"Don't Put All Your Eggs In One Basket": How Cryptocurrency Users Choose and Secure Their Wallets

Yaman Yu
yamanyu2@illinois.edu
Information Sciences, University of Illinois at Urbana-Champaign
Champaign, USA

Tanusree Sharma
tsharma6@illinois.edu
Informatics, University of Illinois at Urbana-Champaign
Champaign, USA

Sauvik Das
sauvik@cmu.edu
Human-Computer Interaction Institute, Carnegie Mellon University
Pittsburgh, USA

Yang Wang
yvw@illinois.edu
Information Sciences, University of Illinois at Urbana-Champaign
Champaign, USA

ABSTRACT

Cryptocurrency wallets come in various forms, each with unique usability and security features. Through interviews with 24 users, we explore reasons for selecting wallets in different contexts. Participants opt for smart contract wallets to simplify key management, leveraging social interactions. However, they prefer personal devices over individuals as guardians to avoid social cybersecurity concerns in managing guardian relationships. When engaging in high-stakes or complex transactions, they often choose browser-based wallets, leveraging third-party security extensions. For simpler transactions, they prefer the convenience of mobile wallets. Many participants avoid hardware wallets due to usability issues and security concerns with respect to key recovery service provided by manufacturer and phishing attacks. Social networks play a dual role: participants seek security advice from friends, but also express security concerns in soliciting this help. We offer novel insights into how and why users adopt specific wallets. We also discuss design recommendations for future wallet technologies based on our findings.

CCS CONCEPTS

• **Human-centered computing** → **User studies**; • **Security and privacy** → *Social aspects of security and privacy*; • **Information systems** → Digital cash.

KEYWORDS

Cryptocurrency, blockchain, crypto wallets, security, privacy, user behavior

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

ACM ISBN 979-8-4007-0330-0/24/05
https://doi.org/10.1145/3613904.3642534

ACM Reference Format:
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 CHI Conference on Human Factors in Computing Systems (CHI '24), May 11–16, 2024, Honolulu, HI, USA.* ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/3613904.3642534

1 INTRODUCTION

Cryptocurrency has seen a significant surge in popular interest. According to data from Coinmarketcap [8], as of September 2023, the market capitalization of all cryptocurrencies exceeds 1 trillion USD. To interact with blockchains and cryptocurrencies, users typically use crypto wallets. Over the past decade, many different types of crypto wallets have been proposed and implemented: hardware-based wallets and software-based wallets, custodial wallets and non-custodial wallets, smart contract wallets, and externally owned accounts [1]. Each of these wallets has benefits and drawbacks for both usability and security [32]. Accordingly, the decision-making process for users — in choosing which wallet(s) to use and for what purpose — has become progressively more complex. Our work provides clarity: we contribute an analysis of why users choose the cryptocurrency wallets they use, and how usability and security considerations factored into that decision-making process.

Recent studies have delved into the risk perceptions and wallet usage behaviors of cryptocurrency users [1, 15, 29, 39, 46]. A majority of these investigations have centered on classifying the perceived risks of both users and non-users, exposing misconceptions related to security, privacy, and anonymity [15, 29, 39, 46]. Subsequent research highlighted behaviors like the concurrent use of multiple wallets and security practices associated with them [1, 15]. Yet, the factors that guide why users choose the wallets they use remain underexplored. This understanding is critical: wallet choice is one of the most significant security decisions that end-users make when interacting with cryptocurrencies. Choosing a custodial wallet means that users are shielded from phishing attacks, but vulnerable to counterparty risk (e.g., the custodian mismanaging their funds or getting hacked). Choosing a hardware wallet means users are shielded from malware risks, but vulnerable to physical

[1] Detailed definitions and explanations of these wallets can be found in Section 2.

world theft and damage. Our research aims to delve into users' experiences and the reasons behind their wallet choices, emphasizing two key dimensions: wallet type and associated devices. We focus on three research questions:

- RQ1: How and why do users use different wallets?
- RQ2: How do users perceive privacy/security risks across different crypto wallets?
- RQ3: How do users apply security measures for different crypto wallets across different devices?

Findings. To answer these questions, we conducted semi-structured interviews with 24 crypto users. To answer RQ1, participants choose wallets based in part on use-case, their prior experience, and their perceptions of security and risk. Notably, for larger transactions or long-term storage, participants leaned towards smart-contract or hardware wallets because they were perceived as having strong security. When dealing with high-stakes or complex transactions, such as interacting with dapps (decentralized applications), participants preferred browser-based self-custodial wallets because these wallets allow for the use of third-party security extensions and provide more screen space for verifying transaction details. Participants also discussed using multiple wallets to distribute their crypto assets and isolate the risk associated with any one wallet getting compromised.

To answer RQ2, participants understood and expressed that different wallet types had different security risks and benefits. For example, while hardware wallets are popularly considered the gold standard for wallet security, participants expressed concern that hardware wallet providers might hold users' private keys and do not provide adequate protection against phishing/scams. In contrast, participants felt that smart contract wallets offered the same or greater level of security relative to hardware wallets owing, in large part, to the availability of social cybersecurity features.

To answer RQ3, we found that participants frequently applied social cybersecurity measures [35, 49] — e.g., social recovery, multi-signature, and soliciting guidance from friends. However, there was a clear desire among participants for more granular social cybersecurity controls to address the new risks and trust dilemmas that arose out of their reliance on social cybersecurity measures.

Contributions. This paper offers three primary contributions: (1) We provide novel insights into *why and how users select specific wallet types* among numerous options. We delve into how users' choices and decision-making processes are influenced by their perceptions of wallet usability, security, and social factors (as summarized in Table 3).

(2) Our research highlights unique security measures among users of different cryptocurrency wallets. Significantly, there is an emerging trend among users to employ extra personal devices of their own as security measures (i.e., guardian accounts) for their smart contract wallets, rather than relying on other people as guardians. Moreover, the incorporation of security extensions in PC browser wallets is becoming increasingly popular. These novel approaches have not been reported in the prior literature.

(3) Building on our findings, we discuss design implications regarding wallet security features and strategies to deliver user-centered, secure wallets.

2 BACKGROUND AND TERMINOLOGY

Blockchain technologies have rapidly evolved since inception, marked by the introduction of Nakamoto's Bitcoin Protocol in 2008 [37, 43]. Initially, Blockchain 1.0 was primarily associated with cryptocurrencies such as Bitcoin, enabling the secure transfer of digital assets [4, 43]. While Bitcoin remains the most popular cryptocurrency, this phase has witnessed the emergence of numerous others such as Dogecoin, Litecoin, and Monero, highlighting the versatile applications of blockchain technology in the realm of digital currencies and payments.

Blockchain 2.0 introduced a paradigm shift by differentiating Bitcoin as a digital asset and the blockchain as a programmable distributed trust infrastructure [4, 43]. Notably, the Ethereum platform, the second-largest blockchain established in 2015, exemplified this functionality. Smart contracts, a fundamental concept in Blockchain 2.0, are self-executing contracts with predefined rules and conditions written in code. With the capacity for smart contract development, Blockchain 2.0 paved the way for more intricate interactions and diverse applications within the blockchain ecosystem. For example, they automate and execute financial transactions, such as peer-to-peer lending and decentralized exchanges of cryptocurrencies, based on predefined conditions. Additionally, smart contracts have played a pivotal role in the adoption and development of Non-Fungible Tokens (NFTs), representing unique digital assets such as digital art, collectibles, and virtual real estate. The use of smart contracts in the NFT space has facilitated the creation, ownership, and trading of digital assets, providing authenticity and provenance on the blockchain. Blockchain 3.0 further expanded the scope of this technology, integrating it into a wide range of industries, governance structures, and aspects of societal justice, thereby giving rise to a multitude of innovative applications [4, 43]. An illustrative example is the Decentralized Autonomous Organization (DAO), a construct of Blockchain 3.0, which leverages blockchain to enable transparent and equitable management. As blockchain technology has evolved through its different phases, cryptocurrency wallets have emerged as indispensable tools. They are not just a means of access, but the very gateway through which users engage with and harness the full potential of blockchain networks, from simple transactions to complex smart contract interactions.

A cryptocurrency wallet is a tool that allows users to store, manage, and transact with cryptocurrencies such as Bitcoin, Ethereum, and other blockchain-based assets. Unlike traditional physical wallets, a cryptocurrency wallet doesn't directly "hold" currency but rather maintains a pair (or many pairs) of cryptographic keys: a public key, which is like an address or account number that others can see and send funds to, and a private key, known only to the owner(s), which is used to sign transactions and access the funds. The wallet interacts with blockchain ledgers to enable users to send and receive digital currency, monitor their asset balance, and interact with smart contracts: i.e., a self-executing program with the terms of a transaction directly written into code. Cryptocurrency wallets come in various forms, including non-custodial and custodial, hardware and software, cold and hot, and externally-owned or contract-based. Below, we describe some of the ways these wallets differ.

Two main features define these wallets: their internet connection status and the level of control they offer over key management functions [15]. Cold wallets, for example, store the private key on a tangible device and remain disconnected from the internet for the majority of the time. These could be hardware, paper, or brain wallets. Among these cold wallets, paper and brain wallets do not have a user interface but a method to record the private key of the crypto account on paper or via memorization (i.e., in the brain). Hardware wallets are specially designed physical devices, typically resembling a USB stick, with popular choices including Ledger and Trezor. Hardware wallets are not able to connect to the network on their own but can connect to the Internet by proxy through a personal computer. The hardware wallet then signs the transactions via the private key and uploads them back to the crypto bridge, which broadcasts them to the rest of the blockchain network as complete. Most hardware wallets do not retain users' private keys. However, there are services, such as Unchained Capital, that offer custodial cold storage solutions. These cold custodial services are not included in the scope of our study.

On the other hand, hot wallets maintain a constant internet connection. Based on the control over the private key, these can be classified into two main types: custodial and self-custodial wallets. Custodial wallets delegate key management responsibilities to third-party services, which could be a centralized exchange (CEX) like Coinbase or Binance, a web wallet service like Blockchain.com, or another entity such as Free Wallet. The third party has full control over your funds while users only have to give permission to send or receive payments. On the flip side, self-custodial, or non-custody wallets, empower users with encrypted ownership of their private key. This not only gives them full control over their funds but also entrusts them with the responsibility of safeguarding them.

There are two main types of Ethereum accounts: externally owned accounts (EOAs) and contract accounts [9]. Thus, self-custodial wallets can further be divided into EOAs wallets and smart contract wallets. EOAs are controlled directly by the user through their private keys, such as MetaMask. Smart contract wallets, in contrast, are controlled, as their name suggests, by a smart contract deployed on the network. Popular options include Argent, The contract is "owned" by an EOA, but the owner's EOA can be changed after deployment. Given this ability, these wallets offer unique features, such as the removal of the user's need to manage seed phrases and providing advanced recovery methods, such as social recovery. However, the introduction of smart contract wallets also presents new challenges. While these wallets make managing cryptocurrency more convenient, they are still subject to the inherent risks of smart contracts, such as vulnerabilities in the contract code or network.

Rather than classifying wallets by their functionality, another approach is based on the devices they operate on, such as desktop wallets and mobile wallets. Mobile wallets are applications installed on mobile devices such as smartphones or tablets. Similarly, Desktop wallets run on operating systems (OS) like macOS. Browser extensions are also popular forms of wallets, which are used on desktop browsers.

3 RELATED WORK

We've organized the discussion of related work into three primary themes: (1) General studies on crypto users, (2) user research on crypto wallets and (3) studies focusing on security and privacy aspects related to crypto wallets.

3.1 Studies on Crypto Users

Prior research has predominantly identified motivations such as financial gain and technical curiosity as driving forces behind user engagement with cryptocurrency [1, 15, 28, 29, 39]. Building on this foundational understanding, a thorough examination of the prior work reveals a concentrated focus on the challenges users face, particularly in terms of usability and experience with cryptocurrencies [11, 20, 47]. The complexity in managing the cryptographic keys that control cryptocurrencies poses a significant hurdle, especially for beginners who often struggle with the technical jargon and foundational concepts, such as key pairs [39, 46]. Moreover, this complexity extends beyond active users to those who are hesitant to adopt cryptocurrencies. Their reluctance is often rooted in the intricate nature of cryptocurrency protocols, compounded by misconceptions about privacy and a general lack of trust in cryptocurrencies [17, 20, 30, 45]. In addressing these trust issues, Sas and Khairuddin have delved into the dynamics between different parties in the cryptocurrency ecosystem, including users, miners, exchanges, and governmental bodies. Their research illuminates social strategies to mitigate trust challenges, such as opting for authorized exchanges to counter dishonest traders [27, 38, 39]. Furthermore, the research conducted in this realm also sheds light on general behavioral patterns among cryptocurrency users, such as storing redundant backups of their private keys [1, 15, 29]. Additionally, it has been observed that users frequently possess multiple types of cryptocurrencies and manage their assets across a range of wallets [29]. However, to the best of our knowledge, no prior studies have specifically investigated *how* users weigh the pros and cons of various wallet options, make their adoption choices, and manage multiple wallets.

3.2 Cryptocurrency Wallets Studies

Crypto Wallets act as the primary point of entry for users to the blockchain. Researchers have broadly studied usability challenges for crypto wallets users [2, 3, 16, 22, 26, 36, 47, 51]. Custodial wallets are often recognized as better user interface design and convenient for novice users [16, 47]. Yet, for beginners, onboarding remains challenging due to difficulty accessing primary features and insufficient explanations of account verification and blockchain terminology [3, 6, 16, 26, 36]. Numerous studies have delved into decentralized exchanges [22–24], revealing a notable absence of human-centered design. The predominant usability challenges in decentralized exchanges mirror those in other self-custodial wallets, such as wallet creation, seed phrase management, transaction status comprehension, and the intricacies of understanding and setting transaction fees [2, 15, 47, 51]. There have been numerous design suggestions put forward to enhance the user experience with crypto wallets. For instance, Chen proposed the incorporation of augmented reality techniques into interaction design [7]. Additionally, there are recommendations for personalized designs tailored

to different user groups. An example of this is the creation of a simplified version specifically for novice users [1, 15]. To support users' learning experiences, it's crucial to offer clear explanations of terminologies and provide comprehensive guidance [3, 16]. Furthermore, there's a pressing need for transparent communication regarding regulatory requirements, such as the Know Your Customer (KYC) process [16]. Despite the extensive research efforts on usability problems and design of various crypto wallets, most studies were not addressing how users operate multiple wallets and what factors shape their decisions.

3.3 Crypto Users' Security and Privacy Perceptions

Several studies have been conducted to understand the risk perception, security, and privacy practices of crypto users [1, 15, 29, 39, 46]. Researchers identified essential risk categories that crypto users perceive as most likely to lead to financial loss: (1) human error, (2) betrayal, and (3) malicious attacks [15, 39]. Fröhlich et al. further established a comprehensive list of threats cryptocurrency users face, derived from an expert elicitation study [14]. Voskobojnikov et al. delved into the unique risk concerns of non-users, such as the social pressure to adopt cryptocurrencies, the challenges of retrieving funds if the owner passes away, and the potential for physical attacks when storing cryptocurrencies at home [46]. Although users are aware of a broad spectrum of risks, many lack a deep understanding of the technology underpinning cryptocurrencies, leading to misconceptions about key management, cryptocurrency addresses, transactions, and fees [1, 15, 29, 31]. Krombholz et al. found that Bitcoin users harbor misconceptions regarding anonymity and privacy on the blockchain [29]. Further research has investigated users' security and privacy practices [1, 12, 15, 39]. Many users are either unaware of, or struggle to adopt, existing security and privacy measures due to usability challenges [12]. While certain security measures are frequently adopted by users, others remain largely unknown. Notably, novices are often less familiar with security practices, such as multi-signature crypto wallets, and use them less often than experienced users [1]. It has also been observed that users frequently employ multiple wallets for different purposes and maintain redundant backups of their private keys to mitigate the risks of accidental loss or human error [15].

3.4 Summary of Gaps in The Literature

Despite the growing body of research on cryptocurrency and its technologies, there are notable gaps in our understanding of how and why users choose to use different types of cryptocurrency wallets: one of the most foundational security decisions users can make in their use of cryptocurrencies. Additionally, prior studies have not explored the human-computer interaction (HCI) aspects of smart contract wallets, a crucial area for comprehending user engagement with these technologies. Our research aims to bridge these gaps by investigating how and why users use different wallets, focusing on the security, usability, and social factors that influence users' wallet adoption and usage. Furthermore, our study explores the unique security measures adopted by users across different wallet types, providing insights into how they navigate and secure their digital assets in the complex and evolving landscape of cryptocurrency.

4 METHOD

We conducted remote semi-structured interviews in English with 24 participants located in the US over Zoom. Each interview lasted between 60 to 90 minutes. Prior to the main study, we pre-tested our interview protocol with 6 pilot sessions. After revising the protocol based on feedback from these pilot studies, we conducted the final round of interviews (n = 24). Each participant was compensated $30 upon completing the interview. The study received approval from an Institutional Review Board (IRB).

4.1 Participants Recruitment

To ensure a diverse range of participants, we utilized multiple recruitment methods: (1) posting from the authors' X (formerly Twitter) accounts and on specific subreddits (/r/ethereum, /r/defi), (2) disseminating the information through Discord channels, and (3) employing snowball sampling. We targeted platforms like Twitter, blockchain-related Discord channels, and subreddits as each of these social media platforms has active cryptocurrency-centered user communities. Prospective participants first completed a screening survey, capturing details such as age, gender, technical background, and experience with crypto wallets, including frequency of use. We selected participants based on their survey responses. Eligible participants needed to be (1) over 18 years old and (2) crypto wallet users. Furthermore, we aimed to include participants with diverse demographics and experience across various wallet types to address our research questions.

4.2 Participant Background

We had a total of 24 participants, with their demographics detailed in Table 1. Our participants skewed young and male. Previous papers indicated that individuals engaged in the blockchain and crypto space are more likely to be younger and male [19, 40]. This suggests that our sample is reflective of the larger population demographics within the web3 community. Seven participants were aged between 18-24, fourteen between 25-34, and three between 35-44; 20 identified as men, and four as women. All participants had prior experience using crypto wallets, though the length of their experience varied. Specifically, nine participants reported over three years of expertise, nine had between 2-3 years, four between 1-2 years, and two had under a year of experience. Out of our interviewees, 18 identified as having a technological background, with criteria like possessing an Information Technology-related degree or experience with programming languages. These participants self-identified as tech-savvy, whereas the remaining six did not.

4.3 Pilots

Our interview protocol is tailored to our research questions: (1) crypto users' varied wallet choices and their reasons for using them; (2) security perception across various wallet types; (3) security measures and challenges associated with wallet usage. Some questions draw inspiration from Fröhlich et al. [15], who interviewed 10 cryptocurrency users about their habits, risk perceptions, wallet usage, backup behaviors, and usability challenges. However, our research provides a more in-depth analysis of why users choose to use the wallets that they use, including both security and non-security considerations. Our scope is broad, covering both mobile and PC

ID	Age	Gender	Tech. Bg.	Exp. (yrs)	Wallet usage
P1	25-34	Male	No	>3	Binance Exchange Browser & Mobile, Trust Mobile
P2	35-44	Male	Yes	>3	Coinbase Exchange Browser & Mobile, MetaMask Browser & Mobile, InstaDApp Mobile, Trust Mobile
P3	35-44	Male	No	<1	Binance Exchange Browser & Mobile, Trust Mobile
P4	25-34	Male	Yes	2-3	Binance Exchange Browser & Mobile, Luno Mobile, Exodus Mobile
P5	25-34	Male	Yes	2-3	Coinbase Exchange Browser & Mobile, MetaMask Browser & Mobile, Zerion Mobile, Trust Mobile
P6	25-34	Male	Yes	>3	Binance Exchange Browser & Mobile, Coinbase Exchange Browser & Mobile, Luno Mobile, Trust Mobile
P7	35-44	Male	Yes	>3	MetaMask Browser & Mobile, Argent Mobile
P8	25-34	Male	No	>3	Coinbase Exchange Browser & Mobile, MetaMask Browser, Argent Mobile
P9	18-24	Male	No	2-3	Coinbase Exchange Mobile, MetaMask Browser
P10	18-24	Male	No	2-3	Binance Exchange Browser & Mobile, Coinbase Exchange Browser & Mobile, MetaMask Browser & Mobile, Ledger Hardware
P11	25-34	Male	Yes	2-3	Binance Exchange Mobile, MetaMask Browser, Trezor Hardware
P12	25-34	Female	Yes	>3	MetaMask Browser, imToken Mobile, Trezor Hardware
P13	18-24	Male	Yes	1-2	Coinbase Exchange Browser & Mobile, Uphold Exchange Browser & Mobile, MetaMask Browser, Phantom Mobile
P14	18-24	Male	Yes	2-3	Coinbase Exchange Browser& Mobile, MetaMask Browser & Mobile, Ledger Hardware
P15	25-34	Female	Yes	>3	Coinbase Wallet Mobile, MetaMask Browser, Ledger Hardware, Trezor Hardware
P16	25-34	Male	Yes	<1	Coinbase Exchange Browser
P17	18-24	Male	Yes	1-2	Coinbase Exchange Mobile, MetaMask Browser
P18	18-24	Male	Yes	1-2	Coinbase Exchange Mobile, MetaMask Browser & Mobile, Phantom Mobile
P19	25-34	Female	No	1-2	OKX Exchange Browser, MetaMask Browser, Rainbow Mobile, Zerion Mobile
P20	25-34	Male	Yes	>3	MetaMask Browser & Mobile, Argent Mobile, Status Hardware
P21	25-34	Male	Yes	2-3	MetaMask Browser, Rainbow Mobile, Safe Mobile, Argent Mobile, Zerion Mobile
P22	25-34	Male	Yes	>3	Coinbase Exchange Browser, MetaMask Browser & Mobile, Ledger Hardware
P23	18-24	Male	Yes	2-3	Coinbase Exchange Browser, MetaMask Browser
P24	25-34	Female	Yes	2-3	Binance Exchange Browser & Mobile, MetaMask Browser & Mobile, Zerion Mobile, OneKey Hardware

Table 1: Participant demographics, technology background, and current wallet usage are presented. Only the wallets presently in use are included, excluding those tried in the past.

platforms and encompassing a diverse range of wallet types. Of particular interest is the emergence of smart contract wallets, which are designed to strike a balance between security and usability. We conducted pilot tests of the interview protocols with six participants. Feedback from these pilot sessions prompted us to refine the phrasing of our interview questions. For instance, during the pilot tests, we posed the question, *"How do you use wallets daily?"* in order to grasp potential participants' usage patterns. However, participants often provided concise responses that lacked specifics about which wallets they used for particular features. Consequently, we revised the question to, *"Please describe the tasks you carry out with the different wallets you use."* Our study results reported in this paper did not include the data collected from the pilot study.

4.4 Semi-structured Interview Procedure

Prior to initiating the study, we obtained informed consent from each participant to conduct and record the session. Participation was voluntary and ensured complete anonymity. It was our priority to minimize the collection of any personally identifiable information. To refrain from biasing participants towards security-focused responses, participants were briefed that the study focus was on comprehending the experiences and challenges of crypto users.

Details about the interview protocol are available in the appendix A. The interview was divided into three specific sections, each corresponding to one of our research questions. (1) *Experience with Cryptocurrency and Wallet Usage*: In the first part, we delved into the participants' history with cryptocurrencies and their typical patterns when using crypto wallets. The discussions revolved around the types of tasks they executed on various devices and with different wallet categories. Furthermore, we sought their insights on the advantages and setbacks encountered while using these wallets. Sample questions included "If you use multiple wallets, how do you store your assets across these wallets? Why? How do you manage these wallets in your regular usage?" "What wallets have you used? Which wallet did you use the most?" "Have you ever encountered any difficulties or challenges using different crypto wallets? On mobile or browser? Could you give me a concrete example?"

(2) *Risk Perception and Concerns*: The second section was constructed to delve deeply into participants' apprehensions and perceived risks associated with cryptocurrency interactions and wallet usage. Initially, we encouraged an open dialogue, prompting participants to articulate their individual perceived vulnerabilities concerning crypto assets. For instance, we posed questions like, "When utilizing this specific wallet, did you have any concerns with your crypto assets" Only after discussing their spontaneous responses, did we introduce a list of potential cryptocurrency threats, drawn from existing literature [14, 15]. This method was chosen to ensure that we didn't steer or bias their initial perceptions but instead offered a comprehensive landscape of recognized risks for further reflection. As the section progressed, to better understand the depth and nuances of their perspectives, we probed deeper with "why"

questions whenever participants expressed varied risk perceptions about different wallets or platforms.

(3) *Security Practices and Experiences*: In the third part, our focus shifted to the participants' protective measures to ensure the safety of their crypto assets. To grasp the motivations behind their practices, we inquired about any past experiences of crypto asset loss and their subsequent coping strategies. This allowed for a richer understanding of behaviors and reactions in the face of such adversities. Example questions from this section were - "Have you done anything to address the concerns you mentioned (in the second section)?" "Have you ever lost a substantial amount of crypto-assets at a time? " "Did you do anything differently before and after the incident/crypto assets loss? Why?"

4.5 Data Analysis

We transcribed interview recordings and analyzed the qualitative data using thematic analysis [13]. Two researchers (including the first author) independently coded a subset of the transcripts, then jointly resolved conflicting codes to develop the codebook. We adopted open coding and a deductive analysis method to delve into participants' usage patterns, concerns, and security measures for various types of wallets and devices. Four researchers convened regularly to discuss emerging codes and themes, ensuring coherent interpretations of the codes. Through this process, we established 139 basic codes, which were further grouped into sub-themes based on the main themes: participants' usage patterns, concerns, and security measures. Some representative themes include: "Different risk perceptions for various wallet types," "Practices for using different wallet types," and "Socio-cultural considerations in wallet choices." The remaining study sessions were coded using this finalized codebook. Following the approach outlined by Braun et al.[5] and Mcdonald et al.[33], we chose not to report inter-coder reliability in our analysis.

4.6 Ethics and Data Protection

Our study plans and data protection measures were thoroughly reviewed and approved by our Institutional Review Board (IRB) to safeguard against undue participant risk. Participants had to read and sign a consent form before interviews, detailing data collection, voluntary participation, and the right to withdraw at any time. To protect participant anonymity, we used multiple measures. Email addresses were only for interview scheduling, and we recorded pseudonyms, not public identifiers, with raw data to ensure confidentiality. All data were securely stored in university server, accessible only to our team. Identifying details were removed or altered during analysis to prevent participant identification. Our findings are reported in a way that prevents tracing responses to individuals, aligning with our commitment to minimize participant risks, comparable to everyday life risks.

5 RESULTS

We report on participants' security and privacy perceptions and behaviors of crypto wallets, organized by wallet types and devices. We first describe participant demographics and then present findings regarding our research questions: (1) participants' usage pattern and reasons for different wallets (*RQ*1), (2) participants' security perceptions across crypto wallet types and devices (*RQ*2), and (3) the security actions they take to counter perceived threats (*RQ*3).

ID	Custodial Wallet	Self-custodial EOAs Wallet	Smart Contract Wallet	Hardware Wallet	Mobile	PC
P1	✓	✓	✗	✗	80%	20%
P2	✓	✓	✓	✗	60%	40%
P3	✓	✓	✗	✗	80%	20%
P4	✓	✓	✗	✗	10%	90%
P5	✓	✓	✗	✗	60%	40%
P6	✓	✓	✗	✗	80%	20%
P7	○	✓	✓	○	30%	70%
P8	✓	✓	✓	○	30%	70%
P9	✓	✓	✗	✗	20%	80%
P10	✓	✓	✗	✓	10%	90%
P11	✓	✓	✗	○	30%	70%
P12	○	✓	✗	✓	20%	80%
P13	✓	✓	✗	✗	25%	75%
P14	✓	✓	✗	○	5%	95%
P15	✓	✓	✗	✓	10%	90%
P16	✓	✗	✗	✗	30%	70%
P17	✓	✓	✗	✗	40%	60%
P18	✓	✓	✗	✗	50%	50%
P19	✓	✓	✗	✗	15%	85%
P20	○	✓	✓	✓	45%	55%
P21	○	✓	✓	✗	99%	1%
P22	✓	✓	✗	✓	5%	95%
P23	✓	✓	✗	✗	20%	80%
P24	✓	✓	○	○	20%	80%

Table 2: Wallets and devices that participants have used. ✓ indicates a wallet currently in use, ✗ signifies a wallet type that was never utilized, and ○ denotes a wallet type that was previously used but is no longer in operation. The final two columns present the percentage of participants who reported using wallets on mobile devices and PCs.

5.1 Participants' Multi-Wallet Usage: Behavior and Rationale (*RQ*1)

23 of our 24 participants reported frequent use of multiple wallets, meaning they use various types of wallets in parallel. The remaining one participant had 4-month experience with crypto and only used Coinbase Exchange via a browser. The 23 participants who used multiple wallets often used a mix of wallet types on various devices (as shown in Table 1 and 2). We will then delve into the participants' usage and rationale for different types of wallets, such as mobile, PC, custodial, self-custodial, and hardware wallets. A specific wallet can have multiple characteristics/types. For instance, MetaMask is a self-custodial wallet that can be used on mobile devices or PCs.

5.1.1 Mobile vs. Personal Computers. Most participants (n=23) shared that they used crypto wallets on both their PC (personal computer) and smartphone. We refer to the former as a "PC wallet" and the latter as a "mobile wallet" hereafter. We found that participants varied in how often and why they elected to use their PC versus mobile wallets. For instance, eighteen participants indicated that they used their PC wallet most of the time, while six participants reported using their mobile wallets most of the time.

Device Preferences: Mobile for Basic Transactions, PC for Complex On-Chain Tasks. Five out of the six participants who favored mobile devices believed that mobile wallets are the most appropriate for their primary wallet usage: cryptocurrency trading or

basic transactions such as sending/receiving crypto. They rarely engaged in complex operations, such as interacting with Decentralized Finance (DeFi) platforms[2], executing smart contracts, or participating in Decentralized Autonomous Organizations (DAOs)[3]. These participants highlighted various advantages of using crypto wallets on mobile devices, such as portability, easy of access, and an enhanced user interface experience. For instance, P2 complimented on the useful account information and its clean structure in mobile wallets: "*Mobile crypto wallet is arranged in a systematic manner that you can be able to view your balance, view your deposit, your asset tracking. That is why I find it easy over the mobile.*" In contrast, participants who often took part in more complex on-chain tasks typically preferred using PC wallets. They highlighted how, when interacting with smart contracts or DeFi platforms, it was useful to have a big screen to be able to see all the relevant information and applications at once. For instance, P15 explained *"If I wanna transfer out of centralized exchange or interact with Opensea, PC is all right there on one screen versus like interacting a combination of mobile and browser or like having to switch between applications on mobile."*

5.1.2 Custodial vs. Self-custodial Wallets. As explained in Section 2, Custodial wallets or Centralized Exchanges (CEX) are platforms where users' crypto assets are managed and stored by a third-party organization. Users do not have direct control over their private keys in such systems. The majority of participants (n=23) experimented with different wallets to find one they found to match their security preferences. Out of the 24 participants, all had experience with centralized exchanges, and 23 had used self-custodial wallets with externally owned accounts (EOA), where the user has full control and responsibility over their private keys (as shown in Table 2).

Using multiple wallets for asset storage. Many participants employ multiple wallets simultaneously. Only four of them predominantly store crypto assets in a single wallet type: two opt for smart contract wallets, while the other two prefer hardware wallets. In contrast, some participants spread their assets across various wallets to mitigate the risk of total loss. For instance, P19 said, "I've allocated 70% of my assets to CEX, with the remaining distributed as 20% in Rainbow, and 10% split between MetaMask and Zerion." However, others like P21 adopt a more balanced approach, noting, "I've nearly equally dispersed my assets across all the wallets I use, though they differ in types - some are bitcoins, others are stablecoins."

Trust Levels in Custodial Wallets: Experienced vs. Novice Perspectives. Every participant uses custodial wallets, albeit for varied reasons. Ten participants mentioned keeping most of their crypto on CEX due to either less than a year's crypto experience or limited activities like holding and trading. Despite understanding the risks of these platforms, they see incidents as unlikely and prefer the convenience. P9 explained *"The CEX I utilize is a prominent international institution. I have faith in it, and I don't believe it's prone to collapse. Such events are beyond our control. If that happens that happens."* In contrast, many participants expressed apprehension regarding the risks associated with custodial wallets and centralized exchange platforms (CEX), especially after the collapse of FTX in 2022 [18]. Participants who had more experience with cryptocurrencies and more technical expertise exhibited less trust and confidence in custodial wallets and centralized exchanges. For example, P7 noted: *"I've been involved in the crypto world for over a decade, and I've witnessed many major players falter. So, never assume an exchange is too big to face issues. Whenever your funds are in an exchange, you should be aware of the risk, as there's no guarantee of their safety."* Experienced participants concurred that while total risk elimination is impossible, it's mitigatable by avoiding crypto storage on centralized exchanges or custodial wallets, using them only for buying or swapping, then quickly moving assets to other wallets.

Transitioning to Self-custodial Wallets Due to Interactions with dapps and Layer 2. Ethereum is a popular public blockchain that supports Turing-complete smart contracts (i.e., can implement any arbitrary computational logic). As the Ethereum ecosystem evolves, the prominence of self-custodial wallets has grown due to their necessity in interacting with decentralized applications (dApps) and the DeFi ecosystem on Ethereum. These dApps typically require connections with self-custodial wallets like MetaMask, allowing direct interaction with Ethereum smart contracts without intermediaries. For instance, P15 participated in a DeFi system that allowed him to earn interest from his crypto assets. He used the self-custodial wallet MetaMask to interact with that DeFi system: *"I thought why not try to earn some interest on it instead of just holding onto it? MetaMask made that possible for me. So I start using it while using CEX."* Participants also mentioned that the ease of interacting with Layer 2 networks, such as zksync (an EVM-compatible zero-knowledge proof Layer 2 rollup), influences their choice of smart contract wallets. Layer 2 systems aim to enhance scalability of base layer blockchains like Ethereum, enabling more transactions and higher throughput. For instance, P8 shared, *"Within the Argent [a smart contract wallet], you can purchase, invest, and even bridge to layer 2. In contrast, MetaMask previously didn't offer these functionalities directly in the app..."*

Hardware wallets have cumbersome user experience. Ten of our participants had previously used hardware wallets for securing their own crypto assets, yet only two continued this practice and retained a substantial amount of assets within it. These two mainly use hardware wallets for long-term storage and seldom transfer funds out. The other eight participants either abandoned hardware wallets after a trial period or were contemplating a switch and exploring alternatives. In describing why, participants mentioned that hardware wallets have cumbersome user interfaces, which reduced participants' confidence in being able to use a hardware wallet for time-sensitive on-chain activities. P8 expressed frustration with the integration process between his Ledger hardware wallet and the MetaMask browser wallet. He found the interaction between Ledger Live and MetaMask particularly perplexing, leading to a significant lack of confidence in accessing his funds and his decision to transfer the majority of his holdings from Ledger to Argent: *"The interaction between Ledger live and meta mask was*

[2]Decentralized Finance (DeFi) platforms use blockchain technology to offer financial services like lending, borrowing, and trading without traditional intermediaries like banks.

[3]DAOs, or Decentralized Autonomous Organizations, are a key component of blockchain ecosystems, primarily on platforms like Ethereum. They enable decentralized, collaborative decision-making and asset management through smart contracts [48].

all very confusing. Both MetaMask and Ledger required approvals, and there were instances where this didn't go smoothly. I just wasn't confident that I would be able to get my funds out. So that's kind of what inspired the move of like most of my holdings from Ledger to Argent." Yet, usability is not the sole reason users moved from hardware wallets to alternatives like smart contract wallets. Risk perception and security considerations also played significant roles, as detailed in the subsequent section 5.2.3.

Wallet Choices Influenced by Friends' Recommendations. Participants expressed a tendency to choose wallets that are popular among their circle of friends, which is in line with findings from prior work that examined factors influencing mobile instant messaging app choices and social cybersecurity more broadly [10, 49]. Recommendations and endorsements from friends enhanced the perceived trustworthiness of these wallets or platforms. Five participants stated that they initially chose custodial wallets based on their friends' recommendations. P2 remarked, "Most of my friends use Coinbase[4], so I believe it's trustworthy." This observation aligns with the broader trend within the blockchain space, where decisions and preferences are often influenced by peer-to-peer interactions rather than centralized authorities or traditional advertising methods. However, participants often neglected potential risks, basing their decisions mainly on the trust they placed in their friends' choices. P6 recounted a costly lesson from blindly trusting a friend's choice, saying, "I didn't initially see a reason to get involved, but when the opportunity arose through the Ponzi scheme, it seemed appealing. Friends, and friends of friends, vouched for its success and profitability. I thought, if my friend is benefiting from it, why shouldn't I give it a try?" The "Ponzi scheme" discussed here was an investment program on an online exchange to earn interest. There was also a noticeable trend among participants to treat crypto wallets like messaging apps, especially for novice users. P4 mentioned, "I use different wallets making transactions, depends on which one my friend is using." This suggests that some users had a misconception about the fundamental workings of crypto wallets, thinking that transactions can only occur between identical wallets.

5.2 Security Factors Influencing Participants' Usage of Different Wallets and Devices (*RQ2*)

Beyond the factors of convenience and portability, participants also cited varying risk and threat considerations when expressing their preference for wallets.

5.2.1 *Mobile vs. Personal Computers.*

Mobile Wallets: Enhanced Focus and Privacy in Crypto Transactions. Participants also reported that mobile devices offer distinct privacy and security advantages due to the focus imposed by the limited screen size. For example, P7 elucidated how he believes he makes fewer errors on mobile wallets because "With just one screen displaying one task at a time, it's simpler to focus on that specific task." Additionally, participants favored mobile wallets because they felt it mitigated risks like shoulder surfing in public spaces. As P3 shared, "Using my cellphone feels more private; nobody needs to know what I'm up to. But with a laptop, it feels like I'm revealing what I'm specifically doing."

PC Wallets: Larger Screen Size and Extensions Enhance Transaction Security and Accuracy. Interestingly, while participants who preferred mobile wallets cited the focus necessitated by small mobile screens as a reason for reducing transaction errors, participants who preferred PC wallets cited the larger screen size afforded by PC wallets made it easier to scrutinize details and thereby reduced the chances of errors and potential financial losses. P2 explained *"I prefer using a PC because it lets me confirm all the details before finalizing a transaction. While a mobile is a compact device, a PC is larger (screen) that allows me to verify all the information I need."* Moreover, the presence of third-party security extensions (e.g., Blowfish, Fire, Revoke.cash) in browsers enhanced the perceived security of PC wallets for some participants, thus predisposing them to execute critical or high-risk transactions on a PC rather than on a mobile platform. P8 explained *"You do have these additional backups when you're on desktop. You have these additional extensions that are kind of watching your back. So definitely riskier on mobile for sure."* Thus, while some participants have both PC and mobile wallets, they often choose the PC wallet for high-risk or critical transactions. For instance, such high-risk transactions could involve significant fund transfers, investments in emerging Initial Coin Offerings (ICOs), or engaging with newly launched or experimental decentralized applications — i.e., digital programs operating on a blockchain.

5.2.2 *Custodial vs. Self-custodial.*

Participants had distinct views on the risks across custodial and self-custodial wallets, as well as the different types of self-custodial wallets. A primary concern with custodial wallets is platform risk, stemming from potential platform collapses and associated legal uncertainties. While many preferred the MetaMask wallet for their self-custodied EOAs, concerns arose over its susceptibility to scams/phishing and error-prone interface design, echoing prior work [51]. Eight participants transitioned to hardware or smart contract wallets in search of a better user experience or enhanced security.

User-friendly CEX Interfaces Mitigate Concerns Over Human Errors and Enhance Trust. Participants were less concerned about human errors or social threats related to custodial wallets. They felt that the user-friendly interface design of CEXs helped prevent user mistakes. P10 noted that *"some centralized exchanges appear to have improved their security disclaimers. For instance, they might indicate compatibility issues, such as mentioning when a transaction isn't suited for an ERC 20-compatible address* [5]*. I believe Coinbase has such warnings in place."* Therefore, pertaining to P10's observation, when centralized exchanges like Coinbase issue warnings to users, it serves as a proactive measure to ensure that transactions are correctly structured, thereby preventing potential mishaps or the loss of funds. The presence of background checks and customer service departments in these platforms convinced participants that they weren't solely responsible for safeguarding their crypto assets when entrusting them to these exchanges.

[4]Coinbase is a digital currency exchange that provides a platform for buying, selling, and storing various cryptocurrencies, as well as offering a custodial wallet service. https://www.coinbase.com/

[5]The Ethereum Request for Comment 20 (ERC-20) stands as a universally embraced standard for crafting fungible tokens within the Ethereum blockchain ecosystem [44].

Social Threat Concerns in Self-Custodial EOAs Wallets. Participants expressed heightened concerns about social threats associated with self-custodial wallets, such as scams and phishing. P18 noted: *"There are a lot of scams out there on Twitter and Discord. It's pretty common for NFT projects be like click this link. You'll get free entity or free crypto. And a lot of people fall for that, especially last year."* Some participants felt that the security measures of self-custodial wallets against social threats are either inadequate or ineffective. P15 explained: *"The current warning in Trust Wallet merely indicates 'high risk.' I believe simply noting 'potential risk' isn't an effective alert. Given that everyone in crypto understands inherent risks, how can we know that there's a heightened risk or potential for a scam?"*

5.2.3 Questioning the Security of Hardware Wallets. Hardware wallets are widely viewed as the most secure option for crypto storage, primarily because they operate offline [42]. However, many agreed that it's only worth using a hardware wallet if one has a large amount of assets. Some participants also questioned the security of hardware wallets, specifically against phishing attacks. P8 highlighted: *"When I saw someone getting phished, others would say, 'You should've used a hardware wallet.' But I wondered, how would a hardware wallet have made any difference? If anything, hardware seems even less effective against phishing."* Several participants highlighted concerns arising from updates and news around the widely-used hardware wallet, Ledger. Ledger announced a security feature, Ledger Recover, in 2023 [21]. Unexpected security risks, like potential private key exposures, spurred some to shift away from hardware wallets. P11 remarked: *"I kept 95% of my assets on Ledger, but concerns about them possibly holding users' private keys made me uneasy. After all, if they aren't your keys, they aren't your assets. Who knows if they might conduct unauthorized transfers?"* To counteract potential risks associated with Ledger updates, some participants opted not to adopt the latest firmware updates. P20 commented: *"When Ledger received flak for mulling over the addition of KYC to their platform, I decided against updating to the newer firmware."* As prior work suggests, people sometimes ignore security updates to avoid other updates that come with installing new versions of software [25] — in so doing, however, participants may unintentionally leave themselves vulnerable to newer exploits that firmware updates might patch.

5.2.4 Smart Contract Wallets: Enhanced Programmable Security but Limited User Understanding. Of our 24 participants, five utilized smart contract wallets. Among the five participants, two stored a substantial part of their long-term assets in these wallets. In Section 2, we highlighted that in contrast to traditional wallets where funds are directly controlled by private keys, smart contract wallets leverage embedded smart contract logic to dictate fund access and management. Thus, smart contract wallets offer personalized security features (e.g., social account recovery, programmatically enforced transaction limits, and multi-signature transaction approvals). While smart contract wallets are becoming increasingly popular for their advanced security features, many participants lack an understanding of and experience with them. Even some who have used these wallets expressed misconceptions as to how they worked, hindering them from fully utilizing smart contract wallets. For example, P7 explained his understanding which was incorrect: *"The issue with the Argent[6] mobile wallet is that it operates as a custodial wallet. You don't possess access to your private keys. It's very similar to a CEX, in the sense that if I don't have access to my keys, I will never consider it safe."* However, smart contract wallets often operate on a self-custodial basis, storing the encrypted private key on the user's own device. The wallet provider usually do not have access to users' private key and nor have control over their assets. However, some participants believed that smart contract wallets offer the same level of security as hardware wallets and have transferred all their funds from Ledger to Argent. P8 noted: *"I'm not entirely sure, but maybe Argent is as secure as cold storage. I might be mistaken, but based on my current understanding, I'm okay with possibly sacrificing a small degree of security to be confident that I can access my funds anytime. I didn't feel that assurance with Ledger."* Participants felt that smart contract wallets offered enhanced security against social threats such as phishing and scams compared to other types of wallets. P20 shared, *"I believe that smart contract wallets have advantages over purchasing a physical device like a Ledger. With smart contract wallets, multiple signers can be set to approve a transaction. Having this extra step might slow things down a bit, but it really helps keep me safe from phishing scams."*

5.2.5 Trust in Crypto Wallets Aligned with Participants' Cultural Background. Participants also discussed their experiences with certain crypto wallets that resonated with their cultural backgrounds. Particularly for novice users, there was a tendency to gravitate towards wallets that felt familiar, even absent an understanding of the underlying mechanics. P4 shared: "I currently reside in the US but have strong ties to Africa. When I first started using cryptocurrency, I wasn't very familiar with its workings. I was in search of a cryptocurrency wallet that would allow me to send money directly to individuals in Africa." A shared cultural context often influenced distinct design preferences and currency conveniences, which in turn fostered greater trust for users. P12, who is based in the US but has ties to China, explained, "In mobile, the one I've used the most is imToken. The founders are actually from Hangzhou, China. They have a good grasp of the habits of Chinese users, and the user experience is very well designed. For instance, many people in China have numerous wallets, and when you have to manage multiple chains, switching wallets is a frequent operation. imToken has a button on the top left corner of the homepage that allows you to manage, delete, or add wallets, which is very intuitive."

5.2.6 Adhoc findings on Privacy Concerns. Given the inherent transparency and accountability characteristics of blockchain, data privacy emerged as a frequent concern among participants (n=5). Participants expressed strong concerns about the potential to be tracked or stalked via their blockchain transaction history. Since anyone can access and analyze this information on the blockchain, there's a risk of associating transactions with individuals, especially if they inadvertently share their wallet address on social media. P24 emphasized the potential security risks, like receiving tainted coins or being targeted for holding significant funds. She noted, "I am really concerned about someone analyzing my on-chain transaction history, which is highly possible. I know there are websites

[6] Argent is a smart contract-based cryptocurrency wallet that offers enhanced security features, user-friendly recovery options, and programmable rules for asset management. https://www.argent.xyz/

and tools that help them do that. They can identify addresses that hold lots of funds and target them with airdrops. So, I normally use Coinbase for transactions, and I use Metamask only for interacting with dapps." Conversely, another participant shared concerns about personal identity leaks from custodial wallets, preferring non-KYC wallets for transactions with unknown parties. P12 shared, "I maintain one wallet address linked to certain KYC-compliant wallets, using it only for transfers with acquaintances. For transactions with strangers, I use wallets like IMToken or other apps. Before Tornado Cash was banned in the US, it was our go-to for token distribution." Beyond the distinct privacy concerns associated with various wallet types, two participants also reported concerns about Non-Fungible Tokens (NFTs) that might reveal personal identifiers. P19 shared that "If you join something, say, a women's exclusive club, and they award you an NFTs as a recognition of your attendance, that could potentially be revealing. Though I am crafting a hypothetical situation here, it seems plausible. Such an NFT in your wallet might indirectly suggest that the account holder is likely a woman." NFTs, beyond being investment assets, can act as markers for crypto users, potentially disclosing vital and sensitive personal details. P24 highlighted, "Anyone can send you anything they want, whether it is tainted assets or offensive in-wallet messages with transactions. We do not have a tool to block or fight back."

5.3 Participants' Crypto Wallet Security Practices (*RQ*3)

To address those concerns in Section 5.2.6, participants typically employed two kinds of security measures. Nine participants highlighted behaviors related to social or cultural security protection. They favored incorporating social interactions in various facets of wallet security, from onboarding and key management to transaction approval and security protection choices. However, they also noted a shortfall in secure social stewardship and the refinement of these social security features. Additionally, participants discussed technological approaches they adopted to bolster wallet security, encompassing third-party extensions, security alerts, and isolation tactics.

5.3.1 Socio-cultural Considerations in Cryptocurrency Wallet Security.

Adopt Security Measures from Trusted Friends with Caution. For novice users, it's common to seek advice from close friends [34]. Some participants mentioned that their friends not only introduced them to cryptocurrencies but also assisted them with setting up their wallets. P17 mentioned that "Onboarding wallet was a shitty experience because there's no way I would have had the confidence to do this without a friend sitting next to me and telling me what to do." However, there was also an underlying discomfort, even with trusted friends, when it came to financial matters. P17 likened this discomfort to entering a password on Netflix — though, in that case, he could simply ask friends to look away. Yet, in the crypto onboarding journey, he felt it was more challenging to navigate that boundary since the friend was viewed as both a steward and a potential threat. Participants even reported experiencing financial loss while learning from friends. P3 shared: "I recall that when I was creating this account, he was there with me. I think I made an error by letting him see my login details. I woke up next morning and find my balance was zero. It was my fault because I was actually too relaxed and never saw the need to protect my wallet." Even experienced users often consulted with friends, especially when it comes to mitigating risks from financial fraud and social threats. P1 noted that "Before investing, I asked my friends. I asked those who have a better knowledge about their opinions of the project then make my own decision."

Social-Based Recovery and Management for Smart Contract Wallets. Smart contract wallets afford social features like social recovery and jointly managed wallets. Many participants shared that they transitioned from CEX, EOA, or hardware wallets to smart contract wallets primarily because of these social features, which addressed their security concerns, particularly in certain unique situations. P20 noted that "If something were to happen to me, like passing away, and I had substantial funds in this Argent wallet, I believe my relatives could access them. On the other hand, if I just left them a seed phrase, they might find it challenging to decipher. Given these considerations, I felt more confident about transferring my funds out of BlockFi [a centralized exchange]."

A particular standout is the guardian feature, which eased participants' worries about key management and self-custody. Guardians on a smart contract wallet can be individuals or devices that the wallet owner selects to assist in securing the wallet, endorsing wallet recoveries, and approving transactions from/to untrusted sources (e.g., in the form of multi-signature). P8 elaborated, "I really like that their addresses are smart contracts. So it, you know, it makes the establishing a guardian really easy. My wife for example is my guardian so if I ever lost access to my account, she could then give me access back, which isn't necessarily possible with MetaMask." However, participants also expressed dissatisfaction with the current social features designed into smart contract wallets. Participants grapple with choosing the right person and deciding how much trust to place in these guardians. P21 noted "I've only set my other devices as guardians. Teaching my parents is too difficult, and even if I succeed, they'll likely forget. With other relatives or friends, I'm unsure about the appropriate amount of permission to grant them. I'm not even certain if I can choose the extent of it." They believed these features could be refined further to better align with users' actual social relationships. Firstly, participants who employed guardians for transaction confirmations typically seek to incorporate an additional layer of protection against phishing and scams. Yet, participants believed existing implementations failed to provide guardians with adequate details to make informed choices. P20 pointed out, "One issue I have with Argent is that when you ask a guardian to approve a transaction, they only see a hexadecimal transaction hash. They don't actually see the details of what they're signing." Furthermore, participants highlighted a significant limitation of smart contract wallet design: i.e., the inability to provide different guardians with different access controls. This lack of granularity raises concerns about trust and control, particularly when users must rely on friends or other social relationships for critical security tasks. P21 commented: "I can't always rely on friends for signing transactions. As for Argent, it doesn't currently allow me to set up different levels of security – like one group of friends to

reset the account and another set just for signing transactions. Everything is bundled together. If you can sign transactions, you can also recover the account, and there's no clear distinction between the two."

5.3.2 Technological Approaches to Bolster Wallet Security.

Browser Extensions. Many participants frequently mentioned third-party security browser extensions as a tool for mitigating risks associated with scams and phishing. These security extensions assisted users in identifying suspicious details in transactions and contracts with which they were about to engage, lowering users' risk of falling prey to phishing scams. P5 stated, "Whenever I am on MetaMask, I use it with revoke.cash for enhanced security. It help me to regain control after transactions. Additionally, the extension shows approval details helping you prevent signing malicious approvals." Participants indicated that security extensions enhanced their confidence and sense of security, leading them to favor conducting more significant transactions on PC wallets over mobile wallets because these security-focused add-ons were not available on mobile wallets. P8 explained: "When you're about to approve a MetaMask transaction, extensions like Fire or Blowfishs quickly verify the smart contract you're engaging with to determine its legitimacy. These tools act as safeguards, making it harder for you to make errors and offering an added layer of protection on browser. Such protections aren't available on mobile wallets now."

Security alert design. Participants believed that warnings are effective at preventing phishing; however, they found the design of warnings in existing wallets to be insufficient. To validate this claim, participants drew comparisons between the data shown by the security-focused extensions described above and the security alerts provided by wallets for smart contract transactions. For instance, P11 mentioned that while the MetaMask signing page displays details about funds being sent to a smart contract, it doesn't provide an indication of the contract call function's purpose nor indications as to its safety. In addition to using third-party security extensions, participants often cross-referenced information from multiple sources to reduce phishing risks. P20, for example, mentioned cross-checking contract details on Etherscan: "What I do is copy and paste the contract address into Etherscan[7]. I then examine if it appears as the type of contract I expect, checking aspects like the volume of transactions occurring, total value loss that they expect and whether the source code is available." The number of transactions and the verification status of a smart contract's source code on Etherscan emerged as crucial markers for determining its authenticity. P10 added, "If a contract address on Etherscan shows merely five transactions, it's probably a scam. Genuine coins have thousands of transactions. Plus, most scams won't make their code public on Etherscan." Participants stressed that wallets should incorporate these validation steps. P22 elaborated, "While some of us can conduct independent research on platforms like Etherscan, it's challenging for newcomers or those without a tech background to discern the intricacies and risks of transactions." Assisting users in recognizing transactional risks and potential consequences is a challenging yet crucial feature that wallets should consider.

Using multiple wallets to isolate risk. Many participants discussed distributing their crypto assets over multiple wallets, thereby reducing risks. For example, P2 explained "Distributing assets evenly across all my wallets enhances security. If one wallet is compromised or accessed without my permission, I can still safeguard my assets in the other wallets." Additionally, participants often set clear boundaries across their multiple wallets, aiming to segregate high-risk activities from their primary assets. For example, P14 mentioned "When it comes to interacting with smart contracts, you usually take some precautions, such as not putting too much money in a single address. And when interacting with riskier dApps, you would create a new wallet."

Participants choose different types of wallet for specific activities based on their security perceptions. As discussed in 5.3.2, many participants believed that using MetaMask to interact with dApps, enhanced by third-party security extensions, lowered the risk of social threats. They often used it as a "frontend" for engaging with networks or experimenting, while saving hardware or smart contract wallets for storing larger crypto assets. P14 articulated this strategy: "I believe in the strategy of risk isolation. For instance, when I want to engage with a decentralized application [digital applications or programs that run on a blockchain], be it a DEX or a DAO, I'd opt for MetaMask. However, I only keep the necessary amount there. I often shift funds from my hardware wallet or Coinbase to MetaMask, treating MetaMask as a transitional platform." Some participants preferred the stability of centralized exchanges (CEX), keeping much of their crypto in custodial wallets, while others, cautious of CEX risks, used them only for buying crypto. This reflects Fröhlich et al.'s findings that users favor custodial wallets for daily transactions but turn to self-custodial or hardware wallets for long-term storage of larger sums [15].

6 DISCUSSION

Our interviews with 24 crypto wallet users delved into how and why users use different types of crypto wallets (RQ1), how their security perceptions differed across these wallets (RQ2), and the measures they took to secure these wallets (RQ3). Past research has primarily focused on users' general security perceptions and behaviors regarding wallets and has highlighted that users sometimes use multiple wallets. Our work provides a more in-depth and nuanced understanding of crypto users' wallet selection (as summarized in Table 3), security perceptions and behaviors, and multi-wallet usage across many wallet categories and devices — including, to our knowledge, the first account of how and why users use smart contract wallets. In this section, we discuss our findings and then share design implications for future wallets.

6.1 Factors influencing users' wallet selection and use

Our study reveals that the choice of various crypto wallets by users is influenced by factors such as usability, security, and social considerations.

[7]Etherscan is a popular Ethereum blockchain explorer and analytics platform, providing detailed information on transactions, smart contracts, addresses, and more. Similar platforms like Tezscan (Tezos) and Algo Explorer (Algorand) serve their respective blockchain networks.

6.1.1 Security Factors. Our participants expressed distinct security concerns and elaborated on how these perceptions shaped their choices of wallets and devices. We observed unique social cybersecurity concerns that our participants had about smart contract wallets, particularly in the processes of choosing, onboarding, and managing guardians. Due to these issues, our participants often preferred to employ their other devices as guardians rather than involving trusted individuals. Our study found that participants preferred mobile wallets for engaging in cryptocurrency trading or conducting basic transactions, such as sending and receiving funds from trusted contacts. First, they valued the enhanced privacy mobile wallets offer in public spaces. Second, they appreciated the smaller screen size, which they found useful in maintaining focus and minimizing human errors, particularly during outdoor use. However, when conducting more complex on-chain transactions such as interacting with decentralized applications, many participants preferred to use PC wallets because they allow for the use of third-party security extensions and because larger screens can surface more relevant information to avoid human errors. While many participants used a combination of both custodial and self-custodial wallets [15], we observed a divide in usage based on security considerations. Some opted for custodial wallets to safeguard their primary assets and to engage in trusted transactions, as they believed these wallets reduce the risk of human error and phishing. These participants kept only a minimal amount of funds in self-custodial wallets for more immediate transactions, thereby shielding the lion's share of their assets from the security risks they perceived in EOAs wallets.

Prior research has indicated that users often keep long-term, high-value crypto assets in hardware wallets [1, 46], a strategy that some of our participants also adopted. However, we found that most of the participants spread their assets across several wallets, and wallet types, to mitigate the risk of a single point of failure. Some of the participants even shifted away from hardware wallets because of the security concerns regarding manufacturer risks and their lack of protection against phishing attacks. Owing in part to social cybersecurity features like social account recovery and multi-signature transactions, some participants discussed moving their funds from hardware to smart contract wallets. In fact, we found that some participants believe that smart contract wallets provide comparable security to hardware wallets, but with a more friendly user experience.

6.1.2 Social Factors. Our study also reported novel insights into how cultural and social dynamics shape wallet choices among users. While prior research on Bitcoin adoption has talked about peer influence in learning about and adopting cryptocurrencies [39], our findings add a new dimension to this understanding. Participants in our study not only followed recommendations from friends and the wider community for wallet selection and security practices, but some also displayed a distinct preference for using digital wallets popular within their social circles. This tendency was rooted in deep trust in their friends' choices and a prevalent misconception that sharing the same wallets eases transactions among peers. Moreover, we uncovered a novel finding that cultural familiarity plays a significant role in shaping trust and design preferences. For instance, some of our participants from China expressed a preference for the Imtoken wallet, which was founded and predominantly staffed by Chinese professionals.

6.1.3 Usability Factors. While our study aligns with previous research in identifying users' needs as a driving factor in wallet and device choices [1, 15, 46], it also reveals novel insights into these preferences. Previous studies found that participants often chose mobile wallets for convenience and ease of access [1]. However, we found that mobile wallets are commonly chosen for basic transactions, such as sending and receiving cryptocurrency. Moreover, our study uniquely identifies a distinct preference among users who frequently use decentralized applications (dApps) for self-custodial Externally Owned Account (EOA) wallets on PCs. This preference is based on the enhanced functionality these wallets offer in terms of a seamless and more integrated connection with dApps. For instance, users can effortlessly link to a dApp for decentralized finance (DeFi) services and conduct digital asset trading directly without leaving the wallet interface on browser, unlike on mobile where switching between multiple apps is often necessary. This insight has not been reported in prior studies. Furthermore, our findings contribute new perspectives on how the design of the user interface (UI) and the overall user experience (UX) influence the adoption or abandonment of crypto wallets. Significantly, we observed a trend moving away from the exclusive use of hardware wallets, highlighting user concerns about their cumbersome UX. Additionally, many users expressed a preference for custodial wallets, which they believe offer a more user-friendly interface compared to other wallet types.

6.2 Social and Technological Security Measures

Cryptocurrencies have garnered a substantial user base, primarily due to their trustless nature, which eliminates the need for third-party centralized validators. However, it is essential to recognize that the concept of blockchain as a completely trustless system presents notable real-world usability challenges, particularly in the domains of private key management and wallet recovery. A novel finding in our study is that users consider the combination of social and technological strategies as an effective approach to achieving a balance between security and usability. Examples of such strategies include social recovery mechanisms, the use of multi-signature, and third-party security extensions, which aim to enhance wallet security. Social recovery allows wallet recovery through trusted contacts, multi-signature requires multiple transaction approvals, and security extensions guard against vulnerabilities like hacking. Prior work [1, 15, 39] has highlighted cryptocurrency users' knowledge and adoption of wallet security practices for key management. These include backing up wallets multiple times, utilizing multi-signature wallets, and disconnecting from the internet. Our study extends this prior work by surfacing novel security strategies users employ to tackle a range of security concerns, spanning key management to phishing and scams. These strategies include social recovery, guardian features, and employing browser extensions and wallet security alerts. Frequently, these strategies involve users leveraging personal connections: e.g., for sourcing advice, making sense of problems, and/or collaborating. For instance, participants often turned to friends for guidance on avoiding onboarding mistakes, investment advice, and applying

security practices (e.g., Two-factor authentication) in different situations. Participants also felt challenged in managing the risks introduced by friends and family members while learning about security through social relationships.

However, in employing these social cybersecurity tools and behaviors, challenges arose when deciding whom to trust, determining the level of control to give various individuals, and weighing the social capital cost of requesting security support from close contacts. For example, existing social cybersecurity features do not offer rewards to encourage guardians to help protect the crypto assets of their owners. Moreover, users expressed some concern that all Guardians specified for social recovery have equal privileges, even though users' trust in different Guardians may vary.

Beyond social cybersecurity measures, we found that participants employed a variety of other security strategies to protect their crypto assets. For example, similar to previous studies, many participants discussed using multiple wallets simultaneously [15]. One unique finding from our data is that among the many different wallets participants manage, they often assign specific activities to certain wallets based on their perceived strengths or vulnerabilities against particular risks. For instance, participants utilize self-custodial EOA wallets solely for on-chain interactions without storing substantial assets in them. Furthermore, they adopt tactics like security extensions and wallet security alerts to counteract the phishing risks associated with self-custodial EOAs wallets on browsers.

6.3 Design Recommendations

Redesign the social recovery and guardians feature. A primary concern for users avoiding self-custody wallets is the complexity of key management. However, placing their assets with a custodial wallet introduces them to risks associated with the platform and third parties. Smart contract wallets with social recovery features provide a middle-ground that helps users regain confidence in self-custodying their assets. Yet, our users have highlighted several problems with the existing implementations. Our participants suggested that existing social recovery features for smart contract wallets are overly simplistic and lack adequate social cybersecurity considerations. Moju-Igbene et al. introduce a design space for social cybersecurity controls, offering insights into enhancing controls' effectiveness by examining different dimensions: hierarchical governance, transparency, rewards, and privacy protection for guardians [35].

Hierarchical governance. In the present design, each guardian has equal rights, with actions needing approval from 50% of them. Every guardian is endowed with equal rights and control, applicable to the same actions. But trust in social relationships isn't just binary; it has shades and nuances. Users need more flexibility and detail in these social cybersecurity features. Wallets could categorize different controls based on risk level and allow users to determine the permissions they wish to delegate to specific individuals. For instance, a user might authorize a family member both to aid in wallet recovery and approve transactions, while permitting a friend solely to approve transactions.

Transparency. Currently, guardians can merely approve owners' requests without any details of the transaction or insights into who else has signed or is awaiting to sign. This absence of detail deprives guardians of the chance to critically evaluate the security implications of their signing actions. This lack of comprehensive information hinders guardians from fully understanding the security stakes of their actions. By providing these insights in wallets, guardians could be better equipped to make informed decisions, enhancing protection for the wallet owner. Yet, this solution could raise some privacy concerns for wallet owners because all their detailed transactions are exposed to the guardians.

Reward system for guardians. Many participants indicated they only added their own wallet addresses instead of friends as guardians due to worries about the social capital expense. They are apprehensive about overly burdening friends with transaction approvals. This underscores the absence of a reward and "penalty" mechanism in the wallet's social cybersecurity design. Offering monetary (e.g., tokens, NFTs) or non-monetary rewards (e.g., reputation score or ranking) for guardians' signing actions can serve as an incentive and a form of positive feedback, encouraging them to safeguard the owner's security. Rather than simplifying human behavior to a basic model of seeking rewards, the proposed reward system is designed to foster trust-building and enhance social interaction between wallet owners and guardians. Prior research [50, 52] supports the idea that rewards can improve response rates among friends, thereby maintaining positive relationships. Implementing such a system could also lessen the burden on owners when involving others in their security measures and provide an avenue for introducing non-users to the web3 space via social connections.

Guardians privacy. Participants expressed concerns about the potential inference of personal relationships through the analysis of public on-chain data. By approving owners' transactions or wallet social recovery, guardians' wallet addresses are public on blockchain and expose them to potential privacy risks. We suggest the integration of advanced cryptographic techniques like zero-knowledge proof (ZKP) [41]to mitigate these concerns. Zero-knowledge proof is a cryptographic method that enables one party to prove the truth of a statement to another party without revealing any additional information. In the context of social cybersecurity, employing zero-knowledge proof could allow guardians to approve the validity of transactions or assist in wallet recovery without exposing their wallet addresses or other identifiable information on the blockchain. This approach could significantly enhance privacy and security in blockchain transactions, providing a solution to the privacy concerns raised by participants.

Redesign the wallet security alert. Phishing and scams remain a major security concern and impact how participants choose wallets. Addressing phishing and scams in cryptocurrency is challenging, especially in the context of self-custody where users have no recourse if they fall prey. These threats not only stem from traditional channels like emails, SMS texts, and phone calls but also arise from airdrops. Any individuals or institutions with knowledge of your wallet address can send crypto assets and accompany them with short text messages (in-wallet messages). This makes it challenging for users to safeguard themselves. The prevalence of these

	Key Management			Device		
Wallet Type	Self-Custodial EOAs Wallet (MetaMask)	Smart Contract Wallet (Argent)	Custodial Wallet (Coinbase)	Hardware Wallet (Ledger)	Mobile Wallet (Trust)	PC Wallet (MetaMask)
Description	Users have full control over their private keys and thus their funds. Direct blockchain interaction and high security responsibility are key features	Operates through smart contracts on a blockchain, allowing programmable rules and enhanced security features like recovery options and multi -signature requirements	Managed by a third party that controls the private keys. These wallets offer ease of use and integrated services, but with potential risks of third-party control	A physical device that stores private keys offline, provid -ing high security against online threats	A wallet in the form of a mobile app, offering convenience and ease of use for managing crypto assets on-the-go	A wallet functioning on a personal computer, available as either a separate application or as a browser extension.
Reasons to use	1. [Usability] Interacting with decentralized applications 2. [Security] Complete ownership of private key and assets	1. [Social Factor & Usability]User friendly social-based recovery and management of wallets 2. [Security] Enhanced programmable security	1. [Social Factors]Friends' recommendations 2. [Usability] User-friendly interfaces 3. [Usability & Security] Trust and confidence on centralized platforms 4. [Security]Using multiple wallets for asset storage to mitigate	1. [Security]Storing large amounts of crypto assets 2. [Security]The offline nature of hardware wallets enhances protection against security attacks	1. [Usability]Portability and ease of access at any location 2. [Security]Cryptocurrency trading or basic transactions such as sending/receiving crypto 3. [Security]Enhanced focus and privacy in public space	1. [Security]Large screen for checking details and reducing transaction errors 2. [Security]High-stake transactions and complex on-chain operations:such as interacting with Decen -tralized Finance (DeFi) platforms 3. [Security]Security exten -sions on browser providing second layer of protection
Reasons not use	1. [Usability] Challenge of key management 2. [Security] Social threat concerns, such as scams and phishing	1. [Social Factor & Usability]Dissatisfaction with social features in smart contract wallets and challenges in choosing, onboarding and managing guardians 2. [Security] Misconceptions of smart contract wallet mechanism	1. [Security] Custodial platform collapse and legal uncertainties	1. [Usability]Cumbersome user experience 2. [Security]Concerns over hardware wallets' security against phishing attacks 3. [Security]Concerns over potential private key exposure to manufacturer of hardware wallets or third parties	1. [Usability]Compact screen and user interface designs are insufficient for managing intricate interactions between wallets and various platforms, like decentralized finance (DeFi) systems	1. [Usability]Mobile wallets are the most appropriate for their primary wallet usage: basic transactions such as sending/receiving crypto

Table 3: Comparison of Six Wallet Types and Insights into User Preferences for Wallet Selection: This table categorizes the first three wallets based on their key management strategies. The later three are classified by the devices they operate on. Additionally, the table contains potential overlaps between these categories, such as wallets utilizing smart contracts that may also function as mobile wallets. The table features three rows sequentially presenting the wallet type description, reasons for use/not use of certain types of wallets, and each reason's classification into usability, security, or social factors.

scams is one reason why some participants gravitate towards custodial wallets, trusting that their customer support helps mitigate the risks associated with phishing and scams. Moreover, those who still opted for self-custody leaned towards using browser wallets over mobile ones for on-chain interactions. By incorporating third-party security extensions, they feel better shielded from phishing and scams.

Nevertheless, our participants' preferences and risk perceptions revealed an admittedly unsurprising need for greater support to help users identify phishing scams *at the moment a transaction occurs*. Beyond integrating machine learning techniques to automatically filter and block phishing/scam addresses and messages, wallets should also focus on delivering clear, comprehensive, and unambiguous security alerts. Participants turn to security extensions like Fire to address the ambiguous security warnings from wallets. Some wallets merely display the risk level and a brief disclaimer to warn users of potential threats. Users typically seek an explanation regarding the source of the risk, wanting to fully comprehend what they're signing for, especially when interacting with smart contracts. We advocate for guiding users with transparent warning messages, which could include details about the simulated outcomes of their signatures, as well as additional security metrics related to the address or contracts they are interacting with. This information could be sourced from third parties (e.g., Etherscan, OpenSea), highlighting cues such as user-reported phish/scam, the verification status of the contract code, and its transaction count and total locked value.

Verification and remediation of phishing/scam in wallets. Despite the rampant occurrence of phishing and scams, users are either largely unaware of remediation strategies for financial losses in cryptocurrency or such strategies simply do not exist. According to our findings and existing literature, users generally do not attempt to recover their keys or reclaim lost funds following an incident [29]. Many times, they identify and acknowledge their financial losses from phishing or scams on their own or with assistance from friends. Participants who experienced asset loss on self-custodial wallets often place the blame on themselves and come to terms with their losses, all without sufficiently understanding security precautions. To our knowledge, wallets presently lack features that assist users in monitoring, verifying, tracing, and educating incidents of phishing and scams. Borrowing from strategies utilized by credit card companies, smart contract wallets could detect anomalous

transactions that divert from a user's typical patterns and pause them prior to a second confirmation. Furthermore, post-incident, it is vital to assist users in ascertaining the aftermath and rationale of the incidents. This aids in shielding them from potential scams on social media platforms where they might seek explanations or remedies for their losses. Within wallets, AI agents or chatbots can be designed to help users review past activities, pinpoint actions that led to the incident, and assess on-chain data to track down misplaced funds. Additionally, chatbots could deliver tailored security education based on the user's specific incidents, thereby equipping them with advanced security measures and shielding them from future phishing attempts and scams. However, when implementing this chatbot feature, it is crucial to approach it with sensitivity. Emphasis on empathy and a gentle tone are essential to help users navigate their trauma.

6.4 Limitations and Future Work

Inherent to qualitative research, our study may not be entirely representative of the whole population of crypto wallet users. We endeavored to gather a sample diverse enough within the cryptocurrency community. We ensured diversity by recruiting participants from varied channels and by seeking a mix of backgrounds. Compared to previous qualitative studies on crypto users [15, 39, 46], our sample is equally diverse, if not more so, in terms of participant age, gender, technical background, and crypto experience. However, all of our participants were in the United States. Given the diverse regulations and policies in different countries, crypto users in regions with stricter restrictions might exhibit distinct behaviors and perceptions. However, these regional variations were not the focus of our study.

Future research could address the demographic and geographical limitations by conducting large-scale survey studies or cross-cultural user studies. Additionally, we highlighted design recommendations related to social cybersecurity features, wallet security alerts, and incident remediation mechanisms within wallets. One such suggestion was to give owners the option to reveal more transaction details to guardians, as well as the actions taken by other guardians. However, many questions regarding the privacy and control of both owners and guardians remain unanswered. For instance, who should have the authority over transaction details or the sharing of guardian signature statuses? Future studies could delve deeper into this design space, examining the trade-offs between usability and security, along with the balance between privacy and transparency.

7 CONCLUSION

We conducted semi-structured interviews with 24 crypto users to explore the reasons behind their wallet choices, as well as their security perceptions and practices associated with different wallet types. We found that participants distributed their assets across various wallets to mitigate the risks of a single point of failure. They chose different wallets for specific tasks based on their unique security perceptions of each wallet. Participants viewed smart contract wallets as being as secure as hardware wallets, using them for high-stakes storage, while they preferred EOAs wallets on browsers for complex transactions, often leveraging third-party security extensions. Our study also highlighted some novel practices of participants, such as adopting social cybersecurity measures and using third-party security extensions. Yet many questions remained unanswered. We advocate crypto wallets as a particularly interesting and timely problem space for usable security and privacy research.

ACKNOWLEDGMENTS

We thank our participants for sharing their insights.

REFERENCES

[1] Svetlana Abramova, Artemij Voskobojnikov, Konstantin Beznosov, and Rainer Böhme. 2021. Bits under the mattress: Understanding different risk perceptions and security behaviors of crypto-asset users. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, USA, 1–19.

[2] Emad Almutairi and Shiroq Al-Megren. 2019. Usability and security analysis of the KeepKey wallet. In *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, Seoul, South Korea, 149–153.

[3] Abdulla Alshamsi and Peter Andras. 2019. User perception of Bitcoin usability and security across novice users. *International Journal of Human-Computer Studies* 126 (2019), 94–110.

[4] Muhammad Nasir Mumtaz Bhutta, Amir A Khwaja, Adnan Nadeem, Hafiz Farooq Ahmad, Muhammad Khurram Khan, Moataz A Hanif, Houbing Song, Majed Alshamari, and Yue Cao. 2021. A survey on blockchain technology: Evolution, architecture and security. *Ieee Access* 9 (2021), 61048–61073.

[5] Virginia Braun, Victoria Clarke, and Nikki Hayfield. 2022. 'A starting point for your journey, not a map': Nikki Hayfield in conversation with Virginia Braun and Victoria Clarke about thematic analysis. *Qualitative research in psychology* 19, 2 (2022), 424–445.

[6] Karoline Busse, Mohammad Tahaei, Katharina Krombholz, Emanuel von Zezschwitz, Matthew Smith, Jing Tian, and Wenyuan Xu. 2020. Cash, Cards or Cryptocurrencies? A Study of Payment Culture in Four Countries. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, Seoul, South Korea, 200–209.

[7] You-Ping Chen and Ju-Chun Ko. 2019. CryptoAR wallet: A blockchain cryptocurrency wallet application that uses augmented reality for on-chain user data display. In *Proceedings of the 21st International Conference on Human-Computer Interaction with Mobile Devices and Services*. ACM, New York, NY, USA, 1–5.

[8] CoinMarketCap. 2023. Cryptocurrency Market Capitalizations | CoinMarketCap. https://coinmarketcap.com/

[9] Chris Dannen. 2017. *Introducing Ethereum and solidity*. Vol. 1. Springer, Berlin, Germany.

[10] Alexander De Luca, Sauvik Das, Martin Ortlieb, Iulia Ion, and Ben Laurie. 2016. Expert and {Non-Expert} attitudes towards (secure) instant messaging. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, USA, 147–157.

[11] 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).

[12] Benjamin Fabian, Tatiana Ermakova, Jonas Krah, Ephan Lando, and Nima Ahrary. 2018. Adoption of security and privacy measures in bitcoin–stated and actual behavior. *Available at SSRN 3184130* (2018).

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

[14] 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.

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

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

[17] Michael Fröhlich, Franz Waltenberger, Ludwig Trotter, Florian Alt, and Albrecht Schmidt. 2022. Blockchain and cryptocurrency in human computer interaction: a systematic literature review and research agenda. In *Designing Interactive Systems Conference*. 155–177.

[18] Shange Fu, Qin Wang, Jiangshan Yu, and Shiping Chen. 2022. FTX collapse: a Ponzi story. *arXiv preprint arXiv:2212.09436* (2022).

[19] Hiroshi Fujiki. 2023. Central bank digital currency, crypto assets, and cash demand: evidence from Japan. *Applied Economics* (2023), 1–19.

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

[21] Pascal Gauthier. 2023. Ledger recover: A message from Pascal Gauthier, chairman &; CEO at Ledger. https://www.ledger.com/blog/ledger-recover-a-message-from-pascal-gauthier-chairman-ceo-at-ledger

[22] Hyeji Jang, Sung H Han, and Ju Hwan Kim. 2020. User perspectives on blockchain technology: user-centered evaluation and design strategies for dapps. *IEEE Access* 8 (2020), 226213–226223.

[23] Hyeji Jang, Sung H Han, Ju Hwan Kim, and Kimin Kown. 2020. Identifying and Improving Usability Problems of Cryptocurrency Exchange Mobile Applications Through Heuristic Evaluation. In *Advances in Usability, User Experience, Wearable and Assistive Technology: Proceedings of the AHFE 2020 Virtual Conferences on Usability and User Experience, Human Factors and Assistive Technology, Human Factors and Wearable Technologies, and Virtual Environments and Game Design, July 16-20, 2020, USA*. Springer, 15–21.

[24] Hyeji Jang, Sung H Han, Ju Hwan Kim, and Kimin Kwon. 2021. Usability evaluation for cryptocurrency exchange. In *Convergence of Ergonomics and Design: Proceedings of ACED SEANES 2020*. Springer, 192–196.

[25] Adam Jenkins, Maria Wolters, and Kami Vaniea. 2023. To Patch, or not To Patch? That is the Question: A Case Study of System Administrators' Online Collaborative Behaviour. *arXiv preprint arXiv:2307.03609* (2023).

[26] Ali Kazerani, Domenic Rosati, and Brian Lesser. 2017. Determining the usability of bitcoin for beginners using change tip and coinbase. In *Proceedings of the 35th ACM International Conference on the Design of Communication*. 1–5.

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

[28] Irni Eliana Khairuddin, Corina Sas, Sarah Clinch, and Nigel Davies. 2016. Exploring motivations for bitcoin technology usage. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. 2872–2878.

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

[30] Minha Lee, Lily Frank, and Wijnand IJsselsteijn. 2021. Brokerbot: A cryptocurrency chatbot in the social-technical gap of trust. *Computer Supported Cooperative Work (CSCW)* 30, 1 (2021), 79–117.

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

[32] Easwar Vivek Mangipudi, Udit Desai, Mohsen Minaei, Mainack Mondal, and Aniket Kate. 2022. Uncovering impact of mental models towards adoption of multi-device crypto-wallets. *Cryptology ePrint Archive* (2022).

[33] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. *Proceedings of the ACM on human-computer interaction* 3, CSCW (2019), 1–23.

[34] Tamir Mendel and Eran Toch. 2023. Social Support for Mobile Security: Comparing Close Connections and Community Volunteers in a Field Experiment. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–18.

[35] Eyitemi Moju-Igbene, Hanan Abdi, Alan Lu, and Sauvik Das. 2022. " How Do You Not Lose Friends?": Synthesizing a Design Space of Social Controls for Securing Shared Digital Resources Via Participatory Design Jams. In *31st USENIX Security Symposium (USENIX Security 22)*. 881–898.

[36] Md Moniruzzaman, Farida Chowdhury, and Md Sadek Ferdous. 2020. Examining usability issues in blockchain-based cryptocurrency wallets. In *Cyber Security and Computer Science: Second EAI International Conference, ICONCS 2020, Dhaka, Bangladesh, February 15-16, 2020, Proceedings 2*. Springer, 631–643.

[37] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. *Decentralized business review* (2008).

[38] Corina Sas and Irni Eliana Khairuddin. 2015. Exploring trust in Bitcoin technology: a framework for HCI research. In *Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction*. 338–342.

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

[40] Fred Steinmetz. 2021. *Behavioural clusters of cryptocurrency users: Frequencies of non-speculative application domains*. Technical Report. BRL Working Paper Series.

[41] Xiaoqiang Sun, F Richard Yu, Peng Zhang, Zhiwei Sun, Weixin Xie, and Xiang Peng. 2021. A survey on zero-knowledge proof in blockchain. *IEEE network* 35, 4 (2021), 198–205.

[42] Saurabh Suratkar, Mahesh Shirole, and Sunil Bhirud. 2020. Cryptocurrency wallet: A review. In *2020 4th international conference on computer, communication and signal processing (ICCCSP)*. IEEE, 1–7.

[43] Melanie Swan. 2015. *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.".

[44] Friedhelm Victor and Bianca Katharina Lüders. 2019. Measuring ethereum-based erc20 token networks. In *Financial Cryptography and Data Security: 23rd International Conference, FC 2019, Frigate Bay, St. Kitts and Nevis, February 18–22, 2019, Revised Selected Papers 23*. Springer, 113–129.

[45] Artemij Voskobojnikov, Svetlana Abramova, Konstantin Beznosov, and Rainer Böhme. 2021. Non-Adoption of Crypto-Assets: Exploring the Role of Trust, Self-Efficacy, and Risk.. In *ECIS*.

[46] Artemij Voskobojnikov, Borke Obada-Obieh, Yue Huang, and Konstantin Beznosov. 2020. Surviving the cryptojungle: Perception and management of risk among North American cryptocurrency (non) users. In *International Conference on Financial Cryptography and Data Security*. Springer, 595–614.

[47] Artemij Voskobojnikov, Oliver Wiese, Masoud Mehrabi Koushki, Volker Roth, and Konstantin Beznosov. 2021. The u in crypto stands for usable: An empirical study of user experience with mobile cryptocurrency wallets. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–14.

[48] Shuai Wang, Wenwen Ding, Juanjuan Li, Yong Yuan, Liwei Ouyang, and Fei-Yue Wang. 2019. Decentralized autonomous organizations: Concept, model, and applications. *IEEE Transactions on Computational Social Systems* 6, 5 (2019), 870–878.

[49] Yuxi Wu, W Keith Edwards, and Sauvik Das. 2022. SoK: Social Cybersecurity. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1863–1879.

[50] Zhuohao Jerry Zhang, Smirity Kaushik, JooYoung Seo, Haolin Yuan, Sauvik Das, Leah Findlater, Danna Gurari, Abigale Stangl, and Yang Wang. 2023. {ImageAlly}: A {Human-AI} Hybrid Approach to Support Blind People in Detecting and Redacting Private Image Content. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*. 417–436.

[51] Zhixuan Zhou, Tanusree Sharma, Luke Emano, Sauvik Das, and Yang Wang. 2023. Iterative Design of An Accessible Crypto Wallet for Blind Users. *arXiv preprint arXiv:2306.06261* (2023).

[52] Haiyi Zhu, Sauvik Das, Yiqun Cao, Shuang Yu, Aniket Kittur, and Robert Kraut. 2016. A market in your social network: the effects of extrinsic rewards on friendsourcing and relationships. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. 598–609.

A APPENDICES

A.1 Interview Protocol

A.1.1 Part 1: Opening. Thank you so much for taking the time to participate in our user study. My name is [INTERVIEWER NAME] and I'm a researcher from the [UNIVERSITY NAME]. Our research is trying to understand users' experience and practices with crypto wallets. Throughout our discussion, I'll be asking you a series of questions. Remember, there's no right or wrong answer. We're keenly interested in your unique experiences and opinions.

Would it be okay if I audio record our session for note-taking accuracy? Please be assured that your identity will be kept confidential, and your real name won't be mentioned in any of our publications or presentations. You're free to ask questions or pause the interview at any point. May I have your consent to record this call?

A.1.2 Part 2: Experiecne with cryptocurrency and wallets usage. Let's begin by discussing your past experience with cryptocurrency. Which tools or platforms have you utilized for managing, storing, or trading them?

- Tell us a bit about your prior crypto exposure, including when and how you got to know cryptocurrencies?
- What was the first wallet you ever used?
- Can you share your experience about how you became familiar with it?
- What crypto management tools have you used? And which of them are you currently using?

- If you use multiple wallets, how do you store your assets across these wallets? Why?
- How do you manage these wallets in your regular usage?
- What activities do you carry out with these wallets? Could you enumerate the tasks you perform for each wallet you are using?
- Which devices do you use these wallets on (Mobile/Personal computer/other)?
- If you utilize different devices, can you estimate the usage percentage for each?
- What are your reasons for using these wallets on these specific devices?
- Which wallet did you use the most?
- What do you think are the pros and cons of this wallet?
- Have you ever encountered any difficulties or challenges using different crypto wallets? On mobile or browser? Could you give me a concrete example?

A.1.3 Part 3: Security and privacy perceptions on wallets.

- (If the participant has used a hardware wallet/smart contract wallet) When did you start using hardware wallets/smart contract wallet?
- What triggered the decision to use a hardware wallet/smart contract wallet?
- When you use hardware wallets/smart contract wallet, did you have any concerns with your crypto assets?
- (If the participant do not use hardware wallets/smart contract wallet anymore) why did you leave hardware wallets/smart contract wallet?
- (Based on participants' answer in previous section), When you use custodial/self-custodial EOA/self-custodial smart contract wallets on your personal computer, have you had any concern toward your crypto assets? What are those concerns?
- How likely are those concerns mentioned could happen to you?
- How did you manage those concerns?
- (Based on participants' answer in previous section), When you use custodial/self-custodial EOA/self-custodial smart contract wallets on your mobile devices, have you had any concern toward your crypto assets? What are those concerns?
- How likely are those concerns mentioned could happen to you?
- How did you manage those concerns?
- I have a couple of examples of threats on wallets. It is not an exhaustive list; feel free to talk about other types of risks if it comes into your mind:
  - Losing crypto-assets by my own mistakes
  - Losing crypto-assets by financial fraud (e.g. Pump and Dump)
  - Losing crypto-assets by social threat (e.g. Scams and phishing)
  - Losing crypto-assets by platform risk (e.g. security vulnerability of wallets and regulation risk of exchanges)
  - Legal uncertainty for the users of crypto-assets and possible prosecution
  - Losing virtual or real-world identity (De-Anonymisation)
  - Receive tainted coin (money from illegal sources, e.g. laundered money)
  - Other threats not mentioned above
- Please select the your concerning threats for each type of wallet (Based on participants' answer in previous section). Please explain why you are concerned about these threats?
- How did you manage these concerns on different wallets?

A.1.4 Part 4: User security practices and desired features on wallets.

- What security features do you know wallets offer to safeguard users' crypto assets?
- What security features have you used on different wallets?
- How well does that work for you? Have you noticed any benefits or encountered any challenges with these security features?
- I have a couple of examples of security practices current wallets provide: (It is not an exhaustive list; feel free to talk about other types of information if it comes into your mind)
  - Two-Factor Authentication
  - Wallet backup in cloud
  - Multisignature
  - Proactive security alerts (e.g. phishing alert on wallet or third party extensions)
  - Lock your wallets with fingerprint
  - Other security features
- Are you aware of these security practices? How did you know these security practices?
- Have you used any of the security practices mentioned above? On which kind of wallet?
- How do you expect privacy and the security concerns to be addressed in crypto wallets?
- If not, what prevents you from utilizing them?
- Have you encountered any incidents?
- Could you please share details about your experience if any?
- Have you lost a substantial amount of crypto-assets at a time?
- What could be the reasons for your incident?
- How did you deal with the incident?
- Did you do anything differently before and after the incident/crypto assets loss? Why?