Web3 Recovery Mechanisms and User Preferences

Easwar Vivek Mangipudi
Supra Research
easwar.vivek@gmail.com

Panagiotis Chatzigiannis
Visa Research
pchatzig@visa.com

Konstantinos Chalkias
Mysten Labs
kostas@mystenlabs.com

Aniket Kate
Purdue University/Supra Research
aniket@purdue.edu

Mohsen Minaei
Visa Research
mominaei@visa.com

Mainack Mondal
IIT Kharagpur
mainack@cse.iitkgp.ac.in

Abstract

In a Web3 (blockchain) setting, account recovery allows users to regain access to their accounts after losing their authentication credentials. Although recovery mechanisms are well-established and extensively analyzed in the context of Web2 systems, Web3 presents distinct challenges. Web3 account access is typically tied to cryptographic key pairs, and private keys are not entrusted to centralized entities. This design improves security, but significantly complicates the recovery process, making it difficult or even impossible for users to regain access after loss of keys. Given the critical role that recovery plays in ensuring long-term feasibility and trust in digital systems, a range of recovery mechanisms have been proposed to accommodate the unique properties of Web3. These mechanisms aim to help users manage key loss without introducing undue friction or risk.

Although there has been an exponential increase in the use of cryptocurrency wallets in the last decade, the popularity and usage of the corresponding recovery mechanisms remain unclear. Furthermore, it is still unclear how users perceive these recovery mechanisms and what they expect from them. In this work, our objective is to empirically understand and analyze user perceptions of the various recovery mechanisms. To this end, we conducted a user survey of 331 participants and asked them to rate different mechanisms on *usability, security* and *availability*. The results show interesting aspects of the user preferences, including their view of sharing keys among different devices and trusting their friends or family. Based on our findings, we provide insight and future directions for the developer and research community.

1 Introduction

In the cryptocurrency world, wallets typically have a private-public key pair to authenticate transactions. This requires the user to obtain and maintain the private key securely to access their accounts. While the strong cryptographic security guarantees of the private key prevent unauthorized transactions, a potential loss of the key can lock out the user of his/her accounts, leading to permanent loss of access to all associated assets. This is an implication of the decentralized nature of blockchains, as there is no single entity with the power to restore access. Since 2009, when Bitcoin was launched, numerous stories have emerged in which users lost access to their funds due to being unable to access their keys for various reasons. As of 2025, about $11-18\%$ of all Bitcoins mined are estimated to be lost [5].

Users who interact with Web2 (or Web 2.0) applications rely on service providers for account recovery when they forget their password or otherwise lose access to their account. The recovery process involves identity verification, security questions, or email verification. However, this centralized process of account recovery is at direct odds with the decentralized architecture of Web3. In the Web3/blockchain world, it is entirely up to the users to manage their accounts safely. In the case of private key loss, no central authority or service provider can recover the account or funds on the user's behalf. In addition, in the case of a private key being stolen by an attacker who then makes an unauthorized transfer, there are no mechanisms to recover the assets due to the blockchain's irreversible nature.

Events such as accidental deletion, device loss, hardware failure, malware, or destruction of the storage medium [7] have the potential to result in the user losing access to a Web3 account and its associated assets. The death of a user also constitutes a loss scenario, as there is no built-in mechanism for transferring access to heirs unless proactive arrangements are made [13]. Funds can also be lost due to user error, such as mistyping a recipient address and sending assets to an account with no known private key [4, 8]. Without safeguards like checksums [40] or QR codes, such incidents effectively mirror key loss. To address these issues, several solutions were proposed for Web3 recovery . These are expected to give users some peace of mind, even in the worst-case scenario where the private key is lost. However, how well users understand different solutions and perceive their usability has not been explored or studied.

Few prior works [34, 60, 73] have explored user perceptions and mental models of cryptocurrency *wallets*. However, user preferences regarding *recovery mechanisms* remain completely unexplored, despite the growing adoption of cryptocurrencies and the recurring cases of asset loss. Understanding user expectations around recovery is, therefore, increasingly important. In this work, we aim to bridge the gap in this understanding and study users' perceptions and preferences about various recovery mechanisms.

Our contributions. We surveyed 331 participants, understanding their views and preferences on different recovery settings. Before asking users to analyze, we first educated them using a short video (2:07 min) on different recovery mechanisms. This is to bring all participants to a sufficient level of understanding. We asked users to analyze and rate each recovery mechanism according to three main properties of *usability, security*, and *availability*.

We present results based on statistical analyses that understand the different groups among the participants. In the survey, we presented different recovery settings to the participants, and based on their responses, we attempted to understand the relationships between how users perceive the recovery mechanisms and the three

properties. We also find which factors contribute to their perceptions, based on statistical tests. We identify the significant settings preferred for each of these properties and provide suggestions to the community on the areas to focus on in the future. Below, we discuss the research questions that we attempt to answer through this study.

1.1 Research Questions

The following key questions guide our research and survey:

RQ1: What are the usage characteristics of the participants for different wallets and recovery mechanisms? To investigate this question, we surveyed the participants about their usage patterns, experiences with cryptocurrency wallets, and their attitudes toward recovery features. We gathered information about how long they have been using cryptocurrency systems, the frequency of usage, and how they rate themselves with respect to cryptography/mathematics related to recovery mechanisms. Based on the responses, we find that the majority of the participants (61%) have been using the cryptocurrency wallet systems for the last $1-5$ years, and many of them are interested in using them for long-term investment and trading. Coinbase, Metamask, and Binance are among the top services that participants use. We asked the participants to rate themselves on a Likert scale of $1-5$ on how well they understand the cryptography of cryptocurrency systems. Based on the responses and the correlations among them measured by the χ^2-test, we identified that our participants behave as two specific groups *Experts* and *Non-experts*.

RQ2: Do users care about recovery mechanisms in cryptocurrency wallets? To address this question, we asked participants about their previous experience with cryptocurrencies and funds. We asked what percentage of their savings they typically invest and if they have ever lost the private key of the wallet. We enquired if they could recover the key or funds in case they lost the key. For participants who have not lost keys or funds, we asked what the likelihood is that they will lose their funds on a scale of $1-5$. To understand their further experiences and knowledge, we asked if they knew anyone in person or through the media who had lost their funds, and to rank their concerns regarding cryptocurrency wallets. Through these questions, we aimed to establish whether users consider recovery mechanisms when selecting wallets and how prominently recovery mechanisms feature as a factor in their decision-making process. From the survey responses, we identify that $61(\sim 18\%)$ of all the participants have lost their keys, and 17 of them could not recover them and lost their funds. The participants also rate 'lack of recovery mechanisms' as one of the primary concerns, with close to a majority (49.5%) of the participants ranking them 4 or higher among 6 choices, showing that recovery mechanisms are indeed crucial to the participants.

RQ3: How do the users perceive different recovery mechanisms based on the identified significant dimensions? To investigate this, we request users to rate different recovery mechanisms on various properties. We first ensured participants had a basic understanding of these properties through clear definitions of usability, security, and availability in the wallet recovery context. We provided an instructional video explaining these concepts and verified comprehension with simple knowledge-check questions. Once a common understanding was established, we asked participants to rate various recovery mechanisms along these three dimensions. Usability and security are understood in the literature [46, 49, 55]; however, Web3 presents a unique challenge of non-availability of the keys and mechanisms due to design differences in how public-private key pairs are handled. Hence, it is indeed important to study *availability* and how users perceive it. Recovery approaches evaluated included single-device key backups (paper, hardware device, cloud service), multi-device key backups (with copies or shares), two-party systems with reputed servers or trusted contacts, and various threshold schemes with different configurations. We find the different recovery mechanism settings and the properties that show significant correlations while fitting linear regression models. We find that the responses to the usability and availability ratings are fairly correlated for different mechanisms and in no setting are all three properties pair-wise correlated for experts and non-experts.

RQ4: What recovery mechanism configurations do users prefer for different properties? Building on RQ2, this question examined which specific recovery configurations users prefer when prioritizing different aspects of wallet recovery. We investigated the preferences between proactive recovery (requiring setup actions in advance) and reactive recovery approaches, optimal threshold configurations with various guardian types (friends/family, reputed servers, and random servers), preferred key storage locations under different scenarios, and the willingness to involve other stakeholders in the recovery process. We also explored how these preferences might vary based on user characteristics, including experience level, amount invested, and past experiences with loss of access to the wallet. The users find splitting the key among personal devices and sharing the keys among the servers and client devices to be more secure, storing the keys on personal devices, cloud servers, or splitting the key among cloud servers to be more available, having copies on personal devices or the cloud to be more usable among the different settings.

Organization of the paper. The rest of this paper is organized as follows. In section 2, we provide definitions of the properties, cryptographic background used in our paper and a general overview of existing recovery methods in the Web3 space. In section 4, we present the survey methodology and describe the recruitment procedure, quality control, pilot studies and the survey instrument. In section 5, we present the results for the different research questions in detail and present the analysis of the different statistical tests used to arrive at the results. In section 6, we discuss our observations from the results. We conclude our paper in section 7.

2 Preliminaries and Background

In this section, we provide the cryptography foundations necessary for our study, as well as the definitions and methods used in the Web3 recovery [43].

2.1 Cryptographic primitives

This section gives an informal overview of the cryptographic tools and concepts that appear throughout the paper.

Threshold signatures. A digital signature scheme allows someone with a secret key sk to sign a message m, producing a signature that others can verify using the corresponding public key pk. A threshold signature scheme extends this idea to a group: the secret key is split among multiple participants. Each participant can produce a partial signature and as long as at least t of them contribute, their partial signatures can be combined into a full signature that is valid under the public key of the group [39, 68]. This enables distributed signing without requiring the reconstruction of the whole secret key. Throughout the work, a (N, T) setting indicates that there are N devices or servers with key material, and any T of them are needed to generate the full signature.

Multi-signatures. In a multi-signature (or MultiSig) scheme, each participant has their own independent key pair $(\mathsf{sk}_i, \mathsf{pk}_i)$. To sign a message m, each participant creates their own signature using their secret key. These individual signatures are then collected to form a combined MultiSig [39, 52]. A MultiSig is valid if at least t of the included signatures are valid on the message. Multi-signature schemes are flexible and can support a wide range of access control structures, though they tend to produce longer signatures compared to threshold schemes. The (N, T) structure is valid in multi signatures as well; at least T among the N signatures are required for authentication.

2.2 Overview of recovery methods

Various methods have emerged to help users regain access to Web3 accounts in the event of loss or compromise of keys. In the following, we summarize the most common approaches and classifications.

- *Backup-based recovery.* A widely used approach that involves storing a copy of the private key or recovery phrase in a secure location. This can include offline devices (e.g., USB drives), encrypted cloud storage, or splitting the key into parts kept in separate places. While familiar to users, this method requires careful handling to avoid both accidental loss and unauthorized access.
- *Seed-phrase based recovery.* Many wallets use seed phrases, typically 12 words, as a backup mechanism. These phrases deterministically generate the private key, offering a balance between usability and security. However, they must be protected as they grant full access to the account.
- *Guardian-based recovery.* Some wallets allow users to appoint trusted individuals or entities as *guardians*, who can help with recovery in the event of key loss. These guardians may be selected based on personal trust (e.g., friends or family) or reputation systems. Guardians do not hold full control of the wallet but can jointly approve recovery actions. This approach is often referred to as social recovery [1, 12] and is a special case of trust-based recovery mechanisms.
- *Multi-key recovery.* Certain wallets, such as those using Multi-Party Computation (MPC), threshold cryptography, or multi-signatures, distribute signing authority across multiple keys. In these systems, losing a single key does not necessarily result in account loss, as the remaining keys can be used to replace or recover the lost one. Recovery can be handled cryptographically or via logic encoded in smart contracts [36].
- *Recovery through pre-signed transactions.* Some users prepare signed transactions in advance that can transfer funds to a backup account if needed [70]. This recovery is different from other approaches, since in this approach, funds are directly recovered instead of recovering the key.
- *Contract-based recovery.* A recent proposal [38] replaces predefined guardians with open recovery mechanisms, allowing anyone to initiate a recovery process subject to longer delays and verification steps. Although this eliminates the need for trusted parties, it may introduce complexity and extended wait times.

2.3 Classification of recovery methods

Recovery methods may be classified according to when the user needs to take action to set up recovery or whether the user needs to recover the secret key or just the funds.

- *Proactive vs. reactive recovery.* A proactive approach requires users to prepare ahead of time, for instance by saving a backup, configuring guardians, or distributing key shares. If the user does not complete these steps, recovery becomes impossible. In contrast, a reactive approach enables recovery after key loss without requiring earlier setup by the user. These methods often rely on system-level functionality, such as smart contracts, and may be more user-friendly as they reduce the cognitive burden at setup time.
  From a usability standpoint, reactive methods are naturally preferred, especially by users who prioritize convenience and quick onboarding. Although all systems involve some setup (e.g., deploying a smart contract), recovery is considered reactive if the user does not need to take explicit preparatory actions [43]. Note that everyday access mechanisms like PINs or passwords are not considered as proactive recovery actions. These are part of standard access control and fall outside of the definition of recovery setup.
- *Account vs. funds recovery.* In most scenarios, users are only concerned with regaining access to their funds. However, some use cases require restoring the original account address itself. This becomes important when external systems are programmed to send funds to a specific account or when that account has associated on-chain logic. Simply recovering the funds to a new account may not be sufficient. This distinction is particularly relevant in programmable environments like Aptos or Libra [16, 35], where accounts support features such as key rotation or delegated withdrawals. In such cases, recovery is more than just asset transfer, as it involves restoring full account functionality.

2.4 Properties of recovery methods

We provide the three key properties [43] of the recovery methods that shape their design and evaluation.

- *Usability* captures how easily users can interact with the recovery system and the Web3 wallet as a whole [56, 57]. In noncustodial wallets, where users are responsible for safeguarding their private keys, usability is often hindered by complex mechanisms

such as seed phrases or the need to coordinate across multiple devices [37, 45, 50].
- *Security* ensures that recovery is only possible by the rightful account owner. Secure systems must defend against threats like unauthorized recovery attempts, denial-of-recovery attacks, and partial key compromises. While stronger security usually involves added layers of authentication or cryptography, these often trade off against ease of use.
- *Availability* refers to whether the recovery system is accessible at the moment of need. For example, methods that depend on third parties (e.g., guardians or other devices) may fail if those parties are unreachable or unwilling to cooperate.

In this study, we request users to analyze each of the recovery methods on these three properties.

2.5 Threats to recovery systems.

Adding recovery features sometimes introduces new risks; these should be thought through while choosing a recovery method. We list the risks below.

- *Unauthorized recovery.* Attackers might initiate a recovery process to take control of a victim's account. This includes scenarios where one or more trusted parties (e.g. guardians) are compromised.
- *Denial of recovery.* Even if guardians or key holders are not malicious, they may be unavailable or refuse to participate unless incentivized, effectively blocking recovery.
- *Key compromise.* In distributed key systems, attackers who gain access to some key shares reduce the threshold for full compromise [59]. If a partial compromise is not addressed quickly, it may escalate into total loss.
- *Privacy leakage.* If an attacker can detect that a recovery process has begun, they may launch targeted attacks (e.g., social engineering or front-running) to interfere. Some recovery schemes (e.g. multi-signature wallets) reveal structural details about how keys are managed. This can give away information about the type of wallet or user behavior. While some wallets aim to obscure these details, implementation quirks (e.g., randomized retries in ed25519 signatures [42]) can compromise this property.

2.6 Related work

Account recovery is a fundamental aspect of digital identity and asset management. In traditional Web2, recovery is typically provider-mediated, relying on centralized mechanisms. Email-based and SMS-based password resets remain dominant, though vulnerable to account takeover and hijacking [32]. Recovery codes are another widely deployed mechanism, but users often misunderstand or mishandle them [51]. These approaches prioritize recoverability but introduce central points of failure due to their centralized nature.

In Web3 and blockchain systems, the burden of recovery shifts entirely to the user, who is responsible for cryptographic key management. A variety of protocols and standards have been proposed. Smart-contract-based social recovery schemes enable recovery via trusted contacts [23], while Stellar SEP-30 defines recoverable wallets without custodians [47]. Other proposals include smartcard backup for cryptocurrency wallets [14], shared-custodial wallets [29], hardware-wallet recovery approaches avoiding root-seed cloning [27], and user-generated data for key recovery in *Reminisce* [19]. Account abstraction proposals such as EIP-4337 also enable account-level recovery [21], and recent work explores social-service-based recoverable wallets [28] and Shamir-based recovery for SSI wallets [22].

Existing recovery methods in the industry. In a commercial product setting, a number of wallets exist with built-in recovery functionalities, such as Argent [1] which combines off-chain recovery with smart contract guardians, Braavos [2] which manages two keys in a 2-of-2 multisignature, Sequence [10] which offers multi-key approaches with session keys, backup keys, and in some versions, network-stored keys [11] requiring multi-signature verification, and Coinbase [58] which provides wallet recovery through shares stored in cloud storage and with service providers, or by encrypting shares with the user's public key. Note that most of these deployed wallets are not just implementing one Web3 recovery approach, but are offering multiple ways of recovery [44] to increase availability.

Some Ethereum proposals like EIP2429 and ERC4337 [41, 66] embed recovery functionalities in Ethereum using guardians, while KELP [38] is a smart contract recovery protocol without guardians. While in both cases a smart contract account is required, the main difference lies in their proactive and reactive nature respectively. Guardians require a proactive configuration unless a default guardian is chosen on the user's behalf by the wallet software, which is not a recommended practice. KELP does not need any such configuration in the absence of guardians. KeyClub and RandRec [6] offer social key recovery protocols for guardians without deep cryptography knowledge using a Verifiable Random Function, offering a different angle on usability. For further recovery solutions in this space, we point the reader to [43].

3 Usability in the Web3 setting

There has also been a spike in interest on usability issues in cryptocurrency systems in the recent past [31, 61, 72, 73]. Voskobojnikov et al [72] discuss several perceived risks of both users and informed non-users in cryptocurrencies. The authors of [73] study and report the user experience by analyzing a large number of public ratings of cryptocurrency wallets. Frohlich et al [48] conducted semi-structured interviews, studied the usability of wallets and proposed models to map users by key management. Krombholz et al [55] studied the flaws in the usage of Bitcoin wallets by performing large-scale survey of security practices of Bitcoin users. Recently, Mangipudi et al [61] studied the user mental models in cryptocurrency wallets; they segregated participants into two groups. All the participants who identified themselves as newbies are considered newbies and everyone else as non-newbies. However, their work focused on wallets while we focus on recovery mechanisms and user preferences regarding them. As far as we know, we are the first to attempt to understand the usability of recovery mechanisms and user perceptions about them.

Usability of recovery methods. Human-centered studies highlight the practical difficulties of Web3 recovery. The CHI'25 study [30] investigates user behaviors and challenges in seed-phrase management. Users' wallet choices and recovery expectations are studied in [25], and trust in custodial vs. non-custodial recovery is analyzed

in [26]. Mobile wallet usability, including recovery workflows, was investigated in [15]. A usability study of a decentralized identity wallet confirms recovery as a central usability issue [18], complemented by evaluations of SSI digital wallets [24]. Additional research, such as heuristic evaluations [17] and user perception studies [20], further illustrates the fragility of user-driven recovery.

Several works bridge Web2 and Web3 recovery models. NIST's report on Web3 emphasizes the shift in responsibility from service providers to individuals [64]. A systematization study on Web authentication under end-to-end encryption highlights how even Web2 applications increasingly face similar constraints when providers cannot mediate recovery [63]. Trustless account recovery mechanisms [53] attempt to replicate Web2-style usability while retaining Web3 decentralization. Empirical studies of decentralized identity wallets [67, 71] also confirm this shift. Owing to the challenges in realizing the recovery methods in Web3, it is important to understand and analyze how users perceive these methods and their preferences.

4 Survey Methodology

To empirically investigate user perspectives on Web3 recovery mechanisms, focusing on their perceived importance, the trade-offs involved, and preferred configurations (addressing RQ1-RQ4, see section 1.1), we designed and deployed an online survey. See Appendix B for the survey instrument. This section details our methodological approach.

4.1 Survey instrument description

Our survey was structured into two main parts. Part I collected data on participants' general background, usage patterns, and prior experiences concerning cryptocurrency wallets. Part II shifted focus to wallet recovery, probing participants' understanding of core recovery concepts and their preferences for various mechanisms and configurations, particularly concerning the trade-offs between usability, security, and availability.

Part I: General Usage and Experience. This initial section aimed to establish a baseline understanding of participants' familiarity and interactions with cryptocurrency wallets. We inquired about the duration and primary purposes of their wallet usage (e.g., long-term investment, trading, regular transactions). Participants listed the wallets they used most often and the reasons for their choices, citing factors like perceived security, ease of use, multi-currency support, and available backup or recovery features.

Furthermore, this part directly addressed participants' experiences with losing wallet access. We asked if they had ever been locked out due to a forgotten password or lost secret key, and if so, how they attempted recovery (e.g., personal backups, provider instructions) and whether they were ultimately successful or if funds were permanently lost. To contextualize their perspectives on recovery, we also explored their perceived likelihood and reasons for potential future fund loss, encompassing concerns like user error, device compromise, or attacks targeting wallet providers. This background information was crucial for interpreting the preferences expressed in the survey's second part.

Part II: Recovery Mechanism Preferences. The second part of the survey delved into user preferences regarding specific recovery mechanisms and their properties. To ensure a common understanding, we initially presented an instructional video [1], describing the key properties of recovery schemes, *usability*, *security*, and *availability*, as discussed in section 2. We verified comprehension with True/False questions before proceeding. Participants then evaluated a variety of recovery strategies—such as single-device backups, multi-device key sharing, guardian-based systems, and threshold schemes—rating each strategy along the three defined dimensions (usability, security, availability).

Following the evaluation of individual strategies, we explored preferences for different configurations and trade-offs. This included assessing views on multi-party recovery thresholds, combinations of personal devices versus external servers for storing key shares, and the choice between proactive (set up in advance) versus reactive (initiated after loss) recovery models. Participants rated each configuration based on its perceived usability, security, and availability, and also indicated the relative importance they place on each property when choosing a recovery solution. This multi-faceted approach allowed us to capture nuanced perspectives on the trade-offs users are willing to accept in different recovery scenarios.

4.2 Pilot Studies

Before launching the full survey, we conducted pilot studies with five participants in-person via an interview to refine the instrument. The pilots focused on evaluating the clarity of instructions and questions, identifying ambiguities (particularly around recovery concepts), assessing the effectiveness of the educational video and definitions, and estimating the survey completion time. Based on the feedback, we identified six questions or associated choices that were ambiguous. Consequently, we removed three questions deemed redundant or imprecise and modified the wording of several choices to enhance clarity and reduce potential confusion.

A significant revision involved the section addressing proactive versus reactive recovery. Initially, this section included a dedicated video followed by a complex matrix question for preference elicitation. Pilot feedback indicated this approach was overly burdensome. We therefore removed both the video and the matrix question, replacing them with a single, streamlined multiple-choice question. This revised question educated participants about the features of proactive and reactive recovery directly within the answer choices, simplifying the task and reducing the time required while still capturing essential preference data.

4.3 Recruitment

Our online survey aimed for broad reach while targeting relevant participants, namely active crypto-wallet users and enthusiasts. To achieve this, we utilized the crowdsourcing platform Prolific.co, following established practices in related user studies [31, 61].

Recruitment from Prolific: Participants were sourced from the US and the UK[2]. We excluded individuals who had participated in our

[1] https://www.youtube.com/watch?v=luSsaqAq4dg

[2] Over 65% of Prolific participants are from the US and UK [9], are English speakers, and are over 18 years old.

pilot studies. Selection was based on a preliminary screening survey (see appendix A) consisting of five questions about wallet usage duration, frequency, and specific wallets used. To filter out irrelevant responses, the question requesting current wallet names required text entry; blank or invalid entries led to exclusion. The screening also confirmed interest in participating in the main, longer survey.

The final survey was deployed on Prolific.co over one week, using multiple batches of $30-50$ participants released at various days and times to mitigate temporal biases [33]. The median completion time was 16.87 minutes. Participants received a median value of 3.37$, corresponding to an estimated hourly wage of 12$ per hour, which aligns with rates reported in similar studies [31, 61, 62].

Ethical Considerations: Prior to starting, all participants received information about the study's purpose, estimated duration, and compensation. We assured anonymity and stated that no personally identifiable information would be collected. Participation was voluntary, with the option to withdraw at any point. Any potentially identifying information inadvertently collected was removed from the dataset. The study protocol and instruments were reviewed and approved by the author's Institutional Review Board (IRB).

4.4 Quality Control

To maintain data integrity, we implemented several quality control measures. An attention check question, asking participants to identify the current month, was included in the survey flow. We also assessed responses to the knowledge-based True/False questions, designed to check comprehension of the concepts presented in the educational video. Participants were required to answer all three questions correctly to be included in the final analysis.

Given the educational video had a runtime of 2 minutes and 7 seconds, we established a minimum completion time threshold. Participants completing the entire survey, including the video viewing time, in less than 7 minutes (suggesting rushing or inattention, potentially finishing the survey sections in under 5 minutes) were excluded.

4.5 Participant Demographics

In total, 550 participants completed the survey via Prolific. After applying our validity criteria and quality checks (section 4.4), 331 valid responses remained for analysis. Detailed demographic information for this final participant pool is presented in table 1. Studies show that the users of Prolific often share general attitudes about security and privacy [65]. Thus, we believe our findings reflect views within the cryptocurrency community.

Summarizing the demographics, 60.4% identified as male and 39.5% as female (with 2 participants preferring not to answer), indicating a sample bias towards male participants, common in crypto-related studies [61]. The largest age group was $35-44$ (28.7%), followed by $25-34$ (21.4%) and $45-54$ (19.3%), suggesting a predominantly younger cohort (under 35). Education levels were relatively high, with 60.7% holding a Bachelor's degree or higher, exceeding general US population statistics [3]. Despite potential expectations of tech-savviness among crowdsourcing participants [54], a majority (58.9%) reported no professional or academic background in IT or computer science. Participants were active crypto users, investing an average of 23.05% of their savings in cryptocurrencies.

Table 1: Participants' Demographics

	Non-expert	Expert	Total
	173	158	331
Gender			
Female	74	55	129
Male	99	101	200
Prefer not to answer	0	2	2
Age			
18-24	34	15	49
25-34	32	39	71
35-44	45	50	95
45-54	40	24	64
55-64	17	16	33
65 or older	5	10	15
Education			
High school	33	33	66
College degree	27	20	47
Bachelor's degree	66	72	138
Master's degree	27	29	56
Doctorate	4	3	7
Prefer not to answer	16	1	17
Employment status			
Full-time	108	115	223
Part-time	26	21	47
Unemployed	12	4	16
Retired	1	2	3
Student	13	5	18
Other	6	8	14
Uncompensated	3	2	5
Prefer not to answer	4	1	5
Background in IT			
Yes	53	68	121
No	109	86	195
Prefer not to answer	11	4	15

Overall, the sample represents a group of young, educated, and financially invested cryptocurrency users.

5 Results

5.1 RQ1: Usage characteristics of different wallets and recovery mechanisms

Two distinct user groups exist. We asked the participants how far they agree that they understand the cryptographic concepts related to performing transactions using cryptocurrency wallets. They were asked to rate on a Likert scale of $1-5$. All the participants answering $(4, 5)$ on the Likert scale are grouped as self-perceived *Experts* and the others as *Non-experts*. We categorized the users based

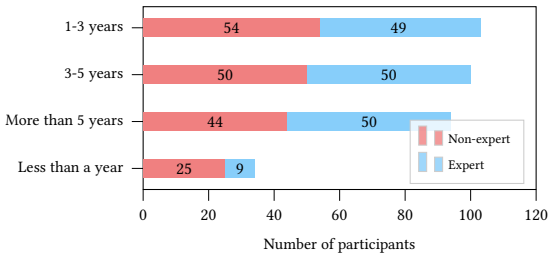

Figure 1: Duration of crypto-wallet usage by the participants.

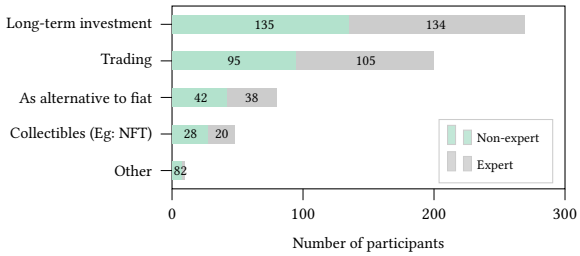

Figure 2: Purpose of using crypto-wallets; Majority of participants use them for long-term investments and trading.

on self-identification; however, this division corroborates with statistical tests from other independent survey responses, regarding usage, preferences, and demographic dimensions. Specifically, responses to the questions that correlated between these two groups are briefed in Table 2. The existence of two groups is similar the existence of (differently arrived at) groups among the participants [61] for cryptocurrency wallet usage. Here, we focus on recovery mechanisms.

The two groups show a strong correlation across different kinds of responses and how they rate different properties of different recovery mechanism settings. The groups show correlations in the percentage of savings invested in cryptocurrency wallets, reasons for choosing the current wallets, their perception of future loss of funds, age, employment in the field of computer science, their usage of the wallets. Their responses also correlate strongly on how they rate different recovery mechanism settings in terms of the properties they offer, as presented in Table 2.

Usage of wallets - duration, purpose and reasons for choosing. Our survey shows that 31.6% of the Experts and ∼ 25.4% of the Non-experts have been using cryptocurrency wallets for more than 5 years and less than 6% and 15% of Experts and Non-experts have started using the wallets in the last one year. The majority of the participants have been using wallets for more than 3 years, compared to previous studies [61] where the majority were more recent adopters. The usage choices are presented in Figure 1.

Figure 2 shows the usage patterns of the existing wallets of the users where the majority of the Non-experts and Experts are using the cryptocurrency wallets for long-term investments and for trading. Figure 3 shows the different reasons for choosing the current most-used cryptocurrency wallets by the participants. Interface being easy to use and the security guarantees being offer by the

Table 2: χ^2 test results for variables with p-value < 0.05, comparing distributions between Experts and Non-experts. df is degrees of freedom. 331 total number total samples.

Variable	χ^2	df	p-value
% of savings in crypto-wallets	99.3927	52	8.38e-05***
Reason for choosing wallet	103.0013	76	2.13e-02*
Ever lost secret key	4.3899	1	3.62e-02*
Likelihood of loss of funds	23.5399	4	9.88e-05***
Hearing about anyone losing funds	6.8098	2	3.32e-02*
Choice of recovery mechanism	17.6214	6	7.25e-03**
Key on personal device - Security	12.1336	4	1.64e-02*
Key on cloud server - Availability	14.9386	4	4.83e-03**
Key copied on cloud servers - Availability	11.4900	4	2.16e-02*
Key split among cloud servers - Usability	10.7122	4	3.00e-02*
Key split between cloud server and user device - Usability	18.3380	4	1.06e-03**
Key copied on multiple user devices - Usability	13.0200	4	1.12e-02*
Key split among multiple user devices - Availability	19.9114	4	5.20e-04***
Key split among cloud servers - Security	25.1631	4	4.67e-05***
Key split between cloud and user device - Availability	25.2433	4	4.49e-05***
Two shares of key - each at client and reputable server - Usability	14.4362	4	6.03e-03**
Two shares of key - each at client and reputable server - Availability	17.4284	4	1.60e-03**
Two shares of key - each at client and friend/relative - Usability	13.9286	4	7.53e-03**
Two shares of key - each at client and friend/relative - Availability	17.1816	4	1.78e-03**
$(100, 5)$ setting with randomly chosen cloud servers - Availability	9.6953	4	4.59e-02*
$(100, 50)$ setting with randomly chosen cloud severs - Availability	17.4994	4	1.55e-03**
$(10, 5)$ setting with key shares at friends/family- Availability	16.0729	4	2.92e-03**
$(10, 5)$ with key shares at reputable servers - Availability	14.5052	4	5.85e-03**
Multi-key with controlling custody	32.5530	4	1.47e-06***
Multi-key recovery	26.5885	4	2.41e-05***
Age	20.8617	5	8.60e-04***
Employment in IT	21.4752	2	2.17e-05***
Usage of wallets	16.2017	2	3.03e-04***

Significance codes: ***$p < 0.001$, **p <0.01, *p <0.05

wallets are the top two reasons followed by the popularity and support for multiple currencies. Regarding choosing the wallets looking at the popularity and rating, 57 participants (29 Experts and

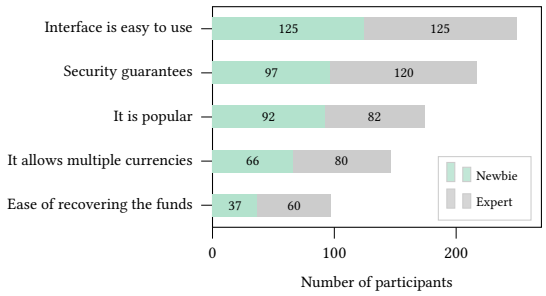

Figure 3: Reasons for choosing the most used cryptocurrency wallets by the participants.

28 Non-experts) chose their current wallets solely based on the ratings and a total of 238 participants mentioned that they did not choose solely on ratings but they are important.

We asked the participants if they lost their key before or not and if not, how likely it is that they may lose their funds in their future on a Likert scale. A majority of the participants who have not lost funds have said that it is unlikely that they will lose their funds in the future (see Figure 4).

Among the participants who have not lost the funds, the majority of them feel (4, 5 on a Likert scale of 1 – 5 with 5 being very unlikely) that it is unlikely that they are going to lose funds/keys in the future (see Figure 4). This shows that participants who have not lost funds before are more inclined to believe that they will not lose funds in the future. This is in spite of the fact that the majority of the participants know of people losing funds either through social media or personally (see Figure 5).

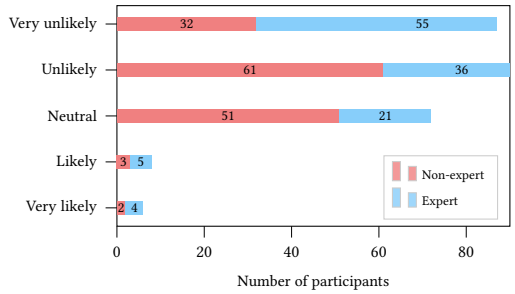

Figure 4: Assumed likelihood of loss of funds, for the participants who have not lost keys/funds.

5.2 RQ2: Do users care about recovery methods?

There have been significant attacks on cryptocurrency wallets and blockchain systems, with various studies showing their vulnerabilities and potential attack vectors [43]. In view of this, it is essential to understand how users view loss of funds, recovery mechanisms, and whether they care about them.

18% *of participants lost their keys before.* Among the participants, 23.4% of Non-experts and 13.9% of participants have lost the keys or funds from their cryptocurrency wallets. That amounts to a total of 61 participants. Out of them, 17 of them could not recover and lost their funds while 44 could recover their funds.

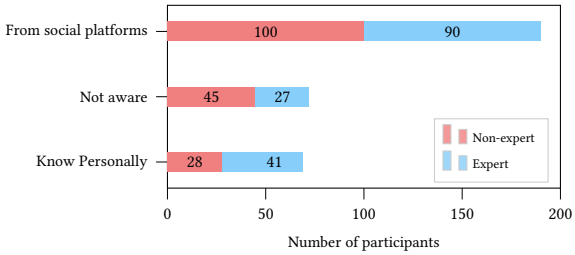

Figure 5: Awareness about loss of funds

Figure 5 shows that 20.8% of the participants know someone who lost keys/funds personally and 57.4% of all the participants have heard of someone losing their funds through social media platforms.

Lack of recovery is among the most significant security concerns. The participants were asked to rank the five security concerns regarding loss of secret key by the user, compromise of the server, compromise of the key *by* the server hosting the key, compromise of the user device by an adversary and lack of proper recovery mechanisms by the wallet providers in the order of lowest (rank - 1) to highest concern (rank - 5). The average of the ranks of the above options are 2.58, 2.83, 3.09, 3.36, 3.38 respectively, showing that lack of recovery mechanisms and compromise of user device by an adversary are among the highest concerns for the participants.

Table 3 shows how many participants have ranked "lack of recovery mechanism" as their lowest (rank - 1) to their highest (rank - 6). 49.5% of the particpants have ranked lack of recovery mechanisms as a major concern (4 or higher). This shows that a close to a majority of the participants are indeed interested and concerned about recovery mechanisms in the wallets they use. Among experts, 54% of the participants rank recovery mechanism at 4 or higher (on a scale of 1-6) as a concern. This shows that the users indeed care about the recovery mechanisms of their wallets.

Table 3: Counts of ranking "lack of recovery mechanism" as a security concern among the participants. 1 is the least concern, 6 is the highest concern

Rank	All	Experts	Non-Experts
1	45	21	24
2	48	20	28
3	68	30	38
4	71	34	37
5	90	47	43
6	3	2	1

Table 4: p-values for different wallet settings for which usability and availability responses significantly correlate

Recovery setting	Coefficient	P-value
Key copies on cloud storages	0.5843	1.37E-29
$(100, 50)$ with random cloud servers	0.5668	1.05E-27
Key copies on cloud storages	0.5518	4.88E-25
$(10, 5)$ with shares at reputable servers	0.5363	3.39E-24
Two copies - Client and Reputable server	0.5534	2.58E-23
Key split among user devices	0.5190	2.43E-22
Two copies - Client and Friend/Relative	0.5216	5.01E-21
Two shares - Client and Reputable server	0.4667	2.98E-18
Key split among cloud storages	0.4749	3.51E-18
Two shares - Client and Friend/Relative	0.4336	2.87E-16
Personal device	0.4891	5.43E-16
$(100, 5)$ with random cloud servers	0.4335	7.88E-15
Key on cloud storage	0.4140	5.13E-13
$(10, 5)$ with shares at family/friends	0.3812	5.20E-13
Key at family/friends	0.4117	3.27E-14
Key on personal device	0.4205	1.49E-10
Key on paper copy	0.3709	1.46E-10

5.3 RQ3: How do the users perceive different recovery mechanisms based on the identified significant dimensions?

The participants have been asked to rate different recovery settings against usability, security, and availability on a Likert scale of $1-5$ where 1 indicated the property being satisfied the least and 5 the highest. The ratings can be viewed as a tuple of 3 elements for each wallet by each participant. For ease of depiction, we convert the ratings into two *Low-L* and *High-H*. This is in line with the standard practices in the literature [69], where a Likert scale is dichotomized. Figure 6 and Figure 7 present the ratings of the participants for the different recovery settings considered in this work when availability is Low (L) and High (H). Similar data for experts is reported in Table 5 in the Appendix.

It can be observed that a maximum of 40.8% participants gave a (H, H, H) rating to any wallet. This shows that the majority of participants do not believe that any recovery setting satisfies all the three mentioned properties. Below, we list key takeaways from Figure 6 and Figure 7.

No Perfect Solution Exists. Most participants believe no wallet solution provides an ideal balance between usability, security, and availability. As shown in fig. 6, fig. 7, users consistently indicate that current solutions fall short of ideal implementation, with no option receiving more than 41% high ratings across all three properties. This widespread perception demonstrates the significant challenge wallet designers face in creating solutions that excel in all critical dimensions simultaneously. The data suggests an inherent tension between these properties, where improvements in one area often necessitate compromises in others, pointing to what could be described as a "trilemma" in wallet design.

Personal Devices and Cloud Services as Leading Options. Personal devices and cloud services emerge as the clear leaders in user preference. Personal devices achieved the highest overall satisfaction at 40.73% rating all properties highly, with cloud services following closely at 38.60%. These two options significantly outperformed all other storage methods, suggesting users gravitate toward solutions that offer direct control or trusted institutional management.

Personal Devices - Mixed Security Perception. While about 80% of participants rated personal devices highly for availability and usability, opinions were divided on security. Approximately half rated personal device security as high, while the other half rated it as low.

Social Recovery Rejection and Low-Performing Options. Users strongly reject wallet solutions that involve family and friends. Storing full keys with family and friends received the worst ratings, with 37.69% of users giving it low scores across usability, security, and availability. Only 13.98% rated this option highly in all three areas. This negative pattern continues with other family/friend approaches - both splitting keys with relatives (26.75% gave low ratings) and creating copies for relatives (22.80% gave low ratings) were unpopular. These consistently poor ratings show that users are uncomfortable with social recovery options regardless of how they're implemented. Despite experts often recommending social recovery for inheritance planning and emergency access, users appear to have fundamental trust concerns about involving personal connections in their cryptocurrency security.

Strategic Trade-offs: Splitting vs. Copying. Users clearly understand the strategic differences between key splitting and key copying approaches. 32% of participants noted that splitting keys between client and reputable server provides high security but low availability and usability. Conversely, only 7% expressed similar concerns when making copies across client and servers. The same pattern was consistent where we had friends/family instead of reputable servers.

The Paper Copy Paradox. Paper copies present a fascinating paradox in user sentiment. While 17.33% of users rated them low across all properties, 15.81% rated them high across the board, highlighting a clear polarization. Moreover, paper copies had the highest percentage (32.83%) of ratings in the "low security but high usability and availability" category, suggesting that although users find paper copies convenient and accessible, they do not consider them secure for storing their keys.

Usability and Availability. We fit linear models (using `lm` model in R language) on the responses to see correlations between different properties perceived by the participants. The usability and availability ratings of the participants correlate for all the recovery settings. Table 4 depicts the settings with significant correlations between the two ratings. The presented p-values are after applying Bonferroni correction. Figure 8 shows the difference in ratings between usability and availability by the participants for the different

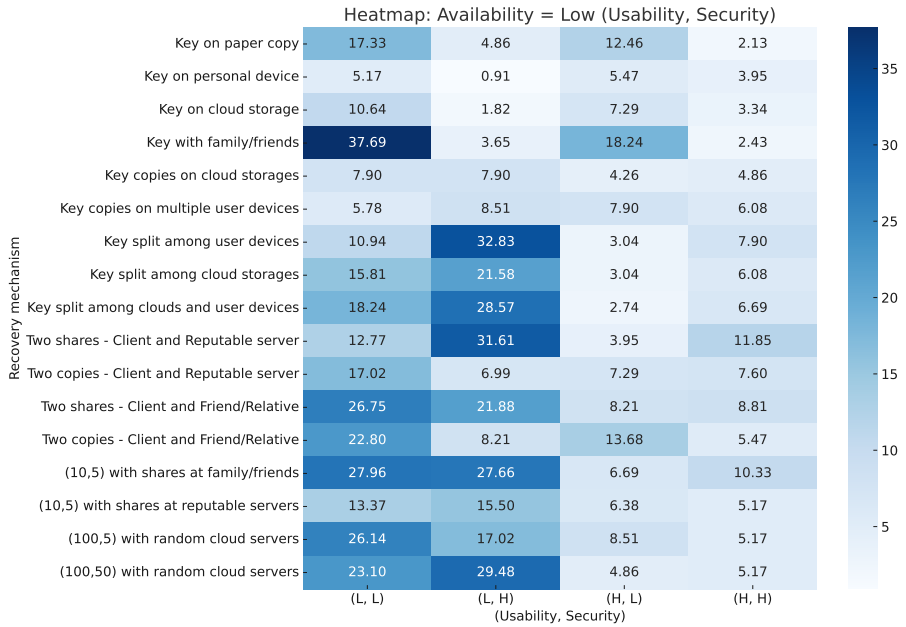

Figure 6: Heat map of participant percentages rating each recovery mechanism setting, with Availability = Low (L). The concentration of the dark blues on the left indicates that the usability is considered Low (L).

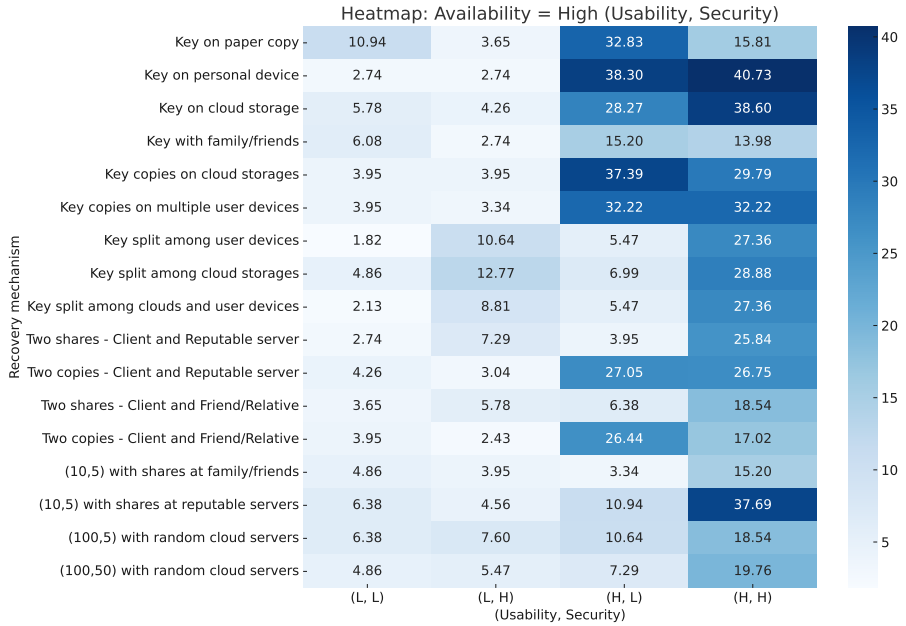

Figure 7: Heat map of participant percentages rating each recovery mechanism setting, with Availability = High (H). The concentration of the dark blues on the right indicates that the usability is considered High (H).

recovery settings. It shows that a majority of participants tend to rate usability and availability similarly indicating that participants may perceive these two dimensions as closely related in practice. This is despite the fact that all the considered participants answered the knowledge-test questions correctly and are indeed aware of the difference between usability and availability. This is significant for the following reason: the Web3 settings are essentially known to introduce availability as a dimension/parameter due to

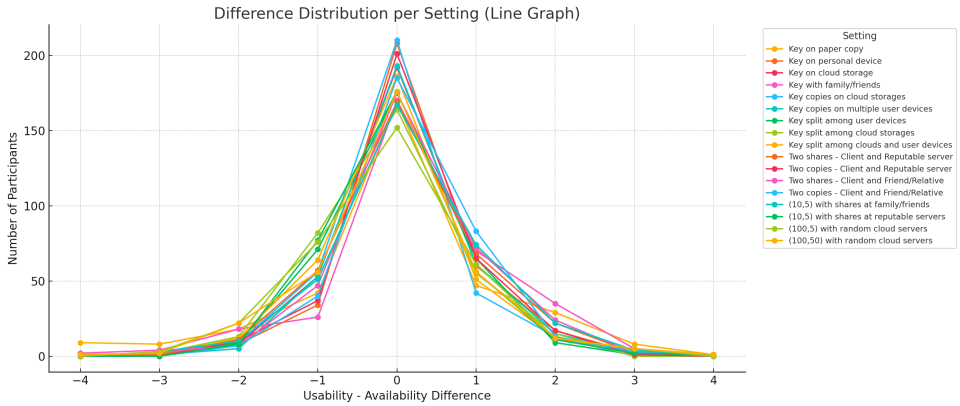

Figure 8: The difference of usability and availability ratings for different recovery settings

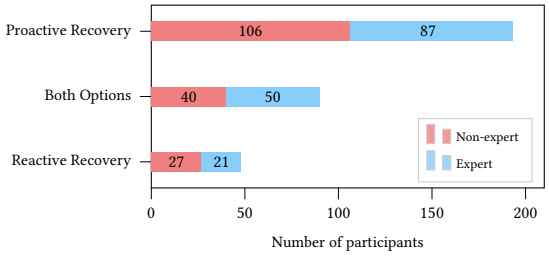

Figure 9: Preference among the Proactive and Reactive recovery mechanisms.

user-centric recovery and decentralization. However, users seem to perceive usability and availability similarly, which is evident from the strong correlation. This shows that even in Web3 settings, it may be sufficient to look at usability and security as in traditional systems.

5.4 RQ4 - What recovery mechanism configurations do the users prefer for different properties?

To answer this question, we look at each individual property and how users rate them for different wallet settings.

Preferred configurations for better usability. Figure 10 presents the counts of usability ratings $1-5$ by the participants. The rows of the figure are in decreasing order of the total values for ratings 4 and 5. Among the various recovery settings, participants prefer placing the keys on personal devices and keeping multiple copies on multiple user devices for better usability. The other top choices are to store the keys in cloud storage, to have multiple copies on different servers in the cloud, and to have multiple copies in cloud storage.

Among other threshold settings, having two copies and $(10, 5)$ setting with reputable servers are perceived as most usable options. However, having two shares with one at a relative or family individual followed by $(100, 50)$ setting with 100 randomly chosen cloud servers and $(10, 5)$ setting with shares at family or friends are among the settings considered least usable by the participants.

Preferred configurations for better security. Figure 11 shows the count of scores from participants for the settings of the recovery mechanism. Participants prefer to split the key among their personal devices, and split the key into two shares, with one share on the client and the other on a reputable server. They also consider splitting the key among few servers and their devices as more secure compared to the other remaining settings. Among the less favored settings for security, having the key at the family or friends is considered least secure, followed by having the key on a paper copy, and then having a share with friends or family while the other share is at the client. This indicates that the participants do not trust the family or friends with their keys and consider store the whole or a share of a key with them to be less secure.

Preferred configurations for better availability. For better availability, participants prefer to have the key on a personal device or cloud storage and copies on multiple cloud storage. These are following by having the private key on multiple user devices or a paper copy. Among the settings with least availability, $(10, 5)$ setting with shares at family or friends is perceived least available followed by having a share with a friend or family among two shares and $(100, 50)$ setting randomly selected cloud servers.

Preference among Proactive and Reactive recovery mechanisms. 58% of all the participants prefer proactive recovery. That amounts to 193 total participants with 87 Experts and 106 Non-experts. 27.1% of the total participants are okay with any recovery method. 14.5% of the participants prefer only reactive recovery mechanisms. See Figure 9 for participants' preference between proactive and reactive recovery and the split between experts and non-experts.

6 Discussion and further take-aways

Given our survey results in section 5, we discuss additional observations.

Settings which satisfy multiple properties. Few settings, like storing the key on personal devices or copying among multiple user

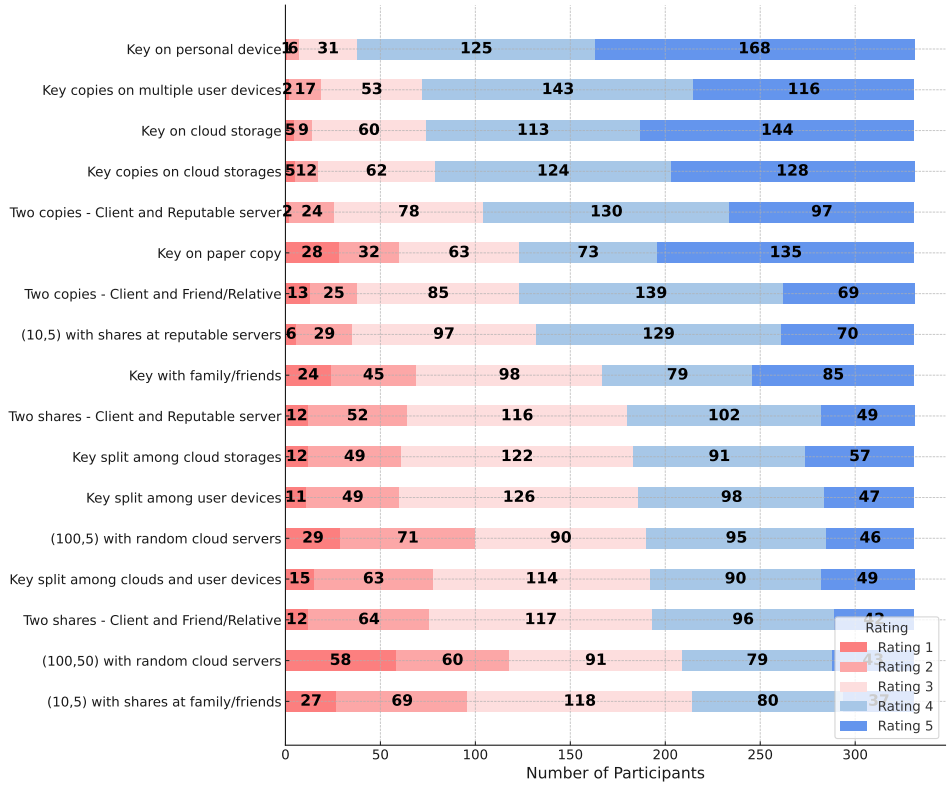

Figure 10: Usability rating of different recovery mechanisms. Left to right, the ratings are $1-5$. Shades of Red indicate Low (1-3) and shades of Blue indicate High (4-5). The choices are presented in decreasing order of total High ratings.

devices, show up among the top 5 settings on usability and availability. However, existing settings are not perceived as satisfying all three properties strongly as indicated by fig. 6, fig. 7. Few settings, like storing the key on personal devices or sharing the key information on a few reputable servers, seem to be considered by some participants to be meeting all three properties. It is important for the research community to develop settings that simultaneously strongly provide all three properties.

Users do not essentially trust family and friends. Participants rated strongly against recovery settings with the total or share of the key at family or friends on all properties. Among the three figures 10, 11, and 12, options with family or friends show up among the least favourable options for the participants. This indicates a lack of trust in friends and family; developers should be mindful of this fact and should offer other settings where the key is shared among different devices or the cloud.

Usability and Availability. The usability and availability ratings of different recovery methods correlate with each other. More often than not (see Fig. 8), these ratings are indeed similar. It shows that even for recovery methods in the Web3 setting, it may be sufficient to view only the security and usability dichotomy. Further study and analysis of other Web3 schemes and settings are needed to establish this fact.

Need for education. Some participants who have not lost the key or funds yet continue to believe that it is unlikely to lose funds in the future. This may not be true and the community should educate the users about the risks of poor choice of recovery settings and should encourage them to opt for settings involving multiple shares among different devices for security. There is also a need to educate the user base on how blockchain and Web3 accounts currently lack the safeguards of traditional asset management channels, which mainly is due to the decentralized nature of blockchain systems and the absence of a centralized authority which can revert or fix errors.

7 Conclusion

While account recovery is a well-established concept in the context of Web2, it presents unique challenges in the Web3 landscape. In Web3, accounts rely on a secure signing-verification key pair, which is not shared with a central entity with Web2 focus on security via decentralization. This distinction makes Web3 account recovery more complex. Fortunately, the Web3 community is experiencing increased interest and effort into recovery mechanisms to provide users confidence that their assets will be available even if they do not have the expertise on managing cryptographic keys.

This study investigates existing account recovery solutions from the user perspective in the blockchain realm. We shed light on the

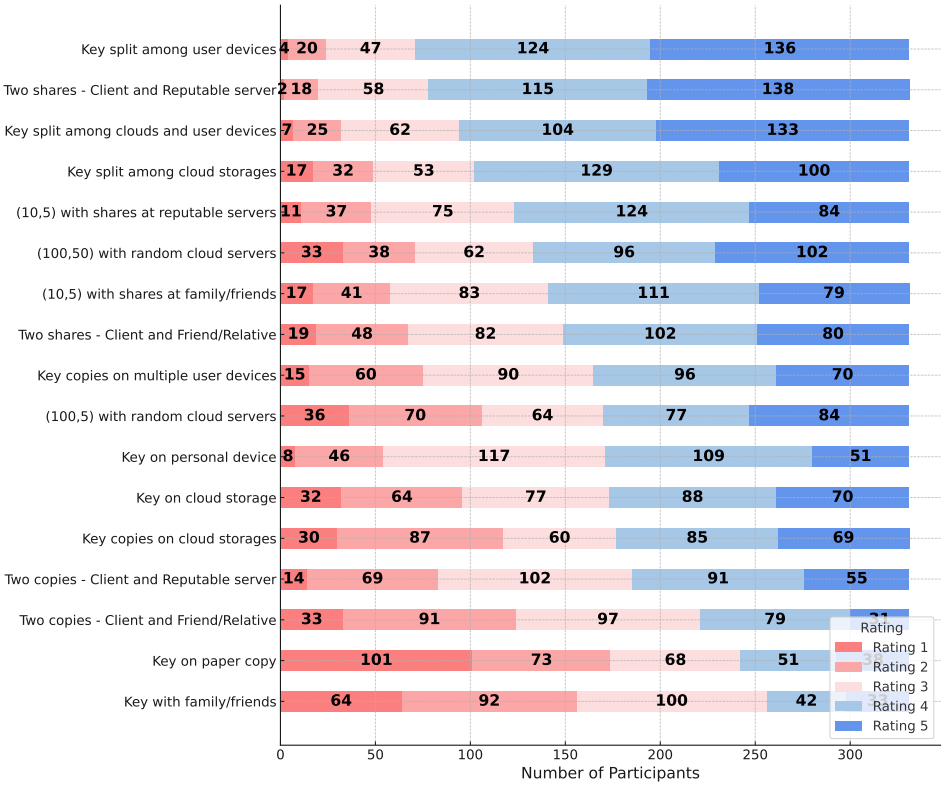

Figure 11: Security rating of different recovery mechanisms. Left to right, the ratings are $1-5$. Shades of Red indicate Low (1-3) and shades of Blue indicate High (4-5). The choices are presented in the increasing order of total Low ratings.

existing approaches regarding their usability, security, and availability that arise in Web3 recovery scenarios and the underlying factors that contribute to user perception. We envision our results as the driving factor in improving future wallet designs for greater blockchain and Web3 adoption.

References

[1] Argent vault security and recovery.
[2] Braavos.
[3] Educational attainment in the united states: 2020. https://www.census.gov/data/tables/2020/demo/educational-attainment/cps-detailed-tables.html.
[4] Eth community discuss dao for reversing funds lost to wrong addresses.
[5] How many bitcoin are lost? | ledger.
[6] Keyclub and randrec: Two new social key recovery schemes.
[7] A man who says he threw away a hard drive loaded with 7,500 bitcoins in 2013 is offering his city $70 million to dig it up from the dump.
[8] People are losing bitcoin cash by accidentally sending it to bitcoin addresses.
[9] Prolific participants. https://researcher-help.prolific.com/en/article/2bb2f4.
[10] Sequence wallet key management.
[11] Torus network documentation.
[12] Web3auth unified recovery management.
[13] What happens to cryptocurrency when you die?
[14] A new secure approach to backup cryptocurrency wallets. In *IEEE Global Communications Conference (GLOBECOM)* (2019).
[15] The u in crypto stands for usable: An empirical study of user experience with mobile cryptocurrency wallets. In *Proceedings of the ACM CHI Conference on Human Factors in Computing Systems* (2021).
[16] The aptos blockchain: Safe, scalable, and upgradeable web3 infrastructure, August 2022.
[17] Custodial vs. non-custodial wallets: Ux and recovery commentary. Technical report, 2022.
[18] An empirical study of a decentralized identity wallet: Usability, security, and user control. In *USENIX Symposium on Usable Privacy and Security (SOUPS)* (2022).
[19] Reminisce: Blockchain private key generation and recovery using user-generated information. *Mathematics* (2022).
[20] User perception of the specifics of cryptocurrency wallets. Master's thesis, University (MSc Thesis), 2022.
[21] Account abstraction: Surveys and analyses of eip-4337 and social recovery. arXiv preprint, 2023.
[22] Practical key recovery model for self-sovereign identity digital wallets. arXiv preprint, 2023.
[23] Smart contract-based social recovery wallet management scheme for digital assets. In *Proceedings of the ACM Symposium on Applied Computing (SAC)* (2023).
[24] Usability evaluation of ssi digital wallets. arXiv preprint, 2023.
[25] How cryptocurrency users choose and secure their wallets. In *Proceedings of the ACM CHI Conference on Human Factors in Computing Systems* (2024).
[26] I can't believe it's not custodial!: Usable trustless key management for crypto wallets. In *Proceedings of the ACM CHI Conference on Human Factors in Computing Systems* (2024).
[27] A practical recovery mechanism for blockchain hardware wallets. arXiv preprint, 2024.
[28] Recoverable decentralized wallet based on social service. *Journal of Engineering Science* (2024).
[29] Shared-custodial wallet for multi-party crypto-asset management (mpc-tss). *Future Internet* (2024).
[30] Of secrets and seedphrases: User behaviors and challenges in seed phrase management. In *Proceedings of the ACM CHI Conference on Human Factors in Computing Systems* (2025).
[31] Abramova, S., Voskobojnikov, A., Beznosov, K., and Böhme, R. Bits under the mattress: Understanding different risk perceptions and security behaviors of crypto-asset users. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (2021), pp. 1–19.
[32] Acar, Y., Fahl, S., et al. You've Got (a Reset) Mail: A Security Analysis of Email-Based Password Reset. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA)* (2021), Springer.

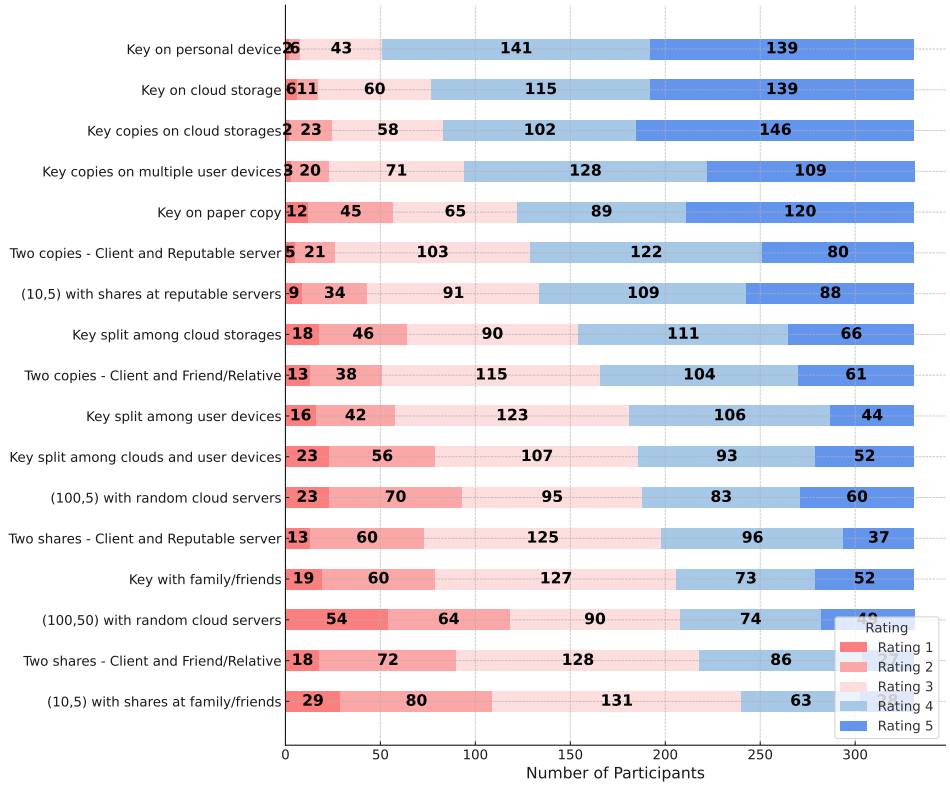

Figure 12: Availability rating of different recovery mechanisms. Left to right, the ratings are $1-5$. Shades of Red indicate Low (1-3) and shades of Blue indicate High (4-5). The choices are presented in the increasing order of total Low ratings.

[33] Albakry, S., Vaniea, K., and Wolters, M. K. What is this url's destination? empirical evaluation of users' url reading. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2020), CHI '20, Association for Computing Machinery, p. 1–12.

[34] Albayati, H., Kim, S. K., and Rho, J. J. A study on the use of cryptocurrency wallets from a user experience perspective. *Human behavior and emerging technologies 3*, 5 (2021), 720–738.

[35] Amsden, Z., Arora, R., Bano, S., Baudet, M., Blackshear, S., Bothra, A., Cabrera, G., Catalini, C., Chalkias, K., Cheng, E., Ching, A., Chursin, A., Danezis, G., Giacomo, G. D., Dill, D. L., Ding, H., Doudchenko, N., Gao, V., Gao, Z., Garillot, F., Gorven, M., Hayes, P., Hou, J. M., Hu, Y., Hurley, K., Lewi, K., Li, C., Li, Z., Malkhi, D., Margulis, S., Maurer, B., Mohassel, P., de Naurois, L., Nikolaenko, V., Nowacki, T., Orlov, O., Perelman, D., Pott, A., Proctor, B., Qadeer, S., Rain, Russi, D., Schwab, B., Sezer, S., Sonnino, A., Venter, H., Wei, L., Wernerfelt, N., Williams, B., Wu, Q., Yan, X., Zakian, T., and Zhou, R. The libra blockchain, 2020. https://diem-developers-components.netlify.app/papers/the-diem-blockchain/2020-05-26.pdf.

[36] Arora, S. S., Badrinarayanan, S., Raghuraman, S., Shirvanian, M., Wagner, K., and Watson, G. Avoiding lock outs: Proactive FIDO account recovery using managerless group signatures. Cryptology ePrint Archive, Report 2022/1555, 2022.

[37] Biddle, R., Chiasson, S., and Van Oorschot, P. C. Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys (CSUR) 44*, 4 (2012), 1–41.

[38] Blackshear, S., Chalkias, K., Chatzigiannis, P., Faizullabhoy, R., Khaburzaniya, I., Kokoris-Kogias, E., Lind, J., Wong, D., and Zakian, T. Reactive key-loss protection in blockchains. In *FC 2021 Workshops* (Mar. 2021), M. Bernhard, A. Bracciali, L. Gudgeon, T. Haines, A. Klages-Mundt, S. Matsuo, D. Perez, M. Sala, and S. Werner, Eds., vol. 12676 of *LNCS*, Springer, Berlin, Heidelberg, pp. 431–450.

[39] Boldyreva, A. Threshold signatures, multisignatures and blind signatures based on the gap-diffie-hellman-group signature scheme. In *International Workshop on Public Key Cryptography* (2002), Springer, pp. 31–46.

[40] Buterin, V., and Van de Sande, A. EIP-55: Mixed-case checksum address encoding, 2016. https://eips.ethereum.org/EIPS/eip-55.

[41] Buterin, V., Weiss, Y., Tirosh, D., Nacson, S., Forshtat, A., Gazso, K., and Hess, T. Erc-4337: Account abstraction using alt mempool, 2021.

[42] Chalkias, K. Soft privacy-related leak in some threshold eddsa wallets, 2023.

[43] Chatzigiannis, P., Chalkias, K., Kate, A., Mangipudi, E. V., Minaei, M., and Mondal, M. SoK: Web3 recovery mechanisms. Cryptology ePrint Archive, Report 2023/1575, 2023.

[44] Chatzigiannis, P., Wang, K. C., Arora, S., and Minaei, M. A Composability Analysis Framework for Web3 Wallet Recovery Mechanisms . In *2025 IEEE Symposium on Security and Privacy (SP)* (Los Alamitos, CA, USA, May 2025), IEEE Computer Society, pp. 1531–1546.

[45] Duggan, G. B., Johnson, H., and Grawemeyer, B. Rational security: Modelling everyday password use. *International journal of human-computer studies 70*, 6 (2012), 415–431.

[46] Felt, A. P., Consolvo, S., Chin, E., Wagner, D., and Egelman, S. I'll accept the risk: Understanding user decision-making in smartphone security warnings. In *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS)* (2012), USENIX Association.

[47] Foundation, S. D. Sep-30: Recoverable wallets. https://stellar.org/protocol/sep-30, 2020.

[48] Frohlich, M., Gutjahr, F., and Alt, F. Don't lose your coin! investigating security practices of cryptocurrency users. In *Proceedings of the 2020 ACM Designing Interactive Systems Conference* (New York, NY, USA, 2020), DIS '20, Association for Computing Machinery, p. 1751–1763.

[49] Garfinkel, S., and Lipford, H. R. *Usable security: History, themes, and challenges*. Morgan & Claypool Publishers, 2014.

[50] Gaw, S., and Felten, E. W. Password management strategies for online accounts. In *Proceedings of the second symposium on Usable privacy and security* (2006), pp. 44–55.

[51] Golla, M., et al. Lost in Translation: A Study of Recovery Codes and Their Misuse. In *USENIX Security Symposium* (2024).

[52] Harn, L. Group-oriented (t, n) threshold digital signature scheme and digital multisignature. *IEE Proceedings-Computers and Digital Techniques 141*, 5 (1994),

307–313.
[53] Hevia, A., et al. I Can't Believe It's Not Custodial!: Usable Trustless Account Recovery. In *USEC Adjunct Proceedings* (2024).
[54] Hitlin, P. Turkers in this canvassing: young, well-educated and frequent users. In *Research in the Crowdsourcing Age, a Case Study* (2016).
[55] Krombholz, K., Judmayer, A., Gusenbauer, M., and Weippl, E. The other side of the coin: User experiences with bitcoin security and privacy. In *International conference on financial cryptography and data security* (2016), Springer, pp. 555–580.
[56] Lewis, J. R., Utesch, B. S., and Maher, D. E. Umux-lite: when there's no time for the sus. In *Proceedings of the SIGCHI conference on human factors in computing systems* (2013), pp. 2099–2102.
[57] Lewis, J. R., Utesch, B. S., and Maher, D. E. Investigating the correspondence between umux-lite and sus scores. In *Design, User Experience, and Usability: Design Discourse* (2015), A. Marcus, Ed., pp. 204–211.
[58] Lindell, Y. Cryptography and mpc in the coinbase prime web3 wallet, 2023.
[59] Makriyannis, N., and Yomtov, O. Practical key-extraction attacks in leading mpc wallets. Cryptology ePrint Archive, Paper 2023/1234, 2023. https://eprint.iacr.org/2023/1234.
[60] Mangipudi, E. V., Desai, U., Minaei, M., Mondal, M., and Kate, A. Uncovering impact of mental models towards adoption of multi-device crypto-wallets. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (New York, NY, USA, 2023), CCS '23, Association for Computing Machinery, p. 3153–3167.
[61] Mangipudi, E. V., Desai, U., Minaei, M., Mondal, M., and Kate, A. Uncovering impact of mental models towards adoption of multi-device crypto-wallets. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (New York, NY, USA, 2023), CCS '23, Association for Computing Machinery, p. 3153–3167.
[62] Minaei, M., Mondal, M., and Kate, A. Empirical understanding of deletion privacy: Experiences, expectations, and measures. In *31st USENIX Security Symposium (USENIX Security 22)* (Boston, MA, Aug. 2022), USENIX Association, pp. 3415–3432.
[63] Nakatsuka, Y., et al. SoK: Web Authentication in the Age of End-to-End Encryption. In *IEEE Symposium on Security and Privacy* (2024).
[64] NIST. A Security Perspective on the Web3 Paradigm. Nist internal report, National Institute of Standards and Technology, 2025.
[65] Redmiles, E. M., Kross, S., and Mazurek, M. L. How well do my results generalize? comparing security and privacy survey results from mturk, web, and telephone samples. In *2019 IEEE Symposium on Security and Privacy (SP)* (2019), pp. 1326–1343.
[66] Schmidt, R., Mota, M., Buterin, V., and naxe. Ethereum EIP2492 - secret multisig recovery, 2019.
[67] Schreiner, F., et al. Usability Evaluation of Self-Sovereign Identity Digital Wallets. *Information Systems Frontiers* (2023).
[68] Shoup, V. Practical threshold signatures. In *Advances in Cryptology—EUROCRYPT 2000: International Conference on the Theory and Application of Cryptographic Techniques Bruges, Belgium, May 14–18, 2000 Proceedings 19* (2000), Springer, pp. 207–220.
[69] Suarez-Garcia, A., Alvarez-Hernandez, M., Arce, E., and Ribas, J. R. Exploring the efficacy of binary surveys versus likert scales in assessing student perspectives using bayesian analysis. *Applied Sciences 14*, 10 (2024), 4189.
[70] Swambo, J., and Poinsot, A. Risk framework for bitcoin custody operation with the revault protocol. In *Financial Cryptography and Data Security. FC 2021 International Workshops* (Berlin, Heidelberg, 2021), M. Bernhard, A. Bracciali, L. Gudgeon, T. Haines, A. Klages-Mundt, S. Matsuo, D. Perez, M. Sala, and S. Werner, Eds., Springer Berlin Heidelberg, pp. 3–20.
[71] Toth, P., et al. Empirical Study of a Decentralized Identity Wallet. In *Symposium on Usable Privacy and Security (SOUPS)* (2022).
[72] Voskobojnikov, A., Obada-Obieh, B., Huang, Y., and Beznosov, K. Surviving the cryptojungle: Perception and management of risk among north american cryptocurrency (non) users. In *International conference on financial cryptography and data security* (2020), Springer, pp. 595–614.
[73] Voskobojnikov, A., Wiese, O., Mehrabi Koushki, M., Roth, V., and Beznosov, K. The u in crypto stands for usable: An empirical study of user experience with mobile cryptocurrency wallets. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (2021), pp. 1–14.

A Screening Survey Instrument

Thank you for joining the survey. In this survey, we aim to understand your usage and preferences for different cryptocurrency wallets. This is an anonymous survey and no personally identifiable information (PII) is collected. We cannot link this information to any of your accounts/identities/wallets.

Q1: How long have you been using a crypto wallet (Eg: Electrum, Coinbase, etc)?
◯ Less than a year ◯ 1-3 years ◯ 3-5 years ◯ More than 5 years ◯ I have never used a crypto wallet

Q2: How frequently do you perform cryptocurrency transactions?
◯ At least once every day ◯ At least once every week ◯ At least once every month ◯ At least once every year

Q3: Approximately how many transactions have you performed in the last one year?
Mark on a Likert scale of 0 - 100

Q4: Add the crypto currency wallet(s) which you use most often.
(a) Wallet 1 ☐
(b) Wallet 2 ☐
(c) Wallet 3 ☐

Q5: Will you be interested in participating in a longer (20 minutes) survey on recovery mechanisms of cryptocurrency wallets? It tries to understand your preferences regarding usage and security models in recovery settings in the wallets. You will be compensated appropriately.
◯ Yes ◯ No

B Survey Instrument

Thank you for joining the survey. In this survey, we aim to understand your usage and preferences for different cryptocurrency wallets. Specifically, we will ask you few questions regarding your use of cryptocurrency wallets as well as your preference regarding different types of cryptocurrency wallets that are in-use today (even if you don't use them). We will also enquire about your desired preferences regarding some specific (hypothetical) cryptocurrency wallet settings. Our aim for these desired preference questions will be to understand which of the presented specific wallet settings do you find acceptable.

B.1 General Usage

In this section, we ask you about usage characteristics and factors that helped you in your choice of the cryptocurrency wallets. Note that, throughout this survey, the terms 'wallet' and 'crypto wallet', would mean a cryptocurrency wallet.

Q1: How long have you been using a crypto wallet (Eg: Electrum, Coinbase etc)?
◯ Less than a year ◯ 1-3 years ◯ 3-5 years ◯ More than 5 years ◯ I have never used a crypto wallet
If 'I have never used a crypto wallet' is selected then skip to the end of survey.

Q2: For what purpose do you use crypto wallets? Multiple options are allowed.
☐ Long-term investment ☐ Trading ☐ Collectibles (Eg:NFT)
☐ As an alternative to fiat/government-issued currency for regular transactions
☐ Other ☐

Q3: What approximate percentage of your savings do you hold in crypto wallets?
(Slide bar from 0-100)

Q4: Which wallet(s) do you use most often? Multiple options are allowed. You can add below if your wallet is not listed.

Table 5: Experts - Percentage of the participants choosing L - Low or H - High for each of the three properties - (Usability, Security, Availability) for the key storage settings

Recovery setting	(L, L, L)	(L, L, H)	(L, H, L)	(L, H, H)	(H, L, L)	(H, L, H)	(H, H, L)	(H, H, H)
Key on paper copy	20.51	13.46	4.49	4.49	12.18	26.92	1.92	16.03
Key on personal device	3.85	3.85	0.64	3.21	5.13	31.41	5.13	46.79
Key at cloud service	6.41	5.13	1.28	5.77	7.69	24.36	4.49	44.87
Key at Family/Friends	37.18	7.69	2.56	4.49	14.74	17.31	0.64	15.38
Key copies on cloud storages	8.33	3.21	7.05	4.49	1.28	33.33	5.13	37.18
Key copies on multiple user devices	7.05	3.21	10.26	3.21	4.49	26.92	5.13	39.74
Key split among user devices	7.69	2.56	27.56	13.46	3.85	6.41	4.49	33.97
Key split among cloud storages	12.18	5.13	17.31	13.46	1.92	6.41	4.49	39.10
Key split between clouds and user devices	16.03	3.85	19.87	8.33	1.92	6.41	6.41	37.18
Two shares - Client and Reputable server	11.54	0.64	28.21	8.33	5.77	4.49	10.90	30.13
Two copies - Client and Reputable server	13.46	3.85	7.05	2.56	3.85	28.85	9.62	30.77
Two shares - Client and Friend/Relative	21.79	5.77	18.59	5.77	7.05	8.33	9.62	23.08
Two copies - Client and Friend/Relative	19.87	3.85	8.97	3.85	10.90	28.85	6.41	17.31

☐ Coinbase ☐ Binance ☐ Electrum ☐ Ledger ☐ Trezor ☐ Metamask ☐ Exodus ☐ ZenGo ☐ Mycelium ☐ Bitso ☐ Luno ☐ Crypto.com ☐ Trust ☐ Other-1 ☐ ☐ Other-2 ☐ ☐ Other-3 ☐

Q5: Why did you choose the wallet you use? Multiple options are allowed.
☐ Security guarantees- I believe my funds will be safe with the wallet ☐ The interface is easy to use ☐ It allows transactions in multiple currencies ☐ Support from developers ☐ Ease of storing keys ☐ Ease to recover the keys ☐ It is popular ☐ Other ☐

Q6: Did you choose your wallet solely based on ratings or reviews of the wallet from a crowd sourced platform like Play Store / AppStore / Reddit etc?
◯ Yes ◯ No but it is important ◯ No it is not important

Q7: Crypto wallets are typically associated with a "secret key" which allows customers to securely access funds. However, some wallets may just involve a password to access the wallet interface and funds. Did you ever lose the secret key or password of your wallet?
◯ Yes ◯ No
If 'No' is selected skip to Q13.

Q8: Which one(s) did you lose?
☐ Secret Key ☐ Password to the the interface

Q9: Could you recover the key/password of the wallet?
◯ No. I lost the funds. ◯ I recovered the key/password using the procedure advised by the wallet ◯ I recovered the key/password from my personal backup ◯ I recovered using other procedure (explain the procedure below) ☐

Q10: How likely do you think it is that you might lose access to your wallet funds in the future? Rate on a scale of 1 (very unlikely) - 5 (highly likely)

Q11: Based on your perception, what might be the reason(s) for losing your wallet funds in the future (choose all the options that apply)
☐ Loss of the secret key or password. (The access to the funds is lost)
☐ A malicious entity/person stealing the funds
☐ Others ☐

Q12: Have you heard of anyone who lost funds from or access to their wallet?
◯ Yes, I know someone personally ◯ Yes, I heard from media platforms (including social media, internet articles, newspapers)
◯ No, I am not aware of anyone

Q13: **Ranking Question** Please rate each wallet security concern on a scale from 1 to 5 (1 = lowest concern, 5 = highest concern), ranking them from most concerning to least concerning. (Note: "server" refers to any remote server owned by a wallet company where the secret key is stored.)
◯ Loss of secret key by the user
◯ Compromise of the server and there by-the secret key being hosted by the server
◯ Compromise of the secret key "by" the server or firm hosting the key
◯ Compromise of user device like phone by an adversary
◯ Lack of proper recovery mechanism by wallet providers
◯ Others (Please describe in the text box below) ☐

Q14: Choose the current month of the year.
◯ August ◯ January ◯ February ◯ September ◯ None of the above

B.2 Section 2 - Preference for different types of recovery mechanisms

In this survey, a 'recovery mechanism' indicates the setup and the execution of key recovery of a cryptocurrency wallet.

PLEASE WATCH THE SHORT VIDEO CAREFULLY.

Questions in the next two sections depend on the points discussed in them.

Note that, for this survey a "key" implies the secret key associated with the wallet. By 'shares' of the key, we mean cryptographically generated random shares of the key.

Before we proceed further, we provide the definitions here again:

Usability A recovery mechanism is usable if it is easy to learn and memorize how to perform a task efficiently and without errors. It should also be pleasant to use.

Security Only the legitimate user should be able to access the funds. Security measures how difficult it is for the attacker to access the funds or recover the keys.

Availability It measures if and how soon a legitimate user can recover funds after starting the recovery process.

In this survey, "external server" means a non-cloud server that might be owned by a friend or relative. A "guardian account" is an account that can securely receive funds if your own account is ever compromised.

Q1: Please choose if the following statements are True or False.
Usability of a recovery mechanism deals with how often you can use the mechanism. ◯
Availability of a recovery mechanism is about if and how soon the users can access their funds after starting the recovery process. ◯
Security of a recovery mechanism is about how easy it is to learn and memorize how to perform the wallet setup and recovery. ◯

Q2: **Recovery Mechanism** Imagine you've lost the secret key to your wallet. Which recovery method would you choose? Note- A "guardian account" is an account that can securely receive funds if your own account is ever compromised.
- (a) Single Private Backup - Recover your key from one secure backup (e.g., a hard disk, USB drive, or paper document).
- (b) Multiple Personal Devices - Reconstruct your key by combining partial backups stored in multiple secure locations you control (e.g., personal servers or devices).
- (c) Single Trusted Contact - Retrieve the key from one trusted friend or family member who holds it.
- (d) Multiple External Servers - Reconstruct your key from pieces stored on separate external servers (cloud servers)
- (e) Single Guardian Account - Transfer all funds to one guardian account.
- (f) Multiple Guardian Accounts - Distribute your funds among multiple guardian accounts.
- (g) Other - Suggest any other recovery approach not listed above. ☐

Q3: Now we shall ask you about how you may rate each of the different wallet recovery options. Single-Device Key Backup: Imagine you have a wallet with its key stored in only one location. Below are various ways to back up this key. Please rate each method on usability, security, and availability using the following 1–5 scale: 1 = Totally unusable, completely insecure, or entirely inaccessible, 5 = Highly usable, very secure, and readily accessible.
- (a) Paper copy
- (b) Personal device like Phone/Laptop/USB stick
- (c) Cloud service
- (d) Friend/Family member

Q4: Multi device key backup: A key can be copied across multiple locations or split among several devices to protect against loss. Below are different ways you might arrange multi-device backups. Please rate each method on usability, security, and availability using the following 1–5 scale: 1 = Totally unusable, completely insecure, or entirely inaccessible, 5 = Highly usable, very secure, and readily accessible.
- (a) Entire key copied to multiple cloud storages (e.g., Google Drive, Dropbox)
- (b) Entire key copied across multiple devices owned by the same user (e.g., USB, laptop)
- (c) Key split (not copied) among multiple personal devices
- (d) Key split (not copied) among multiple cloud storages
- (e) Key split (not copied) between cloud storage(s) and user device(s).

Q5: Two-Party Key Backup: Below are different ways you can split or share your wallet key between two parties (for instance, an external server and yourself, or a friend/relative and yourself). Each approach has its own implications for usability, security,and availability. Please rate each method on usability, security, and availability using the following 1–5 scale: 1 = Totally unusable, completely insecure, or entirely inaccessible, 5 = Highly usable, very secure, and readily accessible.
- (a) One share each on a reputable server and at the client (two total shares). Both the client and the server must come together to recover the key.
- (b) Key present both at the client and a reputable server (full copies in each location). Either the client or the server can recover the key.
- (c) One share each with a friend/relative and at the client (two total shares). Both the client and the friend/relative are required to recover the key.
- (d) Key present both at the client and a friend/relative (full copies in each location). Either the client or the friend/relative can recover the key.

Q6: **Key Setup Configurations** Consider a recovery mechanism through multiple key shares/parts at multiple personal or external devices. When using multiple key shares across multiple devices, the notation (N, T) indicates a threshold scheme where: N = Total number of shares. T = The minimum number of shares needed to reconstruct the key. For example, in a (5,3) setup, any 3 of the 5 share holders must come together to recover the wallet. Please rate each method on usability, security, and availability using the following 1–5 scale: 1 = Totally unusable, completely insecure, or entirely inaccessible, 5 = Highly usable, very secure, and readily accessible.
- (a) $(10, 5)$ with key-parts atfriends/family members
- (b) $(10, 5)$ with all shares at reputable servers (Eg: Google cloud, iCloud)
- (c) $(100, 5)$ with all servers chosen from a random pool of online cloud servers
- (d) $(100, 50)$ with all servers chosen from a random pool of online cloud servers

Q7: Below is a list of recovery mechanisms. Please rate each feature on a scale from 1 (Not important) to 5 (Very important), based on your own perception and usage needs .
- (a) Single key recovery - Key is backed up on a single device

(b) Multi key recovery - Key is shared among multiple devices
(c) Multi-key with controlling custody - Key shared among multiple parties when the majority of shares with the user
(d) Recovery through Friends/Family members
(e) Others ☐

Q8: We characterize recovery mechanisms in to two types -Proactive and Reactive, depending on the setup involved etc. Given a choice, which one you pick for your secret key recovery based on the features of each recovery mechanism listed below the choices.
(a) Reactive Recovery Recovery steps are taken only after the key is lost or compromised. The original public key cannot be used anymore to receive funds. The recovery of funds will take longer. Only smart contract accounts can use this recovery method.
(b) Proactive Recovery Recovery measures are set up in advance. After recovery the original public key can be used anymore to receive funds. Ensures faster access to funds. It can be used by all types of accounts.
(c) Both Options
(d) Others ☐

B.3 Demographics

In these final set of questions, we will ask you about your demographic details.

Q1: What is your age in years?
◯ Under 18 ◯ 18-24 ◯ 25-34 ◯ 35-44 ◯ 45-54 ◯ 55-64 ◯ 65 or older ◯ Prefer not to answer

Q2: Which gender do you identify with ?
◯ Male ◯ Female ◯ Others ◯ Prefer not to answer

Q3: What is the highest level of education you have completed?
◯ High school ◯ College degree ◯ Bachelor's degree ◯ Master's degree ◯ Doctorate ◯ Prefer not to answer

Q4: Which of the following best describes your employment status?
◯ Full-time employment ◯ Part-time employment ◯ Unemployed ◯ Full time uncompensated (Eg: Homemaker, volunteer) ◯ Student ◯ Retired ◯ Other ◯ Prefer not to answer

Q5: Do you currently have a job (or previously worked) in computer science, information technology or some other technical field? Or, if you are a student, do you study one of these topics in your degree program?
◯ Yes ◯ No ◯ Prefer not to answer

Q6: Choose the category that you most identify with regarding usage of crypto wallets?
◯ I use them solely for the interest in technology ◯ I use them primarily as an avenue for trade and investment cryptocurrencies ◯ I am a newbie, started using them for the fear of missing out

Q7: Kindly choose how far do you agree with the statement below. 1-Fully Disagree, 5-Fully Agree: "I understand the underlying cryptography/math related to performing transactions using my wallets."