strategies, to address potentially risk scenarios. The project team should collaborate with professional security companies to perform in-depth security analyses and testing, ensuring the project's long-term security.

4 Related Work

Studies on Blockchain and DeFi. Blockchain employs a decentralization methodology, securely storing data in a specifically structured entity known as a block. In particular, data incorporated into the system becomes impervious to tampering. Blockchain technology has caused profound changes and impacts on traditional Web 2.0 and is becoming a fundamental service of the Web, leading to the emergence of Web 3.0. Blockchain has been widely used in many fields, such as cryptocurrency, financial services, games, trading systems, and IoT [37, 54, 125]. Zheng et al. [125] and Gao et al. [54] reviewed the fundamental techniques in blockchain such as architecture and consensus algorithms, and also discuss several blockchain applications. Di Francesco Maesa and Mori [37] studied non-cryptocurrency blockchain applications and practical problems they solved, indicating that blockchain is a valuable technique for the real world. DeFi is one main application scenario for blockchain. Meyer et al. [83] conducted the systematic literature review about DeFi at three different levels, i.e., micro, meso, and macro. Shah et al. [101] reviewed the various types of DeFi protocol in DeFi products. Bartoletti et al. [17] reviewed the formal methods for DeFi to ensure its correct behavior. Jiang et al. [62] investigated the DeFi running mechanisms and systemically review the DeFi risks. Werner et al. reviewed the features and security of DeFi.

Blockchain and DeFi Governance. In the realm of blockchain and DeFi governance, several studies stand out. Ferreira et al. [50] explored how large corporations can dominate blockchain governance by leveraging their control over critical resources, leading to potential governance capture and challenges to the decentralized ideals of blockchain technology. Messias et al. [82] analyzed voting patterns in the governance mechanisms in the two governance protocols, Compound and Uniswap, revealing significant centralization of voting power. Tan et al. [109] developed a comprehensive conceptual framework for blockchain governance in the public sector, dividing governance decisions into micro, meso, and macro levels to guide the design and implementation of blockchain-based systems in public administration. Khan et al. [64] investigated the role of Nash equilibrium in blockchain governance. Allen and Berg [11] and Allen et al. [12] proposed a descriptive framework to understand blockchain governance, and later develop an exchange theory for Web3 governance. Ekal and Abdul-wahab [42] bridged traditional finance governance models with blockchain-based mechanisms. Kiayias and Lazos [66] conducted a comprehensive examination of the characteristics of blockchain governance. Truchet [113] and Gogel [55] discussed its main forms, offering insights into this emerging field. Liu et al. [79] performed a systematic review analysis, summarizing the concept of blockchain governance as the system and procedures established to ensure that the development and implementation of blockchain technology complies with legal, regulatory, and ethical obligations. Liu et al. [77] summarized 14 architectural patterns for blockchain governance. Furthermore, Liu et al. [78] proposed a governance framework specifically for blockchain technology. Other foundational works [70, 88, 118] have also explored the realm of blockchain governance, offering highly abstract and conceptual insights. Fusco [53] looked at the DeFi revenue models and governance systems based on the analysis of real DeFi applications. Some works studied governance risks and code update. Bekemeier systematically analyzed risks in DeFi, including DeFi governance. Bhambhwani [21] analyzed the top 50 DeFi protocols and indicated potential governance risks. Everts and Weitenberg [43] discussed smart contract governance on smart contract upgrade in permissionless and permissioned blockchains. Reports from international organizations like the

OECD and BIS [25, 47, 84, 120] discussed the current state and potential impacts of DeFi, providing a broader policy perspective. All of these works do not study the governance issues in DeFi applications. We benefit from the previous studies and build a governance taxonomy to study the governance issues in DeFi.

DeFi Security. Since its inception, blockchain technology has held a strong affinity with finance, and as such, its security issues often precipitate substantial financial losses. For example, RONIN[11] lost $624M because the attacker found a way to access the additional validator. The increased focus on blockchain security has led to the emergence of numerous tools to identify and rectify vulnerabilities, such as Slither [49] and ContractFuzzer [61]. Zhou et al. [126] studied the 13 common vulnerabilities and compare different security tools. Nevertheless, these resources are predominantly code-centric, overlooking design-level vulnerabilities, like those that pertain to flash loan attacks. These security gaps depend mainly on human auditing for detection and correction. Li et al. [73] comprehensively analyzed the security issues of DeFi at each blockchain layer. Since DeFi defines an economy system and interacts with the real world, its vulnerability is not only limited in itself weakness but also includes some more complex risk issues. Liu et al. [76] studied the fairness problem in DeFi. Trozze et al. [112] studied the financial fraud in DeFi. Torres et al. [111] studied honeypot smart contracts and developed a tool to detect this scam. Liang et al. [74] studied Ponzi scam in DeFi. Dotan et al. [39] uncovered governance vulnerabilities in governance tokens, which, although designed to decentralize decision-making by allowing user votes on platform changes, are often exploited. Li et al. [71] used Tron and Steem as examples to explore the security vulnerabilities of Delegated Proof-of-Stake blockchains against takeover attacks. Kharman and Smyth [65] used Vocdoni's governance protocol as a case study to illustrate these vulnerabilities, arguing that decentralization is largely a myth.

Code-Design Inconsistency. Inconsistency between code and the documented design is the common issue in software evolution. Wen et al. [117] systematically investigated the inconsistency between code and the documented design in a large dataset. Tan et al. [110] studied the outdated documents and analyze the reason why the document is not synchronized with the latest code. Recent research works use machine learning approaches to detect inconsistencies between code and the documents. Rabbi and Siddik [92] used the Siamese recurrent network to detect inconsistency based on word tokens in code and documents. Kim and Kim [67] employed NLP to detect inconsistent identifiers. Panthaplackel et al. [85] utilized the graph neural networks to detect code-doc inconsistencies based on AST. Rani et al. [93] conducted a literature review on code-design quality and found that most works focus on Java programs, resulting in poor generation performance. All of the works focus on the code function and the designed functionality.

NLP Topic Model and Foundation Model. The topic model [34] is a useful text analysis tool and can identify the topic words in the documents without the training phase. Abdelrazek et al. [10] grouped topic molds into four categories: algebraic, fuzzy, Bayesian probabilistic, and neural topic models. Since the appearance of BERT [36], a large number of deep learning-based topic models have emerged [124], like Sentence-BERT [96] and BERTopic [57]. Recently, the foundation models like ChatGPT and StarCoder [72] have demonstrated outstanding performance on a multitude of tasks related to documents and code. Zhang et al. [123] illustrated that ChatGPT is at the initial level of general intelligence. Prompt [75] technique is critical for these foundation models. Liu et al. [75] systemically investigated prompt engineering in NLP and indicated that research on prompt theory should be enhanced.

[11] https://rekt.news/ronin-rekt/

5 Threats to Validity

In this study, there are some threats-to-validity factors that need to be considered. First, this study primarily focuses on existing DeFi projects and is limited to the global analysis of governance issues. The samples chosen in our study may be affected by selection bias. The DeFi ecosystem is diverse and evolving quickly, with new projects and governance issues emerging. An incomplete sample set may result in biases in the analysis. It is possible that the current research findings may not fully cover future trends in DeFi development. Another issue is that many audit reports do not come with the DeFi category. Therefore, our sample set may not be balanced across different types of DeFi projects and thus the conclusions derived may not be generalized to some specific types of projects. In order to address this problem, we selected up to 17 reputable Web3 security companies and collected over 4,000 audit reports, aiming to include a diverse range of DeFi application projects. Second, we filtered the data using keywords, and further analysis and summaries were conducted using the topic model, BERTopic [57]. While this approach provides a strong analytical framework, there is still some level of subjective judgment when it comes to extracting and interpreting key themes because of the potential bias of AI models. To reduce its impact, the authors conducted multiple independent analysis, and engaged in careful discussions and negotiations to reach a consensus.

6 Conclusion

This article presents a comprehensive study of governance issues in DeFi applications. Drawing on the existing research literature and industry blogs, we propose a novel taxonomy for DeFi governance issues. To analyze governance issues, we collected 4,446 audit reports from 17 reputable Web3 security companies. We identified in the audit reports that 7,346 issues were related to governance according to the governance taxonomy. We discovered that most of the governance problems are associated with ownership and incentive mechanisms. Although governance issues constitute a significant portion of severe problems, the resolution rate for these issues is unsatisfactory. We have observed that the security measures at the design level implemented by the project are inadequate. We found that issues related to DeFi governance design have not received enough attention from project teams and auditors. Although these issues are not directly linked to contract vulnerabilities, they do impact the distribution of benefits across the entire project. Through the analysis of additional 15 DeFi projects, we observed that this discrepancy between the governance design and real-world implementation might be a widespread issue. Our research offers significant insights for researchers, project developers, users, and regulatory bodies. Through this study, we hope to help the public better understand and address governance challenges, thereby promoting the healthy development of DeFi.

References

[1] How We Safeguard Our Smart Contracts (and Governance). 2019. Retrieved from https://blog.oceanprotocol.com/making-ocean-protocols-smart-contracts-and-it-s-governance-unstoppable-45cf99dc1b65
[2] ACM Digital Library. 2023. Retrieved from https://dl.acm.org/
[3] arXiv. 2023. Retrieved from https://arxiv.org/
[4] Connected Papers. 2023. Retrieved from https://www.connectedpapers.com/
[5] Followeraudit. 2023. Retrieved from https://www.followeraudit.com/
[6] How to Set up On-Chain Governance. 2023. Retrieved from https://docs.openzeppelin.com/contracts/4.x/governance
[7] IEEE Xplore. 2023. Retrieved from https://ieeexplore.ieee.org/Xplore/home.jsp
[8] Scopus. 2023. Retrieved from https://www.scopus.com/
[9] Smart Contracts Audit and Security. 2023. Retrieved from https://etherscan.io/directory/Smart_Contracts/Smart_Contracts_Audit_And_Security,timestamp19/07/2023
[10] Aly Abdelrazek, Yomna Eid, Eman Gawish, Walaa Medhat, and Ahmed Hassan. 2023. Topic modeling algorithms and applications: A survey. *Information Systems* 112 (2023), 102131.
[11] Darcy W. E. Allen and Chris Berg. 2020. Blockchain governance: What we can learn from the economics of corporate governance. *The Journal of the British Blockchain Association* 3, 1 (2020), 1–10.

[12] Darcy W. E. Allen, Chris Berg, Aaron M. Lane, Trent MacDonald, and Jason Potts. 2023. The exchange theory of web3 governance. *Kyklos* 76, 4 (2023), 659–675.
[13] The List of Searched Articles. 2023. Retrieved from https://docs.google.com/spreadsheets/d/1CzTdtF-4ufHBh9_js9U01PgLL4eus1LO/edit?usp=drive_link&ouid=111813213768125351842&rtpof=true&sd=true
[14] Adam P. Balcerzak, Elvira Nica, Elżbieta Rogalska, Miloš Poliak, Tomáš Klieštik, and Oana-Matilda Sabie. 2022. Blockchain technology and smart contracts in decentralized governance systems. *Administrative Sciences* 12, 3 (2022), 96.
[15] E. Baninemeh, S. Farshidi, and S. Jansen. 2023. A decision model for decentralized autonomous organization platform selection: Three industry case studies. *Blockchain: Research and Applications* 4, 2 (2023), 100127. DOI: https://doi.org/10.1016/j.bcra.2023.100127
[16] Tom Barbereau, Reilly Smethurst, Orestis Papageorgiou, Johannes Sedlmeir, and Gilbert Fridgen. 2023. Decentralised finance's timocratic governance: The distribution and exercise of tokenised voting rights. *Technology in Society* 73 (2023), 102251. DOI: https://doi.org/10.1016/j.techsoc.2023.102251
[17] Massimo Bartoletti, James Hsin-yu Chiang, and Alberto Lluch Lafuente. 2021. Towards a theory of decentralized finance. In *International Workshops on Financial Cryptography and Data Security (FC '21)*. Matthew Bernhard, Andrea Bracciali, Lewis Gudgeon, Thomas Haines, Ariah Klages-Mundt, Shin'ichiro Matsuo, Daniel Perez, Massimiliano Sala, and Sam Werner (Eds.), Springer, Berlin, 227–232.
[18] Roman Beck, Christoph Müller-Bloch, and John Leslie King. 2018. Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information Systems* 19, 10 (2018), 1.
[19] Felix Bekemeier. 2021. Deceptive assurance? A conceptual view on systemic risk in decentralized finance (DeFi). In *2021 4th International Conference on Blockchain Technology and Applications*. ACM, New York, NY, 76–87. DOI: https://doi.org/10.1145/3510487.3510499
[20] Siddharth Bhambhwani. 2023. Governing Decentralized Finance (DeFi). *SSRN* 4513325. Retrieved from 4513325
[21] Siddharth M. Bhambhwani. 2022. Governing Decentralized Finance (Defi). *SSRN* 4225775. Retrieved from https://ssrn.com/abstract=4225775
[22] Binance. 2022. What Are Governance Tokens? Retrieved from https://www.binance.com/bg/feed/post/42812
[23] Binance. 2022. What Is Tokenomics and Why Does It Matter? Retrieved from https://academy.binance.com/en/articles/what-is-tokenomics-and-why-does-it-matter
[24] Binance. 2023. How DeFi Protocols Generate Revenue and Why It's Important. Retrieved from https://academy.binance.com/en/articles/how-defi-protocols-generate-revenue-and-why-it-s-important
[25] Mike Alonso, Auer A. Raphael, Bluhm Marcel, Borio Claudio, Claessens Stijn, Doerr Sebastian, Frost Jon, Kosse Anneke, Khan Asad, Huang Wenqian, et al. 2021. DeFi Risks and the Decentralisation Illusion1. Retrieved from https://www.bis.org/publ/qtrpdf/r_qt2112b.pdf
[26] Agostino Capponi, Garud Iyengar, and Jay Sethuraman. 2023. Decentralized finance: Protocols, risks, and governance. *Foundations and Trends® in Privacy and Security* 5, 3 (2023), 144–188.
[27] Certik. 2022. NFN-02, Security Assessment Notable. Retrieved from https://certik-public-assets.s3.amazonaws.com/CertiK-Audit-for-Notable-v5.pdf
[28] Certik. 2022. TFF-01, Tokensfarm. Retrieved from https://certik-public-assets.s3.amazonaws.com/CertiK-Audit-for-Tokensfarm-v5-v9.pdf
[29] Certik. 2023. Security Considerations When Designing Blockchain Governance Systems. Retrieved from https://www.certik.com/resources/blog/1oil2sf9hiNQL4ucVxqsrM-security-considerations-when-designing-blockchain-governance-systems
[30] CertikGovernance. 2021. Skynet Security Primitive 3: Governance. Retrieved from https://www.certik.com/resources/blog/SkynetGovernance
[31] Chainsulting. 2022. 6.6.1 Initialze Not Protected, CrowdSwap Staking. Retrieved from https://github.com/CrowdSwap/audits/blob/main/02_Smart_Contract_Audit_CrowdSwap_Staking.pdf
[32] Stefanos Chaliasos, Denis Firsov, and Benjamin Livshits. 2024. Towards a formal foundation for blockchain rollups. arXiv:2406.16219. Retrieved from https://arxiv.org/abs/2406.16219
[33] Amit Chaudhary, Roman Kozhan, and Ganesh Viswanath-Natraj. 2023. Interest rate rules in decentralized finance: Evidence from compound. In *4th International Conference on Blockchain Economics, Security and Protocols (Tokenomics '22)*, 5:1–5:6. Schloss Dagstuhl-Leibniz-Zentrum für Informatik.
[34] Rob Churchill and Lisa Singh. 2022. The evolution of topic modeling. *ACM Computing Surveys* 54, 10s (2022), 1–35.
[35] DeFisec. 2023. How to Spot Hidden Mint Functions. Retrieved from https://defisec.info/how_to_spot_hidden_mint_functions
[36] Jacob Devlin, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova. 2018. Bert: Pre-training of deep bidirectional transformers for language understanding. arXiv:1810.04805. Retrieved from https://arxiv.org/abs/1810.04805
[37] Damiano Di Francesco Maesa and Paolo Mori. 2020. Blockchain 3.0 applications survey. *Journal of Parallel and Distributed Computing* 138 (2020), 99–114. DOI: https://doi.org/10.1016/j.jpdc.2019.12.019

[38] Laszlo Dobos. 2020. Build Finance DAO Hostile Takeover, Treasury Drained. Retrieved from https://cryptoslate.com/build-finance-dao-hostile-takeover-treasury-drained/

[39] Maya Dotan, Aviv Yaish, Hsin-Chu Yin, Eytan Tsytkin, and Aviv Zohar. 2023. The vulnerable nature of decentralized governance in DeFi. In *2023 Workshop on Decentralized Finance and Security (DeFi '23)*. ACM, New York, NY, 25–31. DOI: https://doi.org/10.1145/3605768.3623539

[40] Taner Dursun and Burak Berk Üstündağ. 2021. A novel framework for policy based on-chain governance of blockchain networks. *Information Processing & Management* 58, 4 (2021), 102556. DOI: https://doi.org/10.1016/j.ipm.2021.102556

[41] Paul M. Duvall, Steve Matyas, and Andrew Glover. 2007. *Continuous Integration: Improving Software Quality and Reducing Risk*. Pearson Education.

[42] Hassan Hamid Ekal and Shams N. Abdul-wahab. 2022. DeFi governance and decision-making on blockchain. *Mesopotamian Journal of Computer Science* 2022 (2022), 9–16.

[43] Maarten Everts and Erik Weitenberg (TNO). 2018. Smart Governance for Smart Contracts. Retrieved from https://dutchblockchaincoalition.org/assets/images/default/DBC-Rapport-Smart-governance-for-smart-contracts.pdf

[44] Esatya. 2018. All You Want to Know about DeFi Governance? Retrieved from https://esatya.io/blogs/all-you-want-to-know-about-defi-governance

[45] Ethereum. 2023. Introduction to Ethereum Governance. Retrieved from https://ethereum.org/en/governance/

[46] Ethereum. 2023. Upgrading Smart Contracts. Retrieved from https://ethereum.org/gl/developers/docs/smart-contracts/upgrading/

[47] Eurofi. 2022. Decentralized Finance (DeFi): Opportunities, Challenges and Policy Implications. Retrieved from https://www3.weforum.org/docs/WEF_DeFi_Policy_Maker_Toolkit_2021.pdf

[48] Rainer Feichtinger, Robin Fritsch, Yann Vonlanthen, and Roger Wattenhofer. 2024. The hidden shortcomings of (D)AOs—An empirical study of on-chain governance. In *Financial Cryptography and Data Security (FC '23 International Workshops)*. Aleksander Essex, Shin'ichiro Matsuo, Oksana Kulyk, Lewis Gudgeon, Ariah Klages-Mundt, Daniel Perez, Sam Werner, Andrea Bracciali, and Geoff Goodell (Eds.), Springer Nature, Switzerland, Cham, 165–185.

[49] Josselin Feist, Gustavo Grieco, and Alex Groce. 2019. Slither: A static analysis framework for smart contracts. In 2019 IEEE/*ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB). IEEE*, 8–15.

[50] Daniel Ferreira, Jin Li, and Radoslawa Nikolowa. 2023. Corporate capture of blockchain governance. *The Review of Financial Studies* 36, 4 (2023), 1364–1407.

[51] Stefania Fiorentino and Silvia Bartolucci. 2021. Blockchain-based smart contracts as new governance tools for the sharing economy. *Cities* 117 (2021), 103325.

[52] Robin Fritsch, Marino Müller, and Roger Wattenhofer. 2024. Analyzing voting power in decentralized governance: Who controls DAOs? *Blockchain: Research and Applications* 5, 3 (2024), 100208.

[53] Alessandro Fusco. 2021. *Decentralized Applications: An Empirical Analysis of Their Revenue Models and Governance Systems*. Master's thesis. Politecnico di Milano. Retrieved from https://www.politesi.polimi.it/handle/10589/179487?mode=simple

[54] Weichao Gao, William G. Hatcher, and Wei Yu. 2018. A survey of blockchain: Techniques, applications, and challenges. In *2018 27th International Conference on Computer Communication and Networks (ICCCN)*, 1–11. DOI: https://doi.org/10.1109/ICCCN.2018.8487348

[55] David Gogel. 2021. DeFi beyond the hype: The emerging world of decentralized finance. In *Collab. with Wharton Blockchain and Digital Asset Project and World Economic Forum*. Wharton. Retrieved from https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf

[56] Upgrades Governance. 2023. Upgrades Governance. Retrieved from https://docs.zeppelinos.org/docs/2.4.0/upgrades_governance

[57] Maarten Grootendorst. 2022. BERTopic: Neural topic modeling with a class-based TF-IDF procedure. arXiv:2203.05794. Retrieved from https://arxiv.org/abs/2203.05794

[58] Jens J. Hunhevicz, Pierre-Antoine Brasey, Marcella M. M. Bonanomi, Daniel M. Hall, and Martin Fischer. 2022. Applications of blockchain for the governance of integrated project delivery: A crypto commons approach. arXiv:2207.07002. Retrieved from https://arxiv.org/abs/2207.07002

[59] Johannes Rude Jensen, Victor von Wachter, and Omri Ross. 2021. How decentralized is the governance of blockchain-based finance: Empirical evidence from four governance token distributions. arXiv:2102.10096. Retrieved from https://arxiv.org/abs/2102.10096

[60] Johannes Rude Jensen, Victor von Wachter, and Omri Ross. 2021. an introduction to decentralized finance (DeFi). *Complex Systems Informatics and Modeling Quarterly* 26 (2021), 46–54. Retrieved from https://api.semanticscholar.org/CorpusID:234500185

[61] Bo Jiang, Ye Liu, and Wing Kwong Chan. 2018. ContractFuzzer: Fuzzing smart contracts for vulnerability detection. In *33rd ACM/IEEE International Conference on Automated Software Engineering*, 259–269.

[62] Erya Jiang, Bo Qin, Qin Wang, Zhipeng Wang, Qianhong Wu, Jian Weng, Xinyu Li, Chenyang Wang, Yuhang Ding, and Yanran Zhang. 2023. Decentralized finance (DeFi): A survey. arXiv:2308.05282. Retrieved from https://arxiv.org/abs/2308.05282

[63] Wulf A. Kaal. 2020. Blockchain-based corporate governance. *Stanford Journal of Blockchain Law & Policy* 4 (2020), 3.

[64] Nida Khan, Tabrez Ahmad, Anass Patel, and Radu State. 2020. Blockchain governance: An overview and prediction of optimal strategies using Nash equilibrium. arXiv:2003.09241. Retrieved from https://arxiv.org/abs/2003.09241

[65] Aida Manzano Kharman and Ben Smyth. 2024. Perils of current DAO governance. arXiv:2406.08605. Retrieved from https://arxiv.org/abs/2406.08605

[66] Aggelos Kiayias and Philip Lazos. 2022. SoK: Blockchain governance. arXiv:2201.07188. Retrieved from https://arxiv.org/abs/2201.07188

[67] Suntae Kim and Dongsun Kim. 2016. Automatic identifier inconsistency detection using code dictionary. *Empirical Software Engineering* 21 (2016), 565–604.

[68] Destan Kirimhan. 2023. Importance of anti-money laundering regulations among prosumers for a cybersecure decentralized finance. *Journal of Business Research* 157 (2023), 113558. DOI: https://doi.org/10.1016/j.jbusres.2022.113558

[69] Roman Kozhan and Ganesh Viswanath-Natraj. 2022. Fundamentals of the MakerDAO governance token. In *3rd International Conference on Blockchain Economics, Security and Protocols (Tokenomics '21), Open Access Series in Informatics (OASIcs)*. Vincent Gramoli, Hanna Halaburda, and Rafael Pass (Eds.), Vol. 97, Schloss Dagstuhl–Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 11:1–11:5. DOI: https://doi.org/10.4230/OASIcs.Tokenomics.2021.11

[70] Gabriella Laatikainen, Mengcheng Li, and Pekka Abrahamsson. 2021. Blockchain governance: A dynamic view. In *Software Business*. Xiaofeng Wang, Antonio Martini, Anh Nguyen-Duc, and Viktoria Stray (Eds.), Springer International Publishing, Cham, 66–80.

[71] Chao Li, Balaji Palanisamy, Runhua Xu, Li Duan, Jiqiang Liu, and Wei Wang. 2023. How hard is takeover in DPoS blockchains? Understanding the security of coin-based voting governance. In *2023 ACM SIGSAC Conference on Computer and Communications Security (CCS '23). ACM, New York, NY*, 150–164. DOI: https://doi.org/10.1145/3576915.3623171

[72] Raymond Li, Loubna Ben Allal, Yangtian Zi, Niklas Muennighoff, Denis Kocetkov, Chenghao Mou, Marc Marone, Christopher Akiki, Jia Li, Jenny Chim, et al. 2023. StarCoder: May the source be with you! arXiv:2305.06161. Retrieved from https://arxiv.org/abs/2305.06161

[73] Wenkai Li, Jiuyang Bu, Xiaoqi Li, Hongli Peng, Yuanzheng Niu, and Yuqing Zhang. 2022. A survey of DeFi security: Challenges and opportunities. *Journal of King Saud University–Computer and Information Sciences* 34, 10, Part B (2022), 10378–10404. DOI: https://doi.org/10.1016/j.jksuci.2022.10.028

[74] R. Liang, J. Chen, K. He, Y. Wu, G. Deng, R. Du, and C. Wu. 2024. PonziGuard: Detecting Ponzi schemes on Ethereum with contract runtime behavior graph (CRBG). In *2024 IEEE/ACM 46th International Conference on Software Engineering (ICSE)*. IEEE Computer Society, Los Alamitos, CA, 755–766. DOI: https://doi.ieeecomputersociety.org/

[75] Pengfei Liu, Weizhe Yuan, Jinlan Fu, Zhengbao Jiang, Hiroaki Hayashi, and Graham Neubig. 2023. Pre-train, prompt, and predict: A systematic survey of prompting methods in natural language processing. *ACM Computing Surveys* 55, 9, Article 195 (Jan. 2023), 35 pages. DOI: https://doi.org/10.1145/3560815

[76] Ye Liu, Yi Li, Shang-Wei Lin, and Rong Zhao. 2020. Towards automated verification of smart contract fairness. In *28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE '20)*. ACM, New York, NY, 666–677. DOI: https://doi.org/10.1145/3368089.3409740

[77] Yue Liu, Qinghua Lu, Guangsheng Yu, Hye-Young Paik, Harsha Perera, and Liming Zhu. 2022. A pattern language for blockchain governance. In *27th European Conference on Pattern Languages of Programs*, 1–16.

[78] Yue Liu, Qinghua Lu, Guangsheng Yu, Hye-Young Paik, and Liming Zhu. 2022. Defining blockchain governance principles: A comprehensive framework. *Information Systems* 109 (2022), 102090. DOI: https://doi.org/10.1016/j.is.2022.102090

[79] Yue Liu, Qinghua Lu, Liming Zhu, Hye-Young Paik, and Mark Staples. 2023. A systematic literature review on blockchain governance. *Journal of Systems and Software* 197 (2023), 111576. DOI: https://doi.org/10.1016/j.jss.2022.111576

[80] Jonathan Mellon, Jack Bailey, Ralph Scott, James Breckwoldt, Marta Miori, and Phillip Schmedeman. 2024. Do AIs know what the most important issue is? Using language models to code open-text social survey responses at scale. *Research and Politics*, 11, 1 (2024). DOI: https://doi.org/10.1177/20531680241231468

[81] Messari. 2023. Governor Note: Evolving On-Chain Governance with Element Council. Retrieved from https://messari.io/report/governor-note-evolving-on-chain-governance-with-element-council

[82] Johnnatan Messias, Vabuk Pahari, Balakrishnan Chandrasekaran, Krishna P. Gummadi, and Patrick Loiseau. 2023. Understanding blockchain governance: Analyzing decentralized voting to amend DeFi smart contracts. arXiv:2305.17655. Retrieved from https://arxiv.org/abs/2305.17655

[83] Eva Meyer, Isabell M. Welpe, and Philipp G. Sandner. 2022. Decentralized finance—A systematic literature review and research directions. ECIS 2022 Research Papers. Retrieved from https://aisel.aisnet.org/ecis2022_rp/25

[84] OECD. 2022. Why Decentralised Finance (DeFi) Matters and the Policy Implications. OECD Publishing, Paris. DOI: https://doi.org/10.1787/109084ae-en

[85] Sheena Panthaplackel, Junyi Jessy Li, Milos Gligoric, and Raymond J. Mooney. 2021. Deep just-in-time inconsistency detection between comments and source code. In *AAAI Conference on Artificial Intelligence*, Vol. 35, 427–435.

[86] PeckShield. 2020. *3.2 Front-Running of Proposal Tally, Smart Contract Audit Report for Nodeex Holdings Limited*. Retrieved from https://github.com/peckshield/publications/blob/master/audit_reports/PeckShield-Audit-Report-OneSwap-v1.0.pdf

[87] PeckShield. 2020. Voting Amplification with Sybil Attack, Smart Contract Audit Report for LuckyChip Token. Retrieved from https://github.com/peckshield/publications/blob/master/audit_reports/PeckShield-Audit-Report-ERC20-LuckyChip-v1.0.pdf

[88] Rowan van Pelt, Slinger Jansen, Djuri Baars, and Sietse Overbeek. 2021. Defining blockchain governance: A framework for analysis and comparison. *Information Systems Management* 38, 1 (2021), 21–41.

[89] Kai Petersen, Sairam Vakkalanka, and Ludwik Kuzniarz. 2015. Guidelines for conducting systematic mapping studies in software engineering: An update. *Information and Software Technology* 64 (2015), 1–18. DOI: https://doi.org/10.1016/j.infsof.2015.03.007

[90] Polygon. 2023. Polygon Introduces Governance 2.0 with Proposed Protocol Council for Smart Contract Upgrades. Retrieved from https://www.bitcoininsider.org/article/230047/polygon-introduces-governance-20-proposed-protocol-council-smart-contract-upgrades

[91] Quantstamp. 2020. *QSP-3, DerivaDEX*. Retrieved from https://certificate.quantstamp.com/full/deriva-dex.pdf

[92] Fazle Rabbi and Md Saeed Siddik. 2020. Detecting code comment inconsistency using Siamese recurrent network. In *28th International Conference on Program Comprehension*, 371–375.

[93] Pooja Rani, Arianna Blasi, Nataliia Stulova, Sebastiano Panichella, Alessandra Gorla, and Oscar Nierstrasz. 2023. A decade of code comment quality assessment: A systematic literature review. *Journal of Systems and Software* 195 (2023), 111515. DOI: https://doi.org/10.1016/j.jss.2022.111515

[94] Ezra Reguerra. 2022. CertiK Identifies Arbix Finance as a Rug Pull, Warns Users to Steer Clear. Retrieved from https://cointelegraph.com/news/certik-identifies-arbix-finance-as-a-rug-pull-warns-users-to-steer-clear

[95] Muhammad Habib ur Rehman, Khaled Salah, Ernesto Damiani, and Davor Svetinovic. 2020. Trust in blockchain cryptocurrency ecosystem. *IEEE Transactions on Engineering Management* 67, 4 (2020), 1196–1212. DOI: https://doi.org/10.1109/TEM.2019.2948861

[96] Nils Reimers and Iryna Gurevych. 2019. Sentence-BERT: Sentence embeddings using Siamese BERT-networks. In *Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing (EMNLP-IJCNLP)*. Association for Computational Linguistics, 3982–3992. Retrieved from http://arxiv.org/abs/1908.10084

[97] Pranav Garimidi, Scott Duke Kominers, and Tim Roughgarden. 2020. DAO Governance Attacks, and How to Avoid Them. Retrieved from https://a16zcrypto.com/posts/article/dao-governance-attacks-and-how-to-avoid-them/

[98] Carlos Santana and Laura Albareda. 2022. Blockchain and the emergence of decentralized autonomous organizations (DAOs): An integrative model and research agenda. *Technological Forecasting and Social Change* 182 (2022), 121806. DOI: https://doi.org/10.1016/j.techfore.2022.121806

[99] Bettina Schneider, Ruben Ballesteros, Pascal Moriggl, and Petra M. Asprion. 2022. Decentralized Autonomous Organizations–Evolution, Challenges, and Opportunities. In *Proceedings of the PoEM 2022 Workshops and Models at Work*. Dominik Bork, Souvik Barat, Petra Asprion, Alessandro Marcelletti, Andrea Morichetta, Bettina Schneider, Vinay Kulkarni, Ruth Breu and Philipp Zech (Eds.), Verfügbar unter, London. DOI: https://doi.org/10.26041/fhnw-7346

[100] Openzeppelin Security. 2022. Everyone Can Deploy New Comet Instances, Compound III Audit. Retrieved from https://blog.openzeppelin.com/compound-iii-audit#everyone-can-deploy-new-comet-instances

[101] Kaushal Shah, Dhruvil Lathiya, Naimish Lukhi, Keyur Parmar, and Harshal Sanghvi. 2023. A systematic review of decentralized finance protocols. *International Journal of Intelligent Networks* 4 (2023), 171–181. DOI: https://doi.org/10.1016/j.ijin.2023.07.002

[102] Trishie Sharma, Rachit Agarwal, and Sandeep Kumar Shukla. 2023. Understanding rug pulls: An in-depth behavioral analysis of fraudulent NFT creators. *ACM Transactions on the Web* 18, 1, Article 8 (Oct. 2023), 39 pages. DOI: https://doi.org/10.1145/3623376

[103] Kabir Manandhar Shrestha, Katie Wood, D. Goodman, and M. Mistica. 2023. Do we need subject matter experts? A case study of measuring up GPT-4 against scholars in topic evaluation. In *7th Workshop on Natural Language for Artificial Intelligence (NL4AI '23) Co-Located with 22th International Conference of the Italian Association for Artificial Intelligence (AI* IA '23)*.

[104] Munindar P. Singh and Amit K. Chopra. 2020. Computational governance and violable contracts for blockchain applications. *Computer* 53, 1 (2020), 53–62.
[105] Solidified. 2018. Audit Report for Coder Inc. Retrieved from https://drive.google.com/file/d/1EcY6rE5gVgfDa_XeI6_c7ud_0DLfifUT/view?usp=sharing
[106] Statista. 2022. Decentralized Finance (DeFi)—Statistics & Facts. Retrieved from https://www.statista.com/topics/8444/decentralized-finance-defi/#topicOverview
[107] Dianxiang Sun, Wei Ma, Liming Nie, and Yang Liu. 2024. SoK: Comprehensive analysis of rug pull causes, datasets, and detection tools in DeFi. arXiv:2403.16082. Retrieved from https://arxiv.org/abs/2403.16082
[108] Xiaotong Sun, Charalampos Stasinakis, and Georigios Sermpinis. 2022. Decentralization Illusion in Decentralized Finance: Evidence from Tokenized Voting in MakerDAO Polls. Retrieved from https://api.semanticscholar.org/CorpusID:257687911
[109] Evrim Tan, Stanislav Mahula, and Joep Crompvoets. 2022. Blockchain governance in the public sector: A conceptual framework for public management. *Government Information Quarterly* 39, 1 (2022), 101625. DOI: https://doi.org/10.1016/j.giq.2021.101625
[110] Wen Siang Tan, Markus Wagner, and Christoph Treude. 2024. Detecting outdated code element references in software repository documentation. *Empirical Software Engineering* 29, 1 (2024), 5.
[111] Christof Ferreira Torres, Mathis Steichen, and Radu State. 2019. The art of the scam: Demystifying honeypots in Ethereum smart contracts. In *28th USENIX Security Symposium (USENIX Security '19)*, 1591–1607.
[112] Arianna Trozze, Toby Davies, and Bennett Kleinberg. 2023. Of degens and defrauders: Using open-source investigative tools to investigate decentralized finance frauds and money laundering. *Forensic Science International: Digital Investigation* 46 (2023), 301575.
[113] Marc Truchet. 2022. Decentralized Finance (DeFi): Opportunities, Challenges and Policy Implications. Retrieved from https://www.eurofi.net/wp-content/uploads/2022/05/eurofi_decentralized-finance-defi_opportunities-challenges-and-policy-implications_paris_february-2022.pdf
[114] Uniswap V1. 2018. The Uniswap V1 Smart Contracts. Retrieved from https://docs.uniswap.org/contracts/v1/overview
[115] Uniswap V2. 2020. Governance Reference. Retrieved from https://docs.uniswap.org/contracts/v2/reference/Governance/governance-reference
[116] Shuai Wang, Wenwen Ding, Juanjuan Li, Yong Yuan, Liwei Ouyang, and Fei-Yue Wang. 2019. Decentralized autonomous organizations: Concept, model, and applications. *IEEE Transactions on Computational Social Systems* 6, 5 (2019), 870–878.
[117] Fengcai Wen, Csaba Nagy, Gabriele Bavota, and Michele Lanza. 2019. A large-scale empirical study on code-comment inconsistencies. In *2019 IEEE/ACM 27th International Conference on Program Comprehension (ICPC)*, 53–64. DOI: https://doi.org/10.1109/ICPC.2019.00019
[118] Johannes Werner, Sebastian Frost, and Rüdiger Zarnekow. 2020. Towards a taxonomy for governance mechanisms of blockchain-based platforms. In *Proceedings of the 28th European Conference on Information Systems (ECIS), An Online AIS Conference*. Retrieved from https://aisel.aisnet.org/ecis2020_rp/26
[119] Sam Werner, Daniel Perez, Lewis Gudgeon, Ariah Klages-Mundt, Dominik Harz, and William Knottenbelt. 2022. Sok: Decentralized finance (DeFi). In *4th ACM Conference on Advances in Financial Technologies* (*AFT '22*). ACM, New York, NY, 30–46. DOI: 10.1145/3558535.3559780
[120] WIFPR. 2021. DeFi beyond the Hype: The Emerging World of Decentralized Finance. Retrieved from https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf
[121] Jiahua Xu, Daniel Perez, Yebo Feng, and Benjamin Livshits. 2023. Auto.gov: Learning-based on-chain governance for decentralized finance (DeFi). arXiv:2302.09551. Retrieved from https://arxiv.org/abs/2302.09551
[122] Dirk A. Zetzsche, Douglas W. Arner, and Ross P. Buckley. 2020. Decentralized finance (DeFi). *Journal of Financial Regulation* 6 (2020), 172–203.
[123] Chaoning Zhang, Chenshuang Zhang, Chenghao Li, Yu Qiao, Sheng Zheng, Sumit Kumar Dam, Mengchun Zhang, Jung Uk Kim, Seong Tae Kim, Jinwoo Choi, et al. 2023. One small step for generative AI, one giant leap for AGI: A complete survey on ChatGPT in AIGC era. arXiv:2304.06488. Retrieved from https://arxiv.org/abs/2304.06488
[124] He Zhao, Dinh Phung, Viet Huynh, Yuan Jin, Lan Du, and Wray Buntine. 2021. Topic modelling meets deep neural networks: A survey. arXiv:2103.00498. Retrieved from https://arxiv.org/abs/2103.00498
[125] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang. 2018. Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services* 14, 4 (2018), 352–375.
[126] Haozhe Zhou, Amin Milani Fard, and Adetokunbo Makanju. 2022. The state of Ethereum smart contracts security: Vulnerabilities, countermeasures, and tool support. *Journal of Cybersecurity and Privacy* 2, 2 (2022), 358–378. DOI: https://doi.org/10.3390/jcp2020019

Received 11 January 2024; revised 23 September 2024; accepted 29 January 2025