Changing Trust: Auditing's Impact on Web3 Security from a User Perspective

Anonymous Author(s)

***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.**

1. Introduction

As the decentralized online ecosystem built on blockchain technology, Web3 has revolutionized the digital landscape, boasting a Total Value Locked (TVL) that surpassed 45 billion USD in 2023 [19]. This burgeoning ecosystem has attracted millions of users enthused by the promise of transparency, efficiency, and trustless transactions. However, Web3 is not without its vulnerabilities; by 2023, security breaches had resulted in a staggering 77 billion USD in cumulative financial losses [79].

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. Presently, more than half of all Web3 applications have undergone audits, covering over 80% of the market's total TVL [79]. Further augmenting this trend, audit firms have proactively interacted with the public through expert lectures, incident analysis, and knowledge-sharing initiatives [11], [22], [52].

While security auditing is not a novel concept, the practice of openly disclosing audit-related information 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 [8], [37]. This practice aligns with the risk perception model [15] (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, user's security perceptions, and security practices.

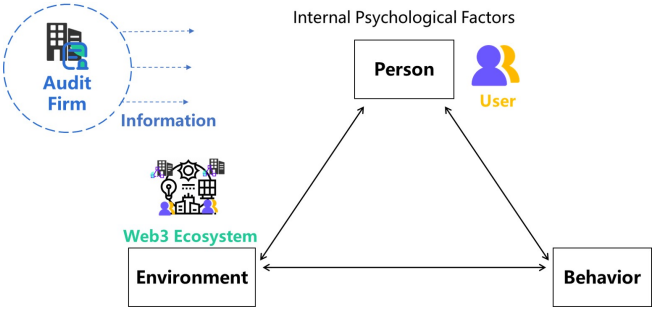

Figure 1: The risk perception model within the Web3 ecosystem [15]. This model demonstrates the mechanism by which a person evaluates input information from the external environment, which, in turn, determines personal behavioral responses. Web3 auditing functions as a novel source of external input information.

RQ1: How do users perceive information accessed from Web3 auditing?

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

RQ3: How does auditing impact Web3 users' behavior?

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 Web3 users ($n = 20$), and an analysis of Reddit discussions, encompassing 905 posts with 5827 comments.

We initially focused on examining three critical dimensions of audit information: accessibility, sufficiency, and comprehensibility. Our findings indicate that users depend on a single source for locating audit information that they find accessible. However, they highlighted concerns regarding the limited depth and breadth of the content. Additionally, the technical complexity of the information often resulted in restricted comprehension. We subsequently delved into user perspectives on the role of Web3 auditing within the ecosystem, 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 behavior within the ecosystem based on the previously discussed perceptions. We discovered that auditing has a limited role in various stages of users' security decision-making processes. Furthermore, our research highlights the significant role of Web3 auditing in fostering security awareness among users within the ecosystem.

This study pioneers 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 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 online environments.

2. Related Work

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

2.1. 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 [29], [71]. 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 delve into stakeholders' trust in blockchains. Sas et al. examine the key characteristics of Bitcoin and their impact on trust among blockchain users, addressing the risks associated with dishonest traders and proposing mitigation strategies [62]. Ooi et al. identify factors like technical safeguards, transaction procedures, and security statements that influence users' perceived trust in blockchain systems [55]. Additionally, previous researchers have identified trust-related risks related to miners, stemming from issues like centralization and dishonest administrators in collaborative mining efforts [38].

Research on user perceptions related to applications within blockchain systems primarily focuses on cryptocurrency and related tools. In cryptocurrencies, Abramova et al. reveal the foremost self-reported motivation among cryptocurrency users [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 [30]. Additionally, some scholars explore cryptocurrency tools. Voskobojnikov et al. identify the potential monetary loss resulting from poor interface design from a user experience perspective [70]. Mai et al. reveal that current cryptocurrency tools struggle to mitigate threats stemming from users' misconceptions [49]. Wang et al. [71] investigate user perception of a specific attack model in decentralized finance applications. 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 representing around 80% of TVL [79]. Drawing from the risk perception model [15], perception serves as the mechanism through which individuals assess their external environment, ultimately shaping their behavioral responses. Consequently, external information delivered through Web3 auditing can profoundly influence users' perceptions within the ecosystem. However, our current understanding lacks insights into how users perceive Web3 auditing.

To address this critical gap, our research questions aim to investigate user perception in two distinct phases. The first phase examines users' perceptions of this external information, formulating RQ1:

RQ1: How do users perceive information accessed from Web3 auditing?

Subsequently, we explore users' perspectives on the role of auditing within the Web3 ecosystem, resulting in the formulation of RQ2:

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

2.2. Auditing for Web-related Applications

Before the emergence of Web3, the general cyberspace was predominantly known as Web2, signifying the second generation of the World Wide Web. This era was characterized by a centralized network ecosystem [73]. In Web2, auditing entails an objective evaluation process to ensure compliance, accuracy, reliability, and security across various domains. This process incorporates diverse practices, including algorithm, security, IT audits, and code reviews [14], [23]. It plays a significant role in enhancing decision-making and operational efficiency [43], finding widespread application. For instance, Google conducts annual standardized security audits with results publicly disclosed online, while details remain nonpublic [1]. Previous research on Web2 auditing can be categorized into three main areas: optimization of auditing methods [51], auditing of online activities [44], and the perception of auditing stakeholders [21].

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

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 [50], [57]. Other scholars have also investigated audit frameworks designed for agile software development [31]. Chen et al. have contributed by offering alternative quantitative tools to gather audit evidence [12], enhancing the quality of collaborative code reviews [34]. Meanwhile, Jang et al. have proposed a rule-based auditing system, extending the scope of vulnerability detection across various contexts [75] Previous research has also placed significant emphasis on user-driven algorithms as a means to enhance audit efficiency [20].

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 assessments of content regulation policies, particularly concerning misinformation [35], [36]. Other scholars have undertaken audits to examine the fairness of advertising policies on social platforms [44] and election outcomes in evidence-based elections [76]. 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 [46], [53], [69].

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 [6]. Furthermore, research has examined how developers assess the quality of code reviews, suggesting that such reviews may offer limited assistance to developers [41], [42]. Kononenko et al. have explored the impact of code reviews on developers and proposed that these reviews can enhance security awareness [58]. Conversely, other studies have highlighted the inhibiting effect of non-professional reviewers on the code review process [17].

In summary, previous research has not explored the influence of audit information on users of audited applications, primarily because Web2 security audits are not publicly disclosed. While disclosing security audit information to users is commonplace in the Web3 ecosystem, it represents a novel concept in Web2. Therefore, investigating its impact on users is beneficial for the development of the Web3 ecosystem and may offer valuable insights and inspiration to enhance the security awareness of Web2 users. Therefore, to address this gap, we introduce RQ3:

RQ3: How does Web3 auditing impact Web3 users' behavior?

3. Study Method

This section outlines the research methods employed in our study. Initially, we conducted a case study to understand the interactions within the Web3 ecosystem between Web3 applications, users, and auditing firms. Based on the findings from the case study, semi-structured interviews (with a total of $n = 20$ participants) were carried out. Finally, we performed an analysis of data from Reddit to gain a comprehensive understanding of users' perceptions of Web3 auditing and its impact on user behavior.

Our study's dataset, encompassing the interview protocol, audit firm homepage information survey, details of selected audit firms, and information on selected subreddits, is now published and accessible. This public online dataset can be found at https://github.com/Anonymousauthor2024/Supplementary-documentation/tree/main.

3.1. Case Study on Web3 Auditing

To gain insights into the interactions between Web3 auditing and users within the Web3 ecosystem, our study explores audit-related information from two perspectives: the applications and the audit firms. This dual approach enables a comprehensive analysis of how users interact with information related to audits. A sample list of our sources of information can be seen in our public online dataset.

3.1.1. Information from Web3 Applicaitons. Our observational study focuses on all Web3 applications with more than 1 billion USD TVL due to their leading position [19]. This includes fifteen Web3 applications, all of which have undergone auditing. We identified pages on the Web3 applications' websites disclosing information about their audits. These pages convey essential information that Web3 applications aim to communicate to users, including their auditing results and practical implementation details within the application. This involves aspects such as the frequency of audits, the overall count of audits conducted, and related details. Subsequently, we employed a hybrid coding method, combining deductive and inductive thematic analysis, to dissect the data collected from these information pages [26].

3.1.2. Information from Web3 Audit Firms. We selected audit firms associated with the above-chosen applications, encompassing 20 firms. More details about these audit firms can be found in our public online dataset. Our focus was on webpages from the official homepages of these Web3 audit firms, which provide information about their auditing practices, and on related social media channels as cited by the audited firms' official websites, such as "Discord" and "X". These audit firms frequently share their activities with Web3 participants, offering valuable insights into their interaction behaviors within the Web3 ecosystem.

We also employed a hybrid coding method for this part of our research. Additionally, we surveyed the information disclosure practices of these 20 audit firms to comprehend their information disclosure practices, thereby supporting the analysis for RQ1: How do users perceive information accessed from Web3 auditing?

Drawing on previous work [33], we designed a survey focusing on three main aspects: 1) firm introduction, 2) presentation of services, and 3) additional security information. Two researchers independently completed this survey, with

the final results derived from a consensus discussion. Given that English and Chinese-speaking users are the primary demographics in the Web3 space [32], we examined both the English and Chinese versions of all audit firms' websites. Notably, one firm exhibited discrepancies in information disclosure between its English and Chinese pages. Consequently, a total of 21 audit firm websites were included in our survey. More detailed information about this survey is provided in our public online dataset.

3.1.3. Framework of Web3 auditing interactions. Drawing on our observations and relevant literature [25], 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.

As inspired by risk perception model [15], we developed a framework for Web3 auditing encompassing stakeholders, information exchange, and interactive behaviors (Figure 2). Web3 auditing impacts the ecosystem by providing audit services to applications. Moreover, audit-related information and other security information disseminated by audit firms reach users, affecting their awareness and, consequently, behaviors such as decision-making. These user behaviors then exert influence on the Web3 ecosystem. This framework guided our subsequent analysis of interviews and social media discussions.

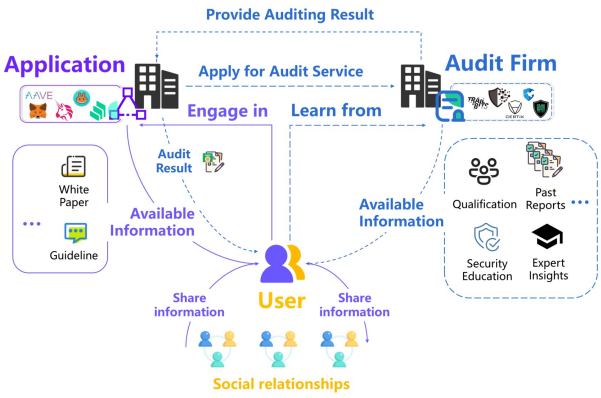

Figure 2: The framework for Web3 auditing encompasses stakeholders, information exchange, and interactive behaviors. Web3 audit firms engage with users in the Web3 ecosystem by providing auditing services to applications and disseminating security information. These information revelation changes can potentially influence users' security awareness and decision-making processes [37].

3.2. Interview Study

To better understand Web3 users' perception of auditing, we recruited Web3 users for semi-structured interviews. This study was approved by the Institutional Review Board (IRB) at [hide for the review], where the study was conducted.

3.2.1. Participant Recruitment. We published our recruitment materials on Twitter, Discord, and Telegram. Additionally, we utilized the personal contacts of the research team to recruit participants. To be eligible for the study, participants needed to 1) know about Web3 auditing, 2) possess experience with Web3 applications, and 3) be over 18 years old.

From July 2022 to August 2023, we interviewed 20 Web3 users via Zoom and Tencent Meeting. Each interview lasted 45-60 minutes, and each participant received a $20 honorarium for their time. We informed users about our study procedures and data protection policy.

Three participants identified as female, while the other seventeen identified as male. Fourteen participants had more than two years of experience with Web3, while six had less than three years of experience. The average experience duration was 3.75 years. The details of participants' demographics can be found in Appendix A.

3.2.2. Interview Protocol. Our interviews began by confirming participant eligibility with questions such as, "Can you explain what Web3 auditing is?" to ensure that their understanding of Web3 auditing was consistent with our research scope. We then explored their awareness and sources of Web3 auditing information by asking, "How did you get Web3 auditing information?" and inquired about their evaluation of its usability. The interviews also delved into their comprehension of the auditing mechanism and initial encounters with the concept, using prompts like, "What do you think audit actually does in the audit cases you have noticed?". Additionally, we examined their views on the role of Web3 auditing within the ecosystem. The final part focused on how auditing impacts their decision-making in the Web3 environment, with questions such as, "How the results of audits may have influenced your subsequent actions or views on the applications?". The detailed interview protocol is available in our public online dataset.

3.2.3. Interview Data Analysis. All interviews were audio-recorded with the informed consent of the participants and subsequently transcribed by the interviewers for analysis. We employed thematic analysis to systematically interpret the data [9]. Initially, two researchers independently analyzed a representative 20% subset of the total transcripts. During this phase, they inductively identified emerging themes, focusing on three primary dimensions: user perceptions of Web3 auditing information, their understanding of the role of Web3 auditing, and the perceived impact of Web3 auditing on user security behaviors.

Following the preliminary discussion and the creation of an initial codebook, both researchers independently coded the remaining 80% of the transcripts. To ensure analytical consistency and integrity, they reconvened at intervals, specifically after each 20% increment of the data had been coded. During these review sessions, the researchers compared their independent sets of codes, debated any discrepancies, and synthesized their interpretations. A code was only added to the shared codebook after a mutual agreement

was reached between the two researchers. This iterative process ensured not only the rigor of the data coding but also the validity of the research findings.

To validate the comprehensiveness of our data, a saturation analysis was conducted. The emerging themes was cataloged in the order of appearance from participants P1 through P20. The absence of novel themes in the later interviews corroborated our assertion that we had achieved theoretical saturation.

3.3. Empirical Analysis on Reddit

Reddit serves as our primary data source for examining community online discussions about Web3 auditing, owing to its role as a major hub for Web3-related discussions [40]. Reddit boasts a diverse user base representing various geographic locations and cultural backgrounds, enabling us to gather more general insights for our research [65]. Detailed information about our methodology and the steps involved is provided in Appendix B.

3.3.1. Data Collection. In the ranking of the top 1000 subreddits provided by Reddit, we identified subreddits related to Web3 under the "crypto" label. This label predominantly includes 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) [7]. Each post underwent a manual review to ensure the presence of the specified keywords. For detailed subreddit information, please check our public online dataset.

3.3.2. Data Preprocessing. Our data preprocessing comprised two main parts. Firstly, we removed sensitive information, such as personally identifiable details, from the data locally before uploading it to GPT-4. This was achieved with the assistance of the open-source toolkit Microsoft Presidio, which can anonymize sensitive data with an accuracy rate of up to 99% [28].

Secondly, we excluded posts unrelated to Web3 auditing using GPT-4 [56]. We employed GPT-4 to identify posts relevant to this domain. The process entailed feeding the model with the definition of Web3 auditing and 100 posts that were explicitly marked for relevance. GPT-4 evaluated each post's title and content, and its decisions were manually verified by two independent researchers, ensuring consistency and accuracy. Any disagreements between the researchers were resolved through discussion to achieve consensus. This procedure resulted in selecting 905 posts to form our preprocessed dataset. These posts span from 2013 to 2023, involving 689 different users.

3.3.3. Content Analysis and Categorization. In this research phase, our primary focus was on categorizing the content of posts related to Web3 auditing. Initially, researchers established classification criteria based on a thematic analysis of 100 randomly selected posts. These criteria were then employed to guide GPT-4 in the classification process, mirroring the data processing approach used in Section 3.3.2. Subsequently, rigorous manual validation was conducted to ensure accuracy.

Our analysis resulted in categorizing posts into three main categories and various subcategories, with examples provided in Appendix B.3.

Category 1 focused on discussions related to the auditing activities of Web3 applications, primarily addressing specific applications' auditing processes. This aided in understanding how Web3 auditing's association with applications influenced user behavior. 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 2 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 3 focused on discussions about the dissemination of security information by audit firms, including posts about activities beyond their core auditing services. This category helped establish a comprehensive understanding of the effects of Web3 auditing on users. It was classified into two subcategories: promoting security practices and disseminating security knowledge.

Additionally, for each post, we selected the top 25% of comments ($n = 5827$) based on the number of upvotes. We adopted this approach of focusing on the most upvoted comments to facilitate a deeper understanding of user reactions.

3.3.4. Sentiment Analysis. In our study, we conducted sentiment analysis on the collected post content using GPT-4 to gain valuable insights into community perspectives [72]. Drawing from the Likert 5-point scale methodology [2], we calculated a sentiment score for each post, ranging from 1 (very negative) to 5 (very positive), with 3 representing a neutral sentiment. We randomly sampled 30% of the data for review and found an accuracy rate exceeding 90% to verify the accuracy of GPT-4's sentiment analysis. The mean sentiment score was 3.31, with a standard deviation of 1.16. More information can be found in Appendix B.4.

3.4. Limitation

Our study has inherent limitations that need consideration when interpreting the findings. Firstly, our interview sample size was limited, making it challenging to generalize to the broader Web3 community. To address this, we supplemented our data with Reddit discussions from over 600 unique users. While informative, this data may not fully represent the wider community due to unknown Reddit user demographics. Nevertheless, it provides general insights into user perspectives, laying the groundwork for future extensive studies.

Another constraint is the experience level of our participants; most had more than a year's worth of involvement with Web3. While this offers valuable insights into the views of more seasoned users, it leaves the perceptions of newcomers underrepresented. The focus on experienced users was largely driven by the emergent and specialized nature of Web3 auditing, a topic that many novices were found to be unfamiliar with during our initial research.

Gender imbalance further limits the generalizability of our findings. The overwhelming majority of interviewees were male, a demographic skew that mirrors existing gender imbalances in the broader Web3 ecosystems, as supported by previous literature [4].

Additionally, our data has an unavoidable cultural and geographic bias, with most participants based in Asia. This bias raises the possibility of regional cultural influences on our findings. To address this, we included Reddit data, which has a globally dispersed user base, primarily using English for discussions, offering a more balanced cross-cultural perspective.

Despite these limitations, our work is a foundation for understanding user perceptions and security concerns related to Web3 auditing. It acts as a stepping stone for more expansive future studies to provide a more comprehensive understanding of these emerging trends and challenges.

4. Perceptions of Information Obtained from Web3 Auditing

This section delves into users' perceptions of the information they receive regarding Web3 auditing. Our analysis is structured around three dimensions [63]: the accessibility of information, the sufficiency of information, and the comprehensibility of information.

4.1. Singularity in Locating Audit Information

Our research uncovers a notable trend: users predominantly turn to an application's official website as their primary source for audit information. The homepage often serves as the initial touchpoint where users expect to find clear and prominent mentions of audit activities. For instance, interviewee P4 consistently visits the application's homepage to ascertain whether the applications have presented any mention of auditing information. *"I usually start by checking their website first. Their documentation often indicates if the application has undergone any audits. From there, I proceed to examine the audit report to ensure the legitimacy of the conducted audit"* (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).

4.2. Gaps in Audit Information Disclosure

Our findings underscore user concerns regarding the perceived insufficiency of available audit information. This is manifested in both the lack of depth in direct audit information and the insufficient comprehensiveness of indirect audit information, leading to a limited understanding of the auditing mechanisms among users.

Twenty percent of our interviewees pointed out the lack of depth of direct audit information, which primarily includes explicit findings, recommendations, and vulnerabilities outlined in audit reports. The audit reports were frequently described as "hurried", "formulaic", and "repetitive", failing to provide specific and meaningful insights. *"I feel many of them are overly simplified. Many audits nowadays adopt a mass-production method to endorse applications and gather funds. 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 6.

A significant gap was also observed in the comprehensiveness of indirect audit information, which covers supplementary materials like the audit firm's reputation and the historical accuracy of their audits. Our review of audit firm homepages (Section 3.1.2) revealed that 38% of firms do not provide detailed descriptions of their audit service processes and a concerning 80% inadequately disclose their auditors' professional credentials, with 62% omitting auditor information entirely. Reddit users echoed these concerns, expressing dissatisfaction with audit information's depth and comprehensiveness. *"I'm trying to dig deeper into this field, but it's hard to find thorough information"* (Post82).

The lack of comprehensiveness in audit-related information hinders users from understanding auditing accurately. This often results in misunderstandings about the scope of audit services. 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 financial auditing... all transactions should undergo auditing... perhaps like financial auditing in Web3"* (P19).

4.3. Challenges in Understanding 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.

Our 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. These 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 requiring 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 auditing information. *"I don't have the capability or time to check their audits formally... The main issue lies in the verifiability of these audits efforts"* (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. The gap between the security scores and the real-world implications has been mentioned by both our interviewees and Reddit discussions. For instance, in a Reddit thread titled *"[Audit Firm] lowers the security score of [Application] from 90 to 38 after it gets rugged"* (Post90), the users' perplexity about the scoring system was palpable. *"Lowering the security score of an application from 90 to 38 after it gets rugged is akin to rating a malfunctioning parachute two out of ten for safety - it should be zero"* (Post90: Comment2), highlighting the challenges users face in interpreting these numerical evaluations.

5. Perceptions of the Role of Web3 Auditing

In this section, we explore users' perspectives on the role of auditing in the Web3 landscape. Our investigation centers on two key aspects: the firms responsible for conducting these audits and the overall influence of auditing on the security and credibility of the Web3 ecosystem.

5.1. 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.

5.1.1. 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.

Interviewees perceive that a firm with a strong reputation is more likely to commit substantial resources, including labor costs, to conduct thorough and detailed audits. Furthermore, users believe any inaccuracies in auditing could substantially damage the audit firm's reputation, incurring a higher opportunity cost. *"I think people will eventually recognize that an audit from a more reputable firm is worthwhile over time"* (P4). Nevertheless, our study reveals considerable ambiguity in how users assess the reputation of audit firms. While respondents readily associated high-quality audits with "well-known" firms, eighty percent of 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 60% of interviewees believe that companies capable of providing audit services to well-known applications naturally possess a good reputation, a minority 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) are already security, 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 indicates a significant gap in the ecosystem. There appears to be a lack of established, objective criteria for evaluating audit firms, leaving users to rely on somewhat nebulous indicators. This absence of clear evaluation metrics makes it difficult for users to make informed decisions about the security of Web3 applications.

5.1.2. Lack of Impartiality and Independence in Audit Firms.

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

Variability in the quality of audits has resulted in user skepticism regarding the impartiality of audit firms. This industry disarray is evident both in Reddit discussions and in

our interviews. Our respondents have reported encounters or awareness of substandard audits, contributing to a selective attention bias [48]. These experiences lead users to perceive the industry as inherently flawed or even corrupt. For instance, one interviewee shared, *"My friend once asked an audit firm to conduct an audit, and the audit report he got was completely wrong. 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, a Reddit user expressed criticism towards irresponsible auditing practices, *"A 3-page document with under 100 words of text, concerning an 'Integer Division Error Accumulation'... there is ZERO evidence of a comprehensive security audit, which is shameful and sickening"* (Post65).

Doubts about the independence of audit firms, given their role as paid service providers, were evident among our interviewees. A quarter of the respondents 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, *"Bribe 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.

5.1.3. Catalysts for Security Education. Despite the prevalent skepticism regarding the integrity and expertise of Web3 audit firms, there is a notable acknowledgment among users of 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 3.1.3, 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 survey, referenced in Section 3.1.2, indicates that 66.67% of these firms provide educational documents on their websites, such as the checklist of smart contract vulnerabilities. This initiative appears to have enhanced user awareness regarding security risks in the Web3 ecosystem, as evidenced by 35% of our 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 garner notable user engagement. Specifically, Subcategory 3.2, which is dedicated to the dissemination of security knowledge such as advice on avoiding risky operations and analyses of recent vulnerabilities, sees an average of 30 responses per post. This is 15% higher than the overall average response rate.

5.2. Perception of Impact of Auditing on Web3 Security

Based on our analysis of online discussions, we find that users hold neutral perceptions of the impact of auditing on Web3 security. The average sentiment score of the discussions regarding the impact of auditing (subcategory 2.3) is 2.89, with a standard deviation of 1.05 (cf. Appendix C Table 4). Discussions with negative sentiments elicit higher average comments and upvotes compared to those with positive sentiments. We further summarize the perceived impacts of auditing on Web3 security from three perspectives: the questioning attitude and the affirmative attitude towards the effectiveness of auditing in enhancing security, and an affirmative attitude recognizing auditing as proof of an application's efforts in security.

5.2.1. 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 users' understanding of the nature of security work and the influence of instances where audited applications have still succumbed to attacks.

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 an outcome-based evaluation, particularly focusing on applications occurring after audits. In our thematic analysis of selected Reddit posts with negative sentiment scores discussing the impact of audits (Subcategory 2.3), we observed that a substantial proportion (50%) highlighted real-world instances where applications, despite undergoing audits, were compromised in cyberattacks. An example of such discussion is illustrated in the post, *"Are DeFi audits meaningless? Two DeFi protocols audited by*

[Audit Firm] were exploited on the same day, totaling 14 million USD" (Post189).

The questioning of audit effectiveness is evident in discussions about audited applications later attacked, as seen in subcategory 1.6. The Post82 described a "rug pull" incident in an audited application, highlighting the disconnect between auditing and the application developers' intentions. Comments varied, with some users questioning the relevance of the audit firm in assessing business intentions *"I'm not sure what the point of mentioning [Audit Firm] here..."* (Post82: Comment6) and others critiquing the audit firm's performance *"Terrible audit company, but have a great name for some reason."* (Post82: Comment7).

5.2.2. Auditing as a Catalyst for Enhanced Security. While a substantial segment of users harbors skepticism about the effectiveness of audits, there is also a notable proportion that views auditing positively, primarily considering it as a mechanism to bolster the security of Web3 applications. This positive perception originates from three primary considerations.

Firstly, proponents from our interviewees of auditing 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 of applications. *"External auditing is imperceptible. Each individual's technical proficiency covers different layers; thus, the involvement of others is crucial in identifying more issues"* (P5). Furthermore, users intuitively sense that supplementary auditing can diminish the probability of hacker attacks, underscoring their belief that audited applications are more secure than unaudited ones. *"It's just like a student submitting his assignment; having a teacher's check undoubtedly improves the submission process compared to self-review"* (P11).

Secondly, users contend that audited applications mitigate or prevent losses resulting from attacks. Some interviewees sensed that supplementary auditing could diminish the probability of hacker attacks, underscoring their belief 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 or application teams avoid attacks and minimize potential damage"* (P16).

5.2.3. Auditing as a Proof to Security Actions. There is an 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 view the willingness to incur this expense as evidence of the application's commitment to security. Even those who express skepticism about the effectiveness of audits acknowledge that the act of undergoing an audit represents an application's dedication to at least the basic security measures. They emphasize that while an audit doesn't guarantee foolproof security, it indicates a sincere commitment. *"Contract security itself cannot achieve 100% protection...Then I think the biggest significance of audit is to give ordinary users confidence, proving that the application is serious about doing things, and he is at least willing to spend money to audit...Comparing to the kind of firm that is not even willing to spend money to disclose the source code for audit"* (P14).

However, our research indicates a notable lack of awareness among users about the actual financial costs of audits. We found that 90% of interviewees could not accurately estimate these costs. This lack of awareness is likely attributable to the limited transparency in pricing information 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 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.

6. Perceived Impact of Web3 Auditing on Users

This section aims to unpack how auditing influences users' behaviors when interacting with the Web3 Ecosystem. We mainly focus on two aspects related to this theme, i.e., the impact on decision-making processes, and the security awareness when using Web3 applications.

6.1. Users' Decision-Making Process

To better understand how users' perceptions of Web3 auditing affect their decision-making, we examine the process with two stages: pre-decision and in-the-moment.

6.1.1. Pre-decision: Limited Engagement.
Our research uncovers patterns in how users engage with audit information before making decisions, especially concerning the time and attention they invest. Two primary dimensions of user behavior emerged: the brevity of time allocation and the superficial focus on audit completion.

When it comes to time commitment, it is noteworthy that 20% of the interviewees reported not spending any time looking for audit results. Among the remaining 80% who do invest time in this endeavor, a significant 75%

indicated that they allocate only a nominal amount of time to audit-related activities. In terms of specific durations, users typically spend a matter of minutes, rarely exceeding ten, on understanding audit reports or findings. *"I just browsed it briefly and didn't look at it seriously"* (P8).

As for the focus of their attention, users are principally concerned with the mere existence of an audit rather than the details in the audit report. The scrutiny applied to the audit report, if any, tends to be cursory. Intricacies such as the tools and methodologies employed by auditors, as well as the credibility of the audit firm, are generally overlooked or ignored by 90% 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).

These user behaviors can be traced back to the perceptions of audit information elaborated upon in Section 4. The complexities of audit documents serve as a deterrent for users who may otherwise want to explore the information in depth. Concurrently, a prevailing lack of trust in the audit process and its outcomes further dissuades users from making an effort to parse through intricate audit details, rendering the information largely ineffectual in influencing pre-decision behavior.

6.1.2. In-the-Moment: Symmetrical Influence. Audit results play a significant role in shaping decision-making moments within Web3 interactions, yet the influence varies depending on the nature of the outcome. Positive audit outcomes do indeed support user engagement and investment, but the impact of negative results in diminishing user involvement appears to be limited.

Negative audit outcomes tend to result in unfavorable expectations from users towards applications. Posts in Subcategory 1.5, primarily focused on negative audit results, demonstrate an average sentiment score of 1.61 with a standard deviation of 0.94. This score reflects a generally negative user attitude towards such audit outcomes. High-upvote comments within this subcategory also consistently mirror this sentiment. *"[Application] is a fraud and not fully backed"* (Post81: Comment 4).

Interestingly, some users expressed indifference to such unfavorable news about negative audit results. This indifference may be attributed to their risk-seeking behavior, operating under the belief that high returns are accompanied by high risks, which in turn influences their decision-making. *"Personally I don't care, worst case scenario I lose the $100 I put in a few weeks ago. Best case, it ends up skyrocketing"* (Post5: Comment9).

6.2. Security Awareness on Web3 Operations

Auditing in the Web3 environment extends beyond merely verifying the security of smart contracts and decentralized applications. It also plays a crucial role in elevating users' overall awareness and understanding of security issues, as depicted in Figure 1. Our findings indicate that information provided by audit firms significantly contributes to enhancing user security awareness and promoting secure behaviors, particularly true for negative information.

Thirty-five percent of the interviewees identified audit reports as educational assets. These reports offer insights into modern 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 resource for me. I see it as an educational tool. I often delve into the smart contract to identify modified lines and even try to comprehend why these changes were made from a security perspective"* (P8).

In addition to formal reports, many audit firms proactively disseminate security-related information across various platforms, further contributing to heightened user awareness. Particularly, users mentioned their engagement with audit firms' social media channels to keep up-to-date with the latest security. These platforms offer not just updates but also analyses of security incidents, explanations of risks in layman's terms, and guidelines on conducting rudimentary audits and code analyses. *"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).

7. Discussion

To contextualize and elucidate the evolving role of auditing within the Web3 environment, this discussion section is organized into three main parts: the rationale for the ascent of auditing within Web3, the challenges this auditing paradigm faces, and the design implications that can guide its future trajectory.

7.1. 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.

7.1.1. Decentralization's Role in Security Awareness. The decentralization Web3 ecosystem, founded on blockchain technology, alters the dynamics of user interaction and security awareness [62]. While centralization in Web2 provided user convenience, it also came at the cost of individual autonomy [74]. Decentralization empowers users with greater control over their digital assets [67], 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 [60]. Secondly, auditing quality becomes crucial as it acts as a form of "market regulation", guiding user decisions and

potentially exposing them to risks if executed irresponsibly, as mentioned in Section 6.1.2. Both aspects underline the necessity for rigorous and transparent auditing in the Web3 ecosystem.

7.1.2. Lack of Regulation and the Demand for Auditing. Web3's minimal regulatory framework [16] stands in stark contrast to the regulatory landscape in Web2. While this allows greater freedom and innovation [45], it also engenders a slew of trust issues [64] and a lack of standardized security protocols [68]. 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 5.1.2, the absence of universally accepted auditing standards could muddy the waters, eroding user trust and potentially jeopardizing the integrity of the entire ecosystem.

7.1.3. Technical Complexity and the Role of Auditing in Usability. Blockchain technology, while revolutionary, introduces a new layer of complexity, often making it difficult for average users to navigate Web3 safely [18]. Auditing serves to bridge this gap in two distinct ways. Firstly, it translates the complex technicalities of smart contracts into more accessible yet detailed auditing results, aiding users in making informed decisions [54]. However, as discussed in Section 6, the current level of readability in these audit reports could still be improved. Secondly, as shown in Section 5.1.3, audit firms take on an educational role [22], further contributing to improving users' understanding of the risks and rewards associated with various Web3 applications [5]. This dual role of auditing as a technical reviewer and educational facilitator makes it a cornerstone in enhancing Web3's usability and overall security.

7.2. Challenges in Web3 Auditing

This subsection elucidates three significant challenges confronting Web3 auditing: information presentation, lack of industry standardization, and community trust issues. These challenges affect the readability of audit reports, erode consumer confidence, and raise questions about the efficacy of auditing in a decentralized environment.

7.2.1. 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 4.3. Therefore, the challenge lies in satisfying the needs of different users simultaneously:

For technically savvy users, detailed audit information, such as audit reports, serves as valuable educational resources and decision-making aids, as discussed in Section 5.1.3. However, as discussed in Section 4.3, users have expressed concerns about the content's repetitive and templated nature, which hinders their ability to locate valuable information. Furthermore, when users attempt to verify the authenticity of audit reports by directly inspecting the source code, they encounter difficulties due to the lack of clear descriptions of error codes, impeding their efficiency in identifying specific lines of code associated with errors.

For ordinary users, while current audit reports incorporate user-friendly elements such as comprehensive security scores and summaries to facilitate user understanding, readability challenges persist, as elucidated in Section 4.3. This issue is closely linked to audit firms' inadequacy of information disclosure. Due to such limited disclosure, as identified in Section 4.2, it becomes impractical to expect users to comprehend auditing mechanisms and related practices fully. Users often possess a limited understanding of auditing processes. This gap in knowledge hinders them from appreciating objective metrics, like the number of vulnerabilities reported, thus making it challenging to gauge an application's security based solely on the content of audit reports, as mentioned in Section 6.1.1.

These challenges have the potential to impede users' understanding and may even discourage them from further engagement [13]. Therefore, optimizing audit information's technical complexity and readability is a critical concern.

7.2.2. Lack of Industry Standards: Impact on Consumer Confidence.

As highlighted in Section 7.1.2, 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 consumer trust and the reputation of audit firms with a strong track record.

Moreover, as highlighted in Section 5.1.2, audit firms currently do not enjoy a particularly strong reputation, with no firm having established a reputable and trustworthy image among users. Allowing the industry to develop without appropriate standards may expose it to the risk of unscrupulous firms exploiting the absence of regulations for short-term gains, potentially exacerbating the issue. This could set the stage for a concerning scenario where low-quality audits become increasingly prevalent.

7.2.3. Community Challenges: Navigating Trustlessness in Web3. The decentralized nature of Web3 has implications for trust models, moving away from centralized authorities to cryptographic and network-based trust [24]. However, this paradigm shift raises societal challenges.

Technical incomprehension makes users trustless in the auditing mechanism, as discussed in Section 4.3. This is

because learning the professional knowledge of blockchain comes with high time costs, serving as a user entry barrier [39]. Without a comprehensive understanding of the technology, placing full trust in blockchain remains difficult [77], [78]. This challenge extends to auditing, which involves explaining security information by presenting a detailed technical analysis.

Furthermore, as discussed in Section 4.2, 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 5.2.3. 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 [27], which in turn exacerbates the instability of users' trust in the auditing process, as found in Section 5.2.1.

The risk of dishonest traders has prevented users from establishing trust in audit firms. This relates to another prevalent fraud issue within the Web3 ecosystem [62]. Malicious Web3 applications frequently employ deceptive strategies to attract users into investing their assets, subsequently executing rug pulls [3]. The decentralized and pseudonymous nature of blockchain complicates holding these fraudsters accountable, thereby burdening users with the full extent of their losses [62]. Consequently, users approach Web3 auditing skeptically after experiencing such widespread fraud, as noted in Section 5.1.2. Their untrust regarding the independence and impartiality of audit firms is consequently from this environment.

Hence, this shapes users' attitudes towards the diversity of auditing, as explored in Section 5.2. On the one hand, users acknowledge that auditing, when conducted with fairness and independence, can provide substantial assistance, benefiting both individual users and the overall ecosystem. However, on the other hand, users maintain skepticism about the possibility of upholding impartiality and independence within this decentralized Web3 environment. As revealed in Section 6.1, this skepticism constrains users' engagement and support for auditing initiatives.

7.3. 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 three critical perspectives: the user, the audit firm, and the broader Web2 Ecosystem. The insights provided herein aim to inform future Web3 auditing practices.

7.3.1. For Users: Leveraging Communities for Technical Understanding. As previously highlighted in Section 7.2.3, the lack of technical understanding among users hinders their ability to trust auditing, and the inadequate disclosure of information leads users to depend on free expert advice from personal connections. Online communities can fill this expert role. These communities usually manifest in two forms: officially sanctioned by audit firms and those spontaneously organized by users, such as Decentralized Autonomous Organizations (DAOs).

Audit firms have already tried to bridge this gap by fostering dedicated communities on platforms like Discord [11]. Within these digital spaces, specialized personnel are available to clarify users' audit-related queries. Moreover, educational activities like community knowledge competitions are frequently organized, enriching users' understanding and rewarding engagement. This approach facilitates users in directly accessing expert knowledge to address their inquiries, which expands their information access channel. Meanwhile, for audit firms, it serves as a means to enhance users' security awareness and showcase their professionalism, thereby bolstering their reputation within the Web3 ecosystem.

DAOs may also serve as potent platforms for information dissemination [61]. 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 4.2.

7.3.2. For Audit Firms: Information Balance and Trust-building Measures. To address the challenges outlined in Section 7.2, audit firms may focus on optimizing the user experience in two primary ways: improving the presentation of audit outcomes 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 provision of absolute security information in audit reports should be inherently interpretable to cater to users, most of whom lack specialized auditing knowledge. Enhancing interpretability could involve incorporating comparative data and industry-specific benchmarks [47], offering users immediate and understandable context without the need to decipher complex audit terminologies. Additionally, it is vital for audit firms to judiciously handle the presentation of absolute numbers, ensuring they align with users' expectations. Overreliance on high scores without proper justification risks eroding the credibility of the audit firm, as mentioned in Section 7.2.1.

For expert users capable of interpreting audit information, enhancing usability is key to fostering trust, as noted in Section 7.2.3. Interactive web platforms, as opposed to static PDF reports, offer a promising solution by facilitating direct engagement with the audit data [70]. Features like side-by-side comparison tools and clickable code snippets enable a deeper, contextual understanding of the findings. Such platforms also serve as valuable tools for audit firms

to understand novice users' challenges in interpreting audit information. By tracking user interactions and integrating feedback mechanisms, audit firms can gather real-time insights, refining their reports and communication strategies to enhance overall user comprehension and trust, thereby 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 regarding dishonest traders in Section 5.1.1. We explore three potential solutions for audit firms to enhance their reputation, which include improving information transparency, strengthening community engagement, and fostering collaboration with the community and industry.

To bolster their reputation and user trust, audit firms need to significantly improve information transparency, as highlighted in Section 7.2.1. 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 5.1.2. A timely upload of such data to a blockchain platform also can further assure users of the firm's impartiality, utilizing the blockchain's inherent resistance to data manipulation.

Enhancing community engagement can significantly improve an audit firm's reputation. As mentioned in Section 5.1.3, firms can build user trust by disseminating security education through social media. Given the trust issues associated with the Web3 ecosystem, the DAOs can be formed for added accountability. 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 7.2.2. The current lack of clear standards undermines user trust. Audit firms can benefit by actively participating in dialogues to establish uniform practices, thereby expediting improvements through shared insights on security and detection technology. Once standardized criteria are established, educating users on these benchmarks will foster both trust and the industry's overall standing.

7.3.3. For the Web2 Ecosystem: Learning from Web3. The security of network environments remains a crucial concern [10], [66], and the Web2 ecosystem can gain valuable insights by examining the practices of Web3 auditing, understanding both its value and the challenges it presents.

Our research underscores the value of third-party security audit disclosures for users. These disclosures not only offer users essential insights for security assessment and decision-making but also serve as a valuable resource for security education, as discussed in Section 6. Therefore, security audit firms and applications within the Web2 ecosystem should consider adopting similar information disclosure practices. This could involve sharing detailed information about their security protocols and making external audit reports publicly accessible.

Taking this proactive approach would not only boost user confidence in Web2 applications but also elevate the visibility and significance of Web2 audit firms within the ecosystem. It would also serve as a means to disseminate valuable security knowledge, promote user security awareness, and adopt more robust security practices throughout the Web2 ecosystem.

Our research has also highlighted the challenges associated with third-party audit information disclosure, as observed in the context of Web3 auditing.

We have offered design implications aimed at improving the usability and credibility of information transmission. Significantly, these insights apply not only to the Web3 domain but also offer valuable insights for Web2 auditors. These include strategies like integrating comparative factors and employing interactive web pages to bolster user comprehension. Enhancing transparency and fostering effective communication of security information within the Web2 ecosystem, inspired by Web3 practices and our research findings, can significantly contribute to elevating security standards and bolstering user trust in the digital landscape, thus creating a more secure online environment [20].

8. Conclusion

This paper presents a pioneering paradigm shift in the understanding of auditing, traditionally seen as a technical exercise focused on developers. We introduce a novel perspective by examining auditing as a form of security information for end-users. Our research offers key insights into how users perceive and are impacted by these security practices, thus shedding light on their behavior. This user-centric viewpoint not only enriches the discourse on Web3 auditing but also has broader implications for auditing in general.

References

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

[2] I Elaine Allen and Christopher A Seaman. Likert scales and data analyses. *Quality progress*, 40(7):64–65, 2007.

[3] Nataliya Amosova, Anna Yu Kosobutskaya, and Olga Rudakova. Risks of unregulated use of blockchain technology in the financial markets. In *4th International Conference on Economics, Management, Law and Education (EMLE 2018)*, pages 9–13. Atlantis Press, 2018.

[4] Jessica Apotheker. Web3 already has a gender diversity problem, February 2023.

[5] Bakri Awaji, Ellis Solaiman, and Lindsay Marshall. Investigating the requirements for building a blockchain-based achievement record system. In *Proceedings of the 5th International Conference on Information and Education Innovations*, pages 56–60, 2020.

[6] Alberto Bacchelli and Christian Bird. Expectations, outcomes, and challenges of modern code review. In *2013 35th International Conference on Software Engineering (ICSE)*, pages 712–721. IEEE, 2013.

[7] Jason Baumgartner, Savvas Zannettou, Brian Keegan, Megan Squire, and Jeremy Blackburn. The pushshift reddit dataset. In *Proceedings of the international AAAI conference on web and social media*, volume 14, pages 830–839, 2020.

[8] Dirk Bergemann and Stephen Morris. Information design, bayesian persuasion, and bayes correlated equilibrium. *American Economic Review*, 106(5):586–591, 2016.

[9] Richard E Boyatzis. *Transforming qualitative information: Thematic analysis and code development*. sage, 1998.

[10] Juan Carlos Roca, Juan José García, and Juan José de la Vega. The importance of perceived trust, security and privacy in online trading systems. *Information Management & Computer Security*, 17(2):96–113, 2009.

[11] Certik. Watchlists, September 2023.

[12] Wei Chen, Wally J Smieliauskas, and Gerhard Trippen. An audit evidence gathering model in online auditing environments. In *2011 IEEE International Conference on Systems, Man, and Cybernetics*, pages 1448–1452. IEEE, 2011.

[13] Chun-Wei Chiang, Eber Betanzos, and Saiph Savage. Exploring blockchain for trustful collaborations between immigrants and governments. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–6, 2018.

[14] David C Chou, David C Yen, and Jim Q Chen. Analysis of the total quality management-based software auditing. *Total Quality Management*, 9(7):611–618, 1998.

[15] Dominic Cooper. Psychology, risk and safety. *Professional Safety*, 48(11):39–46, 2003.

[16] Shaen Corbet, Charles Larkin, Brian Lucey, Andrew Meegan, and Larisa Yarovaya. Cryptocurrency reaction to fomc announcements: Evidence of heterogeneity based on blockchain stack position. *Journal of Financial Stability*, 46:100706, 2020.

[17] Jacek Czerwonka, Michaela Greiler, and Jack 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*, volume 2, pages 27–28. IEEE, 2015.

[18] Joyce Oliveira Déo da Silva and Daiane Rodrigues dos Santos. Study of blockchain application in the logistics industry. *Theoretical Economics Letters*, 12(2):321–342, 2022.

[19] Defillama - defi dashboard, 2023. https://defillama.com/(date of access: June 6, 2023).

[20] Wesley Hanwen Deng, Boyuan Guo, Alicia Devrio, Hong Shen, Motahhare Eslami, and Kenneth 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*, pages 1–18, 2023.

[21] Giuseppe D'Onza, Rita Lamboglia, and Roberto Verona. Do it audits satisfy senior manager expectations? a qualitative study based on italian banks. *Managerial Auditing Journal*, 30(4/5):413–434, 2015.

[22] Dron-Hacken. Excited to greet everyone for our usual friday community talk!, June 2023.

[23] Ann C Dzuranin and Irina Mălăescu. The current state and future direction of it audit: Challenges and opportunities. *Journal of Information Systems*, 30(1):7–20, 2016.

[24] Chris Elsden, Arthi Manohar, Jo Briggs, Mike Harding, Chris Speed, and John Vines. Making sense of blockchain applications: A typology for hci. In *Proceedings of the 2018 chi conference on human factors in computing systems*, pages 1–14, 2018.

[25] Ding Feng, Rupert Hitsch, Kaihua Qin, Arthur Gervais, Roger Wattenhofer, Yaxing Yao, and Ye Wang. Defi auditing: Mechanisms, effectiveness, and user perceptions. *Cryptology ePrint Archive*, 2023.

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

[27] Emilio Ferrara and Zeyao Yang. Measuring emotional contagion in social media. *PloS one*, 10(11):e0142390, 2015.

[28] Alexander Friebely. *Analyzing the Efficacy of Microsoft Presidio in Identifying Social Security Numbers in Unstructured Text*. PhD thesis, Utica University, 2022.

[29] Michael Fröhlich, Felix Gutjahr, and Florian Alt. Don't lose your coin! investigating security practices of cryptocurrency users. In *Proceedings of the 2020 ACM Designing Interactive Systems Conference*, pages 1751–1763, 2020.

[30] Michael Fröhlich, Maurizio Raphael Wagenhaus, Albrecht Schmidt, and Florian Alt. Don't stop me now! exploring challenges of first-time cryptocurrency users. In *Designing Interactive Systems Conference 2021*, pages 138–148, 2021.

[31] César García, Alejandro Guerrero, Joshua Zeitsoff, Srujay Korlakunta, Pablo Fernandez, Armando Fox, and Antonio 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)*, pages 283–288. IEEE, 2021.

[32] Leading countries in web 3.0 development, 2023. LeadingCountriesInWeb3.0Development.

[33] Joseph P. Hasley and Dawn G. Gregg. An exploratory study of website information content. *Journal of theoretical and applied electronic commerce research*, 5(3), 2010.

[34] Austin Z Henley, Kıvanç Muçlu, Maria Christakis, Scott D Fleming, and Christian 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*, pages 1–13, 2018.

[35] Prerna Juneja, Md Momen Bhuiyan, and Tanushree 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*, pages 1–22, 2023.

[36] Prerna Juneja and Tanushree Mitra. Auditing e-commerce platforms for algorithmically curated vaccine misinformation. In *Proceedings of the 2021 chi conference on human factors in computing systems*, pages 1–27, 2021.

[37] Emir Kamenica. Bayesian persuasion and information design. *Annual Review of Economics*, 11:249–272, 2019.

[38] Irni Eliana Khairuddin and Corina 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*, pages 1–13, 2019.

[39] Megan Knittel, Shelby Pitts, and Rick Wash. " the most trustworthy coin" how ideological tensions drive trust in bitcoin. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–23, 2019.

[40] Megan L. Knittel and Rick Wash. How "true bitcoiners" work on reddit to maintain bitcoin. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI EA '19, page 1–6, New York, NY, USA, 2019. Association for Computing Machinery.

[41] Oleksii Kononenko, Olga Baysal, and Michael W Godfrey. Code review quality: How developers see it. In *Proceedings of the 38th international conference on software engineering*, pages 1028–1038, 2016.

[42] Oleksii Kononenko, Olga Baysal, Latifa Guerrouj, Yaxin Cao, and Michael W Godfrey. Investigating code review quality: Do people and participation matter? In *2015 IEEE international conference on software maintenance and evolution (ICSME)*, pages 111–120. IEEE, 2015.

[43] Adriano Koshiyama, Emre Kazim, and Philip Treleaven. Algorithm auditing: Managing the legal, ethical, and technological risks of artificial intelligence, machine learning, and associated algorithms. *Computer*, 55(4):40–50, 2022.

[44] Victor Le Pochat, Laura Edelson, Tom Van Goethem, Wouter Joosen, Damon McCoy, and Tobias Lauinger. An audit of facebook's political ad policy enforcement. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 607–624, 2022.

[45] Jei Young Lee. A decentralized token economy: How blockchain and cryptocurrency can revolutionize business. *Business Horizons*, 62(6):773–784, 2019.

[46] Chang Liu, Krerkkiat Chusap, Zhongen Li, Zhaojie Chen, Dylan Rogers, and Fanghao Song. Continuous collateral privacy risk auditing of evolving autonomous driving software. In *2019 IEEE International Conference on Software Maintenance and Evolution (ICSME)*, pages 363–363. IEEE, 2019.

[47] Walid Maalej, Rebecca Tiarks, Tobias Roehm, and Rainer Koschke. On the comprehension of program comprehension. *ACM Transactions on Software Engineering and Methodology (TOSEM)*, 23(4):1–37, 2014.

[48] Colin MacLeod, Elizabeth Rutherford, Lyn Campbell, Greg Ebsworthy, and Lin Holker. Selective attention and emotional vulnerability: assessing the causal basis of their association through the experimental manipulation of attentional bias. *Journal of abnormal psychology*, 111(1):107, 2002.

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

[50] Suryadipta Majumdar, Gagandeep Singh Chawla, Amir Alimohammadifar, Taous Madi, Yosr Jarraya, Makan Pourzandi, Lingyu Wang, and Mourad Debbabi. Prosas: Proactive security auditing system for clouds. *IEEE Transactions on Dependable and Secure Computing*, 19(4):2517–2534, 2021.

[51] Suryadipta Majumdar, Taous Madi, Yushun Wang, Yosr Jarraya, Makan Pourzandi, Lingyu Wang, and Mourad Debbabi. User-level runtime security auditing for the cloud. *IEEE Transactions on Information Forensics and Security*, 13(5):1185–1199, 2017.

[52] Slow Mist. Update:the @magnatefi has rug pulled $6.4m. their website is offline and the telegram group has been deleted., September 2023.

[53] Michael Mitchell, Guanyu Tian, and Zhi Wang. Systematic audit of third-party android phones. In *Proceedings of the 4th ACM Conference on Data and Application Security and Privacy*, pages 175–186, 2014.

[54] Keshab Nath, Sourish Dhar, and Subhash 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)*, pages 86–89. IEEE, 2014.

[55] Say Keat Ooi, Chai Aun Ooi, Jasmine AL Yeap, and Tok Hao Goh. Embracing bitcoin: users' perceived security and trust. *Quality & Quantity*, 55:1219–1237, 2021.

[56] OpenAi. Introducing chatgpt.

[57] Minjie Ou, Liming Wang, and Hao Xun. Deaps: Deep learning-based user-level proactive security auditing for clouds. In *2019 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 2019.

[58] Andreas Poller, Laura Kocksch, Katharina Kinder-Kurlanda, and Felix Anand 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*, pages 1288–1294, 2016.

[59] Microsoft Presidio. Presidio: Data protection and de-identification sdk.

[60] Michael JW Rennock, Alan Cohn, and Jared R Butcher. Blockchain technology and regulatory investigations. *Practical Law Litigation*, 1:35–44, 2018.

[61] Carlos Santana and Laura Albareda. Blockchain and the emergence of decentralized autonomous organizations (daos): An integrative model and research agenda. *Technological Forecasting and Social Change*, 182:121806, 2022.

[62] Corina Sas and Irni Eliana 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*, pages 6499–6510, 2017.

[63] Andrew Sears, Julie A Jacko, and Michael 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*, pages 353–354. 1997.

[64] Vasundhara Sharma, Anitesh Barua, and Andrew B Whinston. In cryptocurrencies we trust: An empirical analysis of cryptocurrency demand and price. *Available at SSRN 3381067*, 2019.

[65] Philipp Singer, Fabian Flöck, Clemens Meinhart, Elias Zeitfogel, and Markus 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*, pages 517–522, 2014.

[66] Mikko T Siponen. A conceptual foundation for organizational information security awareness. *Information management & computer security*, 8(1):31–41, 2000.

[67] Don Tapscott and Alex Tapscott. *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. Penguin, 2016.

[68] Elissar Toufaily. An integrative model of trust toward crypto-tokens applications: A customer perspective approach. *Digital Business*, 2(2):100041, 2022.

[69] Rahmadi Trimananda, Hieu Le, Hao Cui, Janice Tran Ho, Anastasia Shuba, and Athina Markopoulou. {OVRseen}: Auditing network traffic and privacy policies in oculus {VR}. In *31st USENIX security symposium (USENIX security 22)*, pages 3789–3806, 2022.

[70] Artemij Voskobojnikov, Oliver Wiese, Masoud Mehrabi Koushki, Volker Roth, and Konstantin 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*, pages 1–14, 2021.

[71] Ye Wang, Patrick Zuest, Yaxing Yao, Zhicong Lu, and Roger 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*, pages 1–15, 2022.

[72] Yucheng Wang and Zhicong 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*, pages 1–17, 2023.

[73] Wikipedia. Web 2.0. https://en.wikipedia.org/wiki/Web_2.0.

[74] Aaron Wright and Primavera De Filippi. Decentralized blockchain technology and the rise of lex cryptographia. *Available at SSRN 2580664*, 2015.

[75] Nong Ye, Xiangyang Li, Qiang Chen, Syed Masum Emran, and Mingming Xu. Probabilistic techniques for intrusion detection based on computer audit data. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, 31(4):266–274, 2001.

[76] Filip Zagórski, Grant McClearn, Sarah Morin, Neal McBurnett, and Poorvi L Vora. Minerva–an efficient {Risk-Limiting} ballot polling audit. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 3059–3076, 2021.

[77] Javad Zarrin, Hao Wen Phang, Lakshmi Babu Saheer, and Bahram Zarrin. Blockchain for decentralization of internet: prospects, trends, and challenges. *Cluster Computing*, 24(4):2841–2866, 2021.

[78] Liudmila Zavolokina, Noah Zani, and Gerhard 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*, pages 269–283. Springer, 2019.

[79] Liyi Zhou, Xihan Xiong, Jens Ernstberger, Stefanos Chaliasos, Zhipeng Wang, Ye Wang, Kaihua Qin, Roger Wattenhofer, Dawn Song, and Arthur Gervais. Sok: Decentralized finance (defi) attacks. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 2444–2461. IEEE, 2023.

Appendix A. Summary demographics of the interviewees

TABLE 1: 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

Appendix B. Details in Empirical Analysis on Reddit

B.1. Data Collection

In a ranking of Reddit communities by member count, arranged from the highest to the lowest, each community is labeled based on its primary focus. Notably, communities under the "crypto" label predominantly consist of applications grounded in blockchain technology, reflecting the essence of Web3 communities. Consequently, we identified 10 Web3 communities within the top 1000 Reddit communities under the "crypto" label. These are: r/CryptoCurrency, r/ethereum, r/bitcoin, r/dogecoin, r/NFT, r/CryptoMarkets, r/CryptoTechnology, r/BitcoinBeginners, r/btc, and r/cardano.

To construct our dataset, we initially extracted all posts from the targeted subreddits using relevant keywords. The extraction process was facilitated by the Python Pushshift.io API Wrapper (PSAW) [7]. Our selection of keywords, included terms such as "audit", "auditing", "auditor", "code review", and the names of the 20 audit firms. These firms are noted in Section 3.1.2 as the auditors for Web3 applications with a total value locked (TVL) exceeding 1 billion USD. Following the data extraction, we conducted a manual review of the collected posts to ensure each contained at least one of the specified keywords.

B.2. Data Preprocessing

Our data preprocessing consists of two parts: firstly, the removal of sensitive information from the data before uploading it to GPT-4 [56]; secondly, the exclusion of posts unrelated to Web3 auditing using GPT-4.

Sensitive information removal. Prior to uploading our scraped data to GPT-4, we first performed local anonymization of sensitive information within the dataset. For this task, we utilized the open-source toolkit Microsoft Presidio, specifically designed to ensure sensitive data identification and anonymization [59]. Previous studies have validated its effectiveness, with an accuracy rate of up to 99% in identifying Personally Identifiable Information (PII) [28].

Exclusion of posts irrelevant to web3 auditing with GPT-4. Despite the initial data filtering, certain content unrelated to Web3 auditing, such as topics on centralized financial auditing, remained in the dataset. As outlined in Section 3.1.3, Web3 auditing is conducted by specialized security firms to assess and enhance the security of smart contracts in Web3 applications. We incorporated this definition into GPT-4, alongside 100 randomly sampled Reddit posts, each marked for their relevance to Web3 auditing, with reasons for their classification. This approach assisted GPT-4 in accurately understanding and categorizing the posts. Following the removal of sensitive information, the dataset was processed through GPT-4, where the model evaluated each post's title and content for relevance, providing justifications for its decisions. Posts identified as relevant

by GPT-4 subsequently underwent manual verification by two independent researchers. Discrepancies between the researchers' views and GPT-4's assessment were discussed until consensus was achieved.

This procedure resulted in the selection of 905 posts to form our preprocessed dataset. These posts span a period from 2013 to 2023, involving 689 different users. The analysis of the collected posts revealed that the average length of post titles is 80 characters, while the average length of the main body of the posts extends to 855 characters.

B.3. Data Categorization

In the subsequent phase of our study, we focused on analyzing and categorizing the posts, employing GPT-4 to assist in the standard classification process. The methodology began with two researchers developing classification criteria, starting with 100 posts randomly selected from the dataset previously filtered for relevance to Web3 in the earlier phase. These posts were independently evaluated for their relevance to Web3 auditing. Following this, the researchers met frequently to refine the criteria based on a comparison of the selected posts, aiming to resolve discrepancies and achieve a mutual consensus. This led to the creation of definitive criteria for Web3 auditing and a curated example dataset of 100 posts. The developed criteria were then used as prompts to train GPT-4 in filtering relevant posts, with adjustments made to the prompts to enhance the model's accuracy in evaluating the example dataset. The final step involved applying the refined prompt to all posts, with the explanation of classification presented in Table 5 and the corresponding statistics results presented in Table 2.

TABLE 2: Statistics of categorization Reddit discussions

Category	Subcategory	Post	Comments	Average Comments	Average Upvotes
1	1.1	147	2076	14	43
	1.2	60	2040	34	61
	1.3	34	3533	104	255
	1.4	174	3081	18	67
	1.5	23	3917	170	633
	1.6	17	473	28	54
2	2.1	139	1005	7	21
	2.2	113	1996	18	50
	2.3	68	2425	36	36
3	3.1	61	705	12	24
	3.2	69	2055	30	32

B.4. Sentiment Analysis

Table 3 showcases selected posts with their corresponding sentiment score by GPT-4. The table delineates the number of posts associated with each sentiment class, their respective proportions of the total dataset, and the aggregate count and percentages of comments and upvotes for posts within each sentiment category. This breakdown provides insights into community engagement relative to the sentiment conveyed in the posts.

TABLE 3: GPT-4 Sentiment Classification.

Sentiment Class	**Post Content Example**	**Post**	**Average Comment**
1	Audits in this space don't mean anything.	102	93
2	[Application] Audit Failed	50	30
3	Solidity DApp Audits	376	18
4	USDC is not in danger of collapsing	220	13
5	New crypto audit services being offered!!	157	17

Appendix C. Distribution of Sentiment Classification of Subcategory 2.3

Subcategory 2.3 on Reddit comprises discussions about the effectiveness of auditing. We analyzed the sentiment of these posts to gauge user attitudes. The detailed results are presented in table 4.

TABLE 4: Distribution of sentiment classification of subcategory 2.3

Sentiment classfication	Post	Engagement	
		Average comments	Average upvotes
1: Very negative	8	86.63	41.25
2: Slightly negative	10	30.5	35.2
3: Neutral	37	30.51	28.81
4: Slightly positive	8	26.75	69.88
5: Very positive	5	16.8	34.6
Total	68	35.66	36.47

TABLE 5: Sample for categorization Reddit discussions

Main Category	Subcategories	Sample
1: Discussion of Application Audit Dynamics	1.1: Upcoming Audits	[Application]'s Direction Says a Full Audit is Coming Soon
	1.2: Ongoing Audits	EtherCamps decentralized startup team public code audit by Zeppelin
	1.3: Halted Audits	[Application] Proof-of-Reserves Auditor [Audit Firm] All Work for Crypto Clients
	1.4: Successful Audits	[Audit Firm] Clears [Application] from Bugs
	1.5: Failed Audits	Security Audit Firm Discovers Critical Vulnerability in [Application] Smart Contract System
	1.6: Post-Audit Attacks	Another [Audit Firm] Certified Project Rugs as 3M USD Disappears From [Application] DeFi Exchange
2: Direct Discussion of Web3 Auditing	2.1: How Audits are Conducted	Was the Whisper protocol part of the security audit?
	2.2: Audit Firms	What Is [Audit Firm]?
	2.3: Impact of Audits	So Your Project is Audited... Cool, Cool, Cool
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