I Experienced More than 10 DeFi Scams: On DeFi Users' Perception of Security Breaches and Countermeasures

Mingyi Liu, *Georgia Institute of Technology;* Jun Ho Huh, *Samsung Research;* HyungSeok Han, Jaehyuk Lee, Jihae Ahn, and Frank Li, *Georgia Institute of Technology;* Hyoungshick Kim, *Sungkyunkwan University;* Taesoo Kim, *Georgia Institute of Technology*

https://www.usenix.org/conference/usenixsecurity24/presentation/liu-mingyi

This paper is included in the Proceedings of the 33rd USENIX Security Symposium.

August 14–16, 2024 • Philadelphia, PA, USA

978-1-939133-44-1

Open access to the Proceedings of the 33rd USENIX Security Symposium is sponsored by USENIX.

I Experienced More than 10 DeFi Scams: On DeFi Users' Perception of Security Breaches and Countermeasures

Mingyi Liu[1], Jun Ho Huh[2], HyungSeok Han[1], Jaehyuk Lee[1], Jihae Ahn[1], Frank Li[1], Hyoungshick Kim[3], and Taesoo Kim[1]

[1]*Georgia Institute of Technology*
[2]*Samsung Research*
[3]*Sungkyunkwan University*

Abstract

Decentralized Finance (DeFi) offers a whole new investment experience and has quickly emerged as an enticing alternative to Centralized Finance (CeFi). Rapidly growing market size and active users, however, have also made DeFi a lucrative target for scams and hacks, with 1.95 billion USD lost in 2023. Unfortunately, no prior research thoroughly investigates DeFi users' security risk awareness levels and the adequacy of their risk mitigation strategies.

Based on a semi-structured interview study ($N = 14$) and a follow-up survey ($N = 493$), this paper investigates DeFi users' security perceptions and commonly adopted practices, and how those affected by previous scams or hacks (DeFi victims) respond and try to recover their losses. Our analysis shows that users often prefer DeFi over CeFi due to their decentralized nature and strong profitability. Despite being aware that DeFi, compared to CeFi, is prone to more severe attacks, users are willing to take those risks to explore new investment opportunities. Worryingly, most victims do not learn from previous experiences; unlike victims studied through traditional systems, DeFi victims tend to find new services, without revising their security practices, to recover their losses quickly. The abundance of various DeFi services and opportunities allows victims to continuously explore new financial opportunities, and this reality seems to cloud their security priorities. Indeed, our results indicate that DeFi users' strong financial motivations outweigh their security concerns – much like those who are addicted to gambling. Our observations about victims' post-incident behaviors suggest that stronger control in the form of industry regulations would be necessary to protect DeFi users from future breaches.

1 Introduction

Decentralized Finance (DeFi) is a financial ecosystem built on blockchain platforms like Ethereum. It provides a variety of financial services, mainly executed through smart contracts [48], such as Decentralized Exchanges (DEXs) and lending services. This emerging field has attracted substantial interest, with its Total Value Locked (TVL) reaching a record high of 180 billion USD in November 2021 [17].

With its growing popularity, DeFi has become an attractive target for hacks and scams, which we also refer to as DeFi incidents. The total loss resulting from DeFi incidents in 2023 exceeded 1.95 billion USD [16]. Popular DEXs such as Balancer, Curve Finance, and dYdX were breached due to smart contract vulnerabilities [3, 14, 20]. Additionally, over 263 rug-pull scams were reported in 2023 [16]. The infamous LUNA meltdown (reported in 2022) failed to protect its stablecoin values, incurring a total loss of 60 billion USD [4].

Despite reports being published about numerous DeFi incidents and their losses, people are still heavily using DeFi, and its TVL remains at 130 billion USD in 2024 [17]. Such trends motivated this work and two intriguing aspects: (1) despite the prevalence of security breaches being reported, why do people continue to use DeFi services, and (2) whether people make decisions based on an adequate understanding of security risks and mitigation practices. To date, there is no prior research that thoroughly investigates DeFi users' perceptions of security risks. Prior efforts often focused on smart contract security [10, 26, 38, 49]. Wang *et al.* [46] studied user perceptions of DeFi incidents. However, their investigations were limited to the scope of sandwich attacks.

To bridge this gap, we conducted a semi-structured interview with 14 DeFi users, including real-world victims, and a follow-up online survey ($N = 493$), investigating DeFi users' security risk awareness levels and the adequacy of commonly employed security practices, and how real-world victims respond to DeFi breaches and mitigate risks. These studies have been designed to address the following four research questions:

RQ1: Why do people continue to use DeFi despite numerous DeFi incidents being reported? Traditional Centralized Finance (CeFi) or bank users typically abandon their banks if serious incidents are reported [24]. Our curiosity lies in understanding why DeFi users behave differently.

RQ2: What DeFi risks are users concerned about, and how do they mitigate these risks? DeFi systems introduce unique security risks [52]. Our objective is to understand whether DeFi users have sufficient knowledge about the overall threat landscape, and the security controls that need to be used.

RQ3: How do victims respond to DeFi incidents? Another objective is to understand what actions are taken by victims after experiencing scams or hacks, and investigate the adequacy of their actions in recovering their losses. Our investigation extends to understanding how victims' perceptions change after the incident.

RQ4: How do DeFi users perceive regulation? Regulatory controls may be considered in the future to better protect DeFi users. To that end, we were driven to understand DeFi users' perceived benefits and concerns with respect to introducing regulatory controls.

Our qualitative and quantitative studies reveal that people choose DeFi services because they appreciate its decentralized nature, and the unique investment opportunities they offer (**RQ1**). Many participants consider DeFi to be less secure than CeFi. However, such participants still appreciate the transparency and trustworthiness guarantees of DeFi services, and continue using them anyway. Participants are mainly concerned about rug-pull scams, volatility of crypto prices, and smart contract exploitation (**RQ2**). However, many of them do not know how to effectively mitigate such threats. They often believe that traditional security systems are applicable and equally effective in protecting them from DeFi threats. For instance, many participants falsely believe two-factor authentication (2FA) will mitigate rug-pull or smart contract exploitation types of breaches. Worryingly, many victims simply find other DeFi services, and continue to use them to recover their losses (**RQ3**). Such victims fail to take any other remedy actions, and do not revise their security practices. Surprisingly, more than half of the studied victims explained that their security perceptions did not change after the incident. It seems like their overwhelming financial motivations cloud their security priorities: many participants fall victim to multiple scam or hack incidents, and still use DeFi without carefully considering the security risks. As expected, more participants oppose the idea of regulating DeFi services (**RQ4**) – mainly due to their concerns about paying additional tax and regulatory controls possibly jeopardizing the decentralization benefits of DeFi. Considering that paying tax is a civil obligation, however, and users' tendency to ignore security risks in pursuit of financial gains, our recommendation is to explore decentralized regulations and mandate strong security controls and practices to better protect DeFi users.

Taken together, these key findings represent the major contributions of the paper: a first formal study investigating DeFi users' security concerns and risk mitigation strategies, a list of security misconceptions that need to be addressed, and a thorough report on the security behaviors of DeFi victims and how they can be better protected in the future.

2 Background

In this section, we begin by reviewing DeFi with its characteristics and financial services. We then introduce the hacks and scams that have occurred in the DeFi realm.

2.1 Decentralized Finance (DeFi)

DeFi is a financial ecosystem backed by a blockchain such as Ethereum. These blockchains empower DeFi to have unique characteristics compared to Centralized Finance (CeFi), giving rise to the emergence of distinct DeFi services.

DeFi characteristic. Most DeFi services are implemented as smart contracts [48] on top of a blockchain. DeFi developers encode their protocols and functionalities into smart contracts and deploy them on the blockchain by sending smart contract creation transactions (txs). DeFi users then interact with DeFi services by sending txs to smart contracts of DeFi services. This makes DeFi services inherit characteristics of blockchain such as *decentralization*, *transparency*, and *accessibility*.

In particular, DeFi is *decentralized* due to its foundation on blockchain, which operates in a decentralized manner. Furthermore, the use of smart contracts as the backbone of DeFi implementations, along with recording of all tx histories on the blockchain, ensures the *transparency* of DeFi. Lastly, DeFi employs blockchain accounts, which anyone can create with a private key. DeFi operates through txs, and any account owner can initiate txs. These enhance the *accessibility* of DeFi.

DeFi service. DeFi offers many financial services inspired by CeFi while demonstrating the DeFi characteristics. Similar to CeFi, DeFi provides financial services such as exchanges and lending services. However, DeFi services operate with distinct mechanisms. For example, DEXs often utilize an automated market maker (AMM) mechanism [50], which automatically determines the exchange ratio based on the quantities of tokens in liquidity pools. Additionally, DeFi lending services introduce a unique feature called flashloan [47]. By leveraging the atomicity of blockchain transactions and the programmability of smart contracts, a flashloan allows borrowers to obtain a loan only if they repay it along with its interests within a single transaction. Notably, DeFi offers other various services such as NFTs, insurance, governances, stablecoins, and cross-chain bridges.

2.2 DeFi Hacks

Although the blockchain, the basis of DeFi, is secure, DeFi services might be insecure because of vulnerabilities in their implementations. In this paper, we categorize DeFi hacks into four categories based on the exploited components in DeFi.

Smart contract exploit. Due to the fact that most DeFi protocols are implemented through smart contracts, numerous DeFi hacks have happened by smart contract exploits, resulting in at least 1.57 billion USD losses until May 1, 2022 [51]. For

example, the DAO attack [15] exploited a *re-entrancy* vulnerability, which caused inconsistent state updates. Furthermore, attackers have actively exploited *price oracle manipulation* vulnerabilities, resulting from developers misusing price oracle APIs to get token prices in DeFi services.

Cross-chain bridge exploit. To connect DeFi services operating on different blockchains, DeFi employs *cross-chain bridges*, which facilitate the exchange of assets between two blockchains. Unfortunately, some attackers have identified vulnerabilities within these bridges and exploited them to manipulate tokens without providing assets on the other blockchain. For instance, the Wormhole bridge was exploited by this vulnerability and lost 320 million USD [7].

Private key leakage. Some DeFi hacks occurred due to private key leaks, as these private keys serve as passwords of DeFi accounts. For example, Ronin network's private keys were stolen, resulting in 625 million USD losses [11].

DeFi front-end attack. DeFi services are typically based on smart contracts and DeFi users should send txs on blockchain to interact with them. This might be a big hurdle for regular DeFi users, and DeFi developers provide some web pages (front-ends) to improve their usability. However, some attackers exploited the web pages to make users interact with the web pages to send tokens to attackers rather than trading with DeFi services [12].

2.3 DeFi Scams

Similar to CeFi users, DeFi users are also susceptible to various scams, including phishing. However, DeFi scams differ from CeFi scams due to the unique characteristics of DeFi.

Rug-pull. In DeFi ecosystems, anyone, including scammers, can launch their own DeFi services. Therefore, scammers create fraudulent services and persuade DeFi users to invest their money in these scams. In the end, scammers abandon their projects and disappear with the funds from DeFi users. We call such scams *rug-pulls*. In particular, there have been numerous rug-pulls involving DeFi scam tokens, resulting in losses exceeding 240 million USD [6].

Stablecoin meltdown. To connect DeFi with CeFi, DeFi developers introduced *stablecoins* [30], which are pegged to fiat currencies – stablecoins such as USDT and USDC are pegged to the USD. DeFi users believe that stablecoins are backed by an adequate reserve of fiat currencies or certain algorithms to uphold their values. However, some stablecoins failed to maintain their values, leading DeFi users to panic sell significant amounts of these stablecoins, ultimately resulting in a stablecoin meltdown. For instance, the "LUNA meltdown" failed to keep the value of its stablecoin, UST, which was backed by an algorithm, resulting in 60 billion USD losses [4].

Phishing. DeFi ecosystems are not immune to phishing attacks, similar to the CeFi ecosystems. DeFi phishers often reach out to potential victims via email or social media, attempting to obtain the victims' private keys or tricking them into initiating specific txs. Specifically, DeFi phishers may deceive victims into sending txs that include hidden token approval txs, thereby granting the phishers access to drain tokens from the victims' wallets.

Airdrop scam. One particular phishing method in DeFi involves using airdrops, where developers distribute tokens to DeFi users to advertise their services. Airdrop scammers exploit this process by sending their tokens to wallets of potential victims. These potential victims, upon receiving these unexpected tokens, may visit phishing websites or DeFi services to investigate the activities happening in their wallets. While they interact with phishing websites or DeFi services, they may leak their private keys or initiate some fraudulent txs as mentioned. Therefore, they are more likely to fall victim than to traditional phishing via email or social media.

3 Methodology

To investigate the motivations and risk perceptions of DeFi users relevant to our research questions, we conducted a two-phase study. Initially, we performed in-depth interviews with 14 users, obtaining qualitative insights into their experiences. Based on the findings from the first study, we executed a quantitative survey with 493 DeFi users to validate and expand our understanding. Ensuring ethical and responsible research practices, both study designs received thorough review and approval from our Institutional Review Board (IRB). Minimizing data collection, we only gathered necessary personal information and stored responses under pseudonyms to ensure anonymity. Importantly, participants were informed of their right to withdraw at any time. Supplementary study materials, including the interview guide, codebook, and survey questionnaire, are available in a GitHub repository[1].

3.1 Study 1: Semi-structured Interview

We aimed to gain a comprehensive understanding of user perceptions of DeFi, including their views on hacks and scams. To achieve this objective, we conducted semi-structured interviews with DeFi users ($N = 14$).

Design. The interview protocol was designed with four sections to sequentially address our research questions. (1) For **RQ1**, we asked participants about their perceptions of DeFi. Specifically, participants discussed their *preference* between DeFi and CeFi, along with justifications for their choices. (2) For **RQ2**, we explicitly inquired about participants' perceived DeFi risks and their mitigation strategies. (3) For **RQ3**, participants who were victims shared their experiences and reactions to DeFi hacks or scams. We also explored whether these incidents affected their perceptions of DeFi. (4) For **RQ4**, we

[1] https://github.com/mingyiliu95/defi-user-study

gathered participants' opinions on regulations that could mitigate DeFi hacks and scams. Notably, to ensure the accuracy and coherence of our interviews, we conducted three pilot interviews and primarily revised wording for clarification based on their feedback. We excluded these pilot interviews from our data analysis.

Recruitment. To ensure we interviewed actual DeFi users, we implemented a rigorous two-step recruitment process. Firstly, we advertised our study through popular channels within active DeFi communities like Twitter, Telegram, Discord, and through word-of-mouth. In our recruitment advertisement, we stated that the purpose of our study was to understand user perceptions of cryptocurrency trading. Secondly, potential participants completed a screening questionnaire designed to filter for active DeFi users over the age of 18. This questionnaire included questions about the decentralized application (dApp) usage, community involvement, and experiences with DeFi hacks or scams. Specifically, participants were asked: a) if they had interacted with dApps; if so, b) the names of the dApps they used most frequently; c) their role in the DeFi community (e.g., regular users, dApp developers); and d) if they had experienced DeFi hacks or scams. We then invited participants who accurately listed dApps, including those who identified themselves as victims of DeFi incidents, for interviews. Each participant received 20 USD as compensation.

Data collection and analysis. We conducted 14 online interviews via recorded video calls, averaging 65 minutes in length. After transcribing the videos, two researchers independently coded each interview and discussed their codes to reach a consensus. This coding process was iterated for all 14 interviews, resulting in 148 codes and a Cohen's κ inter-coder reliability score [22] of 0.89. As appended in Appendix A, the interview study was deemed complete once code saturation was reached without new codes emerging that addressed the research questions.

Demographics. Table 1 presents the detailed demographics of our interview participants ($N = 14$). The sample was predominantly male and younger, but there was a varied representation in terms of income and educational background. Participants ranged from newcomers to seasoned users in their cryptocurrency experience. Additionally, we disclosed whether participants were DeFi developers, considering the potential for bias from them. Lastly, we specifically targeted participants who had experienced DeFi misconduct, resulting in eleven self-identified victims in our interviews.

Table 1: The demographics of interview participants.

ID	Gender	Age	Education	Income	Crypto YoE[1]	Dev[2]	Victim
P1	Female	18-24	Bachelor's	$50k-75k	3-5	No	Yes
P2	Female	18-24	Bachelor's	$50k-75k	1-3	No	Yes
P3	Male	18-24	Bachelor's	$25k-50k	1-3	No	Yes
P4	Male	25-34	After bachelor's	$200k+	7-9	Yes	Yes
P5	Male	25-34	After bachelor's	$50k-75k	3-5	No	Yes
P6	Male	25-34	High school	<$25k	3-5	No	No
P7	Male	25-34	Bachelor's	<$25k	3-5	No	Yes
P8	Male	25-34	Bachelor's	$25k-50k	3-5	No	Yes
P9	Male	35-44	After bachelor's	$100k-125k	3-5	No	Yes
P10	Male	18-24	Bachelor's	$150k-175k	3-5	No	Yes
P11	Male	18-24	Bachelor's	N/A	3-5	Yes	No
P12	Male	18-24	High school	<$25k	1-3	Yes	Yes
P13	Male	18-24	High school	N/A	3-5	No	No
P14	Male	25-34	Bachelor's	$75k-100k	1-3	No	Yes

[1] Abbreviated for *Years of Experience*; [2] Abbreviated for *Developer*.

3.2 Study 2: Large-scale Survey

Based on the results of the interview study, we conducted a quantitative study via an online survey ($N = 493$) on Prolific[2] to statistically validate our observations from the interviews on a large scale.

Design. We structured the survey into four sections, mirroring our interview design. (1) For **RQ1**, we inquired about participants' positive and negative experiences with DeFi, and their *preference* for DeFi over CeFi. Specifically, we assessed factors such as *security*, *usability*, *transparency*, and *trust*, identified in the interviews as influencing DeFi preferences. (2) Addressing **RQ2**, we asked participants to select and rank the most concerning DeFi risks identified from interviews. We then queried about the countermeasures they had adopted to mitigate these risks. (3) When tackling **RQ3**, we probed participants' unfortunate experiences with DeFi hacks or scams, including the type of incident, their remedial actions, and any changes in perception. We did not pre-select victims for our survey to accurately represent the real-world proportion of users affected by DeFi incidents. (4) For **RQ4**, we gathered participants' views on DeFi regulations, asking them to express their support or opposition to regulatory oversight and explain their reasons. We included demographic questions at the survey's start and inserted two attention-checking questions within the sections on RQ1 and RQ3.

Recruitment. Because there was no pre-defined filter on Prolific to screen DeFi users, we used a screening questionnaire to recruit DeFi users for the full survey. Initially, we applied three built-in Prolific filters to ensure participants a) had used cryptocurrencies, b) maintained an approval rate above 95% for past submissions, and c) were U.S. residents to minimize cultural and regulatory differences. In the screening questionnaire, we asked if participants considered themselves DeFi users and, for validation, to name the dApp they most frequently used along with its smart contract address. Respondents who accurately listed dApps were deemed eligible and invited to participate in the full survey. We added the Prolific IDs of eligible participants to an allowlist, ensuring only those selected could take the survey. Despite a significant drop-off,

[2] https://www.prolific.com/

this screening process was necessary to ensure the validity of the participants. Compensation was set at 0.30 and 2.50 USD for completing the screening questionnaire and full survey, respectively.

Data collection and analysis. From June to October 2023, we received 4,380 responses to the screening questionnaire. We invited 1,134 eligible participants, of whom 550 submitted the full survey, averaging a completion time of 15 minutes. We analyzed 493 valid responses, excluding incomplete submissions, failed attention checks, or non-compliant responses (e.g., out-of-range ranks). Due to the non-normal distribution of the collected data, we employed non-parametric statistical tests for our analysis. We performed Mann-Whitney U tests and Chi-squared tests of independence (each at a significance level of $\alpha = 0.05$) to compare two answers (questionnaire options). Since each answer was compared to every other answer pairwise, we applied Bonferroni correction. In addition to p-values, we computed rank-biserial correlation r[3] to report the effect size.

Demographics. The demographics of our survey participants ($N = 493$) are presented in Table 2. Our sample predominantly consisted of males (82.4%) and individuals under 44 years old (78.0%), with average and median ages of 37.75 and 35, respectively. Furthermore, 77.0% held a degree at or above a Bachelor's level. Although we omitted specific occupation distribution due to diverse responses, "Computer and Mathematical" occupations were the most common (15.6%).

To assess the representativeness of our participants, given the scarcity of quantitative user studies in the DeFi arena, we compared our demographics with those from research targeting general crypto-asset users [2]. Our study had a higher proportion of male participants than the reference (77.5%) and a younger demographic, with the majority aged between 25 and 34 years (38.3%), as opposed to the reference study's primary age group of 35-44 years (36.2%). Our respondents also had higher educational attainment than the general U.S. population [43], aligning closely with the referenced study, where 77.2% of participants had at least a Bachelor's degree.

Table 2: The demographics of survey participants.

Item	Property	All (N=493) % of participants
Gender	Male	82.4
	Female	16.0
	Non-binary	1.2
	No answer	0.4
Age	18-24	9.7
	25-34	38.3
	35-44	30.0
	45-54	14.2
	55-64	6.1
	65 or above	1.6
Education	No schooling	0.0
	No high school	0.0
	High school	21.7
	Bachelor's	59.2
	After bachelor's	17.8
	Other	0.8
	No answer	0.4
Income	<$25k	6.5
	$25k-50k	17.4
	$50k-75k	22.9
	$75k-100k	18.7
	$100k-125k	11.8
	$125k-150k	8.9
	$150k-175k	3.4
	$175k-200k	2.4
	$200k+	6.5
	No answer	1.4

4 Results

This section presents the study results addressing our research questions. We report qualitative findings in §4.1, quantitative validations in §4.2, and summarize key takeaways in §4.3.

4.1 Interview Study Results

4.1.1 Perceptions of DeFi

Focusing on tackling **RQ1**, we compared users' perceptions of DeFi and CeFi and analyzed why users prefer or do not prefer DeFi over existing CeFi services.

[3]The thresholds for interpreting effect sizes as small, medium, and large are 0.10, 0.30, and 0.50, respectively.

Preference. Most interview participants preferred DeFi over CeFi for various reasons: a few participants highlighted ease of access and use as the main reason, while some cited additional features, transparency, and reliability as the reasons for preferring DeFi. For example, P14 highlighted accessibility benefits: "*I don't have to open up an account. I just need a unique wallet.*" A small number of participants shared neutral or more negative feedback on DeFi, explaining their concerns related to security issues, excessive fees, and lack of experience. P2, for instance, explained "*Since I'm a beginner [in trading], I would go with traditional [fiat CeFi].*" We identify security, usability, transparency, trust, and profitability as common themes affecting preference to use DeFi, and provide example quotes below.

Security. Only a few interview participants mentioned security as a reason for preferring DeFi: "*DeFi is a more secure way to make transactions*" (P3). Half of those who did not prefer DeFi emphasized its insecurity. P13 explained "*Because [of] the amount of hacks... it sounds like it would be very difficult to secure [DeFi].*"

Usability. In response to the question about reasons for preferring to use DeFi, some interview participants mentioned that DeFi is easier to use, referring to fast transaction and interoperability advantages. For example, P5 explained "*[DeFi is] easier to use... You can go to DeFi and actually make quick transactions.*" P10 mentioned the ease in which crypto assets can be transferred: "*exchange from one protocol to*

another [is] easier compared to stock exchange." Several participants also mentioned the convenience factor associated with not having to verify their identity to set up and activate accounts. Among those who preferred DeFi for reasons other than usability, some mentioned their concerns about the steep learning curve.

Transparency. Half of those interview participants who preferred to use DeFi mentioned transparency. P4 explained "*No backroom dealings... Everything is public.*" These participants expressed concerns about the opaqueness of the practices employed by crypto and fiat CeFi services: "*You don't know what the bank's security is [but] you know what the DeFi security is... it's all on chain*" (P11).

Trust. Some preferred to use DeFi because they do not trust the operations of fiat CeFi services, "*[Fiat CeFi] is not nearly as safe as everybody thinks it is. I don't trust the regular financial system*" (P11). On the contrary, one interview participant explained that he lost trust in DeFi and stopped using it: "*I don't use any of them [dApps] anymore... I don't really trust them apart from hacks*" (P8).

Profitability. Many participants acknowledged the profitability side of DeFi as the main reason for preferring to use DeFi. P7, for example, explained financial opportunities: "*There are a lot of opportunities to have a twenty percent APY income, so I put my money to the DeFi and earn the yield.*" However, there were also several participants who expressed expensive transaction fees as a reason for carefully choosing dApps: "*Fees are important. If I see competitive [tx] fees, I like to use them [more] often*" (P6).

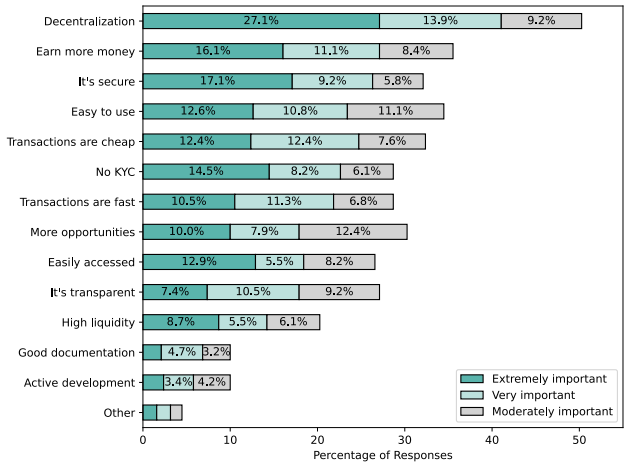
4.1.2 Perceptions of DeFi risks and mitigation

This section explores **RQ2**, and reports details about DeFi users' security concerns and mitigation strategies.

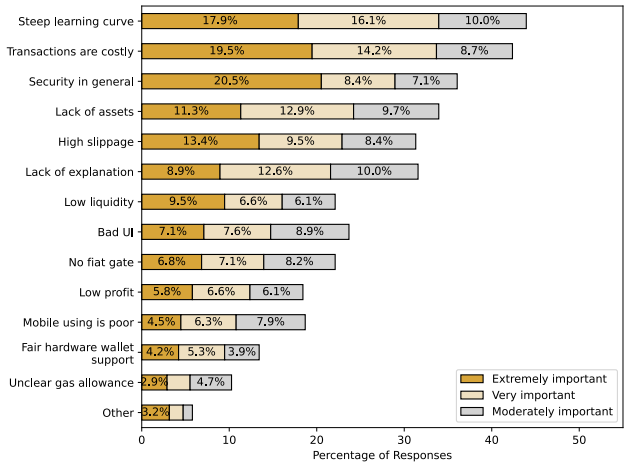
Perceived risks. With respect to the perceived risk questions, many participants expressed concerns about `smart contract exploitation`, some mentioned specific vulnerabilities: "*There are a lot of risks in the lending protocol like oracle price manipulation*" (P7). Several participants were concerned about cryptocurrency price volatility and associated `financial risks`. The third most frequently mentioned risk was `rug-pull`, a common pump-and-dump exit scam orchestrated by the project owners. P6 expressed concerns about the lack of regulations to protect DeFi users from rug-pulls: "*Without it being regulated by someone, there's always the risk of investing in a rug-pull project.*"

Other frequently noted risks include `theft of private key` from wallets, `instability of stablecoins` (risk of de-pegging from 1 USD), and `airdrop scam` related to malicious tokens stored in wallets, each of which was mentioned by a few participants. `Phishing` and `regulatory uncertainty` were each mentioned once.

Risk mitigation. Participants reported mitigation strategies



(a) The survey results about love points of DeFi.



(b) The survey results about pain points of DeFi.

Figure 1: The survey results about love/pain points of DeFi.

and security practices they have employed to mitigate the risks they were concerned about. To deal with the risk of rug-pull and smart contract exploitation, most participants explained they perform thorough research on a given crypto project before investing. For instance, P9 said "*We do our research about the token [first]... and make sure it's a safe and reliable token before we buy [them].*" To address the risks associated with private key compromise, some participants said they rely on hardware wallets to safeguard private keys. P7 explained "*A hacker can't take my crypto private key because I use a hardware wallet.*"

P4 and P6 explained that they regularly revoke token approvals to mitigate rug-pull risks. Token approval allows dApps to access users' wallets, and transfer tokens on users' behalf. This reduces users' re-approval efforts and txs costs. However, token approval is often configured to allow unlimited token transfers, and such configurations could be ex-

ploited by malicious dApps to transfer the entire balance. To that end, P4 shared thoughts on the risk of failing to revoke token approvals in a timely manner: "*If you leave them approved, you could have a bad upgrade [with] a vulnerability that might be exploited. And if you've approved unlimited amounts, then they can just spend all [of] your tokens...*"

Overconfidence in two-factor authentication. P2 and P10 shared their strategy of using two-factor authentication (2FA) to mitigate many of the DeFi risks, including rug-pull and smart contract exploitation. P10 mentioned "*Two-factor authentication has been one of the best solutions for keeping wallets safe.*" Although 2FA is an integral security practice for protecting user accounts in CeFi platforms, it is not supported on non-custodial (decentralized) wallets [33]. We report this as a critical security misconception: DeFi users being overly confident in the use of 2FA to protect their wallets, and, as a result, paying less attention to other important security practices.

4.1.3 Real-world experience with DeFi breaches

To address **RQ3**, we study real-world victims' experiences and how they responded to a scam or hack.

Type of breaches. DeFi scams were reported more often than hacks by the interviewed victims. Among those who experienced DeFi hacks, several victims mentioned being affected by smart contract exploits, while some mentioned suffering from private key compromise. For example, P4, who is a dApp developer, shared an incident that involved the exploitation of a re-entrancy vulnerability in their smart contract: "*We lost million[s of dollars], it was not a good time... It was a re-entrancy vulnerability, and the audit completely missed it.*"

With respect to DeFi scam experiences, many participants encountered rug-pull incidents: "*He [the founder] deployed two smart contracts. One was fine [but] another was a rug-pull*" (P7). Several participants fell victim to phishing scams: "*I was DM-ed [direct messaged] by somebody who said, you just joined this channel, click this link to verify your account... I logged into my MetaMask... [and] half an hour later... everything was gone*" (P12).

Response actions. We asked interview participants about the immediate actions taken after experiencing the last scam or hack incident. Their responses include adopting new security practices, asking the support or development team for assistance, or not taking any action. Some victims mentioned they increased the net investment size, and moved to other DeFi services to quickly recover their loss. Among those who adopted a new security practice, P12 responded to a phishing scam by "*... disconnecting my wallet from every site, and revoking every [token] approval that I had out there.*" Several victims who contacted the development team received no response, or a premature response that was not particularly helpful. P3, for instance, said "*I sent an email... but I did not get any reply, [and] I moved on.*" P5 shared a similar experience: "*[They said] they will get back to me, but I never heard from them again.*" One victim, who experienced rug-pull, contacted an IP lawyer in an attempt to sue the development team but stopped after learning about the low probability of getting anything back. Some of the victims, who were affected by phishing and rug-pull breaches, did not take any action.

Perception changes. Our objective was to understand how victims' security perceptions may have been affected by the breaches. We asked "*has your belief or perception of DeFi changed after experiencing the DeFi hack or scam*?" Surprisingly, most interview participants explained their security perceptions of DeFi did not change; some even mentioned that their confidence in DeFi platforms increased despite the breach, praising the previously realized profits, and often blaming themselves for being careless. P3, for instance, lost about 4,700 USD in a recent rug-pull incident but said "*my belief in cryptocurrency has grown stronger after [experiencing] that [DeFi scam] because I made good money from it... An opportunity to make money is something I believe in.*" P9 blamed themselves: "*Oh, my belief did not change! I just felt like I was the victim of my own circumstance... Not doing enough research before diving into it... it was my fault basically.*" P11 explained that it was a risk that they were willing to take for financial gain.

Blame distribution. Lastly, we analyzed the distribution of stakeholders that the victims held accountable for the experienced breaches. A few interview participants simply blamed hackers and scammers. About half of the participants blamed developers: "*It is the responsibility of the developers to spot their loophole [first]... and make amendments for investors' security*" (P3). Most participants held themselves accountable, and explained that they should have done more research prior to using a DeFi service.

4.1.4 DeFi regulation preferences

This section delves into **RQ4** and investigates DeFi users' perceptions of regulations. The U.S. Securities and Exchange Commission (SEC) issued a statement [13] in 2021 outlining "pseudonymity" and "lack of transparency" issues associated with DeFi. In 2022, the SEC amended "Rule 3b-16" of the Exchange Act [40] to include all DeFi platforms in the "exchange" category. In the latest 2023 statement [23], the SEC explained that DeFi platforms need to conform to laws governing securities.

Given this background, our interview participants shared mixed feelings about regulation. Many participants shared positive feedback whereas the majority provided opposing feedback. Participants who endorsed DeFi regulation believed that it would promote DeFi security, reduce financial loss, and protect them from adversaries. P6, for example, explained "*A malicious user should be punished... there needs to be some justice...*" Opposing participants were worried that regulation efforts sit uneasily with the decentralized and unregulated

fundamentals of DeFi. Some were also concerned about regulations discouraging innovation, and tax implications.

4.2 Online Survey Results

4.2.1 Perceptions of DeFi

We focus on validating the interview results for **RQ1** in this section. The survey was designed to distinguish exchanges and lending platforms as two different DeFi services. However, because the user perceptions were not too different between the two services, we decided to simplify the analysis and report the aggregated results.

First, we derived and coded the aspects of users' enjoyment and frustration in DeFi, based on our interviews and a preliminary industry study [19]. From the initial pilot study, we noticed that people take too long and find it difficult to rank all given options based on relative importance. Hence, in the final survey design, we asked survey respondents to select and rank no more than three *love/pain points*. Figure 1 shows the results sorted by weighted scores, where "Extremely important," "Very important," and "Moderately important" represent 3, 2, and 1 scores, respectively. The detailed results of the statistical tests are presented in Appendix C. Due to page limits, we only report and discuss highly ranked love/pain points.

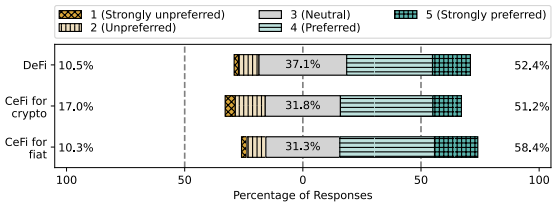
Love points. `Decentralization` was considered to be the most important love point. Our subsequent security analysis, however, revealed that many participants have an inadequate understanding of decentralization and thus are optimistic about this characteristic contributing to security. `Earn more money` ranked second, indicating that financial gains are important motivations for using DeFi services [19].

Pain points. Participants regarded steep learning curves and high transaction (tx) costs, which are classified as *usability*, and *security* issues, as the most important pain points. It's understandable that users deem DeFi tx fees expensive because, in addition to the inevitable gas fee[4], dApps may also impose liquidity taker fee on tx to reward market creators who provide liquidity, and this fee varies among dApps. In this case, some developers lowered their tx fees to offer a more cost-friendly environment [1, 42].

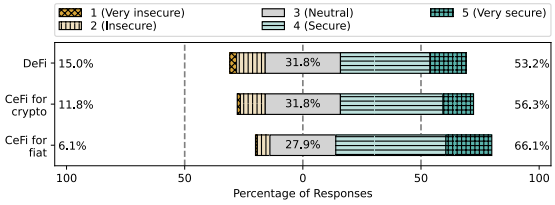
Second, from the interview responses, we identified *security*, *usability*, *transparency*, and *trust* as the most common reasons (thematic codes) influencing users' *preference* for DeFi and CeFi systems. We report our Likert scale question results from the survey, which has been designed to investigate users' comparative perceptions.

Preference. In contrast to the interview responses, our survey results did not show a dominant preference for DeFi. Participants' preference rates are summarized in Figure 2a. We observed a statistically significant difference in preference rates between crypto CeFi and fiat CeFi ($p < 0.01$) but the effect size was small ($|r| = 0.12$).

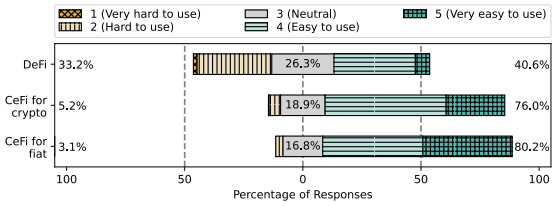
[4] Blockchain miners' reward for executing transactions.



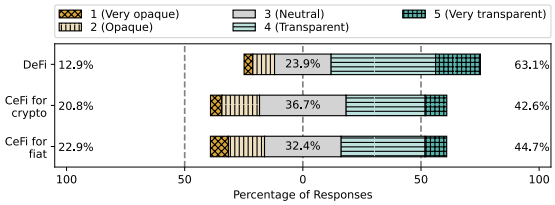
(a) The comparison in terms of *preference*



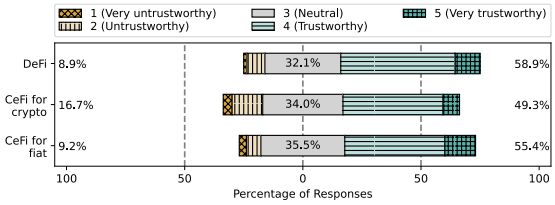
(b) The comparison in terms of *security*



(c) The comparison in terms of *usability*



(d) The comparison in terms of *transparency*



(e) The comparison in terms of *trust*

Figure 2: The comparison of survey participants' perceptions between DeFi, CeFi for crypto, and CeFi for fiat.

Security. Unsurprisingly, Figure 2b shows that users perceive DeFi as slightly less secure than CeFi. Statistical tests in Table 3 revealed significant differences in security perception between DeFi and fiat CeFi ($p < 0.001$), and between crypto CeFi and fiat CeFi ($p < 0.01$). The effect sizes were small in both cases ($|r| = 0.15$ and $|r| = 0.13$).

We also asked an open-ended question about the reasons for their perceived security ratings: 39.8% considered DeFi to be secure due to its `decentralization` characteristic; this observation is well aligned with the love points explained before,

Table 3: Results showing significant differences in Mann-Whitney U tests under Bonferroni correction for DeFi's and CeFi's rate distributions of *preference*, *security*, *usability*, *transparency*, and *trust*. The p-values and effect sizes in rank-biserial correlation r are reported.

Item	*Preference*		*Security*		*Usability*		*Transparency*		*Trust*	
	DeFi	CeFi_C	DeFi	CeFi_C	DeFi	CeFi_C	DeFi	CeFi_C	DeFi	CeFi_C
CeFi_C[1]		–		–	p = 2.2e-30 r = 0.46	–	p = 1.1e-8 r = – 0.23	–	p = 8.4e-4 r = – 0.13	–
CeFi_F[2]		p = 9.0e-3 r = 0.12	p = 4.4e-4 r = 0.15	p = 2.1e-3 r = 0.13	p = 6.0e-35 r = 0.55	p = 2.1e-3 r = 0.13	p = 3.1e-7 r = – 0.23			p = 1.1e-2 r = 0.11

[1] Abbreviated for *CeFi for cryptocurrency*; [2] Abbreviated for *CeFi for fiat currency*.

in which the `it's secure` love point also recorded a high ranking. However, some explanations were not particularly convincing. For example, one participant believed that "*decentralized [service] is always more safe than centralized [service]*" (S512). Some participants mistakenly equated the decentralization of DeFi with that of the underlying blockchain and thus reported a misbelief about the security guarantees: "*[DeFi is] more secure because a hacker would have to override an entire blockchain [to steal funds in DeFi]*" (S12). `Self-custody of private keys` was also mentioned frequently (23.9%). One participant explained "*[DeFi is] secure if the private keys are well stored*" (S20), which is not the case. Some participants (19.3%) considered DeFi to be secure simply due to `no hack or scam experience`.

Among those who considered DeFi to be insecure, 55.8% of such participants mentioned `rampant hacks or scams` as the main reason. One participant explained "*I have [used] malicious smart contracts that steal your funds before*" (S398). `Decentralization` was the second most frequently mentioned reason (23.3%) for feeling insecure. For example, S224 explained "*[DeFi services] are easier to exploit than centralized [services].*" Furthermore, some participants associated decentralization with a lack of regulations and controls, and emphasized such liberal aspects as a reason for feeling less confident about DeFi.

Taken together, we report that a significant portion of participants over-estimate DeFi's security due to their limited understanding of the concept of `decentralization`. Such participants do not seem to be aware of the new attack vectors introduced through the use of smart contracts [52].

Usability. The overall sentiment, as shown in Figure 2c, was that both crypto and fiat CeFi are easier to use than DeFi ($p <$ 0.001 in both cases). Near-large and large effect sizes further emphasize the magnitude of differences ($|r| = 0.46$ and $|r| =$ 0.55) which was somewhat unexpected since our interview results revealed some participants prefer DeFi due to its fast transaction and interoperability benefits (See §4.1.1).

We asked survey participants to explain the usability scores they assigned to DeFi. Among 60.1% of explanations that provided negative feedback, 40.2% mentioned `steep learning curve`. Many participants felt overwhelmed by the new technologies they had to learn and use, including the concept of dApps, blockchains, and the interactions with non-custodial wallets. 11.8% of such participants explained `it's complex`, and 8.3% mentioned the learning curve associated with `blockchain knowledge required`. However, among those negative feedback, a noticeable 14.4% mentioned that using DeFi was `easy after education`. These observations indicate that users may struggle initially and face various learning challenges but through continued use and some educational support, DeFi could become an easier platform to use.

Transparency. We defined *transparency* in our survey as the extent to which a subject discloses operational and transactional details. Evidence gathered through Figure 2d and Table 3 validates that participants perceive DeFi to be more transparent: distribution of perceived transparency differed significantly between DeFi and other two CeFi services ($p <$ 0.001 in both cases), demonstrating small to medium effect sizes ($|r| = 0.23$ in both cases).

Trust. Survey results, summarized in Figure 2e and Table 3, indicate that users consider crypto CeFi to be the least trustworthy platform – its perceived trust level distribution showed statistically significant differences compared to both DeFi ($p <$ 0.001, $|r| = 0.13$) and fiat CeFi ($p < 0.05$, $|r| = 0.11$).

4.2.2 Perceptions of DeFi risks and mitigation

This section presents large-scale validation for **RQ2**, focusing on DeFi users' security concerns and preventive measures.

Perceived risks. The survey questions about risks were constructed based on those frequently mentioned codes. We asked survey participants to select three most concerning risks and rank them based on concern levels. The concern level distributions (ordered by weighted scores) are shown in Figure 3, and the statistical significance between the distributions is measured and reported in Appendix D. In line with the interview findings, `rug-pull`, `financial risks`, and `smart contract exploitation` were the top three DeFi risks that survey participants were concerned about.

Risk mitigation. Figure 4 presents the security practices commonly employed by our survey participants to mitigate the originally reported three security concerns. First, in line with

Table 4: The preventive measures adopted by survey participants against *rug-pull*, *financial risk*, and *smart contract exploitation*.

Preventive Measures	Rug-pull				Financial Risk				Smart Contract Exploit			
	Non-victim N=250		Victim N=74		Non-victim N=237		Victim N=53		Non-victim N=138		Victim N=64	
I do my own research	155	(62.0%)	42	(56.8%)	118	(49.8%)	34	(64.2%)	59	(42.8%)	37	(57.8%)
I only invest how much I am willing to lose	144	(57.6%)	48	(64.9%)	156	(65.8%)	32	(60.4%)	59	(42.8%)	38	(59.4%)
I check crypto news almost daily	85	(34.0%)	26	(35.1%)	83	(35.0%)	14	(26.4%)	38	(27.5%)	13	(20.3%)
I enable two-factor authentication to secure my wallets	49	(19.6%)	16	(21.6%)	106	(44.7%)	25	(47.2%)	45	(32.6%)	22	(34.4%)
I deal more with stablecoins	44	(17.6%)	8	(10.8%)	53	(22.4%)	9	(17.0%)	16	(11.6%)	12	(18.8%)
I store my crypto in several wallets	39	(15.6%)	15	(20.3%)	69	(29.1%)	15	(28.3%)	39	(28.3%)	28	(43.8%)
I have cold/hardware wallets	31	(12.4%)	14	(18.9%)	61	(25.7%)	7	(13.2%)	33	(23.9%)	17	(26.6%)
I bookmark official sites and smart contract addresses	26	(10.4%)	12	(16.2%)	37	(15.6%)	8	(15.1%)	28	(20.3%)	14	(21.9%)
I regularly check and revoke token approvals	22	(8.8%)	13	(17.6%)	27	(11.4%)	10	(18.9%)	20	(14.5%)	13	(20.3%)
I use a strategy that averages my buy-in price	18	(7.2%)	9	(12.2%)	37	(15.6%)	16	(30.2%)	15	(10.9%)	5	(7.8%)
I audit smart contract myself	16	(6.4%)	8	(10.8%)	15	(6.3%)	6	(11.3%)	19	(13.8%)	7	(10.9%)
I use a separate browser for my wallets	16	(6.4%)	7	(9.5%)	28	(11.8%)	8	(15.1%)	20	(14.5%)	11	(17.2%)
I don't think there are preventive measures to mitigate this risk	10	(4.0%)	4	(5.4%)	7	(3.0%)	0	(0%)	5	(3.6%)	0	(0%)
I don't have preventive measures to mitigate this risk	6	(2.4%)	1	(1.4%)	3	(1.3%)	0	(0%)	10	(7.2%)	2	(3.1%)
Other	5	(2.0%)	4	(5.4%)	2	(0.8%)	0	(0%)	0	(0%)	1	(1.6%)

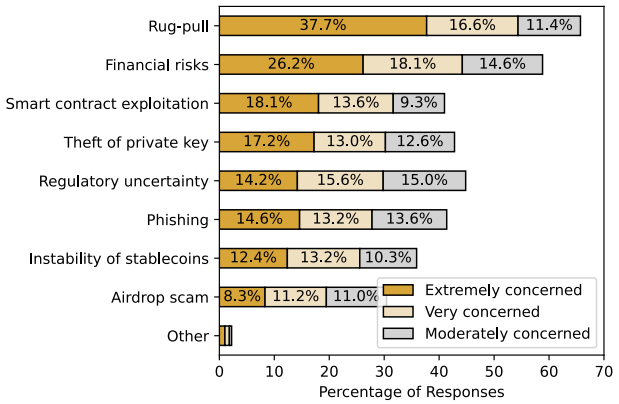


Figure 3: The DeFi risks that concern survey participants.

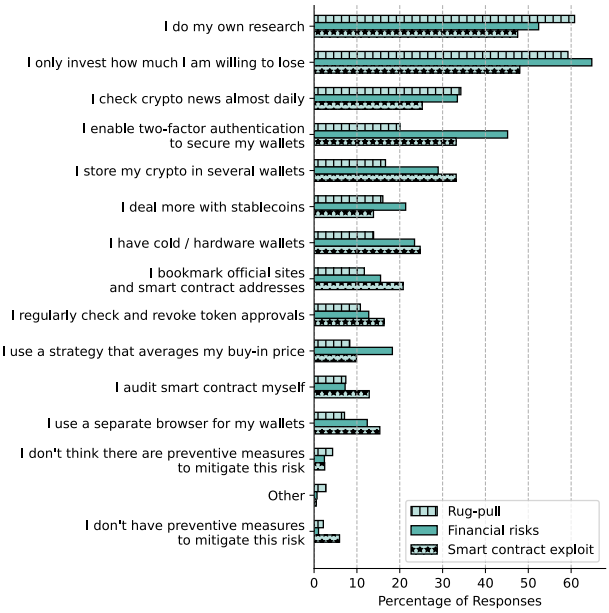


Figure 4: The survey results about how they mitigate *rug-pull*, *financial risks*, and *smart contract exploitation*.

the interview responses, the most commonly practiced strategy involved `I do my own research` and `I only invest how much I am willing to lose`, which are somewhat general investment strategies. Second, token approvals are a critical attack vector. Yet, the adoption rate of the most appropriate countermeasure, `I regularly check and revoke token approvals`, was only practiced by 10.8% of participants who shared their concerns about rug-pull scams. Although 2FA is not suitable for preventing rug-pulls, financial loss, and smart contract exploits, participants reported high adoption rates of 2FA for those three risks: recording 20.1%, 45.2%, and 33.2% adoption rates. Among participants who adopted at least one *technical* solution (2FA, hardware wallet, or revoking token approvals) for each risk, 62.4%, 80.4%, and 65% were using 2FA, respectively. Among such 2FA users, 57.1%, 56.5%, and 49.3% were using 2FA as the *only* technical countermeasure – indicating that the majority may be overconfident in the security guarantees offered by 2FA.

Influence of DeFi incidents. We also investigated whether falling victim to DeFi hacks or scams affects users' security perceptions and practices. Table 4 compares practices employed by non-victims and victims to mitigate their top three concerns. Noticeably, the victims' adoption rate for "revoking token approvals" was slightly higher in all three risks. Victims used the `I store my crypto in several wallets`

Table 5: DeFi Hack type encountered by survey participants, and whether they had a loss to that incident.

DeFi Hack Type	Occurrence	Loss
Smart contract exploitation	22 (37.9%)	14 (63.6%)
Cross-chain bridge attack	11 (19.0%)	9 (81.8%)
Theft of private key for my own wallets	9 (15.5%)	6 (66.7%)
Protocol front-end attack	6 (10.3%)	5 (83.3%)
Theft of private key for protocol smart contract	4 (6.9%)	2 (50.0%)
Other	3 (5.2%)	1 (33.3%)
I have no idea	3 (5.2%)	1 (33.3%)

Table 6: DeFi Scam type encountered by survey participants, and whether they had a loss to that incident.

DeFi Scam Type	Occurrence	Loss
Rug-pull	40 (54.8%)	31 (77.5%)
Phishing	16 (21.9%)	8 (50.0%)
Wallet dusting/Airdrop scam	9 (12.3%)	5 (55.6%)
Stablecoin meltdown	4 (5.5%)	2 (50.0%)
Other	3 (4.1%)	3 (100%)
I have no idea	1 (1.4%)	0 (0%)

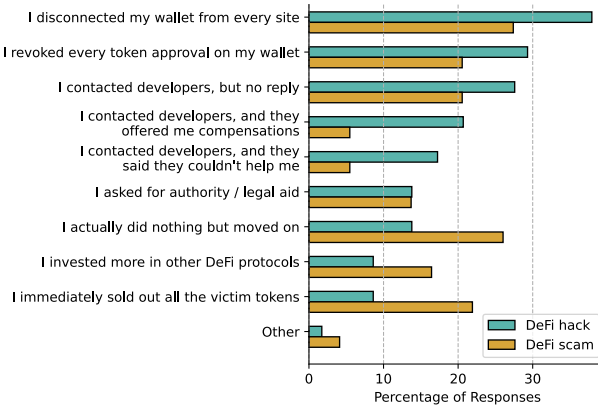


Figure 5: The actions that victims in survey participants took after the latest DeFi incident that they experienced.

strategy more frequently than non-victims to prevent rug-pull and smart contract exploits. Hence, there may be some tendency for victims to become more vigilant. Chi-squared tests, however, did not show significant differences between the two groups in all three risks ($p = 0.51$, $p = 0.23$, and $p = 0.46$).

There were also a few concerning trends: integral practices such as timely checking and revoking token approvals and opting for hardware wallets were not sufficiently adopted by victims. Further, the misconception about 2FA being adequate in mitigating the top three concerns was also prevalent among the victims.

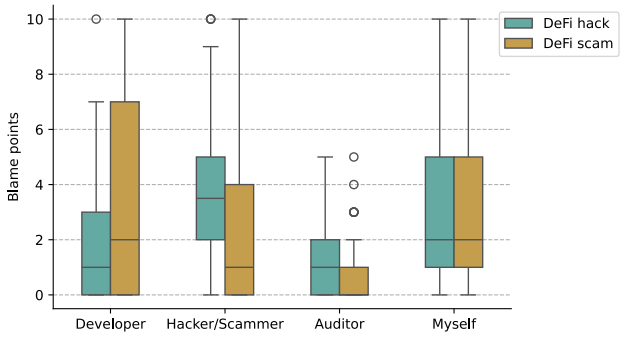


Figure 6: The blame distribution by victims in the latest DeFi incident that they experienced.

4.2.3 Real-world experience with DeFi breaches

To address **RQ3**, we validated the interview results on real-world victims' experiences, perceptions, and responses to scams or hacks.

Being affected multiple times. In the online survey, we defined a DeFi hack as "*the act of identifying and then exploiting vulnerabilities in the DeFi domain*", and provided unauthorized wallet access and dApp exploit as two examples. 11.8% of the participants reported having previously experienced a DeFi hack at least once – we refer to such participants as "victims". We then inquired victims about the number of times they have experienced DeFi hacks: the mean number of hacks was 1.8 ($\sigma = 1.6$). Similarly, we defined a DeFi scam as "*the act of tricking users or pretending to be a valid dApp, and stealing users' crypto assets*", and hinted that common DeFi scams include transferring malicious cryptocurrency to victims' wallets or being affected by rug-pulls. In line with the interview results, more participants seem to have fallen victim to DeFi scams than hacks: 14.8% of participants reported having experienced DeFi scams at least once. Surprisingly, the mean number of experienced scams was 4.7 ($\sigma = 12.5$). Worryingly, some participants mentioned experiencing more than 10 scams in the past. We contacted the victims again to confirm those numbers.

Type of breaches. Victims reported the category of the DeFi hack they recently fell into, which is presented in Table 5. `Smart contract exploitation` was the most prevalent attack, experienced by 22 victims. 9 victims suffered private key theft on their wallets. Other breaches are related to different vulnerabilities as discussed in §2. Regarding DeFi scams, Table 6 confirms that `rug-pull` is the most dominant scam: more than half of the victims were affected. `Phishing` ranked second. Despite the prevalence of phishing attacks and the number of affected victims, the overall concern level for phishing (as reported in Figure 3) was much lower than other risks such as financial risk or private key theft. We surmise this may be due to the fact that phishing incidents do not always result in a direct financial loss: indeed, just 50.0% of `phishing`

Table 7: The number of survey participants choosing each reason for unchanged or strengthened belief in DeFi after the incidents.

DeFi Hack		DeFi Scam	
Reason	Count	Reason	Count
`It was a risk that I was willing to take`	16 (55.2%)	`It was a risk that I was willing to take`	23 (59.0%)
`I am making profits regularly from DeFi`	12 (41.4%)	`It was my fault, I could have been smarter`	21 (53.8%)
`It was my fault, I could have been smarter`	11 (37.9%)	`The technology outweighs the downside of scams`	17 (43.6%)
`I made more research after the hack`	11 (37.9%)	`I made more research after the scam`	15 (38.5%)
`The technology outweighs the downside of hacks`	10 (34.5%)	`I can use trustworthy DeFi apps`	14 (35.9%)
`I can use trustworthy DeFi apps`	9 (31.0%)	`I am making profits regularly from DeFi`	13 (33.3%)
`I am a full-time DeFi trader`	3 (10.3%)	`Other`	2 (5.1%)
`Other`	0 (0%)	`I am a full-time DeFi trader`	0 (0%)

victims reported losing money as a result of the incident; in comparison, a significantly larger proportion of victims reported financial implications in the case of `rug-pull` (77.5%) and `smart contract exploitation` (63.6%).

Response actions. Figure 5 presents a summary of the victims' response actions and the frequency of occurrence. The most frequent response action was "disconnect wallet" and "revoke token approval" – however, their overall adoption rates were just 27.4% and 20.5% after scams, respectively. Worryingly, 13.8% of hack victims and 26.0% of scam victims failed to take any action. These findings are in line with the observations reported in §4.2.2: users generally lack knowledge about appropriate security practices that need to be considered after being affected by a breach. Another concerning trend entails several victims (16.4% after scams) increasing the net investment amount, and using other DeFi services to quickly recover their loss. Such victims may not have put in any effort to improve their security practices even after experiencing various hacks and scams, including rug-pull (23.5%) and smart contract exploitation (11.8%), and merely focused on finding new DeFi services to generate profit again.

Perception changes. The survey results confirmed interview observations at a larger scale: 50.0% of hack victims and 53.4% of scam victims indicated that their security perceptions did not change or confidence increased despite experiencing the hack or scam. Their reasons are summarized in Table 7. For both scams and hacks, "willingness to take risks" was the most prevalent reason for unchanged perceptions, followed by "making regular profits" and "self-blaming". Taken together, these results suggest that DeFi users' financial motivations are very strong, and previous experiences and educational support may have minimal impact on improving their security practices.

Blame distribution. For validation, we asked our survey participants to compose blame points, with a sum of ten, for developers, hackers/scammers, auditors, and themselves, regarding the most recent incident they fell into. The survey results are summarized in Figure 6. In line with the interview results, self-blame was prevalent in both incidents. Even the victims held themselves more accountable than developers for being affected by a DeFi hack. We observed a very wide interquartile blame range for developers in the scam scenario: this may be due to the prevalence of `rug-pull` experiences, in which the developers often play the role of scammers.

4.2.4 DeFi regulation preferences

The survey responses confirmed interview observations. 46.9% of the participants disagreed with the statement "*I am in favor of DeFi being regulated by authorities.*" 35.3% agreed, and the rest were neutral. The top three reasons for endorsing regulation were `contribute to making DeFi secure` (46.2%), `less financial loss for users` (37.7%), and `penalize nefarious persons` (34.3%). In comparison, the most prevalent reason for opposing regulation was `regulation brings in taxes` (53.1%), followed by `regulation hinders innovation` (48.5%) and `nefarious persons' misconduct still` (34.3%).

We also examined how the number of adopted mitigation techniques (RQ2) and DeFi scam/hack experiences (RQ3) influence users' regulation preferences. The first investigation involved dividing participants into three groups for each of the top three risks: those who did not adopt any mitigation technique, those who adopted one or two techniques, and those who adopted more than two. We did not, however, find any statistically significant difference in the regulation preference rates between those three groups. The second investigation involved comparing regulation preference rates between victims and non-victims: again, we did not identify any significant difference between the two groups.

Defining an adequate level of regulation is a complicated issue, and warrants further investigation. However, considering that security risks are often being ignored by DeFi users due to their strong financial motivations, and the most concerning implication of regulation is related to paying additional tax (this is a civil obligation anyway), we carefully hint toward developing an appropriate level of regulations to mandate strong security practices, and help victims protect their assets.

4.3 Key Takeaways

In this section, we highlight the key findings based on the evidence gathered from the two studies. First, profitability and

decentralization, as one would expect, are the two key factors contributing to users' preference for DeFi. Users often blindly believe that decentralization alone translates to strong security and reliability. However, despite this common misconception, users still perceive DeFi as less secure compared to other CeFi services (See §4.1.1 and §4.2.1). Second, similar to security behaviors observed in cryptocurrency systems [2], DeFi users do not employ adequate security controls to mitigate their top concerns. Alarmingly, DeFi users appear overly confident that 2FA will effectively protect them from common DeFi threats. In contrast to the victim characteristics reported in [9], DeFi victims did not show significant improvement in employed security practices compared to non-victims, implying that experience and education may have a limited impact (See §4.1.2 and §4.2.2). Third, `rug-pull` was the most prevalent breach experienced by the victims, and this observation aligns with the overall concern levels and the findings in [6]. `Phishing` was another prevalent attack among the victims, but the perceived concern levels were ranked among the bottom three risks. This contrasting trend may be explained by the fact that phishing does not always result in a direct financial loss (See §4.1.3 and §4.2.3). Fourth, contrary to CeFi victim behaviors [24], prior hack or scam experiences do not seem to affect many DeFi users' security perceptions and confidence in DeFi services. Their strong financial motivations seem to outweigh security priorities and concerns. These observations also suggest that experience and education may be insufficient to help users employ better security practices (See §4.1.3 and §4.2.3). Last, the primary concern for opposing DeFi regulation was paying tax. Considering that the primary objective of DeFi users is to maximize profit, this observation is unsurprising. Many expressed a willingness to sacrifice the potential security benefits of regulation (See §4.1.4 and §4.2.4).

5 Discussion

We present actionable recommendations based on our key findings, and discuss the limitations of the two studies.

5.1 Recommendations

Regulating DeFi to protect users. DeFi victims have a tendency to ignore security risks and pursue financial gains – some victims experienced multiple scam or hack incidents as a result. Such behaviors diverge significantly from previous findings related to internet scams [5, 9] where victims typically employ stronger protective measures after encountering frauds. Perhaps this difference can be explained partially by the analogy developed by Mills *et al.* [36], Delfabbro *et al.* [18], and Johnson *et al.* [28]: they present the idea that cryptocurrency users' trading practices and addictions often resemble gambling behaviors. Our results support their analogy. P13 mentioned "*Some of these DeFi projects are, in my opinion, basically [like] gambling*." If this analogy is accurate, then providing educational support and gaining more experience alone may not be effective in protecting DeFi users. Similar to how the internet gambling industry is heavily regulated to protect gamblers [35], the DeFi industry may also need to mandate strong security controls through regulation and regular audit requirements.

Regulating DeFi is a complicated issue: 46.9% of survey participants opposed the idea, expressing concerns about decentralization benefits being jeopardized through heavy regulation practices. Hence, the community must collectively work toward a decentralized form of regulation. For instance, the concept of a decentralized organization could be employed to facilitate autonomous management of DeFi project memberships [44]. Such organizations would conduct audits and enforce compliance through the means of verifying project team identity, analyzing whitepapers and roadmaps, and auditing project codes. Scam projects or projects that lack security controls would be rejected. Only those that pass the audits and compliance checks would be issued, e.g., a membership certificate – users can check this information before safely engaging with a reliable DeFi service.

Correcting security misconceptions. We identified several security misconceptions. First, many users underestimate the importance of reviewing and revoking token approvals. Educational support and regular reminders are necessary to help users adopt best practices for re-configuring token grant limits to minimize risks. MetaMask wallet, for example, offers comprehensive educational materials related to revoking token approvals [34]. In addition, we imagine a reminder feature that regularly prompts users to review their current approvals would also be effective. Second, users often believe that DeFi platforms provide an equal level of security as the underlying blockchain technology – such an inadequate security mental model needs to be improved, and users need to understand that DeFi platforms are just as prone to common online attacks. Last, many users seem to believe that 2FA is consistently effective against various DeFi threats. To help users understand the security protections offered through 2FA and its limitations, we suggest clarifying the covered threats in the 2FA settings of custodial wallets (e.g., Coinbase 2FA setting[5]) that users use to access DeFi services.

5.2 Limitations

This work has limitations because of its empirical nature. Though applied validation questions about DeFi usage, we relied on self-reported data to recruit DeFi users, which could not prevent participants from giving desirable or repetitive survey responses. In addition, participants' awareness and understanding of different DeFi hacks and scams may influence the self-reported type of incidents they suffered. Another key limitation of our study is the absence of a standardized frame-

[5] https://accounts.coinbase.com/security/settings

work for analyzing the diverse range of DeFi services and applications, which may result in significant variations in user perceptions of their usefulness and security. This limitation restricts our ability to understand how specific DeFi users, such as borrowers or lenders, perceive these factors compared to others. Future studies need to consider these compound factors through the control of demographics. Furthermore, to best accurately reflect the real-world distribution, we did not control the number of victim and non-victim participants. Therefore, we lacked sufficient responses from victims for more in-depth statistical analysis. We also note that we did not ask victims about their net profit or loss. Without this information, we cannot strongly claim that all victims are making short-sighted investment decisions – some victims, despite being affected by several scams or hacks, may be accepting carefully calculated risks to continue investing in DeFi and generating net profit. Investigation of such a strategic group of victims would be an intriguing future work. Lastly, Table 2 and Appendix B show our survey participants' yearly income and their asset distribution percentages in the crypto market and DeFi, respectively. The risk-taking behavior revealed in this paper may not apply to users who are wealthy or arrange a significant percentage of income in DeFi.

6 Related Work

User studies in DeFi. With the increasing popularity of DeFi, researchers have conducted various user studies within the DeFi ecosystems. For instance, Wang *et al.* [46] discovered that many DeFi users lack awareness of sandwich attacks and exhibit a high tolerance for them even after being educated about these attacks – this observation is similar to our report about users' attitudes toward DeFi incidents. However, they also explain that DeFi traders believe they would learn "how to avoid further losses" from losing money, and by being attacked once, they will be motivated to learn and protect themselves next time. These perceptions, studied in the context of a single sandwich attack and non-victims, conflict with our analysis on real-world victims: despite being affected by various DeFi scams and hacks, many victims continued to use DeFi services without revising their security practices. Additionally, Guan *et al.* [25] identified misconceptions among DeFi users, such as the belief that stablecoin developers collaborate with regulatory entities like governments. They also reported various perceived risks related to stablecoins. Our risk concern analysis, however, revealed that the aggregated stablecoin risk is one of the least concerning risks.

Feng *et al.* [21] explored users' perceptions of DeFi auditing and found that interview participants had difficulties interpreting technical audit reports, indicating a gap in the effectiveness of DeFi auditing. Chaliasos *et al.* [8] conducted user studies with DeFi security practitioners to evaluate whether DeFi security tools meet their needs. Notably, these related works do not address our research questions, thereby motivating this paper.

Mitigations of DeFi incidents. Several research approaches have been pursued to prevent DeFi hacks and scams before they occur. A significant direction includes identifying smart contract vulnerabilities through techniques such as fuzzing [10, 26, 38, 49], symbolic execution [31, 32, 37], and static analysis [29, 39, 41]. These methods have successfully detected numerous smart contract vulnerabilities before they could be exploited. Regarding efforts to mitigate scams, Cernera *et al.* [6] discovered that 60% of tokens on Ethereum and Binance Smart Chain last less than one day and highlighted patterns of rug-pulls. Huang *et al.* [27] developed a prediction model to identify NFT rug-pull projects before incidents occur. Conversely, Wang *et al.* [45] focused on recovery from DeFi incidents. To revert exploit txs, they introduced new types of tokens and NFTs, named ERC-20R and ERC-721R, which allow for transaction reversal.

7 Conclusion

Based on a semi-structured interview and a follow-up large-scale survey, we investigated DeFi users' security perceptions and the adequacy of commonly employed security practices. Our results showed that DeFi users tend to have inadequate understanding of the security controls, and ignore security risks to pursue financial motivations. Many participants falsely believed 2FA (not supported in non-custodial wallets) can protect them from most of the common DeFi threats. Our investigation of victims revealed more worrying behaviors: many victims' security perceptions did not change after experiencing scams or hacks, and they continued to use other DeFi services to quickly recover their losses without revising security practices. The majority of such victims failed to take any remedy actions after the incident. Victim behaviors indicate that educational support and gaining more experience may have a limited impact – a much stronger control, such as decentralized regulation, may be necessary to mandate adequate security practices and protect users.

References

[1] 1inch Network. The 1inch router v5 is released. https://blog.1inch.io/the-1inch-router-v5-is-released/, 2022.

[2] S. Abramova, A. Voskobojnikov, K. Beznosov, and R. Böhme. Bits under the mattress: Understanding different risk perceptions and security behaviors of crypto-asset users. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI)*, Yokohama, Japan, May 2021.

[3] Balancer. Balancer acknowledged being hacked. https://twitter.com/Balancer/status/1695777503699435751, 2023.

[4] Bloomberg. How $60 billion in terra coins went up in algorithmic smoke. https://www.bloomberg.com/graphics/2022-crypto-luna-terra-stablecoin-explainer/, 2022.

[5] M. Button, C. Lewis, and J. Tapley. Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal*, 27: 36–54, 2014.

[6] F. Cernera, M. La Morgia, A. Mei, and F. Sassi. Token spammers, rug pulls, and sniper bots: An analysis of the ecosystem of tokens in ethereum and in the binance smart chain (BNB). In *Proceedings of the 32st USENIX Security Symposium (Security)*, Anaheim, CA, Aug. 2023.

[7] Certik. Wormhole bridge exploit incident analysis. https://www.certik.com/resources/blog/1kDYgyBcisoD2EqiBpHE51-wormhole-bridge-exploit-incident-analysis, 2022.

[8] S. Chaliasos, M. A. Charalambous, L. Zhou, R. Galanopoulou, A. Gervais, D. Mitropoulos, and B. Livshits. Smart contract and defi security tools: Do they meet the needs of practitioners? In *Proceedings of the 46th International Conference on Software Engineering (ICSE)*, Lisbon, Portugal, Apr. 2024.

[9] H. Chen, C. E. Beaudoin, and T. Hong. Securing online privacy: An empirical test on internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in human behavior*, 70: 291–302, 2017.

[10] J. Choi, D. Kim, S. Kim, G. Grieco, A. Groce, and S. K. Cha. SMARTIAN: Enhancing smart contract fuzzing with static and dynamic dataflow analyses. In *Proceedings of the 43rd International Conference on Software Engineering (ICSE)*, Madrid, Spain, May 2021.

[11] CoinDesk. Axie infinity's ronin network suffers $625m exploit. https://www.coindesk.com/tech/2022/03/29/axie-infinitys-ronin-network-suffers-625m-exploit/, 2022.

[12] CoinDesk. Defi protocol balancer says web front end is 'under attack'. https://www.coindesk.com/business/2023/09/20/defi-protocol-balancer-says-web-front-end-is-under-attack/, 2023.

[13] C. A. Crenshaw. Statement on defi risks, regulations, and opportunities. https://www.sec.gov/news/statement/crenshaw-defi-20211109, 2021.

[14] Curve Finance. Curve finance acknowledged being hacked. https://twitter.com/CurveFinance/status/1685693202722848768, 2023.

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

[16] De.Fi Security. De.Fi rekt report: Crypto losses reach $1.95b in 2023. https://de.fi/blog/de-fi-rekt-report-crypto-losses-reach-1-95b-in-2023, 2023.

[17] DeFiLlama. Defillama dashboard. https://defillama.com, 2024.

[18] P. Delfabbro, D. King, J. Williams, and N. Georgiou. Cryptocurrency trading, gambling and problem gambling. *Addictive Behaviors*, 122: 107021, 2021.

[19] Dex.Blue. Defi user survey — the results & insights. https://medium.com/dexdotblue/defi-usage-survey-the-results-insights-b3481275019b, 2020.

[20] dYdX. dydx acknowledged being hacked. https://twitter.com/dYdX/status/1725921897848914353, 2023.

[21] D. Feng, R. Hitsch, K. Qin, A. Gervais, R. Wattenhofer, Y. Yao, and Y. Wang. Defi auditing: Mechanisms, effectiveness, and user perceptions. *Cryptology ePrint Archive*, 2023.

[22] J. L. Fleiss, B. Levin, and M. C. Paik. *Statistical methods for rates and proportions*. John Wiley & Sons, 2013.

[23] G. Gensler. Statement on alternative trading systems and the definition of an exchange. https://www.sec.gov/news/statement/gensler-statement-ats-041423, 2023.

[24] V. Giang and M. Dang. 10 days that have roiled markets: A timeline of the banking chaos. https://www.nytimes.com/article/svb-silicon-valley-bank-collapse-timeline.html, 2023.

[25] Y. Guan, Y. Yu, T. Sharma, K. Qin, Y. Wang, and Y. Wang. Poster: Examining user perceptions of stablecoins: Understandings and risks. In *Symposium on Usability, Privacy, and Security (SOUPS)*, 2023.

[26] J. He, M. Balunović, N. Ambroladze, P. Tsankov, and M. Vechev. Learning to fuzz from symbolic execution with application to smart contracts. In *Proceedings of the 26th ACM Conference on Computer and Communications Security (CCS)*, London, UK, Nov. 2019.

[27] J. Huang, N. He, K. Ma, J. Xiao, and H. Wang. Miracle or mirage? a measurement study of nft rug pulls. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, 7(3):1–25, 2023.

[28] B. Johnson, S. Co, T. Sun, C. C. Lim, D. Stjepanović, J. Leung, J. B. Saunders, and G. C. Chan. Cryptocurrency trading and its associations with gambling and mental health: A scoping review. *Addictive Behaviors*, 136:107504, 2023.

[29] S. Kalra, S. Goel, M. Dhawan, and S. Sharma. ZEUS: Analyzing safety of smart contracts. In *Proceedings of the 2018 Annual Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, Feb. 2018.

[30] A. Klages-Mundt, D. Harz, L. Gudgeon, J.-Y. Liu, and A. Minca. Stablecoins 2.0: Economic foundations and risk-based models. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, virtual, Oct. 2020.

[31] J. Krupp and C. Rossow. teEther: Gnawing at ethereum to automatically exploit smart contracts. In *Proceedings of the 27th USENIX Security Symposium (Security)*, Baltimore, MD, Aug. 2018.

[32] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor. Making smart contracts smarter. In *Proceedings of the 23rd ACM Conference on Computer and Communications Security (CCS)*, Vienna, Austria, Oct. 2016.

[33] MetaMask. When two-factor authentication? https://support.metamask.io/privacy-and-security/when-two-factor-authentication/, 2024.

[34] MetaMask. How to revoke smart contract allowances/token approvals. https://support.metamask.io/privacy-and-security/how-to-revoke-smart-contract-allowances-token-approvals/, 2024.

[35] B. Miller. The regulation of internet gambling in the United States: It's time for the federal government to deal the cards. *Journal of the National Association of Administrative Law Judiciary*, 34:527, 2014.

[36] D. J. Mills and L. Nower. Preliminary findings on cryptocurrency trading among regular gamblers: A new risk for problem gambling? *Addictive behaviors*, 92:136–140, 2019.

[37] M. Mossberg, F. Manzano, E. Hennenfent, A. Groce, G. Grieco, J. Feist, T. Brunson, and A. Dinaburg. Manticore: A user-friendly symbolic execution framework for binaries and smart contract. In *Proceedings of the 34th IEEE/ACM International Conference on Automated Software Engineering (ASE)*, San Diego, CA, Nov. 2019.

[38] T. D. Nguyen, L. H. Pham, J. Sun, Y. Lin, and Q. T. Minh. sFuzz: An efficient adaptive fuzzer for solidity smart contracts. In *Proceedings of the 42nd International Conference on Software Engineering (ICSE)*, Seoul, South Korea, June–July 2020.

[39] S. So, M. Lee, J. Park, H. Lee, and H. Oh. VERISMART: A highly precise safety verifier for ethereum smart contracts. In *Proceedings of the 41st IEEE Symposium on Security and Privacy (Oakland)*, San Francisco, CA, May 2020.

[40] The U.S. Securities and Exchange Commission. Amendments regarding the definition of "exchange" and alternative trading systems (ATSs) that trade U.S. treasury and agency securities, national market system (NMS) stocks, and other securities. https://www.sec.gov/files/rules/proposed/2022/34-94062.pdf, 2022.

[41] P. Tsankov, A. Dan, D. Drachsler-Cohen, A. Gervais, F. Buenzli, and M. Vechev. Securify: Practical security analysis of smart contracts. In *Proceedings of the 25th ACM Conference on Computer and Communications Security (CCS)*, Toronto, ON, Canada, Oct. 2018.

[42] Uniswap. Introducing uniswap v3. https://blog.uniswap.org/uniswap-v3, 2021.

[43] U.S. Census Bureau. U.S. Census Bureau quickfacts. https://www.census.gov/quickfacts/, 2024.

[44] A. Wang. Rethinking the rule and role of law in decentralized finance. In *2022 IEEE 24th Conference on Business Informatics (CBI)*, volume 02, pages 118–125, 2022. doi: 10.1109/CBI54897.2022.10057.

[45] K. Wang, Q. Wang, and D. Boneh. ERC-20R and ERC-721R: reversible transactions on ethereum. *arXiv preprint arXiv:2208.00543*, 2022.

[46] Y. Wang, P. Zuest, Y. Yao, Z. Lu, and R. Wattenhofer. Impact and user perception of sandwich attacks in the defi ecosystem. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI)*, New Orleans, LA, Apr.–May 2022.

[47] M. Wolff. Introducing Marble: A smart contract bank. https://medium.com/marbleorg/introducing-marble-a-smart-contract-bank-c9c438a12890, 2018.

[48] G. Wood et al. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151(2014):1–32, 2014.

[49] V. Wüstholz and M. Christakis. Harvey: A greybox fuzzer for smart contracts. In *Proceedings of the 28th ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE)*, virtual, Nov. 2020.

[50] J. Xu, K. Paruch, S. Cousaert, and Y. Feng. SoK: Decentralized exchanges (DEX) with automated market maker (AMM) protocols. *ACM Computing Surveys (CSUR)*, 2023.

[51] Z. Zhang, B. Zhang, W. Xu, and Z. Lin. Demystifying exploitable bugs in smart contracts. In *Proceedings of the 45th International Conference on Software Engineering (ICSE)*, Melbourne, Australia, May 2023.

[52] L. Zhou, X. Xiong, J. Ernstberger, S. Chaliasos, Z. Wang, Y. Wang, K. Qin, R. Wattenhofer, D. Song, and A. Gervais. SoK: Decentralized finance (DeFi) attacks. In *Proceedings of the 44th IEEE Symposium on Security and Privacy (Oakland)*, San Francisco, CA, May 2023.

A Interview Code Saturation Results

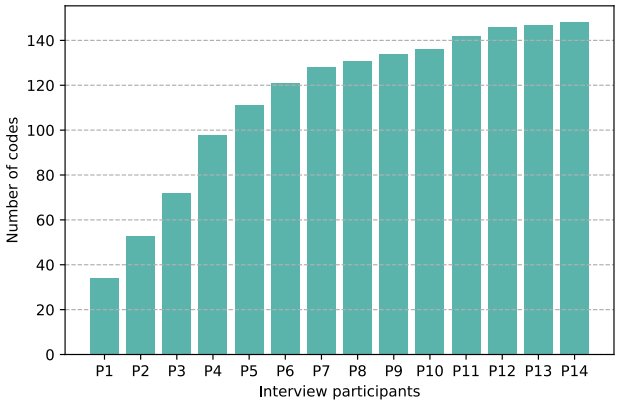


Figure 7: Code saturation status for the interview study

B Survey Results of Trading Experience and Asset Distribution

Table 8: Survey participants' YoE[1] in cryptocurrency and DeFi and their asset distribution.

Item	Property	All	Non-victim	Victim
		N=493	*N*=391	*N*=102
Crypto YoE	Mean	4.6	4.5	5.1
	Median	4.0	4.0	4.0
	Std. deviation	4.8	4.2	6.4
% of asset in Crypto	Mean	16.9	15.7	21.1
	Median	10.0	10.0	15.0
	Std. deviation	17.9	17.1	20.2
DeFi YoE	Mean	2.3	2.2	2.5
	Median	2.0	2.0	2.0
	Std. deviation	1.4	1.4	1.3
% of Crypto in DeFi	Mean	22.3	21.6	24.8
	Median	10.0	10.0	13.5
	Std. deviation	28.5	28.6	28.1

[1] Abbreviated for *Years of Experience*.

C Statistical Results of DeFi Perceptions of Love/Pain Points

Table 9: Results showing significant differences in Mann-Whitney U tests under Bonferroni correction for DeFi's importance distribution of *love points*. The p-values and effect sizes in rank-biserial correlation r are reported.

Decentralization	It's transparent	More opportunities	Active development	Good documentation
	p = 1.0e-5 r = – 0.29	p = 1.5e-5 r = – 0.27	p = 1.7e-4 r = – 0.36	p = 5.0e-4 r = – 0.33
It's secure	It's transparent	More opportunities	Active development	
	p = 6.9e-5 r = – 0.29	p = 1.0e-4 r = – 0.27	p = 3.8e-4 r = – 0.36	

Table 10: Results showing significant differences in Mann-Whitney U tests under Bonferroni correction for DeFi's importance distribution of *pain points*. The p-values and effect sizes in rank-biserial correlation r are reported.

Security in general	Mobile using is poor	Lack of explanation	Lack of assets	Unclear gas allowance	No fiat gate	Bad UI
	p = 4.3e-6 r = – 0.36	p = 3.1e-5 r = – 0.28	p = 5.4e-4 r = – 0.23	p = 3.5e-4 r = – 0.34	p = 1.4e-4 r = – 0.28	p = 5.5e-5 r = – 0.29
Transactions are costly	Mobile using is poor					
	p = 1.6e-4 r = – 0.29					

D Statistical Results of DeFi Perceived Risks

Table 11: Results showing significant differences in Mann-Whitney U tests under Bonferroni correction for DeFi's concern distribution of *perceived risks*. The p-values and effect sizes in rank-biserial correlation r are reported.

Rug-pull	Financial risks	Theft of private key	Phishing	Regulatory uncertainty	Instability of stablecoins	Airdrop scam
	p = 1.1e-3 r = – 0.14	p = 3.7e-5 r = – 0.19	p = 1.6e-7 r = – 0.25	p = 1.6e-9 r = – 0.28	p = 1.5e-6 r = – 0.24	p = 4.7e-10 r = – 0.33
Airdrop scam	Financial risks	Smart contract exploitation				
	p = 4.8e-4 r = 0.19	p = 5.3e-4 r = 0.20				