Of Secrets and Seedphrases: Conceptual Misunderstandings and Security Challenges for Seed Phrase Management among Cryptocurrency Users

Farida Eleshin*
Human Computer Interaction Institute
Carnegie Mellon University
Pittsburgh, Pennsylvania, USA
feleshin@andrew.cmu.edu

Qi Sun*
Human Computer Interaction Institute
Carnegie Mellon University
Pittsburgh, Pennsylvania, USA
1067557192sunqi@gmail.com

Mengzhe Ye
Human Computer Interaction Institute
Carnegie Mellon University
Pittsburgh, Pennsylvania, USA
mengzhey@andrew.cmu.edu

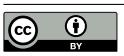
Sauvik Das
Human-Computer Interaction Institute
Carnegie Mellon University
Pittsburgh, Pennsylvania, USA
sauvik@cmu.edu

Jason I. Hong
Human-Computer Interaction Institute
Carnegie Mellon University
Pittsburgh, Pennsylvania, USA
jasonh@cs.cmu.edu

Abstract

Cryptocurrency adoption has surged dramatically, with over 500 million global users. Despite the appeal of self-custodial wallets, which grant users control over their assets, these users often struggle with the complexities of securing seed phrases, leading to substantial financial losses. This paper investigates the behaviors, challenges, and security practices of cryptocurrency users regarding seed phrase management. We conducted a mixed-methods study comprising semi-structured interviews with 20 participants and a comprehensive survey of 643 respondents. Our findings reveal significant gaps in users' understanding and practices around seed phrase security and the circumstances under which users share their seed phrases. We also explore users' mental models of shared accounts and strategies for handling cryptocurrency assets in the event of death. We found that the majority of our participants harbored significant misconceptions about seed phrases that could expose them to significant security risks — e.g., only 43% could correctly identify an image of a seed phrase, many believed they could reset their seed phrase if they lost them. Moreover, only a minority have engaged in any estate planning for their crypto assets. By identifying these challenges and behaviors, we provide actionable insights for the design of more secure and user-friendly cryptocurrency wallets, ultimately aiming to enhance user confidence in managing their crypto assets reduce their exposure to scams and accidental loss of assets, and simplify the creation of bequeathment plans.

*Both authors contributed equally to this research.



CHI '25, Yokohama, Japan

ACM ISBN 979-8-4007-1394-1/25/04
https://doi.org/10.1145/3706598.3713209

CCS Concepts

• **Security and privacy** → *Human and societal aspects of security and privacy*; Usability in security and privacy;

Keywords

seedphrase, private key, cryptocurrency wallets, backups, custodial, non-custodial, usability

ACM Reference Format:
Farida Eleshin, Qi Sun, Mengzhe Ye, Sauvik Das, and Jason I. Hong. 2025. Of Secrets and Seedphrases: Conceptual Misunderstandings and Security Challenges for Seed Phrase Management among Cryptocurrency Users. In *CHI Conference on Human Factors in Computing Systems (CHI '25), April 26–May 01, 2025, Yokohama, Japan.* ACM, New York, NY, USA, 19 pages. https://doi.org/10.1145/3706598.3713209

1 Introduction

An estimated 575 million people worldwide own some form of cryptocurrency — up from just 5 million in 2016 [3]. A separate 2024 survey estimates that nearly 40% of all adults in the U.S. own cryptoassets, and 63% of these crypto users hope to obtain more such assets over the next year [1]. This surge in cryptocurrency adoption has attracted both experienced and inexperienced investors to the crypto space [49], many of whom have limited knowledge of cryptographic concepts such as seed phrases and private keys [5, 28]. Yet, for the estimated 70% of users who self-custody at least some of their crypto assets [4], knowledge of these concepts — and how to secure them — is essential to protecting their assets against theft and device failure.

A significant security touch point for those who use self-custodial wallet software (like MetaMask and Coinbase Wallet) is the *seed phrase*: a list of human readable words (typically twenty-four words) from which the user's private key can be derived. Anyone who has access to a user's seed phrase can get full access to the cryptocurrency assets associated with its corresponding public key address

Figure 1: An example of a seed phrase. A seed phrase is a list of words that can be used to recover one's private key for cryptocurrency wallets. For Bitcoin wallets, a seed phrase is typically 24 words.

[35]. Mismanagement of one's seed phrase has already lead to irreversible losses, with an estimated $1.7 billion USD in cryptocurrency having been stolen from self-custodial wallets in 2023 [32].

This mismanagement occurs because, as noted by prior work, users find managing cryptographic keys and seed phrases to be complex [7, 15, 43, 44]. Trust and the usability of digital wallets are notable issues [23, 24, 48]. Some individuals misunderstand the cryptographic elements that underpin cryptocurrencies [18, 30]. Others, especially novices, find dealing with security keys to be daunting [14]. In the context of cryptocurrencies, these challenges are not merely inconvenient, they can cause serious errors and financial loss, for example if passwords are forgotten [24] or key pairs are accidentally erased [43]. While past work discusses the complexities of seed phrase management for end-users, we don't yet understand how cryptocurrency users attempt to secure their seed phrases in practice, how they learn about seed phrase security, how they respond to breaches in seed phrase security, and how these practices generalize across a broad population of users. Without this understanding, it is difficult to design systems that can assist users with securing their phrases. Thus, we ask:

RQ1 How do users secure their seed phrases, if at all? Where do they learn these strategies?

RQ2 How do experiences with seed-phrase related breaches influence users' behaviors and practices regarding seed phrase security and risk awareness?

Recognizing that requiring users to manage and secure their own seed phrases is a limiting factor for widespread adoption and security, many cryptocurrency projects are now exploring social cybersecurity mechanisms to simplify wallet recovery and security [47]. By understanding the circumstances under which users are more likely to share seed phrases, such as in social or collaborative settings, researchers and practitioners can design targeted interventions to raise awareness about the risks involved and provide users with tools to protect their accounts[10]. Thus, we also ask:

RQ3 When, why, and how do users share seed phrases with one another? What are users' mental models and practices about shared accounts?

RQ4 How do people manage inheritance and bequeathment of seed phrases in the event of their passing?

We employed a two-phased, mixed-methods approach to answer our research questions. We started with semi-structured interviews with 20 participants, to understand a broad range of strategies that users employ, information sources that users rely upon, and social practices with respect to securing their seed phrases. We followed up with a survey of 643 respondents, to help generalize these insights to a broader and more representative sample population.

Our study revealed widespread confusion and inadequate management of seed phrases. For example, only 43.4% of our survey participants were able to correctly recognize an image of a seed phrase. Among those who could correctly recognize a seed phrase, around 58% believed they could choose and reset their seed phrases. Novices especially struggled with seed phrase security, but both experienced and novice users reported falling prey to cryptocurrency scams (20% vs. 29%). Finally, only a small minority of participants had contingency plans for transferring their crypto assets upon death or incapacity. Although 22% of participants shared seed phrases for recovery purposes, many participants acknowledged the importance of planning for account recovery but did not take corresponding actions. This lack of estate planning is especially dangerous for self-custodial cryptocurrency contexts where third-party custodians may not be able to steward the transfer of wealth.

2 Background

Self-custody involves manually managing one's assets through a cryptocurrency wallet, unlike "hosted" or "custodial" solutions where third-party custodians like Coinbase or Binance manage the logistics of interacting with the blockchain. "Not your keys, not your crypto" is a common credo among many cryptocurrency users, underscoring the principle that if you do not control your private keys, you do not truly own your cryptocurrency.

Self-custody provides protection against counterparty risk and regulatory uncertainty. However, it also exposes users to security risks such as phishing, smart contract exploits, and scams [2].

A *cryptocurrency wallet* is a digital tool used to interact with blockchain networks, enabling users to send and receive cryptocurrencies. It stores the private and public keys necessary for transactions and monitors asset balances across various blockchains [5, 19, 21]. Wallets come in different forms, including software, hardware, and paper wallets, and can be categorized along a number of dimensions.

One categorization is hot and cold wallets [19]. Hot wallets, being directly linked to the Internet, are more susceptible to being targeted by malicious attacks. Typical forms include software like desktop apps, mobile apps, or browser extensions. In contrast, cold wallets are usually offline, providing better security but at the cost of convenience. These include hardware wallets, paper wallets, or even memorized "brain" wallets [13].

An alternative categorisation is custodial and noncustodial wallets [5]. *Custodial wallets*, which are services provided by third parties, are responsible for the management of keys [5]. These wallets are popular among users due to their user-friendly nature, as they create a layer of abstraction that eliminates the need for users to understand the underlying cryptography. An example of such third-party services can be seen in cryptocurrency exchanges [5], where users' funds are stored in a combined manner using both

hot and cold wallets. Users do not have complete control over their crypto-assets, but are given assurances that they will be able to withdraw their assets if they choose to do so. Therefore, exchanges offer some of the functionalities that are typically associated with conventional wallets, allowing users to utilize them as such [5]. However, it is important to note that storing large amounts of assets in exchanges can be risky, as there is a potential for permanent financial losses in the event of shutdowns or hacking incidents [31]. Two infamous such incidents include the Mt. Gox cryptocurrency exchange "hack" in which 850,000 bitcoin was lost to third-party attackers (worth approximately 82 billion USD as of December 2024), and the more recent FTX exchange bankruptcy.

In contrast, *non-custodial wallets* give users the power to directly oversee their keys, offering personalization and autonomy [40, 43]. Examples include MetaMask, Coinbase Wallet, Electrum, and mobile wallets like Trust Crypto Wallet [5]. However, non-custodial wallets place a significant security burden on users [22] and can lead to errors that are hard to fix. For example, if users don't protect their private keys or seed phrases, they can lose their assets.

3 Related Work

We discuss two areas of related work, namely past work on usability and people's perceptions of cryptocurrency wallets, and past work on seed phrases specifically.

3.1 Usability and User Perceptions of Cryptocurrency Wallets

Prior studies reveal that users of cryptocurrency wallets vary in their security choices and adopt diverse methods for protection [15, 43].

Previous work has also studied the security measures employed by cryptocurrency wallet users, including their behavior and the mental models they adopt while using their wallets [30, 44]. These studies all emphasize the importance of seed phrases, which are critical for protecting cryptocurrency wallets [27].

Past work has identified motivations, risk assessment, and coin management tool usage as key themes in user experience with mobile cryptocurrency wallets. One study found that users' choice of coin management tools is influenced by their knowledge, understanding of security practices, and their intent to use cryptocurrencies as an investment or as a currency [44]. Another study found that users are motivated by financial, ideological, and technical interests, and they assess and balance key risks such as human error, betrayal, and malicious attacks [17].

Other work has highlighted the security risks of weak passwords and stressed the importance of strong authentication mechanisms for Bitcoin wallets [42]. A study on cryptocurrency tools found that they are not effective in mitigating threats arising from users' misconceptions about security and privacy [30]. Consequently, users often struggle to securely manage their private keys or mistakenly believe that they are anonymous. This can lead to financial losses and fraud [30].

To understand the risks and concerns of cryptocurrency users, one study analyzed the behavior and perceptions of 395 crypto-asset users [5]. This study found that users can be classified into three groups based on their security practices and motivations: cypherpunks, hodlers, and rookies. Cypherpunks and hodlers prefer non-custodial wallets to maintain control over their keys, while rookies opt for custodial solutions due to their lower level of confidence. The study suggests that wallets should be customized based on user profiles and that effective risk communication and transparent key management are essential for improving security practices [ibid].

Several studies have highlighted the challenges users face in handling secure keys [15, 18, 20, 43, 45]. The tools available for managing these keys are often complex and difficult to use. This lack of user-friendly design exposes users to various risks, as even small mistakes or vulnerabilities in security measures could result in permanent loss without any possibility of recovering their funds [25]. Both experienced users and newcomers can lose money due to the complexity of key management, simple errors, or security breaches [25]. For example, it is estimated that millions of dollars worth of bitcoins have been permanently lost because individuals have misplaced or forgotten their keys [38, 39].

Our study builds on past work by delving deeper into the intricacies of user interactions with cryptocurrency wallets, in particular focusing on the nuances of seed phrase management and the widespread confusion surrounding it. Unlike previous studies that often provide a high-level overview of security practices and user motivations, our research provides a detailed analysis of seed phrase usage. Furthermore, we examine contingency planning aspects of digital asset management, an area that has been largely neglected in past research. Previous work in this space has been primarily legal articles discussing whether cryptocurrencies can be considered legal inheritable assets [36] and arguments for involving lawyers or other third parties for supervision and assistance [37]. Our research analyzed user data to understand the current state and challenges of cryptocurrency inheritance planning. This focus on practical and often overlooked aspects of cryptocurrency management offers new insights and critical perspectives that extend and enhance the existing literature.

3.2 Seed Phrases Management Practices - Security Practices, Usability, Perception, and Mental Models

Past research suggests that users recognize the importance of seed phrases but struggle with their complexity, leading to a variety of backup strategies of varying levels of effectiveness [31]. For example, users commonly employ insecure practices for storing and backing up seed phrases, such as writing them down on paper or storing them digitally in unprotected locations, increasing the risk of theft or loss [14]. Prior work also discusses how misconceptions about seed phrases can lead to risky behaviors, highlighting the need for user education on seed phrase security and proper management practices [28, 44].

Voskobojnikov et al. explored the perceptions and management of risks among cryptocurrency users and non-users [43], finding that misunderstandings about cryptocurrencies can lead to skewed risk perceptions and dangerous errors. They highlighted the challenges new users face in understanding key management and encryption practices, which can result in mistakes such as accidental loss of critical codes such as private keys and seed phrases.

Our work builds on this prior work by identifying a broader set of strategies users employ to secure their seed phrases through an in-depth interview study, as well as by estimating the relative frequency of how these strategies are used across a more representative sample of survey respondents.

3.3 Seed phrases and Estate Planning

Despite the increasing prevalence of cryptocurrency, estate planning for digital assets remains underexplored. Studies indicate that most cryptocurrency users lack contingency plans for transferring assets upon death or incapacity, with only a small fraction sharing seed phrases with trusted parties for recovery purposes [36, 37]. This gap has significant implications, as the loss of private keys can result in permanently inaccessible funds [37]. For instance, Prost et al. explored the legal and practical challenges of inheriting cryptocurrencies, emphasizing the need for tools and processes that simplify the transfer of digital assets while maintaining security [37]. Similarly, Omelchuk et al. analyzed the features of cryptocurrency inheritance, identifying the lack of awareness and resources as a significant barrier to effective estate planning [36]. Our work builds on these findings by interrogating how and why users engage in estate planning practices for cryptocurrencies and proposing actionable recommendations for improving estate planning practices. By integrating insights from our survey and interview data, we aim to address the gap in understanding how cryptocurrency users approach long-term asset security and inheritance.

4 Method

We conducted a mixed-methods study, beginning with exploratory semi-structured interviews and followed by a larger-scale survey. This approach combined in-depth qualitative insights with broader, generalizable trends, enabling us to understand participants' perceptions and management of seed phrases and the factors influencing their behavior. Using directed storytelling [11], we captured participants' knowledge, usage patterns, social dimensions, and experiences with shared crypto wallet accounts. The subsequent survey quantified and generalized our interview findings. This research was approved by our institution's IRB, and all study materials are available in the Appendix (A).

4.1 Rationale for the Mixed-Methods Approach

The dual-method approach was essential for addressing our research questions comprehensively. The interviews provided qualitative insights into user behaviors, challenges, and attitudes, which informed the design and focus of the survey. For example, the interview findings about ease-of-access trade-offs and misunderstandings about seed phrases guided the survey questions about backup methods and perceived security risks. Conversely, the survey allowed us to validate and generalize the qualitative findings, offering a broader view of user trends. Together, these methods provided a robust framework for understanding how users conceive of, secure, back-up, and share their seed phrases.

4.2 Semi-structured Interview

The semi-structured interviews were designed to explore participants' conceptual understanding of seed phrases, their security practices, and their strategies for sharing and transferring cryptocurrency assets. Interviews were conducted remotely via video conferencing platforms to ensure participant accessibility and convenience. This approach allowed us to reach a diverse group of participants across different regions while maintaining a safe and controlled study environment.

Demographic	Quantity	Description
Gender	15	Male
	5	Female
Education Level	10	4-year college degree
	8	Master's degree
	1	Doctoral degree
	1	High school degree
Employment	9	Full-time
	7	Part-time
	2	Self-employed
	1	Unemployed
	1	Preferred not to answer
Familiarity	15	Significant familiarity
	5	Some familiarity

Table 1: Demographics

4.2.1 Interview Recruitment. We recruited participants via targeted Twitter advertisements and outreach to local cryptocurrency interest groups and university clubs. Prospective participants completed a screening survey to confirm eligibility, which required U.S. residency, being 18 or older, and experience with cryptocurrency and seed phrases. After quality control, 27 individuals were excluded, and semi-structured interviews (30–45 minutes each) were conducted with the remaining 20 participants. Data collection occurred from June to December 2023, and participants received $15 USD for completing the interview.

4.2.2 Interview Participants. Table 1 presents demographics of our interview participants. All our participants were 19-36 years old with 75% of them being male. About 50% of the participants reported having a 4-year college degree or higher. Employment status varied, with many reporting full-time employment, part-time, or self-employment. A notable aspect is the respondents' familiarity with cryptocurrencies and blockchain technology, where 75% expressed significant familiarity. This demographic profile suggests a technologically adept and educationally advanced group, reflecting a targeted interest in the subject matter of the study.

Participants reported using a wide range of crypto wallets, with Binance (Custodial), MetaMask (Non-custodial), and Trust Wallet (Non-custodial) being the most prevalent. Wallets like Coinbase (Coinbase Web is custodial, Coinbase wallet is non-custodial), Robinhood (Custodial), Trust Wallet, and specialized ones like Wazirx (Custodial) for NFTs were also popular. Many of our participants used multiple wallets as has been reported by prior work [47], with numbers ranging from 2 up to 20.

4.2.3 Interview Content. Participants were first asked to fill out a demographic survey regarding their age, gender, occupational

Participant ID	Age	Gender Identity	Employment Status	Education Level	Cryptocurrency Familiarity
P1	36	Male	Full-time	Doctoral degree	Significant familiarity
P2	26	Male	Self-employed	4-year college degree	Significant familiarity
P3	34	Male	Full-time	4-year college degree	Significant familiarity
P4	23	Male	Full-time	4-year college degree	Significant familiarity
P5	26	Male	Full-time	Master's degree	Significant familiarity
P6	23	Male	Part-time	4-year college degree	Significant familiarity
P7	24	Male	Part-time	4-year college degree	Significant familiarity
P8	25	Female	Part-time	Master's degree	Significant familiarity
P9	26	Male	Part-time	4-year college degree	Significant familiarity
P10	25	Male	Part-time	Master's degree	Significant familiarity
P11	19	Male	Full-time	4-year college degree	Significant familiarity
P12	20	Male	Unemployed	High School degree	Some familiarity
P13	20	Male	Part-time	4-year college degree	Significant familiarity
P14	29	Male	Prefer not to answer	Master's degree	Some familiarity
P15	23	Male	Full-time	4-year college degree	Significant familiarity
P16	24	Male	Self-employed	Master's degree	Some familiarity
P17	23	Male	Full-time	Master's degree	Some familiarity
P18	24	Male	Full-time	4-year college degree	Significant familiarity
P19	24	Female	Part-time	Master's degree	Significant familiarity
P20	22	Female	Full-time	Master's degree	Some familiarity

Table 2: Interviewee demographic information

situation, educational attainment, and familiarity with cryptocurrencies and blockchain technology. In the actual interview, we probed people's understanding of seed phrases by posing basic questions about them. Then, participants were asked more targeted questions aimed at eliciting relevant experiences corresponding to our research questions. Our full set of questions is in the Appendix (A).

4.3 Survey

The survey was developed to build upon the findings from the interviews, translating key themes into quantifiable measures. Insights from the interviews, such as common misconceptions about seed phrases and frequently used backup methods, informed the creation of our survey questions.

4.3.1 Survey Recruitment and Participant Demographics. We recruited 643 respondents through Qualtrics XM [1], ensuring a diverse participant pool in terms of cryptocurrency experience, age, and geographic location. Participants were 18 years or older and required to have some prior experience with cryptocurrency. Prior work in HCI suggests a survey sample size of 384 is typically sufficient to obtain results within the 95% confidence interval of the true population value for a population of 100 million individuals [33]. Moreover, the number of participants needed does do not markedly increase as the population size increases (e.g., only 384 survey respondents needed are needed for a 95% confidence estimate for a population of 1 million individuals as well) [ibid]. Since there are an estimated 575 million cryptocurrency users worldwide [3], we can surmise that our population of 643 survey respondents is sufficiently substantial to generalize to this broader population of cryptocurrency users within a 5% margin of error.

[1] https://www.qualtrics.com/

4.3.2 Survey Content. The survey investigated individuals' habits and behaviors regarding cryptocurrency, focusing on their motivations and experiences. It initially asks participants to identify a seed phrase (see Figure 1) and then explores their understanding and management of seed phrases, including methods for safeguarding and coping with potential loss. It also examines how users learn about backing up seed phrases and their level of trust in others for securing them. Additionally, the survey addresses comprehension of shared accounts and strategies for asset transfer upon death. For detailed questions, please refer to the Appendix(A).

4.3.3 Overview of Survey Participants' Cryptocurrency Usage Behaviors. Table 4 offers an overview of our survey participants crypto behaviors. We categorized respondents based on their ability to correctly identify a seed phrase. Of our 643 participants, only 43.4% (279 individuals) were able to accurately identify a seed phrase, and 56.6% (364 individuals) could not.

	Experienced	Novices	N
Total count (N)	199 (31.0%)	444 (69.0%)	643
Identified seed phrase	174 (62.4%)	105 (37.6%)	279

Table 3: Breakdown of total number of Experienced users and Novices, and how many correctly identified a seed phrase

We then separated respondents into experienced users (individuals with more than 2 years of experience) and novices (individuals with less than 2 years of experience) 69% (444 individuals) were novices and 31% (199 individuals) were experienced users. The majority of our survey respondents (44.2%) reported having used cryptocurrency between 1 and 5 years, though a large number (20.3%) also reported having been involved for less than 6 months.

The predominant motivation for trading cryptocurrency was financial planning (58.6%). Research (45.0%), monetary transactions (37.1%), and entertainment (32.4%) were also significant motivators, while fewer participants cited work (16.1%) as their primary reason (N=643). Custodial web wallets were the most commonly used (60.8%), likely because of their user-friendly interfaces and the convenience of integrated trading features, which reduce the need for technical knowledge about seed phrases or private key management. The popularity of these wallets could also explain why so many participants were unable to correctly recognize a seed phrase: people who only use custodial web wallets may never be directly exposed to one. Mobile wallets (42.0%) and desktop wallets (33.5%) were also widely used. Hardware wallets, while more secure, were used by 11.3% of respondents, while paper wallets and other types were each used by 1.6%.

Coinbase Wallet (non-Custodial) was the most preferred wallet software, with 62.4% of users indicating it as their choice. Binance (Custodial) (15.6%) and Coinbase Web (21.6%) (Custodial) were also popular, while Metamask (8.0%) (Non-custodial) and other providers (7.3%) had smaller user bases.

The vast majority of participants (85.7%) used between 1 and 5 active trading wallets suggesting users' preference for diversifying their holdings across multiple wallets as has also been documented more qualitatively in prior work [47]. A smaller group of participants (7.2%) used between 5 and 10 wallets, while only a few (2.4%) used more than 10 wallets. Notably, 4.7% of participants did not maintain any active trading wallets.

Most participants (68.0%) stored their cryptocurrency assets across 1 to 5 wallets. There was also a significant number who used 5 to 10 wallets (21.8%), and 10.5% used more than 10 wallets. Interestingly, 15.7% of participants did not store cryptocurrencies in any wallets, which might indicate the usage of exchange platforms or custodial solutions for their holdings.

Category	Frequency (%)
Experience Duration	
Less than 6 months	132 (20.3%)
6 months to 1 year	135 (20.8%)
1 to 2 years	177 (27.2%)
2 to 5 years	143 (22.0%)
More than 5 years	56 (8.6%)
Motivation	
Research	251 (38.6%)
Financial Planning	327 (50.3%)
Work	90 (13.8%)
Monetary Transactions	207 (31.8%)
Entertainment	181 (27.8%)
Wallet Type	
Hosted Web Wallet	339 (52.2%)
Non-Hosted Web Wallet	327 (50.3%)
Desktop Wallet	90 (13.8%)
Mobile Wallet	207 (31.8%)
Hardware Wallet	181 (27.8%)
Paper Wallet	9 (1.4%)
Other	9 (1.4%)
Preferred Wallet Provider	
Binance	251 (38.6%)
Coinbase Wallet	327 (50.3%)
Coinbase Web	90 (13.8%)
Metamask	207 (31.8%)
Other (please specify)	41 (6.3%)
Number of Active Trading Wallets	
0	26 (4.0%)
1-5	557 (85.7%)
5-10	45 (6.9%)
More than 10	15 (2.3%)
Number of Wallets with Crypto Stored	
0	87 (13.4%)
1-5	327 (50.3%)
5-10	121 (18.6%)
More than 10	58 (8.9%)

Table 4: Summary of Participant Responses (N=643)

4.4 Data Analysis

4.4.1 Qualitative Coding. To analyze the interview data, we first organized the transcripts of the interviews with 20 participants and the notes taken by the researchers. Two researchers reviewed all the transcripts and notes, identifying salient statements and conducting an initial round of open coding. To ensure consistency in interpretation and analysis, the two researchers discussed the codes and used affinity diagrams to categorize and analyze them. They then summarized the findings and conclusions based on the research questions. Based on these findings, we developed follow-up questions to inform the survey.

4.4.2 Quantitative Analysis. We collected survey data from 650 cryptocurrency users and asset owners worldwide. After cleaning the data to remove discrepancies and inconsistencies, we had 643 responses used in the final analysis. Descriptive statistics were used to provide a foundational understanding of the dataset, ensuring that any observed differences in inferential statistics are grounded in the actual data distribution.

5 Results

We proceeded to examine the mindset and practices of individuals in securing their seed phrases, as well as how they acquire these security strategies (RQ 1). We also explored if and how users experienced situations where they either lost or had their seed phrases stolen, and how those experienced affected their awareness of risk and their subsequent security behaviors (RQ 2). We then delved into people's understanding of sharing seed phrases and the use of shared accounts for cryptocurrency wallets (RQ 3). Finally, we unpacked participants' strategies — or lack thereof — for bequeathment of their cryptoassets (RQ 4). Note that we use participant number to refer to specific interviewees as shown in Table 2, e.g., P2 or P15.

5.1 How Users Secure their Seed Phrases (RQ1)

5.1.1 Safety level and ease of access are primary considerations.

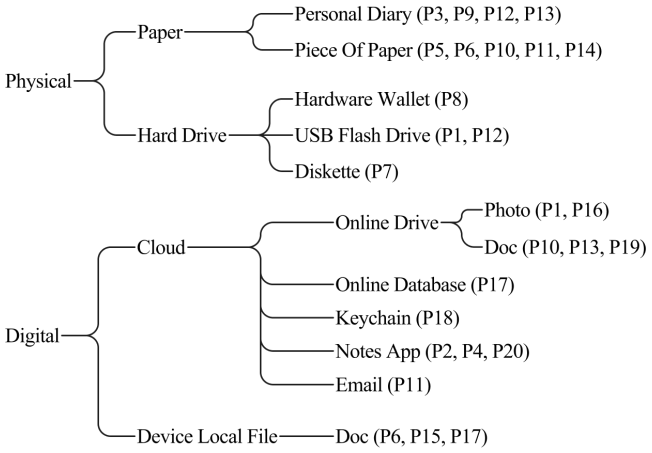


Figure 2: Seed phrase storage methods

Interview: Our interview results showed that when choosing methods to back up their seed phrases, participants primarily considered two factors: security and ease of access. They employed a range of strategies, including both digital and physical storage methods, carefully balancing the need for safety with ease of access.

Several participants considered level of safety to be the most important consideration when employing methods to back up their seed phrases. These participants chose offline storage rather than storage in third-party applications that can connect to the internet (P3, P5, P6, P9, P12, P14), encrypted their storage method (P2, P6, P8, P12), and split the seed phrases into different parts to back up pieces of their seed phrase in different places (P8).P3 was one of our most experienced participants and managed 10-15 wallets simultaneously. When discussing how he backed up his seed phrases, he appeared very cautious, even being reluctant to share with us how he backed up his seed phrases — he viewed even discussing his strategies as a potential security threat. He wrote down his seed phrases in a personal paper diary over which he expressed the need to have full control. *"I have a personalized diary. Very very personal diary. Even my wife doesn't know about my seed phrases, I keep it as personal as that. I don't want anybody having access to my account." (P3)*

The other important factor that many users considered when choosing strategies for backing up their seed phrases was the ease of access. These participants expressed being more concerned with the possibility of losing access to their wallet because they would not be able to find their seed phrases themselves than the possibility of a third-party adversary stealing their seed phrase.

For example, P1 had one primary wallet. He took a screenshot of the seed phrases and stored the image in Google Drive because it is always accessible, even though he was told not to do so: *"I think that most wallets they have this notification. They [the wallet software] reminded you not to use the image (screenshot). But actually, I use the image. I put it in the Google Drive. If I put it somewhere else, I probably forgot it." (P1)*

He was aware that saving a screenshot of his seed phrase in Google Drive was perhaps not as secure against remote adversaries as, e.g., writing the seed phrase down on paper. However, he believed that the realities of his living situation made a paper backup less practical: *"I have one seed phrase I put in my book. But I have kids I will worry about it sometime days later too, they throw it away and it's gone." (P1)*

Similarly, P10 also avoided paper backups because they can be easily lost, preferring cloud storage to ensure that he would not lose or misplace it: *"I have a folder of my important documents, including my passport and other stuff... I chose the folder because they told me that I needed to keep it safe on a physical medium. And that is where I won't misplace it. But I will share that. I'm going to misplace it a few years from there. So that is the reason I saved it as a digital file in my Google Drive as well." (P10)* P1's and P10's choice to use Google Drive was not unique — Many participants expressed another practical reason they elected for less secure, but more convenient methods of backing up their seed phrase: they did not have a lot of money invested in the crypto assets attached to their wallets and didn't use crypto wallets often. As such, they rarely considered the possibility of someone stealing their seed phrases or what could happen if they got leaked. Many of these participants expressed backing up their seed phrases on their cell phone, which they always had handy. For example, they used the notes app (P2, P4, P20), saved screenshots in their photo album (P16), or saved them in a password manager like Apple's key-chain (P18).

Survey: The survey showed that among the two factors, ease of access often dominated participants' security strategies — even among experienced users. This finding reflects the practical trade-offs that participants made, particularly for wallets with less significant assets or those they accessed frequently. For instance, some experienced users relied on convenient but less secure storage methods, like cloud backups, to avoid the risk of forgetting their seed phrases or losing access. Notably, experienced users did not neglect security; rather, their strategies often balanced convenience with perceived risks. Indeed, the survey results showed that paper backups were the most popular choice, with 39% of respondents opting for this method. Paper backups were also considered the safest (167 responses) and the most convenient (161 responses) method.31% of our survey respondents also chose cloud storage to backup their seed phrases, despite advice from the crypto community that "cold" (offline) backups are more secure.

Backup method	Experienced users		Novice users		All users	
No backup	6	2.2%	14	5.0%	20	7.2%
Paper	43	15.4%	64	22.9%	107	38.4%
External Drive	35	12.5%	52	18.6%	87	31.2%
Internal Drive	21	7.5%	42	15.1%	63	22.6%
Cloud	38	13.6%	50	17.9%	88	31.5%
Email	26	9.3%	44	15.8%	70	25.1%
Memorizing	14	5.0%	26	9.3%	40	14.3%
Other	3	1.1%	1	0.4%	4	1.4%

Table 5: Seed phrase backup method (Multi-selection)

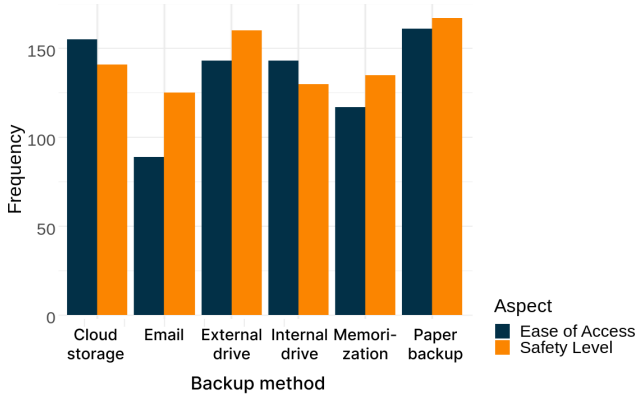


Figure 3: Safety and Ease of Access trade-off for securing seed phrases (N=279 (subgroup that identified seed phrase))

5.1.2 Sources of Learning Security Methods. Understanding how and where people learn strategies for securing their seed phrases can help inform the design of future interventions for improving people's awareness and knowledge of seed phrase security.

Interview: Our interview results revealed that users not only learn knowledge through online communities but also make friends and learn from each other about management, trading, and security practices. For instance, P2 mentioned learning about different people's crypto journeys, feeling accepted in the online community, and making friends he never thought possible. *"The people's crypto journey is something that is very unique. We have a social media community, and crypto community in my area. It's virtual, so it made me some friends that I didn't think in my dreams I could be friends with. And it's something that I'm more accepted." (P2)* P4 learned to store his seed phrases in a notes app from friends in online communities. P7 joined many groups on Telegram, becoming closer to the members and learning about cryptocurrency trading through their conversations. *"I'm also in some groups where they tell you about the management of your account, how to use cryptocurrencies. And they also tell you a good deal." (P7)* The same happened with P12: *"We share common interests concerning crypto progress and downfalls, things that can happen. You might lose some currencies, and you might also gain. So we do talk about each problem we face together." (P12)* Many participants reported choosing how to back up their seed phrases independent of any external influence. Participants tried some of the storage methods they had heard about, but they chose the one they thought was the most reliable based on their own experience. For example, P13 chose to store one of the copies of his seed phrases in a cloud document that required two different passwords to access. He mentioned that he knew it was not safe to store seed phrases online, but his previous experience led him to believe that local documents are even less secure: *"Last year, my computer wiped its memory. So I had to replace it. I don't just keep it on local anymore, so I put everything on the cloud for that." (P13)*

Survey: While our interview participants largely attributed learning about cryptocurrencies from online communities, we found that online communities were the *second* most popular source of information reported in our survey. Our survey participants who had backed up their seed phrases (N=266) rated the wallet apps they used as their most preferred source (61.3%) for learning about how to backup their seed phrase, higher than online communities (46.2%), people close to them (45.2%), books, news, articles (43%), and social media (37.6%). This preference is understandable, as many interview participants did not know much about cryptocurrency when they first created a cryptocurrency wallet account.

While fewer than half of our survey participants reported learning about seed phrase security from online communities, our interviews suggest that those who do are greatly influenced by these communities. Given that there are no explicit quality controls for information shared on these communities, however, it would be prudent for future work to audit security advice provided on these online communities for correctness. These findings highlight the critical importance of wallet software in communicating key information about seed phrase security to end-users — for many users, the onboarding process for creating a new wallet account may be users' only exposure to thinking about seed phrase security at all.

Method	Frequency
Wallet apps	171 (61.3%)
Online communities	129 (46.2%)
People close to you	126 (45.2%)
Books, news, articles	120 43.0%)
Social media	105 (37.6%)

Table 6: Preferred methods for learning security strategies (Multi-selection)

5.1.3 ***Conflation of Seed Phrases and Passwords.*** Both our interview and survey suggests that participants often conceptually conflated passwords and seedphrases, and that this conflation led to how they approached securing their seed phrases and shaped ill-conceived expectations: e.g., that a seed phrase can be manually chosen and reset like a password.

Interview: Our interviews revealed that many participants conflated seed phrases and passwords. For example, both were viewed as digital secrets to be secured, and so any strategies a user used to secure their passwords were also applied to seed phrases. For instance, P2, P4, and P12 backed up their seed phrases along with their passwords in online documents.

Sometimes, the conflation was deeper and more conceptual. For instance, P16 complained that he couldn't reset seed phrases like he could passwords, reflecting a conceptual misunderstanding that has significant security implications: *"There's no forget password choice where yeah we reset all the password options in there. So that's pretty scary." (P16)*

Passwords can be reset because they are chosen secrets that are stored by a third-party custodian and can be reset if that custodian can separately authenticate the user. But seed phrases are not chosen secrets, they are generated secrets that are cryptographically tied to a corresponding public key hash. There is no resetting a seed phrase — if it is lost or stolen, then any assets associated with its corresponding public key hash are also lost.

We also found that many people reported backing up seed phrases in the same manner they stored passwords. For example, P18 mentioned he backs up his seed phrases securely in Apple's Keychain software, where he stored other passwords in his MacBook. P2 and P4 saved their seed phrases in the notes app on their phones. P12 reported keeping his seed phrases with other important documents.

In addition, we found that participants demonstrated misunderstandings about seed phrases, often conflating them with passwords: for example, many participants believed they could directly choose their seed phrases much like they could their passwords, and believed that it might be possible to "reset" their seed phrases in the same way.

Survey: Our survey results also revealed a widespread misunderstanding among participants about the roles and significance of seed phrases compared to passwords. When asked about the information required to transfer a cryptocurrency wallet to a new device, 52% of participants incorrectly identified "Username and Password" as sufficient, a stark contrast to the 47% who correctly recognized the importance of the "Recovery Seed Phrase". This indicates a significant gap in understanding, as seed phrases—not usernames or passwords—are essential for recovering and accessing non-custodial wallets. Moreover, in our survey, 58% of participants reported that they could choose any seed phrase, just as they would choose a password for other apps.

These conceptual misunderstandings were further evident when participants were asked about securing their wallets. Among non-custodial wallet users, 75% of responses made no mention of securing "Recovery Seed Phrases" or "Private Keys". Furthermore, among the 99 non-custodial wallet users, 59% did not identify "Recovery Seed Phrases" or "Private Key" as necessary for transferring wallet information to a new device. These findings suggest that many participants lack a clear understanding of the critical role seed phrases play in securing and recovering cryptocurrency wallets.

This conflation likely arises from treating seed phrases like passwords, which are replaceable and typically backed by custodial recovery systems. However, seed phrases are irreplaceable cryptographic keys, and their loss results in permanent inaccessibility to the associated assets.

Our findings underscore the need for improved education on the unique role of seed phrases. Wallet providers should focus on designing user-friendly, explicit onboarding materials that clearly distinguish seed phrases from traditional authentication methods like passwords and emphasize their irreplaceable nature.

5.1.4 *Experienced Users Engage in More Secure Behaviors.*

While our interview sample was too small for us to notice differences between users with more and less experience, our survey highlighted that more experienced users engaged in more secure behaviors.

Survey: Our survey showed that people with more experience generally employed more secure practices, particularly for wallets with significant assets or long-term holdings. For example, experienced users were more likely to adopt offline or encrypted backups compared to novices, who often relied on less secure options like screenshots or cloud storage. This finding highlights that while experienced users showed a better understanding of secure practices overall, their choice of storage methods could still vary depending on the perceived importance of the wallet and the assets it held. Among the 279 participants who identified seed phrases, crypto experienced users (with over two years of experience) had a lower percentage of no seed phrase backup at 5.7%, compared to novices (with less than two years of experience) at 8.6%. Additionally, compared to novice users, experienced users were less likely to use cloud backup (13.6% vs. 17.9%) and email backup (9.3% vs. 15.8%).

Method	%	Count
Username and Password	56%	208
Private Key	28%	106
Recovery Seed Phrase	13%	50
Wallet Password	35%	132
Two-Factor Authentication Codes	31%	117
Email Address associated with Wallet	22%	82
Backup Files from Wallet Application	7%	26

Table 7: Misconception of seed phrase purpose (N=279, multi-selection)

Information required	%	Count
Username and Password	52%	149
Private Key	39%	112
Recovery Seed Phrase	47%	135
Wallet Password	34%	99
Two-Factor Authentication Codes	38%	109
Email Address associated with Wallet	32%	93

Table 8: Misconception of seed phrase usage (N=279, multiselection)

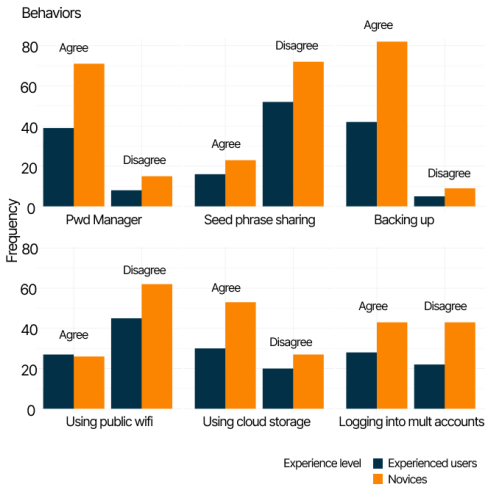
5.2 Loss and scams motivate improved security practices (RQ2)

Many cryptocurrency users report being the target and/or victim of phishing scams. Analyzing how experiences with asset loss and scams influence these users' security practices can be instructive in designing interventions to enhance users' security awareness.

5.2.1 *Many Novices and Experienced Users Report Falling for Scams.*

We analyzed participants with different levels of cryptocurrency experience to examine the relationship between their experience and the likelihood of being scammed or making mistakes with their seed phrases.

Interview: Our interview participants reported falling prey to scams as novices, when they first started to use non-custodial cryptocurrency wallets. For example, P19 and her mother started investing in cryptocurrency projects casually. It was not until they realized that they had invested in a cryptocurrency ponzi scheme that they delved deeper into how cryptocurrencies work and started learning more about crypto scams and engaging in due diligence. *"We got scammed and we were like, Wait, what just happened? And then we started reading more about it." (P19)*



QuestionNo	Behavior
Pwd Manager	Using password manager to avoid reusing passwords
Seed phrase sharing	Sharing seed phrase on public forum
Backing up	Backing up crypto wallet periodically
Using public Wifi	Using public Wi-Fi to access crypto wallets or perform transactions
Using Cloud Storage	Using cloud storage services to store a backup of your seed phrase
Logging into mult accounts	Log into crypto accounts and make transactions on multiple devices

Figure 4: Comparison between experienced users and novice security practice

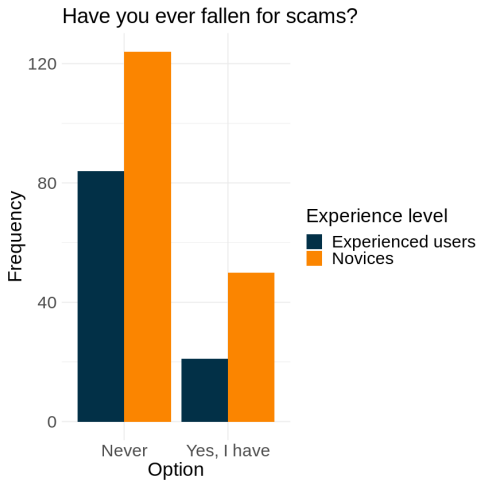


Figure 5: Fallen for scams (N=279)

Survey: From our survey, out of 279 participants who correctly identified seed phrases, 105 were experienced users (with over 2 years of cryptocurrency usage) and 174 were novices (with less than 2 years of experience). Among the experienced users, 21 (20%) reported being scammed. In contrast, 50 out of 174 novices (approximately 29%) reported being scammed.

5.2.2 Losses can be Catalysts for Novice Users to Improve Security Practices. Experiences of loss were often due to inadequate knowledge about crypto security practices and served as a key catalyst for participants improving their security behaviors. This finding is consistent with previous research findings that reacting to live security threats and negative experiences often triggers a change in security behavior. Prior work suggests that experiencing security threats can create "teachable moments" [26] where users may be more receptive to learning about and updating their security behaviors. While negative experiences can motivate security behavior changes, post-loss interventions must prioritize emotional support and compassionate guidance. Educational approaches should acknowledge the psychological burden of such losses, offering constructive, non-judgmental strategies for improving security practices.

Interview: P6 gradually learned the importance of seed phrases after losing access to his crypto assets multiple times. The first time he lost access was because he did not know he needed to record his seed phrase at all: *"At first, I didn't even know what a seed phrase is. So I didn't write it down. So I just kind of like wasted that clip toward it." (P6)*

The second time was due to not understanding that seed phrases need to be kept confidential: *"The second time is when I put it [his seed phrase] into a GitHub public repository. I kind of thought, Well, nobody's visiting that repository that much. So there is no harm. And immediately within seconds, it was just kind of stolen. That was painful because I lost maybe $20. So since then, I have tended to learn more about the security of crypto wallets." (P6)*

After that, P6 said he stored his seed phrases offline on his own device, but his own inability to access the storage files caused frustration in locating those files himself. *"I kind of always forget how I actually named it, and the Windows file search is very bad. It takes ages to search through your whole database and so on." (P6)*

Similar to P6, a colleague of P15 inadvertently shared seed phrases of a communal crypto wallet on GitHub, again because the colleague was new to cryptocurrencies and did not understand the need to keep seed phrases secret. This incident was used as a cautionary tale for other colleagues. *"One of the junior interns accidentally uploaded a difference to the GitHub readme that is very serious...we just use it as a very, very good example to like joking with others and say, Hey, don't upload your seed phrase to GitHub." (P15)*

5.3 Sharing Seed Phrases or Accounts (RQ3)

Exploring how and why individuals choose to share—or not share—their seed phrases and accounts provides insight into their conscious decision-making and the associated risks. Participants were cautious about directly sharing their seed phrases with others, acknowledging the inherent risks associated with such sharing.

5.3.1 Sharing Seed Phrases in Low Stakes Scenarios.

Interview: From our interviews, P6's research project required him to use a cryptocurrency wallet with his coworker. Despite the absence of personal financial risks associated with the research account, P6 assumed responsibility for the outcomes of the research. He chose to share the wallet's seed phrase with his co-worker on paper. This decision was influenced by their physical proximity, making paper copies convenient while also mitigating the risk

of seed phrase leakage that could potentially result from online sharing. P6 reflected: *"Since he really sat in the same room as me, I could just come and write these words myself. So there was no problem with that. But to be honest, if I had to share it over the internet I would maybe trust like Telegram or something like that because it is encrypted." (P6)*

P5 taught his friends how to use a crypto wallet. Even though P5 was very cautious about his own seed phrases' safety, he was not concerned about sharing the seed phrase of the educational demo wallet since it did not contain assets worth real money. To keep P5 and his friend's wallets safe, this wallet they created while teaching was only used during the teaching process, and neither of them would trade with it after the tutorial was over. Reflecting on this teaching experience, P5 explained: *"We used that wallet as a demo. So I was teaching them how to use crypto wallets. Otherwise, I don't share my seed phrases and circumstances." (P5)*

5.3.2 Sharing Seed Phrases in High-Stakes Scenarios.

Interview: Only two of our interview participants reported sharing seed phrases for wallet accounts with significant monetary assets. These participants discussed sharing seed phrases in situations where they had or had developed significant trust with a partner, either because of a familial or fiduciary relationship, or because they had set rules and extensive prior experience working with those partners.

P9 had two experiences of crypto account sharing. A friend of P9's used to pay him to manage his cryptocurrency wallet. P9 managed his friend's seed phrases and made transactions for him. P9 secured his friend's seed phrases in the same way that he secured his own — by writing them down, and not sharing them with anyone else.

P9 also shared an account with several friends. In this case, P9's major concern was with the people he shared it with, rather than the security of the wallet itself. When asked how he mitigated those concerns, he explained the basis for his trust in his partners stemmed from prior experience and from the presence of agreed-upon rules for how to distribute the assets in the shared wallet: *"we've not had issues in the past three years since ... we have set rules if you're done or if you're tired of investing, or you want to pull out this how we calculate the percentage ratio and you take back your initials and the current profit and everything and you leave. That's how we do it." (P9)*

Like P9, P19 shared her seed phrases and all account information with her mother. P19 is a student and reported having limited time to manage her account herself, so part of this sharing was born out of need. Additionally, P19 and her mother had complete trust in each other, so she allowed her mother to access any information she needed and to make trades on her behalf — both in and outside of crypto. P19 said: *"She has access to everything she wishes, all the PINs and access to everything that is financial for me." (P19)*

Survey: Based on our survey, a substantial majority of users — about 79% of the 279 participants who recognized seed phrases correctly — have never tried sharing cryptocurrency accounts with others. Moreover, nearly half of our respondents (49%) have never shared their *seed phrases* with anyone.

Among participants who *did* share seed phrases for wallets that contained substantial crypto-assets, they primarily reported sharing with people they knew personally and deeply trusted. Our survey results showed that among all participants reported sharing accounts (145), a significant number expressed agreement (65) and strong agreement (35) that they trusted the individuals with whom they shared their seed phrases. Among the 279 participants who recognized seed phrases, Personal relationships and history played a crucial role in this trust for 133 respondents (48%). Other factors that improved participants' trust in who participants shared their seed phrases with included knowledge and understanding of seed phrase security (44%), legal agreements and documentation (40%), the reputation and credibility of the individual (37%), and third-party verification or validation (18%).

5.4 Digital Contingency Plans (RQ4)

We also inquired into people's plans for bequeathing their crypto assets to their intended beneficiaries. In traditional finance, centralized custodians can facilitate the bequeathment and inheritance process; these custodians would not be able to facilitate the bequeathment of assets tied to non-custodial crypto wallets. It is of critical importance, therefore, to understand if and how users think about bequeathment of these assets, and to develop techniques to facilitate this bequeathment. Nevertheless, we found that very few participants, none in our interviews and only around 22% in our survey, made any such plans.

Interview: P17, when asked about their bequeathment plans, captured the general ethos we encountered towards crypto bequeathment plans: *"I'll lose all my money if I'm dead."* More generally, none of our 20 interviewees had considered arrangements for transferring their crypto assets to an intended beneficiary in the event of their death.

From our interviews, we found participants had two primary reasons for *not* implementing a bequeathment plan. First, our participants were generally young (mostly in their 20s, with the oldest being 36), and thus may not have have felt much urgency to create such a plan. Secondly, many of our participants felt that their investment in crypto was too limited to warrant a bequeathment plan. For example, P15 said: *"I don't have too much money in crypto. But if I did have much money in crypto, maybe I would set up a will or something. Put it somewhere safe with my seed phrase. So my inheritors can claim those assets on blockchain later."* P20 exemplified both of these points, saying, *"I think the main reasons are that first I do not invest that much money in here. And second, I feel like I don't see any imminent death call me."*

Survey: Consistent with our interview results, very few of our survey respondents reported having a backup plan for the inheritance of their digital assets. Among the 279 participants who correctly recognized a seed phrase, only 22% of respondents shared their seed phrases with family members for account recovery in case of death or serious injury; 9% shared their seed phrases for account recovery purposes alone. However, 57% of our participants indicated that sharing seed phrases with family members is an important method for asset recovery in emergencies. In short, while most participants recognized the importance of sharing seed

Factor	Percentage	Count
Personal relationship and history with the individual	48%	139
Legal agreements and documentation	40%	114
Knowledge and understanding of seed phrase security	44%	126
Reputation and credibility of the individual	37%	106
Third-party verification or validation	18%	53
Other (please specify)	1%	4

Table 9: Reasons for choosing the people to share seed phrases with

phrases with trusted contacts for account recovery, only a minority actually did so.

6 Discussion

6.1 Conceptual Conflation Between Passwords and Seed Phrases May Allow for Analogical Learning

Our research indicates that people often conflate seed phrases with passwords, and treat them similarily in terms of security attitudes and behaviors. However, this conflation can lead to security risks.

First, when passwords are used to authenticate into custodial services (e.g., one's bank account), they are typically supplemented with additional security measures like two-factor authentication and the custodian checking for contextual risk factors (e.g., an unusual IP address). This can lead to a sense of "shared" responsibility over security between the user and custodian [9]. In contrast, seed phrases alone provide complete access to one's wallet. There are no additional security measures, and users are solely responsible for its security. Second, passwords can often be reset if forgotten. In contrast, seed phrases are algorithmically generated and cannot be reset. Third, if a user's custodial bank account password is compromised, the custodial bank can reverse unauthorized transactions. In contrast, blockchain transactions are irreversible.

The combination of these factors make losing one's seed phrase more catastrophic than losing a password. Users unaware of this difference can permanently lose access to their wallets — and the assets in those wallets — if they inadequately store or lose their seed phrases. The emotional toll of such losses can be significant, especially for individuals who have invested considerable time and resources into building their cryptocurrency portfolios. Individuals may experience feelings of guilt, frustration, or helplessness when they lose access to their funds due to preventable mistakes. This emotional distress may also erode users' trust in self-custody practices or cryptocurrency systems more broadly. Therefore, efforts to educate users on seed phrase security should be designed with empathy, acknowledging the emotional weight of potential losses. This possibility highlights the necessity of considering ease of access when storing seed phrases to avoid loss due to human error [16].

This conflation also presents an opportunity to use analogical reasoning for educating users about seed phrases by leveraging their existing knowledge of passwords. Newby *et al.* demonstrated that analogies are powerful tools for introducing new concepts to learners [34]. Similarly, Bishop *et al.* found that analogical methods are particularly effective in the field of computer security, although they noted the importance of clearly delineating the analogy to ensure its effectiveness [8].

One of our survey results was that wallet apps are the most preferred point of interaction for learning about crypto security practices. As such, we recommend emphasizing the differences between passwords and seed phrases during the crypto wallet onboarding process to deepen users' understanding of seed phrases. For example, popular non-custodial crypto wallet apps such as MetaMask, Trust Wallet, and Coinbase Wallet guide users through setting up their accounts and passwords before generating seed phrases. We suggest using this onboarding process to introduce seed phrases by highlighting the similarities and differences between passwords and seed phrases. In this tutorial, it would be useful to highlight, for example, that seed phrases cannot be chosen or reset, and that a big piece of crypto wallet security is keeping their seed phrase secure, and that doing so is solely their responsibility.

6.2 Facilitating the Creation of Cryptocurrency Contingency Plans

We found a widespread lack of digital contingency plans for one's cryptocurrency assets in the case of death or incapacitation. This issue is not unique to cryptocurrencies — e.g., Lustbader et al. reports that only 24% of young adults aged 18-34 had engaged in any kind of estate planning [29]. While traditional finance offers well-defined mechanisms for asset inheritance, assets stored in non-custodial wallets can be permanently lost without proper planning. Despite understanding the importance of sharing seed phrases for emergency account recovery, we found that only 22% of our survey participants actually did so.

The barriers to creating contingency plans are primarily psychological. Most participants were young and felt that their crypto investments were too limited to warrant extensive planning. However, presumably these users purchased these crypto assets in the hope that they would, in the future, appreciate in value. Having mechanisms in place to ensure the security and availability of these assets, thus, should still be a priority.

Given these barriers, we recommend that future work explores mechanisms for automating the process of creating a crypto bequeathment plan. For example, once a user has exceeded a trading volume that they believe to be "significant", the wallet application might ask the user to specify a designated beneficiary. Beneficiaries might be specified through a wallet address if they are already familiar and onboarded with crypto, or an email address if not. For beneficiaries who are crypto novices, the wallet application should

provide these designated beneficiaries with a step-by-step tutorial to creating their own wallet so that they may be the recipients of the assets of the inactive wallet. For blockchains that support smart contracts (e.g., Ethereum), smart contracts may facilitate this transference process — e.g., the funds might automatically transfer if original wallet has been inactive for a set period of time, or if two or more trusted contacts confirm that the original account holder has passed or has become incapacitated. For blockchains that do not support smart contracts (e.g., Bitcoin), it may be prudent for the user to partner with custodial services [2] that can simplify the bequeathment process while still providing users with full control over their assets.

6.3 Ongoing Need for Cryptocurrency Literacy for Users of All Experience Levels

Only 279 out of our 643 survey participants (43.4%) were able to correctly identify a seed phrase, though all 643 reported having experience with investing in cryptocurrency. And even among those who were able to correctly identify a seed phrase, many believed that they could choose their own seed phrase and have them reset if lost. These findings suggest that there is a need to improve end-user literacy of seed phrases in order to reduce users' exposure to scams and accidental loss of assets.

Our survey results, for example, indicated that 29% of novice users and 20% of experienced users reported being scammed. Therefore, educational initiatives targeting scam prevention are crucial for users at all experience levels. These programs should focus on key areas such as identifying common scams and understanding the basic principles of blockchain technology and cryptocurrency transactions. Additionally, users can be encouraged to install extensions or plug-ins that identify and alert them to potential scams, as well as learn about remedial actions in case of a scam [6].

We note, however, that educational interventions alone will not be enough to fully reduce users' exposure to scams — even the most vigilant users may sometimes fall prey to scams. Accordingly, it is also necessary to design non-custodial wallets and tools that nudge users towards safe behaviors and help users make informed decisions.

6.4 Limitations

For our interviews, we only recruited participants that resided in the United States, which may not be fully representative of the cryptocurrency community — we note however that the purpose of the interview study was to be generative and exploratory, not generalizable. While we recruited survey participants from all around the world, the survey required participants to have English reading and writing proficiency. The recruitment platform we used, Qualtrics XM, screened participants for these skills. However, we recognize that this criterion may have introduced a bias in our sample, it may have missed behaviors, assumptions, particularly affecting representation from non-English-speaking countries.

Demographics of cryptocurrency users in past studies have shown that the user base of cryptocurrencies is predominantly male, mostly aged 18-45 years, with a large portion having a bachelor's degree or higher [12] [46] [41]. Our interview participants mostly match these demographics, though our oldest participant was only 36.

Lastly, many interview participants mentioned that they had not invested much money in cryptocurrencies, so our interview population is not fully representative of people who have larger investments.

[2]As of 2024, services like Unchained exist for this purpose: https://unchained.com/inheritance

7 Conclusion

Our study provides a comprehensive exploration of cryptocurrency users' strategies for securing and backing up their seed phrases, their practices and perceptions surrounding the sharing of seed phrases, and their understanding and practice of digital contingency plans. We found that many users harbor significant misconceptions about seed phrases: the majority of our survey respondents, for example, could not accurately recognize a seed phrase. Even among those who could, many believed that seed phrases could be chosen and reset like passwords. We identified that users learn their security strategies from a mix of personal connections, online resources, and by drawing parallels with traditional password management. Despite recognizing the importance of seed phrases, many users still engage in risky behaviors — such as failing to backup their seed phrases entirely — which exposes them to potential breaches and losses.

Moreover, the vast majority of users in our study had no bequeathment plan for their crypto assets, running the risk of permanently losing their assets in the event of their death or injury since there are no third-party custodians who can scaffold the inheritance process by default. Overall, our research highlights the need for interventions that improve users' knowledge of seed phrases and seed phrase security, and the need to design non-custodial crypto wallets in a manner that nudges users towards safe and secure behaviors even with limited knowledge. By addressing these challenges, we can improve the security and usability of cryptocurrency wallets, and reduce the likelihood of users falling prey to scams.

Acknowledgments

This work was generously funded, in part, by a gift from IOHK. We also extend our thanks to Yang Wang, Tanusree Sharma, Yaman Yu, and Kyrie Zhixuan Zhou for helpful discussions that informed the design of our interview protocol. We would also like to thank Yousif Alnajjar, Nancy Zuo, and Roong Vorasucha for their contributions to this work.

References

[1] [n. d.]. 2024 Cryptocurrency Adoption and Sentiment Report. https://www.security.org/digital-security/cryptocurrency-annual-consumer-report/
[2] [n. d.]. Crypto Users Lost $2B to Hacks, Scams and Exploits in 2023, De.Fi Says. https://www.coindesk.com/tech/2023/12/27/crypto-users-lost-2b-to-hacks-scams-and-exploits-in-2023-defi-says/
[3] [n. d.]. Crypto users worldwide 2016-2023. https://www.statista.com/statistics/1202503/global-cryptocurrency-user-base/
[4] [n. d.]. Self-Custody: The Rise of Full Control over Digital Assets. https://www.arringtoncapital.com/blog/self-custody-the-rise-of-full-control-over-digital-assets/
[5] Svetlana Abramova, Artemij Voskobojnikov, Konstantin Beznosov, and Rainer Böhme. 2021. Bits under the mattress: Understanding different risk perceptions and security behaviors of crypto-asset users. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–19.

[6] Massimo Bartoletti, Stefano Lande, Andrea Loddo, and Livio Pompianu. 2021. Cryptocurrency Scams: Analysis and Perspectives. *IEEE Access* 9, 1 (January 2021), 1–1. https://doi.org/10.1109/ACCESS.2021.3123894

[7] Aaron W Baur, Julian Bühler, Markus Bick, and Charlotte S Bonorden. 2015. Cryptocurrencies as a disruption? empirical findings on user adoption and future potential of bitcoin and co. In *Open and Big Data Management and Innovation: 14th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2015, Delft, The Netherlands, October 13-15, 2015, Proceedings 14*. Springer, 63–80.

[8] Matt Bishop and Karen Nance. 2013. The Strengths and Challenges of Analogical Approaches to Computer Security Education. In *Information Assurance and Security Education and Training*, R. C. Dodge and L. Futcher (Eds.). IFIP Advances in Information and Communication Technology, Vol. 406. Springer, Berlin, Heidelberg, 129–136. https://doi.org/10.1007/978-3-642-39377-8_24

[9] Roman Bögli. 2023. *A Security Focused Outline on Bitcoin Wallets*. Ph. D. Dissertation. OST Ostschweizer Fachhochschule.

[10] E. F. Briefer, F. Rybak, and T. Aubin. 2013. Does true syntax or simple auditory object support the role of skylark song dialect? *Animal Behaviour* 86 (2013), 1131–1137. Issue 6. https://doi.org/10.1016/j.anbehav.2013.09.019

[11] Hanington Bruce and Bella Martin. 2019. *Universal Methods of Design: 125 Ways to Research Complex Problems, Develop Innovative Ideas, and Design Effective Solutions*. Rockport.

[12] José Campino and Shiwen Yang. 2024. Decoding the cryptocurrency user: An analysis of demographics and sentiments. *Heliyon* (February 2024). https://doi.org/10.1016/j.heliyon.2024.e26671

[13] Poulami Das, Sebastian Faust, and Julian Loss. 2019. A formal treatment of deterministic wallets. In *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*. 651–668.

[14] 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).

[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, 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 (DIS '20)*. Association for Computing Machinery, New York, NY, USA, 1751–1763. https://doi.org/10.1145/3357236.3395535 Published: 03 July 2020.

[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] 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.

[19] Mordechai Guri. 2018. Beatcoin: Leaking private keys from air-gapped cryptocurrency wallets. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, 1308–1316.

[20] Christopher Henry, Kim Huynh, Gradon Nicholls, and Mitchell Nicholson. 2019. *2018 Bitcoin Omnibus Survey: Awareness and Usage*. Technical Report. Bank of Canada Staff Discussion Paper.

[21] I. Honak and S. Babii. 2022. Types of cryptocurrency wallets. *Innovative Economy* (2022), 95–103. Issue 1. https://doi.org/10.37332/2309-1533.2022.1.13

[22] Charles M Kahn, Francisco Rivadeneyra, and Tsz-Nga Wong. 2020. Eggs in one basket: Security and convenience of digital currencies. *FRB St. Louis Working Paper* 2020-32 (2020).

[23] 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.

[24] 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.

[25] 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.

[26] Ponnurangam Kumaraguru, Steve Sheng, Alessandro Acquisti, Lorrie Faith Cranor, and Jason Hong. 2008. Lessons from a real world evaluation of anti-phishing training. In *2008 eCrime Researchers Summit*. IEEE, 1–12.

[27] Junchao Lin, Jason I Hong, and Laura Dabbish. 2021. " It's our mutual responsibility to share" The Evolution of Account Sharing in Romantic Couples. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (2021), 1–27.

[28] Gunnar Lindqvist, Joakim Kävrestad, Dennis Modig, and Ali Mohammad Padyab. 2021. How do Bitcoin Users Manage Their Private Keys?. In *7th International Workshop on Socio-Technical Perspective in IS Development (STPIS 2021)*, Vol. 3016. 11–21.

[29] Rachel Lustbader. [n. d.]. 2023 Wills and Estate Planning Study. https://www.caring.com/caregivers/estate-planning/wills-survey/. Accessed: 2024-05-25.

[30] 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.

[31] Tyler Moore, Nicolas Christin, and Janos Szurdi. 2018. Revisiting the risks of bitcoin currency exchange closure. *ACM Transactions on Internet Technology (TOIT)* 18, 4 (2018), 1–18.

[32] Florence Muchai. 2024. MetaMask hits over 30 Million active users – What's all the fuss about? https://cryptonews.net/news/security/28592209/#:~:text=Meta%20Mask%20goes%20mainstream%20in%20adoption&text=These%20stats%20virtually%20match%20the,during%20the%20last%20six%20months

[33] Hendrik Müller, Aaron Sedley, and Elizabeth Ferrall-Nunge. 2014. Survey research in HCI. *Ways of Knowing in HCI* (2014), 229–266.

[34] T.J. Newby, P.A. Ertmer, and D.A. Stepich. 1995. Instructional analogies and the learning of concepts. *Educational Technology Research and Development* 43, 1 (March 1995), 5–18. https://doi.org/10.1007/BF02300478

[35] Ehsan Nowroozi, Seyedsadra Seyedshoari, Yassine Mekdad, Erkay Savaş, and Mauro Conti. 2022. Cryptocurrency wallets: assessment and security. In *Blockchain for Cybersecurity in Cyber-Physical Systems*. Springer, 1–19.

[36] Snizhanna Alina Oleksandr Omelchuk, Inna Iliopol. 2021. Features of Inheritance of Cryptocurrency Assets. *Ius Humani Law Journal* (March 2021), 103–122. https://doi.org/10.31207/ih.v10i1.233

[37] Frédéric Prost. 2022. Inheritance and Blockchain: Thoughts and Open Questions. *arXiv* (2022). https://doi.org/10.48550/arXiv.2212.01194

[38] JJ Roberts and N Rapp. [n. d.]. Nearly 4 million Bitcoins lost forever, new study says, November 2017.

[39] Scott Ruoti, Jeff Andersen, Daniel Zappala, and Kent Seamons. 2015. Why Johnny still, still can't encrypt: Evaluating the usability of a modern PGP client. *arXiv preprint arXiv:1510.08555* (2015).

[40] 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.

[41] J. K. Shanmugam, Barathy Doraisamy, Santhi Appannan, Parteeban Varatarajoo, and Nurul Jannah Abdul Aziz. 2023. An Empirical Research on Factors Affecting the Acceptance of Bitcoin in the Northern Region of Malaysia. *East Asian Journal of Multidisciplinary Research* 2, 5 (2023), 2009–2030. https://doi.org/10.55927/eajmr.v2i5.3840

[42] Marie Vasek, Joseph Bonneau, Ryan Castellucci, Cameron Keith, and Tyler Moore. 2017. The bitcoin brain drain: Examining the use and abuse of bitcoin brain wallets. In *Financial Cryptography and Data Security: 20th International Conference, FC 2016, Christ Church, Barbados, February 22–26, 2016, Revised Selected Papers 20*. Springer, 609–618.

[43] 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.

[44] 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.

[45] Rick Wash, Emilee Rader, Ruthie Berman, and Zac Wellmer. 2016. Understanding password choices: How frequently entered passwords are re-used across websites. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. 175–188.

[46] Yoon-Chow Yeong, Khairul Shafee Kalid, K.S. Savita, M.N. Ahmad, and Maryam Zaffar. 2022. Sustainable cryptocurrency adoption assessment among IT enthusiasts and cryptocurrency social communities. *Sustainable Energy Technologies and Assessments* 52, Part A (2022), 102085. https://doi.org/10.1016/j.seta.2022.102085

[47] 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*. 1–17.

[48] Zhixuan Zhou, Tanusree Sharma, Luke Emano, Sauvik Das, and Yang Wang. 2023. Iterative design of an accessible crypto wallet for blind users. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*. 381–398.

[49] Karolis Zilius, Tasos Spiliotopoulos, and Aad van Moorsel. 2023. A dataset of coordinated cryptocurrency-related social media campaigns. In *Proceedings of the International AAAI Conference on Web and Social Media*, Vol. 17. 1112–1121.

A Appendix

A.1 Interview Questions

(1) What do users know about seed phrases?
- What do the seed phrases mean to you?
- Why did you start using cryptocurrency wallets? What are the reasons for continuing use?
- Have you joined any online or offline community groups to learn about cryptocurrency best practices? What did you learn from them?

(2) Why and how do users secure their seed phrases? Where do they learn these strategies?
- How many wallets do you currently manage? What are the most frequently used applications?
  - Are there any common backup methods they recommend? Which one?
  - How many of them explain how important seed phrases are?
- In your mind, how important is it to secure the seed phrases? Why?
- What, if anything, do you do to keep your seed phrase secure?
  - For each strategy:
    (a) Can you explain in detail how you record the seed phrases? How do you protect it? How many backups do you have?
    (b) Why do you employ this strategy?
    (c) Who are you trying to protect against?
    (d) Where did you learn about this strategy?
      * came from friends/ colleagues who also use crypto, from reading online resources like some accounts on social media/ from news articles?
      * Where are the strategies you learned but did not follow?
    (e) What are the worst consequences hat could happen if you didn't employ this strategy?
- Scenario Question (ask only if they don't say much for the securing seed phrase section): Let's say a friend of yours received a message from a vendor that they need to send their seed phrase over so that the vendor can verify a purchase. They come to you asking for advice on how to proceed. What would you say to this friend?
- (If they didn't mention about how to back up)Do you back up your seed phrase? How do you back up the seed phrase? Why did you choose these methods of backing up your seed phrase?

(3) What are the feelings of users to go through the account recovery process?
- Have you ever been through the account recovery process? (e.g., if you lost your password, the wallet was stolen, or the device you had the wallet on was damaged or lost, or you need to import to a new device.)
  (a) If yes:
    - could you describe it
    - Have you failed in the recovery like recovering or importing to a new device, what reason? Could you walk us through what was happening?
  (b) If no:
    - Do you know how to recover an account if you lose your seed phrase?

(4) When, why, and how do users share seed phrases with one another?
- Have you ever intentionally shared your seed phrase with others?
  (a) For each person:
    - With who? Why?
    - How did you share the seed phrase with this person?
    - Have you ever needed to use this social backup?
- Has anyone ever intentionally shared their seed phrase with you?
  (a) Who? Why?
  (b) What measures have you taken to store it securely?
- *(only ask if no one has ever shared with them) Imagine that a close friend of yours who is new to cryptocurrency asked you to keep a copy of their seed phrase for backup purposes. Would you accept? Why or why not? What concerns would you have?*

(5) What is users' mental model about shared accounts?
- Scenario question: Imagine that you and a few friends have decided to invest in cryptocurrency together. You have all agreed to use a shared account for your cryptowallet, where you can pool your funds and make trades as a group.
  (a) What kind of account would you choose to create? (e.g., a single account actively shared by several people; an account that can be accessed by others; threshold signature account, etc.)
  (b) Who would you choose to share the account with? (relationship to you? Personalities? Experience?)
  (c) Can you walk me through the most the recent time you need to use shared account, to keep the money safe, what will be some strategies to create the the joint account?
  (d) How would you feel about the security and privacy level of the account?
  (e) Would you trust your friends others to manage the account? How would you handle conflicts or disagreements within the group regarding the use of the account?

(6) What are the pain points when you use the seed phrases most recently?
- During your experience of using seed phrases to access crypto wallets, have you ever experienced any difficulties or pain points when using seed phrases? If so, can you describe the situation and what specifically caused the issue?
- What improvements or changes could be made to the process of using seed phrases that would make it more user-friendly or less prone to errors or security risks?

(7) How do people manage their crypto wallets if they pass away?
- Do you have a plan in place for your cryptocurrency assets in the event of your death? If yes, can you describe it?

- In your opinion, what steps should crypto owners take to ensure that their digital assets are managed properly in the event of their death?

A.2 Survey Questions

(1) Crypto trading habits and behaviors
  (a) Are you at least 18 years old?
    - Yes
    - No
  (b) How long have you been using crypto?
    - Less than 6 months
    - 6 months to 1 year
    - 1 to 2 years
    - 2 to 5 years
    - More than 5 years
  (c) What motivated you to start trading crypto? Check all that apply.
    - Research (i.e to research how it works, scholarly purposes, etc)
    - Financial Planning (i.e. investment)
    - Work (i.e for a business transaction)
    - Safety for money transactions (i.e because
    - it is one of the safest ways of transaction in a decentralized system)
    - Entertainment
    - Other:– – – – – – – – –
  (d) What kind of wallet do you mostly use to store the majority of your coins? Choose all that apply (make sure at least one item is checked off)
    - Hosted Web Wallet (e.g., wallets provided by cryptocurrency exchanges like Coinbase, and Binance)
    - Non-hosted Web Wallet (e.g.,MetaMask, Electrum)
    - Desktop Wallet (e.g., Bitcoin Core, Exodus)
    - Mobile Wallet (e.g., BRD, Mycelium)
    - Hardware Wallet (e.g., Ledger Nano S, Trezor)
    - Paper Wallet (Offline paper storage) Other (please specify)
  (e) What is your most used crypto trading platform?
    - Binance
    - Coinbase
    - Metamask
    - Other (please specify)
  (f) Of all the trading software you currently use, how many wallets do you trade with in total? (e.g. If you have 3 wallets on Metamask, that counts as 3.)
    - 0
    - 1-5
    - 5-10
    - More than 10
  (g) How many transactions have you done in the past month
    - 0
    - 1-5
    - 5-10
    - More than 10

(2) People's mental model of seed phrases People's mental models and understanding of seed phrases Seed phrase backup - What is people's understanding and awareness of safety measures of seed phrases? How do people rely on others to take additional safety precautions for their seed phrases?
  (a) As it relates to cryptocurrencies/web3, please select the option that best represents this image: (insert image)

    - Address
    - Passwords
    - Seed Phrase
    - CAPTCHA

    If selected C. Seed Phrase, proceed to question 2(b)
  (b) If you change your device and need to transfer everything into that new device, what information or items are generally required to import your cryptocurrency wallet to your new device? Assume you still have access to your wallet application but need to restore your account. (Choose the minimum required)
    - Username and Password
    - Private Key
    - Recovery Seed Phrase
    - Wallet Password
    - Two-Factor Authentication Codes
    - Email Address associated with Wallet
    - Backup Files from Wallet Application
    - None of the Above
  (c) Imagine a scenario where both your computer and phone were stolen, making your digital wallet inaccessible. Which of the following would you need for successful account recovery? (Choose the minimum required)
    - Recovery Seed Phrase
    - Private Key
    - Backup of Seed Phrase stored on an External Device
    - Access to Registered Email or Phone Number for Verification
    - Physical Security Token or Two-Factor Authentication Device
    - A New Device with the Wallet Application Installed
    - None of the Above
  (d) Can you choose your own wallet account seed phrases?
    - Yes, I can choose it like I choose the account password for other apps.
    - No, they cannot be chosen.
  (e) Suppose you see a friend replying to a post on a public forum asking people to share their seed phrase. How safe is this?
    - 1- Very Unsafe

- 2- Unsafe
- 3 - Somehow Safe
- 4 - Safe
- 5 - Very Safe

(f) Have you ever fallen for scams or did something wrong with your seed phrases?
- Yes I have
- Never

(g) Please specify your experience regarding falling for scams and/or did something wrong with your seed phrases.

(h) On a scale of 1-5, for each of the following behaviours, choose how much you agree with the following statement: This behaviour will keep my crypto wallet safe.
- Using a password manager, to avoid reusing passwords
  - 1 = Strongly Disagree
  - 2 = Disagree
  - 3 = Neutral
  - 4 = Agree
  - 5 = Strongly Agree
- Sharing seed phrase on public forum
  - 1 = Strongly Disagree
  - 2 = Disagree
  - 3 = Neutral
  - 4 = Agree
  - 5 = Strongly Agree
- Backup crypto wallet periodically
  - 1 = Strongly Disagree
  - 2 = Disagree
  - 3 = Neutral
  - 4 = Agree
  - 5 = Strongly Agree
- Using public WiFi to access crypto wallets or perform transactions
  - 1 = Strongly Disagree
  - 2 = Disagree
  - 3 = Neutral
  - 4 = Agree
  - 5 = Strongly Agree
- Using cloud storage services to store a backup of your seed phrase
  - 1 = Strongly Disagree
  - 2 = Disagree
  - 3 = Neutral
  - 4 = Agree
  - 5 = Strongly Agree
- Storing a large percentage of your crypto assets in an online wallet
  - 1 = Strongly Disagree
  - 2 = Disagree
  - 3 = Neutral
  - 4 = Agree
  - 5 = Strongly Agree
- Login into crypto accounts and make transactions
  - 1 = Strongly Disagree
  - 2 = Disagree
  - 3 = Neutral
  - 4 = Agree
  - 5 = Strongly Agree

(i) How do you currently back up your cryptocurrency wallet's seed phrase? (Check all that apply)
- No need to backup
- **Paper Backup: Writing the seed phrase on paper and storing it securely.**
- **External Drive: Saving on a USB drive or external hard disk.**
- **Internal Drive: Storing in a file on your computer's hard drive.**
- **Cloud Service: Using services like Google Drive or Dropbox.**
- **Email: Keeping a copy in your email account.**
- **Memorization (in my brain).**
- Other: [Please specify].

(j) On a scale of 1-5, choose how much you agree with the following statement: I feel that this method makes it easy for me to access my seed phrase backup.
- Paper Backup
  - 1 = Strongly Disagree
  - 2 = Disagree
  - 3 = Neutral
  - 4 = Agree
  - 5 = Strongly Agree
- External Drive
  - 1 = Strongly Disagree
  - 2 = Disagree
  - 3 = Neutral
  - 4 = Agree
  - 5 = Strongly Agree
- Internal Drive
  - 1 = Strongly Disagree
  - 2 = Disagree
  - 3 = Neutral
  - 4 = Agree
  - 5 = Strongly Agree
- Cloud Service
  - 1 = Strongly Disagree
  - 2 = Disagree
  - 3 = Neutral
  - 4 = Agree
  - 5 = Strongly Agree
- Email
  - 1 = Strongly Disagree
  - 2 = Disagree
  - 3 = Neutral
  - 4 = Agree
  - 5 = Strongly Agree
- Memorizing in the brain
  - 1 = Strongly Disagree
  - 2 = Disagree
  - 3 = Neutral
  - 4 = Agree
  - 5 = Strongly Agree

(k) On a scale of 1-5, choose how much you agree with the following statement: I feel that this method makes is safe and secure.

- Paper Backup
  - 1 = Strongly Disagree
  - 2 = Disagree
  - 3 = Neutral
  - 4 = Agree
  - 5 = Strongly Agree
- External Drive
  - 1 = Strongly Disagree
  - 2 = Disagree
  - 3 = Neutral
  - 4 = Agree
  - 5 = Strongly Agree
- Internal Drive
  - 1 = Strongly Disagree
  - 2 = Disagree
  - 3 = Neutral
  - 4 = Agree
  - 5 = Strongly Agree
- Cloud Service
  - 1 = Strongly Disagree
  - 2 = Disagree
  - 3 = Neutral
  - 4 = Agree
  - 5 = Strongly Agree
- Email
  - 1 = Strongly Disagree
  - 2 = Disagree
  - 3 = Neutral
  - 4 = Agree
  - 5 = Strongly Agree
- Memorizing in the brain
  - 1 = Strongly Disagree
  - 2 = Disagree
  - 3 = Neutral
  - 4 = Agree
  - 5 = Strongly Agree

(3) Users' learning methods about seed phrase

(a) On a scale of 1-5, choose how much you agree with the following statement: I learned a lot about backing up seed phrases from (the following methods)

- Cryptocurrency wallet apps usage
  - 1 = Strongly Disagree
  - 2 = Disagree
  - 3 = Neutral
  - 4 = Agree
  - 5 = Strongly Agree
- Social media feeds (e.g. Facebook, Twitter, Instagram)
  - 1 = Strongly Disagree
  - 2 = Disagree
  - 3 = Neutral
  - 4 = Agree
  - 5 = Strongly Agree
- Books, news, or articles
  - 1 = Strongly Disagree
  - 2 = Disagree
  - 3 = Neutral
  - 4 = Agree
  - 5 = Strongly Agree
- People close to you i.e friends and family
  - 1 = Strongly Disagree
  - 2 = Disagree
  - 3 = Neutral
  - 4 = Agree
  - 5 = Strongly Agree
- Online communities, chat groups and forums (Reddit, Discourse, and Discord groups)
  - 1 = Strongly Disagree
  - 2 = Disagree
  - 3 = Neutral
  - 4 = Agree
  - 5 = Strongly Agree

(4) People's trust in others regarding seed phrases

(a) Have you ever shared your seed phrases with someone else for any of the following reasons? Choose all that apply

- For a shared account (i.e you and others invest in cryptocurrency together, or you may have created a single account actively shared by others, or you created a threshold signature account, etc.)
- For backup purposes (part of your seed phrases)
- For account recovery (i.e your loved ones will be able to recover the crypto if you pass away or are severely injured)
- I haven't shared my seed phrases with anyone
- Other (please specify)

(b) On a scale of 1-5, choose how much you agree: I trust individuals I've shared with my seed phrases with.

- 1 = Strongly Disagree
- 2 = Disagree
- 3 = Neutral
- 4 = Agree
- 5 = Strongly Agree

(c) In your opinion, what are the most critical factors influencing trust when it comes to sharing seed phrases with others? (Choose all that apply)

- Personal relationship and history with the individual
- Legal agreements and documentation
- Knowledge and understanding of seed phrase security
- Reputation and credibility of the individual
- Third-party verification or validation Other (please specify)

(d) In the event of your passing, how do you envision your spouse or beneficiaries gaining access to your cryptocurrency holdings? Please select the most suitable option

- Recovery Seed Phrase
- Private Key
- Backup of Wallet Data stored on an external device
- Access to Registered Email or Phone Number for Verification
- Physical Security Token or Two-Factor Authentication Device
- A new device with the wallet application installed
- None of the Above (Please specify the reason)

(e) Can you explain your answer to the previous question?

If chosen any other option apart from (c) in 2(a), proceed to Q5.

(5) For the following questions, please focus your responses on a single cryptocurrency wallet (e.g. MetaMask, Electrum, Trust Wallet, etc) for this survey. Choose either your most important wallet or the one you use most frequently. Please specify the wallet you choose below.
(6) Which of the following methods do you use to secure your crypto wallet? Choose all that apply
- Username and Password
- Private Key
- Recovery Seed Phrase
- Wallet Password
- Two-Factor Authentication Codes
- Email Address associated with Wallet
- Backup Files from Wallet Application
- Pin
- Other (pleasee specify)

(7) How do you manage and secure your login credentials for your cryptocurrency wallet?
(8) How do you backup your login credentials?
(9) How would you recover your account in case you lose it? Do you use a dedicated device or computer for cryptocurrency transactions and wallet access?
(10) How do you manage and secure your digital assets in the event of the loss or theft of a device?
(11) Do you employ any form of encryption for your encryption for your cryptocurrency wallet backups or data?
(12) In case of a security breach or suspicious activity, what is your immediate response?
(13) How aware are you of the security features provided by the cryptocurrency platforms you use?
(14) Do you use any third-party security tools to enhance the security of your cryptocurrency transactions? If so, please list which ones.
(15) Have you heard of the term 'seed phrase" before? If so, what do you think a seed phrase is?
(16) How confident are you in your method of securing your cryptocurrency holdings?
(17) People's understanding of shared accounts?
- Have you tried sharing wallets / accounts with others (i.e created a single wallet actively shared by several people, or a wallet that others can access, or a threshold signature account, etc)?
  - Yes
  - No
- Think about the last time you shared a wallet / account with someone else. Why did you share this wallet? Choose all that apply.
  - Facilitating joint financial goals or investments
  - Ensuring access to assets in case of emergencies or incapacitation
  - Enhanced trust and transparency in the relationship
  - Simplifying the management of shared crypto assets
  - Other (please specify)
- Which of the following would you prefer to enhance the security of shared accounts? Choose all that apply
  - Setting passwords for the seed phrases
  - Splitting up seed phrases into multiple phrases
  - Keeping multiple wallets
  - Investing less money
  - Setting up the rules for trading, conflicts, and quitting
  - Other (please specify)