"I just have faith in my wallet to not mismanage my crypto": Investigating Changes in Users' Security Perceptions Post-FTX Collapse

Mingyi Liu
Georgia Institute of Technology
Atlanta, Georgia, USA
mingyiliu@gatech.edu

Nivedita Singh
Sungkyunkwan University
Seoul, Republic of Korea
singhnivvy@g.skku.edu

Jun Ho Huh
Samsung Electronics
Suwon, Republic of Korea
junho.huh@samsung.com

Hyoungshick Kim
Sungkyunkwan University
Seoul, Republic of Korea
hyoung@skku.edu

Taesoo Kim
Georgia Institute of Technology
Atlanta, Georgia, USA
taesoo@gatech.edu

Abstract

Non-custodial wallets (NCWs) grant users full control over their keys and crypto assets, whereas custodial wallets (CWs) rely on centralized exchanges. Security breaches at major exchanges are on the rise, exemplified by the 2022 FTX fraud, yet their influence on users' security perceptions and risk mitigation behaviors remains understudied.

We conducted 22 semi-structured interviews and a follow-up survey with 430 participants to address this gap concerning the FTX incident. We find that learning about FTX reduced trust in CWs and increased perceived security of NCWs. However, most users who were using non-SEC-compliant (equally risky) CWs did not transfer crypto to mitigate potential threats, showing continued trust in current wallets. Those who did often moved all funds from CWs to traditional banks rather than adopting NCWs. Notably, only one-third of survey participants were aware that centralized exchanges hold their private keys, and many still used noncompliant exchanges.

CCS Concepts

• **Security and privacy → Human and societal aspects of security and privacy**; • **Human-centered computing → Empirical studies in HCI**.

Keywords

Cryptocurrency wallets, Custodial and non-custodial wallets, Financial security incidents, Usable security

ACM Reference Format:
Mingyi Liu, Nivedita Singh, Jun Ho Huh, Hyoungshick Kim, and Taesoo Kim. 2026. "I just have faith in my wallet to not mismanage my crypto": Investigating Changes in Users' Security Perceptions Post-FTX Collapse. In *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems (CHI '26), April 13–17, 2026, Barcelona, Spain.* ACM, New York, NY, USA, 20 pages. https://doi.org/10.1145/3772318.3791341

CHI '26, Barcelona, Spain

ACM ISBN 979-8-4007-2278-3/26/04
https://doi.org/10.1145/3772318.3791341

1 Introduction

Cryptocurrencies, or crypto, are digital currencies secured by cryptographic techniques that enable transparent, immutable peer-to-peer transactions on blockchain networks [39]. Bitcoin[1] and Ethereum[2] are the most prominent cryptocurrencies by market capitalization. A recent executive order mandates the creation of a strategic Bitcoin reserve managed by the U.S. government, further intensifying global interest in Bitcoin [46]. To purchase, store, or trade crypto assets, users must use either a non-custodial (self-managed) wallet (NCW) or a custodial wallet (CW) managed by a centralized exchange. The key difference is that NCWs give users complete control over their private keys, while CWs entrust key management to the exchanges.

Unfortunately, centralized exchanges have not always proven reliable. In 2024, financial losses from centralized exchange breaches reached a new record, exceeding those reported from decentralized finance services [21]. Even well-established services with millions of globally registered users were affected as well; some of the largest breaches include the Mt. Gox hack [44] (2014), the Futures Exchange (FTX) CEO scam [40] (2022), and the most recent Bybit operational security breach [9] (2025). About 480 million, 8.9 billion, and 1.5 billion USD in crypto assets were stolen from these three incidents. The fundamental problem, in all three cases, is that exchanges store users' crypto assets and manage their private signing keys. Consequently, any serious security breach targeting an exchange could compromise users' assets. Despite such risks, their user base continues to grow rapidly, with Binance, a leading centralized exchange, announcing it has surpassed 280 million users in July 2025 [6]. Turning to NCW alternatives, however, comes with its own set of user experience challenges: while NCWs eliminate custodial risks, they

[1] https://bitcoin.org/en/
[2] https://ethereum.org/en/

also impose substantial usability burdens. NCW users must securely manage their private keys, and mistakes like losing or mishandling them can lead to permanent asset loss. For enhanced security, users often adopt hardware wallets [52], where NCWs are installed, that require carrying physical devices to authorize transactions, and they may eventually need to transfer their crypto assets to a centralized exchange to cash out. Such usability and accessibility frictions make NCWs not necessarily the most practical option for all users. Taken together, wallet choice often depends on individuals' willingness to take on the responsibility of securely managing keys and recovery phrases, and their preference for convenience and ease of access.

In this paper, we investigate how awareness of large-scale centralized exchange breaches influences users' security perceptions of custodial and non-custodial wallets, and their resulting mitigation actions. We focus on the FTX incident due to its unprecedented scale, and it being widely recognized as the first major financial mismanagement led by a rogue CEO [25]. Although the incident occurred in November 2022, it continues to hold significant relevance due to its breach scale (largest known to date) and the involvement of a rogue CEO exploiting their own users. Indeed, the FTX breach has been the focus of numerous recent studies [41, 43, 52]. Prior work has largely analyzed market reactions [3, 7, 13, 48], while user-centered perspectives remain understudied. Understanding how crypto users' security perceptions and behaviors change after becoming aware of a major exchange breach is important, as it can reveal users' misconceptions about the breach and its security risks. Security decisions made based on such misconceptions may expose users to new risks or hinder them from appropriately addressing current risks. Ultimately, those insights can form a firm basis for clear guidance on how breach information should be documented and communicated to crypto users to help them understand associated risks better, and take appropriate actions immediately to mitigate risks. To bridge this research gap, we conduct two complementary studies: a semi-structured interview study with 22 crypto wallet users, and a follow-up online survey with 430 participants. The interview study provides detailed qualitative insights into users' reasoning and thinking processes through open-ended questions, which guide the design of the follow-up online survey. The survey then confirms these trends and observations on a larger scale, and precisely measures their significance using statistical tests. This mixed-methods approach offers a more comprehensive understanding of users' perceptions and behaviors than qualitative methods alone. Both studies were designed to answer the following two research questions in the context of the FTX case study:

RQ1: How does exposure to large-scale centralized exchange breaches affect users' security perceptions of CWs and NCWs? Our focus is on understanding whether security perceptions change as anticipated—with trust in CWs declining—or if they change in an unexpected manner.

RQ2: What risk mitigation actions do users take based on changed security perceptions? Understanding how users react to large-scale breaches is crucial for assessing if their security perception changes indeed lead to anticipated and informed risk mitigation, such as reconsidering the use of CWs and turning to NCW alternatives in response to major exchange failures like the FTX collapse. This research question examines how shifts in users' mental models influence their decisions on wallet usage and self-protection strategies.

The two study results indicate that users' confidence in CW security generally declines after learning about the FTX scam (**RQ1**), while their perceived security of NCWs increases slightly. These users recognize that centralized exchanges are inherently vulnerable to collapse risks, such as those caused by rogue CEOs, whereas NCWs offer more control over their crypto assets. Users taking action following the FTX scam tend to choose Coinbase, an SEC-compliant[3] CW, as their next reliable wallet option (**RQ2**). MetaMask and Ledger (a hardware wallet) are NCWs that are also popularly adopted. Users transferring crypto assets from their CWs often select traditional banks as a safer custody alternative. A novel observation is that CW-only users (i.e., those with no prior NCW experience) are more likely to lose complete trust in CWs and ultimately transfer everything to banks.

A small group of users shows unexpected trends, including instances of growing confidence in CW security, and losing confidence in NCW security (**RQ1**). Such participants believe that external factors, such as regulatory oversight, will enhance CW security over time. Users who report declining confidence in NCWs often provide incorrect answers to knowledge questions about the FTX incident, suggesting that misinterpretations of CW breaches may negatively affect their perceptions of NCW security. Further, perception change does not always translate into action. Most users of non-SEC-compliant CWs, after reporting a drop in confidence in CWs, do not transfer their crypto assets to mitigate noncompliant CW risks (**RQ2**)—indicating that even significant hacks and scams may not be sufficient to motivate users to explore compliant CWs or self-custody options in NCWs. Upon examining reasons for inaction, we identify another concerning group: 16.9% of survey participants who prioritized trusting their NCWs but are, in fact, using alternative CW options. Some in this group continue to use non-SEC-compliant CWs even after learning about the incident, and incorrectly believe they have self-custody over their wallets and crypto assets.

Taken together, these key observations represent the major contributions: based on the first systematic investigation into users' security perception and behavioral changes following a large-scale CW scam, we identify concerning groups of users who report growing confidence in CW security (and declining confidence in NCWs), those who correctly understand CW risks but take no action, and those who mistakenly believe they have self-custody over their non-SEC-compliant CWs. These findings underscore the need to improve the quality of

[3]We use the term "SEC-compliant" to refer to an exchange that publicly and regularly files financial statements with the U.S. Securities and Exchange Commission, which makes these filings accessible through their EDGAR database: https://www.sec.gov/search-filings. See §2.3 for details.

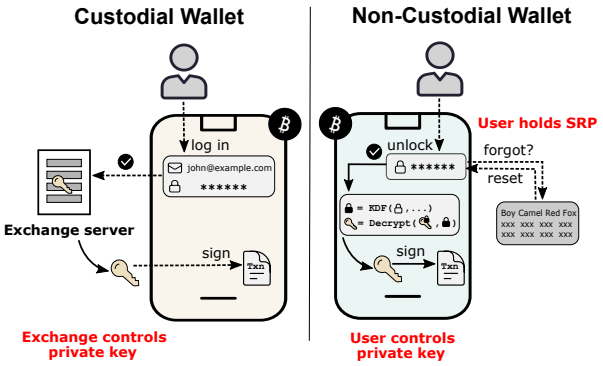


Figure 1: Comparison of security and authentication mechanisms in CWs and NCWs. CW users (left) authenticate via exchange-managed credentials, with private keys held by the exchange. NCW users (right) retain control of their private keys, which are stored locally and backed up via secret recovery phrases (SRPs).

incident summaries shared with end users—summaries should detail the exact causes of incidents, provide guidelines to help users assess their own security risks (e.g., listing CWs/NCWs to avoid), and recommend specific, easy-to-follow actions for immediate mitigation of similar risks. We recommend that centralized exchanges implement custody verification steps for users to confirm that private keys, which authorize crypto transactions, are stored on the exchange's servers. Only 35.3% of survey participants correctly understood this aspect of key storage, and this key finding, for the first time, provides quantitative evidence of a long-suspected misconception in crypto custody.

2 Background and Threat Model

This section provides foundational context in four components. We begin by outlining the architecture of crypto wallets, contrasting custodial and non-custodial designs to clarify how asset custody relates to user authentication and risk exposure. We then introduce the collapse of FTX to illustrate the real-world consequences of centralized custody failures. Next, we explain the regulatory role of SEC compliance for centralized exchanges and the best practice mitigation steps that follow from this context. Lastly, we present the threat model and scope, which define the security risks we focus on and the primary boundaries of our analysis.

2.1 Custodial vs. Non-Custodial Wallets

Crypto wallets enable users to manage their digital assets, including sending and receiving crypto and interacting with blockchain-based services. They typically appear to users as mobile applications, browser extensions, web dashboards, or dedicated hardware devices, and are broadly categorized as custodial or non-custodial based on who controls the private keys authorizing transactions. Figure 1 presents the differences in authentication and asset management methods.

Custodial wallets. CWs such as Coinbase and Crypto.com provide interfaces that are similar to traditional investment platforms, allowing users to view balances, initiate trades, or withdraw funds. An example mobile interface is shown in Appendix B (Figure 8a). CWs delegate private key control to third-party services, typically centralized exchanges. Users log in using credentials managed by the exchange, which signs transactions on their behalf. This model improves usability but introduces a single point of failure and creates reliance on the exchange's integrity and security practices.

Non-custodial wallets. The interfaces of software NCWs differ from CWs primarily in the presence of key management and wallet recovery features (Figure 8b in Appendix B). NCWs give users direct control over their private keys, which are stored locally and commonly encrypted with a user-defined password. This enables full self-custody, eliminating reliance on intermediaries for asset access and transaction authorization. To safeguard against key loss, NCWs support secret recovery phrases (SRPs)—mnemonic phrases that can be used to regenerate the private key. SRPs allow wallet recovery on new devices but also concentrate risk: anyone with the phrases can access the assets.

This architectural distinction underscores a fundamental trade-off between usability and control: CWs prioritize convenience and platform-managed security, whereas NCWs offer greater autonomy at the cost of increased user responsibility.

2.2 The FTX Collapse

FTX, founded in 2019, rapidly grew into one of the world's largest custodial exchanges, serving over five million users and valued at 32 billion USD by 2022 [19]. In November 2022, the exchange collapsed after revelations that customer funds had been diverted to Alameda Research, a trading firm also controlled by founder Sam Bankman-Fried [22]. This misuse of custodial assets, coupled with weak governance and limited regulatory oversight, triggered a liquidity crisis, leaving many users unable to recover their funds [8, 47]. The collapse constituted one of the largest financial fraud cases in U.S. history [25]; Bankman-Fried was subsequently convicted and sentenced to 25 years in prison [42]. The incident exposed the structural vulnerabilities of opaque custodial models and prompted renewed interest in transparency mechanisms such as Proof of Reserves (PoR). While PoR enables partial verification of exchange-held assets through cryptographic techniques, it often fails to account for liabilities, remains susceptible to manipulation, and depends on the trustworthiness of third-party auditors [29, 30].

The FTX collapse highlighted the risks of centralized asset control and underscored the need for user-verifiable protections, particularly in environments lacking robust regulatory oversight.

2.3 SEC Compliance in Centralized Exchanges

The U.S. Securities and Exchange Commission (SEC) oversees financial institutions that hold or manage customer assets. In

this paper, an exchange is considered "SEC-compliant" when it is registered as a reporting entity, and is legally required to submit regular financial statements. These obligations apply only to centralized exchanges (custodial wallets) that maintain control over users' assets, while non-custodial wallets, by design, fall outside the scope of SEC regulation. Specifically, SEC-compliant exchanges must publicly disclose information such as their assets, liabilities, and risk factors through annual, quarterly, and current reports submitted to the SEC's EDGAR system [45]. These disclosures increase transparency by enabling external scrutiny of an exchange's financial health and governance practices. While SEC compliance does not guarantee technical security, it provides legal accountability and greater assurance that custodial assets are subject to standardized financial reporting and monitoring. This regulatory context is relevant to our study because SEC compliance signals stronger financial oversight that helps protect against the types of asset mismanagement (rogue CEO risks) that contributed to FTX's failure. Therefore, SEC-compliant exchanges—those that consistently provide all required financial statements and are confirmed to meet industry standards—can be considered as relatively safer and more financially secure alternatives upon selecting a custodial wallet.

An ideal security practice for a crypto user who has recently learned about a large-scale exchange breach (like the FTX scam) would involve the following steps: (1) comprehend the security risks and specifics of the breach; (2) verify whether their current wallet complies with SEC regulations, and assess if it is exposed to the same security risks highlighted by the incident; (3) if the user's wallet or exchange is also at risk, promptly find safer (SEC-compliant) CWs or reputable NCWs; and (4) transfer their crypto assets to these safer options.

2.4 Threat Model and Scope

The threat model in consideration focuses on risks associated with wallets being managed by centralized exchanges. Specifically, we consider scenarios where exchanges (e.g., FTX) mismanage user assets, engage in fraudulent activities, or collapse due to operational or security failures. In such cases, custodial wallet (CW) users may lose access to their assets because exchanges, rather than users, control the private keys. We study users' awareness of such CW-specific risks, and how their security perceptions change after learning about the FTX scam. Non-custodial wallets (NCWs) eliminate this dependency by granting users sole control over their private keys, thereby mitigating those custodial risks while placing responsibility on users to securely protect their keys and remember strong passwords. We do not consider threats specific to NCWs (e.g., insecure key management), and how such risks may have affected users' NCW adoption decisions. NCW security awareness analysis is beyond the scope of this work.

3 Related Work

Digital finance and security incident response. Beyond crypto, prior HCI research has explored how individuals engage with digital financial systems and react to security incidents. Regarding digital finance, a diary study by Lewis *et al.* [31] revealed a persistent trade-off between convenience and *trust* in everyday cashless payments, showing that users often adopt technologies despite privacy concerns. We extend this observation to the crypto context, identifying a parallel yet distinct trade-off between convenience and *custody control*: users continually weigh the ease of CWs against the risks of delegating asset control. Furthermore, Li *et al.* [32] demonstrated that digital P2P payments can strengthen *interpersonal trust* and social dynamics. While their work highlights trust in low-risk social payment settings, our study investigates *institutional trust* between users and centralized exchanges in a high-risk security context, examining how such trust erodes following systemic failures like the FTX collapse.

Research on general security incidents provides further insight into user behavior. Mayer *et al.* [37] identified a sizable "intention–behavior gap" in reactions to data breaches, showing that recognizing risks does not necessarily lead to protective action. Our study confirms this phenomenon persists even in a *high-stakes financial context*. Despite diminished perceived security of centralized exchanges post-FTX, many users still chose not to migrate to safer alternatives, relying on "faith" in their current providers. Regarding risk communication failures, Zou *et al.* [53] found that data breach notifications often suffer from readability issues and hedge terms that obscure risks. To address such clarity issues in our own recommendations, we refer to a foundational work by Felt *et al.* [16], who demonstrated that concrete, imperative instructions significantly improve user adherence to security warnings. Similarly, Kelley *et al.* [26] showed that the use of consistent and uniform warning formats, referred to as standardized "nutrition labels," are effective in simplifying complex disclosures. We apply those insights to ground our design recommendations, suggesting that crypto incident reports must prioritize *actionability* and *standardization* to facilitate prompt risk mitigation.

Security perceptions and wallet behavior. A systematic review of security vulnerabilities in crypto wallets [24] highlighted persistent risks across storage, software, and operating system layers. However, against this broader technical backdrop, prior studies have shown that users' misconceptions about private key management and wallet architecture significantly influence their behavior when using crypto wallets. Mai *et al.* [35], for example, found that flawed mental models—including misconceptions about key storage, transaction processes, and perceived anonymity—can expose users to risks such as data leakage and fund loss. These vulnerabilities are further compounded by usability issues, such as unintuitive interfaces and inconsistent support for wallet recovery and risk mitigation [15, 24, 28, 49, 50]. A clear behavioral divide exists between CWs, which are perceived as more

convenient and user-friendly, and NCWs, which offer greater control but demand higher technical competence. Sharma *et al.* [41] emphasized that effective use of NCWs requires proper user education on key management and wallet recovery procedures. Abramova *et al.* [1] identified distinct user groups and showed that "cypherpunks" (experienced crypto users) prefer self-managed security solutions. This resonates with our finding that users with an accurate understanding of wallet custody were more likely to adopt hardware wallets following the FTX incident. An interview-based study by Yu *et al.* [52] explored the reasons behind wallet choices, finding that users selected different wallets based on both security concerns and task-specific needs. Our work complements theirs by providing event-driven insights, along with quantitative evidence, e.g., on users' custody mental models and the use of noncompliant CWs.

While prior research has largely focused on persistent misconceptions and isolated usability issues, our study investigates how real-world breaches, specifically the collapse of FTX, reshape user perceptions and behavior over time. Some respond by reverting to traditional banks, while others remain reliant on custodial services. These findings highlight a persistent gap between security perceptions and actual behavior, emphasizing the need for behaviorally grounded interventions and clearer education on wallet security.

User perceptions and mitigations after scams. Beyond traditional cyber threats, crypto users are increasingly targeted by diverse, customized fraudulent schemes, including impersonation fraud and deceptive promotional campaigns [23, 33, 36]. A recent study [2] deployed "honey tweets" seeking wallet support to lure scammers, and revealed their scam techniques and routines, aiming either to steal victims' secret recovery phrases or to induce direct payments. Froehlich *et al.* [18] identified persistent risky behaviors among users even after high-profile breaches, such as reusing private keys or relying on insecure platforms. In a recent study of DeFi victims, Liu *et al.* [34] showed that victims continued to use high-risk DeFi services without changing their security practices, motivated by financial opportunity rather than risk awareness. Notably, even victims of multiple scams rarely adopted effective countermeasures, and many held inaccurate beliefs about the effectiveness of traditional security controls.

In contrast, our study is the first to systematically delve into a large-scale centralized exchange breach, more precisely the FTX collapse, from a user-centered perspective. We analyze how learning about a major CW breach influences users' perceptions of wallet security and their actual mitigation behavior. Our findings reveal that although trust in CWs declines, users often do not take protective actions such as migrating to NCWs. Instead, many either continue using their existing CWs, or transfer everything to traditional banking systems—these observations highlight a distinct pattern of perceptual shifts in CW/NCW security and the lack of counter behaviors being pursued.

4 Study 1: Semi-structured Interview

This section presents the methodology and findings from our qualitative study, which explores how users' security perceptions shifted and the risk mitigation strategies they adopted after learning about the FTX collapse. This study was approved by the Institutional Review Board (IRB), which reviewed the study protocols and materials to ensure participants' privacy and well-being, and the study did not collect any sensitive information such as wallet addresses. The informed consent form, interview guide, and codebook for this study are available in the supplementary material.

4.1 Interview Methodology

Design. The interview protocol, which includes five different sections, was designed to answer the two research questions. In the first section, we probed participants about their wallet usage history and their ability to distinguish between CWs and NCWs. Participants were asked when they started using each wallet, why they adopted it, and, if applicable, why they later discontinued using wallets they had previously used. We then provided brief explanations of CWs and NCWs. CWs were described as *"wallets associated with a centralized exchange that takes custody of your digital assets; usually, you have an account with that exchange."* For NCWs, we noted that *"non-custodial or personal wallets allow you to self-custody, which means you have full control over your assets."* After this, participants were asked to categorize each wallet they mentioned as either a CW or an NCW and to explain their reasoning. Sample questions included *"Is it a custodial wallet or a non-custodial wallet? Why do you think it is a custodial/non-custodial wallet?"* To ensure certain degree of relevance and quality in participants' answers, we ended the interview at this point if participants were unaware of the existence of NCWs.

The second section studied participants' knowledge of crypto wallets and the FTX incident. We asked participants about the perceived advantages and disadvantages of using CWs and NCWs, including any concerns they have regarding wallet security and usability. We then assessed participants' awareness of the FTX incident. To avoid framing risks, we did not provide any explanation about the incident during the interview. We asked an open-ended question, asking participants to describe the incident solely from their own understanding: *"Could you try to describe the FTX scam incident with respect to when it happened, what happened, why it happened, who were affected, and how they were affected?"*

With this context defined, the third section focused on addressing **RQ1** by examining how the FTX collapse influenced participants' perceptions of the security and reliability of CWs and NCWs, along with the reasons for these changes. We asked four separate questions covering both security and reliability perceptions for each wallet type: *"How did the FTX scam incident affect your security/reliability perceptions of CW/NCW, and why?"* To answer **RQ2**, the fourth section investigated strategies employed by users to reduce similar risks following the incident, focusing on crypto transfers (including both

source and destination wallets) and their choices to either continue using, adopt new, or abandon certain wallets. Interview questions included: *"Did you transfer your crypto assets to a different exchange service or a personal non-custodial wallet after learning about the FTX scam incident?"* and *"Did you decide to use a different crypto wallet or stop using an active wallet after learning about the FTX scam incident?"* Participants were also asked to explain reasons behind their decisions.

In the final section, participants were asked to answer knowledge questions about the security features of CWs and NCWs, including passwords, private keys, and secret recovery phrases. They were also asked to explain how each of these is stored and recovered if lost. In particular, we first asked questions about passwords and keys in relation to CWs, then repeated the same questions for NCWs and additionally covered questions about secret recovery phrases, which are specific to NCWs. For instance, we asked, *"If you forget your password/secret recovery phrase, how would you recover or reset it?"* and *"Where are the public and private keys stored?"*

We conducted three pilot interviews to refine the clarity of our protocol; those results were not included in the final analysis. Each interview concluded with a post-interview survey designed to collect demographic information, and assess participants' understanding of general crypto fundamentals and security practices. Some knowledge questions were adapted from prior work [5, 27], while others were developed for this study. These questions were also used in Study 2.

Recruitment. To ensure response reliability, we recruited participants through Prolific[4] and applied its built-in screeners first: participants were required to (a) be adults, (b) speak English, (c) show a Prolific approval rate of at least 95%, (d) reside in the U.S. to minimize cultural and regulatory variations, and (e) have prior cryptocurrency experience. We then used a short screening survey distributed on Prolific, which asked participants to select the wallets they had used, confirm whether they were aware of the FTX collapse, and state if they had used FTX. Only those aware of the incident were invited to participate in the interview. Participants were compensated with 0.30 USD for completing the screening survey and 20 USD for the interview.

Data collection and analysis. We conducted and recorded online video interviews, with the first and second authors alternating as the primary interviewer while the other attended to ensure protocol consistency. We terminated five sessions where participants failed to provide wallet-use proof, provided inconsistent wallet first-setup dates, or showed a lack of awareness of NCWs. In total, 22 interviews were completed, with an average duration of 66 minutes (range: 46–84 minutes), concluding in September 2023. We transcribed the interview recordings and conducted an inductive codebook thematic analysis [20]. Two researchers independently coded an initial subset of transcripts and met after each transcript to discuss and resolve coding discrepancies. After multiple rounds of collaborative refinement, we conducted a reliability check on the jointly coded subset and achieved a Cohen's κ [17] of 0.86. Common sources of disagreement included whether to assign a new code for infrequent responses or place them under the "Other" category, as well as differences in coding granularity. These discrepancies were discussed and resolved prior to finalizing the codebook. The remaining transcripts were then coded by one researcher using the finalized codebook to ensure consistency. Recruitment stopped when additional interviews yielded no new insights relevant to our research questions. Across all interviews, the coding process resulted in a final set of 92 codes. In addition, to ensure the validity of our qualitative study, we excluded responses from participants who misidentified wallet categories when analyzing perception changes related to CWs and NCWs. These responses were included, however, in our analysis of behavioral changes following the incident.

Table 1: Interview participants' demographics and crypto wallet experience.

Item	Property	$n = 22$	% of participants
Gender	Male	12	54.5%
	Female	7	31.8%
	Non-binary	3	13.6%
Age	18-24	3	13.6%
	25-34	7	31.8%
	35-44	5	22.7%
	45-54	4	18.2%
	55-64	3	13.6%
	65 or above	0	0.0%
Education	No schooling	0	0.0%
	No high school	0	0.0%
	High school	6	27.3%
	Bachelor's	10	45.5%
	After bachelor's	6	27.3%
Income	<$25k	4	18.2%
	$25k-50k	5	22.7%
	$50k-75k	6	27.3%
	$75k-100k	1	4.5%
	$100k-125k	2	9.1%
	$125k-150k	2	9.1%
	$150k-175k	1	4.5%
	$175k-200k	0	0.0%
	$200k+	1	4.5%
Total Crypto Value	$0-1k	13	59.1%
	$1k-10k	6	27.3%
	$10k-100k	2	9.1%
	$100k+	1	4.5%
Crypto Years of Experience	<1	0	0.0%
	1-3	8	36.4%
	3-5	7	31.8%
	5-7	2	9.1%
	7-9	4	18.2%
	>9	1	4.5%
Adopted Wallets Type	CW only	2	9.1%
	NCW only	1	4.5%
	CW and NCW	19	86.4%
FTX User	Yes	7	31.8%
	No	15	68.2%

Demographics and crypto experience. Table 1 lists the demographic information and crypto experience of our interview participants. Our participant pool was predominantly younger and male. While experience levels varied, most participants reported modest crypto holdings, typically less than

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

10,000 USD in value. Most participants had experience using both CWs and NCWs; notably, seven participants were former users of FTX. Additional participant details, including wallet adoption and knowledge scores, can be found in Appendix B.

4.2 Interview Results

4.2.1 Understanding Wallets and the Incident. To assess participants' knowledge and gather background details necessary to thoroughly investigate changes in participants' security perceptions and behaviors (the two RQs), we first examined the responses from the first section: this initial analysis allowed us to explore participants' awareness of wallet types, their interpretation of the FTX incident, and their knowledge of the security features of crypto wallets shown in Figure 1.

Custody awareness. To evaluate the participants' awareness of the differences in custody characteristics between CWs and NCWs, along with their ability to correctly distinguish the two wallet types, we asked participants to categorize all wallets they currently use or have used in the past as either CWs or NCWs. Worryingly, seven participants incorrectly categorized one or more wallets. For example, P5 correctly identified Binance as a CW but incorrectly classified Coinbase as an NCW. Participants' explanations revealed that misidentifying CWs as NCWs was often due to the misconception that they retained full control over their crypto assets while using a CW. As P13 explained, referring to the CW and NCW definitions introduced earlier, *"I have complete control... based on the two definitions."* Some exchanges, such as Coinbase and Crypto.com, offer both CW and NCW options, which may contribute to confusion among users who believed they were using a CW when they were actually using an NCW. For simplicity, we refer to participants with an accurate understanding of wallet categories as *custody-aware* users, and those with an inadequate understanding as *custody-unaware* users throughout this paper.

Incident awareness. In the following step, we inquired about the root cause of the FTX incident to assess how accurately the participants understood the key details about the incident—this assessment was essential for us to examine later how an accurate or inaccurate understanding of the incident might influence security perceptions and risk mitigation behaviors. When asked about the root cause, over half of the participants correctly attributed it to the CEO's mismanagement of users' assets. For example, P11 explained, *"FTX was closely connected to Alameda Research... they had used some user deposits to engage in some of that [investment] activity..."* Participants who misunderstood the cause of the incident provided a variety of answers, such as money laundering, Ponzi schemes, and theft by either the CEO or hackers. P15, for example, believed that *"The guy running it stole people's money... I think the guy was a criminal."*

Security features knowledge. To gain a deeper insight into whether participants correctly comprehend the custodial features of CWs/NCWs, as well as the fundamental security assurances and risks associated with private key management, we examined their understanding of the storage locations of private keys. Establishing this prior context is integral for subsequent analysis that examines how key management factors affect users' choices regarding the adoption of new wallets, or continued use of current wallets. Fewer than half (9 out of 22) of participants correctly identified that CWs store private keys on centralized servers, and almost half (10 out of 22) were aware that users hold the private key in NCWs. Surprisingly, only a few participants ($n = 3$) accurately identified private key ownership for both wallets, suggesting a significant gap in users' understanding of private key ownership. Additional analyses on participants' knowledge of security features are provided in Appendix A.

4.2.2 RQ1: Security Perception Changes. Next, to answer RQ1, we investigated how users' security perceptions of CWs and NCWs changed after learning about the FTX collapse, along with the reasons they attributed to those changes. In addition, we also examined users' perceptions of wallet reliability; however, the findings were largely aligned with those related to security perception, so we exclude them from this section for brevity.

Changes in CW security perceptions. We expected participants' confidence in CW security would decline after learning about the FTX collapse, and more than half of the participants indeed responded in this expected manner. A significant portion of such participants mentioned EXCHANGES CONTROL FUNDS as the primary reason for feeling less secure. For example, P17 remarked, *"They're controlling my money that I cannot move or do anything without their permission."* Some participants expressed concerns about EXCHANGE COLLAPSE RISKS, such as *"What if this happened tomorrow with my custodial wallets?"* (P10). A few participants mentioned insufficient regulations and declining confidence in the broader crypto industry.

Conversely, some participants reported that their CW security perception remained unchanged following the incident. A common reason was that these participants were already aware of EXCHANGES CONTROL FUNDS and the associated risks. Some cited PRIOR INCIDENT LESSONS, such as *"Because so many of them [centralized exchanges] collapsed. I can name like 5 or 10 of them"* (P11). That is, most participants who expressed no security perception change already had low confidence in CW security. Notably, P7 reported unchanged perception due to trust in an established CW, stating *"I'm with something that's established and been there a long time, so I'm not worried."*

Changes in NCW security perceptions. Given the studied FTX collapse involved a centralized exchange breach, we anticipated that users' trust in NCW security would not be negatively impacted. Most participants responded as expected, with just two exceptions. About half of participants reported feeling more secure about NCWs, primarily because they recognized that USERS CONTROL FUNDS completely. P14 commented, *"It's almost better to lose it on your own merit than someone else's mistake,"* highlighting the importance of asset ownership. Less frequently cited reasons for improved NCW security

perception include NCWs' robustness to centralized exchange collapses and users' full control over wallet credentials: *"It's all in your possession—on your phone or on your computer..."* (P15). The other half reported unchanged perceptions of NCW security. Similar to the reasons supporting positive changes, participants cited having complete control over crypto assets and NCWs' ability to withstand exchange collapses as two important reasons. P9 and P22 were two exceptions, expressing negative changes in their security perception of NCWs. Notably, their explanations reflected concerns about crypto as a whole rather than NCW-specific security properties. For example, *"I don't hold cryptocurrency, like in any second, it's unreliable. It's risky. It devalues so fast"* (P22). P9 became more skeptical after the incident, *"I just think that all crypto wallets are not safe now."*

RQ1 takeaways. Taken together, those observations regarding RQ1 were mostly in line with our expectations: learning about the FTX collapse was associated with a general decline in crypto users' perceived security of CWs, accompanied by a modest improvement in their perception of NCW security. The primary reasons for users' diminished sense of CW security were their awareness that exchanges control their assets and the potential collapse risks. Such risks associated with centralized exchanges are related to the "platform risk" discussed in prior work [18]. Conversely, users' recognition or reinforcement of their full control over crypto was the main reason for an increased sense of security toward NCWs.

4.2.3 RQ2: Risk Mitigation Behaviors. To address RQ2, we studied how participants adjusted their wallet adoption behaviors to mitigate the risks following the FTX incident, with a focus on wallet selections and crypto transfers.

Wallet selections. Contrary to initial expectations, the marked shift in security perception discussed in §4.2.2 did not lead to a corresponding change in participants' wallet choices. Most participants reported no changes to their wallet list; they neither adopted new wallets nor discontinued those already in use. A few participants stopped using certain wallets, but none began using a new wallet after learning about the breach.

About half of the participants who kept their wallet list unchanged cited trust in their CWs. P9 stated, *"I just have faith in my [custodial] wallet to not mismanage my crypto,"* reflecting reliance on previously established trust rather than an informed assessment of wallet security and FTX-like risks. While a manual review confirmed that all but one of these participants used SEC-compliant wallets, such faith-based decision-making behavior may be problematic—particularly given that noncompliant CWs may still be used, carry greater financial risks, and are best avoided. A smaller group of participants continued using the same wallets because they trusted their NCWs. These participants were custody-aware users, as they had correctly identified all wallet categories earlier in the interview. For example, P4 explained, *"It just basically reaffirmed my opinion... that I should use non-custodial [wallets]."* Some other participants expressed comfort with the custodial risk because they held relatively small amounts of crypto. As P12 shared, *"because I don't have that much in terms of assets, I'm comfortable with the risk of it being in a custodial wallet."* Less common reasons for no wallet changes include paused or limited engagement and uncertainty about best options. Some participants hinted at practicality and usability considerations. P19, for example, cited their established usage pattern: *"all the wallets I use, like, they're used for distinct purposes,"* suggesting that fixed specific needs and routines shaped their choices. Likewise, P22 explained their reliance on centralized exchanges as transactional bridges: *"the money goes into the exchange, and then it goes out."* While not dominant, these examples highlight that usability considerations also played a role in some users' decisions.

Among those who stopped using at least one wallet, a few participants discontinued both CWs and NCWs due to a loss of confidence in the entire crypto industry after the FTX collapse. More participants, however, chose to stop using only CWs, and expressed a growing preference for their NCWs: *"I very much preferred non-custodial [wallets] after the FTX incident"* (P13).

Crypto transfer. Changes in users' security perceptions did not generally correspond to crypto transfers between wallets—most participants, regardless of their understanding of the differences between CWs and NCWs, did not transfer crypto assets following the FTX incident. Participants commonly cited that the amount of crypto stored in their wallets was too small to justify cumbersome countermeasures, such as setting up new wallets. Many participants expressed trust in the wallets they used, including both CWs and NCWs, and explained that they did not feel it was necessary to relocate their assets: *"My cryptocurrencies were already [in] self-custody or in a safe place I trusted"* (P6). These participants were confirmed to be custody-aware users, and all CWs they mentioned, except one reported by P7, were SEC-compliant. Worryingly, P7, who took no action, believed that the risks of the FTX scam did not apply to other centralized exchanges: *"The FTX wasn't connected to them in any way, so I didn't give it any thought at all."* Some custody-aware participants reported learning about various CW risks through prior security breaches and had already made transfers before the FTX collapse. For example, P20 transferred crypto to a hardware wallet prior to the event: *"I had already taken everything off exchanges before that happened."* Participants P18 and P21, who mistakenly believed their NCWs were CWs, did not take any action because they were UNSURE WHERE TO safely transfer their crypto: *"FTX was like a big one. I was waiting to see, was anybody else gonna be exposed?"* (P18). Less frequently cited reasons for not transferring crypto include being lazy and incurring transfer fees.

Among those who transferred their crypto following the incident, transfers from CWs to NCWs and transfers from CWs to ordinary bank accounts were equally common, regardless of participants' understanding of the differences between CWs and NCWs. On one hand, most participants who transferred to banks had multiple wallet options (both NCWs and CWs) but

chose banks due to growing concerns about wallet security in general. Specifically, P10, who incorrectly categorized their NCWs as CWs, stated, *"I assumed it was the same risk... leaving it on this crypto wallet or if I transfer it to that one."* P11 and P22, two former FTX users, withdrew their crypto in time, and avoided losses. *"I transferred it all through the banking system, and fortunately, it all went through because I did it early... "* said P11. On the other hand, all participants who transferred crypto from CWs to NCWs relied on NCWs they had been using before the incident, rather than setting up a new wallet: *"Because I wanted to go from custodial to non-custodial. I didn't want to leave it with [CW Redacted]"* (P14).

RQ2 takeaways. Regarding RQ2, the key observations reported above show that changes in participants' security perceptions did not always translate into adequate risk mitigation: the majority of users neither explored new wallet options nor transferred their crypto assets to safer wallets, e.g., SEC-compliant CWs or well-established NCWs. While "insignificant amounts of crypto" was a frequently cited and understandable reason for not taking action, another commonly cited reason was "trusting current wallets," which revealed more problematic security behaviors. Specifically, some users who expressed trust in their CWs were in fact using non-SEC-compliant CWs. When transferring crypto assets, many participants with both NCW and CW options chose to move their funds to traditional bank accounts, which may suggest diminished trust in crypto wallet security in general.

5 Study 2: Large-scale Survey

We designed a follow-up questionnaire based on interview findings, and conducted it online on Prolific ($N = 430$) to statistically validate these observations at scale. This second study also received approval from the IRB, and both the informed consent form and the full survey are available in our supplementary material.

5.1 Survey Methodology

Design. The survey comprised five sections, mirroring the previous interview format. The first section focused on participants' experience with crypto wallets, starting with questions about the time they started using crypto wallets, and the total value of their crypto assets in USD. Given a list of wallets, participants were asked to identify all the crypto wallets they had used, specify which ones they are currently using, and estimate how their crypto assets were distributed among those wallets. We then randomly selected one wallet currently in use and, if applicable, one wallet that participants have stopped using. For each selected wallet, participants ranked their reasons for adopting or stopping use, and distinguished the wallet type (CW or NCW) based on the same definitions used in the previous interview study. In the second section, we studied participants' knowledge of crypto wallets, and their understanding of the FTX incident. For each wallet type, participants were asked to rank the advantages and disadvantages by importance, rate their perceived security and usability levels on a Likert scale, and rank the reasons behind those ratings. We then asked participants whether they were aware of the FTX incident. If they were, we proceeded to ask *"Why did the FTX collapse happen?"*, offering multiple choice options based on themes identified in the interview study.

The third section was designed to address **RQ1**. Participants reported perceived changes in the security and reliability of CWs and NCWs using Likert scales that ranged from "Significantly decreased" to "Significantly increased." The survey asked: *"How did the FTX collapse and learning about the incident influence your perceived security/reliability level of CWs/NCWs?"* addressing security, reliability, and CWs and NCWs in separate questions. For each category of "perception change direction"—negative, none, or positive change—as indicated by participants, we collected importance rankings for the reasons behind perception change, using the reasons identified in earlier interview study.

Table 2: Survey participants' demographics and crypto wallet experience.

Item	Property	$N = 430$ % of participants
Gender	Male	67.2
	Female	30.7
	Non-binary	1.6
	No answer	0.5
Age	18-24	10.7
	25-34	34.9
	35-44	30.5
	45-54	16.3
	55-64	4.4
	65 or above	3.3
Education	No schooling	0.0
	No high school	0.5
	High school	28.6
	Bachelor's	50.5
	After bachelor's	18.4
	Other	1.4
	No answer	0.7
Income	<$25k	11.4
	$25k-50k	18.4
	$50k-75k	21.9
	$75k-100k	17.2
	$100k-125k	8.8
	$125k-150k	9.5
	$150k-175k	3.7
	$175k-200k	1.4
	$200k+	5.3
	No answer	2.3
Total Crypto Value	$0-1k	44.2
	$1k-10k	35.6
	$10k-100k	8.6
	$100k+	0.7
	No answer	10.9
Crypto Years of Experience	<1	2.6
	1-3	17.4
	3-5	42.6
	5-7	21.2
	7-9	9.1
	>9	7.2
Adopted Wallets Type	CW only	32.3
	NCW only	4.4
	CW and NCW	63.3
FTX User	Yes	24.7
	No	75.3

To address **RQ2** in the fourth section, we asked participants if they transferred crypto after learning about the incident. The survey defined *transfer* as "transferring a portion of your crypto assets from any of your wallets, or selling a portion of your crypto assets and withdrawing cash from any of your wallets." Participants who indicated they did not transfer ranked their reasons for not doing so; those who did transfer identified the source and destination wallets involved. We also collected information about wallets that participants began using or stopped using after the incident: *"Which of the following wallets are the ones that you started/stopped using after learning about the FTX collapse?"*

The final section assessed participants' knowledge of wallet security features, such as whether passwords can be reset, if secret recovery phrases can be retrieved, and where private keys are stored. The survey concluded with knowledge questions about general crypto concepts and Internet security practices also referred to in the interview study. Two attention-check questions were included, and demographic questions were placed at the start of the survey.

Recruitment. To ensure participant quality and consistency, we applied built-in Prolific filters, checking for (a) adults, (b) prior cryptocurrency experience, (c) an approval rate above 95%, (d) fluency in English, and (e) U.S. residency. Participants were not restricted by wallet types. Compensation for completing the survey was 3.50 USD, and each took about 21 minutes.

Data collection and analysis. By October 2024, 777 complete responses were initially received. Of these, 2 responses failed the attention check, and 306 failed fact validation, including inaccurate wallet start dates (e.g., earlier than the official launch) or reporting the same wallet as both "newly adopted" and "stopped-use" after the FTX incident. An additional 39 responses contained conflicting answers, e.g., stating that a wallet was adopted for self-custody but later identified as a CW. This thorough screening ensured data quality, leaving 430 valid responses. We used non-parametric tests, as is standard for analyzing ordinal data and Likert responses. Specifically, we performed Mann-Whitney U tests and Chi-squared tests of independence, each at $\alpha = 0.05$. When performing multiple pairwise comparisons, we applied the Bonferroni correction to control Type I error. To complement p-values and better characterize the magnitude of observed effects, we calculated the rank-biserial correlation coefficient[5] (r) and reported the effect size. In addition, to maintain consistency with the interview study, we excluded responses from custody-unaware participants in analyses of CW and NCW perceptions, while including them in behavioral analyses.

Demographics and crypto experience. Table 2 provides an overview of the demographics and crypto wallet engagement among our survey participants. The sample was predominantly male (67.2%) and relatively young, with 76.1% under 44 years old (mean = 37.5, median = 36.0). Most participants (68.9%) held a bachelor's degree or higher. Additionally, while we omitted detailed occupation information due to response diversity, "computer and mathematical" occupations were most frequently reported (15.1%). Regarding participants' crypto experience, 24.7% were former FTX users. Based on reported wallets, we found that the majority (63.3%) had adopted both CWs and NCWs.

To evaluate the representativeness of collected responses, we compared our sample's demographics and crypto experience with those reported in a prior study targeting general crypto users [1]. In contrast to the referenced study, which reported 77.5% of male participants, our data included a smaller proportion of males. We targeted a slightly older population with 24.0% over 45, compared to just 17.7% reported in the reference study. Moreover, the crypto held by the majority of our sample was less than 10,000 USD in value, whereas this group represented only 45.8% of the population in the reference study. This difference may be due to their use of multiple recruitment channels. Lastly, our samples demonstrated longer crypto experience compared to the reference study, with a smaller proportion of participants having less than one year of experience, and a larger proportion reporting over 7 years.

5.2 Survey Results

5.2.1 Understanding Wallets and the Incident. We quantified our findings on users' awareness of wallet categories, interpretations of the incident, and understanding of wallet security features.

Custody awareness. Participants were asked to identify the category (CW vs. NCW) for a wallet in current use and, if applicable, one they had stopped using. First, 56.5% of survey respondents either answered at least one question incorrectly or selected "I have no idea," demonstrating an inadequate understanding of the custody characteristics of the wallets they used. Notably, only 58.5% of former FTX users correctly identified the wallet provided by FTX as a CW. Second, we found that participants were more prone to misidentify a CW as an NCW than vice-versa, with a Chi-squared test revealing a significant difference ($\chi^2(2, N = 808) = 18.82$, $p < 0.001$). Specifically, when participants were given three response options (CW, NCW, or "I have no idea"), 21.4% of answers to CW items were incorrectly labeled as NCW, whereas 11.9% of answers to NCW items were incorrectly labeled as CW. This trend suggests that many participants falsely believed they had full control over their crypto assets while using CWs (centralized exchanges). At the individual wallet level, Coinbase was most often misclassified as an NCW, accounting for 30.8% of cases in which CWs were incorrectly identified as NCWs.

Incident awareness. 65.1% of participants indicated awareness of the FTX collapse. Aligned with interview findings, 71.8% of those correctly identified "funds mismanaged by the CEO" as the primary cause from a list of multiple-choice options. Other respondents chose inaccurate reasons like "funds theft by the CEO" (13.6%), "money laundering" (8.6%), and "hacks" (1.4%). In addition, the Chi-squared test showed

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

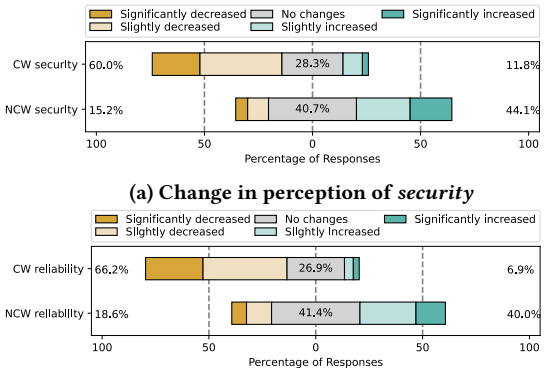
Table 3: Survey participants' responses to questions about security features. The correct answers are shown in bold.

Context	Question & Options	$N = 430$ (%)
CW	*I can reset/recover the password.*	
	• **True**	**75.8**
	• False	10.2
	• I have no idea	14.0
	Where is the private key stored?	
	• **Wallet provider's end**	**35.3**
	• User's end	18.1
	• Both of above	28.1
	• I have no idea	18.4
NCW	*I can reset/recover the password.*	
	• **True**	**40.9**
	• False	43.7
	• I have no idea	15.3
	Where is the private key stored?	
	• Wallet provider's end	5.1
	• **User's end**	**65.1**
	• Both of above	12.3
	• I have no idea	17.4
	I can reset/recover the seed phrase/ secret recovery phrase.	
	• True	19.3
	• **False**	**65.1**
	• I have no idea	15.6

no significant difference in cause awareness distributions between FTX users and non-FTX users but a significant one between custody-aware and custody-unaware groups ($\chi^2(4, N = 280) = 11.10$, $p = 0.03$). This suggests that general custody awareness, rather than direct experience, was more strongly associated with accurate incident interpretation.

Security features knowledge. Table 3 presents survey participants' responses to knowledge questions about wallet security features. The low accuracy rate of 35.3% indicates that participants are substantially confused about where private keys are stored in CWs. This confusion may stem from exchanges rarely explicitly explaining in their help or security sections that users do not hold their private keys on their own devices. Exchanges often use simple phrases like *"we manage your private keys"* and emphasize their implemented security measures [10, 11]. In contrast, marketing and educational efforts around NCWs appear more effective: over 65% of participants correctly acknowledged that users retain ownership of their private keys and that secret recovery phrases cannot be reset or recovered if lost. Losing both credentials will result in permanent loss of access to the NCW and all assets stored within. Notably, 41.7% of custody-aware users correctly identified private key ownership in both wallet types, compared to 19.3% of custody-unaware users; however, the difference was not statistically significant. This suggests that while custody awareness might relate to better understanding, explicit education on key ownership remains necessary.

5.2.2 RQ1: Security Perception Changes. We quantified changes in users' wallet security perceptions and their underlying reasons.



(a) Change in perception of *security*

(b) Change in perception of *reliability*

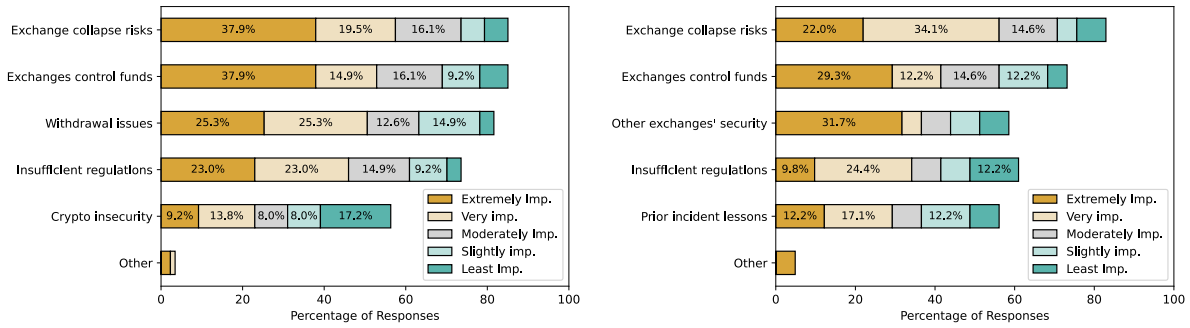
Figure 2: Changes in survey participants' perceptions of Custodial Wallet (CW) and Non-Custodial Wallet (NCW).

Perception change results. Figure 2 presents Likert-scale changes in participants' *security* and *reliability* perceptions of CW and NCW. Regarding security, the trends align with interview findings: participants reported a sharp decline in their perception of CW security, and a notable improvement in their perception of NCW security. The Mann-Whitney U test confirmed a significant difference in security perception changes between CW and NCW ($U = 4875.50$, $Z = -7.89$, $p < 0.001$), with a large effect size ($|r| = 0.54$). For reliability, participants' perceptions mirrored security changes but showed a more pronounced negative shift for CWs. A significant difference was also observed between reliability change distributions for the two wallet types ($U = 4648.50$, $Z = -8.21$, $p < 0.001$), again with a large effect size ($|r| = 0.56$).

We also analyzed differences in perception changes between FTX users and non-FTX users, as shown in Appendix B. FTX users, who were directly affected, were less likely to select "No changes" and showed a stronger tendency to form more negative perceptions toward both wallet types after the incident. However, statistical tests revealed no significant differences in perception change distributions between the two groups.

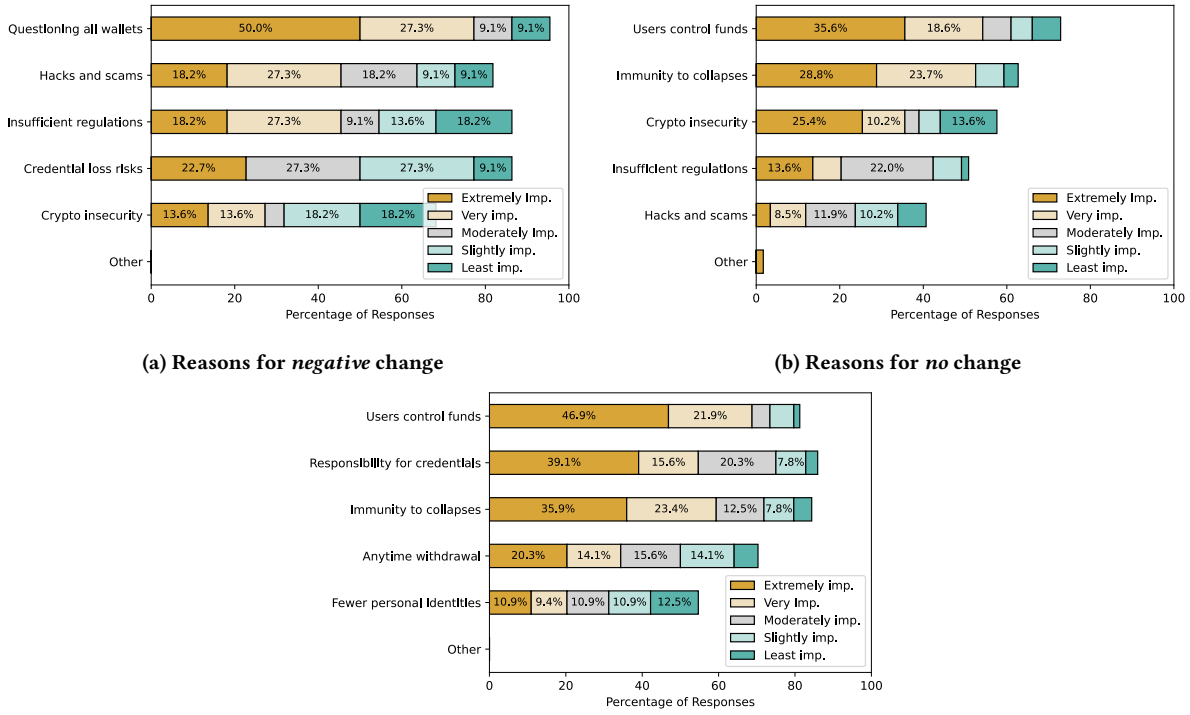
Given the mostly similar factors driving security and reliability perception changes, this section explains changes in security perception. Figure 3 and Figure 4 show each factor's importance in influencing participants' CW and NCW security perception changes, respectively. Results are sorted by weighted scores (5: "Extremely important" to 1: "Least important").

Changes in CW security perceptions. As illustrated in Figure 3a, participants who reported negative changes ("Significantly decreased" or "Slightly decreased") in their CW security perception ranked EXCHANGE COLLAPSE RISKS as the top reason. The second most important reason was their awareness of EXCHANGES CONTROL FUNDS. Additionally, these two reasons also emerged as primary factors in Figure 3b, explaining why participants' CW security perceptions remained unchanged.



(a) Reasons for *negative* change **(b) Reasons for *no* change**

Figure 3: Reasons for survey participants' perception changes in Custodial Wallet (CW) security.



(a) Reasons for *negative* change **(b) Reasons for *no* change**

(c) Reasons for *positive* change

Figure 4: Reasons for survey participants' perception changes in Non-Custodial Wallet (NCW) security.

This indicates that some participants were already aware of the risks associated with exchange collapse and exchanges managing user funds.

Moreover, no responses collected during the interview study indicated positive change in CW security perception; consequently, a text box was included in the survey, allowing participants to explain such choices. After manually coding the reasons for positive changes, we observed that participants expressed optimism, believing that such events would compel exchanges or external entities to aggressively enhance CW security and reduce future risks. Specifically, 41.2% of those participants expressed confidence in REGULATORY OVERSIGHT: *"Custodial [wallets] will have to answer to the government if it fails"* (S50). The second most common reason was INCREASED USER CAUTION (29.4%), with participants noting elevated risk awareness, such as *"...leading to improved security measures and better user awareness regarding custodial wallets"* (S788). Furthermore, 23.5% emphasized efforts from CWs, expecting

that CW WOULD ENHANCE SECURITY for various reasons. For example, S421 stated that CWs would do so *"to regain users' trust in exchanges"*, while S97 believed *"other wallets wanted to ensure they didn't suffer the same fate"* and would implement necessary security measures.

Changes in NCW security perceptions. First, our analysis revealed that participants with negative, no change, and positive shifts in their security perceptions of NCWs provided increasingly correct answers regarding the causes of the FTX collapse, at 68.2%, 76.3%, and 84.4% accuracy, respectively. This indicates that a larger proportion of participants in the negative perception change group misinterpreted the incident, thereby possibly amplifying its negative impact on security perceptions of NCWs.

Second, the quantitative analysis identifies the primary factors influencing the three types of changes in users' NCW security perceptions. As illustrated in Figure 4a, participants who reported a decline in their NCW security perceptions predominantly cited that they were QUESTIONING ALL WALLETS following the incident. While elevated caution is understandable, this response underscores a common misunderstanding among such participants regarding the root causes of the incident. Figure 4b shows that the predominant reasons for participants' unchanged perceptions of NCW security—USERS CONTROL FUNDS, and IMMUNITY TO COLLAPSES—reflect a strong prior awareness of NCWs' security properties. The ability of users to fully control their crypto emerged as the most important reason driving improved perceptions of NCW security (see Figure 4c).

To better understand the key factors influencing perception shifts in users who reported negative changes in CW security while also expressing positive changes toward NCW security, we analyzed their top-ranked (i.e., "Extremely important") reasons for these shifts across both wallet types. The most common pairing, cited by 29.5% of such participants, was EXCHANGES CONTROL FUNDS for negative CW perception changes and USERS CONTROL FUNDS for positive NCW perception changes. This observation suggests that these participants can differentiate between centralized and non-custodial environments and view personal control as a protective measure against institutional risks.

5.2.3 RQ2: Risk Mitigation Behaviors. We validated the interview findings through a quantitative analysis of users' wallet choices and crypto transfer decisions.

Wallet selections. Survey participants were slightly more proactive than interviewees, with only 53.8% choosing not to update their wallet list after learning about the incident. Specifically, 25.2% of survey respondents stopped using wallets other than the already ceased FTX wallet, while 35.5% adopted new wallets. The top ten discontinued and newly adopted wallets are detailed in Table 4. Notably, participants primarily discontinued the use of CWs, including those with large user bases like Coinbase and Binance. Regarding new wallet adoption, while Coinbase remained a top choice, participants exhibited diverse preferences, with several NCWs also ranking highly.

Table 4: The top ten wallets stopped and adopted by survey participants after the incident, with non-custodial wallets in bold text.

Stopped Wallets	(%)	Adopted Wallets	(%)
Coinbase	28.8	Coinbase	22.6
Binance US	27.3	**MetaMask**	14.0
Coinbase Wallet	19.7	**Coinbase Wallet**	12.9
KuCoin	10.6	**Ledger**	11.8
Binance	9.1	Crypto.com	8.6
Robinhood Crypto	9.1	Robinhood Crypto	7.5
Gemini	6.1	PayPal Crypto	7.5
Trust Wallet	6.1	**Trust Wallet**	5.4
Exodus	6.1	Kraken	5.4
Webull Crypto	4.5	Binance US	4.3

Table 5 in Appendix B lists the newly adopted wallets among custody-unaware and custody-aware participants. Hardware NCWs, such as Ledger and Trezor, were particularly favored by custody-aware participants: Ledger's adoption rate rose to 20.0%, compared to just 4.2% among custody-unaware users. This indicates that failures of centralized exchanges, exemplified by the FTX collapse, may have motivated users with a clear mental model of wallet custody to seek stronger security measures, such as those offered by hardware wallets. However, a closer investigation revealed that only 17.4% of participants who adopted new NCWs were first-time NCW users, with the majority of new adoptions coming from those already familiar with NCWs. Taken together, while the FTX collapse appears to have elevated NCW adoption, its impact on initiating first-time NCW use may have been limited.

Crypto transfer decision. We asked participants whether they *transferred* their crypto after learning about the incident. Consistent with the interview findings, most survey participants (70.7%) did not transfer their crypto following the incident. However, FTX users were more inclined to make transfers, and a Chi-squared test confirmed that this behavior significantly differed from that of non-FTX users ($\chi^2(1, N = 280) = 23.89$, $p < 0.001$). Conversely, statistical tests revealed no significant difference in transfer decisions between custody-aware and unaware participants.

Reasons for no transfer. Figure 5 presents reasons, ranked by weighted importance, for participants' decisions not to transfer crypto after the incident. Similar to the interview findings, participants most commonly cited insufficient crypto holdings as the primary reason for not transferring. The second leading reason was participants' trust in the NCWs they were using. However, among those who prioritized this reason, 16.9% did not actually use an NCW, as confirmed by their reported wallet list. More alarmingly, 30.0% of these participants actively used non-SEC-compliant CWs. This means they continued to face greater risks linked to centralized exchanges while mistakenly believing they were using NCWs with complete control over their assets. Third, 52.5% of participants who selected TRUST MY CWs as their most important reason were using non-SEC-compliant CWs. Among this group, 61.9% stored over half of

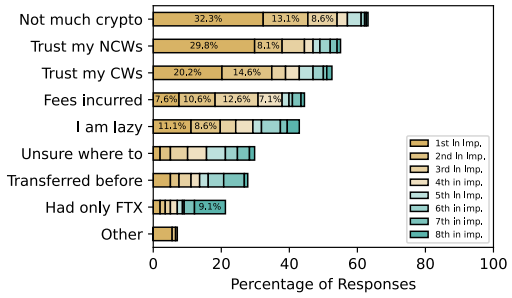


Figure 5: Reasons for survey participants not transferring funds after the incident.

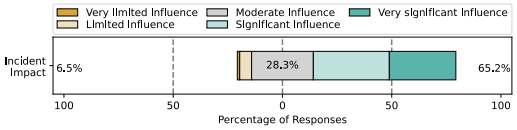


Figure 6: Perceived influence of the incident among survey participants who transferred funds.

their total assets in such noncompliant CWs, 47.6% stored more than 75%, and notably, 28.6% entrusted their entire holdings, exposing themselves to risks similar to the FTX collapse.

Crypto transfer flow. For participants who altered their asset storage after the FTX collapse, Figure 6 highlights the incident's significant role in motivating transfers. We also collected data on wallets involved in both inflows and outflows of crypto transfers. Figure 7 depicts the most common transfer patterns, with a 3.0% threshold for clarity, where the node size corresponds to the weighted degree[6]. The most dominant transfer flow was observed among 24.7% of participants who cashed out their crypto from Coinbase. Transfer patterns from other CWs, including Binance (US), to bank accounts were also prevalent.

Notably, the Chi-squared test revealed that turning to banks was more evident among CW-only users, as their outflow destinations differed significantly ($\chi^2(2, N = 156) = 7.92$, $p = 0.02$) from those using at least one NCW. Specifically, 83.3% of CW-only users who made transfers included banks as a destination, and 90.0% of them transferred exclusively to banks. We initially hypothesized that this behavior was due to most CW-only users using a single CW, leaving them no other choice but to cash out. However, among CW-only users who exclusively transferred to banks, the majority (72.2%) were actually using multiple CWs. These observations suggest that the FTX collapse led to a notable decline in confidence in CWs among many CW-only users, motivating them to fall back to traditional banks over any CWs. Lastly, we did not observe such differences in transfer destinations between custody-aware and custody-unaware participants.

[6]The weighted node degree is the sum of the edge weights for edges incident to that node.

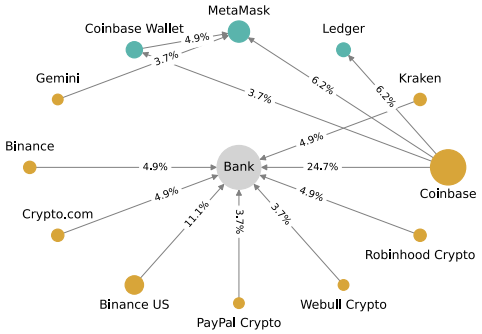


Figure 7: Post-incident crypto transfer flows reported by survey participants. Directed edges represent the direction of transfers between wallets and banks, with edge weights indicating the percentage of participants who reported each transfer. Node sizes are proportional to the total transfer activity (sum of incoming and outgoing amounts). Node colors distinguish CWs (shown in orange) from NCWs (shown in teal).

6 Discussions

In this section, we provide a summary of the concerning group of crypto users identified in the two studies, offer actionable recommendations, and discuss the limitations of our work.

6.1 Concerning User Groups

We outline several concerning insights derived from the two studies—drawing primarily on our survey results, which largely align with the interview findings—that we believe have important implications for the broader crypto security community. The majority of participants failed to correctly identify the type of wallets they used, and only a small portion were aware that the private keys to their crypto assets were actually held by centralized exchanges when using CWs.

Regarding RQ1, becoming aware of the FTX collapse resulted in an overall decrease in crypto users' trust in CWs, along with a slight increase in their perception of NCW security. Notably, former FTX users were more likely to develop negative views about the security of both wallet types. Unexpectedly, some participants cited anticipated regulatory enhancements that might follow the incident as a reason for feeling more secure about using CWs. Additionally, we found that misinterpreting the cause of the centralized exchange incident could exacerbate users' negative shifts in perceived NCW security.

Regarding RQ2, shifts in participants' security perceptions did not always lead to sufficient risk mitigation: most users neither explored alternative wallet options nor moved their crypto assets to more reliable wallets (e.g., SEC-compliant CWs or well-established NCWs). A commonly cited reason, "trusting current wallets" indicated concerning security practices. Notably, a significant portion of users who trusted their CWs were using non-SEC-compliant CWs, and used them to store all their crypto assets. Another concerning group included

users who reported trusting their NCWs but turned out to be CW-only users, some of them using non-SEC-compliant CWs—those users may have falsely believed they had full control over their assets through self-custody. Within the small number of users who engaged in risk mitigation actions, some exhibited desirable behavioral changes. Such participants started using NCWs or SEC-compliant CWs after learning about the incident. However, learning about the FTX collapse had a modest impact on motivating CW-only users to transition to NCWs for the first time.

6.2 Recommendations

Enforce active custody verification. Our findings revealed a critical knowledge gap: 56.5% of participants could not correctly identify their wallet types, and only 35.3% understood that CWs hold their private keys. To timely fix this incorrect mental model, wallet providers need to move on from passive textual explanations that are prone to issues of habituation [4]. Instead, based on the concept of *beneficial friction* [14], we recommend implementing mandatory custody-verification steps during the wallet onboarding process. User interfaces should require users to actively confirm the correct custody method (e.g., "Exchange controls keys" vs. "I control keys") before continuing with the next onboarding steps. This mandatory cognitive step helps users establish an accurate understanding of asset control from the initial wallet onboarding phase, directly addressing the common misconceptions identified in our study. However, given that users often struggle to understand cryptographic concepts [51], the effectiveness of such mandatory steps is not guaranteed and should be examined through future empirical studies.

Action-first disclosures. Our work identified that most participants did not transfer their crypto assets after learning about the FTX incident. As Zou *et al.* [53] show, vague and overloaded data breach notifications often lead to user inaction. Therefore, we argue that incident disclosures should prioritize *actionability* over *comprehensiveness*. Drawing from security warning research [16], which suggests that concrete instructions significantly improve user adherence, breached exchanges should feature an imperative instruction at the top of a message (e.g., "Withdraw available funds as soon as possible!") before providing detailed and technical explanations of the incident. We envision these directives being issued when sending alert emails or messages, or shown directly to affected users when they log in to victim exchanges.

Standardize the content of incident reports. Our studies found that users often misunderstood the causes and scope of centralized exchange breaches, at times leading to undesirable behaviors such as moving assets to other noncompliant platforms with similar risks. To mitigate this, incident reports—whether issued by affected exchanges or news organizations—should follow a more standardized format with key elements: a concrete exposure timeline, a plain-language explanation of the root cause, a summary of affected user groups and asset types, and an easy-to-follow guide for securing wallets, identifying compliant CWs, and safely migrating crypto. A prior work on "Privacy Nutrition Label" [26] reinforces the effectiveness of using standardized formats. Such reports can help users assess risks in the services they use and take timely, informed mitigation actions. Regulators may consider establishing standardized, user-focused disclosure templates for licensed platforms to follow when reporting major breaches.

To support and motivate wallet providers and exchanges to adopt these recommendations above and comply with SEC requirements, we propose that regulators manage a wallet/exchange reliability review platform. This platform would be used by crypto users when choosing a wallet. It would provide details on SEC compliance, the adoption of standardized incident reporting, and adherence to industry-standard security protocols for protecting users' accounts and assets.

6.3 Limitations

The empirical nature of this work introduces certain limitations. First, our analysis relies on self-reported data, which can occasionally be inaccurate or incomplete. For example, although we provided a list of popular wallets and allowed free-text responses, participants may have left out options or opted not to disclose all wallets in use. This limitation may have affected follow-up analyses, including the identification of CW-only or NCW-only users. Second, the retrospective nature of reporting perception and behavior changes related to a past event inherently limits the recall accuracy. To reduce this risk, our interview screening excluded participants without prior knowledge of the FTX collapse. We also removed responses from survey participants who could not correctly remember their FTX and other wallet adoption dates and usage periods (e.g., reporting use before the wallet launch date). Due to these strict validation criteria, recruiting and studying eligible FTX users was challenging and time-consuming, with each study phase taking several months.

Third, many participants reported low trading activity, with 44.2% of survey respondents holding total crypto assets below 1,000 USD. While this may raise concerns about representativeness, statistical tests found no significant perception or behavior differences between users above and below this asset threshold, suggesting our findings may still be informative across user segments. Fourth, to ensure the internal validity of our analysis of perceptions across different wallet types, we excluded responses from participants who misidentified their wallet type. As a result, this approach may reduce generalizability by potentially under-representing users with limited knowledge of wallet types and their differences. Fifth, participants may have also experienced other crypto-related events or read articles about security breaches involving other CWs and NCWs, and based on the applied methodology, it is infeasible to independently analyze the sole effects of users being exposed to the FTX incident details. To ensure participants focused exclusively on the context of the FTX scam, we designed the entire interview and survey questions to center around the FTX incident, including prompts for participants to leave items unchecked if they seem unrelated to the FTX

incident. This work does not seek to establish a strict/sole causal relationship between the FTX incident and security perception changes, but aims to document a highly probable outcome of being exposed to the FTX scam based on participants' self-reported perception changes and strong emphasis on the event details. Lastly, as the underlying causes and security implications of the FTX incident may vary from those of other notable centralized exchange events (e.g., the recent Coinbase data breach [12]), our findings on users' security perception and behavioral changes should be generalized with caution and may not directly apply to other incidents.

7 Conclusion

This study presents the first systematic investigation of how crypto users' security perceptions and behaviors evolved following the FTX collapse. Our findings reveal that while trust in CWs generally declined and perceptions of NCW security improved, these shifts rarely led to corresponding behavioral changes. Most users did not transfer their assets or adopt new NCWs, often citing insignificant crypto holdings or continued trust in their current CWs. An important finding is that many users fundamentally misunderstood wallet custody—only about one-third correctly recognized that exchanges control users' private keys in CWs. When CW users took action, they frequently transferred assets to traditional banks rather than exploring SEC-compliant CW or NCW alternatives, indicating a mere loss of trust in centralized crypto services instead of a shift toward self-custody alternatives. The persistence of these fundamental misconceptions suggests that current risk communication practices are insufficient to support informed risk mitigation and safe wallet selection. To bridge this gap, we propose exploring behaviorally grounded interventions, such as *mandatory custody verification* during onboarding and *action-first*, *standardized* incident disclosures. Future work should evaluate the efficacy of these design strategies in helping users better understand wallet risks and take timely protective actions.

Acknowledgments

We would like to express our appreciation to the interview and survey participants for sharing their experiences and insights. We also thank the anonymous reviewers for their constructive feedback on this paper. This work was supported by the Sui Foundation, Samsung, and the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korean government (MSIT) (No. RS-2023-00229400 and No. RS-2024-00459638).

References

[1] Svetlana Abramova, Artemij Voskobojnikov, Konstantin Beznosov, and Rainer Böhme. 2021. Bits Under the Mattress: Understanding Different Risk Perceptions and Security Behaviors of Crypto-Asset Users. In *Proceedings of the 2021 ACM Conference on Human Factors in Computing Systems (CHI)*. Yokohama, Japan.

[2] Bhupendra Acharya, Muhammad Saad, Antonio Emanuele Cinà, Lea Schönherr, Hoang Dai Nguyen, Adam Oest, Phani Vadrevu, and Thorsten Holz. 2024. Conning the Crypto Conman: End-to-end Analysis of Cryptocurrency-based Technical Support Scams. In *Proceedings of the 45th IEEE Symposium on Security and Privacy (Oakland)*. San Francisco, CA.

[3] Erdinc Akyildirim, Thomas Conlon, Shaen Corbet, and John W Goodell. 2023. Understanding the FTX exchange collapse: A dynamic connectedness approach. *Finance Research Letters* 53 (2023), 103643.

[4] Bonnie Anderson, Anthony Vance, C Brock Kirwan, Jeffrey L Jenkins, and David Eargle. 2016. From warning to wallpaper: Why the brain habituates to security warnings and what can be done about it. *Journal of Management Information Systems* 33, 3 (2016), 713–743.

[5] Daniela Balutel, Marie-Hélène Felt, Gradon Nicholls, and Marcel-Cristian Voia. 2024. Bitcoin Awareness, Ownership and Use: 2016–20. *Applied Economics* 56, 1 (2024), 33–58.

[6] Binance News. 2025. From Our CEO: 8 Years of the Community That Built Binance. https://www.binance.com/en/blog/from-our-ceo/410079164840 8331081.

[7] Elie Bouri, Elham Kamal, and Harald Kinateder. 2023. FTX Collapse and systemic risk spillovers from FTX Token to major cryptocurrencies. *Finance Research Letters* 56 (2023), 104099.

[8] Business Insider. 2024. Some wealthy people lost millions in the FTX collapse. But others say they've lost their entire life savings. https://www.businessinsider.com/ftx-collapse-sam-bankman-fried-victime-impact-statements-prosecutors-sentencing-2024-3.

[9] Sandy Carter. 2025. Latest On The Bybit Record Breaking 1.4 Billion Dollar Crypto Hack. https://www.forbes.com/sites/digital-assets/2025/02/21/latest-on-the-bybit-record-breaking-14-billion-dollar-crypto-hack/.

[10] Coinbase. 2024. Is a Crypto Address Linked to My Coinbase Account Safe to Display Publicly? https://help.coinbase.com/en/coinbase/privacy-and-security/other/is-a-crypto-address-safe-to-display-publicly.

[11] Coinbase. 2024. What Is a Private Key? https://www.coinbase.com/learn/crypto-basics/what-is-a-private-key.

[12] Coinbase. 2025. Protecting Our Customers - Standing Up to Extortionists. https://www.coinbase.com/blog/protecting-our-customers-standing-up-to-extortionists.

[13] Thomas Conlon, Shaen Corbet, and Yang Hu. 2023. The Collapse of FTX: The End of Cryptocurrency's Age of Innocence. *The British Accounting Review* (2023), 101277.

[14] Anna L Cox, Sandy JJ Gould, Marta E Cecchinato, Ioanna Iacovides, and Ian Renfree. 2016. Design frictions for mindful interactions: The case for microboundaries. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. 1389–1397.

[15] Shayan Eskandari, Jeremy Clark, David Barrera, and Elizabeth Stobert. 2018. A First Look at the Usability of Bitcoin Key Management. *arXiv preprint arXiv:1802.04351* (2018).

[16] Adrienne Porter Felt, Alex Ainslie, Robert W. Reeder, Sunny Consolvo, Somas Thyagaraja, Alan Bettes, Helen Harris, and Jeff Grimes. 2015. Improving SSL Warnings: Comprehension and Adherence. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 2893–2902. doi:10.1145/2702123.2702442

[17] Joseph L Fleiss, Bruce Levin, and Myunghee Cho Paik. 2013. *Statistical Methods for Rates and Proportions*. John Wiley & Sons.

[18] Michael Froehlich, Philipp Hulm, and Florian Alt. 2021. Under Pressure. A User-Centered Threat Model for Cryptocurrency Owners. In *Proceedings of the 2021 4th International Conference on Blockchain Technology and Applications*. 39–50.

[19] Shange Fu, Qin Wang, Jiangshan Yu, and Shiping Chen. 2023. FTX Collapse: A Ponzi Story. In *Proceedings of the 2023 International Conference on Financial Cryptography and Data Security (FC)*. Bol, Brač, Croatia.

[20] Greg Guest, Kathleen M MacQueen, and Emily E Namey. 2011. *Applied Thematic Analysis*. Sage Publications.

[21] Hacken. 2024. The Hacken 2024 Web3 Security Report. https://wp.hacken.io/wp-content/uploads/2024/12/2024-Web3-Security-Report.pdf.

[22] Sallee Ann Harrison. 2024. A Timeline of the Collapse at FTX. https://apnews.com/article/ftx-bankruptcy-binance-timeline-c519d50b9059aa8bff0ce8b6cd26c40e.

[23] Greg Hou. 2021. Cryptocurrency Money Laundering and Exit Scams: Cases, Regulatory Responses and Issues. *Understanding Cryptocurrency Fraud* (2021), 83.

[24] Sabine Houy, Philipp Schmid, and Alexandre Bartel. 2023. Security Aspects of Cryptocurrency Wallets—A Systematic Literature Review. *ACM Computing Surveys (CSUR)* (2023).

[25] Aaron Katersky. 2024. Disgraced former FTX CEO Sam Bankman-Fried sentenced to 25 years for financial fraud, must forfeit $11 billion for victims. https://abcnews.go.com/US/sam-bankman-fried-sentenced-thursday-financial-fraud/story?id=108554809.

[26] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W Reeder. 2009. Standardizing privacy notices: an online study of the nutrition label approach. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 1573–1582.

[27] Lydia Kraus, Ina Wechsung, and Sebastian Möller. 2014. A Comparison of Privacy and Security Knowledge and Privacy Concern as Influencing Factors for Mobile Protection Behavior. In *Workshop on Privacy Personas and Segmentation*.

[28] Katharina Krombholz, Aljosha Judmayer, Matthias Gusenbauer, and Edgar Weippl. 2016. The Other Side of the Coin: User Experiences with Bitcoin Security and Privacy. In *Proceedings of the 2016 International Conference on Financial Cryptography and Data Security (FC)*. Christ Church, Barbados.

[29] Ledger. 2023. Crypto Proof of Reserves – A Guide. https://www.ledger.com/academy/crypto-proof-of-reserves-audit.

[30] Ledger. 2023. Proof of Reserves (PoR). https://www.ledger.com/academy/glossary/proof-of-reserves-por.

[31] Makayla Lewis and Mark Perry. 2019. Follow the Money: Managing Personal Finance Digitally. In *Proceedings of the 2019 ACM Conference on Human Factors in Computing Systems (CHI)*. Glasgow, Scotland, UK.

[32] Lingyuan Li, Guo Freeman, and Bart Knijnenburg. 2024. Beyond Just Money Transactions: How Digital P2P Payments (Re)shape Existing Offline Interpersonal Relationships. *Proceedings of the ACM on Human-Computer Interaction* 8, CSCW1 (2024). https://doi.org/10.1145/3637301

[33] Xigao Li, Anurag Yepuri, and Nick Nikiforakis. 2023. Double and Nothing: Understanding and Detecting Cryptocurrency Giveaway Scams. In *Proceedings of the 2023 Annual Network and Distributed System Security Symposium (NDSS)*. San Diego, CA.

[34] Mingyi Liu, Jun Ho Huh, HyungSeok Han, Jaehyuk Lee, Jihae Ahn, Frank Li, Hyoungshick Kim, and Taesoo Kim. 2024. I Experienced More than 10 DeFi Scams: On DeFi Users' Perception of Security Breaches and Countermeasures. In *Proceedings of the 33rd USENIX Security Symposium (Security)*. Philadelphia, PA.

[35] Alexandra Mai, Katharina Pfeffer, Matthias Gusenbauer, Edgar Weippl, and Katharina Krombholz. 2020. User Mental Models of Cryptocurrency Systems - A Grounded Theory Approach. In *Proceedings of the 2020 USENIX Symposium on Usable Privacy and Security (SOUPS)*. Virtual.

[36] Alana Maurushat and Dan Halpin. 2022. Investigation of Cryptocurrency Enabled and Dependent Crimes. In *Financial Technology and the Law: Combating Financial Crime*. Springer, 235–267.

[37] Peter Mayer, Yixin Zou, Byron M. Lowens, Hunter A. Dyer, Khue Le, Florian Schaub, and Adam J. Aviv. 2023. Awareness, Intention, (In)Action: Individuals' Reactions to Data Breaches. *ACM Transactions on Computer-Human Interaction* 30, 5 (2023). https://doi.org/10.1145/3589958

[38] MetaMask. 2024. How Can I Reset My Password? https://support.metamask.io/managing-my-wallet/resetting-deleting-and-restoring/how-can-i-reset-my-password/.

[39] Satoshi Nakamoto. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf.

[40] Nathan Reiff. 2024. The Collapse of FTX: What Went Wrong With the Crypto Exchange? https://www.investopedia.com/what-went-wrong-with-ftx-6828447.

[41] Tanusree Sharma, Vivek C Nair, Henry Wang, Yang Wang, and Dawn Song. 2024. 'I Can't Believe It's Not Custodial!': Usable Trustless Decentralized Key Management. In *Proceedings of the 2024 ACM Conference on Human Factors in Computing Systems (CHI)*. Honolulu, HI.

[42] Camomile Shumba. 2022. US Justice Department Wants FTX Fraud Allegations to Be Investigated. https://www.coindesk.com/policy/2022/12/02/us-justice-department-wants-ftx-fraud-allegations-to-be-investigated/.

[43] Janice Jianing Si, Tanusree Sharma, and Kanye Ye Wang. 2024. Understanding User-Perceived Security Risks and Mitigation Strategies in the Web3 Ecosystem. In *Proceedings of the 2024 ACM Conference on Human Factors in Computing Systems (CHI)*. Honolulu, HI.

[44] Yoshifumi Takemoto and Sophie Knight. 2014. Mt. Gox files for bankruptcy, hit with lawsuit. https://www.reuters.com/article/business/mt-gox-files-for-bankruptcy-hit-with-lawsuit-idUSBREA1R0FX/.

[45] The U.S. Securities and Exchange Commission. 2025. Exchange Act Reporting and Registration. https://www.sec.gov/resources-small-businesses/going-public/exchange-act-reporting-registration.

[46] The White House. 2025. Fact Sheet: President Donald J. Trump Establishes the Strategic Bitcoin Reserve and U.S. Digital Asset Stockpile. https://www.whitehouse.gov/fact-sheets/2025/03/fact-sheet-president-donald-j-trump-establishes-the-strategic-bitcoin-reserve-and-u-s-digital-asset-stockpile/.

[47] U.S. Department of Justice. 2024. Samuel Bankman-Fried Sentenced to 25 Years for His Orchestration of Multiple Fraudulent Schemes. https://www.justice.gov/opa/pr/samuel-bankman-fried-sentenced-25-years-his-orchestration-multiple-fraudulent-schemes.

[48] David Vidal-Tomás, Antonio Briola, and Tomaso Aste. 2023. FTX's downfall and Binance's consolidation: The fragility of centralised digital finance. *Physica A: Statistical Mechanics and Its Applications* 625 (2023), 129044.

[49] Artemij Voskobojnikov, Borke Obada-Obieh, Yue Huang, and Konstantin Beznosov. 2020. Surviving the Cryptojungle: Perception and Management of Risk Among North American Cryptocurrency (Non)Users. In *Proceedings of the 2020 International Conference on Financial Cryptography and Data Security (FC)*. Kota Kinabalu, Malaysia.

[50] Artemij Voskobojnikov, Oliver Wiese, Masoud Mehrabi Koushki, Volker Roth, and Konstantin Beznosov. 2021. The U in Crypto Stands for Usable: An Empirical Study of User Experience with Mobile Cryptocurrency Wallets. In *Proceedings of the 2021 ACM Conference on Human Factors in Computing Systems (CHI)*. Yokohama, Japan.

[51] Justin Wu and Daniel Zappala. 2018. When is a Tree Really a Truck? Exploring Mental Models of Encryption. In *Proceedings of the 2018 USENIX Symposium on Usable Privacy and Security (SOUPS)*. Baltimore, MD.

[52] Yaman Yu, Tanusree Sharma, Sauvik Das, and Yang Wang. 2024. 'Don't put all your eggs in one basket': How Cryptocurrency Users Choose and Secure Their Wallets. In *Proceedings of the 2024 ACM Conference on Human Factors in Computing Systems (CHI)*. Honolulu, HI.

[53] Yixin Zou, Shawn Danino, Kaiwen Sun, and Florian Schaub. 2019. You 'Might' Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications. In *Proceedings of the 2019 ACM Conference on Human Factors in Computing Systems (CHI)*. Glasgow, Scotland, UK.

A Supplementary Analysis: Wallet Recovery Misunderstandings

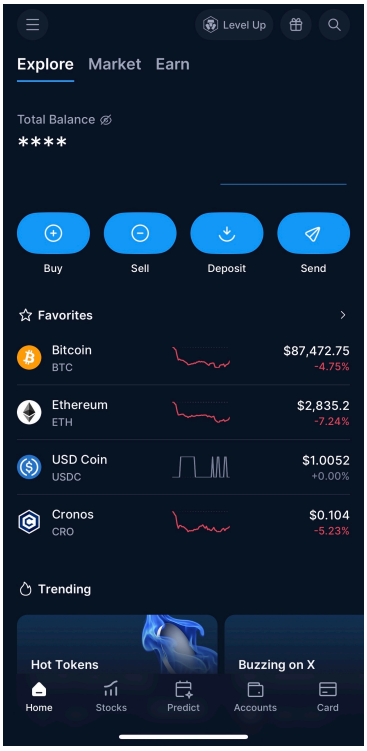
Interview findings. Almost all participants understood that their CW passwords could be recovered or reset if lost, through other user-controlled factors such as an email or phone number. While NCW passwords can also be reset [38] and most participants were aware, many mistakenly described the reset process as similar to that of the CW scenario. Only a few participants correctly noted that resetting an NCW password requires access to the private key or secret recovery phrases: *"If I forget the password, I have to provide the [secret recovery] phrases"* (P20). However, if the SRPs for an NCW are lost, they cannot be recovered. Nonetheless, a considerable portion of participants mistakenly believed that lost SRPs could still be retrieved.

Survey findings. Echoing the interview study, Table 3 shows that most participants (75.8%) knew CW passwords could be reset, as ownership can be verified through identity information provided to the exchange. Yet, only 40.9% correctly believed that NCW passwords could also be reset or recovered—an option available if users retain access to their secret recovery phrases or private keys [38]. This suggests that crypto users have limited understanding of NCW recovery mechanisms.

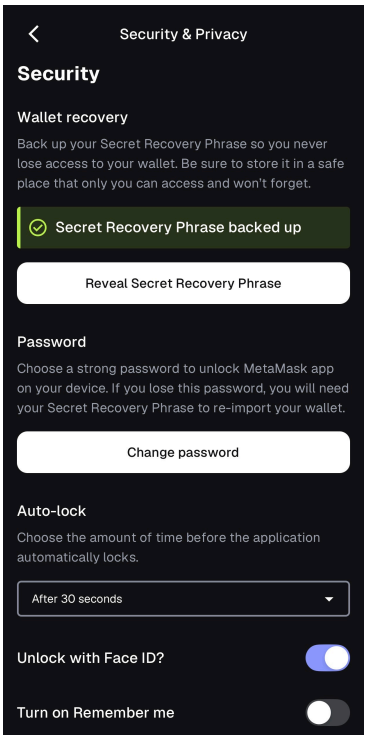
B Supplementary Figures and Tables

Table 5: The top ten wallets adopted by survey participants after the incident, with non-custodial wallets in bold text.

Custody-Unaware Users	(%)	Custody-Aware Users	(%)
Coinbase	20.8	Coinbase	24.4
Coinbase Wallet	16.7	**Ledger**	20.0
MetaMask	12.5	**MetaMask**	15.6
Robinhood Crypto	8.3	PayPal Crypto	11.1
Crypto.com	6.3	Crypto.com	11.1
Trust Wallet	6.3	Kraken	8.9
Binance US	6.3	**Coinbase Wallet**	8.9
Webull Crypto	4.2	Binance	6.7
PayPal Crypto	4.2	Robinhood Crypto	6.7
Ledger	4.2	**Trezor**	6.7

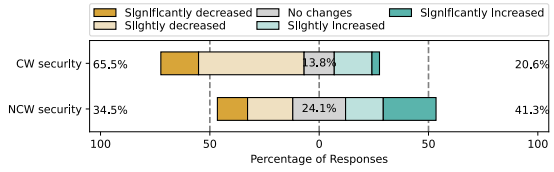


(a) Example interface from the Crypto.com mobile app (a CW). The home dashboard resembles a centralized exchange platform, displaying the user's portfolio and providing options to buy, sell, deposit, and send crypto assets. (© Crypto.com, used for illustrative purposes.)

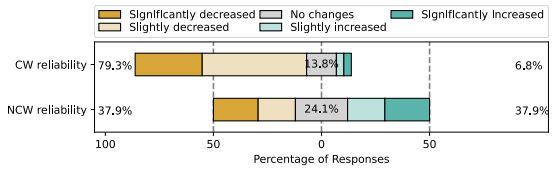


(b) Example interface from the MetaMask mobile app (an NCW). This screen illustrates how NCWs give users full control over wallet recovery and access, including managing the secret recovery phrase and local password settings. (© MetaMask, used for illustrative purposes.)

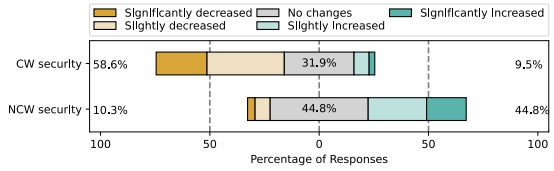
Figure 8: Representative mobile interfaces of a CW (Crypto.com, left) and an NCW (MetaMask, right), included to complement the technical diagrams in Figure 1.



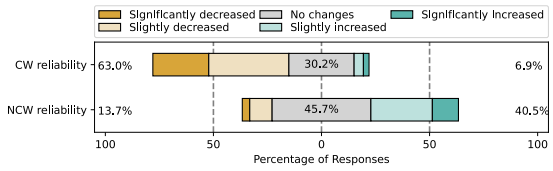
(a) Change in perception of *security* - FTX users



(b) Change in perception of *reliability* - FTX users



(c) Change in perception of *security* - non-FTX users



(d) Change in perception of *reliability* - non-FTX users

Figure 9: Changes in survey participants' perceptions of Custodial Wallet (CW) and Non-Custodial Wallet (NCW), grouped by FTX users and non-FTX users.

Table 6: Interview participants' demographics, wallet usage, and knowledge scores (out of 10), with (*a*, *b*) indicating points for crypto fundamentals and security practices, respectively.

ID	Gender	Age	Education	Income	Crypto Value	Crypto YoE	CW User	NCW User	FTX User	Knowl. Score
P1	Male	45-54	High school	$25k-50k	$0-1k	1-3	Yes	Yes	No	7 (3, 4)
P2	Female	45-54	Bachelor's	$25k-50k	$0-1k	3-5	Yes	Yes	No	9 (4, 5)
P3	Male	18-24	Bachelor's	$75k-100k	$0-1k	1-3	Yes	No	No	N/A
P4	Male	35-44	High school	<$25k	$1k-10k	1-3	Yes	Yes	Yes	7 (4, 3)
P5	Male	25-34	Bachelor's	$125k-150k	$0-1k	1-3	Yes	No	Yes	8 (4, 4)
P6	Male	25-34	High school	<$25k	$0-1k	3-5	Yes	Yes	Yes	9 (4, 5)
P7	Male	45-54	High school	$50k-75k	$0-1k	7-9	Yes	Yes	No	8 (4, 4)
P8	Male	25-34	After bachelor's	>$200k	>$100k	5-7	Yes	Yes	No	8 (3, 5)
P9	Male	55-64	After bachelor's	$100k-125k	$1k-10k	3-5	Yes	Yes	Yes	6 (2, 4)
P10	Male	25-34	Bachelor's	$50k-75k	$1k-10k	1-3	Yes	Yes	No	5 (2, 3)
P11	Male	35-44	Bachelor's	<$25k	$1k-10k	7-9	Yes	Yes	Yes	9 (4, 5)
P12	Female	35-44	After bachelor's	$125k-150k	$0-1k	3-5	Yes	Yes	No	8 (3, 5)
P13	Male	25-34	Bachelor's	$150k-175k	$1k-10k	3-5	Yes	Yes	No	7 (4, 3)
P14	Other	25-34	High school	$25k-50k	$10k-100k	7-9	Yes	Yes	No	9 (5, 4)
P15	Female	45-54	After bachelor's	$25k-50k	$1k-10k	3-5	Yes	Yes	No	9 (4, 5)
P16	Male	18-24	Bachelor's	$25k-50k	$0-1k	1-3	Yes	Yes	Yes	6 (2, 4)
P17	Other	18-24	High school	<$25k	$0-1k	7-9	Yes	Yes	No	10 (5, 5)
P18	Female	55-64	Bachelor's	$50k-75k	$0-1k	1-3	No	Yes	No	1 (0, 1)
P19	Female	35-44	Bachelor's	$50k-75k	$0-1k	1-3	Yes	Yes	No	7 (3, 4)
P20	Female	55-64	After bachelor's	$100k-125k	$10k-100k	> 9	Yes	Yes	No	9 (4, 5)
P21	Other	25-34	Bachelor's	$50k-75k	$0-1k	3-5	Yes	Yes	No	9 (4, 5)
P22	Female	35-44	After bachelor's	$50k-75k	$0-1k	5-7	Yes	Yes	Yes	9 (4, 5)