Understanding User-Perceived Security Risks and Mitigation Strategies in the Web3 Ecosystem

Janice Jianing Si
janice.sijianing@connect.um.edu.mo
University of Macau
Macao, China

Tanusree Sharma
tsharma6@illinois.edu
University of Illinois at Urbana-Champaign
Champaign, United States

Kanye Ye Wang*
wangye@um.edu.mo
University of Macau
Macao, China

ABSTRACT

The advent of Web3 technologies promises unprecedented levels of user control and autonomy. However, this decentralization shifts the burden of security onto the users, making it crucial to understand their security behaviors and perceptions. To address this, our study introduces a comprehensive framework that identifies four core components of user interaction within the Web3 ecosystem: blockchain infrastructures, Web3-based Decentralized Applications (DApps), online communities, and off-chain cryptocurrency platforms. We delve into the security concerns perceived by users in each of these components and analyze the mitigation strategies they employ, ranging from risk assessment and aversion to diversification and acceptance. We further discuss the landscape of both technical and human-induced security risks in the Web3 ecosystem, identify the unique security differences between Web2 and Web3, and highlight key challenges that render users vulnerable, to provide implications for security design in Web3.

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**.

KEYWORDS

Web3 ecosystem, security risk, user perception, mitigation strategy

ACM Reference Format:
Janice Jianing Si, Tanusree Sharma, and Kanye Ye Wang. 2024. Understanding User-Perceived Security Risks and Mitigation Strategies in the Web3 Ecosystem. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24), May 11–16, 2024, Honolulu, HI, USA.* ACM, New York, NY, USA, 22 pages. https://doi.org/10.1145/3613904.3642291

1 INTRODUCTION

As the next generation of the Internet, Web3 aims to establish a transparent, decentralized ecosystem that does not rely on any centralized entities, thereby restoring data and asset ownership to the users [108]. Constructed on the foundation of blockchain technology, Web3 encompasses various components such as decentralized applications (DApps), non-fungible tokens (NFTs), and distributed autonomous organizations (DAOs). It is projected to grow into a six trillion-dollar industry by 2023 [69, 101, 102]. The engagement of governmental entities, exemplified by the Hong Kong government, also highlights its potential for economic innovation [45, 46, 113]. However, the complexity of Web3's technologies also introduces significant security risks, such as smart contract vulnerabilities [73, 83, 86] and private key leakage [30, 54, 65, 81, 91], leading to substantial financial losses, exemplified by the 200 million USD lost to hacker attacks in Q2 2023 [19].

In contrast to the traditional Web server architecture, commonly known as the Web2, where the safeguarding of user data is highly dependent on security mechanisms implemented by the centralized service providers, the decentralization of Web3 eliminates the authority of these entities [108]. This implies that users must protect their own security to a greater extent instead of relying on other institutions. For example, Web3 users need to control their own private keys independently [23, 58, 112]. The distinctive responsibility of users to ensure their own security means that the security of their digital assets and even the entire ecosystem is heavily influenced by their security behavior. Therefore, **comprehending users' perceptions of security** emerges as a critical endeavor, as it could not only deepen our understanding of their safety behavior but also guide the improvement of more robust systems.

Despite the importance of the user's responsibility in the security landscape of Web3, much of the existing academic research has concentrated on the technical layers of Web3 security, with a distinct lack of focus on the **user's perspective**. We strive to fill this gap by investigating user-perceived security risks and their adopted mitigation strategies in the Web3 ecosystem. Our study is to enhance the security and user experience in Web3, driven by a holistic understanding of user behavior and concerns. We propose the following research questions (RQs) to guide our inquiry:

RQ1: What security risks do users perceive at different layers of the Web3 ecosystem?

RQ2: What mitigation strategies have users adopted to address concerns at different layers of the Web3 ecosystem?

In this paper, we employ a two-stage study to address these two RQs. Firstly, we construct a Web3 ecosystem user interaction framework to facilitate the understanding of user interaction behaviors through observational research and open coding analysis. This framework comprises four layers: the blockchain system, Web3 DApp, online community, and off-chain cryptocurrency ecosystem. Secondly, based on this framework, we conduct semi-structured

*Corresponding author

CHI '24, May 11–16, 2024, Honolulu, HI, USA

ACM ISBN 979-8-4007-0330-0/24/05…$15.00
https://doi.org/10.1145/3613904.3642291

interviews (n = 21) to ascertain their perceived security risks at different layers of the Web3 ecosystem and the strategies they employ to mitigate these risks. Our findings reveal 12 security concerns expressed by users at various interaction levels and four types of measures implemented to address these concerns.

This paper makes three distinct contributions:

- First, through our research, we have gained an in-depth understanding of the security issues that are of primary concern to users when utilizing Web3, thereby better comprehending their apprehensions. This provides a novel perspective for research on security challenges in the blockchain domain.
- Second, our study develops a user interaction framework for the Web3 ecosystem, identifying security concerns across interaction layers. The framework also serves as a foundation in Web3 security based on user perspective, providing a comprehensive viewpoint for future research.
- Third, we have focused on understanding how users protect themselves when facing security challenges at different layers of the Web3 ecosystem, an aspect that has been neglected in previous research. This provides design implications for enhancing Web3 security from a user's perspective.

2 RELATED WORK

In this section, we explore the existing work concerning the Web3 ecosystem's security challenges and user perceptions. We aim to identify the gaps that our research addresses, particularly in light of how users perceive and mitigate security risks in Web3 applications.

2.1 Security Challenge in Web3 Ecosystem

The Web3 ecosystem represents an evolved form of decentralized digital infrastructure, substantially built on blockchain technology. It is designed to foster a user-centric internet experience by enabling features such as decentralized finance (DeFi), DAOs, and peer-to-peer digital asset transactions without the need for centralized intermediaries. According to Zhou et al. [115], the security challenges within the Web3 framework can be systematically categorized into five distinct layers: network layer, blockchain consensus layer, smart contract layer, protocol layer, and auxiliary services layer. Each of these layers targets different aspects of the ecosystem: the network and blockchain consensus layers primarily address the blockchain system itself; the smart contract layer focuses on contract implementation; and the protocol and auxiliary services layers are concerned with the design and functionality of Web3 applications. Below, we provide a succinct exploration of these layers in terms of three broad categories.

Blockchain System: This category encapsulates both the network and blockchain consensus layers. Vulnerabilities at this foundational level have extensive repercussions for the entire Web3 ecosystem. Research has covered an array of threats such as Eclipse attacks [37, 43], Distributed Denial of Service (DDoS) attacks [61, 90], and anomalies in consensus mechanisms like double-spending attacks [10]. While these studies make invaluable contributions from a technical standpoint, they often neglect the user experience and perception of these challenges.

Smart Contract: Positioned at the core of transactional logic within the Web3 ecosystem, the smart contract layer involves programmable contracts that execute automatically under predetermined conditions. Academic discourse has provided a rich technical analysis of vulnerabilities, including reentrancy issues [73, 86] and delegate call injection attacks [83]. However, these works seldom delve into how users navigate or perceive these vulnerabilities.

Web3 Applications: Incorporating both the protocol and auxiliary services layers, this category is where applications like DeFi and DAOs operate. Previous studies have scrutinized security issues specific to this layer, such as sandwich attacks [76, 99, 114] and flash loan attacks [77, 96]. Although some research has proposed real-time detection tools [94, 99, 109, 111], these solutions are highly technical and often overlook the actual user experience and security perception.

The security of the Web3 ecosystem necessitates a joint effort from two ends, which are the users and the underlying technology. We do recognize the importance of technology solutions. However, while these works have produced an extensive analysis of the technical security challenges of Web3, such as smart contract vulnerabilities, DeFi risks [15, 74, 94, 115], and the deployment of protective technologies [3, 11, 57, 59, 82, 95], security incidents and user losses persist unabatedly [100]. Consequently, we consider conducting the endeavors from a comprehensive understanding of the user end which is currently overlooked. There is a pressing need to understand not only the security vulnerabilities and their technical remedies but also the users' perspectives on these vulnerabilities, their responses to technical solutions, and the measures they adopt—or neglect—to safeguard themselves. This understanding is crucial as it provides valuable insights for developing more effective security policies and fostering a secure Web3 environment.

2.2 Security Awareness of Web3 Users

User perception of security in the Web3 ecosystem has gradually garnered attention, with a growing body of work addressing this crucial aspect. Most of these studies, however, have primarily focused on two main areas: private key management for digital wallets [65, 81, 91] and cryptocurrency asset management [30, 54]. Only a few studies have focused on the exploration of user perception within the realm of DeFi [99]. These topics indeed serve as the cornerstone for understanding how users interact securely within the Web3 space but they lack comprehensiveness.

For ordinary users, the complexities of encryption techniques and key management can be daunting [65, 81, 91]. Instances abound where mishandling of private keys has led to irreversible loss of assets. Scholars have proposed a variety of solutions from diverse perspectives, such as the utilization of cold wallets [51, 87], mnemonic backups [79], and multi-signature methods [41, 60, 68]. However, these studies have often not been integrated with an understanding of user perceptions, which is crucial for their practical application. Consequently, it remains uncertain whether these strategies can effectively mitigate the risk of key loss from the user's perspective.

Managing cryptocurrency portfolios introduces another layer of complexity and risk [30, 54]. Research indicates that users often lack sufficient knowledge to implement security measures effectively, exacerbated by challenges related to trust and privacy [30, 50, 81, 92].

Various studies also have attempted to cluster users based on their behavior and security perceptions concerning cryptocurrency management [1, 22, 32, 92], yet these efforts fail to provide a complete picture of the user experience in the Web3 space.

Furthermore, despite the issue of DeFi security within the Web3 ecosystem having increasingly garnered attention, there remains a dearth of user security awareness studies on this subject. For instance, Wang et al. [99] conducted research on users' awareness of the security risk posed by sandwich attacks in DeFi. However, this investigation was narrowly focused on a single security risk within the DeFi domain, thereby lacking in comprehensiveness. Other studies explore user perceptions on DeFi topics like auditing [28, 47] and stablecoins [40] but overlook security.

Previous studies were limited to narrow topics within the Web3 ecosystem and had a fragmented understanding of users, lacking a systematic summary covering user security awareness and mitigation strategies. Our objective is to fill these gaps by proposing a framework that helps understand user interactions in the Web3 ecosystem, guiding to a comprehensive, fundamental view of user perception and behavior, thereby providing a theoretical basis for improving the security of the ecosystem.

3 USER INTERACTIONS IN WEB3 ECOSYSTEM

We conducted an observational study to gain a foundational understanding of how users interact within the Web3 ecosystem. This preparatory study informed the design of our subsequent in-depth interviews, enabling us to design the interview protocol.

3.1 Study Method

To understand user interactions in the Web3 ecosystem, our observational study consisted of two key steps: information collection and open coding analysis.

We selected Ethereum as the focus of our observational study due to its leading Total Value Locked (TVL) and the extensive number of active protocols it hosts [20]. Our primary data was sourced from three key information channels listed on "ethereum.org", the official website of the Ethereum Foundation. These sources offer insights into how users interact within the ecosystem. Appendix A contains a sample list of our sources of information.

- **Officially Linked Articles:** These are found in ethereum.org's "Introduction to Web" section. They serve as both introductory resources and tutorials, detailing various interactive applications and outlining step-by-step user interactions with specific DApps.
- **On-chain Web3 DApps:** Links from the above articles and the Ethereum official website direct users to specific DApp homepages. For example, various DeFi projects such as lending, exchanges, liquid staking, and bridges, as well as the NFT marketplaces. These sites typically feature interactive sections and list tools necessary for user interaction.
- **Community-based User Discussions:** We observed user interactions on the official community platform provided by DApps, such as Discord. Users frequently share their activities with the project operators and others, providing insight into their interactions within the Web3 ecosystem.

We employed a hybrid coding method of deductive and inductive thematic analysis [29, 44] to dissect the data gathered from our primary sources. The deductive approach facilitated the establishment of five predefined themes, while the inductive coding process enabled the organization of four core user interaction scenarios that are frequently employed in this study. The detailed process of developing and iterating the framework using these two coding methods is described in Appendix B.

3.2 User Interaction Framework within the Web3 Ecosystem

The final user interaction framework within the Web3 ecosystem is depicted in Figure 1. This framework identifies the four primary scenarios of user interaction within the Web3 ecosystem: blockchain systems, Web3 DApps, online communities, and off-chain cryptocurrency ecosystems. Although the framework does not specifically encompass DApps such as games and the Metaverse, which preserve certain Web2 interaction paradigms (e.g., genres like the multiplayer online battle arena, commonly known as MOBA) [104], the generalizability is not compromised. This is attributed to the fact that fundamental interactions like liquidity mining, staking, and NFT trading in these DApps are often mirrored in other specific DApps, ensuring the framework's broad universality.

3.2.1 User Interactions with the Blockchain System. User interaction within the blockchain system spans reference points 1-3 in Figure 1 and includes a variety of behaviors, such as accessing specific blockchain networks and submitting transactions. In addition to users, blockchain operators develop and maintain the network and its protocols, and miners and verifiers process on-chain transactions. 1) Users have two main interaction options: the first is running an independent node to join the network, which requires technical expertise; the second, more common approach involves selecting a chain via digital wallet software for asset management and transactions. 2) Operators develop and maintain these application protocols. 3) Miners and verifiers validate and package transactions. The transaction records packaged on-chain are publicly transparent and verifiable for any user of the blockchain system.

3.2.2 User Interactions with the Web3 DApp. The interaction between users and Web3 DApps encompasses reference points 4-9 in Figure 1 and involves engaging with smart contracts provided by the application's project team. Besides users, DApp operators and other users are involved stakeholders. 4) Smart contracts of the DApp are deployed on the blockchain system. 5) When accessing a DApp, users choose from various DApps deployed on the blockchain and connect their digital wallet to the DApp, typically through its GUI. 6) Interacting with the DApp involves sending transactions on the blockchain to call functions in the smart contract. These smart contracts execute operations based on pre-defined rules and log the results on the blockchain. The DApp operators are responsible for maintaining and developing both 7) the smart contracts and 8) the GUI, with their contact information usually accessible through the GUI. 9) Smart contracts establish connections between users. For example, users can realize customer-to-customer (C2C) transactions with other users through smart contracts in DApp.

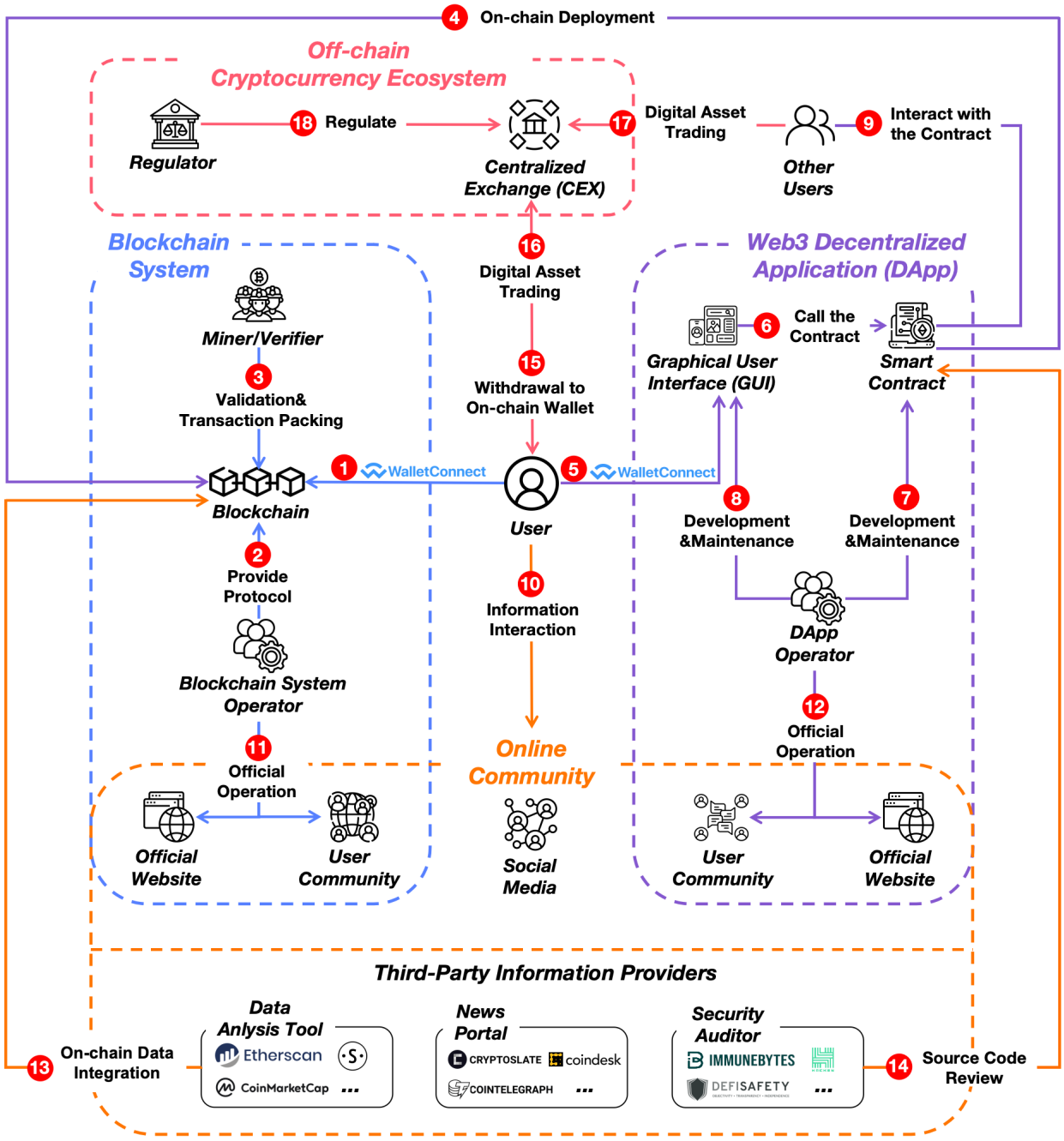

Figure 1: User Interaction Framework within Web3 Ecosystem. In the Web3 ecosystem, user interactions are mainly concentrated in four parts: blockchain system, Web3 DApp, online community, and off-chain cryptocurrency ecosystem. The connecting lines depicted in the diagram are not limited to representing user interactions but also include the activities of other stakeholders within the ecosystem, as well as the associations between key components. The numerical identifiers associated with the connecting lines in the figure serve as reference points during the comprehensive elucidation of the framework in Section 3.2.

3.2.3 User Interactions with the Online Community. The interaction between users and online communities corresponds to reference points 10-14 in Figure 1. 10) Users mainly interact with three types of information sources in online communities, which are operator-managed information sources, including official websites and user communities, social media, and third-party information providers.

- **Official Website & User Community:** The first type of online community is the official website and user community, which are both managed by the blockchain system and Web3 DApp operators. The operators of the 11) blockchain system and 12) DApp are responsible for managing and maintaining their respective project's official website and user community. On the official website, the operator displays basic project information, technical documents, and community information. They also maintain official accounts in user communities such as online forums, blogs, or chatrooms, where they regularly release information. Users can access project-related information through the official website and engage in discussions or interactions with other users in various communities.
- **Social Media:** The second type of online community is social media, represented by platforms such as Twitter. On these platforms, in addition to viewing the information released by official accounts, users can also follow many key opinion leaders (KOLs) in the Web3 community. Additionally, users can connect with other users on social media to exchange information and ideas.
- **Third-Party Information Provider:** The last type of online community is the third-party information provider, which can be categorized into three main groups. 13) The first group includes data analysis tools, such as the Ethereum blockchain explorer Etherscan [24], which records detailed information such as transaction data on the Ethereum chain. The second group comprises news portals, such as CryptoSlate [17], which provide users with timely news briefings related to Web3. 14) The third group consists of security audit companies, such as ImmuneBytes [48], which offer users smart contract audit reports. By interacting with these providers, users can easily access the information they desire.

3.2.4 User Interactions with the Off-chain Cryptocurrency Ecosystem. Interactions in off-chain cryptocurrency markets are a significant part of the Web3 ecosystem, as detailed in Figure 1 reference points 15 to 18. Off-chain interactions primarily occur through centralized exchanges (CEXes) and are often favored for simple token transactions or for avoiding on-chain gas fees. 15) Users can engage in direct asset trading on these off-chain platforms. 16) To transfer assets to a blockchain, users must provide their wallet address to the centralized exchange to facilitate the transfer. 17) Users can also interact with the other users of CEXes to conduct C2C transactions. 18) Lastly, CEXes are regulated by governmental bodies such as the Securities Regulatory Commission, making their official documents an additional valuable source of information for users.

4 INTERVIEW STUDY METHOD

In this section, we provide details about ethical considerations, recruitment, the research procedure, as well as design limitations.

4.1 Ethical Considerations

This study has been approved by the Institutional Review Board (IRB) at the University of Macau where the study was conducted. We did not collect any personally identifiable information from our participants. During our semi-structured interviews, we ensured that participants were aware of their right to decline to answer any questions without any impact on their participation compensation. The responses we cite in our findings are meant to illustrate patterns of user behavior, not unique or potentially identifiable circumstances of any individual.

4.2 Recruitment and Demographics

Web3 users chat on messaging platforms like Discord, Telegram, and Twitter are common places for discussion and information sharing [38]. To recruit participants for our study, we used the direct recruitment (n = 19) combined with snowball sampling (n = 5) method. We initially reached out to users in group chats on platforms, including Discord channels, Telegram discussion groups, and Twitter. We disseminated recruitment information, clarified the purpose of our research, and explained the methods we would employ to gather information.

Our recruitment and interview processes were intertwined rather than independent. Before the interview process, potential participants are guided through an exclusion procedure, as detailed in Appendix C. This process involves a series of questions to ascertain their interaction level and experience within the Web3 ecosystem.

During the interviews, we inquired if the directly recruited participants could share our recruitment information within their networks, leading to an additional 5 participants across four snowball sampling chains. We ensured balanced representation to prevent sample homogeneity domination by any single chain. This method, effective in capturing diverse perspectives, is common in previous studies [39, 70, 72]. In total, we contacted 24 (19 + 5) potential participants and interviewed 21 (16 + 5) who met our criteria. Table 1 summarizes participants' demographics.

4.3 Semi-structure Interview

Interviews were conducted between June and August 2023. We conducted interviews with 21 participants via online audio meeting. Each interview lasted 50-80 minutes. All interviewees understand that interviews will be recorded and their statements may be quoted anonymously in the final report. All data is considered confidential.

Our interview was structured into three distinct sections: personal information, security concerns, and mitigation strategies. First, participants were asked to provide personal information such as their occupation, and the duration of their involvement with Web3. In the second part, based on the user interaction framework obtained from our observational study, we designed interview questions from four aspects: blockchain system, Web3 DApp, online community, and off-chain cryptocurrency ecosystem. In the third section, participants were asked about any measures they had taken to mitigate the security concerns identified in the second section and the effectiveness of these measures. Follow-up questions were asked for detailed information about their Web3 interactions. A complete list of interview questions is provided in Appendix D.

Table 1: Interview Participants Demographics. In this study, four distinct snowball sampling chains were established, delineated as follows: 1) P01-P03-P08. 2) P04-P14. 3) P10-P13. 4) P17-P21. The remaining participants were incorporated into the study through direct recruitment. The participants recruited for this study were drawn from a diverse range of backgrounds, including technical developers, financial investors, and general users who were attracted to Web3 due to their personal interests. The participants' experience with Web3 interactions varied, ranging from several months to multiple years. Although some participants may not have extensive experience with DApps, they possess sufficient knowledge of cryptocurrencies.

ID	Gender	Country /Region	Use Span	Working Industry
P01	M	Chinese Mainland	>1yr	Software Development
P02	M	Singapore	>1yr	Business, Management, or Financial
P03	M	Chinese Mainland	6mo-1yr	PhD Student (Software Engineering)
P04	F	Hong Kong	>1yr	Business, Management, or Financial
P05	M	Chinese Mainland	>1yr	Software Development
P06	F	Chinese Mainland	>1yr	Business, Management, or Financial
P07	M	Malaysia	>1yr	Web3 Software Development
P08	M	Chinese Mainland	6mo-1yr	Law
P09	M	Taiwan	>1yr	Undergraduate Student
P10	F	Chinese Mainland	3-6mo	Business, Management, or Financial
P11	M	Chinese Mainland	>1yr	Software Development
P12	M	Taiwan	>1yr	Undergraduate Student
P13	M	Chinese Mainland	6mo-1yr	Software Development
P14	F	Hong Kong	>1yr	Key Opinion Leader
P15	M	Chinese Mainland	>1yr	Web3 Software Development
P16	M	Chinese Mainland	3-6mo	Undergraduate Student
P17	F	Chinese Mainland	3-6mo	Undergraduate Student
P18	M	Chinese Mainland	>1yr	Network Security
P19	F	Singapore	>1yr	Key Opinion Leader
P20	M	Chinese Mainland	6mo-1yr	Business, Management, or Financial
P21	M	Chinese Mainland	>1yr	Web3 Security

4.4 Data Analysis

Our methodology for analyzing the interview data involved a joint inductive-deductive approach, broken down into four principal steps. This approach aimed to systematically identify both security concerns and potential mitigations within the Web3 ecosystem.

In the first step, two researchers independently scrutinized a sample comprising 20% of the total interview transcripts. Each researcher inductively identified emerging themes related to Web3 security, based on thematic analysis [44]. After this initial identification, the researchers convened to compare and contrast the themes each had identified. Discrepancies were discussed, and themes were refined to generate a codebook specifically designed to capture Web3 security concerns and mitigation strategies.

To validate the reliability of the codebook, we randomly selected another 10% of the interview transcripts for independent, deductive analysis by the two researchers. This resulted in a Cohen's Kappa score of $\kappa = 87.7$ [67], indicating high interrater reliability and mutual understanding of the codebook and its constituent themes. Disagreements, though rare, were discussed among all researchers involved, leading to further refinement of the codebook. Lastly, the remaining 70% of the interview transcripts were divided between the two researchers, who then deductively applied the refined codebook. The outcomes of this coding were synthesized into a coherent set of findings that adhered to the structure of the codebook.

An assessment of data saturation was carried out by listing all emergent themes according to the sequence of the interviews, from P01 to P21. Our analysis revealed that no new themes emerged in the latter interviews, bolstering our confidence in the claim that our dataset had reached theoretical saturation. Accordingly, we believe that the framework developed provides a comprehensive insight into the security landscape of Web3 as perceived by its users.

4.5 Limitation

Our study has identified two principal limitations: the regional homogeneity of our interviewees and the unbalanced gender representation among participants.

Our respondent sample is mainly from Asian countries, especially mainland China. While the decentralized and global nature of blockchain technology reduces the likelihood of location-based bias affecting our conclusions, the geographical focus could introduce localized perspectives or concerns. Although we acknowledge this, our study serves as an exploratory investigation that offers initial insights into Web3 security. It is intended to pave the way for more expansive, geographically diverse studies that could enrich our understanding of global perspectives on these security issues.

Our participant group exhibits a gender imbalance, with females constituting only a third of the sample. Existing research strongly corroborates the gender gap in Web3 and cryptocurrency sectors [33–35]. This imbalance in our study might limit the range of security concerns raised, potentially skewing the insights toward predominantly male perspectives.

These limitations, while not affecting our core findings, do highlight areas where additional inquiry is warranted. In terms of geography, subsequent studies should aim for a broader, more varied geographical distribution to gain a more holistic understanding of Web3 security issues. Concerning the gender imbalance, targeted research focusing on the unique security experiences and perceptions of women in the Web3 environment could provide valuable insights into an often-overlooked segment of this ecosystem.

By consciously addressing these limitations, future research endeavors could yield a more comprehensive and nuanced landscape of Web3 security concerns and solutions.

5 SECURITY CONCERNS WITH WEB3 ECOSYSTEM (RQ1)

Through a combination of in-depth interviews and qualitative analysis, we have identified 12 primary security concerns that span the four foundational layers of the Web3 ecosystem: the blockchain system, Web3 DApps, online communities, and the off-chain cryptocurrency infrastructure. This section will delve into each of these concerns, providing a user-centric view of the security challenges at each interaction layer. The breakdown is contained in Table 2.

5.1 User Concerns with Blockchain System

As the foundational layer in the Web3 ecosystem, the blockchain system is the first point of interaction for users. The majority of respondents indicated a relatively high level of confidence in this layer's security. Their trust is largely rooted in the belief that blockchain systems have matured sufficiently to offer a stable and secure environment. One succinctly put it *"If the underlying blockchain system has problems that make ordinary users feel unsafe, then there is no point in participating in the blockchain"* (P05). However, a minority did voice concerns, which were chiefly centered around two aspects: centralization and system reliability.

Centralization. Centralization remains anathema to the fundamental tenets of blockchain, which espouse decentralized control and distributed authority. Users voiced concerns about the existence of central nodes with disproportionate influence, identifying them as potential single points of failure. *"...Perhaps it currently has very few nodes. If one of these nodes possesses significant computing power and fails, the entire system could become paralyzed"* (P11).

While the majority of participants (17 out of 21) prefer established blockchain systems with minimal concerns, a subset harbors reservations about engaging with newer blockchains. P19 expressed his concerns when involved in airdrop tasks [26] of a new blockchain, *"Some airdrop tasks necessitate transferring funds and engaging in other interactive activities on a new chain. My primary concern is whether an individual or group will exert control over this new chain and potentially manipulate my transactions"* (P19). The predominant apprehension among these users is the potential for abuse of power within the blockchain system. In instances where individuals or organizations controlling a blockchain system engage in such behavior, they may manipulate transaction data to the detriment of other users.

System reliability. Reliability stands as another pivotal factor in shaping user trust. Any glitches, vulnerabilities, or inefficiencies can have far-reaching consequences, ranging from data loss to failed transactions. P04 recounted her unsettling experience when interacting with a new blockchain, stating, *"I don't know why my transaction hasn't arrived after a long time, I don't know if the chain is under attack, and I'm not sure if my funds are directly lost"* (P04). Notably, mainstream chains like Ethereum, BSC, and Polygon did not trigger the same level of concern. Participants cited their long-standing market presence as a testament to their resilience against security threats, as P18 noted, *"These mainstream chains have operated for extended periods without crashing, demonstrating that their systems possess comprehensive measures and mechanisms for resisting and responding to security attacks"* (P18).

5.2 User Concerns with Web3 DApp

The Web3 DApps layer is of importance in the user's journey through the Web3 ecosystem. Concerns in this realm crystallize around four distinct categories: rug pulls, smart contract vulnerabilities, interactions with untrusted third parties, behavioral habit leakage, and multi-platform coordination anxiety.

Rug pull. The act of "rug pull"—where a project's operators entice investment before suddenly withdrawing and nullifying token value—is a looming threat, particularly in emerging Web3 sectors. Almost universally, participants conveyed apprehensions about becoming rug pull victims. Several admitted to having suffered financial losses due to such schemes. P09 recounted his experience with a project that utilized a blind box draw to entice daily investment, *"If you won the blind box, rewards would be returned. The orchestrator initially lulled users into a false sense of security before altering the contract on the final day, absconding with a substantial amount of USDT belonging to users"* (P09). Other participants expressed similar concerns when engaging with unfamiliar projects. *"Some project parties promise high returns and I worry that it may be a scam"* (P03). These security concerns arise from rug pull perpetrated by project parties and serve to undermine investor confidence while damaging the reputation and credibility of the broader blockchain ecosystem.

Smart contract mechanical vulnerabilities. Smart contracts are self-executing contracts with the terms of the agreement directly written into code. They serve as the backbone of DApps, providing the rules and logic that govern user interactions. However, the very features that make smart contracts revolutionary also make them susceptible to various risks, ranging from inherent design flaws to exploitable code vulnerabilities.

Interviewees with a technical background overwhelmingly identified smart contracts as the primary security issue in DApps. Concerns were twofold: firstly, issues arising from the design of the smart contract mechanism, and secondly, those originating from code vulnerabilities. For instance, some interviewees cited *"potential backdoors, special permissions for contract owners"* (P03), and *"deliberately flawed token issuance mechanisms"* (P01) as pressing concerns. Others pointed out specific code vulnerabilities such

Table 2: User Concerns with Web3 Ecosystem. We identified 12 security concerns in the Web3 ecosystem across four layers. These concerns are categorized by their interaction scenarios in the table.

Interaction Scenarios	Security Concerns	Explanation
Blockchain System	Centralization	Some people have too much power to manipulate the entire system, which deviates from the concept of decentralization.
	System reliability	The ability of the system to operate stably and resist attacks and other security threats.
Web3 DApp	Rug pull	DApp teams misuse their control over smart contracts to defraud investors by withdrawing liquidity, manipulating token prices, or abruptly closing projects.
	Smart contract mechanical vulnerabilities	Vulnerabilities in smart contract code and design mechanisms that could be exploited by hackers to steal funds or corrupt data.
	Authorized untrusted third parties	Authorizing the wallet to an untrusted third party allows them to transfer assets without notifying the user.
	Behavioral habit leakage	Hackers can learn the on-chain habits of a wallet owner by studying their transaction records.
	Multi-platform coordination anxiety	Users are worried and uneasy due to the operational complexity of multi-platform collaboration, security risks, and the uncertainty that cross-platform interactions may bring.
Online Community	Social engineering attack	Use deceptive means such as phishing to induce the victim to authorize the private key by using the victim's curiosity, trust, greed, and other psychology.
Off-chain Cryptocurrency Ecosystem	Compliance supervision	CEXes are supervised by relevant agencies. If there are any violations, it will affect its business operations and may lead to the freezing of user assets.
	CEXes collapse	CEXes may shut down due to poor management or malicious activities, leading to user asset loss.
	Illegal asset transaction	Participate in asset transactions that violate laws and regulations, or receive funds from unknown sources.
	Personal privacy leakage	Personally identifiable information uploaded by Know Your Customer (KYC) requirements was compromised.

as *"integer overflow*[1] *"* (P18) and *"reentrancy attacks*[2] *"* (P21) as potential pitfalls. Almost universally, these technically inclined users viewed smart contract security as their most significant worry during interactions with DApps.

On the flip side, non-technical users appeared less cognizant of the risks associated with smart contracts. *"I am aware that there may be issues with smart contracts, but I am not sure what specific problems may arise"* (P10). Even more concerning, some displayed misplaced confidence in the infallibility of deployed smart contracts. *"I believe that contract code that is already running on the blockchain should not have any problems. If there were any issues, it would not exist on the blockchain"* (P14). This statement was made in the context of her belief that there are always technically proficient individuals eager to verify smart contract codes. She holds a strong conviction that if a contract hasn't been compromised, it signifies that it has undergone successful verification and is free of issues.

Authorized untrusted third parties. The Web3 DApp ecosystem includes not only well-intentioned developers and users but also malicious third parties with the intent to misappropriate assets. These malevolent actors may abuse user-authorized data, manipulate code during transmission, or mimic legitimate projects, thus posing a range of security risks. Responses from the interviewees highlighted a generalized but palpable sense of concern and ambiguity about interacting with unfamiliar projects. *"I'm very worried about whether there will be some security issues with the projects I will be interacting with, but I don't know what they will do to me"* (P09). Instances of rogue actors deploying counterfeit DApps to mislead users are concerning. These DApps mimic legitimate URLs, posing a significant risk. P07 expressed this concern, *"I fear inadvertently accessing a fraudulent project's homepage and, upon linking my wallet and authorizing the contract, losing all funds contained therein"* (P07). Given the difficulty of vetting the long-term trustworthiness of these entities, respondents indicated that concerns about unauthorized third parties are likely to persist throughout their interactions within the Web3 environment.

[1] An integer overflow occurs when the result of an arithmetic operation exceeds the maximum value that can be stored in the integer's bit representation. For example, if we add 1 to the maximum value of uint8, which is 255, the result is 0, causing an integer overflow [28, 56, 93].

[2] The attacker writes an attacking contract contains the malicious code, calls the victim's contract and executes a loop in their own Fallback function to repeatedly execute a portion of the victim's contract code, thereby achieving the purpose of the attack [6, 28, 93].

Behavioral habit leakage. The transparency and immutability of blockchain technology can also serve as a double-edged sword, particularly concerning behavioral habit leakage. Given that all transactions and activities within DApps are permanently recorded and publicly available, there is the potential for third parties to analyze these data for patterns, potentially compromising user privacy. While most interviewees did not express significant concern about this issue, a subset was notably apprehensive. P11 indicated that if hackers could analyze their transaction history, targeted attacks might follow, *"If a hacker analyzes my transaction records through on-chain data, they may orchestrate a targeted attack"* (P11). Most other respondents (18 out of 21), however, downplayed such fears, largely attributing their unconcern to not being crypto whales[3] Nonetheless, they acknowledged the theoretical risk involved.

Multi-platform coordination anxiety. Engaging with Web3 DApps typically involves traversing various platforms, each with its own set of authentication and authorization demands. This multi-faceted process not only complicates user interactions but also elevates the potential for security breaches and fraud. The repeated need to verify identity and grant permissions across different platforms inherently increases exposure to such risks. P09 detailed this when discussing cross-chain bridges, *"In the airdrop task, I must acquire Ethereum tokens, transfer them across chains via bridges, and authorize on multiple platforms to interact with the desired DApp, increasing the risk of attacks"* (P09). Such concerns were also expressed by one respondent who was not proficient in English. *"Many of the interactive platforms of Web3 operate in English, a language barrier for me, so I can only explore them by myself. Additionally, I need to switch between many platforms. I was worried about accidentally hitting something in the process"* (P13).

5.3 User Concerns with Online Community

Online communities have emerged as an essential interface for users to interact with the Web3 ecosystem. They serve as a critical resource for information, opinion sharing, discussion, and problem-solving. Despite their utility, these platforms are not without risks—most notably the risk of social engineering attacks.

Social engineering attack. In line with existing literature [53], our interviews revealed that social engineering attacks, particularly phishing schemes, are a significant concern within Web3 online communities. These attacks exploit human psychological factors like curiosity, fear, and greed to deceive users into divulging personal information or assets.

Newer users in these communities are particularly vulnerable to phishing links, which are often disguised to look like legitimate information or offers. P17 shared, *"I check for airdrop mission information on Discord every day, but now there are too many phishing links that look similar. After clicking on one, I found that the website page was almost identical to the official website. It's difficult for me to determine if it's real or fake"* (P17). More experienced users, while less susceptible, are not entirely immune. *"Frequent community interaction exposes me to phishing, and I worry about mistakenly authorizing my wallet on a fake site"* (P19).

[3]Crypto whales are individuals or organizations that own a large amount of a coin or NFT collection. The size of the holding has to be large enough to cause a ripple effect on the price of the coin or NFT if the holder sells it all at once [107].

All of the users we interviewed reported encountering phishing attacks, albeit in different forms. Some scammers impersonate or even hijack official accounts to disseminate fraudulent information. Others engage in private messaging, posing as project administrators or tech support and sending seemingly benign links or files. More advanced forms of these attacks involve inducing users to download malware that steals sensitive information. The high incidence and evolving sophistication of social engineering attacks in Web3 online communities are causing users to remain vigilant of the interactions they engage in within these platforms.

5.4 User Concerns with Off-chain Cryptocurrency Ecosystem

Although CEXes are not the primary focus for blockchain interaction, they maintain a significant role within the broader Web3 ecosystem, often boasting higher trading volumes than DeFi markets. Despite being overseen by centralized institutions, our interviewees voiced concerns related to potential CEXes collapse, regulatory compliance, illegal asset transactions, and privacy leaks.

CEXes collapse. The collapse of CEXes involves the sudden cessation of their operations due to a variety of factors, including capital chain disruptions, security breaches, and investor pullouts. The closure of these platforms can result in irrecoverable losses for users. All interviewees displayed little worry for the security of major, high-volume CEXes like Binance. Concerns were primarily directed toward smaller exchanges with limited user bases. *"There are frequent news reports of exchanges suddenly closing, resulting in the loss of user assets. I worry about whether such an issue could occur on the exchange I use"* (P06). Personal experience also heightened concerns for some; P13 recounted an instance where an exchange he used declared bankruptcy. Although he was able to transfer their assets within a limited timeframe, the experience left him more apprehensive. Even with regulatory safeguards in place, the possibility remains that users may not be able to recover their assets should an exchange collapse.

Compliance supervision. CEXes must adhere to various local and international regulations to maintain legal operations. Non-compliance can lead to severe consequences, including operational bans. In countries with strict crypto regulations like China, this creates an additional layer of concern for users. *"One of my friends was investigated in the past. I don't know if that could happen to me one day, or if there would be any legal measures taken against me"* (P04). Users also questioned the security risks of using network proxies to circumvent regional restrictions. *"Due to regional restrictions, I have to use a network proxy to interact with CEXes. I'm not sure if this increases my security risks"* (P08). A prevailing concern among interviewees was the possibility of CEXes shutting down due to regulatory constraints. *"In the past, due to Singapore's cryptocurrency regulation, FTX went bankrupt. This kind of thing has certainly happened more than once. If my funds were there, the loss would be severe"* (P02). Regulatory compliance issues thus stand as a significant concern among our respondents regarding CEXes.

Illegal asset transactions. Despite regulatory safeguards, the risk of illegal asset transactions persists within CEXes. This risk poses significant legal and financial repercussions for innocent users who

may inadvertently transact with such assets. Interviewees indicated that concerns were relatively low but present. A couple of respondents were particularly worried, citing anecdotes from friends who had faced issues. *"If the counterparty you're transacting with seeks to exchange illegal funds, there's little you can do to prevent it. Even if you've done nothing wrong, your assets may still be frozen"* (P20). While not widespread, the concern about illegal asset transactions remains a notable issue among a subset of users.

Personal privacy leakage. The necessity for users to undergo KYC identity verification at CEXes has raised privacy concerns among our interviewees. These CEXes require a wide array of personal information—ranging from government-issued identification to contact details—creating a vulnerability for potential data leakage and consequent privacy compromise. Though none of our interviewees had directly experienced any security breaches, they still reported a high level of discomfort surrounding the KYC process. This unease stems primarily from fears about the potential future misuse of their personal data. P02 encapsulated these concerns, *"While I'm safe at the moment, exposing my personal information makes me worry about what's really going to happen in the future"* (P02). For Chinese users, strict regulations intensify these concerns, raising fears about potential government actions. *"If someone reports me, I feel like it will be easy to find me in the real world based on the personal information I uploaded on the centralized exchange"* (P08). This sentiment highlights a broader issue of trust and the tension between regulatory compliance and individual privacy.

6 MITIGATION STRATEGIES FOR DIFFERENT CONCERNS (RQ2)

Our study also uncovers the various mitigation strategies that users employ to address their security concerns in the Web3 ecosystem. These strategies have been organized into four overarching categories: risk assessment, risk aversion, risk diversification, and risk acceptance, each detailed in Figure 2. These categories align with specific security concerns they are designed to mitigate. In the following sections, we will delve into how users implement these strategies to address the diverse security concerns they face.

6.1 Risk Assessment

Risk assessment is a common mitigation strategy employed by respondents to reduce the financial risks associated with engaging in a new project. With little initial understanding of the project's landscape, users often find themselves confronted with an array of potential security risks such as rug pulls, unreliable smart contracts, and more. To mitigate these challenges, users typically engage in a multi-faceted risk assessment that involves four specific methods: open-source consultation, undergoing product trials, code reviews, and soliciting community advice.

Open-source consultation. Users frequently resort to open-source information and tools to assess the reliability and professionalism of blockchain systems and DApps when faced with ambiguous security implications. Trusted sources typically include white papers, team profiles, and financial statements. As P07 noted, *"The reliability of a project's technology may be enhanced if one of its founding team members has prior experience working at a market leader such as Binance"* (P07). Respondents with financial backgrounds often assess a project's credibility based on its investors, *"If Binance is an investor in the project, it is likely to be reliable due to the rigorous and thorough review process employed by such a large company"* (P04). Additionally, open-source tools such as revoking access and detecting vulnerabilities in smart contracts provide extra security layers, as P13 put it, *"Before interacting with a smart contract, I can input the contract into a vulnerability detection tool for analysis, saving me the effort of manually checking for vulnerabilities"* (P13). Participants perceive open-source consultation as a valuable tool for understanding a project's technical prowess.

Product trial. Product trials in Web3 DApps help users address concerns about rug pulls and multi-platform operations. These trials offer a hands-on assessment of a project's operational flow and underlying mechanisms. P19 described the experiences of product trials with a small amount of assets for avoiding rug pulls, *"First, use a small amount of money to experience and see if there is anything unreasonable in the business logic of this project"* (P19). Technical users utilize testnets [89] to safely experiment without affecting real assets. *"The test tokens used during the testing phase have no impact on the real tokens in the official version, so you can try them with confidence"* (P12). In the context of multi-platform collaboration, users also adopt this approach to enhance their proficiency in complex operations. *"Repeat the operation between multiple platforms several times. If there are no problems, you will feel more at ease"* (P13). Product trials offer respondents an early understanding of the project's working principles, reducing unease during formal funding interactions due to unfamiliarity.

Code review. A more technical approach to risk assessment involves code reviews, which are predominantly conducted by users with a technical background. This strategy aims to validate the project's business logic and functionality, *"The project's business logic, transaction strategy, and all operations involving user transactions can be verified by checking the code for issues"* (P05). Users also mentioned that continuous verification is essential as projects might switch codes, *"Always verify the contract before finalizing a transaction, as unscrutinized changes by the project team could lead to unintended asset authorization"* (P09). Respondents with technical backgrounds find code reviews beneficial in identifying potential security risks, enabling them to avoid risky projects.

Seeking community advice. Users often seek community input to mitigate uncertainties, especially those related to rug pulls and social engineering attacks. Users post their questions in online communities or consult with trusted individuals on social media. As P16 put it, *"If I come across a new project and I'm uncertain about its security, I will go to Discord and inquire if anyone is familiar with this project, if anyone has used it, and what their impressions are"* (P16). Positive feedback from other community members can significantly alleviate users' concerns about this project. Similarly, when respondents encountered suspected social engineering attacks in online communities, they sought help from others. *"When uncertain about an airdrop, I check community feedback. Shared experiences often reveal if it's a phishing attempt"* (P17). Seeking community advice, according to the respondents, provides insights into the project's development and community activity, both crucial indicators of project credibility.

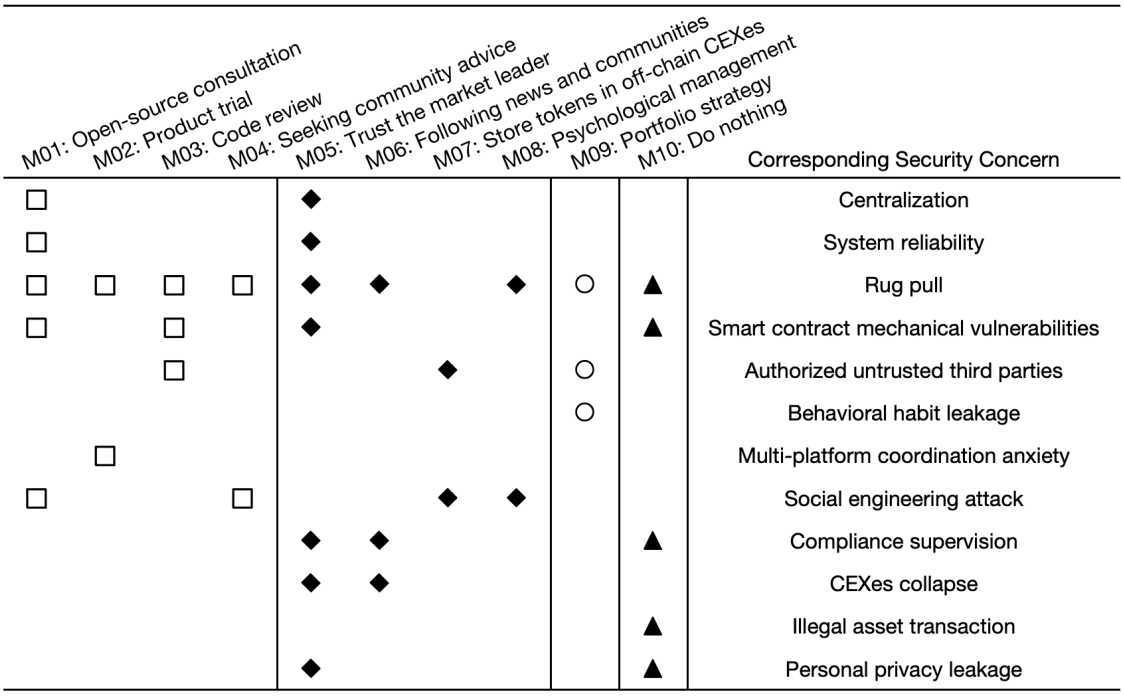

Figure 2: Mitigation strategies for different concerns. This matrix elucidates the relationship between users' security concerns and specific mitigation strategies. The matrix's initial row enumerates ten distinct strategies (M01 to M10), and the terminal column outlines the security concerns that each measure is equipped to mitigate. These ten strategies have been classified into four primary types, each symbolized by a unique icon: □ risk assessment, ♦ risk aversion, ○ risk diversification, and ▲ risk acceptance. Indeed, multiple mitigation strategies can address a single security concern, and conversely, a single strategy may tackle multiple concerns.

6.2 Risk Aversion

Risk aversion encompasses a set of proactive strategies aimed at avoiding potential security risks. These strategies are especially relevant when the perceived threats are significant or their scope is indeterminate. Respondents adopt this approach to eliminate the risks associated with engaging in uncertain projects. The mitigation strategies include four practices: trusting the market leader, following news and communities, storing tokens in off-chain CEXes, and psychological management.

Trusting the market leader. This strategy allows users to mitigate risks across various layers, including the blockchain system, Web3 DApps, and the off-chain cryptocurrency ecosystem. Users often opt to interact only with established projects that have demonstrated security reliability. In this study, market leaders refer to blockchain platforms or DApp protocols with the highest TVL, or CEXes with the greatest market share [66], which are preferred for their substantial user base and verified security. *"The most well-known projects with the largest number of users are usually pioneers in their field. Their continued existence in the market and resilience against attacks demonstrate their technical proficiency"* (P18). Several respondents (7 out of 21) also emphasized their confidence in these market leaders' capacity for effective emergency responses. *"Even if something goes wrong with such a project, users are likely to receive better compensation because these companies are not short on funds"* (P02). Across the board, respondents deemed this a straightforward yet effective risk mitigation approach.

Following news and communities. This strategy mainly targets the risk of "rug pulls" in Web3 DApps and security vulnerabilities linked to off-chain CEXes. Users rely on news platforms for timely and comprehensive updates on anomalous market states, evolving project developments, and pertinent regulatory guidelines. This information allows users to stay abreast of market fluctuations and respond promptly to prevent loss . *"These news platforms can publish news very quickly. They serve as a centralized information platform, which is more convenient than visiting individual project websites for information"* (P06). Community discussions were highlighted as another critical real-time information source by respondents. *"Community members often promptly report project anomalies, offering a faster alert system than news outlets, which face delays due to editorial processes"* (P11). Keeping informed with community insights and news updates could effectively provide a keen awareness to users of emerging risks under discussion.

Storing tokens in off-chain CEXes. Storing tokens in off-chain CEXes serves as a countermeasure against risks like unauthorized

wallet access within Web3 DApps and social engineering threats. By keeping assets off-chain, users mitigate the risks tied to on-chain interactions. *"This way, even if I am attacked or my wallet is stolen, I will not lose anything"* (P14). Users also apply this approach to evade social engineering attacks. *"Phishing links target the funds in my wallet, so as long as I keep them off-chain, they are relatively safe"* (P15). Respondents cited the centralized nature of CEXes as a contributing factor to their sense of security. *"It's like keeping funds in a bank. It's less risky than storing them in the digital wallet"* (P16). Participants believe that through centralized fund management, security concerns in decentralized networks have been mitigated effectively.

Psychological management. This measure primarily aims to manage risks stemming from human factors such as impulsiveness, curiosity, greed, and other psychological factors. Respondents pointed out that psychological disposition plays a significant role in susceptibility to scams. *"I used to believe it purely out of impulsiveness when I saw a well-promoted project, thinking that I could really make a lot of money, but in the end, I found out that it was a scam planned by the project party"* (P16). Subsequent restraint of impulsive tendencies has helped to reduce unnecessary risks. *"You must avoid greed and not assume that good things will happen to you"* (P12). Regarding phishing links, respondents concurred that avoiding the impulse to click unfamiliar links is generally sufficient to mitigate the threats. *"Phishing links are indiscriminate attacks. Those who are not driven by curiosity can completely avoid being attacked"* (P07). The interviewees agreed that managing their psychology can largely prevent falling into traps.

6.3 Risk Diversification

Risk diversification is a mitigation strategy that involves dispersing assets across multiple projects or savings methods. This tactic aims to minimize the impact of a security breach or financial loss in any single project or wallet. To this end, respondents employ diverse investment and asset management approaches.

Portfolio strategy. Adapting principles from traditional financial investment [42], respondents use portfolio strategy to minimize financial loss, particularly those caused by Web3 DApps security risks. This approach consists of allocating assets across a range of DApp projects so that any loss incurred in one project associated with security issues such as rug pull and smart contract mechanical vulnerabilities remains within acceptable limits. *"investment inevitably involves financial losses. At such times, it's crucial to ensure that your losses are bearable"* (P02). In addition to investing funds in different projects, managing funds in different wallets is also a measure of risk diversification. *"If you're concerned about potential security risks in a new project, simply create a new wallet and store only enough gas fees for interaction"* (P15).

Diversification is not merely a financial tactic but a comprehensive risk mitigation approach. It allows for more resilient asset management in the face of both financial volatility and potential security breaches. By diversifying assets across multiple projects or platforms, respondents are able to ensure that even if a security issue occurs on one project or platform, it will not have an uncontrollable and unbearable impact on the entire portfolio.

Respondents agree that the portfolio strategy, a key aspect of risk diversification, is effective in mitigating security concerns associated with Web3 DApps. This strategy's efficacy lies in its capacity to distribute risk, thereby insulating the entire portfolio from the adverse effects of a single project's failure. However, while portfolio diversification can reduce risk, it does not eradicate it entirely. The strategy's success is contingent upon careful project selection and ongoing portfolio monitoring. Thus, despite the perceived efficacy of the portfolio strategy, maintaining vigilance in project engagement is essential.

6.4 Risk Acceptance

Risk acceptance is a strategy acknowledging and bearing certain risks and their potential outcomes. This approach becomes relevant when respondents face financial security risks that are either uncontrollable or challenging to mitigate.

Doing nothing. A number of interviewees recognized that some risks, such as rug pulls and smart contract vulnerabilities at the Web3 DApp layer, as well as regulatory and security risks in the off-chain cryptocurrency ecosystem, are largely outside their sphere of influence. For instance, concerning rug pulls, they noted that despite conducting thorough due diligence, it's possible to still fall victim to malicious actions by the project's operators. *"If I have carefully checked the relevant information before participating and still encounter the rug pull, then I can do nothing but bear the loss because I can not control the project parties' behavior"* (P21).

Further, nearly one-third of respondents (8 out of 21) feel powerless over CEXes' unpredictability. *"If the exchange is shut down due to compliance issues, we ordinary users have nothing to do"* (P02). They also noted that they have no protection against receiving illegal assets on CEXes. *"When you choose to conduct C2C transactions with a user, you have no way of knowing whether the funds they transfer to you are legal. You can only bear the consequences yourself"* (P19). Regarding the issue of personal privacy leakage that may be caused by CEXes' KYC certification, one respondent who is worried about this chose to accept it after weighing the benefits and privacy leakage. *"The privacy I provided has already been leaked in the network environment outside the blockchain, so here I choose to accept the possible risks for the sake of profit"* (P02).

This approach of "doing nothing" isn't so much a strategy as it is an acknowledgment of the limitations individuals face in the context of broader systemic risks. While it does not offer an effective solution, it does provide a realistic perspective on risk management in a landscape marked by uncertainties and complexities.

7 DISCUSSION

Our research explores user perceptions of Web3 security issues and associated mitigation strategies. In this section, we first discuss a more general taxonomy of Web3 user security concerns, and how users perceive them. Then, we discuss how Web3 users behave differently than Web2 users in terms of security awareness. Finally, we discuss how stakeholders should address these security challenges when designing future applications.

7.1 Source of Security Issue in Web3 Ecosystem

Building on the analysis of user security concerns in the previous section, we categorize these concerns into three primary sources: technical security, regulatory security, and human-induced security, as outlined in Figure 3. Technical security issues arise from factors such as blockchain system centralization, smart contract vulnerabilities, and multi-platform coordination in Web3 DApps. Regulatory security pertains to legal considerations affecting asset security, including compliance and the legality of off-chain transactions. Human-induced security involves risks generated by individual actions, often exploiting existing vulnerabilities. This categorization aims to illuminate the varying levels of user awareness and perception across these different types of security risks.

7.1.1 Technical Security Concerns. Our findings indicate that technical security is generally not a primary concern for most users, save for a few who have specialized technical backgrounds. The intricacy of blockchain technology often serves as a high barrier to understanding for lay users, leading to blind spots and rendering some users less aware of specific security risks inherent in the system. Our results are consistent with prior studies, for example, Wang et al. [99] found that some users remain unaware of "sandwich attacks" due to a lack of technical expertise. Gao et al. [32] also highlighted the cognitive challenges non-technical users face in understanding intricate technical concepts.

The limited technical understanding of many users can inadvertently lead them to underestimate the potential security threats tied to blockchain platforms. For instance, some may hold the false belief that assets stored on well-known blockchain platforms are inherently secure, while not fully comprehending the risks associated with flawed smart contract designs. Although some users may be aware that smart contracts, once deployed, cannot be altered, they may not be cognizant of the fact that upgrades can be made through various mechanisms such as proxy contracts, logic contracts, and storage contracts. Such gaps in understanding provide avenues for malicious actors to exploit vulnerabilities, especially during the upgrade process, thereby posing financial risks to users.

The gap in technical understanding among general users raises important questions for both developers and educators in the Web3 space. As blockchain technology continues to mature, making it more accessible and comprehensible for ordinary users becomes increasingly important.

7.1.2 Regulatory Security Concerns. Regulatory security issues are predominantly a concern within the off-chain cryptocurrency ecosystem, particularly with CEXes. CEXes operate under stringent regulations and must obtain proper authorization from regulatory bodies in their jurisdiction. These regulations often include compliance with counter-terrorism financing, KYC, and anti-money laundering (AML) protocols [14, 55].

Failure to adhere to these regulations can lead to serious consequences for CEXes, such as increased scrutiny from authorities or even bankruptcy. As outlined in Section 5.4, users trading on these platforms are thereby exposed to substantial risks, ranging from asset freezing to total loss. High-profile cases, like the collapse of the FTX exchange, serve as cautionary tales, underscoring the gravity of these risks [7, 31].

Despite the stringent implementation of KYC and AML protocols designed to identify and curb suspicious activities, these systems are not foolproof. Users can still face the risk of unwittingly receiving illegal assets. For example, a user selling cryptocurrency on a CEX might unintentionally receive assets that were acquired through illegal means by the buyer, risking the subsequent freezing of the assets. Our study found that although this issue is a concern for users, there was a consensus among respondents that effective solutions are difficult to find, a finding shown in Section 6.4.

The concerns around regulatory security underscore the need for ongoing dialogue between CEXes, regulators, and users. On one hand, CEXes could benefit from adopting more robust risk management measures and providing clearer communication about potential risks. On the other hand, regulatory bodies should consider the implications of stringent regulations that might unintentionally expose users to heightened risk.

7.1.3 Human-Induced Security Concerns. Human factors emerged as a central theme in the security concerns articulated by our interviewees. Specifically, the focus was primarily on rug pulls orchestrated by Web3 DApps' project parties and social engineering attacks that occur in online communities. These issues intensify the security risks surrounding user assets, primarily because of the unpredictability and uncontrollability inherent in human behavior.

For instance, rug pulls in the context of a Web3 DApp involve the malicious intent of project owners who may unexpectedly abscond with investor funds. As discussed in Sections 5.2 and 6.4, this issue garnered significant attention among interviewees, all of whom had taken steps to mitigate against such risks. The unpredictable nature of rug pulls poses a challenge in risk assessment, as investors cannot easily determine the likelihood of such events. Previous studies have corroborated the frequency and severity of rug pulls within the DeFi investment landscape, urging investors to exercise caution [2, 16, 21].

Similarly, social engineering attacks also fall under the realm of unpredictable and uncontrollable human behavior. Such attacks can be executed without requiring direct user involvement and use a range of tactics to deceive users. Section 5.3 elaborates on how interviewees reported the prevalence of phishing links within online communities, an observation supported by existing literature [4, 9, 105]. However, our respondents were actively seeking countermeasures to protect themselves, as detailed in Section 6.

These findings suggest that the Web3 community could benefit from targeted educational efforts addressing human-induced security concerns, alongside the development of trust mechanisms or vetting processes for Web3 projects. Additionally, since the unpredictability of human behavior presents a constant risk, tools, and services that empower users to make informed decisions could be vital in enhancing overall security within the Web3 ecosystem.

7.1.4 The Influence of User Background Diversity on Security Perception. Our findings indicate that there are differences in security perceptions between non-technical participants (P02, P04, P06, P08, P10, P14, P17, P19) and others with a technical background or experience. These differences underscore the potential influence of user background on their security awareness within Web3.

Non-technical users often have a limited understanding of security risks, leading to potential blind spots. Despite this, some

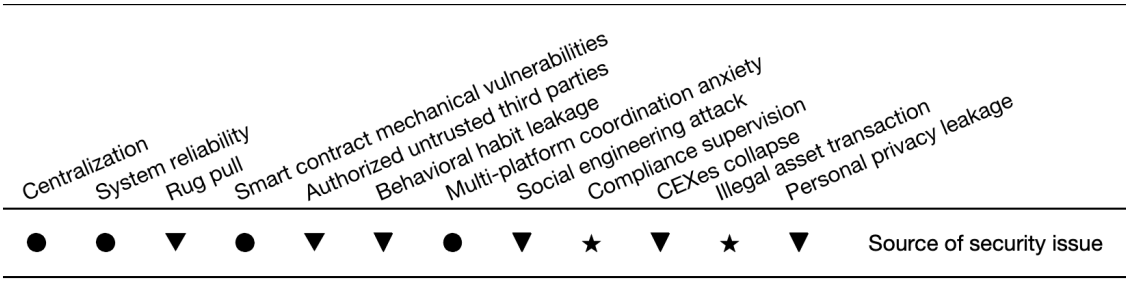

Figure 3: Taxonomy of Security Concerns. The first row of the matrix lists the specific user security concerns we identified in Section 5. The second row delineates the correlation between the user security concerns and the source of security issues. The three symbols employed here signify three distinct categories of security issue sources: ● technical security, ⋆ regulatory security, and ▼ human-induced security.

of them appear to have little interest in expanding their knowledge. P14, as referenced in Section 5.2, believes that technically proficient individuals always verify smart contracts, implying the contract already deployed in the chain is problem-free. However, she overlooks potential risks, such as reentrancy attacks and other exploitations [28]. P02 and P10 were confident that hackers targeted the crypto whales but not them, thereby ignoring the importance of smart contract code security.

This is in sharp contrast to the technology-centric view, for example, P05, which attributes all issues to smart contract code and advocates for code review as a mitigation strategy. Nevertheless, a disproportionate focus on coding practices can lead to a neglect of code low-related security concerns, such as vulnerabilities to social engineering attacks, resulting in a broader spectrum of security challenges. P01, P12, and P15 believe that if no loopholes are found in the contract code before participating in the project, there is a high probability that there will be less serious security problems later. But this seems to have weakened their vigilance against security risks led by human factors such as rug pull.

The emergence of such instances within our research highlights the necessity of understanding differences in users' security perceptions. This exploration can guide the development of more effective user education programs and security policies. Informed by the Technology Acceptance Model (TAM) [18], the Availability Heuristic [13], and theories of Overconfidence Bias and Optimism Bias [84], we formulate three hypotheses within this context:

- **H1:** A positive correlation exists between users' technical expertise and their comprehension of security risks.
- **H2:** A positive correlation exists between users' concerns about security risks and the number of attacks they have experienced in the past.
- **H3:** A negative correlation exists between users' trust in technology and their awareness of potential risks.

These hypotheses could provide an initial point for a quantitative investigation into this critical aspect of the Web3 ecosystem to further verify the understanding of the security perception of diverse users.

7.2 Contrasting User-Perceived Security Issues in Web2 and Web3 Environments

Our investigation into Web3's user-perceived security concerns reveals issues unique to its decentralized architecture, contrasting with the centralized Web2. While Web2 has been subject to comprehensive scrutiny—covering security vulnerabilities ranging from real-world privacy leaks [8] to social engineering attacks [80]—Web3 introduces its unique array of challenges. These security issues are not mere extensions of their Web2 counterparts; rather, they are fundamentally distinct, driven by Web3's unique architecture and user interaction dynamics. As a result, a nuanced, comparative exploration between these two platforms becomes imperative. Such a study will not only illuminate why some security strategies that are effective in the Web2 world might be inadequate for Web3 but will also inspire Web3-specific security frameworks. This section is committed to dissecting these disparities, thereby enriching our understanding of the rapidly changing security landscapes within the Web3 sphere. Our comparison primarily focuses on two dimensions: their intrinsic nature, characterized by centralization in Web2 versus decentralization in Web3, and their operational mechanisms, typically monolithic in Web2 as opposed to fragmented in Web3.

Disparities in ecosystem characteristics and their security implications. One of the most striking differences between Web2 and Web3 resides in the core architecture of their ecosystems: Web2 is centralized, while Web3 is decentralized [108]. This fundamental distinction causes a marked shift in user priorities concerning security. In the Web2 domain, the primary concern is the protection of personal data. Conversely, in Web3 environments, users tend to prioritize asset security over data privacy.

Within Web2 platforms, users often find their data centralized on servers managed by major tech companies like Google, Facebook, and YouTube. These platforms lure users with free services, subsequently amassing considerable stores of identity and behavioral data. Such centralization increases the risk of unauthorized data usage and privacy violations. Contrastingly, Web3, which is built on the foundation of blockchain technology, eliminates the need for a centralized authority to manage user data and assets [112]. This

decentralization places the responsibility for data and asset management squarely on the users themselves. While on-chain transactions are pseudonymous, providing some level of privacy, this is contingent on not linking blockchain addresses to real identities. Nevertheless, as indicated in Section 5, off-chain cryptocurrency systems still pose potential risks to personal privacy.

Asset security, which often is not perceived as the most serious risk by users in Web2 due to protective mechanisms provided by centralized institutions like banks, gains prominence in Web3. Section 5 lists twelve security concerns, of which all but one ("Personal privacy leakage", focusing on off-chain personal privacy) directly relate to asset security. In Web2, users can seek institutional support for security issues like social engineering attacks, whereas Web3 users must independently handle security. Although some cryptocurrency platforms can blacklist fraudulent transactions, such actions are generally reactive and not consistently available for all users. Thus, Web3 users are compelled to devise their security strategies, a challenge distinct from Web2 experiences. This situation intensifies user concerns about asset security, highlighting an urgent need for innovative, Web3-specific security solutions.

Disparities in operational workflows and their security implications. Centralization and decentralization bring about contrasting operational workflows in Web2 and Web3 platforms. Web2 is typically characterized by a monolithic, server-client architecture [71]. This architecture centralizes services like search, social networking, and transactions into one platform, simplifying the user experience, and thus negating the need for users to hop between multiple platforms. In contrast, Web3's decentralized nature leads to fragmented services [103] that often necessitate multi-platform collaboration to accomplish end-to-end operational processes.

This fragmentation in Web3 adds layers of complexity to user operations. For example, in Web2, a user can seamlessly move from product selection to payment and customer service within a single e-commerce platform. The platform automates various steps such as navigation and data caching. In Web3, tasks like DeFi interactions involve more intricate steps and multiple platforms. Users not only need to manage assets through digital wallets and purchase coins from exchanges but also engage in complex operations like smart contract authorization and cross-chain asset deployment. Furthermore, the use of native tokens in Web3 DApps necessitates additional asset management tasks for users.

This fragmented operational landscape in Web3 introduces unique security challenges. Users may find themselves navigating a gamut of risks, from transaction front-running to on-chain asset theft [12], along with issues such as rug pulls, as discussed in Section 5.2. Multi-platform collaboration increases the system's vulnerability, introducing additional security issues like flash loan attacks. Interviewed users voiced their apprehensions about these intricate workflows and the diverse risks that multi-platform interactions bring, as explored in detail in Section 5.

Due to the multi-entity collaboration involved in these fragmented workflows, security solutions from the Web2 ecosystem are often not directly translatable to Web3. This operational fragmentation gives rise to Web3-specific security concerns, requiring users to independently devise strategies for mitigating these risks, as cataloged in Figure 2 in Section 6. As a result, enhancing security in the Web3 landscape demands bespoke solutions that address its unique challenges and operational intricacies.

7.3 Design Implications

This section aims to shed light on actionable design considerations for enhancing user security within the multifaceted Web3 ecosystem, which includes blockchain systems, Web3 DApps, online communities, and off-chain cryptocurrency networks. Drawing on the insights gathered from our empirical study—specifically, those outlined in Section 6 and Section 7.1—we focus on addressing the triad of security issues identified: technical deficiencies, regulatory limitations, and human-induced vulnerabilities.

It is worth mentioning that since previous solutions to the security design of digital wallets have been discussed in academia [5, 25, 36, 49], we do not focus on the optimal design of the wallet here.

Reducing technical security issues through education. Our research underscores a shortfall in user understanding of technical security within the Web3 ecosystem, often leading to misplaced confidence and the overlooking of potential risks. For instance, the intricacies of smart contract revocation are often misunderstood. Bridging this gap requires educational initiatives from ecosystem stakeholders to improve user awareness and security issue comprehension.

Developers of blockchain systems could go beyond mere documentation to deliver technical security insights in user-friendly formats, such as easy-to-digest video animations. By incentivizing user engagement with these educational resources, developers can empower users with a better grasp of both the risks and possible mitigation strategies. Meanwhile, operators of Web3 DApps could offer comprehensive yet accessible introductory guides that spell out potential security risks, complemented by real-time prompts highlighting specific interactions where risks could emerge. Finally, community leaders could enhance technical education by hosting online seminars featuring knowledgeable users who can elucidate technical security aspects, thereby fostering a community-centered learning environment conducive to mutual assistance.

Reducing regulatory security issues through information dissemination. As detailed in Section 7.1, users often find themselves with limited avenues for addressing security challenges emanating from regulatory constraints. The influence of external regulatory bodies severely curtails the effectiveness of any user-initiated preventative measures. According to our findings in Section 6, users frequently resort to staying updated through news outlets as their primary strategy, using such real-time information to make timely decisions, such as asset transfers. In light of this, the subsequent discussion emphasizes the critical role various stakeholders can play in mitigating these challenges.

News portals can significantly contribute by expanding the scope and channels of information dissemination to ensure timely, widespread access. For example, users could opt-in to specific CEXes-related updates delivered through a plethora of mediums—be it news platforms, email notifications, or official social media accounts like Twitter. Additionally, the introduction of innovative presentation formats, such as expert analyses and opinion pieces, can help deepen user comprehension of the implications of regulatory changes, thereby enabling more informed decision-making.

On the other hand, CEXes have a responsibility to offer users actionable emergency plans from the get-go. These plans should be easily accessible. CEXes should also maintain active, transparent communication, especially during the preliminary stages of any regulatory implementations. This could include publishing regular updates and statements, as well as sending multiple reminders to users. The aim is to prevent users from missing critical information that could impact the security of their assets.

Reducing human-induced security issues through risk detection. Human-induced security risks pose a significant concern for users navigating the Web3 ecosystem. The inherent unpredictability and uncontrollability associated with human behavior make these risks particularly challenging to manage. Timely detection and alerts, or even direct mitigation of these risks at their origin, could significantly alleviate user concerns. Existing literature on risk detection systems [64, 110] mainly focuses on platforms other than DApps or online communities. This discussion, therefore, turns its lens on the potential for implementing risk-detection plugins within DApps and online communities, offering a fresh viewpoint on risk management in these environments.

For Web3 DApps, developers could explore the integration of specialized plugins designed to identify vulnerabilities and potential security threats. These plugins would be capable of interpreting, monitoring, and auditing both smart contract code and on-chain data. Upon identifying red flags, such as sudden spikes in token sales from the developers or tokens that can be bought but not sold, these plugins could automatically notify users through the interface or send background notifications. This could enhance user response and reduce the need for manual transaction checks, mitigating the impact of security breaches. Similarly, online community administrators could also embed risk detection mechanisms within their platforms. For example, a plugin could automatically scan and assess the risk level of external links shared within the community. If high-risk links, such as phishing schemes, are detected, the plugin could block them at the source, preventing further dissemination and thereby increasing the overall security of the platform.

8 CONCLUSION

In this study, we introduce a user interaction framework of the Web3 ecosystem. Utilizing this as a foundation, we delve into the security concerns of users corresponding to each layer of the framework and their respective countermeasures to mitigate security risks. Our comprehensive exploration illuminates users' perception of security within the Web3 ecosystem, thereby offering valuable insights corresponding to security which could potentially steer the evolution of the various programs within the Web3 landscape.

ACKNOWLEDGMENTS

This work is supported by the Macao Science and Technology Development Fund (File no. 0129/2022/A and no. 0078/2023/AMJ) and the University of Macau (File no. MYRG-CRG2022-00013-IOTSC-ICI). We would like to thank the Faculty of Science and Technology, University of Macau for providing a travel grant to support the presentation of this work. We would also like to thank Prof. Yang Wang for the discussion on this paper.

REFERENCES

[1] Svetlana Abramova, Artemij Voskobojnikov, Konstantin Beznosov, and Rainer Böhme. 2021. 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*. 1–19.

[2] Sharad Agarwal, Gilberto Atondo-Siu, Marilyne Ordekian, Alice Hutchings, Enrico Mariconti, and Marie Vasek. 2023. Short Paper: DeFi Deception–Uncovering the prevalence of rugpulls in cryptocurrency projects. Stichting Financial Cryptography/International Financial Cryptography ....

[3] Ayman Alkhalifah, Alex Ng, Paul A Watters, and ASM Kayes. 2021. A mechanism to detect and prevent ethereum blockchain smart contract reentrancy attacks. *Frontiers in Computer Science* 3 (2021), 598780.

[4] AA Andryukhin. 2019. Phishing attacks and preventions in blockchain based projects. In *2019 international conference on engineering technologies and computer science (EnT)*. IEEE, 15–19.

[5] Myrto Arapinis, Andriana Gkaniatsou, Dimitris Karakostas, and Aggelos Kiayias. 2019. A formal treatment of hardware wallets. In *Financial Cryptography and Data Security: 23rd International Conference, FC 2019, Frigate Bay, St. Kitts and Nevis, February 18–22, 2019, Revised Selected Papers 23*. Springer, 426–445.

[6] Nicola Atzei, Massimo Bartoletti, and Tiziana Cimoli. 2017. A survey of attacks on ethereum smart contracts (sok). In *Principles of Security and Trust: 6th International Conference, POST 2017, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2017, Uppsala, Sweden, April 22-29, 2017, Proceedings 6*. Springer, 164–186.

[7] BBCNews 2023. Crypto giant FTX collapses into bankruptcy. https://www.bbc.com/news/business-63601213.

[8] France Bélanger and Robert E Crossler. 2011. Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly* (2011), 1017–1041.

[9] Chandra Sekhar Bhusal. 2021. Systematic review on social engineering: Hacking by manipulating humans. *Journal of Information Security* 12 (2021), 104–114.

[10] George Bissias and Brian Neil Levine. 2020. Bobtail: Improved Blockchain Security with Low-Variance Mining.. In *NDSS*.

[11] Agostino Capponi, Ruizhe Jia, and Ye Wang. 2023. Blockchain Private Pools and Price Discovery. In *AEA Papers and Proceedings*, Vol. 113. American Economic Association, 253–256.

[12] Agostino Capponi, Ruizhe Jia, and Ye Wang. 2023. Do Private Transaction Pools Mitigate Frontrunning Risk? *Cryptology ePrint Archive* (2023).

[13] John S Carroll. 1978. The effect of imagining an event on expectations for the event: An interpretation in terms of the availability heuristic. *Journal of experimental social psychology* 14, 1 (1978), 88–96.

[14] CEX and DEX 2023. Forskellen mellem CEX og DEX. https://www.binance.com/da-DK/feed/post/217547.

[15] Huashan Chen, Marcus Pendleton, Laurent Njilla, and Shouhuai Xu. 2020. A survey on ethereum systems security: Vulnerabilities, attacks, and defenses. *ACM Computing Surveys (CSUR)* 53, 3 (2020), 1–43.

[16] Lin William Cong, Kimberly Grauer, Daniel Rabetti, and Henry Updegrave. 2023. The Dark Side of Crypto and Web3: Crypto-Related Scams. *Available at SSRN 4358572* (2023).

[17] CryptoSlate 2023. CryptoSlate - News, Insights, and Data. https://cryptoslate.com/.

[18] Fred D Davis. 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly* (1989), 319–340.

[19] DeFi Lost 2023. De.Fi Rekt Report: Over 204m dollars Lost in Q2 2023. https://de.fi/blog/de-fi-rekt-report-over-204m-lost-in-q2-2023.

[20] DefiLemma 2023. DefiLlama - Total Value Locked All Chains. https://defillama.com/chains.

[21] Saulo Dos Santos, Japjeet Singh, Ruppa K Thulasiram, Shahin Kamali, Louis Sirico, and Lisa Loud. 2022. A new era of blockchain-powered decentralized finance (DeFi)-a review. In *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE, 1286–1292.

[22] Janna Lynn Dupree, Richard Devries, Daniel M Berry, and Edward Lank. 2016. Privacy personas: Clustering users via attitudes and behaviors toward security practices. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. 5228–5239.

[23] Shayan Eskandari, Jeremy Clark, David Barrera, and Elizabeth Stobert. 2018. A first look at the usability of bitcoin key management. *arXiv preprint arXiv:1802.04351* (2018).

[24] Etherscan 2023. The Ethereum Blockchain Explorer. https://etherscan.io/.

[25] Ittay Eyal. 2022. On cryptocurrency wallet design. In *3rd International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2021)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik.

[26] Sizheng Fan, Tian Min, Xiao Wu, and Wei Cai. 2023. Altruistic and Profit-oriented: Making Sense of Roles in Web3 Community from Airdrop Perspective. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–16.

[27] Sizheng Fan, Tian Min, Xiao Wu, and Cai Wei. 2023. Towards understanding governance tokens in liquidity mining: a case study of decentralized exchanges. *World Wide Web* 26, 3 (2023), 1181–1200.

[28] Ding Feng, Rupert Hitsch, Kaihua Qin, Arthur Gervais, Roger Wattenhofer, Yaxing Yao, and Ye Wang. 2023. DeFi Auditing: Mechanisms, Effectiveness, and User Perceptions. *Cryptology ePrint Archive* (2023).

[29] Jennifer Fereday and Eimear Muir-Cochrane. 2006. Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *International journal of qualitative methods* 5, 1 (2006), 80–92.

[30] Michael Fröhlich, Felix Gutjahr, and Florian Alt. 2020. Don't lose your coin! Investigating Security Practices of Cryptocurrency Users. In *Proceedings of the 2020 ACM Designing Interactive Systems Conference*. 1751–1763.

[31] FTX collapse 2023. The Collapse of FTX: What Went Wrong With the Crypto Exchange? https://www.investopedia.com/what-went-wrong-with-ftx-6828447.

[32] Xianyi Gao, Gradeigh D Clark, and Janne Lindqvist. 2016. Of two minds, multiple addresses, and one ledger: characterizing opinions, knowledge, and perceptions of Bitcoin across users and non-users. In *Proceedings of the 2016 CHI conference on human factors in computing systems*. 1656–1668.

[33] Gendergap 2023. Web3 Already Has a Gender Diversity Problem. https://www.bcg.com/publications/2023/how-to-unravel-lack-of-gender-diversity-web3.

[34] Gendergap 2023. WEB3 DEMOGRAPHICS: THE USERS BEHIND WEB3. https://movementstrategy.com/editorial/users-web3-demographics/.

[35] Gendergap 2023. The Web3 gender gap, by the numbers. https://www.bcg.com/publications/2023/how-to-unravel-lack-of-gender-diversity-web3.

[36] Rosario Gennaro, Steven Goldfeder, and Arvind Narayanan. 2016. Threshold-optimal DSA/ECDSA signatures and an application to bitcoin wallet security. In *Applied Cryptography and Network Security: 14th International Conference, ACNS 2016, Guildford, UK, June 19-22, 2016. Proceedings 14*. Springer, 156–174.

[37] Arthur Gervais, Ghassan O Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan Capkun. 2016. On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. 3–16.

[38] Sam Gilbert. 2022. Crypto, web3, and the Metaverse. *Bennett Institute for Public Policy, Cambridge, Policy Brief* (2022).

[39] Leo A Goodman. 1961. Snowball sampling. *The annals of mathematical statistics* (1961), 148–170.

[40] Yongqi Guan, Yaman Yu, Tanusree Sharma, Kaihua Qin, Yang Wang, and Ye Wang. [n. d.]. Examining User Perceptions of Stablecoins: Understandings and Risks. ([n. d.]).

[41] Jongbeen Han, Mansub Song, Hyeonsang Eom, and Yongseok Son. 2021. An efficient multi-signature wallet in blockchain using bloom filter. In *Proceedings of the 36th Annual ACM Symposium on Applied Computing*. 273–281.

[42] Barry Hedley. 1977. Strategy and the "business portfolio". *Long range planning* 10, 1 (1977), 9–15.

[43] Ethan Heilman, Alison Kendler, Aviv Zohar, and Sharon Goldberg. 2015. Eclipse attacks on {Bitcoin's}{peer-to-peer} network. In *24th USENIX security symposium (USENIX security 15)*. 129–144.

[44] Judith A Holton. 2007. The coding process and its challenges. *The Sage handbook of grounded theory* 3 (2007), 265–289.

[45] Hong Kong CBDC 2023. Hong Kong Monetary Authority to Prepare for Retail CBDC. https://www.coindesk.com/policy/2023/06/09/hong-kong-monetary-authority-to-prepare-for-retail-cbdcs/.

[46] Hong Kong Web3 2023. Hong Kong Sets Up Task Force for Web3 Development. https://www.coindesk.com/policy/2023/07/03/hong-kong-sets-up-task-force-for-web3-development/.

[47] Zhuangtong Huang, Jiawei Zhu, Zhongyu Huang, Yixin Xu, Jerome Yen, and Ye Wang. 2022. Safeguarding the Unseen: a Study on Data Privacy in DeFi Protocols. *arXiv e-prints* (2022), arXiv–2211.

[48] Immunebytes 2023. Blockchain Audit Services. https://www.immunebytes.com/.

[49] Stanislaw Jarecki, Aggelos Kiayias, Hugo Krawczyk, and Jiayu Xu. 2016. Highly-efficient and composable password-protected secret sharing (or: How to protect your bitcoin wallet online). In *2016 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 276–291.

[50] Irni Eliana Khairuddin and Corina Sas. 2019. An Exploration of Bitcoin mining practices: Miners' trust challenges and motivations. In *Proceedings of the 2019 CHI conference on human factors in computing systems*. 1–13.

[51] Abdul Ghaffar Khan, Amjad Hussain Zahid, Muzammil Hussain, and Usama Riaz. 2019. Security of cryptocurrency using hardware wallet and qr code. In *2019 International Conference on Innovative Computing (ICIC)*. IEEE, 1–10.

[52] Gaurish Korpal and Drew Scott. 2022. Decentralization and web3 technologies. (2022).

[53] Katharina Krombholz, Heidelinde Hobel, Markus Huber, and Edgar Weippl. 2015. Advanced social engineering attacks. *Journal of Information Security and applications* 22 (2015), 113–122.

[54] Katharina Krombholz, Aljosha Judmayer, Matthias Gusenbauer, and Edgar Weippl. 2017. The other side of the coin: User experiences with bitcoin security and privacy. In *Financial Cryptography and Data Security: 20th International Conference, FC 2016, Christ Church, Barbados, February 22–26, 2016, Revised Selected Papers 20*. Springer, 555–580.

[55] KYC 2023. What Is KYC and Why Does It Matter For Crypto? https://www.coindesk.com/learn/what-is-kyc-and-why-does-it-matter-for-crypto/.

[56] Enmei Lai and Wenjun Luo. 2020. Static analysis of integer overflow of smart contracts in ethereum. In *Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy*. 110–115.

[57] Jing Li, Tianming Yu, Ye Wang, and Roger Wattenhofer. 2022. Dynamic byzantine broadcast in asynchronous message-passing systems. *IEEE Access* 10 (2022), 91372–91384.

[58] Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, and Qiaoyan Wen. 2020. A survey on the security of blockchain systems. *Future generation computer systems* 107 (2020), 841–853.

[59] Zecheng Li, Bin Xiao, Songtao Guo, and Yuanyuan Yang. 2022. Securing deployed smart contracts and DeFi with distributed TEE cluster. *IEEE Transactions on Parallel and Distributed Systems* 34, 3 (2022), 828–842.

[60] Hung-Zih Liao and Yuan-Yuan Shen. 2006. On the elliptic curve digital signature algorithm. *Tunghai Science* 8 (2006), 109–126.

[61] Il-Kwon Lim, Young-Hyuk Kim, Jae-Gwang Lee, Jae-Pil Lee, Hyun Nam-Gung, and Jae-Kwang Lee. 2014. The analysis and countermeasures on security breach of bitcoin. In *Computational Science and Its Applications–ICCSA 2014: 14th International Conference, Guimarães, Portugal, June 30–July 3, 2014, Proceedings, Part IV 14*. Springer, 720–732.

[62] Dan Lin, Jiajing Wu, Qishuang Fu, Yunmei Yu, Kaixin Lin, Zibin Zheng, and Shuo Yang. 2023. Towards Understanding Crypto Money Laundering in Web3 Through the Lenses of Ethereum Heists. *arXiv preprint arXiv:2305.14748* (2023).

[63] Xuan Luo, Zehua Wang, Wei Cai, Xiuhua Li, and Victor CM Leung. 2020. Application and evaluation of payment channel in hybrid decentralized ethereum token exchange. *Blockchain: Research and Applications* 1, 1-2 (2020), 100001.

[64] Penghui Lv, Yu Wang, Yazhe Wang, and Qihui Zhou. 2021. Potential risk detection system of hyperledger fabric smart contract based on static analysis. In *2021 IEEE Symposium on Computers and Communications (ISCC)*. IEEE, 1–7.

[65] Alexandra Mai, Katharina Pfeffer, Matthias Gusenbauer, Edgar Weippl, and Katharina Krombholz. 2020. User mental models of cryptocurrency systems-a grounded theory approach. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. 341–358.

[66] Marketleader 2023. What Is a Market Leader? https://www.investopedia.com/terms/m/market-leader.asp.

[67] Mary L McHugh. 2012. Interrater reliability: the kappa statistic. *Biochemia medica* 22, 3 (2012), 276–282.

[68] Victor S Miller. 1985. Use of elliptic curves in cryptography. In *Conference on the theory and application of cryptographic techniques*. Springer, 417–426.

[69] Alex Murray, Dennie Kim, and Jordan Combs. 2023. The promise of a decentralized internet: What is Web3 and how can firms prepare? *Business Horizons* 66, 2 (2023), 191–202.

[70] Chaim Noy. 2008. Sampling knowledge: The hermeneutics of snowball sampling in qualitative research. *International Journal of social research methodology* 11, 4 (2008), 327–344.

[71] Haroon Shakirat Oluwatosin. 2014. Client-server model. *IOSR Journal of Computer Engineering* 16, 1 (2014), 67–71.

[72] Charlie Parker, Sam Scott, and Alistair Geddes. 2019. Snowball sampling. *SAGE research methods foundations* (2019).

[73] Daniel Perez and Benjamin Livshits. 2021. Smart contract vulnerabilities: Vulnerable does not imply exploited. In *30th USENIX Security Symposium (USENIX Security 21)*. 1325–1341.

[74] Purathani Praitheeshan, Lei Pan, Jiangshan Yu, Joseph Liu, and Robin Doss. 2019. Security analysis methods on ethereum smart contract vulnerabilities: a survey. *arXiv preprint arXiv:1908.08605* (2019).

[75] K Vara PrasadRao, P Karthik Sai RadhaKrishna, G Mani Chandra Teja, and Sandeep Kumar Panda. [n. d.]. Blockchain based Smart Contract deployment on Ethereum Platform using Web3. js and Solidity. ([n. d.]).

[76] Kaihua Qin, Liyi Zhou, and Arthur Gervais. 2022. Quantifying blockchain extractable value: How dark is the forest?. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 198–214.

[77] Kaihua Qin, Liyi Zhou, Benjamin Livshits, and Arthur Gervais. 2021. Attacking the defi ecosystem with flash loans for fun and profit. In *International conference on financial cryptography and data security*. Springer, 3–32.

[78] Matthieu QUINIOU. [n. d.]. Immersion in web3 and DeGen community. ([n. d.]).

[79] Hossein Rezaeighaleh and Cliff C Zou. 2019. New secure approach to backup cryptocurrency wallets. In *2019 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 1–6.

[80] Fatima Salahdine and Naima Kaabouch. 2019. Social engineering attacks: A survey. *Future internet* 11, 4 (2019), 89.

[81] Corina Sas and Irni Eliana Khairuddin. 2017. Design for trust: An exploration of the challenges and opportunities of bitcoin users. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 6499–6510.

[82] Sarwar Sayeed, Hector Marco-Gisbert, and Tom Caira. 2020. Smart contract: Attacks and protections. *IEEE Access* 8 (2020), 24416–24427.
[83] Clara Schneidewind, Ilya Grishchenko, Markus Scherer, and Matteo Maffei. 2020. ethor: Practical and provably sound static analysis of ethereum smart contracts. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*. 621–640.
[84] Robert J Shiller. 1999. Human behavior and the efficiency of the financial system. *Handbook of macroeconomics* 1 (1999), 1305–1340.
[85] Ian Sommerville. 2011. *Software Engineering, 9/E*. Pearson Education India.
[86] Liya Su, Xinyue Shen, Xiangyu Du, Xiaojing Liao, XiaoFeng Wang, Luyi Xing, and Baoxu Liu. 2021. Evil under the sun: understanding and discovering attacks on Ethereum decentralized applications. In *30th USENIX Security Symposium (USENIX Security 21)*. 1307–1324.
[87] Saurabh Suratkar, Mahesh Shirole, and Sunil Bhirud. 2020. Cryptocurrency wallet: A review. In *2020 4th international conference on computer, communication and signal processing (ICCCSP)*. IEEE, 1–7.
[88] Miguel A Teruel and Juan Trujillo. 2020. Easing ĐApp Interaction for Non-Blockchain Users from a Conceptual Modelling Approach. *Applied Sciences* 10, 12 (2020), 4280.
[89] Testnet 2023. Testnet. https://en.wikipedia.org/wiki/Testnet.
[90] Marie Vasek, Micah Thornton, and Tyler Moore. 2014. Empirical analysis of denial-of-service attacks in the bitcoin ecosystem. In *Financial Cryptography and Data Security: FC 2014 Workshops, BITCOIN and WAHC 2014, Christ Church, Barbados, March 7, 2014, Revised Selected Papers 18*. Springer, 57–71.
[91] Artemij Voskobojnikov, Borke Obada-Obieh, Yue Huang, and Konstantin Beznosov. 2020. Surviving the cryptojungle: Perception and management of risk among North American cryptocurrency (non) users. In *International Conference on Financial Cryptography and Data Security*. Springer, 595–614.
[92] Artemij Voskobojnikov, Oliver Wiese, Masoud Mehrabi Koushki, Volker Roth, and Konstantin Beznosov. 2021. The u in crypto stands for usable: An empirical study of user experience with mobile cryptocurrency wallets. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–14.
[93] vulnerability 2023. SMART CONTRACT SECURITY. https://ethereum.org/en/developers/docs/smart-contracts/security/#integer-underflows-and-overflows.
[94] Bin Wang, Han Liu, Chao Liu, Zhiqiang Yang, Qian Ren, Huixuan Zheng, and Hong Lei. 2021. Blockeye: Hunting for defi attacks on blockchain. In *2021 IEEE/ACM 43rd International Conference on Software Engineering: Companion Proceedings (ICSE-Companion)*. IEEE, 17–20.
[95] Bin Wang, Xiaohan Yuan, Li Duan, Hongliang Ma, Chunhua Su, and Wei Wang. 2022. DeFiScanner: Spotting DeFi Attacks Exploiting Logic Vulnerabilities on Blockchain. *IEEE Transactions on Computational Social Systems* (2022).
[96] Dabao Wang, Siwei Wu, Ziling Lin, Lei Wu, Xingliang Yuan, Yajin Zhou, Haoyu Wang, and Kui Ren. 2021. Towards a first step to understand flash loan and its applications in defi ecosystem. In *Proceedings of the Ninth International Workshop on Security in Blockchain and Cloud Computing*. 23–28.
[97] Qin Wang, Rujia Li, Qi Wang, Shiping Chen, Mark Ryan, and Thomas Hardjono. 2022. Exploring web3 from the view of blockchain. *arXiv preprint arXiv:2206.08821* (2022).
[98] Ye Wang, Yan Chen, Haotian Wu, Liyi Zhou, Shuiguang Deng, and Roger Wattenhofer. 2022. Cyclic arbitrage in decentralized exchanges. In *Companion Proceedings of the Web Conference 2022*. 12–19.
[99] Ye Wang, Patrick Zuest, Yaxing Yao, Zhicong Lu, and Roger Wattenhofer. 2022. Impact and user perception of sandwich attacks in the defi ecosystem. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–15.
[100] Web3 losses 2023. Web3 losses exceed $1 billion in 2023 as Base projects add to exploits in August. https://www.theblock.co/post/248550/web3-losses-exceed-1-billion-in-2023-base-exploits.
[101] Web3 market 2023. Why Web3.0 blockchain technology is driving a six trillion dollar market. https://www.techrepublic.com/article/web-blockchain-technology-market/.
[102] Web3 market data 2023. Web3.0 blockchain market. https://www.marketresearchfuture.com/reports/web-3-0-blockchain-market-10746.
[103] Web3complex 2023. Web 3.0 Is Too Complicated. https://www.coindesk.com/layer2/2022/01/03/web-30-is-too-complicated/.
[104] Web3game 2023. Web3 Gaming Is Dead. Long Live Web2.5 Gaming. https://medium.com/@chiyoungkim/web3-gaming-is-dead-long-live-web2-5-gaming-6d265e3049af.
[105] Kristin Weber, Andreas E Schütz, Tobias Fertig, and Nicholas H Müller. 2020. Exploiting the human factor: Social engineering attacks on cryptocurrency users. In *Learning and Collaboration Technologies. Human and Technology Ecosystems: 7th International Conference, LCT 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings, Part II 22*. Springer, 650–668.
[106] Ming-Hui Wen, Cing-Yu Huang, Ying-Chen Chen, and I-Ching Lin. 2023. Exploring Factors Influencing Community Consensus Building of Web3 Decentralized Apps. In *International Conference on Human-Computer Interaction*. Springer, 408–420.
[107] whales 2023. What Are Crypto Whales and Why Are They Important? https://www.coindesk.com/learn/what-are-crypto-whales-and-why-are-they-important/.
[108] What is Web3 2023. Introduction to Web3. https://ethereum.org/en/web3/#introduction.
[109] Siwei Wu, Dabao Wang, Jianting He, Yajin Zhou, Lei Wu, Xingliang Yuan, Qinming He, and Kui Ren. 2021. Defiranger: Detecting price manipulation attacks on defi applications. *arXiv preprint arXiv:2104.15068* (2021).
[110] Kazuhiro Yamashita, Yoshihide Nomura, Ence Zhou, Bingfeng Pi, and Sun Jun. 2019. Potential risks of hyperledger fabric smart contracts. In *2019 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*. IEEE, 1–10.
[111] Akif Yüksel. 2021. Mitigating sandwich attacks in Kyber DMM. (2021).
[112] Rui Zhang, Rui Xue, and Ling Liu. 2019. Security and privacy on blockchain. *ACM Computing Surveys (CSUR)* 52, 3 (2019), 1–34.
[113] Chenhang Zhou, Yu Chen, Roger Wattenhofer, and Ye Wang. 2023. Print Your Money: Cash-Like Experiences with Digital Money. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–7.
[114] Liyi Zhou, Kaihua Qin, Christof Ferreira Torres, Duc V Le, and Arthur Gervais. 2021. High-frequency trading on decentralized on-chain exchanges. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 428–445.
[115] Liyi Zhou, Xihan Xiong, Jens Ernstberger, Stefanos Chaliasos, Zhipeng Wang, Ye Wang, Kaihua Qin, Roger Wattenhofer, Dawn Song, and Arthur Gervais. 2023. Sok: Decentralized finance (defi) attacks. In *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2444–2461.
[116] Vivian Ziemke, Benjamin Estermann, Roger Wattenhofer, and Ye Wang. 2023. What Determines the Price of NFTs? *arXiv preprint arXiv:2310.01815* (2023).

A SAMPLE LIST FOR SOURCES OF INFORMATION

We have listed examples of the three types of information sources respectively in Table 3. For the first category, officially linked articles, we provide three examples identified from the "Introduction to Web3" section on "ethereum.org". We have added hyperlinks to these information sources in the table. The second category encompasses on-chain Web3 DApps. Here list of several DApp instances sourced from the official Ethereum website. The third category comprises community-based user discussions, exemplified by user comments obtained from the Discord channel.

B FRAMEWORK DEVELOPMENT AND ITERATION

Initially, we employed deductive coding to delineate five pre-established themes, and then inductive coding to recognize four principal user interaction scenarios. Subsequently, we validated the justifiability of these scenarios via a literature review. The framework's refinement was achieved through an iterative process of discussion and amendment, collaboratively undertaken by two researchers.

Deductive Coding: In software engineering, interaction modeling involves various elements such as the end-user, interaction object, association, message, and information [85]. Building on this, we identified five themes describing user interactions in the Web3 ecosystem: *behavioral interaction*, *informational interaction*, *interaction objects*, *interaction tools*, and *interaction stakeholders*. Given the possibility of overlapping insights from different information sources, we streamlined our findings after completing the coding. Redundant codes were eliminated, and the remaining ones were organized hierarchically based on inter-code relationships. An example coding scheme can be found in Figure 4.

Inductive Coding: After identifying the "interaction object" through deductive coding, we used an inductive approach to analyze their correlations and discern interrelationships. Subsequently, we

Table 3: Sample List for Sources of Information. We have listed examples of the three types of information sources respectively: officially linked articles, on-chain Web3 DApps, and community-based user discussions.

Source of Information	Sample of Selected Information Source
Officially Linked Articles	Introduction to Web3
	What is Web3? The Decentralized Internet of the Future Explained
	Making Sense of Web 3
	Why Decentralization Matters
	The Web3 Landscape
	The Web3 Debate
On-chain Web3 DApps	Lending and borrowing: Aave, Compound, Oasis
	Exchanges: Uniswap, Curve, Loopring
	Liquid staking: Lido, Ankr
	Bridges: Multichain, Rubic
	NFT marketplaces: OpenSea, SuperRare, Rarible
Community-based User Discussions	User 2023/08/11 17:16 Yesterday tried to make a swap in the Arbitrum network from USDC.e to ETH, Swap showed tx 20$+ Normally, this operation takes max 0.2$ on Sushi/DefiLlama/other Dexes
	User 2023/08/23 10:52 MetaMask is primarily a browser-based wallet optimized for Ethereum dApp interactions, while Trust Wallet is a mobile-first, multi-chain wallet with broader cryptocurrency support and integration with Binance. It depends on your requirements.
	User 2023/08/24 14:11 Hi I'm looking for Uniswap contract address on Avalanche. It's not on this page: https://docs.uniswap.org/contracts/v3/reference/deployments Does anyone know where I can find it? Thanks!

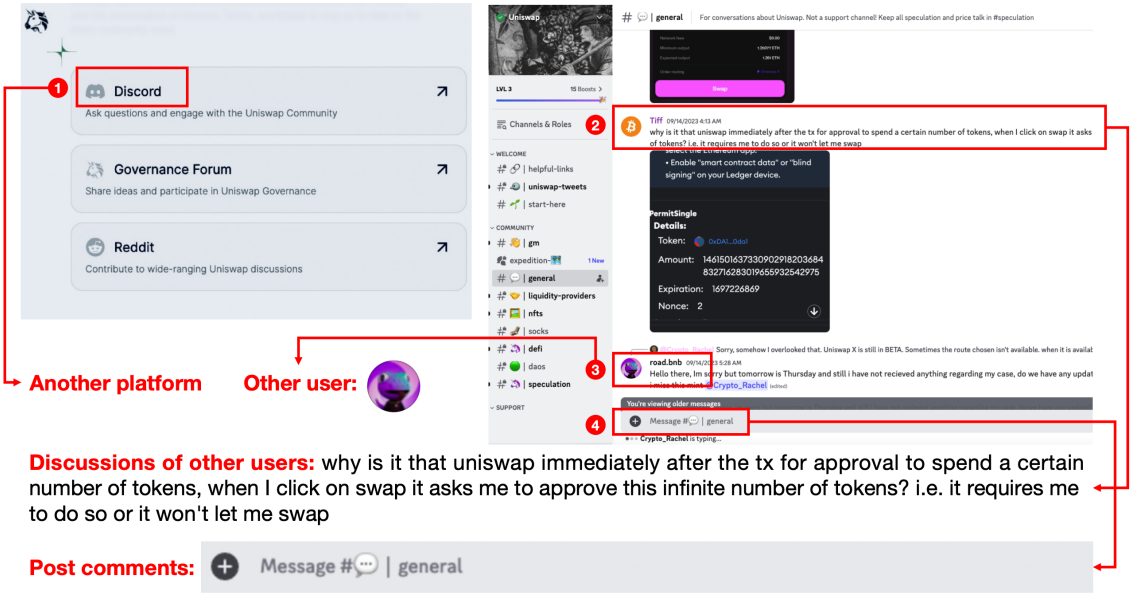

Figure 4: A Case of Coding Scheme. On Uniswap's homepage, 1) "Discord" is encoded as an "interaction object". 2) Click the link to enter the Uniswap channel in Discord, and encode the "discussions of other users" in the channel into information content, which is a type of "interaction object". 3) Encode "other users" as a type of "interaction stakeholder". 4) Encode "post comments" as a type of "behavioral interaction". When no coding theme that meets the five preset categories can be found on the page, the next specific information source is changed.

identified four principal interaction scenarios between users and the Web3 ecosystem: *blockchain system*, *Web3 DApp*, *online community*, and *off-chain cryptocurrency ecosystem*.

In order to confirm the strong consistency between academic discussions of Web3 interactive objects and our observational findings, we conducted a literature review using the keywords search method on Google Scholar. We employed the keyword search, utilizing at least one of the following terms: "Web3", "blockchain system", "decentralized application", "DApp", "community", "off-chain interaction", "CEX", "Decentralized finance", "user behavior", "interaction behavior", "apply scenario", "interaction scenario". This approach led us to pertinent academic research that aligns with the four interaction scenarios we identified, as outlined in Table 4.

Subsequently, two researchers collaboratively conceived an initial idea for a preliminary Web3 user interaction framework based on the coding results. This initial framework underwent an iterative refinement process, involving cycles of discussions and modifications until consensus was reached on the framework's structure and details.

C EXCLUSION METHOD

Before conducting the interviews, we lead potential participants to answer the following questions to determine whether they have interacted with and experienced the Web3 ecosystem.

- Are you familiar with blockchain technology?
- Could you briefly describe your understanding of Web3?
- When did you come into contact with Web3?
- Have you ever used any Web3 applications? Could you list them simply?
- Have you ever purchased or traded cryptocurrencies or NFTs?

We employed the exclusion method, where users who expressed interest but were completely unfamiliar with our research question were excluded. However, potential participants with less experience and gradual exposure to Web3 will be retained because our research is based on users with varying experiences, not users with no experience at all.

D INTERVIEW PROTOCOL

D.1 Personal Information

1. Which country are you from?
2. What is your age range?
3. What is your occupation/area of expertise?

D.2 Basic Behavior and Experience

1. Please briefly talk about your understanding of web3.
2. When did you start contacting the Web3 project?
   - 2.1. How did you learn about this project?
   - 2.2. What was your motivation for participating in the project?
3. What blockchain platforms or Web3 application experience have you used? (the first and most recent one)
   - 3.1. Why use it? How did you learn about it?
   - 3.2. Which one is used most often?
4. Please give examples of the functions you used in these platforms or applications. What are the most frequently used functions?
   - 4.1. Which function is the most frequently used one?
   - 4.2. What needs do these functions meet for you?
   - 4.3. What is the frequency of use?
5. For the Web3 project you mentioned earlier, can you tell me why you chose it from similar products? What factors have you considered?
6. Which blockchain platform are the Web3 projects you use based on?
   - 6.1. Will your chosen Web3 project be available on other blockchains? What other chains can it be used on?
   - 6.2. So why did you choose XXX chain? Why not use other platforms?
   - 6.3. Are you involved in any other Web3 projects on other chains?
7. Please think back to your experience when you first participated in the Web3 project. What information would you know in advance before using it?
   - 7.1. What information was collected from which sources, and what decisions did this information allow you to make?
8. Will you take the initiative to understand how the project works and look for some security suggestions and risk warning information at the beginning of using it?
   - 8.1. Yes: From what channel? What do you pay the most attention to, and will this help you in future use?
   - 8.2. No: Why was this information not provided during the initial engagement?
9. Do you participate in online communities? (For example, the forum officially operated by the project, as well as the discord community, and following social media such as Twitter)
   - 9.1. What do you do in the main community?
   - 9.2. What information will you pay attention to in the community? How will this information help or impact your use of Web3 projects?
10. Have you heard about or paid attention to some security incidents that occurred in blockchain systems or Web3 applications? Or are you aware of some security risks?

D.3 Security Concerns and Mitigation Strategies

1. How do you define blockchain system and Web3 project security? What kind of projects do you think can be considered security?
2. Do you evaluate security before choosing which chain or Web3 project to participate in?
   - 2.1. How important do you think security is?
   - 2.2. What else will you focus on?

For Blockchain Systems

3. How do you evaluate the security of a blockchain platform? Please explain with specific examples.
   - 3.1. What kind of blockchain platform is safe in your opinion? What factors make you feel safe? What factors may cause you to worry about security?

Table 4: Literature Review of the Web3 Interaction Scenario. The second column lists the titles of pertinent academic literature. These works are relevant to each interaction scenario, thereby affirming the active engagement of these scenarios within the current academic discourse.

Interaction Scenarios	Title of Related Literature
Blockchain System	Exploring Web3 from the view of blockchain [97]
	Decentralization and Web3 technologies [52]
	Blockchain based smart contract deployment on Ethereum platform using Web3.js and solidity [75]
Web3 DApp	Cyclic Arbitrage in Decentralized Exchanges [98]
	What Determines the Price of NFTs? [116]
	Easing DApp interaction for non-blockchain users from a conceptual modeling approach [88]
Online Community	Altruistic and profit-oriented: making sense of roles in Web3 community from airdrop perspective [26]
	Immersion in Web3 and DeGen community [78]
	Exploring factors influencing community consensus building of Web3 decentralized Apps [106]
Off-chain Cryptocurrency Ecosystem	Towards understanding crypto money laundering in Web3 through the lenses of Ethereum heists [62]
	Towards understanding governance tokens in liquidity mining: a case study of decentralized exchanges [27]
	Application and evaluation of payment channel in hybrid decentralized Ethereum token exchange [63]

4. How secure do you think the blockchain systems you are currently involved in are? What factors led you to give such an evaluation?
5. Have you personally experienced blockchain platform security issues so far?
  5.1. Yes: What security issues were encountered? What are the consequences? What are the countermeasures?
  5.2. No: Are there any security concerns about blockchain platforms? What exactly? (No worries: Why no worries?)
    5.2.1. Why is there such concern?
    5.2.2. What did you do to ease your worries? Are the measures effective?
    5.2.3. Will it affect your continued use? What are the reasons for continued use despite concerns?

For Web3 DApps

6. Please tell us how you evaluate the security of a Web3 project based on your experience. Please give specific examples.
  6.1. What kind of projects do you think are safe? What factors make you feel safe?
  6.2. What factors may cause your security concerns?
7. Do you think your experience so far has been safe?
  7.1. Yes: Why do you think so? What factors make you feel safe?
  7.2. No: jump to 8.
8. Have you ever faced security issues?
  8.1. Yes: Can you recall what exactly happened?
    8.1.1. What are the consequences?
    8.1.2. Did the consequences have a big impact on you?
    8.1.3. Were you aware of this type of security issue before this? Did it catch your attention at that time?
    8.1.4. Have you taken any measures to address this security issue? is it effective?
    8.1.5. Have you encountered similar problems after this experience?
  8.2. No: jump to 9.
9. Are there any security concerns in your past use experience?
  9.1. What specific security issues are you worried about? (Finance, personal information, account theft, cyber-attacks)
  9.2. What is the level of concern? What are you most worried about?
  9.3. In which aspect of the project do such concerns appear?
  9.4. Why are you worried? Are there any operations, information, or some properties of the blockchain itself (consensus mechanism) that make you feel uneasy?
  9.5. Do you know what causes your concerns?
  9.6. Was this concern present from the beginning or did it arise as you gained a deeper understanding of the project?
  9.7. Is this concern specific to a specific platform or app, or is it common when you participate in Web3 projects?
10. Are there levels of these concerns you mentioned? Which worry worries you the most? Why?
11. Regarding the concerns you mentioned, will this affect your continued use of the Web3 project?
  11.1. Yes: Did you give up using it directly, or did you decide not to continue using it after trying to alleviate your concerns? What are the mitigation measures?
  11.2. No: Why do you still choose to use it despite security concerns? What factors motivate you to continue using? Are there measures to alleviate concerns?
12. In your past experiences, have you taken any measures to mitigate the worries you mentioned earlier? Or what did

you do to prevent yourself from encountering the previous experience again?
- **12.1.** Yes: What measures have been taken? What exactly did you do?
  - **12.1.1.** Which specific concern is it intended to mitigate?
  - **12.1.2.** How did you learn about this solution? It is accumulated through your personal experience and from the Internet retrieve solutions, or ask others for help?
  - **12.1.3.** Is this measure/strategy difficult to implement?
  - **12.1.4.** Are concerns effectively mitigated?
  - **12.1.5.** Do you know of other solutions (technical, non-technical)?
- **12.2.** No: Why not take action?
  - **12.2.1.** Do you think it is not necessary to take measures?
  - **12.2.2.** Will any measures be taken afterward?

13. Did you take mitigation measures for every concern?

For Online Communities

14. Do you think online communities will indirectly bring security risks to Web3 applications?
- **14.1.** Yes: Please tell us what security risks you are aware of.
  - **14.1.1.** Are you worried that you may encounter such a problem?
  - **14.1.2.** Are there any measures to deal with possible security issues?
  - **14.1.3.** Are the measures effective in protecting your security? Or has it effectively alleviated your security concerns?
- **14.2.** No: Do you know that some hackers will conduct phishing activities through online communities, or that some projects' official social media accounts will be stolen?

15. What are the characteristics of posts that you consider to be security risks in online communities?
- **15.1.** What would you do if the project you were using had such a security risk in the online community?
- **15.2.** Does it affect your continued use? What factors made you choose to continue using it?

16. 16.1. Are there any measures to deal with possible security issues?
- **16.2.** Are the measures effective in protecting your security? Or has it effectively alleviated your security concerns?

For Off-chain Cryptocurrency Ecosystem

17. Do you have any interaction with CEXes?

18. Do there exist any security concerns during this process? What exactly? Why did it occur?
- **18.1.** Will it affect continued use?
- **18.2.** Are there any measures to deal with possible security issues?
- **18.3.** Are the measures effective in protecting your security? Or has it effectively alleviated your security concerns?