

Exploring User Perceptions of Security Auditing in the Web3 Ecosystem

Molly Zhuangtong Huang*, Rui Jiang*, Sharma Tanusree†, and Kanye Ye Wang*

*University of Macau

†Pennsylvania State University

{yc37968, dc02764, wangye}@um.edu.mo, tfs5747@psu.edu

Abstract—In the rapidly evolving Web3 ecosystem, transparent auditing has emerged as a critical component for both applications and users. However, there is a significant gap in understanding how users perceive this new form of auditing and its implications for Web3 security. Utilizing a mixed-methods approach that incorporates a case study, user interviews, and social media data analysis, our study leverages a risk perception model to comprehensively explore Web3 users’ perceptions regarding information accessibility, the role of auditing, and its influence on user behavior. Based on these extensive findings, we discuss how this open form of auditing is shaping the security of the Web3 ecosystem, identifying current challenges, and providing design implications.

I. INTRODUCTION

As a decentralized online ecosystem built on blockchain technology, Web3 has revolutionized the digital landscape, with a Total Value Locked (TVL) exceeding 45 billion USD in 2023 [24]. This ecosystem has attracted millions of users, drawn by the promise of transparency, efficiency, and trustless transactions. However, Web3 is not without vulnerabilities; by 2023, security breaches had led to cumulative financial losses totaling 77 billion USD [98].

Given the increasing incidence of security threats, Web3 auditing has emerged as an implementation to safeguard the ecosystem. This process involves an external mechanism for enhancing smart contract security in Web3 applications before deployment, with the subsequent findings shared openly with the user community. To date, more than half of all Web3 applications have undergone audits, covering over 80% of the market’s total TVL [98]. Further augmenting this trend, audit firms have proactively interacted with the public through expert lectures, incident analysis, and knowledge-sharing initiatives [27], [66], [14].

While security auditing is not a novel concept, the practice of openly disclosing audit-related information

*Corresponding author is Kanye Ye Wang (wangye@um.edu.mo).

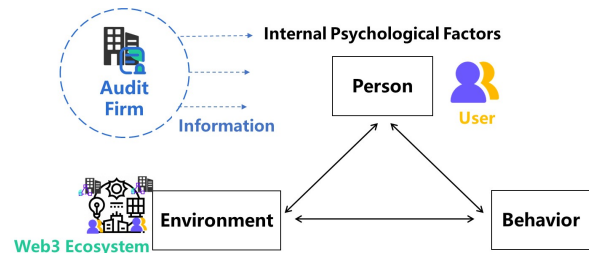


Fig. 1: The risk perception model in the Web3 ecosystem [19] demonstrates how a person evaluates external input, which then shapes their behavior. Web3 auditing serves as a new source of external input.

to users, as prevalent in Web3 auditing, is notably unique. In the Web3 ecosystem, audit firms have become critical stakeholders that disseminate security information to the Web3 ecosystem, which can further alter the security practices of users [49], [9]. This practice aligns with the risk perception model [19] (cf. Figure 1), which indicates that external environmental factors influence an individual’s sense of security.

Despite the role of auditing in shaping users’ security perceptions and behaviors, existing research in the Web3 realm has overlooked this dimension. This study seeks to fill this gap by focusing on the user’s perspective towards Web3 auditing, aiming to illuminate how these perceptions guide user behavior and engagement within the ecosystem. Therefore, we follow the risk perception model to study the following research questions (RQs) to explore the three dimensions within with the involvement of Web3 auditing: The information exchange between stakeholders, users’ perceptions of security, and security practices.

RQ1: How do users perceive security information obtained from Web3 auditing?

RQ2: How do users perceive the role of Web3 auditing in enhancing security within the Web3 ecosystem?

RQ3: How do users perceive the impact of Web3 auditing on their interactions with audited applications?

We conducted mixed-methods studies to explore users’ perceptions of Web3 auditing within the Web3 ecosystem. This research comprised a case study about audit firms and Web3 applications, interviews with 20 Web3 users, and an analysis of Reddit discussions, encompassing 905 posts with 2490 comments.

We initially examined three critical dimensions of security information from auditing: accessibility, sufficiency, and comprehensibility. Our findings show that users rely on a single source for audit information they find accessible but raised concerns about the limited depth and scope of the content. Additionally, the technical complexity often restricted users' comprehension. We subsequently delved into user perceptions on the role of auditing in enhancing Web3 security, from their views on audit firms and the impact of auditing in Web3. Our findings indicate that users evaluate the quality of audit firms' work primarily based on their reputation and skepticism about their impartiality and independence, yet recognize their role in providing education. Additionally, our analysis identified varying user attitudes regarding the efficacy of auditing in bolstering security. At the same time, there was a general agreement on its importance in proving the security efforts of applications. Finally, we analyzed the impact of Web3 auditing on user interactions with audited applications. We found that auditing plays a limited role in various stages of users' security decision-making processes. However, our research emphasizes the significant role of Web3 auditing in fostering security awareness among users within the ecosystem.

This study pioneers in examining Web3 auditing from a user perception perspective, uncovering user interactions with, understandings of, and values placed on Web3 auditing practices. Our findings offer immediate implications for user-centric security in Web3 and lay a foundation for enhanced user engagement with security mechanisms. Additionally, the insights gained from this study extend beyond Web3, providing a template for transparent security auditing that positively impacts user engagement and security across digital ecosystems. Ultimately, this research serves as a cornerstone for future Web3 security initiatives and a model for usable security in various cyberspaces.

II. RELATED WORK

In this section, we explore prior research from two key perspectives: first, studies on the security perceptions of Web3 users, and second, studies related to auditing practices of web-based applications.

A. Security Perception of Web3 Users

The Human-Computer Interaction (HCI) community has recognized blockchain security issues, leading to various user studies aimed at comprehending user behavior, security perceptions, and security-related practices [36], [43]. These studies investigating the security perceptions of Web3 users can be categorized into two main groups based on their focus: those targeting blockchain technology and those concentrating on blockchain applications.

Studies on blockchain technology explore stakeholders' trust in blockchains. Sas et al. examine the

characteristics of Bitcoin like decentralization, aiming to address the risks posed by dishonest traders and proposing mitigation strategies [79]. Ooi et al. identify factors such as technical safeguards, transaction procedures, and security statements that influence users' perceived trust in blockchain systems [70]. Additionally, previous research has highlighted trust-related risks associated with miners, arising from issues like centralization and dishonest administrators in collaborative mining efforts [51].

Research on user perceptions related to applications within blockchain systems primarily focuses on cryptocurrency and related tools. In the context of cryptocurrencies, Abramova et al. found that cryptocurrency users face challenges in securely using cryptocurrencies, such as the reliance of novices on external custodial solutions [1]. Froehlich et al. pioneered the connection between privacy personas and user behavior, suggesting that both knowledge and motivation regarding secure behavior influence users' risk perceptions [34]. Additionally, some scholars explore cryptocurrency tools. Voskoboynikov et al. identify the potential monetary loss resulting from poor interface design from a user experience perspective [89]. Mai et al. reveal that current cryptocurrency tools struggle to mitigate threats stemming from users' misconceptions [63]. Wang et al. [90] investigate user perception of a specific attack model in decentralized finance applications. Si et al. found that Web3 users have significant security concerns regarding the overall ecosystem [82]. This comprehensive investigation provides invaluable insights into how users engage with and perceive the Web3 ecosystem.

Web3 auditing has gained significant importance in the past two years within the Web3 ecosystem. Approximately 50% of applications have undergone multiple audits, collectively accounting for around 80% of TVL [98]. According to the risk perception model [19], perception is the process by which individuals assess their external environment, ultimately shaping their behavioral responses. Therefore, external information provided through Web3 auditing can strongly influence users' perceptions within the ecosystem. However, our current understanding lacks insights into how users perceive Web3 auditing.

B. Auditing for Web-related Applications

Before the emergence of Web3, cyberspace was primarily referred to as Web2, representing the second generation of the World Wide Web. This era was characterized by a centralized network ecosystem [92]. In Web2, auditing involves an objective evaluation process to ensure compliance, accuracy, reliability, and security across various domains. This process includes practices such as algorithm audits, security audits, IT audits, and code reviews [28], [18]. Auditing plays a critical role in enhancing decision-making and operational efficiency [57], with widespread application.

For example, Google conducts annual standardized security audits, publicly disclosing some results online, while keeping detailed information confidential¹. Previous research on Web2 auditing can be grouped into three main areas: optimization of auditing methods [65], auditing of online activities [58], and the perceptions of auditing stakeholders [26].

Prior research has primarily centered on optimizing audit methods, yielding many approaches. Some scholars have introduced an optimized security auditing framework tailored for cloud environments [72], [64]. Other scholars have also investigated audit frameworks designed for agile software development [35]. Chen et al. have contributed by offering alternative quantitative tools to gather audit evidence [16], enhancing the quality of collaborative code reviews [42]. Meanwhile, Jang et al. have proposed a rule-based auditing system, extending the scope of vulnerability detection across various contexts [94]. Previous research has also placed significant emphasis on user-driven algorithms as a means to enhance audit efficiency [25].

Prior research has also dedicated considerable attention to employing auditing for Web2 activities, focusing on evaluating the security of various online systems and platforms. Juneja et al. conducted comprehensive assessments of content regulation policies, particularly concerning misinformation [47], [48]. Other scholars have undertaken audits to examine the fairness of advertising policies on social platforms [58] and election outcomes in evidence-based elections [95]. Additionally, Michael Mitchell et al. have conducted audits addressing system security and privacy for third-party Android phones, autonomous driving software, and virtual reality devices, respectively [67], [60], [88].

Some studies have also delved into the perception of stakeholders in the realm of Web2 auditing. Since Web2 audits are typically not publicly disclosed, previous research has primarily centered on developers reviewing audit results. Prior research has revealed that developers are primarily motivated to choose audits to identify and rectify defects [7]. Furthermore, research has examined how developers assess the quality of code reviews, suggesting that such reviews may offer limited assistance to developers [55], [56]. Kononenko et al. have explored the impact of code reviews on developers and proposed that these reviews can enhance security awareness [75]. Conversely, other studies have highlighted the inhibiting effect of non-professional reviewers on the code review process [22].

In summary, previous research has not explored the influence of audit practice on users, primarily because Web2 security audits are not publicly disclosed. While sharing security audit information with users is common in the Web3 ecosystem, it remains a novel concept in Web2. Therefore, investigating the impact of security audit information released by third-party

¹<https://cloud.google.com/security/compliance/iso-27001>

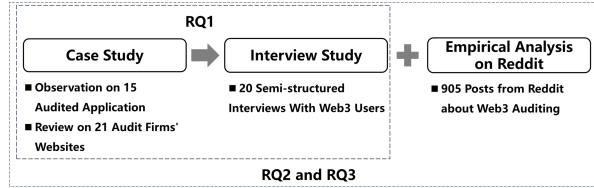


Fig. 2: Research Method and RQ Relationship. The case study offers a framework for understanding Web3 auditing and provides an empirical foundation for analyzing RQ1 and RQ2. The interview study provides qualitative insights for all RQs, while Reddit analysis supplements and cross-validates the interview findings.

entities on users is beneficial for the development of the Web3 ecosystem and may offer valuable insights to improve the security awareness of Web2 users.

To address the research gap concerning users' perspectives on Web3 auditing, we formulated the following RQs based on the risk perception model [19], as illustrated in Figure 1, exploring three key dimensions: First, considering that Web3 auditing acts as an external source of security information, we focus on *RQ1: How do users perceive security information from Web3 auditing?* Next, recognizing that Web3 auditing introduces new stakeholders into the Web3 ecosystem, we explore *RQ2: How do users perceive the role of Web3 auditing in enhancing security within the Web3 ecosystem?* Finally, acknowledging that user behavior is shaped by their perceptions, which may be influenced by Web3 auditing, we investigate *RQ3: How do users perceive the impact of auditing on their interactions with audited applications?*

III. STUDY METHOD

This study was approved by the Institutional Review Board (IRB) at [hidden for review]. We first conducted a case study to structure the Web3 ecosystem's interaction framework by examining application and audit firm disclosures. Following this, we conducted 20 semi-structured interviews with Web3 users and analyzed 905 Reddit posts to supplement and cross-validate the interview findings, as shown in Figure 2

A. Case Study on Web3 Auditing

To gain insights into the interactions between Web3 auditing and users within the Web3 ecosystem, our study explores security information from auditing through two perspectives: the audited applications and the audit firms. Details includes the sample information sources, selected audit firms, and the systematic review protocol are available in Appendix E.

1) *Information from Web3 Audited Applications:* Our observational study focuses on all Web3 applications with over 1 billion USD TVL as of August 1, 2023, due to their leading position [24]. This includes 15 Web3 applications, all of which have undergone

audits. We identified pages on the applications’ websites disclosing audit information. These pages convey essential details Web3 applications aim to communicate to users, including audit results and implementation specifics such as audit frequency, total audits conducted, and related information. We then employed a hybrid coding method, combining deductive and inductive thematic analysis, to analyze the data from these pages [31].

2) *Information from Web3 Audit Firms:* By examining all firms that provided audit services to Web3 applications with a TVL exceeding 1 billion USD, we identified 20 audit firms. We selected the homepages of these 20 audit firms as our observation targets to examine how they interact within the Web3 ecosystem. Our focus was on webpages from the official homepages of these Web3 audit firms, which provide information about their auditing practices, such as whitepapers, blogs, and related social media channels cited by the audited firms’ official websites, such as Discord and X. For these sources, we employed a hybrid coding method and conducted a systematic review of the information disclosure practices of 20 audit firms [31], drawing from previous work [41]. The systematic review protocol we designed focused on three main aspects: a) firm introduction, b) presentation of services, and c) additional security information.

Two researchers independently reviewed the website content of each firm and filled out the review protocol accordingly. The final results were derived through a consensus discussion. Notably, our systematic review of audit firm websites, including those in various languages, revealed that only three offered multilingual options. Of these, two provided identical English translations across all languages, while one displayed a distinct self-introduction in the Chinese version, highlighting its contributions to China’s blockchain industry. This observation led to the inclusion of 21 audit firm websites in our comprehensive review. This method allowed us to summarize quality of security information from auditing users received, provided objective validation for interviews findings, and specifically supported the analysis of perceptions of security information from auditing (RQ1) and the role of auditing in enhancing security (RQ2).

3) *Framework of Web3 auditing interactions:* Drawing on our observations from both Web3 applications and audit firms, as well as relevant literature [30], we defined **Web3 auditing**, conducted by specialized security firms, as an external mechanism for enhancing smart contract security in Web3 applications, typically culminating in public audit disclosures.

Inspired by the risk perception model [19], we developed a framework for Web3 auditing that encompasses stakeholders, information exchange, and interactive behaviors (Figure 3). Web3 auditing impacts the ecosystem by providing audit services to Web3 applications. Moreover, audit-related information and

other security information disseminated by audit firms reach users, potentially affecting their awareness and behaviors, such as decision-making. These user behaviors, in turn, exert influence on the Web3 ecosystem.

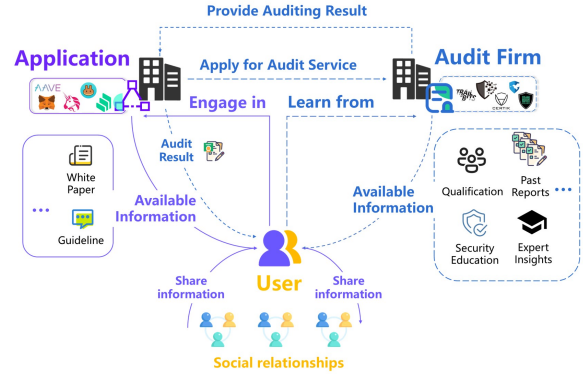


Fig. 3: The framework for Web3 auditing encompasses stakeholders, information exchange, and interactive behaviors. Web3 audit firms engage with users in the Web3 ecosystem by providing auditing services to applications and disseminating security information. These information revelation changes can potentially influence users’ security awareness and decision-making processes [49].

B. Interview Study

We then recruited Web3 users² for semi-structured interviews to capture users’ subjective perceptions. AppendixC provides a summary of our interview study’s demographics, the interview protocol, and details of the recruitment process.

1) *Participant Recruitment:* We published our recruitment materials on Twitter, Discord, and Telegram, and also leveraged the research team’s personal contacts to recruit participants. To be eligible, participants needed to 1) be familiar with Web3 auditing, such as engaging with audit results of Web3 applications, 2) have experience using Web3 applications like Binance, Metamask, or Uniswap, and 3) be over 18 years old. Between July 2022 and August 2023, we interviewed 20 Web3 users via Zoom and Tencent Meetings. Each interview lasted 45-60 minutes, and participants received a \$20 honorarium. Participants were informed about our study procedures and data protection policy. Three participants identified as female, and the remaining seventeen as male. Fourteen participants had over three years of experience with Web3 applications, while six had less than three. The average experience was 3.75 years.

2) *Interview Protocol:* Our interview protocol is divided into three sections, each aligned with a central research question: perceptions of security information from auditing (RQ1), perceptions of the auditing role

²An individual who participates in the Web3 ecosystem through decentralized applications [82].

in enhancing security (RQ2), and the impact of auditing on user interactions with audited applications (RQ3). We use the ladder questioning technique [76] to systematically progress through levels of inquiry, fostering a deep understanding of Web3 users' perceptions through a multi-layered conversational approach. We begin with questions about actions to explore the interviewees' experiences within our focal themes. For example, "Could you describe some Web3 auditing tasks you recall?" to elicit specific actions related to Web3 auditing. Next, we shift to questions about knowledge, such as "How do you obtain audit-related information?" to understand the sources and structures of knowledge that guide and influence actions. This encourages interviewees to explain their reasoning with questions like "How do you know that?" This method extracts holistic insights and encourages reflection on how they obtain and understand information. Lastly, we pose questions about personal perceptions. Questions like "How do you perceive this information? Why?" and "What is your view on the role of auditing?" aim to uncover the deeper values and beliefs underpinning their perceptions.

3) *Interview Data Analysis*: All interviews were audio-recorded with the informed consent of the participants and subsequently transcribed for analysis. We conducted the thematic analysis to systematically interpret the data [11]. Initially, two researchers independently analyzed a representative 20% of the transcripts, identifying emerging themes related to user perceptions of Web3 auditing, understanding of its role, and its impact on user security behaviors.

After developing an initial codebook, both researchers independently coded the remaining 80% of the transcripts, meeting regularly after each 20% increment to ensure consistency. They discussed discrepancies and refined their interpretations, adding a code to the shared codebook only after reaching a mutual agreement. This iterative process enhanced the rigor and validity of our findings. To validate the comprehensiveness of our data, a saturation analysis was conducted. Emerging themes were cataloged in the order of appearance from participants P1 through P20. The absence of novel themes in the later interviews confirmed that we had achieved data saturation.

C. Empirical Analysis on Reddit

We also incorporate discussions from the Web3 community about auditing into our research. Reddit serves as our primary data source for examining community discussions on Web3 auditing, given its role as a major hub for Web3-related communities [53]. Reddit's diverse user base, spanning various geographic locations and cultural backgrounds, allows us to gather broader insights [83]. Appendix ?? provides additional details on this study, including information about the selected Reddit communities and the GPT-4 analysis [45].

1) *Data Collection and Preprocessing*: In the ranking of the top 1000 subreddits provided by Reddit, we identified subreddits related to Web3 under the "crypto" label, which focused on blockchain-based applications, leading to the selection of 10 subreddits. For our dataset, we extracted posts from these subreddits using keywords related to auditing. This extraction process was facilitated by the Python Pushshift.io API Wrapper (PSAW) [8]. More details on the selection criteria are presented in Appendix D-A.

Data preprocessing was conducted in two stages to ensure privacy and data integrity. First, we removed private information from the data we collected with the Microsoft Presidio toolkit, achieving up to 99% accuracy in anonymization [33]. Subsequently, we refined the dataset by employing GPT-4 [71] to exclude posts unrelated to Web3 auditing. We defined Web3 auditing for GPT-4 and provided it with 100 manually verified relevant posts. The collected posts were then assessed by GPT-4, which evaluated each post's title and content for relevance. The two researchers randomly sampled 100 posts from GPT-4's output to evaluate accuracy, ensuring it exceeded 90%. This thorough process yielded a final dataset of 905 posts and 2490 comments, spanning from 2013 to 2023, contributed by 3264 unique users.

2) *Content Analysis and Categorization*: We first conducted a content analysis to achieve thematic categorization. To categorize the posts, we established classification standards using an iterative inductive thematic analysis approach [69]. We randomly selected 100 posts, divided into groups of 10. Two researchers conducted open coding on the first group to identify initial themes, which were then applied to subsequent groups. As new themes emerged, they were incorporated into the classification criteria. This process continued until all posts were classified. Disagreements were resolved by consensus, and inter-rater reliability, measured using Cohen's Kappa [10], exceeded 0.8, indicating substantial agreement. This sample also served as the test set for evaluating GPT-4's accuracy.

After establishing the classification standard, we adjusted GPT-4 to perform the classification task. We designed prompts and used the already categorized 100 posts as a test set to fine-tune our prompts until GPT-4 could accurately classify 90% of the posts. Next, we utilized the GPT-4 API to classify all posts according to the established standards. Finally, a random sample of 100 posts was reviewed, with an accuracy rate exceeding 90%. Our analysis resulted in categorizing posts with examples provided in Table VI in Appendix D-B. Additionally, we randomly sampled 10% of the comments for qualitative analysis to better understand community reactions to posts across different categories, following established practices in HCI research. [39]. To maintain privacy and uphold ethical standards, all Reddit user quotations in the main text were paraphrased to prevent identification through

search functions.

Category 1 focused on direct discussions about Web3 auditing itself, offering insights into how users discussed, comprehended, and evaluated Web3 auditing. Discussions were further divided into subcategories focusing on the mechanism of auditing (What), the auditors and audit firms (Who), and the impact of auditing (How).

Category 2 focused on discussions related to the auditing activities of Web3 applications, primarily addressing specific applications' auditing processes. Subcategories within this category were defined based on the audit status: upcoming audits, ongoing audits, halted audits, successful audits, failed audits, and post-audit attacks.

Category 3 focused on discussions about the dissemination of security information by audit firms, including posts about activities beyond their core auditing services. It was classified into two subcategories: promoting security practices and disseminating security knowledge.

3) *Quantitative Analysis of User Attitude*: We conducted further quantitative analysis on the categorized discussions to understand Web3 users' attitudes toward auditing-related content. Specifically, we performed **sentiment analysis** to gauge the community's attitudes [91], using GPT-4 as the sentiment analysis tool. Based on the Likert 5-point scale methodology [3], GPT-4 assigned a sentiment score to each post, ranging from 1 (very negative) to 5 (very positive), with 3 representing neutral sentiment. A random sample of 100 posts was reviewed, with an accuracy rate exceeding 90%, confirming GPT-4's sentiment analysis accuracy. Details of the accuracy validation are provided in Appendix D-C. The sentiment analysis results primarily assess users' attitudes toward the role of Web3 auditing, aiding in the analysis of user perceptions (Section V-B). It also helps evaluate users' attitudes on audit dynamics, contributing to an understanding of auditing's impact on interactions with audited applications (Section VI-A2).

D. Limitation

Our study has inherent limitations that should be considered when interpreting the findings. First, our interview sample size is limited, making it difficult to generalize to the broader Web3 community. To address this, we supplemented our data with Reddit discussions from over 3000 unique users. While informative, this data may not fully represent the wider community due to unknown Reddit user demographics. Nonetheless, it provides pioneering insights and lays the groundwork for future studies. Another limitation is the experience level of our participants, as most had over a year of involvement with Web3. While this offers valuable insights from seasoned users, it underrepresents the perceptions of newcomers. The focus on experienced users was driven by the specialized nature of Web3

auditing, a topic unfamiliar to many novices during our initial research. Gender imbalance also limits the generalizability of our findings, with the majority of interviewees being male, reflecting the broader gender imbalance in the Web3 ecosystem [5]. Additionally, our data has cultural and geographic biases, as most participants were based in Asia. This raises the possibility of regional cultural influences on our findings. To address this, we included Reddit data, which draws from a globally dispersed user base, primarily using English, offering a more balanced cross-cultural perspective. Lastly, we acknowledge the limitation of not considering recall in our initial validation of GPT-4's accuracy. However, upon recalculation, we found the recall rate consistently above 80%, indicating good overall accuracy in our results. Despite these limitations, our work offers a foundational understanding of user perceptions and security concerns related to Web3 auditing, serving as a stepping stone for more comprehensive future studies.

IV. PERCEPTIONS OF SECURITY INFORMATION OBTAINED FROM WEB3 AUDITING

This section explores users' perceptions of the security information they receive about Web3 auditing, structured around three dimensions [80]: information accessibility, sufficiency, and comprehensibility.

A. Singularity in Locating Security Information from Auditing

Our study reveals a notable trend: users primarily rely on an application's official website as their main source for audit security information. All interviewees indicated that the application's homepage often serves as the initial point where they expect clear and prominent mentions of audit activities. For example, interviewee P4 consistently checks the homepage to see if any security information from auditing is mentioned. *"I usually start by checking their website. The documentation often indicates whether the application has undergone an audit. From there, I review the audit report to verify the audited results."* (P4).

Interestingly, this focus on official websites seems to induce tunnel vision among our interviewees. Despite the availability of multiple channels for disseminating audit information—including social media, developer forums, and blockchain-specific browsers—our participants seldom venture beyond official websites to gather such details. *"In most cases, you can find review information on their website. . . If they have undergone an auditing, they might emphasize it as it becomes one of their selling points"* (P6).

B. Gaps in Security Information Disclosure

Our findings highlight user concerns about the perceived insufficiency of available security information from auditing. This is evident in both the lack of depth in direct security information and the insufficient

comprehensiveness of indirect information, leading to a limited understanding of auditing mechanisms among users.

Four interviewees noted the lack of significant depth in direct security information from auditing, which primarily includes explicit findings, recommendations, and vulnerabilities outlined in audit reports. The reports were often described as “hurried”, “formulaic”, and “repetitive”, failing to provide specific and meaningful insights. *“I feel many of them are overly simplified. Many audits adopt a mass-production method to endorse applications and gather funds merely. The resulting report is concise, just a few pages, and the content lacks depth”*(P1). The perceived superficiality of audit reports fosters user skepticism about their usability, diminishing their impact on user behavior, which will be further elaborated in Section VI.

Three interviewees also noted the lack of comprehensiveness in indirect audit information, including supplementary materials like the historical accuracy of their audits. *“I think a lot of audit-related information is incomplete and a lot of things are not disclosed.”*(P17). Our review of audit firm websites provides empirical evidence for this finding: 38% of firms lack detailed descriptions of their audit processes, and 80% inadequately disclose auditors’ professional expertise, with 62% omitting auditor information entirely.

The lack of comprehensiveness in security information from auditing prevents users from accurately understanding the audit process, often leading to misconceptions about the scope of audit services, as noted in our interviews. For instance, three interviewees with computer development backgrounds equate Web3 audits with “code reviews”, viewing them as solely focused on identifying smart contract vulnerabilities. *“It’s like an audit firm examining the code for harmful bugs and issuing a certification”*(P3). In contrast, P19, with a background in financial accounting, inappropriately extends the scope of Web3 audits to include aspects such as financial background and business activity checks. *“For [Application]’s auditing... all transactions should undergo auditing... perhaps similar to financial auditing in Web2”*(P19).

C. Challenges in Understanding Security Information

Our study reveals that Web3 users, regardless of their experiences and technical background, frequently struggle to understand technical Web3 audit information, such as audit reports, and interpret the presentation of audit results, such as numerical evaluation on the application security level.

Four Interviewees with less experience reported feeling overwhelmed by the content of audit reports. The computer science terminologies and codes prevalent in audit reports pose a significant barrier to understanding for users with limited technical expertise. For

instance, P20 considered that the technical-oriented information hindered her understanding of the report content and diminished her ability to assess the report’s reliability. *“Because it’s difficult for me to understand, I can’t just go and read the audit report”*(P20). Consequently, users with limited technical expertise may use third-party interpretations to navigate these complexities. *“I usually look at the interpretations provided by some tech experts in the chat groups and cross-validate the information”*(P20).

Even for technically proficient users, deciphering audit reports remains a challenging and time-consuming endeavor. Eight interviewees reported that audit reports frequently lack standardized formatting and presentation, introducing additional cognitive burdens. For example, P14, a computer science doctoral student, noted the laborious process of sifting through highlighted vulnerabilities, often further complicated by disorganized report structures that require meticulous, line-by-line code analysis. *“However, in some audit reports, the entire code was copied without specifying errors in the initial lines, resulting in a rather untidy presentation”*(P14). This scenario leads to added complexity and a high time cost for users in personally verifying the correctness of Web3 audit results. Consequently, this adds another layer of skepticism concerning the authenticity and trustworthiness of audit information. *“I don’t have the capability or time to check their audits formally”*(P10).

Furthermore, while audit firms make efforts to render information more comprehensible, for instance, by using numerical values to demonstrate the security levels of Web3 applications, these endeavors are not always perceived as effective by users. Four of our interviewees and Reddit discussions have mentioned the gap between the security scores and the real-world implications. For instance, in a Reddit post titled *“The security score drops from 90 to 38 following a rug pull incident”*(Post90), the user’s confusion about the scoring system was palpable. *“Lowering an application’s security score from 90 to 38 after it gets rugged is incomprehensible ... it should be zero.”*(Post90:Comment2), highlighting the challenges users face in interpreting these numerical evaluations.

V. PERCEPTIONS OF THE ROLE OF WEB3 AUDITING IN SECURITY ENHANCEMENT

In this section, we explore users’ perspectives on the role of auditing in enhancing Web3 security. Our investigation focuses on two key aspects: users’ perceptions of the firms conducting these audits and their perceptions on the impact of Web3 auditing on the security of the ecosystem.

A. Perception of Audit Firms

This subsection examines users’ perceptions of audit firms in the Web3 ecosystem. Our first finding is that users use firms’ reputations to evaluate the quality of

work provided by audit firms. Secondly, we notice that the impartiality and independence of these firms are subjects of skepticism. Lastly, we note that the educational role of audit firms is positively recognized.

1) *Correlation Between Reputation and Quality:* Our findings indicate that users commonly associate the quality of an audit with the reputation of the audit firm. However, there exists a significant ambiguity in the methods users employ to evaluate the reputation of these audit firms.

Eleven interviewees perceive that a firm with a strong reputation is more likely to invest substantial resources, including labor, to conduct thorough and detailed audits. Additionally, users believe that inaccuracies in auditing could severely harm the audit firm's reputation, resulting in higher opportunity costs. *"I think people will eventually recognize that an audit from a more reputable firm is worthwhile over time"*(P4). However, our study reveals significant ambiguity in how users assess the reputation of audit firms. While ten interviewees easily associated high-quality audits with "well-known" firms, sixteen interviewees struggled to name more than one audit firm.

Additionally, there is a divergence of opinions concerning the role of reputation in evaluating the capabilities of audit firms. While twelve interviewees believe that firms capable of providing audit services to well-known applications naturally possess a good reputation, three interviewees hold a contrary view. They argue that established applications might already have skilled internal security teams, leading them to question whether external audit firms can offer value commensurate with their high costs. *"Because they (well-established applications) have already been security for a long time, whether or not they have an audit report will not affect their authority and security... The audit report firm may not have [Application]'s team is professional"*(P16). The ambiguity in how users assess audit firms' reputations and perceived quality highlights a significant gap in the ecosystem.

2) *Lack of Impartiality and Independence in Audit Firms:*

Our findings indicate that users frequently question the impartiality and independence of audit firms, due to two primary factors: the inconsistency in audit quality from the industry's nascent stage and the commercial nature of these firms as paid service providers.

Variability in audit quality has led to user skepticism about the impartiality of audit firms. This industry disarray is evident in both Reddit discussions and our interviews. Interviewees reported encounters with substandard audits, contributing to selective attention bias [62]. These experiences lead users to perceive the industry as flawed or corrupt. *"My friend once got a completely wrong audit report. The error code mentioned in it was not the code of my friend's firm at all... It seemed they didn't read it at all and just issued a report casually... I think this phenomenon*

is widespread"(P16). Similarly, in the discussions on Reddit about audit firms, 76% of posts expressed criticism towards irresponsible auditing practices. *"The brief three-page report, scarcely filled with a hundred words about an 'Accumulated Error from Integer Division' ... it lacks any solid proof ... This is both disappointing and disturbing"*(Post65).

Doubts about the independence of audit firms, given their role as paid service providers, were evident among our interviewees. A quarter of the interviewees expressed skepticism, citing the commercial nature of these firms as a barrier to disclosing negative results about applications. *"They've had prior business dealings, so it's unlikely they'll openly criticize or 'bring down' their clients"*(P17). This sentiment of mistrust is also echoed in Reddit discussions, where users question the objectivity of these firms. For instance, on Reddit, when users questioned why an application received a high-security score, others insinuated that it was due to the audit firm accepting bribes, *"Slip a bribe to the audit team."*(Post266: Comment13).

It is noteworthy that one of our interviewees, P15, expressed a firm belief in the independence of audit firms. As a developer at a Web3 audit firm, P15 has the advantage of directly witnessing the interactions between audit firms and applications, which provides him with insights into their processes. Unfortunately, such insights are typically beyond the reach of regular users. *"Then we can observe many of their daily interactions... we can see how they progressively address issues... so I am acquainted with their process... but this information is challenging for ordinary users to access"*(P15). However, his perspective suggests that enhancing the scope of information disclosure could be a potential solution to the mistrust regarding the independence of audit firms.

3) *Catalysts for Security Education:* Despite the prevalent skepticism regarding the integrity and expertise of Web3 audit firms, users have noted the crucial educational role these entities fulfill.

Audit firms in the Web3 domain have expanded their roles beyond their fundamental duties of auditing applications, emerging as pivotal sources of security knowledge. As expounded in Section III-A3, their responsibilities encompass more than just security auditing. These firms proactively engage in public education on security matters, utilizing diverse channels, including their official websites and social media platforms. Our review of information disclosure on audit firm homepages also provides evidence supporting this practice, as 66.67% of these firms provide educational documents on their websites, such as checklists of smart contract vulnerabilities.

This education effort appears to have enhanced user awareness regarding security risks in the Web3 ecosystem, as evidenced by seven interviewees acknowledging that they have acquired substantial security insights from the information shared by these audit firms.

“They explain why certain approaches don’t work and then teach you how to conduct audits. I’ve also gained valuable insights into code analysis from their content”(P17). A parallel trend is evident on Reddit, where posts related to security education(Subcategory 3.2) received positive feedback from users. For example, one post titled *“[Application] contract exploit: Revoke permissions in wallet”*(Post14) received appreciative responses, with users expressing gratitude. *“Thanks for providing information, I’ve done a revoke”*(Post14:Comment 26).

B. Perception of Impact of Auditing on Web3 Security

Our interviews revealed diverse user opinions on the security impact of Web3 auditing, a trend also observed in online community discussions. Discussions on the impact of auditing (Subcategory 1.3) had a slightly negative average sentiment score of 2.89. Based on our further qualitative analysis, we categorize user perception into three types: questioning attitudes towards the effectiveness of auditing in enhancing security, affirmative attitudes towards the effectiveness of auditing in enhancing security, and affirmative attitudes towards the role of auditing as proof of an application’s security efforts.

1) *Questioning the Effectiveness*: Our study uncovers a skeptical perspective among users that the preventive effectiveness of auditing in averting security breaches is limited. This skepticism primarily stems from two aspects: users’ understanding of the nature of security work, as revealed in our interviews, and the influence of instances where audited applications have still succumbed to attacks, as identified in our analysis of Reddit discussions.

Five interviewees in our study articulated the perceived limitations of audits, viewing them from the perspective of security work itself. They opined that audits primarily serve a post-attack remedial role. In other words, audits are often seen as mechanisms for identifying and resolving risks only after a security breach has occurred. *“Even if everyone conducts audits and identifies all existing vulnerabilities, new ones may still be discovered...No Web3 application code is absolutely error-free and secure”*(P5).

The skepticism regarding audit effectiveness on Reddit predominantly centers on outcome-based evaluations, particularly focusing on incidents that occur after audits. This perspective is evident in posts directly discussing the impact of audits (Subcategory 1.3), where we found that half of the posts highlighted real-world instances in which applications, despite undergoing audits, were compromised in cyberattacks. An example of such a discussion is illustrated in the post: *“Do Web3 audits hold any value? On a single day, two Web3 applications verified by [Audit Firm] suffered breaches, with losses summing up to 14 million USD”*(Post189).

2) *Auditing as a Catalyst for Enhanced Security*: A notable proportion views auditing positively, primarily as a mechanism to enhance the security of Web3 applications. This positive perception stems from three main considerations:

Firstly, five interviewees argue that the external scrutiny involved in the audit process complements and augments the security measures implemented by the application developers. They believe specialized audit teams possess the technical insight and expertise to identify vulnerabilities that may elude even seasoned developers. *“External auditing is imperceptible. Each individual’s technical proficiency covers different layers; thus, the involvement of others is crucial in identifying more issues”*(P05). This support for external auditing is also reflected in Reddit discussions, which can be seen as an endorsement of the impact of auditing. For example, a post reporting a senator’s support for regular audits received 510 upvotes. *“A crypto advocate stressed that [application] must always be fully backed by liquid assets, with regular audits”* (Post57). Most of the sample comments under the post similarly expressed support for external audits. *“She is right. Mandating that [application] be backed and audited would be a commendable regulatory measure”* (Post57:Comment2). Secondly, users believe that audited applications help mitigate or prevent losses from attacks. Three interviewees felt that additional auditing could lower the probability of hacker attacks, reinforcing their perception that audited applications are more secure than unaudited ones. *“I think that auditing can reduce the likelihood of such attacks to some extent”*(P3). Thirdly, and notably, even those users who express skepticism about the effectiveness of current audit practices continue to recognize the intrinsic value of auditing. They acknowledge its role in facilitating ongoing risk assessment, patching vulnerabilities, and validating the security credentials of applications. *“Right now, it’s a bit of a mess, but it’s something you have to do...Auditing should ideally help users avoid attacks and minimize potential damage”* (P16).

3) *Auditing as a Proof to Security Actions*: There is almost universal agreement that undergoing an audit signifies an application’s responsibility and commitment to its user base, particularly in terms of financial costs. However, users’ vague understanding of these financial costs may render this affirmative attitude unsubstantiated.

The financial cost of conducting an audit is generally considered significant, making it a substantial investment for any application party. Hence, users perceive the willingness to bear this expense as a sign of the application’s commitment to security. Even those skeptical about the effectiveness of audits recognize that undergoing one demonstrates a commitment to basic security measures. They emphasize that while an audit does not guarantee foolproof security, it indicates a sincere commitment. *“Contract security itself cannot*

achieve 100% protection...the greatest value of an audit is to give ordinary users confidence, showing that the application is serious about its security and at least willing to invest in an audit.”(P14).

However, our research indicates a notable lack of awareness among users about the actual financial costs of auditing. We found that eighteen interviewees could not accurately estimate these costs. Of the two interviewees who knew about the prices, both learned from friends who had received for audit services, and the price ranges they mentioned varied significantly, from several thousand to tens of thousands of dollars. This lack of awareness is likely attributable to the limited transparency in pricing information that audit firms provide. Our analysis of these firms’ websites revealed that a significant 95% do not furnish specific pricing details. Among these, 71% completely lacked any pricing information, while the remaining 29% provided only vague statements about potential costs.

In summary, regardless of their personal opinions on the effectiveness of audits, users predominantly view the act of undergoing an audit as indicative of an application’s attempt to act responsibly and its commitment to security.

VI. PERCEIVED IMPACT OF WEB3 AUDITING ON USERS INTERACTIONS WITH AUDITED APPLICATION

This section aims to explore how users perceive the impact of auditing on their interactions with audited application in the Web3 ecosystem, focusing mainly on two aspects: impact on decision-making processes and security awareness when using Web3 applications.

A. Users’ Decision-Making Process

We explore how users’ perceptions influence their decision-making in two phases: First, the limited impact of Web3 auditing on users’ time and effort before making decisions, as found in our interviews. Second, the asymmetrical influence of audit results on users’ willingness to engage with applications during the decision-making moment, as observed in online community discussions.

1) *Pre-decision: Limited Impact:* Our interviewees reported two key dimensions of users’ behavioral tendencies when interacting with audited applications before making decisions: a brief time commitment and a cursory focus on the completion status of audits. When it comes to **time commitment**, it is noteworthy that four interviewees reported not spending any time looking for audit results. Among the remaining sixteen who do invest time in this endeavor, fifteen indicated that they allocate only a minimal amount of time to audit-related activities. In terms of specific durations, users typically spend just a few minutes, rarely exceeding ten, on understanding audit reports or findings. *“I just browsed it briefly and didn’t look*

at it seriously”(P08). Regarding **their focus**, users are primarily concerned with the mere existence of an audit rather than the details within the report. Any scrutiny applied tends to be cursory. Complexities such as the tools and methodologies used by auditors, as well as the credibility of the audit firm, are generally overlooked or ignored by eighteen of our interviewees. *“I don’t think it is necessary to read the audit report...I at least know that this application has been audited”*(P15).

2) *In-the-Moment: Asymmetrical Influence:* Our findings, based on community discussions focused on the audit dynamics of applications (Category 2), show that audit results can influence decision-making behavior, though the impact varies depending on the outcome. Positive audit results encourage user engagement, while the effect of negative outcomes on reducing user involvement appears limited.

Positive audit outcomes tend to boost users’ confidence in the application. Posts in Subcategory 2.4 primarily focused on successful audit results, where the application passed and was deemed secure. These posts have an average sentiment score of 4.01, indicating a generally positive user attitude toward successful audits. The comments on these posts also reflect users’ approval of the application. *“There’s a reason [Application] is regarded pretty positively around here.”*(Post4:Comment1).

On the other hand, negative audit outcomes tend to result in unfavorable expectations from users towards applications. Posts in Subcategory 2.5 primarily focused on failed audit results, where the audit identified security issues such as high-risk vulnerabilities. These posts have an average sentiment score of 1.61, reflecting a generally negative user attitude toward such outcomes. The comments on these posts also consistently mirror this sentiment. *“[Application] is deceptive and lacks complete backing.”*(Post81: Comment4).

Interestingly, some users expressed indifference to such unfavorable news about negative audit results. This indifference may be attributed to their inherent risk-seeking behavior, operating under the belief that exceptionally high returns are accompanied by high risks, which in turn influences their decision-making. *“Personally, I’m not too worried; in the worst-case scenario, I lose the \$100 I invested ... In the best case, the value could soar”*(Post5:Comment9).

B. Security Awareness on Web3 Operations

Auditing in the Web3 environment goes beyond proving the security of Web3 applications; audit firms also play an active educational role, as noted in Section V-A3. Our findings show that the information provided by audit firms significantly enhances user security awareness and shapes secure behaviors.

Seven interviewees identified audit reports as educational assets. These reports offer insights into mod-

ern security practices, technologies, and auditing processes. Users use these documents as a starting point for self-education in security, diving into the details of the smart contracts to understand the alterations made and their security implications. *“It’s a valuable for me...I often examine the smart contract to identify modified lines and try to understand why those changes were made.”* (P8).

In addition to formal reports, many audit firms disseminate security-related information across various platforms, further contributing to heightened user awareness. Users mentioned engaging with audit firms’ social media channels to stay updated with the latest security news. These platforms offer updates, analyses of security incidents, explanations of risks in layman’s terms, and guidelines for conducting basic audits and code analyses. *“The audit firm explained what went wrong and then taught how to fix it. I’ve gained valuable insights into code analysis from this”*(P17). Similarly, security knowledge shared by audit firms in the community also be appreciated by users. *“That’s actually great advice! Thank you!”*(Post10:Comment6).

VII. DISCUSSION

To clarify the evolving role of auditing in the Web3 environment, this discussion is organized into three parts: the rationale behind the rise of auditing in Web3, the challenges this auditing paradigm faces, and the design implications for its future development.

A. The Unique Characteristics of Web3 Auditing

We dissect the complexities inherent to Web3 and contrast them with the more familiar Web2 framework. Our focus is to explain how these unique attributes—namely decentralization, lack of regulation, and technical complexity—create both challenges and opportunities for auditing in the Web3 realm.

1) *Decentralization’s Role in Security Awareness:* The decentralization Web3 ecosystem, founded on blockchain technology, alters the dynamics of user interaction and security awareness [79]. While centralization in Web2 provided user convenience, it also came at the cost of individual autonomy [93]. Decentralization empowers users with greater control over their digital assets [86], thereby elevating the urgency of security risks [1]. The consequences of such decentralization are twofold. Firstly, trust shifts from centralized institutions to decentralized community entities, such as audit firms, which play an integral role in shaping users’ risk assessments and security decisions [77]. Secondly, auditing quality becomes crucial as it acts as a form of “market regulation”, guiding informed user decisions and potentially exposing them to risks if executed irresponsibly. Both aspects underline the necessity for rigorous and transparent auditing in the evolving Web3 ecosystem.

2) *Lack of Regulation and the Demand for Auditing:* Web3’s minimal regulatory framework [20] stands in stark contrast to the regulatory landscape in Web2. While this allows greater freedom and innovation [59], it also engenders a slew of trust issues [81] and a lack of standardized security protocols [87]. In response, Web3 auditing has emerged as a potential instrument to navigate this unregulated space. Through the mechanism of third-party auditing, applications can demonstrate adherence to security standards and best practices. However, as highlighted in Section V-A2, the absence of universally accepted auditing standards could muddy the waters, eroding user trust and potentially jeopardizing the integrity of the entire ecosystem.

3) *Technical Complexity and the Role of Auditing in Usability:* Blockchain technology, while revolutionary, adds a layer of complexity that often makes it challenging for average users to navigate Web3 safely [23]. Auditing helps bridge this gap in two key ways. First, it translates the technical complexities of smart contracts into more accessible, yet detailed, audit results, aiding users in making informed decisions [68]. However, as noted in Section VI, the readability of current audit reports still needs improvement. Second, as discussed in Section V-A3, audit firms play an educational role [27], enhancing users’ understanding of the risks and rewards associated with various Web3 applications [6]. This dual role of auditing, as both a technical reviewer and educational facilitator, is crucial in improving Web3’s usability and overall security.

B. Challenges in Web3 Auditing

This section highlights three key challenges in Web3 auditing: information presentation, lack of industry standardization, and community trust issues. These challenges hinder the readability of audit reports, undermine user confidence, and raise doubts about the security role of audits.

1) *Information Gap: Balancing Technical Proficiency and Readability:* Balancing the professionalism and readability of existing audit information is a significant challenge. Auditing, a specialized field, discloses information in technical knowledge, which can present the professionalism of audit firms while posing a technical barrier for common users, as found in Section IV-C. Therefore, the challenge lies in satisfying the needs of different users concurrently:

For technically savvy users, detailed audit information, such as audit reports, serves as valuable educational resources and decision-making aids, as discussed in Section V-A3. However, as noted in Section IV-C, users have expressed concerns about the repetitive and templated nature of the content, which hinders their ability to find valuable information. Meanwhile, when users try to verify the authenticity of audit reports by inspecting the source code, they face challenges due to the lack of clear descriptions of

error codes, making it difficult to efficiently identify specific lines of code associated with errors.

For ordinary users, while current audit reports include user-friendly elements such as security scores and summaries to facilitate understanding, readability challenges persist, as elucidated in Section IV-C. This issue is linked to audit firms' inadequate information disclosure. Due to such limited disclosure, as noted in Section IV-B, it is impractical to expect users to fully comprehend auditing mechanisms and related practices, leading to a limited understanding of auditing processes. This gap hinders them from appreciating objective metrics, like the number of vulnerabilities reported, making it challenging to trust an application's security based solely on audit reports, as mentioned in Section VI-A1.

These challenges can hinder users' understanding and may even discourage further engagement [17]. Therefore, optimizing the technical complexity and readability of audit information is a critical concern. Prior privacy policy research offers valuable insights, as both fields focus on conveying complex information to users [12]. A detailed comparison of the two areas of research is provided in Appendix B.

2) Lack of Industry Standards: Impact on User Confidence:

As highlighted in Section VII-A2, the absence of standardized auditing practices can lead to confusion and decrease user trust. The industry's lack of uniform standards and regulations creates uncertainty for users, making it difficult to distinguish between high-quality and low-quality audits. Especially when an audited application still has vulnerabilities and experiences attacks, users lack consistent criteria to assess the level of responsibility of the audit firm. They may not know whether the vulnerability resulted from the audit firm's negligent information or if the vulnerabilities existed beyond the scope of the audit's due diligence. This standardization gap damages user trust and the reputation of audit firms with a strong track record.

Moreover, as highlighted in Section V-A2, audit firms currently lack a strong reputation, with none having established a trustworthy image among users. Allowing the industry to develop without appropriate standards risks unscrupulous firms exploiting the absence of regulations for short-term gains, potentially worsening the problem. This could lead to an increase in low-quality audits.

3) Community Challenges: Navigating Trustlessness in Web3:

The decentralized nature of Web3 shifts trust models from centralized authorities to cryptographic and network-based trust, raising societal challenges [29]: Technical incomprehension makes users feel trustless in the auditing mechanism, as discussed in Section IV-C. This is because learning the professional knowledge of blockchain comes with high time costs, serving as a significant user entry barrier [52]. Without a comprehensive understanding

of the technology, placing full trust in blockchain remains difficult [97], [96]. This challenge extends to auditing, which involves explaining security information by presenting a detailed technical analysis.

Furthermore, as discussed in Section IV-B, the lack of depth and comprehensiveness in audit information impedes users' ability to understand and appreciate the auditing process. This insufficiency in information undermines the foundation of trust that users have in auditing, as referenced in Section V-B3. Consequently, when negative news related to audits emerges, this already fragile trust is further compromised. Negative news inherently possesses a stronger propensity for dissemination due to its emotional impact [32], which in turn exacerbates the instability of users' trust in the auditing process, as found in Section V-B1.

The risk of dishonest traders has hindered users from trusting audit firms, a reflection of prevalent fraud issues within the Web3 ecosystem [79]. Malicious Web3 applications often employ deceptive strategies to attract users into investing their assets, subsequently executing rug pulls [4]. The decentralized and pseudonymous nature of blockchain further complicates holding these fraudsters accountable, leaving users to bear their full financial losses [79]. Consequently, users approach Web3 auditing skeptically after experiencing such widespread fraud, as noted in section V-A2. Their distrust in the independence and impartiality of audit firms stems from this volatile environment.

Hence, this shapes users' attitudes toward the diversity of auditing, as explored in Section V-B. On one hand, users recognize that auditing, when conducted with fairness and independence, can offer significant benefits to both individual users and the broader ecosystem. However, on the other hand, users remain skeptical about the ability to maintain impartiality and independence in the decentralized Web3 environment. As revealed in Section VI-A, this skepticism limits users' engagement with auditing initiatives.

C. Design Implications

While technological advancements are undeniably essential for improving Web3 auditing, this paper focuses on a user-centric perspective. We examine the design implications from two critical perspectives: the user and the audit firm. The insights provided herein aim to inform future Web3 auditing practices.

1) For Users: Leveraging Communities for Technical Understanding:

As noted in Section VII-B3, the lack of technical understanding among users hinders their ability to trust auditing, and inadequate information disclosure leads them to rely on free expert advice from personal connections. Online communities can step in to fill this expert role. These communities generally take two forms: those officially sanctioned by audit firms and those spontaneously organized by users, such as Decentralized Autonomous Organizations (DAOs).

Audit firms have sought to bridge this gap by fostering dedicated communities on platforms like Discord [14]. In these digital spaces, specialized personnel are available to address users' audit-related queries. Additionally, educational activities, such as community knowledge competitions, are regularly organized to enhance users' understanding and reward engagement. This approach gives users direct access to expert knowledge, expanding their information channels. For audit firms, it boosts users' security awareness and showcases their professionalism, thereby strengthening their reputation within the Web3 ecosystem.

DAOs may also serve as potent platforms for information dissemination [78]. Within DAOs, technically proficient users can review and interpret audit reports, followed by a community-wide evaluation through voting. This decentralized approach not only enhances community knowledge but also incentivizes valuable contributions by knowledgeable individuals through the tokens awarded within the DAO framework. Consequently, this approach addresses the sustainability issues observed when users rely on personal networks to seek unpaid assistance, as found in Section IV-B.

2) *For Audit Firms: Information Balance and Trust-built Measures:* To address the challenges in Section VII-B, audit firms can optimize the user experience by improving audit outcome presentations and enhancing firm reputation.

Strategies for optimized information balanced presentation. Optimizing the presentation of audit results helps balance the professionalism and readability of existing audit information, facilitating effective communication between audit firms and users. A multipronged strategy is suggested for delivering informative and accessible audit outcomes.

The security information in audit reports should be inherently interpretable to accommodate users, most of whom lack specialized auditing knowledge. Enhancing interpretability could involve incorporating comparative data and industry-specific benchmarks [61], providing users with immediate, understandable context without the need to decipher complex audit terminologies. Additionally, audit firms must carefully consider how absolute figures are presented to meet users' diverse comprehension levels. Overemphasizing high audit scores without sufficient explanation may undermine the firm's credibility, as discussed in Section VII-B1. Such practices risk creating an information gap that could reduce the effectiveness of the audit report in communicating security standings.

For expert users capable of interpreting audit information, enhancing usability is key to fostering trust, as noted in Section VII-B3. Interactive web platforms, rather than static PDF reports, offer a promising solution by enabling direct engagement with the audit data [89]. Features like side-by-side comparison tools and clickable code snippets provide a deeper, contextual understanding of the findings. These platforms

also serve as valuable tools for audit firms to identify novice users' specific challenges in interpreting audit information. By tracking user interactions and integrating real-time feedback mechanisms, audit firms can gather insights to refine their reports and communication strategies, ultimately enhancing user comprehension and trust, and contributing to the evolution of auditing practices.

Reputation enhancement through transparency and collaboration. This research reveals that a positive reputation can effectively mitigate users' concerns about dishonest traders, as discussed in Section V-A1. We explore three potential solutions for audit firms to enhance their reputation: improving information transparency, strengthening community engagement, and fostering collaboration with both the community and the industry.

To bolster their reputation and user trust, audit firms need to significantly improve information transparency, as noted in Section VII-B1. A dual-faceted approach can be employed to address this. First, firms should disclose in-depth details about their audit methodologies, procedures, and outcomes, supported by the establishment of professional communities and dedicated channels for information sharing. Second, to emphasize their role as unbiased third parties, audit firms should be transparent about their interactions with the applications being audited. This can include revealing automated analyses, manual assessments, and remediation steps within the auditing workflow, as mentioned in Section V-A2. Timely uploading of this data to a blockchain platform can further assure users of the firm's impartiality, leveraging the blockchain's inherent resistance to data manipulation [82].

Enhancing community engagement can significantly improve an audit firm's reputation. As mentioned in Section V-A3, firms can build user trust by disseminating security education through social media [40]. Given the trust issues associated with the Web3 ecosystem, the DAOs can be formed for added accountability [37]. These DAOs can compel firms to conduct white-hat activities post-security incidents and may even define compensation conditions in cases where the audit firm is culpable.

Industry-wide collaboration to standardize audit practices is essential for reputation enhancement, as noted in Section VII-B2. The current lack of clear standards undermines user trust. Audit firms can benefit by actively participating in dialogues to establish uniform practices and expediting improvements through shared insights on security and detection technology [50]. Once standardized criteria are established, educating users on these benchmarks will foster both trust and the industry's overall standing.

VIII. CONCLUSION

This paper presents a pioneering shift in the understanding of auditing, traditionally viewed as a technical

exercise for developers. We introduce a novel perspective by examining auditing as a form of security information for end-users. Our research provides valuable insights into how users perceive and are affected by these security practices, shedding light on their behavior. This user-centric approach not only enriches the discourse on Web3 auditing but also contributes to the secure development of the decentralized ecosystem.

ACKNOWLEDGMENT

This work was supported in part by the funding from the Science and Technology Development Fund (FDCT) of Macau SAR under File No. 0078/2023/AMJ and 0129/2022/A; and the funding from University of Macau under File No. MYRG-GRG2024-00052-FST.

REFERENCES

- [1] S. Abramova, A. Voskobojnikov, K. Beznosov, and R. Böhme, "Bits under the mattress: Understanding different risk perceptions and security behaviors of crypto-asset users," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021, pp. 1–19.
- [2] I. Adjerid, A. Acquisti, L. Brandimarte, and G. Loewenstein, "Sleights of privacy: Framing, disclosures, and the limits of transparency," in *Proceedings of the ninth symposium on usable privacy and security*, 2013, pp. 1–11.
- [3] I. E. Allen and C. A. Seaman, "Likert scales and data analyses," *Quality progress*, vol. 40, no. 7, pp. 64–65, 2007.
- [4] N. Amosova, A. Y. Kosobutskaya, and O. Rudakova, "Risks of unregulated use of blockchain technology in the financial markets," in *4th International Conference on Economics, Management, Law and Education (EMLE 2018)*. Atlantis Press, 2018, pp. 9–13.
- [5] J. Apotheker, "Web3 already has a gender diversity problem," Feb. 2023. [Online]. Available: <https://www.bcg.com/publications/2023/how-to-unravel-lack-of-gender-diversity-web3>
- [6] B. Awaji, E. Solaiman, and L. Marshall, "Investigating the requirements for building a blockchain-based achievement record system," in *Proceedings of the 5th International Conference on Information and Education Innovations*, 2020, pp. 56–60.
- [7] A. Bacchelli and C. Bird, "Expectations, outcomes, and challenges of modern code review," in *2013 35th International Conference on Software Engineering (ICSE)*. IEEE, 2013, pp. 712–721.
- [8] J. Baumgartner, S. Zannettou, B. Keegan, M. Squire, and J. Blackburn, "The pushshift reddit dataset," in *Proceedings of the international AAAI conference on web and social media*, vol. 14, 2020, pp. 830–839.
- [9] D. Bergemann and S. Morris, "Information design, bayesian persuasion, and bayes correlated equilibrium," *American Economic Review*, vol. 106, no. 5, pp. 586–591, 2016.
- [10] N. J.-M. Blackman and J. J. Koval, "Interval estimation for cohen's kappa as a measure of agreement," *Statistics in medicine*, vol. 19, no. 5, pp. 723–741, 2000.
- [11] R. E. Boyatzis, *Transforming qualitative information: Thematic analysis and code development*. sage, 1998.
- [12] W. Brunotte, L. Chazette, L. Kohler, J. Klunder, and K. Schneider, "What about my privacy? helping users understand online privacy policies," in *Proceedings of the International Conference on Software and System Processes and International Conference on Global Software Engineering*, 2022, pp. 56–65.
- [13] S. Bugiel, S. Heuser, and A.-R. Sadeghi, "Flexible and fine-grained mandatory access control on android for diverse security and privacy policies," in *22nd USENIX Security Symposium (USENIX Security 13)*, 2013, pp. 131–146.
- [14] Certik, "Watchlists," September 2023. [Online]. Available: <https://discord.com/channels/972341869864435803/1039841599976378368/1151147333216649316>
- [15] Y. Chang, S. F. Wong, C. F. Libaque-Saenz, and H. Lee, "The role of privacy policy on consumers' perceived privacy," *Government Information Quarterly*, vol. 35, no. 3, pp. 445–459, 2018.
- [16] W. Chen, W. J. Smieliauskas, and G. Trippen, "An audit evidence gathering model in online auditing environments," in *2011 IEEE International Conference on Systems, Man, and Cybernetics*. IEEE, 2011, pp. 1448–1452.
- [17] C.-W. Chiang, E. Betanzos, and S. Savage, "Exploring blockchain for trustful collaborations between immigrants and governments," in *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018, pp. 1–6.
- [18] D. C. Chou, D. C. Yen, and J. Q. Chen, "Analysis of the total quality management-based software auditing," *Total Quality Management*, vol. 9, no. 7, pp. 611–618, 1998.
- [19] D. Cooper, "Psychology, risk and safety," *Professional Safety*, vol. 48, no. 11, pp. 39–46, 2003.
- [20] S. Corbet, C. Larkin, B. Lucey, A. Meegan, and L. Yarovaya, "Cryptocurrency reaction to fomic announcements: Evidence of heterogeneity based on blockchain stack position," *Journal of Financial Stability*, vol. 46, p. 100706, 2020.
- [21] B. Custers, S. van der Hof, and B. Schermer, "Privacy expectations of social media users: The role of informed consent in privacy policies," *Policy & Internet*, vol. 6, no. 3, pp. 268–295, 2014.
- [22] J. Czerwonka, M. Greiler, and J. Tilford, "Code reviews do not find bugs. how the current code review best practice slows us down," in *2015 IEEE/ACM 37th IEEE International Conference on Software Engineering*, vol. 2. IEEE, 2015, pp. 27–28.
- [23] J. O. D. da Silva and D. R. dos Santos, "Study of blockchain application in the logistics industry," *Theoretical Economics Letters*, vol. 12, no. 2, pp. 321–342, 2022.
- [24] "Defillama - defi dashboard," 2023, [https://defillama.com/\(date of access: June 6, 2023\)](https://defillama.com/(date%20of%20access%3A%20June%206%2C%202023)).
- [25] W. H. Deng, B. Guo, A. Devrio, H. Shen, M. Eslami, and K. Holstein, "Understanding practices, challenges, and opportunities for user-engaged algorithm auditing in industry practice," in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 2023, pp. 1–18.
- [26] G. D'Onza, R. Lamboglia, and R. Verona, "Do it audits satisfy senior manager expectations? a qualitative study based on italian banks," *Managerial Auditing Journal*, vol. 30, no. 4/5, pp. 413–434, 2015.
- [27] Dron-Hacken, "Excited to greet everyone for our usual friday community talk!" June 2023. [Online]. Available: <https://discord.com/channels/930851702297485393/951405721344434187/1134427674614431814>
- [28] A. C. Dzurani and I. Mălăescu, "The current state and future direction of it audit: Challenges and opportunities," *Journal of Information Systems*, vol. 30, no. 1, pp. 7–20, 2016.
- [29] C. Elsdén, A. Manohar, J. Briggs, M. Harding, C. Speed, and J. Vines, "Making sense of blockchain applications: A typology for hci," in *Proceedings of the 2018 chi conference on human factors in computing systems*, 2018, pp. 1–14.
- [30] D. Feng, R. Hitsch, K. Qin, A. Gervais, R. Wattenhofer, Y. Yao, and Y. Wang, "Defi auditing: Mechanisms, effectiveness, and user perceptions," in *International Conference on Financial Cryptography and Data Security*. Springer, 2023, pp. 320–336.
- [31] J. Fereday and E. Muir-Cochrane, "Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development," *International journal of qualitative methods*, vol. 5, no. 1, pp. 80–92, 2006.
- [32] E. Ferrara and Z. Yang, "Measuring emotional contagion in social media," *PLoS one*, vol. 10, no. 11, p. e0142390, 2015.
- [33] A. Friebely, "Analyzing the efficacy of microsoft presidio in identifying social security numbers in unstructured text," Ph.D. dissertation, Utica University, 2022.
- [34] M. Fröhlich, M. R. Wagenhaus, A. Schmidt, and F. Alt, "Don't stop me now! exploring challenges of first-time cryptocurrency users," in *Designing Interactive Systems Conference 2021*, 2021, pp. 138–148.
- [35] C. García, A. Guerrero, J. Zeitsoff, S. Korlakunta, P. Fernandez, A. Fox, and A. Ruiz-Cortés, "Bluejay: a cross-tooling audit framework for agile software teams," in *2021*

- IEEE/ACM 43rd International Conference on Software Engineering: Software Engineering Education and Training (ICSE-SEET)*. IEEE, 2021, pp. 283–288.
- [36] M. Y. Guan, J. Li, J. Hu, Z. Gu, Y. Wang, Z. Lu, and K. Y. Wang, “From digital art to crypto art: The evolution of art brought by nft,” *International Journal of Human-Computer Interaction*, pp. 1–20, 2024.
- [37] Y. Guan, Y. Yu, T. Sharma, K. Qin, Y. Wang, and Y. Wang, “Examining user perceptions of stablecoins: Understandings and risks.”
- [38] H. Habib, Y. Zou, Y. Yao, A. Acquisti, L. Cranor, J. Reidenberg, N. Sadeh, and F. Schaub, “Toggles, dollar signs, and triangles: How to (in) effectively convey privacy choices with icons and link texts,” in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021, pp. 1–25.
- [39] H. Habib, M. B. Musa, M. F. Zaffar, and R. Nithyanand, “Are proactive interventions for reddit communities feasible?” in *Proceedings of the International AAI Conference on Web and Social Media*, vol. 16, 2022, pp. 264–274.
- [40] S. Hanson, L. Jiang, and D. Dahl, “Enhancing consumer engagement in an online brand community via user reputation signals: A multi-method analysis,” *Journal of the Academy of Marketing Science*, vol. 47, pp. 349–367, 2019.
- [41] J. P. Hasley and D. G. Gregg, “An exploratory study of website information content,” *Journal of theoretical and applied electronic commerce research*, vol. 5, no. 3, 2010. [Online]. Available: <http://dx.doi.org/10.4067/S0718-18762010000300004>
- [42] A. Z. Henley, K. Muçlu, M. Christakis, S. D. Fleming, and C. Bird, “Cfar: A tool to increase communication, productivity, and review quality in collaborative code reviews,” in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018, pp. 1–13.
- [43] Z. Huang, J. Zhu, Z. Huang, Y. Xu, J. Yen, and Y. Wang, “Safeguarding the unseen: a study on data privacy in defi protocols,” 2023.
- [44] C. Hutto and E. Gilbert, “Vader: A parsimonious rule-based model for sentiment analysis of social media text,” in *Proceedings of the international AAI conference on web and social media*, vol. 8, no. 1, 2014, pp. 216–225.
- [45] M. S. Jalali and A. Akhavan, “Integrating ai language models in qualitative research: Replicating interview data analysis with chatgpt,” *System Dynamics Review*, 2024.
- [46] C. Jensen, C. Potts, and C. Jensen, “Privacy practices of internet users: Self-reports versus observed behavior,” *International Journal of Human-Computer Studies*, vol. 63, no. 1-2, pp. 203–227, 2005.
- [47] P. Juneja, M. M. Bhuiyan, and T. Mitra, “Assessing enactment of content regulation policies: A post hoc crowd-sourced audit of election misinformation on youtube,” in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 2023, pp. 1–22.
- [48] P. Juneja and T. Mitra, “Auditing e-commerce platforms for algorithmically curated vaccine misinformation,” in *Proceedings of the 2021 chi conference on human factors in computing systems*, 2021, pp. 1–27.
- [49] E. Kamenica, “Bayesian persuasion and information design,” *Annual Review of Economics*, vol. 11, pp. 249–272, 2019.
- [50] P. G. Kelley, L. Cesca, J. Bresee, and L. F. Cranor, “Standardizing privacy notices: an online study of the nutrition label approach,” in *Proceedings of the SIGCHI Conference on Human factors in Computing Systems*, 2010, pp. 1573–1582.
- [51] I. E. Khairuddin and C. Sas, “An exploration of bitcoin mining practices: Miners’ trust challenges and motivations,” in *Proceedings of the 2019 CHI conference on human factors in computing systems*, 2019, pp. 1–13.
- [52] M. Knittel, S. Pitts, and R. Wash, ““ the most trustworthy coin” how ideological tensions drive trust in bitcoin,” *Proceedings of the ACM on Human-Computer Interaction*, vol. 3, no. CSCW, pp. 1–23, 2019.
- [53] M. L. Knittel and R. Wash, “How “true bitcoiners” work on reddit to maintain bitcoin,” in *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, ser. CHI EA ’19. New York, NY, USA: Association for Computing Machinery, 2019, p. 1–6. [Online]. Available: <https://doi-org.libezproxy.um.edu.mo/10.1145/3290607.3312969>
- [54] S. Kokolakis, “Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon,” *Computers & security*, vol. 64, pp. 122–134, 2017.
- [55] O. Kononenko, O. Baysal, and M. W. Godfrey, “Code review quality: How developers see it,” in *Proceedings of the 38th international conference on software engineering*, 2016, pp. 1028–1038.
- [56] O. Kononenko, O. Baysal, L. Guerrouj, Y. Cao, and M. W. Godfrey, “Investigating code review quality: Do people and participation matter?” in *2015 IEEE international conference on software maintenance and evolution (ICSME)*. IEEE, 2015, pp. 111–120.
- [57] A. Koshiyama, E. Kazim, and P. Treleaven, “Algorithm auditing: Managing the legal, ethical, and technological risks of artificial intelligence, machine learning, and associated algorithms,” *Computer*, vol. 55, no. 4, pp. 40–50, 2022.
- [58] V. Le Pochat, L. Edelson, T. Van Goethem, W. Joosen, D. McCoy, and T. Lauinger, “An audit of facebook’s political ad policy enforcement,” in *31st USENIX Security Symposium (USENIX Security 22)*, 2022, pp. 607–624.
- [59] J. Y. Lee, “A decentralized token economy: How blockchain and cryptocurrency can revolutionize business,” *Business Horizons*, vol. 62, no. 6, pp. 773–784, 2019.
- [60] C. Liu, K. Chusap, Z. Li, Z. Chen, D. Rogers, and F. Song, “Continuous collateral privacy risk auditing of evolving autonomous driving software,” in *2019 IEEE International Conference on Software Maintenance and Evolution (ICSME)*. IEEE, 2019, pp. 363–363.
- [61] W. Maalej, R. Tiarks, T. Roehm, and R. Koschke, “On the comprehension of program comprehension,” *ACM Transactions on Software Engineering and Methodology (TOSEM)*, vol. 23, no. 4, pp. 1–37, 2014.
- [62] C. MacLeod, E. Rutherford, L. Campbell, G. Ebsworthy, and L. Holker, “Selective attention and emotional vulnerability: assessing the causal basis of their association through the experimental manipulation of attentional bias,” *Journal of abnormal psychology*, vol. 111, no. 1, p. 107, 2002.
- [63] A. Mai, K. Pfeffer, M. Gusenbauer, E. Weippl, and K. Krombholz, “User mental models of cryptocurrency systems—a grounded theory approach,” in *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, 2020, pp. 341–358.
- [64] S. Majumdar, G. S. Chawla, A. Alimohammadifar, T. Madi, Y. Jarraya, M. Pourzandi, L. Wang, and M. Debbabi, “Prosas: Proactive security auditing system for clouds,” *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 4, pp. 2517–2534, 2021.
- [65] S. Majumdar, T. Madi, Y. Wang, Y. Jarraya, M. Pourzandi, L. Wang, and M. Debbabi, “User-level runtime security auditing for the cloud,” *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 5, pp. 1185–1199, 2017.
- [66] S. Mist, “Update:the @magnatefi has rug pulled \$6.4m. their website is offline and the telegram group has been deleted.” September 2023. [Online]. Available: https://twitter.com/SlowMist_Team/status/1694970619375583325
- [67] M. Mitchell, G. Tian, and Z. Wang, “Systematic audit of third-party android phones,” in *Proceedings of the 4th ACM Conference on Data and Application Security and Privacy*, 2014, pp. 175–186.
- [68] K. Nath, S. Dhar, and S. Basishtha, “Web 1.0 to web 3.0: evolution of the web and its various challenges,” in *2014 International Conference on Reliability Optimization and Information Technology (ICROIT)*. IEEE, 2014, pp. 86–89.
- [69] J. Neale, “Iterative categorization (ic): a systematic technique for analysing qualitative data,” *Addiction*, vol. 111, no. 6, pp. 1096–1106, 2016.
- [70] S. K. Ooi, C. A. Ooi, J. A. Yeap, and T. H. Goh, “Embracing bitcoin: users’ perceived security and trust,” *Quality & Quantity*, vol. 55, pp. 1219–1237, 2021.
- [71] OpenAi, “Introducing chatgpt.” [Online]. Available: <https://openai.com/blog/chatgpt/>
- [72] M. Ou, L. Wang, and H. Xun, “Deaps: Deep learning-based user-level proactive security auditing for clouds,” in *2019 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2019, pp. 1–6.
- [73] M. Pascalev, “Privacy exchanges: restoring consent in privacy self-management,” *Ethics and Information Technology*, vol. 19, no. 1, pp. 39–48, 2017.

- [74] I. Pollach, "A typology of communicative strategies in online privacy policies: Ethics, power and informed consent," *Journal of Business Ethics*, vol. 62, pp. 221–235, 2005.
- [75] A. Poller, L. Kocksch, K. Kinder-Kurlanda, and F. A. Epp, "First-time security audits as a turning point? challenges for security practices in an industry software development team," in *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, 2016, pp. 1288–1294.
- [76] B. Price, "Laddered questions and qualitative data research interviews," *Journal of advanced nursing*, vol. 37, no. 3, pp. 273–281, 2002.
- [77] M. J. Rennock, A. Cohn, and J. R. Butcher, "Blockchain technology and regulatory investigations," *Practical Law Litigation*, vol. 1, pp. 35–44, 2018.
- [78] C. Santana and L. Albareda, "Blockchain and the emergence of decentralized autonomous organizations (daos): An integrative model and research agenda," *Technological Forecasting and Social Change*, vol. 182, p. 121806, 2022.
- [79] C. Sas and I. E. Khairuddin, "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*, 2017, pp. 6499–6510.
- [80] A. Sears, J. A. Jacko, and M. S. Borella, "Internet delay effects: how users perceive quality, organization, and ease of use of information," in *CHI'97 Extended Abstracts on Human Factors in Computing Systems*, 1997, pp. 353–354.
- [81] V. Sharma, A. Barua, and A. B. Whinston, "In cryptocurrencies we trust: An empirical analysis of cryptocurrency demand and price," *Available at SSRN 3381067*, 2019.
- [82] J. J. Si, T. Sharma, and K. Y. Wang, "Understanding user-perceived security risks and mitigation strategies in the web3 ecosystem," in *Proceedings of the CHI Conference on Human Factors in Computing Systems*, 2024, pp. 1–22.
- [83] P. Singer, F. Flöck, C. Meinhart, E. Zeitfogel, and M. Strohmaier, "Evolution of reddit: from the front page of the internet to a self-referential community?" in *Proceedings of the 23rd international conference on world wide web*, 2014, pp. 517–522.
- [84] A. Soumelidou and A. Tsohou, "Towards the creation of a profile of the information privacy aware user through a systematic literature review of information privacy awareness," *Telematics and Informatics*, vol. 61, p. 101592, 2021.
- [85] V. Švábenský, J. Vykopal, and P. Čeleda, "What are cybersecurity education papers about? a systematic literature review of sigese and iticse conferences," in *Proceedings of the 51st ACM technical symposium on computer science education*, 2020, pp. 2–8.
- [86] D. Tapscott and A. Tapscott, *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. Penguin, 2016.
- [87] E. Toufaily, "An integrative model of trust toward cryptotokens applications: A customer perspective approach," *Digital Business*, vol. 2, no. 2, p. 100041, 2022.
- [88] R. Trimananda, H. Le, H. Cui, J. T. Ho, A. Shuba, and A. Markopoulou, "{OVRseen}: Auditing network traffic and privacy policies in oculus {VR}," in *31st USENIX security symposium (USENIX security 22)*, 2022, pp. 3789–3806.
- [89] A. Voskobojnikov, O. Wiese, M. Mehrabi Koushki, V. Roth, and K. Beznosov, "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*, 2021, pp. 1–14.
- [90] Y. Wang, P. Zuest, Y. Yao, Z. Lu, and R. Wattenhofer, "Impact and user perception of sandwich attacks in the defi ecosystem," in *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, 2022, pp. 1–15.
- [91] Y. Wang and Z. Lu, "Making sense of post-match fan behaviors in the online football communities," in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 2023, pp. 1–17.
- [92] Wikipedia, "Web 2.0," https://en.wikipedia.org/wiki/Web_2.0.
- [93] A. Wright and P. De Filippi, "Decentralized blockchain technology and the rise of lex cryptographia," *Available at SSRN 2580664*, 2015.
- [94] N. Ye, X. Li, Q. Chen, S. M. Emran, and M. Xu, "Probabilistic techniques for intrusion detection based on computer audit data," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 31, no. 4, pp. 266–274, 2001.
- [95] F. Zagórski, G. McClearn, S. Morin, N. McBurnett, and P. L. Vora, "Minerva—an efficient {Risk-Limiting} ballot polling audit," in *30th USENIX Security Symposium (USENIX Security 21)*, 2021, pp. 3059–3076.
- [96] J. Zarrin, H. Wen Phang, L. Babu Saheer, and B. Zarrin, "Blockchain for decentralization of internet: prospects, trends, and challenges," *Cluster Computing*, vol. 24, no. 4, pp. 2841–2866, 2021.
- [97] L. Zavolokina, N. Zani, and G. Schwabe, "Why should i trust a blockchain platform? designing for trust in the digital car dossier," in *Extending the Boundaries of Design Science Theory and Practice: 14th International Conference on Design Science Research in Information Systems and Technology, DESRIST 2019, Worcester, MA, USA, June 4–6, 2019, Proceedings 14*. Springer, 2019, pp. 269–283.
- [98] L. Zhou, X. Xiong, J. Ernstberger, S. Chaliasos, Z. Wang, Y. Wang, K. Qin, R. Wattenhofer, D. Song, and A. Gervais, "Sok: Decentralized finance (defi) attacks," in *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2023, pp. 2444–2461.

APPENDIX A

RELATIONSHIP BETWEEN THE RESEARCH METHODS, FINDINGS, AND RQS

Table I serves as a supplementary explanation of the relationships between our research methods, findings, and RQs. It highlights which methods contributed to specific findings and how they address the formulated RQs.

APPENDIX B

COMPARISON BETWEEN PRIVACY POLICY RESEARCH AND WEB3 AUDITING RESEARCH

We recognize the importance of privacy policy research in conveying information to users and acknowledge the similarities with Web3 auditing, particularly in terms of how complex terminology impacts user comprehension. However, due to the fundamental differences in the ecosystems where these two operate, our findings on Web3 auditing can provide novel insights for the secure development of the Web3 ecosystem. Therefore, in this section, we first compare the key differences between privacy policies and Web3 auditing that lead to distinct user perceptions and design implications. We then explore the similarities, highlighting how Web3 auditing can benefit from insights gained in privacy policy research.

A. Key Differences between Privacy Policy Research and Web3 Auditing Research

While privacy policy research offers valuable insights, there are significant differences between privacy policies and Web3 auditing. These following differences highlight the unique challenges and considerations specific to Web3 auditing, underscoring the need for tailored research in this area.

Differences in Information Delivery: Privacy policies are mandatory agreements that users must accept before using most applications, often without needing to actively retrieve them [13]. In contrast, Web3 audit results are supplementary security information that

TABLE I: The relationship between the research methods, findings, and RQs, where check marks indicate which method contributed to each finding. From the table, it is clear that our interview method supported most of the findings, while the case study and Reddit analysis served to supplement and cross-validate the findings from the interviews.

Section	Subsection	Subsubsection	Case Study	Interview	Reddit
Perceptions of Security Information Obtained from Web3 Auditing(RQ1)	Singularity in Locating Audit Information	Rely on Application's Official Website		✓	
	Gaps in Audit Information Disclosure	Lack of Depth		✓	
		Lack of Comprehensiveness	✓	✓	✓
	Challenges in Understanding Information	Technical Web3 Audit Information		✓	
Perceptions of the Role of Web3 Auditing in Security Enhancement(RQ2)	Perception of Audit Firms	Presentation of Audit Results		✓	✓
		Correlation Between Reputation and Quality		✓	
		Lack of Impartiality and Independence in Audit Firms		✓	✓
	Perception of Impact of Auditing on Web3 Security	Catalysts for Security Education	✓	✓	✓
		Questioning the Effectiveness		✓	✓
		Auditing as a Catalyst for Enhanced Security		✓	✓
		Auditing as a Proof to Security Actions	✓	✓	✓
Perceived Impact of Web3 Auditing on Users' user Interactions with Audited Application(RQ3)	Users' Decision-Making Process	Pre-decision: Limited Impact		✓	
		In-the-Moment: Asymmetrical Influence			✓
	Security Awareness on Web3 Operations	Enhance Usable Security		✓	✓

users do not directly encounter in the application interface. Therefore, for Web3 auditing, it is important to consider whether audit information is easily accessible to users (Section IV). However, as we found that users generally reported easy access to audit information, no additional design recommendations were made in this regard.

Differences in User Decision-Making: Privacy policy research focuses on users granting permission for applications to access their personal data [15], with prior studies highlighting how privacy policies influence users' data management behavior. These studies also reveal the existence of the "privacy paradox," where users value privacy but rarely read policies or seek more information [54]. Web3 audits, however, primarily affect users' evaluations of whether to engage with Web3 applications. As such, the focus here is on how audit information influences users' decision-making (Section VI). These two areas differ significantly in how they impact users, leading to distinct design implications for information transparency. While privacy policy research emphasizes transparency in data collection [2], Web3 auditing focuses on the transparency of the auditing process.

Differences in Application Information Disclosure Motivation: Privacy policy disclosure is legally required, meaning applications are often passive in providing this information and may obfuscate unethical data handling practices [74]. In contrast, Web3 audits are voluntary security verification measures aimed at building trust through third-party certification, with additional costs paid to external security firms. Therefore, when proposing design implications, privacy studies focus on preventing users from overlooking potential privacy violations, using solutions like optimizing informed consent methods [21], [73]. In contrast, Web3 auditing research emphasizes whether users recognize the security practices of applications (Section V) and how to design audit information to enhance user trust.

Differences in Educational Role: Security awareness related to privacy in Web2 is often enforced by government regulations and integrated into school curricula, ensuring users receive basic knowledge

through mandatory mechanisms [84]. In the decentralized Web3 ecosystem, there is no centralized authority responsible for security education. Therefore, design implications for security awareness target different entities. While privacy policy research focuses on professional groups like students or employees with similar knowledge backgrounds and skill levels [85], Web3 auditing targets end users in a more complex environment. Our research found that Web3 audit firms and decentralized organizations play a crucial role in educating users about security (Section V-A3), offering valuable insights into general security education, as covered in our design implications(Section VII-C1).

B. Similarities between Privacy Policy Research and Web3 Auditing Research

Though privacy policy research and Web3 auditing address different domains, they share several user challenges that Web3 auditing can learn from. These similarities provide opportunities for Web3 auditing to adopt proven strategies from privacy policy studies to improve user comprehension and trust.

Similarities in User Challenges with Technical Complexity: Both privacy policies and Web3 audit reports contain technical language that can overwhelm users, making it difficult to fully understand the content [13]. Research in privacy policy studies shows that simplifying language or using visual aids, such as icons, can improve user comprehension [38]. Similarly, Web3 auditing could benefit from adopting these strategies by presenting audit results in a more accessible format.

In fact, some of these practices have already been adopted by Web3 auditing, such as using absolute security scores. However, this introduces a new challenge, as we found that users struggle to understand the relationship between the score and actual security (Section IV-C).

Similarities in Lack of Standardization and Consistency: Both privacy policies and Web3 audits face challenges due to the lack of standardization in how information is presented. In the case of privacy policies, this lack of consistency across platforms makes it difficult for users to compare and understand the privacy practices of different services [21]. This is similarly

reflected in Web3 auditing, where audit reports can vary significantly depending on the auditing firm, making it hard for users to consistently evaluate security practices across different decentralized applications (Section IV). Drawing from privacy policy research, Web3 auditing practices could benefit from developing standardized formats and criteria (Section VII-C2), helping users better navigate and compare audit results across various platforms.

Similarities in User Skepticism Towards Effectiveness: User skepticism about the effectiveness of privacy policies has been well-documented, with users often feeling that privacy policies provide little real protection and serve more as a formality [46]. Similarly, Web3 users may question the value of audit reports, often due to distrust in audit firms and a lack of understanding of the audit information (Section V).

To address this skepticism, privacy research has recommended greater transparency and user-centered communication to improve trust [46]. Web3 auditing could adopt similar approaches by making audit processes more transparent and involving users in the auditing ecosystem, such as providing clear and detailed explanations of how audits are conducted and the security guarantees they offer (Section VII-C2).

C. Conclusion

Through this comparison, it becomes clear that while privacy policy research provides valuable insights that can inform Web3 auditing practices, not all findings are directly transferable. Strategies such as simplifying language, standardizing information formats, and using layered disclosures to enhance transparency and user comprehension are highly applicable to Web3 auditing, given the similar user challenges related to information complexity.

However, the unique characteristics of Web3 auditing, arising from the blockchain technology, require additional design considerations that may not apply to privacy policy research. For example, although Web3 auditing has adopted readability enhancements similar to those in privacy policy research, our study reveals that these efforts alone are insufficient for Web3 users. The trustless nature of decentralized systems demands not only greater transparency but also clarity in how audit information is generated, verified, and validated (Section VII-B3). This highlights the need for advanced mechanisms that go beyond readability, such as real-time verification tools, which we propose as part of our recommendations (Section VII-C2).

Therefore, our research focuses on users’ perceptions of security information disclosures practices in decentralized environments and proposes design recommendations to address the unique needs and challenges users face in such ecosystems—areas not covered by privacy policy research—contributing to the secure development of decentralized systems.

APPENDIX C DETAILS ABOUT INTERVIEW

In this section, we provide the details of our interview study, including a demographic summary of the interviewees and the strategies and criteria used for recruiting them. Additionally, the interview protocol is provided in Appendix F for easier reference.

A. Demographic Summary of Interviewees

The details of participants’ demographics can be found in Table II.

TABLE II: Demographic summary of interviewees. Note: gender is denoted as M (Male) or F (Female). The “Experience” refers to the number of years of experience in Web3.

	Self Report Occupation	Gender	Country	Experience
1	Web3 Investor	M	Ukraine	6
2	Student	M	China	2
3	Student	M	Singapore	2
4	Student	M	USA	2
5	Developer	M	China	4
6	Web3 Operator	M	China	3
7	Web3 Developer	M	China	4
8	Student	M	China	4
9	Student	M	Switzerland	3
10	Student	M	Switzerland	5
11	Investor	M	China	6
12	Student	M	Nigeria	3
13	Investor	M	China	3
14	Student	M	China	2
15	Developer	M	China	6
16	Developer	M	China	5
17	Student	M	China	7
18	Unemployed	F	China	5
19	Accountant	F	Australia	2
20	Web3 Operator	F	China	1

B. Interview Recruitment and Screening

This subsection details the strategies and criteria used for recruiting interviewees, including the steps taken to ensure a rigorous and unbiased selection process.

Our recruitment initiatives were implemented across various social media platforms, namely X, Discord, and Telegram, and were further supported by the utilization of our research team’s personal networks. The sample recruitment message disseminated was as follows:

“We are a team of researchers from [University Name redacted for peer review] dedicated to exploring user perceptions of Web3 auditing. Our goal is to conduct interviews with Web3 users to gain insight into their experiences and viewpoints regarding auditing practices. Participation will be confidential, with interviews carried out individually via Zoom or a comparable platform. Recordings will be made for the sole purpose of research and will be accessed only by the research team. Each interview will last approximately 45 minutes, and participants will be remunerated \$20 for their time and insights. If interested, please contact XX at [Researcher’s Email].”

To participate in the study, individuals were required to demonstrate a basic understanding of Web3 auditing, have experience using Web3 applications, and be at least 18 years of age. The screening process was conducted through online textual communication, where candidates were asked to articulate their knowledge of Web3 auditing by explaining the concept and providing examples, thus allowing us to assess their familiarity with the subject matter. They were also required to discuss their primary Web3 applications and usage intentions to evaluate their hands-on experience in the field. Age verification was included in the screening to ensure all participants met the minimum age requirement. Adherence to these criteria was imperative, and only those meeting all specified conditions were extended an invitation to contribute to the research.

APPENDIX D

DETAILS ABOUT EMPIRICAL ANALYSIS ON REDDIT

This section is dedicated to elucidating the comprehensive methodology and results of our empirical analysis conducted on Reddit, thereby ensuring transparency and reproducibility of our research findings.

A. Details About Data Collection

Table III provides detailed information about the selected subreddits from which data were extracted, whereas Table IV lists the specific keywords used for data extraction.

TABLE III: Information on Selected Subreddits. The table details the rank, name, and number of members (in millions).

Rank	Name	Members (M)	Rank	Name	Members (M)
69	r/CryptoCurrency	7	380	r/CryptoMarkets	1.6
231	r/ethereum	2.6	442	r/CryptoTechnology	1.3
81	r/bitcoin	5.9	531	r/BitcoinBeginners	1.1
240	r/dogecoin	2.4	534	r/btc	1.1
369	r/NFT	1.6	689	r/cardano	0.689

TABLE IV: Keywords used for Reddit PSAW extraction, categorized into common terms related to Web3 auditing and names of 20 audit firms as noted in Section III-A2. These firms audit Web3 applications with a TVL exceeding 1 billion USD.

Keyword Type	Keywords
Auditing Related Terms	audit, auditing, auditor, code review
Audit Firms	Certora, CertiK, Peckshield, Quantstamp, ABDK, BlockSec, ChainSecurity, ConsenSys Diligence, DeFiSafety, Hexens, MixBytes, OpenZeppelin, OtterSec, Oxorio, Runtime Verification, SigmaPrime

B. Details About Classification Tasks Using GPT-4

In our research, we utilized GPT-4 for three classification tasks:

TABLE V: Classification of Sentiment by GPT-4. This table categorizes sampled posts into five sentiment classes based on their content, from very negative (1) to very positive (5).

Sentiment Class	Post Content Example
1: Very Negative	Audits in this space don't mean anything.
2: Slightly Negative	[Application] Audit Failed
3: Neutral	Solidity DApp Audits
4: Slightly Positive	USDC is not in danger of collapsing
5: Very Positive	New crypto audit services are being offered!!!

- 1) Filtering Out Posts Unrelated to Web3 Auditing:** The first task involved filtering out posts that were not related to Web3 auditing.
- 2) Categorizing Posts by Topic:** The second task was categorizing posts related to Web3 auditing by specific topics. Table VI provides the samples for categorization.
- 3) Assigning Sentiment Scores:** The third task involved assigning sentiment scores to relevant posts based on their content. Samples representing different sentiment scores are available for review in Table V.

1) Development of GPT-4 Classification Prompts:

The process of developing prompts for GPT-4 classification followed these steps:

Sampling and Labeling: We employed a random sampling approach to ensure the representativeness of our dataset. A total of 100 posts were sampled. These posts were then independently labeled by two researchers, each receiving 10 posts per round for a total of 10 rounds. This ensured that researchers consistently worked with smaller, manageable groups of posts, enhancing focus and reducing the likelihood of error.

Comparison and Consensus: After each round of labeling, the results were compared using inter-rater reliability analysis. Discrepancies between the researchers were recorded, and discussions were held to resolve any disagreements. After 10 rounds of discussion, a consistent classification guideline was finalized. Cohen's Kappa [10] was used to calculate inter-rater reliability, yielding a value over 0.8, which indicates substantial agreement.

Classification Standard Development and Prompt Creation: After establishing the classification standard, we translated the guidelines into a prompt for GPT-4. The prompt was tested on the labeled subset of 100 data, with accuracy metrics used to evaluate GPT-4's performance. The prompt was iteratively adjusted until GPT-4 consistently achieved 80% accuracy. During this process, we also conducted an error analysis to refine the prompt further by addressing common misclassifications.

Validation Process: Once the prompt was finalized, we used GPT-4 to classify the entire dataset. To validate the model's performance, a second random

sample of 100 posts was taken. These posts were independently labeled by two researchers, following the established classification guidelines. Accuracy was recalculated to ensure model performance. If the overall accuracy fell below 90%, we re-examined both the prompt and the classification standard for possible improvements, repeating the prompt refinement process if necessary. This ensured that the final classification met the pre-defined performance threshold.

2) *Classification Task Prompts:* We provide the prompts used for the three classification tasks below.

First Classification Task Prompt: Filtering Out Posts Unrelated to Web3 Auditing.

“I will give you the titles and content of some Reddit posts, and you will need to use this information to determine whether they are related to Web3 auditing. First, let me tell you what Web3 auditing is. Web3 auditing, conducted by specialized security firms, acts as a crucial external mechanism for assessing and bolstering the security of smart contracts in Web3 applications. This process typically concludes with the public disclosure of their audited status. Please understand this definition, and then I will give you some examples to tell you whether these contents are related to Web3 auditing to help you learn and understand.”

Second Classification Task Prompt: Categorizing Posts Related to Web3 Auditing by Topic.

“Main Category 1: Direct Discussion of Web3 Auditing”

- *1.1: How Audits are Conducted* - Discussions on methodologies and processes of audits.
- *1.2: Audit Firms/Auditors* - Discussions on organizations or individuals conducting audits.
- *1.3: Impact of Audits* - Discussions on the effectiveness and importance of audits.

Main Category 2: Discussion of Application Audit Dynamics

- *2.1: Upcoming Audits* - Discussions on audits about to commence.
- *2.2: Ongoing Audits* - Discussions on audits currently in progress.
- *2.3: Halted Audits* - Discussions on audits that have been interrupted or canceled.
- *2.4: Successful Audits* - Discussions on audits concluded successfully.
- *2.5: Failed Audits* - Discussions on audits that did not meet goals or standards.
- *2.6: Post-Audit Attacks* - Discussions on attacks faced by applications after an audit.

Main Category 3: Security Dynamics of Auditing Firms

- *3.1: Security Practices of Audit Firms* - Discussions on security practices in application.
- *3.2: Security Knowledge of Audit Firms* - Discussions on security knowledge shared by firms.

Task: Classify the following post into one of the main categories and subcategories with one-sentence reasons. You should return your response in the following format: ‘The Main Category is {number} because...; the subcategory is {number} because...’.

Third Classification Task Prompt: Assigning Sentiment Scores

“Please analyze the sentiment of the text based on the title and content I provide and classify the text into one of the following five levels: 1: Very Negative, 2: Slightly Negative, 3: Neutral, 4: Slightly Positive, 5: Very Positive.”

C. Details About Sentiment Analysis Selection

In this section, we detail the methodology for selecting our sentiment analysis tools. As mentioned in Section III-C3, we used GPT-4 to perform the sentiment scoring task, where GPT-4 calculated a sentiment score for each post, ranging from 1 (very negative) to 5 (very positive), with 3 representing a neutral sentiment. This process follows the same flow described in Section D-B.

We evaluated both VADER [44] and GPT-4 [71] for their capabilities to analyze textual sentiment. We selected VADER as a comparison tool due to its widespread use in social media sentiment analysis [91]. However, VADER calculates sentiment scores on a scale from -1 to 1, with compound scores greater than 0.05 indicating positive sentiment and less than -0.05 indicating negative sentiment, while GPT-4 operates on a Likert 5-point scale. These different scoring systems are not directly comparable. To ensure a fair comparison, we mapped VADER and GPT-4 results to a unified three-category sentiment scale: negative, neutral, and positive. Based on this mapping, we evaluated the accuracy of sentiment analysis. Through the analysis of sampled posts, we found that GPT-4 achieved an accuracy rate of 91%, significantly outperforming VADER’s 62%. Therefore, GPT-4 was selected as the sentiment analysis tool for this study due to its higher accuracy in reflecting community sentiment.

Additionally, we further evaluated GPT-4’s accuracy on the 1-5 scale using the ground truth sample posts. The results showed an overall accuracy rate of 92%. We also calculated the recall values for each of the five

sentiment levels: 1 (very negative) at 92%, 2 (slightly negative) at 75%, 3 (neutral) at 100%, 4 (slightly positive) at 82%, and 5 (very positive) at 100%. This indicates that GPT-4 tended to classify “slightly negative” posts as neutral. Upon further examination, we found that these posts often exhibited sentiments close to neutral, causing the model to lean towards neutral classifications. Despite this, GPT-4’s overall recall reached 92%, demonstrating well performance in sentiment analysis accuracy.

D. Details About Descriptive Analysis

This section presents the descriptive statistical analysis of community engagement by category, as detailed in Table VII.

APPENDIX E DETAILS ABOUT CASE STUDY

In this section, we provide details about our case study, including examples of three key sources of information related to Web3 audits, systematically outlined in Table VIII, along with a comprehensive overview of the 20 selected audit firms, including their homepages and web addresses, as detailed in Table IX. Additionally, we present the results of our review of the information disclosure practices on the homepages of 21 audit firms, as discussed in Section E-C. These details aim to enhance the transparency of our study and provide readers with a clear understanding of the foundational elements upon which our research is built.

A. Information About Selected Audit Firms Websites

B. Sample List for Sources of Information

C. Web3 Auditing Website Review and Result

1) Firm Introduction: How does the audit firm introduce its services?

- Through a brief description (e.g. “We specialize in providing top-notch smart contract auditing services”) - 15 (71%)
- With a mission statement or slogan (e.g. “Securing the decentralized world”) - 18 (86%)
- Showcasing their team members and their expertise - 2 (10%)
- Other - 1 (5%)

How does the auditing firm introduce its firm advantages?

- Client base - 15 (71%)
- Experience - 13 (62%)
- Unique selling points or competitive advantages - 12 (57%)

How does the audit firm present its credit?

- Industry partnerships (e.g. “We collaborate with major blockchain platforms”) - 11 (52%)
- Notable clients (e.g. “Our clients include Aave, Compound, and MakerDAO”) - 18 (86%)

- Successful audits (e.g. “We have conducted 100% successful audits with no exploited cases”) - 4 (19%)
- Awards or recognitions (e.g. “Winner of the 2022 Blockchain Security Excellence Award”) - 5 (24%)
- Testimonials or endorsements from clients or industry experts - 9 (43%)
- Other - 3 (14%)

2) Presentation of Service: How does the auditing firm describe its service process?

- Flowchart or infographic - 9 (43%)
- Step-by-step description - 4 (19%)
- No information - 8 (38%)

What is the scope of the auditing firm’s services?

- Security consulting - 11 (52%)
- Penetration testing - 10 (48%)
- Bug bounty programs - 8 (38%)

Is the distinction between various services provided by Web3 audit firms clearly defined?

- Unclear, difficult to understand - 10 (48%)
- Not very clear, vague - 4 (19%)
- Yes, clear and understandable - 7 (33%)

Does the auditing firm provide post-audit support?

- Yes, they offer post-audit support - 2 (10%)
- No, they do not provide post-audit support - 18 (86%)

Are the audit reports publicly available or accessible upon request?

- Publicly available on the company’s website - 16 (76%)
- Accessible upon request with client consent - 8 (38%)
- Not available for public access - 2 (10%)

Does the audit firm have a standardized audit report format or do they customize reports?

- Standardized format for all audit reports - 20 (95%)
- Customized reports based on client requirements - 0 (0%)
- Combination of standardized and customized reports - 1 (5%)

How does the auditing firm present its pricing structure?

- Customized quotes depending on specific project requirements - 4 (19%)
- Tiered pricing with different service levels or features - 1 (5%)
- No information - 16 (76%)

Does the auditing firm have a strong track record of successful audits without exploited cases?

- Yes, they have a proven history of successful audits - 1 (5%)
- No, they have a history of exploited cases despite their audits - 1 (5%)
- No information - 19 (90%)

TABLE VI: Sample for categorization Reddit discussions

Main Category	Subcategories	Sample
1: Direct Discussion of Web3 Auditing	1.1: How Audits are Conducted	Was the Whisper protocol part of the security audit?
	1.2: Audit Firms	What Is [Audit Firm]?
	1.3: Impact of Audits	So Your Project is Audited... Cool, Cool, Cool
2: Discussion of Application Audit Dynamics	2.1: Upcoming Audits	[Application]’s Direction Says a Full Audit is Coming Soon
	2.2: Ongoing Audits	EtherCamps decentralized startup team public code audit by Zeppelin
	2.3: Halted Audits	[Application] Proof-of-Reserves Auditor [Audit Firm] All Work for Crypto Clients
	2.4: Successful Audits	[Audit Firm] Clears [Application] from Bugs
	2.5: Failed Audits	Security Audit Firm Discovers Critical Vulnerability in [Application] Smart Contract System
	2.6: Post-Audit Attacks	Another [Audit Firm] Certified Project Rugs as 3M USD Disappears From [Application] DeFi Exchange
3: Discussion of Web3 Security (Related to Audit Firms)	3.1: Security Practices of Audit Firms	[Audit Firm] Debunks Rumours of 532M USD Smart Contract Hack – crypto.news
	3.2: Security Knowledge of Audit Firms	Analysis of the 600 USD million theft

TABLE VII: Descriptive Statistical Analysis of Community Engagement by Category. This table aggregates statistical measures across various subcategories, providing absolute values and percentages for posts, comments, upvotes, and involved users. Additionally, it presents average values for comments and upvotes. Each category is defined by distinct themes as referenced in Table VI, where a full description of each category can be found. These statistics objectively reflect the level of community interaction within each category, offering insights into how different topics garner varying degrees of engagement from the community

Category	Subcategory	Post		Involved Users		Comments			Upvote		
		Amount	Percentage	Amount	Percentage	Amount	Percentage	Average	Amount	Percentage	Average
1	1.1	139	15.4%	632	19.4%	1005	4.3%	7.2	6254	10.3%	21.0
	1.2	113	12.5%	373	11.4%	1996	8.6%	17.7	3689	6.1%	49.6
	1.3	68	7.5%	104	3.2%	2425	10.4%	35.7	8678	14.4%	36.5
2	2.1	147	16.2%	298	9.1%	2076	8.9%	14.1	11727	19.4%	42.5
	2.2	60	6.6%	126	3.9%	2040	8.8%	34.0	14568	24.1%	61.5
	2.3	34	3.8%	69	2.1%	3533	15.2%	103.9	910	1.5%	255.2
	2.4	174	19.2%	388	11.9%	3081	13.2%	17.7	2919	4.8%	67.4
	2.5	23	2.5%	40	1.2%	3917	16.8%	170.3	5604	9.3%	633.4
	2.6	17	1.9%	35	1.1%	473	2.0%	27.8	2480	4.1%	53.5
3	3.1	61	6.7%	498	15.3%	705	3.0%	11.6	1445	2.4%	23.7
	3.2	69	7.6%	701	21.5%	2055	8.8%	29.8	2186	3.6%	31.7
Overall		905		3264		23306		25.8	60460		66.8

3) **Additional Security Information: How security-related knowledge or information does the auditing firm share on its homepage?**

- Blog articles - 15 (71%)
- Security guides or checklists - 14 (67%)
- Whitepapers or reports - 7 (33%)

Does the auditing firm provide any additional resources or tools for developers or projects?

- Educational materials - 14 (67%)
- Security frameworks or templates - 9 (43%)
- Open-source tools or libraries - 8 (38%)

Does the audit firm have a strong presence on social media or community platforms?

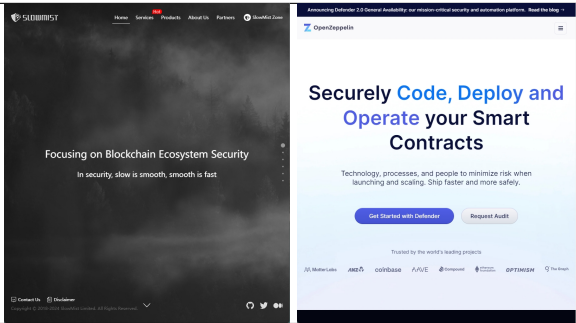
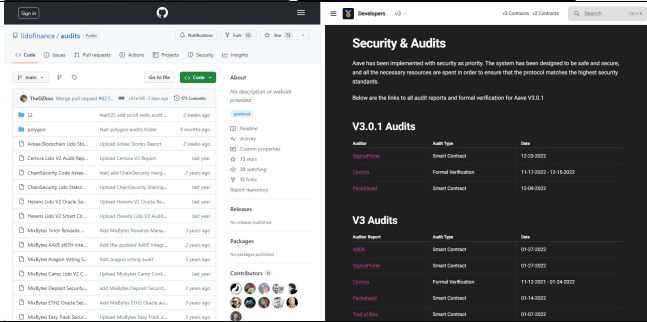
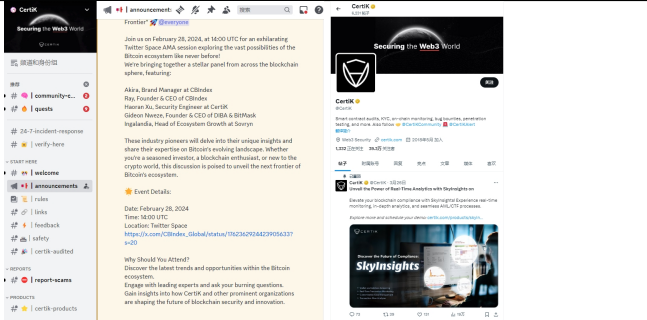
- Yes, they have an active presence on popular platforms (e.g. Twitter, LinkedIn, Telegram, Discord) - 14 (67%)
- They have some presence, but it’s not very active or engaging - 5 (24%)
- No, they have little to no presence on social media or community platforms - 2 (10%)

1) How security-related knowledge or information does the audit firm share on its homepage? (Mul-

iple choice)

- a) Blog articles (e.g., informative articles on smart contract security, industry trends, and best practices)
 - b) Webinars or workshops (e.g., online events discussing security topics and challenges)
 - c) Whitepapers or reports (e.g., in-depth research and analysis of security topics)
 - d) Security guides or checklists (e.g., resources to help projects improve their security)
 - e) Podcasts or interviews (e.g., conversations with industry experts and thought leaders)
 - f) Other
- 2) Does the audit firm have a strong presence on social media or community platforms? (Multiple choice)
- a) Yes, they have an active presence on popular platforms (e.g., Twitter, LinkedIn, Telegram, Discord)
 - b) They have some presence, but it’s not very active or engaging.
 - c) No, they have little to no presence on social

TABLE VIII: The three types of Information Sources and sample captures with related links.

Source of Information	Sample of Selected Information Source	Link of Source Sample
Official Websites of Audit Firms		https://www.slowmist.com/ https://www.openzeppelin.com/
Audit-Related Webpages from Web3 Applications		https://github.com/lidofinance/audits https://docs.aave.com/developers/deployed-contracts/security-and-audits
Social Media Interactions		https://twitter.com/CertiK https://discord.com/channels/97234186-9864435803/972352337479884840

- media or community platforms.
- d) Other
- 3) Does the audit firm provide any additional resources or tools for developers or applications? (Multiple choice)
 - a) Open-source tools or libraries (e.g., tools for smart contract analysis or vulnerability detection)
 - b) Educational materials (e.g., tutorials, guides, or courses)
 - c) Security frameworks or templates (e.g., resources to help projects implement security best practices)
 - d) Other

1. How do you get audit-related information?
 - a. Where do you get that information?
 - i. What channels or sources did you use to gather different information and knowledge about audits?
 - ii. Do you try to find it on other channels? Like application websites/social media, audit firm's websites or social media? If yes/no, why?
 - b. Why do you get that audit-related information?

Questions about philosophy

1. How do you perceive the information you get? Why?
 - a. Is it sufficient/reliable/useful?
 - b. What risks can be mitigated by audit results?
 - c. Will there still be significant security risks to an audited application?
 - d. Do you think the audited vulnerabilities will be fixed?
 - e. Do you think it is important for an application to be audited?
2. To what extent are you able to understand the

APPENDIX F
INTERVIEW PROTOCOL

A. Perception of Audit Information

Audit Information

Questions about action

1. Can you tell me about your relevant experience with Web3 auditing?

Questions about knowledge

TABLE IX: Overview of Audit Firms and Their Web3 Security Engagements. The table enumerates auditing firms alongside their web addresses and details the top 15 Web3 applications they have audited, with respective market values and application websites.

Auditing Firm	Firm Website	Audited Application	Market Value	Application Website
certora	https://www.certora.com/	Lido	\$14.727b	https://lido.fi/
		AAVE	\$4.856b	https://aave.com/
certik	https://www.certik.com/	JustLend	\$4.64b	https://portal.justlend.org/
		Uniswap	\$3.22b	https://uniswap.org/
		stUSDT	\$1.784b	https://twitter.com/stusdt
		JustStables	\$1.522b	https://just.network/
peckshield	https://peckshield.com/	AAVE	\$4.856b	https://aave.com/
		MakerDAO	\$4.519b	https://makerdao.com/en/
		Instadapp	\$1.908b	https://instadapp.io/
		Convex Finance	\$1.867b	https://www.convexfinance.com/
quantstamp	https://quantstamp.com/	PancakeSwap	\$1.365b	https://pancakeswap.finance/
		Lido	\$14.727b	https://lido.fi/
ABDK	https://abdk.consulting/	Curve Finance	\$2.105b	https://curve.fi/
		AAVE	\$4.856b	https://aave.com/
blocksec	https://blocksec.com/	PancakeSwap	\$1.365b	https://pancakeswap.finance/
chainsecurity	https://chainsecurity.com/	Lido	\$14.727b	https://lido.fi/
		Uniswap	\$3.22b	https://uniswap.org/
		Summer.fi	\$2.239b	https://app-summer.fi/
consensus diligence	https://consensus.io/diligence/	Uniswap	\$3.22b	https://uniswap.org/
		Rocket Pool	\$1.795b	https://rocketpool.net/
defisafety	https://www.defisafety.com/	Uniswap	\$3.22b	https://uniswap.org/
Hexens	https://hexens.io/	Lido	\$14.727b	https://lido.fi/
mixbytes	https://mixbytes.io/	Lido	\$14.727b	https://lido.fi/
		Convex Finance	\$1.867b	https://www.convexfinance.com/
OpenZeppelin	https://www.openzeppelin.com/	AAVE	\$4.856b	https://aave.com/
		Coinbase Wrapped Staked ETH	\$2.254b	https://www.coinbase.com/
		Compound Finance	\$1.944b	https://compound.finance/
OtterSec	https://osec.io/	PancakeSwap	\$1.365b	https://pancakeswap.finance/
Oxorio	https://oxor.io/	Lido	\$14.727b	https://lido.fi/
runtime verification	https://runtimeverification.com/	MakerDAO	\$4.519b	https://makerdao.com/en/
sigmaprime	https://sigmaprime.io/	Lido	\$14.727b	https://lido.fi/
		AAVE	\$4.856b	https://aave.com/
		Rocket Pool	\$1.795b	https://rocketpool.net/
slowmist	https://www.slowmist.com/	PancakeSwap	\$1.365b	https://pancakeswap.finance/
	https://cn.slowmist.com/			
statemind	https://statemind.io/	Lido	\$14.727b	https://lido.fi/
trail of bits	https://www.trailofbits.com/	AAVE	\$4.856b	https://aave.com/
		MakerDAO	\$4.519b	https://makerdao.com/en/
		Curve Finance	\$2.105b	https://curve.fi/
		Compound Finance	\$1.944b	https://compound.finance/
		Rocket Pool	\$1.795b	https://rocketpool.net/
Zellic	https://www.zellic.io/	PancakeSwap	\$1.365b	https://pancakeswap.finance/

content of audit information?

- a. How about the auditing report?
- b. How about the other information related to auditing?
3. How long do you typically invest in audit information?
4. What aspects of audit information do you pay attention to?
5. Do you know:
 - a. How many applications have been audited in the market?
 - b. Have all well-known applications been audited? Why?

B. Perception of Auditing

Auditing Mechanism

Questions about action and knowledge

1. What do you know about the process looks like?
2. How do you know about the process?
3. What aspect do you think is audited, and how do you know that?
4. How long will the audit last, and how many labor resources will the audit take? How do you know that?
5. What is the cost? How do you know?

Audit Firm

Questions about action

1. Can you name a few audit firms?

Questions about knowledge

1. How do you remember it?
 - a. If yes, to what extent do you know these audit firms? Can you tell me some information? And how did you know?
 - b. Have you ever followed the audit firm's social media accounts or official website?
 - c. Among those, which one do you think is famous or reputable, and why do you think it is famous or reputable?
 - i. If not, why can't you remember the name of the audit firm?

Questions about philosophy

1. What do you think of these audit firms?
 - a. Do you think the audit firms are reliable, and how can you judge how reliable they are? Will you read different audit firm reports for the same application?
 - b. How do you think audit firms are responsible for the audit results?
 - c. Are you concerned about the independence of the audit firm?
 - d. Before the audit begins, how do you think the audit firms and the applications will confirm the cooperation?
 - e. During the audit, what are the responsibilities of the audit firms, and what needs to be done?
 - f. After the audit is completed, do you feel that the audit firm has any responsibilities to bear?
 - g. Assuming that something goes wrong with an audited application, what should the related audit firm do?

Auditor

Questions about action

1. Have you ever noticed the auditor in charge of the audit, and how do you find out?
 - a. If yes, would you do an auditor's background check?
 - b. If not, why didn't you pay attention to the auditor's information?

Questions about knowledge

1. How do auditors work together on the same application?

Questions about philosophy

1. How do you perceive the auditor?
 - a. Do you think there are any competencies that auditors need? Why do you think so?
 - b. How much responsibility do you think auditors have for the results of the audit?
 - c. What do you think is the responsibility of auditors?

Audit Method

Questions about action

1. Do you know about automated audit tools/manual auditing?

Questions about knowledge

1. How did you come to know about them?
 - a. As for automated audit tools:
 - i. Who do you think is using audit tools?
 - ii. How do you think audit tools implement audits?
 - iii. Have you ever tried to conduct a personal audit using an audit tool?
 1. Under what circumstances would you go about using it?
 2. What is the reason you didn't use it?
 - b. As for manual auditing:
 - i. What do you think about manual auditing?
 - ii. Who is responsible for manual audits?

Questions about philosophy

1. Do you find the audit tool reliable?
2. Do you think the introduction of artificial intelligence in auditing will replace manual auditing?
3. Do you find the results of the manual audit reliable?
4. What do you think would be the difference between a manual audit and a tool audit? Why?

Audited Application

Questions about action

1. What do you think the applications should do when applying for an audit?

Questions about knowledge

1. How do you know?
 - a. Is there anything need to prepare?
 - b. Will members of the application be involved in the audit process?
 - c. Do you think the application will modify the code after the audit is over?
 - d. Do you think the application will need to do anything after the audit, and how do you know?
 - e. Is the audit content of the audit report consistent with the final contract? Who is responsible for supervising it?

Questions about philosophy

1. How would you define or assess an audit firm's independence when it comes to its relationship with the applications? And why is this important in your opinion?
2. Are you worried that the involvement of the application will affect the confidence in the audit results?
3. How would you judge that an audit firm regularly serves the same application?

General Perception

Questions about philosophy

1. Do you find it difficult to understand the audit process?
 - a. In terms of technical knowledge (Unable to understand technical terms, unable to understand the core of the problem, unable to understand threat rating)

- b. In terms of reporting (Poor legibility, lack of charts, color highlights, too long)
 - c. In terms of Audit firms (The auditors, audit time, and audit methods are not clear, the audit standards are not uniform, and the judgment of vulnerabilities and the classification of risk levels are inconsistent)
2. Do you think audits are a necessity?
 3. Do you think audits have limitations?
 - a. Are there any specific areas where you believe audits may fall short or have certain limitations? Do limitations affect your decision-making and attitude towards audit?

6. I just asked you about auditors, audit firms, audit methods, and audit reports. Which of these factors do you think you would pay more attention to?
7. Are there any ways you think can avoid or reduce the limitations of Web3 audit?
 - a. Unified auditing standards? such as web2 audit firms
 - b. Industry Autonomous Committees of Industry Organizations?
 - c. External government regulation institutions?
 - d. Audit firm's compensation services or insurance services?

C. Impact on User Behavior

Questions about action

1. Could you share your previous experiences with application audits?
 - a. How the results of those audits may have influenced your subsequent evaluation of the applications?
 - b. How the results of those audits may have influenced your subsequent interactions with the applications?

Questions about knowledge

1. How much attention do you personally place on audits?
 - a. How much time do you spend reading the contents of the audit report?

Questions about philosophy

1. How well will you understand the information?
 - a. To what extent do you think it is necessary to understand audit information?
 - b. Will you make any efforts to improve your understanding?
 1. How to do?
 2. Why?
 - c. How do you care about whether there is an audit and the results of the audit?
 - i. Are you involved in unaudited applications? Why
2. Does whether the application has been audited affect your decision-making?
 - a. How will the audit results of the applications affect your decision-making? Why?
3. Does the diversity of application-related audit reports (not only one firm's audit) affect your decision-making?
4. What does auditing mean to you?
 - a. Do you see it as something that involves responsibility, a specific process, and produces certain outcomes?
5. Have you considered urging an application to conduct an audit?

D. Demographic Information

1. What is your age, city, and occupation?
2. How are your computer skills/technical knowledge of blockchain systems?
3. How long have you been involved in Web3 or using Web3 applications?
4. What Web3 applications have you used?