Uncovering Impact of Mental Models towards Adoption of Multi-device Crypto-Wallets

Easwar Vivek Mangipudi
Purdue University
emangipu@purdue.edu

Udit Desai
IIT Kharagpur
uditdesai2206@iitkgp.ac.in

Mohsen Minaei
Visa Research
mominaei@visa.com

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

Aniket Kate
Purdue University
aniket@purdue.edu

ABSTRACT

The ever-increasing cohort of cryptocurrency users saw a sharp increase in different types of crypto-wallets in the past decade. However, different wallets are non-uniformly adopted in the population today; Specifically, emerging multi-device wallets, even with improved security and availability guarantees over their counterparts, are yet to receive proportionate attention and adoption.

This work presents a data-driven investigation into the perceptions of cryptocurrency users towards multi-device wallets today, using a survey of 255 crypto-wallet users. Our results revealed two significant groups within our participants—Newbies and Non-newbies. These two groups statistically significantly differ in their usage of crypto-wallets. However, both of these groups were concerned with the possibility of their keys getting compromised and yet are unfamiliar with the guarantees offered by multi-device wallets. After educating the participants about the more secure multi-device wallets, around 70% of the participants preferred them; However, almost one-third participants were still not comfortable using them. Our qualitative analysis revealed a gap between the actual security guarantees and mental model for these participants—they were afraid that using multi-device wallets will result in losing control over keys (and in effect funds) due to distribution of key shares. We also investigated the preferred default settings for crypto-wallets across our participants, since multi-device wallets allow a wide range of key-share distribution settings. In the distributed server settings of the multi-device wallets, the participants preferred a smaller number of reputed servers (as opposed to a large non-reputed pool). Moreover, considerations about threat model further affected their preferences, signifying a need for contextualizing default settings. We conclude the discussion by identifying concrete, actionable design avenues for future multi-device wallet developers to improve adoption.

1 INTRODUCTION

The cryptocurrency boom has seen millions of people adopting digital assets; the recent economic successes [23, 25, 28] have enthused a broad population to explore them. The diversity in the needs and objectives of these cryptocurrency users is vast, ranging from just being enthused by technology to trading, sometimes even using all of their savings. With increasing adoption and valuation, the attacks on the system have also seen a rise. To combat these attacks, designers constantly improve the security models with different architectures and user preferences in mind. However, the number of users of each popular cryptocurrency wallet (or crypto-wallet) such as Coinbase [3, 4] and Binance [1, 2] indicates higher popularity of wallets that seem (cryptographically) weaker in the security model they offer. This popularity can be because of various reasons, including people trusting the wallet firms, opting for wallets based on popular opinions and different security attitudes, etc. These variations in knowledge, understanding of security models and risk perception may also significantly affect the choice of wallets.

Recent studies [48, 49, 54, 62, 80] attempted to understand usability and challenges while performing transactions with crypto-wallets in-use. They analyze the wallets using cognitive walkthrough [45] and also study the common misconceptions by the users regarding role of wallet firm [80].

The focus of most of these previous works has been to characterize the *usability* and understanding of the in-use traditional single-device wallets. However, so far, there have been no studies regarding the emerging (and arguably more secure [46]) *multi-device wallets* that analyze the users' mental model of the security and key management of multi-device wallets with a goal to understand barriers towards their adoption. To put simply, a single-device wallet is a wallet with secret information (a secret key) stored in a single location. In contrast, in a multi-device wallet, the secret information is divided and stored on multiple devices, including servers hosted by the wallet firm and the user's devices. Owing to the increasing risks of key-compromise attacks [32, 78] and exchange hacks [7, 21, 24] on single-device wallets, one may expect a greater enthusiasm for the new and emerging multi-device wallets (e.g., Torus wallet [12], ZenGo [14]) which significantly mitigates these issues. However, in terms of adoption, multi-device wallets lag far behind their single-device counterparts. This raises an important unanswered question: Is there an inherent gap between users' security expectations and the guarantees provided by current multi-device solutions, or are the multi device wallets just ahead of their time? In this work, we seek an answer to this question.

Specifically, in this work, we attempt to understand the user's perception towards multi-device wallets and qualify the gap between their designed security models of key management and the users' mental model. We consider distributed cryptography [9, 41] and its usability along with user preferences in wallets. Specifically, we conducted a survey-based study of 255 participants; analyzed their responses qualitatively and quantitatively to understand their current usage, choices, and if they are willing to change them given certain minimum information. Primarily, we investigate three research questions (**RQ**s):

RQ1: *What are the current usage-based groups, their preferences of wallets, and on what factors are they based?*

We investigated this question by asking the participant detailed questions on their current cryptocurrency wallets, their usage, along the features that made them choose a particular wallet. We enquire if their choice has been affected by ratings and reviews of the existing wallets. We also investigate their familiarity with different wallet types, including single and multi-device wallets, and their security concerns. Based on usage and preference responses, we analyze that all the participants behave as two groups: Newbies and Non-newbies. The newbies are recent users, while the non-newbies are relatively experienced users who have been using the wallets longer and invest more savings. The majority of participants use single-device wallets; however, more than 75% of the participants are concerned about losing funds by losing the key at the client device or compromising the secret key at the servers. At this point in the survey, both the groups are not very familiar with multi-device wallets.

RQ2: *Provided essential and sufficient information, are the users willing to shift to multi-device wallets? If not, why not?*

We investigated this question by first providing the users with essential knowledge regarding both single-device and multi-device wallets and then collecting feedback on the preferences. In particular, we asked the participants to watch two short videos on single and multi-device wallets. These videos explain the single-device wallets, their challenges, and how multi-device wallets mitigate them. After the videos and knowledge-check, we collected the preferences and feedback if the participants were willing to adopt multi-device wallets. 71.9% of participants mentioned they are ready to shift to multi-device wallets; however, 20.8% of the participants wanted to stick to single-device wallets.

RQ3: *What default key-management and architectural settings do they prefer for different wallets?*

We investigated this question by taking feedback for single and multi-device wallets on the secret information (key) location preferences under different possible attacks. We also took feedback regarding the choice of key storage of wallets under various government characteristics where the wallet firm may host servers in locations governed by multiple laws. We find that these government characteristics significantly impact the participants' key-location preferences from the survey. We also analyze how the participants prefer different settings, including the number of servers of the wallet firm storing the user keys. 63.13% of the participants preferred a small number of reputed servers compared to 31.76% choosing a higher number of servers. We provide a principled analysis of users' preferences by obtaining insights into why the users would or would not select multi-device wallets.

We observe that our results offer a few interesting insights and novel research directions for the threshold/distributed cryptography research itself. In the study, the participants expressed a desire for more control over their keys even when using multi-device wallets, the research community can focus on models achieving the same. The researchers should also consider more general adversary and access structures for multi-device wallets; however, the current distributed cryptographic literature and practice are pretty thin beyond the standard $(T-1)$-out-of-N adversary. The participants also identified a privacy-accountability trade-off between existing types of multi-device wallets, which presents an exciting challenge for the distributed cryptography community.

2 CLASSIFYING CRYPTOCURRENCY WALLETS

All cryptocurrency wallets today use paired secret keys and public keys [33, 56], where a wallet's address is derived from its public key. However, storing and accessing a secret key is a non-trivial problem and varies from one class of wallet to another. In this section, first, we briefly summarize the existing classification of wallets and identify that they often ignore the underlying security model of wallets. Then we present a new classification to address this issue.

Existing classifications of the cryptocurrency wallets. Several classes [22, 26, 40] of cryptocurrency wallets exist today depending on different dimensions—*hot and cold* wallets, *custodial and non-custodial* wallets [26, 48] etc. Hot wallets are connected to the internet while cold wallets are not. To perform a transaction with the cold wallet, the secret key needs to be taken from the offline storage like paper or QR code and employed. In another classification, a *non-custodial wallet* refers to a simple model of wallets where the secret key resides at user device. These wallers are notorious for loss or misplacement of keys and subsequent loss of funds—∼20% of all mined bitcoin lost this way [6]. In contrast, *custodial wallets* refer to ones where the secret key is not of the user (device) but at the firm which is offering the wallet. Every time the user makes a transaction, they authenticate to the firm which performs the transaction on their behalf. While this safeguards against the loss of key at the user, it forces the user to trust the firm operating the wallet. A popular way to achieve custodial wallet mechanism is to place the keys at the cryptocurrency exchanges that offer wallets and transact on behalf of the users. This approach is susceptible to attacks by hackers on exchanges and affects very large user bases [7, 16–18, 21, 24, 61]. Thus, it is quite evident that storing the keys at a single location is a security risk, irrespective at the user (client-side) or the firm (server-side).

A relatively new type of wallets solve these issues—it distributes the secret keys into multiple shares [9, 77] and places them at different locations. Depending on the specific application and scenario, these locations can be a combination of different firms/servers, devices owned by a single or multiple users.

Need for new security-focused classification. Note that the existing classifications of wallets presented so far focus far more on how the wallet is *used* rather than the underlying nuanced security models (e.g., how the security of the keys is guaranteed). While Hot-Cold classification focuses on wallets' connection to the internet, Custodial-Non custodial notion classifies the wallets as whether the key is only with the user or the remote server. However, in all cases, irrespective of if the key is placed at the user or the server or connected to the internet, compromising the single key location compromises the funds; the multi-device wallets mitigate this security risk [46]. Understanding this risk by explicitly stating the security model is essential. If the users appreciate the underlying security model, they can make informed choices about their wallets.

Hence, to investigate the user risk perception and mental model regarding the security of different wallets which is invariably related to the key location, we classify all the wallets into *single-device* and *multi-device* wallets with the key being stored at a single location or distributed among multiple locations.

2.1 Classification into Single-device and Multi-device wallets

Single-device wallets store the keys at a single location; the location can be a client device or a remote server hosting the data of the firm offering the wallet. If the user loses access to the device, they can not access any funds associated with the account. The different well-known single-device wallet types, including paper, desktop/mobile, hardware, and exchange wallets, are presented in Appendix A. These wallets provide control of the key to a single entity – the user or the wallet firm. In a multi-device wallet, the secret information is placed on multiple locations/devices; any subset of a particular size or higher of the devices should respond to authorize the transaction. These devices are held by one or more entities, including users and remote servers of the firm.

Single-device and multi-device wallets - Security. In a single-device wallet, since the key is in a single location , it introduces a single point of failure for the loss of the key. Loss of keys by the users and exchange hacks [6, 7, 16–18, 21, 24, 61] show that the single-device wallets are highly vulnerable to loss or compromise from an adversary. In an multi-device wallets, as key material is distributed among multiple locations, loss or compromise of a single device does not lead to loss of key; the attackers need to compromise multiple servers simultaneously to compromise the keys. Hence they are more resistant to stealing keys by the adversaries and are less prone to key loss.

Recently, Eyal [46] analyzed and has shown that for a wallet, an increase in the number of associated heterogeneous keys improves security. It shows that the probability of users losing access and adversaries gaining access is lower for multi-device (multi-key) wallets than single key scenarios. Hence, multi-device wallets are more *secure* than the single-device counterparts. Several different approaches [34, 46, 55, 67] mitigating the security risks of the single-device wallets also indicate that multi-device wallets have been invariably proposed as schemes to achieve better security than single-device wallets. In this study, we investigate the users' mental model regarding the security offered by the multi-device wallets and the gap between the proposed and perceived security.

Single-device and multi-device wallets - Trust and Usability. The trust and usability aspects of single-device and multi-device wallets are more nuanced. For single-device wallets, since the key is placed in a single location, the users need to trust the single entity or location not to get compromised for the safety of their funds. In contrast, for multi-device wallets, users need not trust a single entity like in exchange wallets since the secret information is distributed. Naturally, since the key is distributed among multiple entities, multi-device wallets achieve higher replication of the keys.

For an multi-device wallet, when part of the key is placed on the client device, key-recovery is straightforward in case of device loss since the other parties can generate new shares. Also, with a good choice of threshold structure, the keys can be made highly available [55] similar to single-device scenario. It should be noted that depending on the setting multi-device wallets can also provide complete control of the key to the user like the single-device wallets. For example, consider a scenario when the key is divided into two shares and one of the shares is placed on the client device. In this case, the transaction does not go through without client authorization irrespective of how the second share is shared among multiple servers.

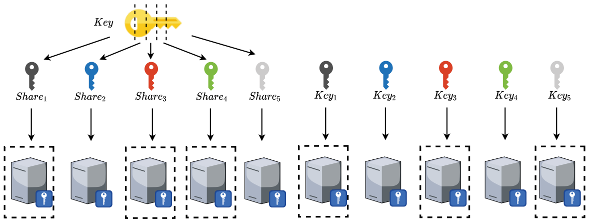
Though the interface of many multi-device wallets (Eg: ZenGo, Torus) is similar to single-device wallets for making transactions, multi-device wallets typically have a higher setup time. The usability issues and misconceptions of users regarding wallets pointed out by Voskobojnikov et al. [80] like confusion on the part of participants regarding transaction and mining fees, cancellation of transactions, lack of transparency from the blockchain regarding the state of the transaction is likely to be common between both single-device and multi-device wallets since they are not dependent on the location of key or authorization.

While the focus of this work is on the security model of different wallets and the users' perception about them, we uncover interesting mental models regarding usability aspects. The perceptions of usability directly affect the different preferred settings and thresholds for the multi-device wallets; we discuss them in Section 5.

2.2 Subclasses of Multi-device wallets

We further classify the multi-device wallets into two types *Multisig wallets* and *Threshold wallets*. In a multisig (multi-signature) wallet [19, 27, 43], N different keys are generated and placed on N devices such that signatures [36, 37, 60] from at least T devices are needed to authorize the transaction. These keys may be placed on devices of different users or a single user. For example, multiple keys are given to different people in a board of a firm such that at least a subset of them need to provide the signature for the transaction or payment to go through. The set of signatures authorizing the transaction, reveals the access structure (N, T) of the distribution of the keys used. Both multisig wallet and threshold wallet (depicted in Figure 1) employ an access structure where the secret information is distributed among N locations such that any T or more locations need to respond to authorize the transaction. We call it the (N, T) access structure. In a threshold wallet[11, 20], a single secret key is *secret-shared* [35, 75] among N devices out of which T or more devices provide a partial signature. The partial signatures are collected and aggregated into a single (threshold) signature [37, 53] to authorize the transaction.

The signature generated as threshold signature does not reveal [13, 53] the underlying access structure among the clients or which parties signed the transaction. Threshold signature is similar to a single regular signature, unlike multisig, which is a concatenation of multiple signatures, so it offers better storage efficiency. However, threshold signatures are dependent on the exact cryptographic scheme and are not widely available for all the signature schemes. This is not an issue with multisig schemes as they can be realized using any signature scheme, but they impose scripting [74] requirements.



(a) $(5,3)$**-Threshold wallet** **(b)** $(5,3)$**-Multisig wallet**

Figure 1: Multi-device wallets. (a) Threshold Wallet: Key-shares of a single key are generated and stored in different locations. (b) Multisig Wallet: Multiple (different) keys are stored on different devices (can be different client devices). A subset of shares or keys – threshold T or more – are required to sign the transaction in each case.

3 RELATED WORK

3.1 Usability of cryptocurrency systems

Many recent studies [8, 48, 49, 54, 79, 80] have focused on usability issues and challenges of cryptocurrency systems. Few studies have also explored issues of trust in blockchain systems, the trust challenges/risks and ways to mitigate them [73]. Recently, Mai et al. [66] brought out the general misconceptions of users in using cryptocurrency systems regarding keys, anonymity, and fees. They investigate misconceptions on the generation of cryptographic keys, which may lead to their mishandling and loss of funds. Voskobojnikov et al. [79] study the risk perceptions of both users and informed non-users of cryptocurrencies. They discuss several perceived risks, including loss of keys by the participants and risk mitigation strategies for different cryptocurrencies.

Usability. Cryptocurrency users face challenges regarding usability and understanding of the security implications of features of the wallets. Blockchains and cryptocurrencies also suffer from entry barriers and the perception of usability between users and non-users [49, 54, 79]. Beznosov et al. [80] study the user experience of wallets by analyzing the ratings of famous cryptocurrency wallet applications. They study more than 45K reviews and reveal that users have several misconceptions regarding the features and interface, including how different mining and transaction fees are collected, leading to grave errors in handling the secret keys and currency transfers.

Krombholz et al. [62] performed a large-scale survey and evaluation of different security practices of Bitcoin users and brought out the perceptions and flaws in the usage of bitcoin wallets. Halpin et al. [8] studied the usability problems in using crypto-wallets like ZCash while achieving privacy through Tor and VPNs. Here they identify that most users find it difficult to set up wallets and integrate with anonymization tools like Tor. Frohlich et al. [48] study the usability of wallets and security practices by conducting semi-structured interviews of participants and propose a model to map the users by their exposure to the internet and key management. More recently, Abramova et al. [29] classified all the crypto-wallet users into three groups of cypherpunks, hodlers, and rookies. They measured multiple factors, including perceived notions of self-efficacy, vulnerability, concern, etc, for clustering and observed specific differences in the preferences of different types of wallets, measures taken to secure their wallets etc.

Building on this line of research, along with security issues we investigated and uncovered different perceived usability aspects and how they affect the choice of threshold settings in multi-device wallets. For example, some participants preferred lower thresholds in multi-device wallets for lower transaction (submission) delay.

3.2 Key management in wallets

Passwords are still a popular form of authentication [57] and are even used by many cryptocurrency wallets. However, the underlying authentication mechanism for cryptosystems is through public-key cryptography using secret-key, public-key pairs. Usability issues of public-key cryptography in encrypted e-mail have been studied [50, 51, 76] to report that key management by the end-users is indeed a complex task. To uncover usability issues in bitcoin key management, Eskandari et al. [45] conducted a cognitive walk-through of bitcoin applications, brought out shortcomings, and provided a framework for evaluating cryptographic key management systems.

Vulnerabilities in wallets. Single devices wallets are vulnerable to several attacks; Vasek et al. [78] study how brain wallets are prone to offline password guessing attacks. They show that most brain wallets are vulnerable and can be drained within a day of creation. Arapinis et al. [32] study the vulnerabilities of the hardware wallets by modeling their security in the Universal Composability framework. They analyze a few well-known hardware wallets in their framework and show that they are vulnerable to payment, address generation, and chain attacks. Bui et al. [38] study how computer/desktop wallet applications are vulnerable; even without privileges, the attacker can impersonate the endpoints of remote procedure calls (RPC) and transfer funds. While multi-device wallets mitigate the risks of single-device wallets by distributing the secret information among many devices, they still can be vulnerable to attacks. Aumasson and Shlomovits [20] show ways to attack the implementations of schemes like threshold-ECDSA [52, 64]; they also suggest ways to mitigate them.

Several works [39, 67, 71] studied the vulnerabilities in single device wallets and proposed various ways to mitigate them. Instead of storing the secret key in the memory, Dai et al. [39] suggest storing in the seed of the secret key in a trusted part of the hardware such that no adversary can access to it. Barber et al. [34] propose a super wallet - sub wallet mechanism where the currency is placed in the super wallet and transferred to sub wallets in smaller quantities as and when required; Rezaeighaleh and Zou [71] propose a deterministic sub wallet key generation from the super wallet seed. Marcedone et al. [67] proposed a two-factor signature generation mechanism in hardware wallets to be secure against malicious hardware vendors. He et al. [55] propose a distributed key management mechanism for better availability of keys in a multi-device wallet setting where the key is distributed among multiple servers; the proposed scheme provides high availability of the keys for the users. It is evident from the different approaches [34, 46, 55, 67] that multi-device wallets have been invariably proposed as schemes to mitigate the security risks of single-device wallets. This work contributes to understanding how the different users perceive the security of multi-device wallets and if there is a gap between offered and perceived security, thereby affecting their adoption.

4 METHODOLOGY

In this section, we discuss our survey-based study design to understand the wallets' usage and user preferences.

4.1 Survey instrument

Our primary survey instrument had two parts. In part I, we asked general questions regarding users' experiences with different crypto-wallets. In part II, we probed users' preferences for two broad classes of wallets—single-device and multi-device wallets after grounding their understanding with videos discussing these wallets. Our full survey instrument is included in Appendix D.

Part I: Usage characteristics, experiences with current wallets and factors responsible for choosing a wallet (RQ1). We start part 1 of our study with a survey by asking which wallets are most often used by the participant and what factors impacted this choice. Specifically, we probed the impact of factors like wallets' interfaces, security guarantees, operation in multiple currencies, ease of recovery, as well as the relative importance of crowdsourced ratings or reviews from famous personalities on the choice of a particular wallet. Next, to uncover experiences with their current wallets, we asked if our participants ever lost a key or password, resulting in the loss of crypto funds and their most significant security concern regarding cryptocurrency wallets. We also adopted two sets of questions from earlier work to understand our participant attitudes better. These questions measured perceived vulnerability and perceived self-efficacy regarding safeguarding the funds and secret keys in crypto-wallet settings [29]. Finally, we asked the participant how familiar they were with each wallet– paper, exchange, desktop/mobile, threshold, and multisig wallets. These questions helped us estimate the user-familiarity levels with different wallets presented in the next part of our study.

Part II: Users' preference for multi-device wallets and their default settings (RQ2, RQ3). In the second part, we first educated the participants about different wallets using two short videos, each approximately 2 minutes long. The first video [1] discussed different single-device wallets and their pros and cons. The second video [2] showed how multi-device wallets solve problems of single-device wallets and discussed the two multi-device types — threshold and multisig wallets. Informing the participant using the videos helps us bring all participants to a similar understanding of wallets and helps us analyze their responses more confidently. To assess whether the participants have indeed watched and understood the content, we ask three knowledge-based questions (with justifications for their answers) after each video.

We first explain why multi-device wallets may be more secure (as explained in Section 2.1) and survey if the participants are willing to shift to them. After inquiring about the specific reasons for shifting (or not), we study the different settings they prefer.

After showing the videos, first, we asked users' preference of the location for storing the key of an exchange wallet. This question helps us understand if the users trust the exchange and any single location among different client devices and remote servers. We further asked the participants about the vulnerability of various key storage locations of single-device wallets. Next, we inquired if the participants were willing to shift to multi-device wallet if the wallet developer provided it. We also asked between threshold and multisig wallets which one do they prefer and why.

To understand the participants' preferred settings for the multi-device wallets, we asked them to choose among three different settings with varied umber of servers and threshold values. In this part, we essentially uncover participants' preferences regarding the reputation of the server hosts and the total number of servers. Furthermore, we explored the participants' preference regarding storing the secret keys for single-device wallets in the face of different attack scenarios and preference regarding the distribution of the shared keys among different devices for multi-device wallets.

Finally, we asked questions to investigate the participants' preferences regarding the key locations. Specifically, we showed users scenarios regarding different threat models (e.g., governments viewing and blocking access to the information hosted on servers in their jurisdiction). Then we asked where the participants preferred to store or the key (share) *by default* among the options provided in the single device and multi-device wallet settings for these different threat models. These questions provide us with information regarding the desired settings of wallets under various threat models.

Essentially, we first educated the user regarding the advantages of multi-device wallets and checked if they are willing to shift to them. If they are not ready to shift even at the cost of security, we analyzed the reasons. We then studied the different preferred settings for the multi-device wallets, including server setup under various government characteristics.

4.2 Pilot Studies

Before final deployment, we conducted two pilot studies for our survey. In the first, we piloted the survey using in-person interviews for six participants to test the comprehensibility of the survey questions and measure the average completion time.

Initially, the survey videos were shown to the participants consecutively, followed by four knowledge-check questions. However, during the first pilot, participants demonstrated a loss of attention, evident from the incorrect answers to our follow-up knowledge-check questions. However, when asked to explain the wrong answers, participants reevaluated and desired to change their responses, hinting at a cognitive overload. We divided the videos into two sections to address this problem and ask questions about each video separately. Responses from this first pilot also prompted us to simplify some questions which asked to rank provided options—we ended up converting them to equivalent Likert scale questions.

After incorporating the changes, we conducted a second pilot study using a crowdsourcing platform named Prolific.co, which is regularly used for academic advertising surveys. We recruited 20 (pre-screened) participants for further feedback. We asked additional follow-up questions to check the ambiguity of questions and answers in this pilot. 90% of the participants found no ambiguity

[1] Can be found at https://www.youtube.com/watch?v=rH1bcbeoPew
[2] Can be found at https://www.youtube.com/watch?v=LVa00yiOBjA

in the survey. Additionally, we asked to explain the answers to knowledge-check questions to nudge participants to be attentive to our educational videos on single-device and multi-device wallets. We also increased the knowledge-check questions to three per video, totaling six instead of the earlier four for more stringent checking of the acquired knowledge.

4.3 Recruitment

Our online survey is scalable to a large number of participants. Consequently, we uncovered interesting user behaviors and attitude patterns using statistical analysis. However, one key challenge of our recruitment procedure was to target the cryptocurrency wallet users and enthusiasts. To that end, following the approach taken by Abramova et al., [29], we recruited participants from two sources—(i) The crowdsourcing platform Prolific.co, and (ii) social media platform Twitter to reach broader cryptocurrency community.

Recruitment from Prolific: For Prolific, we chose participants both from the US and UK [3]. We also ensured that they had not taken our pilot studies. We selected our participants using a screening survey conducted before the full survey. This screening survey consisted of seven questions about the wallets they were using, for how long, and how frequently they used those wallets (see screening survey instrument in Appendix C). To avoid irrelevant user responses, we made the question about their current wallet a text entry question. We removed all the participants who left the text field blank or entered an invalid wallet name. We also asked screening survey participants whether they were interested in a future longer survey.

We deployed the final survey in multiple batches of 30 – 50 participants on multiple days and different times over one week. WEe did this setup for the distribution to counter any anomalous time dependencies due to the effect of events occurring at a specific time [31]. The median time of completion of the survey was 21 minutes 52 seconds and the compensation was 4$ for each participant (indicating an hourly wage of 10.88$, comparable to prior studies [29]). Furthermore, participant feedback from the pilot study on prolific showed that 95% of the participants were satisfied with the payment. We used additional stringent quality control criteria (Section 4.4) to ensure the quality of responses in our final dataset.

Recruitment from Twitter: To reach out to a greater cryptocurrency user community (beyond Prolific userbase), following prior work, we also tweeted using the Authors' Twitter accounts to take part in this anonymous survey [29]. For participants from Twitter, again, we only kept the participants who self-reported to be more than 18 years old, speak English, and cryptocurrency users with valid wallet names. For participants from Twitter, we announced a raffle of 50$ gift card for every 25 participants using anonymous email ids collected to give away the gift cards. Similar to Prolific, we used the quality control criteria (Section 4.4) on the Twitter responses too.

Ethical Considerations. For all participants, before the survey began, we informed the participants of the purpose of the study, its estimated duration, and the compensation. We further assured the participants that we would not collect any personally identifiable information (PII) from them. Participants could abort and return the survey at any time during the study. Any identifying information like email ids, Twitter handles, etc., related to the participant is removed from the collected responses to preserve the anonymity of the participants. Our study was examined and approved by the lead author's Institutional Review Board (IRB).

4.4 Quality Control

To ensure the quality of responses, we randomly added an attention check question asking them to choose the current month of the year. Apart from that, we consider responses only from those participants who have answered our knowledge-based (Yes/No) questions satisfactorily (to check if they watched our videos). More specifically, we consider only those participants who answered at least two out of three correctly in each subset. Furthermore, if a participant answered two or more questions wrong, one author manually checked the corresponding explanation to see if the participant was knowledgeable. For example, one of the questions asked about the loss of funds upon an Exchange wallet compromise, participant $P25$ disagreed and responded —"*compromise of the server holding the keys does not necessarily mean my money is lost*". This participant has understood the question and has an idea about the correct answer but over-thought the questions. Correspondingly, they chose the wrong option; we included all such participants in our final study even when they answered more than two questions wrong in each set. There were 22 such responses. When watched at regular speed, the total length of videos was 4 minutes 35 seconds; hence we also exclude participants who finished the survey in less than 15 minutes, including watching the study. Since that would have implied they completed both parts of the study in around 10 minutes or less, signifying the poor quality of responses (also manually verified via checking qualitative responses).

4.5 Participant Demographics

A total of 334 participants responded to the survey on Prolific. We discarded the responses that did not meet the validity criterion and passed our quality control checks (Section 4.4). Finally, there were 210 valid responses from Prolific. Additionally, we collected 45 valid responses out of the 250 from the Twitter platform. We present detailed demographics of our participants in Appendix Table 3.

In total, 72.15% of the participants identified themselves as male and 27.45% as female, while one participant preferred not to answer, indicating a male bias in our sample. Among the different age groups, the 25 – 34 age group dominated the total population with more than half of the total at 52.15% followed by 18 – 24 and 35 – 44 age groups at 21.56% and 20% respectively. Thus, our study has a larger younger population than older (> 35). The participants in our survey are also more educated than the general US population [5], with 73.32% of the participants having a Bachelor's degree or higher. While one expects the participants from crowdsourcing platforms like Prolific to be tech-savvy [59], more than half of the participants (50.98%) of our participants reported that they do not have any background experience in the information technology (IT) field.

[3] Over 65% of the participants on Prolific are from the US and UK [10] who speaks English and more than 18 years of age

Importantly, our participants are active users of different crypto-wallets, where they invest 29.56% of their savings on average across all participants. We provide our participants' crypto-wallet usage pattern in Figure 2. They also follow different social media and reputed personalities for ratings and reviews in choosing their wallets as shown in Figure 4a and Figure 11 in Appendix. Overall, a majority of our participants are young, well-educated who have invested in cryptocurrency.

4.6 Analysis Method

Coding free text answers. We coded all the free text answers and explanations for questions from our survey to segregate and uncover different perceptions of the participants. Two researchers have independently coded all the free-text responses using a common codebook. Across the various questions, the inter-rater agreement – Cohen's κ [68] was in the range $0.7-1$, indicating substantial agreement. The coders met and resolved the disagreements to arrive at the final codes.

Statistical Analysis. We used statistical hypothesis testing to uncover different correlations and identify the significant factors affecting the various preferences and choices of the participants. We used Chi-Squared (χ^2) test [15, 70] for the different responses of all the questions to uncover correlations between groups of participants and their preferences. We also used the Mann-Whitney U test [65] between participant groups to compare their characteristics. For our tests on the multi-answer questions, we treat each option as an independent question/answer. Our results for the χ^2 tests have been presented in Table 1 and for Mann-Whitney U test are presented in Appendix Table 4. For all the tests, the significance level α was 0.05, which was further adjusted using Bonferroni multiple-testing correction [72].

4.7 Limitations

We conducted the study to uncover factors affecting the users' preferences in choosing their wallets. While we tried to cover the aspects comprehensively, one should interpret our study in the context of limitations like all the previous studies. We collected 255 responses from platforms Prolific and Twitter. The responses from Prolific were limited to UK and US. Cryptocurrencies have proliferated and used various people varying in understanding, knowledge, and preferences. Restricting to two countries and online platform Twitter may be restricted in terms of the range of preferences uncovered, including any geographical or cultural influences on the choices made. However, we obtain interesting insights into the mindset of the crypto-users in choosing the single-device and multi-device wallets. We bring out interesting observations regarding the participants' desire for control over their funds even in conditions of possible compromise.

Our survey and the two videos included in it have been in English. We required the participants to speak English which might have excluded any non-English speaking population and resulted in possible language and cultural bias. It would indeed be an interesting future work to identify and understand these biases and their effect on the choices made in choosing wallets. However, we believe our study covers a significant range of crypto users with varied experiences obtained while dealing with cryptocurrencies.

5 RESULTS

5.1 Current usage-based groups and factors affecting users' choice of wallets - RQ1

We begin by categorizing our participants into two distinct usage-based groups: *Newbie* and *Non-newbie*. We report the usage, preferences of each group and compare them. We also analyzed the security-related preferences of these groups.

5.1.1 *Two different user groups exist with different familiarity and usage.*

We first divided the users into usage-based groups to capture various behaviors and understand their preferences. Recall that Abramova et al. [29] analyze and group all the participants into three categories. They found perceived vulnerability and self-efficacy show the most significant separation among their groups. Following the work [29], we investigated the perceived vulnerability and self-efficacy by asking the same set of questions. However, analysis of these responses has not resulted in any meaningful clustering owing to no statistically significant differences between these groups for self-reported survey responses (e.g., regarding familiarity and usage of crypto-wallets).

Interestingly, the self-identified categories correlated well with the survey responses regarding expertise and preferences. Specifically, we asked the participants to identify themselves among three types — (i) I use them solely for the interest in technology (ii) I use them primarily as an avenue for trade, buying and selling cryptocurrencies (iii) I am a newbie, started using them for fear of missing out the crypto boom. The pairwise Mann-Whitney U tests between responses from these three categories (for familiarity with wallets and usages) depicted a lack of statistically significant difference between the first and second categories (see Table 5 in Appendix for pairwise p-values for 3 group classification). Hence we group all the participants choosing the first two options as *Non-newbies* and the participants self-reporting as newbies under the *Newbies* group. These two groups significantly correlated with their responses as indicated by the low p-values (see Table 1). We present the mean values for different responses among these two groups in Table 4 in the Appendix.

Specifically, responses to the questions which significantly correlated with these two groups are in Table 1 (p-values are with Bonferroni correction). The key differences occurred in the duration of usage of the crypto-wallets, percentage of savings invested in crypto assets, background knowledge in computer science/information technology (IT), and the purpose of use (trading). The other set of factors that differentiate the two groups is familiarity with different wallet types.

5.1.2 *The current majority of users are recent adopters and use them for long-term investment.*

Majority of current crypto users are 'recent' adopters. Of the total participants surveyed, a total of 65% have reported having started using crypto-wallets only since the last two years and 33% have started using less than a year ago. This shows the rapidly expanding nature of cryptocurrencies in recent years. Among the Non-newbie group, a total of 59.8% of participants have been using it for the last two years. All the participants using the wallets for more than 4 years are in the Non-newbie group, accounting for 17.25% of that group. Among

Table 1: Chi-squared test results for different questions including demographics for Newbies and Non-newbies. The number of samples is 255. In the table, we only show the variables that have significant p-values. df is the degrees of freedom.

Variable	χ^2	df	p-value
Number of years	39.1284	3	1.63e-08***
% of savings invested	27.1900	4	1.81e-05***
Background in IT	24.3844	2	5.06e-06***
Usage - Trading	17.10456	1	3.53e-05***
Familiarity-wallet			
Paper	18.0435	4	0.0012**
Exchange	42.6121	4	1.24e-08***
Desktop/Mobile	31.6182	4	2.28e-06***
Hardware	49.3694	4	4.88e-10***
Multisig	28.5448	4	9.67e-06***
Threshold	28.1623	4	1.15e-05***

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

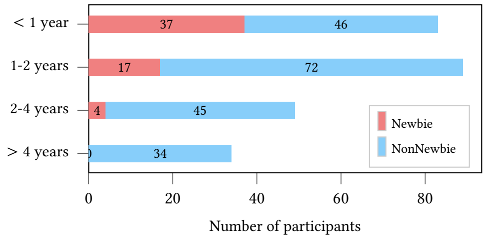


Figure 2: Duration of crypto-wallet usage by the participants. The majority are recent adopters using them for the last two years.

the Newbie group, 63.7% have started using only in the last year while a total of 93% have reported using them for the previous two years. This is expected as the group identifies itself as one adopting cryptocurrencies for fear of missing out on the crypto boom. Figure 2 shows the total number of users for each time period[4]. It indicates that the majority of our participants are recent adopters using them for less than two years.

Users employ cryptocurrencies as long-term investment far more than as an alternative to fiat currency. 80.3% of the participants reported using cryptocurrencies as a long-term investment, and only 20.8% use them as an alternative for fiat currency. 81.02% of newbies use them for long-term investment where the corresponding percentage among non-newbies is 79.69%. Among non-newbies, 23.8% report using cryptocurrencies as an alternative to fiat currency, and only 10.34% of newbies use it for the same.

Most users use single-device wallets. Most of the participants use single device wallets, including hardware wallets like Trezor (presented in Figure 8 in Appendix). Of these Coinbase and Binance seem to be popular among both the Newbie and Non-newbie groups. 60% of all the participants use Coinbase, whereas 37.2% use Binance. The participants had a choice to enter up to 3 unlisted wallets in the 'Other' fields, The wallets listed by participants varied widely, including TrustWallet, Ziglu, Atomic, Dharma, and ZenGo.

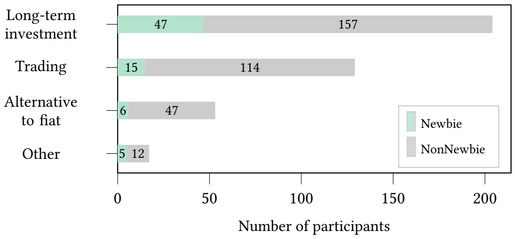


Figure 3: Purpose of using crypto-wallets. The majority of participants use them for long-term investments and trading.

See Figure 9 in Appendix for the reasons for choosing the different wallets and the corresponding number of participants. Among the different reasons, the one with the highest number of participants among the Non-newbie group is the security guarantees offered by the wallet with 75.6% opting it whereas the among Newbie group, it is the ease of usage of interface with 77.5%.

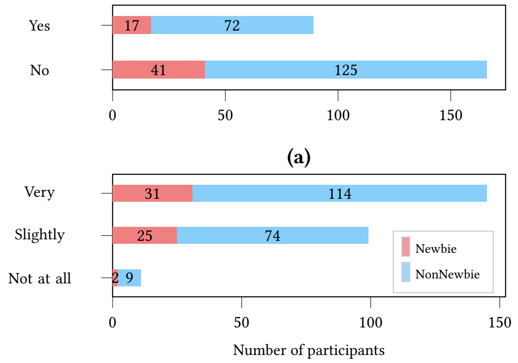
The most cited reasons for choosing the wallets among the participants across the two groups are the security guarantees they offer, the ease of interface, support for multiple currencies, and the popularity of the wallets

Type of security concerns for user groups. Different participants consider different issues as security concerns for the wallets. However, the biggest concern among them is the loss of funds by compromise of server and secret key hosted by the remote server (see Figure 10 in Appendix). The next biggest concern for both groups is the lack of proper recovery mechanisms for the secret key. These are followed closely by the other concerns of compromise and loss of key at the user device and server, loss of secret key by the user in both the groups.

5.1.3 Users consider ratings to be important. **Ratings and reviews in crowd-sourced platforms heavily affect users' choice of wallets**. Ratings of the wallets seem to affect the users' choice to a great extent – 34.9% of total participants have claimed to choose their wallets *solely* based on ratings of wallets on crowd-sourced platforms like Play Store and App Store. 56.8% of all have reported that ratings and reviews by famous personalities are 'very important' compared to 38.8% who mentioned that they are 'slightly important'. Only 4.3% have claimed ratings and reviews are not important at all. In both the Newbie and Non-newbie groups, at least 29% of each group have claimed to have chosen the wallets solely based on ratings showing their significance (see Figure 4a and Figure 4b).

Social Media as a source of knowledge. Among the different social media followed by the participants for learning about wallets, Twitter and Youtube occupy the top positions, followed by Reddit and Facebook. We asked the participants to choose (or add) all the social media they follow in the survey. The percentage of participants using Twitter, YouTube, Facebook and Reddit among Non-newbies are 59.89%, 36.54%, 27.91%, 27.91% and the corresponding numbers for the other group are 34.48%, 18.96%, 13.79%, 34.48%

[4] Questions with a single answer are displayed in red-blue and ones with multiple answers are shown in green-grey bar graphs.



(a)

(b)

Figure 4: Response to the questions (a) Was the wallet chosen solely based on ratings (b) Importance of ratings and reviews while choosing a wallet. They show that ratings are reviews are important to many participants.

(see Figure 11 in Appendix). The number of Reddit followers in the Newbie group is higher than the other social media except for Twitter, showing its increasing popularity among the more recent users.

5.1.4 Users are less familiar with multi-device wallets. The self-reported familiarity with the different wallet terms indicates that the users are unfamiliar with multi-device wallets. On a Likert scale of $1 - 5$ with 1 being "Not-familiar at all", only 3.5% of all the participants claimed that they are 'very familiar' with the threshold wallet while 49.1% claimed to be "Not-familiar at all". The corresponding percentages for multisig wallets are 3.13%, 42.7%. The mean familiarity over all the wallet types for the Newbie group is 2.02 and for the Non-newbie group is 3.05. The familiarity of the groups with the multi-device wallets is lower at 1.39 and 2.26, respectively. The corroborates with the names of different wallets reported to be used by the participants (see Figure 8 in Appendix) where single-device wallets dominate and shows that the participants are less familiar with multi-device wallets.

To overcome this lack of familiarity in the latter part of the survey and to bring all the participants to a similar level of understanding of multi-device wallets, we designed and presented two short videos explaining the advantages and disadvantages of single and multi-device wallets. The videos are followed by two sets of 3 questions each for the explanations are sought. 120 participants got all the 6 correct, showing increased knowledge and familiarity after the videos.

5.2 Users' willingness to shift towards multi-device wallets - RQ2

5.2.1 The majority of users are willing to shift to multi-device wallets but few are not. After learning about multi-device wallets, when asked which wallet they prefer, 67% of all the participants chose multi-device wallets over all other options (see Figure 5a). The majority of participants also wish to shift to multi-device wallets if their current firm offers it. At least 70% of each group wanted to make the shift (see Figure 5b). However, the remaining – slightly less than 30% of each group were not willing to use multi-device wallets. Table 2 shows the percentage of participants, the reason for retaining single-device wallets and shifting to multi-device wallets. Believing that single-device wallets are more secure, simple to use and retaining control of the secret key are the main motives across the users for remaining with single-device wallets. There is no correlation among the Newbie and Non-newbie groups and their choices of shifting to multi-device wallets (as indicated by high p values in the χ^2 analysis).

Table 2: Reasons from our open coding and % of participants for their willingness (non willingness) to shift from single-device wallet to multi-device wallet.

	Reasons	%
Not willing	Single-device wallets are more secure	37.5%
	Single-device wallets are simple to use	25%
	I do not want to lose control of keys	20.8%
	Other reasons	16.6%
Willing	Multi-device wallets are more secure	79.2%
	Other reasons including availability	20.78%

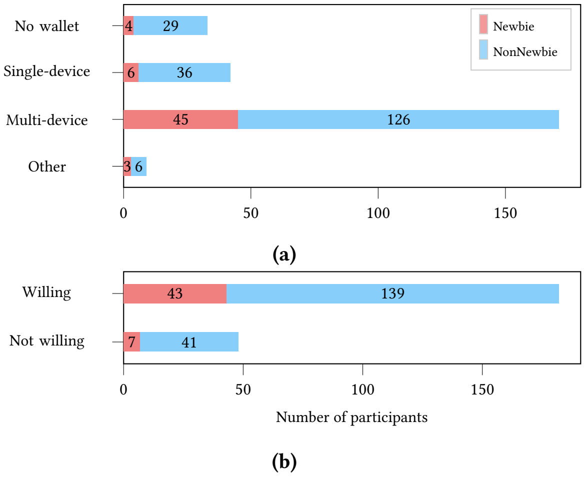
Reasons for shifting to multi-device wallets. Most participants who chose 'Yes', opted it because multi-device wallets offer better security features like overcoming single point of failure— P53 explained *"Better security because you need multiple devices to gain access. This also means that even if one device is compromised the attacker can't gain access"*. 79.2% of the participants choosing to shift opted multi-device wallets for better security features (see Table 2).

Around 20.8% participants (of the ones choosing to shift) wanted to shift to multi-device wallets for reasons including ease of access from any device of their choice, better availability in case of loss of a device and ease of recovery. P202 wrote *"I can access my wallet from several devices, that's better as I don't have to depend on one device all the time"*. In the case of multi-device wallets, when a single device is compromised the other parties can refresh the shares. Some participants realise this and chose to shift to multi-device wallets as the key recovery is easier. In those lines, P213 opined *"It is much easier to recover your security keys in a multi-device wallet than a single-device wallet."*

Reasons for not shifting to multi-device wallets. Among the participants who opted not to shift to multi-device wallets, when asked to explain, the responses ranged over a few factors — believing that the single-device wallets are more secure and preferring the simplicity to placing the trust only on the self to safeguard the keys.

37.5% of the participants who stick to single-device wallets believe that they are more secure than the multi-device wallets. They wrote *"Personal hardware keys should be secure enough" (P18)*, *"I will still stick to my single wallet device because it is difficult to compromise."(P99)*. However, this is a flawed mental model of security, since it is shown [46] that multi-device wallets are more secure than single-device wallets. 20.8% participants wish to use single-device wallets since they want to hold on to the key themselves. Few answered, *“I prefer to be responsible for my keys. If I lose them, that is my fault”(P1)*, *“Id rather keep the key on me at all times so I know where it is and who has it, I only trust myself”(P25)*. Another participant P38 preferred single-device wallets for their simplicity, they said *“I’m happy with the simplicity and current security available with a single-device wallet”*.

In multi-device wallets, multiple devices need to communicate and aggregate the signatures collected to compute the final signature. This may induce some delays and also affect the availability. Few participants preferred to stick to single-device wallets for the availability of the keys. P101 mentioned *“I prefer that I try my best to keep the single key safe than run into server down-times. If I decide to use a Multi-device scheme, the devices might have a downtime”*.



(a)

(b)

Figure 5: (a) Preference among the single-device and multi-device wallet types. (b) Willingness of participants to shift to multi-device wallet from the currently used a single-device wallet.

5.2.2 Among multi-device wallets, users prefer threshold wallets for their privacy. In a threshold wallet, the threshold signature [37] generated to authenticate a transaction does not reveal the access structure i.e., the signature does not reveal the (N, T) values. In a multisig wallet, the access structure and T (minimum number of required signatures) are revealed. When asked to choose among multi-device wallets, 63.95% of the Non-newbie group and 68.96% of the Newbie group participants chose threshold wallet over the multisig wallet as shown in Figure 6.

These participants opted for threshold wallet for its privacy properties like not revealing the access structure. On these lines, P158 commented *“threshold wallet withholds a little more information like the N and T values and this provides more security”*. Some participants realized not knowing the N and T values makes it difficult for the adversary to decide on how many devices to compromise. This provides better security apart from the privacy offered from the threshold signature.

In a multisig wallet, several signatures are collected and aggregated by concatenation whereas, in a threshold wallet, the threshold signature appears similar to a single device signature. Hence the total data needed to represent the threshold signature is lesser than the multisig signature, making it more space-efficient. While this is a technical aspect to grasp, few participants understand this and have opted for threshold wallet. P246 commented *“Multi-sig wallets are inefficient - requiring several signatures wasting gas. Better implement a threshold wallet with MPC to reduce inefficiencies”*.

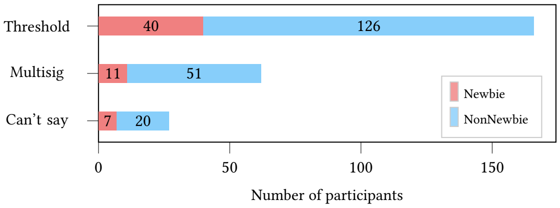


Figure 6: Preference among the multi-device wallets types – threshold and multisig wallets. Majority choose threshold wallets for offered privacy.

Participants chose multisig wallets for their simplicity and *because* it reveals the access structure (N, T). P146 commented *“It is easier for me to know how many devices and threshold I will require to be able to authenticate a transaction. It is easy to use too”*. Multisig wallet signature reveals which parties have provided the signature; if the signature is generated by any collusion, the colluding parties are revealed in the signature. Some participants prefer this over not knowing who signed. Participant P240 who chose the option ‘Can not say’ wrote *“The Multisig system clearly labels who the bad nodes are in a collusion attack, which information is missing from the threshold. OTOH, Multisig adds more load on the transactions, as more sigs is more data”*.

After familiarizing themselves through the presented videos, more than two-thirds of participants in our study were willing to shift to multi-device wallets. Among the ones who wish to use only single-device wallets, 37.5% (wrongly) believe that they are more secure than the multi-device wallets. 20.8% of them choose so because they do not want to lose control over the keys. It should be noted here that, multi-device wallets can indeed provide control over the keys to users. For example, if one share among the two total shares of the key is placed on the user device, no entity can access the key and funds without user’s approval and authentication. Among the multi-device wallets, the participants prefer the threshold wallets for the privacy properties they offer. A smaller set of participants prefer the multisig wallet for the simplicity and accountability they impose on the signers. We further investigate the attitude of the participants in terms of security by studying the default security settings they prefer for the different wallets.

5.3 Preferred default settings for crypto-wallets - RQ3

5.3.1 In single-device wallets retaining agency over key is preferred over the risk of account compromise. It is natural to choose a particular location for a secret key depending on the risk perception of certain attacks on the system. Hence to understand the participants’ risk perception, we investigated their preferred key-storage location for a single-device wallet under different attack scenarios. When asked to choose a location of secret key storage under the specific threat of client-device compromise, the choice of a maximum number of participants of each group is “Multiple remote servers (each storing the key)”. This can be expected as under the client compromise scenario one would expect users to opt for remote servers. Hosting the key on multiple remote servers increases the availability of key while also increasing the risk of being compromised. Many participants in both the groups opted for client devices including dekstop/mobile, paper and hardware tokens as the preferred location for client storage (see Figure 12 in Appendix). This indicates that even under vulnerabilities and client device compromise, many still wish to retain control over the secret key and thereby the agency over the funds. In the remote server compromise scenario (see Figure 13 in Appendix) the three key storage locations chosen by the highest number of participants are paper, client desktop/mobile, and hardware token.

5.3.2 *For multi-device wallets, users weigh reputation over distributing the attack surface.*

To understand the settings that the users prefer for multi-device wallets, the participants were asked to pick among three choices — (i) smaller number of reputed servers (ii) large number of servers with much lower threshold (iii) large number of servers with high threshold. In case of smaller number of reputed servers, they would provide higher availability with very few servers needing to respond, however the attacker just needs to compromise those few servers. In the second option, the servers are randomly chosen (with certain criterion) among many servers across globe but with lower threshold. Here the attacker is not readily sure of which servers to attack even though the threshold is small. The last option has higher threshold indicating that the attacker needs to compromise a very high number of servers.

More than half of participants placed their trust in reputation rather than the inability of attacker to compromise large number of servers distributed across globe. 65.48% of Non-newbies and 55.17% of Newbies chose small number of servers ($(10, 5)$ in Figure 7) hosted by reputed firms. Participants seem to trust the reputed servers to take good security measures as their reputation is at stake in case of compromise. P38 wrote *“I prefer servers to be hosted by well known reputed firms as they are likely to have in place stringent security measures to stop any breaches.”* Few chose smaller number of servers since maintaining and keeping track of a large number of them can be a complex task; they wrote, *“Keep it simple. More servers, more things to go wrong” (P244).*

Among the parties who opted for choices with more number of servers, increasing the number of servers for the adversary to attack is the most quoted reason. P25 said *“The more there are the harder it will be to be compromised. Being random servers its also harder to track them down”*. Another interesting aspect is that reputed firms can become centres for targeted attacks by the adversaries. In view of this one participant P76 said *“I would prefer randomly chosen servers as they are less likely to be targeted than established companies”*, while choosing $(100, 50)$ setting. The participants who chose larger number of servers and low threshold $(100, 5)$ opted for high availability of keys; even if many servers are down, the secret information is available to the clients.

Users wish to distribute trust for a fixed total number of devices. To understand if the participants were willing to distribute trust among more entities, they were asked if thy are willing to increase the value of T (threshold) for a given N (total servers) in a multi-device wallet. 60.4% of the Non-newbie group opted to increase the value of T while 36.54% chose not to. In the Newbie group, these percentages stood at 53.44% and 44.82% (see Figure 14 in Appendix). Increasing the value of T would imply distributing the trust among more devices/people. However, since signatures from any T or more are required to authenticate a transaction, it would mean higher communication overhead and possible delays if that person/device does not respond as expected. Thus the trade-off would be between distributing the trust against higher availability of the keys. Few participants choosing ‘Other’ indicated that they do not wish to simply distribute the secret key among more parties but carefully tailor the threshold for a particular scenario.

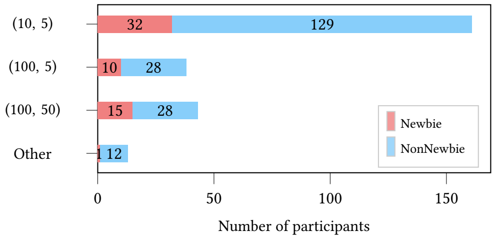


Figure 7: Preferred settings for (N, T) multi-device wallet. N is the total devices and T is minimum number of devices needed to generate signature. $(10, 5)$ is with servers hosted by reputed firms. In other settings servers are chosen randomly across the globe.

5.3.3 *The government policies affect the preference for share-distribution.*

Any server hosted in a particular country is subject to the local government privacy policies. Depending on the policy, few governments may be able to view or even block access to any cryptocurrency server data if they wish (here we assume a setting where the governments do not share data with each other). Thus, location of the hosted server is significant in terms of privacy and availability of keys to the users. Our survey explores users’ preferences of location of these servers for different secret-key distributions among client devices and remote servers. We investigate these preferences for both single-device and multi-device wallet scenarios under different government characteristic settings. For Threshold wallets, the participants were allowed to choose from (i) sharing the key among servers (ii) dividing the key into two parts (say $Share_1$ and $Share_2$), placing one part $Share_1$ on the client and sharing the second part $Share_2$ among all the servers.

Users do not prefer server locations where governments can block data access. For threshold wallets, whenever the government can not block access, irrespective if the government can view the data, at least 50% participants of Newbie group are willing to opt for sharing the key only among servers. In the case when the government can block access, less than 37.93% chose to share among servers with 63.79% choosing to share between the client device and the servers. In the Non-newbie group, more than 55% always wanted to place a share on the client device which went up to 69% when the government can deny access to the data (see Figure 16 in

Appendix). The responses are significantly correlated against the different government characteristics with χ^2 test p-value of 0.001. Thus government policies significantly affect choice of location for secret information and majority of users wish to have a share of the key on their devices when government can deny access.

In short, in our study, majority of the participants wish to retain control over the secret key in-spite of vulnerabilities. They prefer the keys to be hosted by a smaller number of servers hosted by reputed firms; they also like to increase the threshold for a fixed total number of servers to distribute trust further. Their choices of key location are affected by the governments' ability to block access to their secret information. var

6 IMPLICATIONS

Our study offers the developers specific insights into the settings and server architectures for their wallets. We also observe some interesting threshold cryptographic research problems for the community to consider.

Educating the users. As participants prefer multi-device wallets for better security, this study encourages developers who have developed or are considering a multi-device version of their wallets. However, about 37% of participants who were unwilling to shift to multi-device wallets, believed that single-device wallets are more secure than multi-device wallets. This flawed mental model needs to be addressed by educating the users about the security features of the multi-device wallets. About 20.5% of them wanted to stick to single-device wallets because they did not want to lose control over the keys. This should encourage the multi-device wallet developers to choose settings where they provide control of the keys to the user and convince them of the same.

Distributed server setup for multi-device wallets. While choosing a distributed server setup to host the shared keys, our study can significantly help developers arrive at a setting. We learn that the majority of the participants prefer a smaller set of reputed servers in locations where the governments cannot deny access to the data (see 5.3.3). Among the different share distributions (or access structures), as chosen by the participants, the developers should consider always placing a share on the client device to give them control (see Section 5.3.1). This can be achieved by generating two shares of the secret key $Share_1$ and $Share_2$, placing say $Share_1$ on the client device, and dividing $Share_2$ among multiple servers. Note that threshold wallet ZenGo [14] already follows this pattern, although with only one server share, while Torus [12] wallet offers no such control to the users.

General adversary access structure. In fact, the developers can consider general adversary structure secret sharing (GASS) [44, 47, 58, 63] for their wallets. In a typical threshold cryptographic setting, the adversary can corrupt up to a fixed fraction of players. However, GASS considers more general adversary corruption patterns, in which the adversary is allowed to corrupt any set of players in some pre-defined collection of sets (or access structure). Developing personalized threshold wallets based on GASS enables the developer to realize individual users' adversary mental models better and be more realistic for a wallet design. General adversary structure secret sharing and threshold signing for multi-device wallets can be an interesting design and implementation target for the research community and the wallet developers.

We note that implications of the user control go beyond the multi-device wallets setting and are also highly relevant for NIST threshold cryptography efforts [9] as well as fast-growing multi-party computation (MPC) based privacy-preserving machine learning (PPML) [30, 69]. For example, in the context of NIST's threshold cryptography initiative, it will be an interesting research problem to design a secure threshold ECDSA protocol that maintains the users' control over their keys in the wallets. The current threshold ECDSA protocols [42, 52, 53, 64] cannot securely realize users' control in the above-described setting where one of the two shares is re-shared among the servers.

Threshold vs. Multisig wallets. Threshold and multisig wallets offer interesting trade-offs concerning accountability and privacy. While many participants prefer the privacy provided by the threshold wallet, some do not wish to use them for the exact reason that they do not reveal enough information (see Section 5.2.2). If a signature is generated under collusion, the information of who is involved is not revealed in a threshold signature but is revealed under multi-signatures.

This study shows that users understand and consider the trade-offs in two types of multi-device wallets. This motivates security research towards signature generation and wallet design to offer the best of both worlds, including privacy and accountability. Since participants are concerned about space requirements of multisignatures in wallets (see Section 5.2.2), developing space-efficient multisignature schemes is an interesting problem to consider for the developers.

7 CONCLUSION

This study brings out a number of interesting behavioural patterns and mental models of the current crypto-wallet users. In our study, the participants behaved in two specific ways, either as Newbies or Non-newbies. The Newbies are the new entrants and are interested in the ease of usage of interface and popularity of the wallets. The Non-newbie group has relatively been using the crypto-wallets for a longer; they are naturally more familiar with different wallets. The majority of both groups use single device wallets and are not very familiar with multi-device wallets. A majority of both the groups use the wallets for long-term investments and very little as an alternative to fiat currency. Both the groups are concerned with the compromise of the key at the servers or client devices.

When educated about multi-device wallets that can mitigate both the issues of client-device or remote server compromise, most participants are willing to shift. The ones who are not, wish to retain complete control of the key. They also like the convenience of single-device wallets. Among the two types of multi-device wallets, namely threshold, and multisig, the majority of users prefer threshold wallets for their privacy properties over their multisig counterparts. Under different vulnerabilities, the participants prefer having control over the funds by having a share of the secret key on their local devices. The preferences of the participants are also greatly affected by the government policies at locations where the servers containing secret information are hosted.

Finally, the study offers some specific insights into the users' expected multi-device wallet threat models. This in turn presents some interesting threshold cryptographic research problems for the community to consider.

ACKNOWLEDGEMENTS

We thank Omer Shlomovits and Patrick McCorry for helpful comments and feedback on the multi-device wallets. This work has been partially supported by the National Science Foundation under grant CNS-1846316.

REFERENCES

[1] Binance. http://binance.com.

[2] Coin ranking - binance exchange. https://coinranking.com/exchange/-zdvbieRdZ%2Bbinance.

[3] Coinbase. http://coinbase.com.

[4] Coinbase revenue and usage statistics (2021). https://www.businessofapps.com/data/coinbase-statistics/.

[5] Educational attainment in the united states: 2020. https://www.census.gov/data/tables/2020/demo/educational-attainment/cps-detailed-tables.html.

[6] Fortune - nearly 4 million bitcoins lost forever. https://fortune.com/2017/11/25/lost-bitcoins/.

[7] Hackers move 760 million from the 2016 bitfinex hack. https://therecord.media/hackers-move-760-million-from-the-2016-bitfinex-hack/.

[8] Holistic privacy and usability of a cryptocurrency wallet. https://arxiv.org/pdf/2105.02793.pdf/.

[9] Nist- projects - multi-party threshold cryptography. https://csrc.nist.gov/Projects/threshold-cryptography.

[10] Prolific participants. https://www.prolific.co/#check-sample.

[11] Refresh when you wake up: Proactive threshold wallets with offline devices. https://arpa.medium.com/threshold-signature-explained-brining-exciting-apps-with-tss-8a75b43e19bf.

[12] Torus wallet. https://tor.us.

[13] Why threshold signature wallets are better than multisig: Top 5 reasons. https://sepior.com/blog/top-5-reasons-threshold-signature-wallets-are-better-than-multisig.

[14] Zengo wallet. https://zengo.com.

[15] Smooth tests of goodness of fit: An overview. *International Statistical Review / Revue Internationale de Statistique*, 58(1):9–17, 1990.

[16] Poloniex loses 12.3pc of its bitcoins in latest bitcoin exchange hack. https://www.coindesk.com/markets/2014/03/05/poloniex-loses-123-of-its-bitcoins-in-latest-bitcoin-exchange-hack/, 2014.

[17] Details of $5 million bitstamp hack revealed. https://www.coindesk.com/markets/2015/07/01/details-of-5-million-bitstamp-hack-revealed/, 2015.

[18] Chinese bitcoin exchange okex hacked for $3 mln, police not interested. https://cointelegraph.com/news/chinese-bitcoin-exchange-okex-hacked-for-3-mln-police-not-interested, 2017.

[19] Multisig wallets explained. https://medium.com/block-journal/multi-sig-wallets-explained-5544c122a1de, 2019.

[20] Attacking threshold wallet. https://eprint.iacr.org/2020/1052.pdf, 2020.

[21] A comprehensive list of cryptocurrency exchange hacks. https://selfkey.org/list-of-cryptocurrency-exchange-hacks/, 2020.

[22] Sok: A taxonomy of cryptocurrency wallets. https://eprint.iacr.org/2020/868.pdf, 2020.

[23] Bitcoin price history. https://www.investopedia.com/articles/forex/121815/bitcoins-price-history.asp, 2021.

[24] The complete list of crypto exchange hacks. https://www.hedgewithcrypto.com/cryptocurrency-exchange-hacks/, 2021.

[25] Crypto: A new asset class. https://www.goldmansachs.com/insights/pages/crypto-a-new-asset-class-f/report.pdf, 2021.

[26] Custodial vs. non-custodial wallets. https://www.gemini.com/cryptopedia/crypto-wallets-custodial-vs-noncustodial, 2021.

[27] Multisig wallet security. https://medium.com/the-capital/multisig-wallet-security-e2a1dee95cc0, 2021.

[28] Total cryptocurrency market cap, 2021. https://coinmarketcap.com/charts/, 2021.

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

[30] Mohammad Al-Rubaie and J Morris Chang. Privacy-preserving machine learning: Threats and solutions. *IEEE Security & Privacy*, 17(2):49–58, 2019.

[31] Sara Albakry, Kami Vaniea, and Maria K. Wolters. 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*, CHI '20, page 1–12, New York, NY, USA, 2020. Association for Computing Machinery.

[32] Myrto Arapinis, Andriana Gkaniatsou, Dimitris Karakostas, and Aggelos Kiayias. A formal treatment of hardware wallets. In Ian Goldberg and Tyler Moore, editors, *Financial Cryptography and Data Security*, pages 426–445, Cham, 2019. Springer International Publishing.

[33] Nicola Atzei, Massimo Bartoletti, Stefano Lande, and Roberto Zunino. A formal model of bitcoin transactions. In Sarah Meiklejohn and Kazue Sako, editors, *Financial Cryptography and Data Security*, pages 541–560, Berlin, Heidelberg, 2018. Springer Berlin Heidelberg.

[34] Simon Barber, Xavier Boyen, Elaine Shi, and Ersin Uzun. Bitter to better — how to make bitcoin a better currency. In Angelos D. Keromytis, editor, *Financial Cryptography and Data Security*, pages 399–414, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[35] Amos Beimel. Secret-sharing schemes: A survey. In *International conference on coding and cryptology*, pages 11–46. Springer, 2011.

[36] Mihir Bellare and Gregory Neven. Identity-based multi-signatures from rsa. In *Cryptographers' Track at the RSA Conference*, pages 145–162. Springer, 2007.

[37] Gerrit Bleumer. *Threshold Signature*, pages 611–614. Springer US, Boston, MA, 2005.

[38] Thanh Bui, Siddharth Prakash Rao, Markku Antikainen, and Tuomas Aura. Pitfalls of open architecture: How friends can exploit your cryptocurrency wallet. In *Proceedings of the 12th European Workshop on Systems Security*, pages 1–6, 2019.

[39] Weiqi Dai, Jun Deng, Qinyuan Wang, Changze Cui, Deqing Zou, and Hai Jin. Sblwt: A secure blockchain lightweight wallet based on trustzone. *IEEE Access*, 6:40638–40648, 2018.

[40] Poulami Das, Sebastian Faust, and Julian Loss. A formal treatment of deterministic wallets. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, CCS '19, page 651–668, New York, NY, USA, 2019. Association for Computing Machinery.

[41] Yvo Desmedt. *Threshold Cryptography*, pages 1288–1293. Springer US, Boston, MA, 2011.

[42] Jack Doerner, Yashvanth Kondi, Eysa Lee, and Abhi Shelat. Threshold ecdsa from ecdsa assumptions: The multiparty case. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 1051–1066, 2019.

[43] Manu Drijvers, Kasra Edalatnejad, Bryan Ford, Eike Kiltz, Julian Loss, Gregory Neven, and Igors Stepanovs. On the security of two-round multi-signatures. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 1084–1101, 2019.

[44] Karim Eldefrawy, Seoyeon Hwang, Rafail Ostrovsky, and Moti Yung. Communication-efficient (proactive) secure computation for dynamic general adversary structures and dynamic groups. In Clemente Galdi and Vladimir Kolesnikov, editors, *Security and Cryptography for Networks(SCN)*, volume 12238 of *Lecture Notes in Computer Science*, pages 108–129. Springer, 2020.

[45] Shayan Eskandari, Jeremy Clark, David Barrera, and Elizabeth Stobert. A first look at the usability of bitcoin key management. *arXiv preprint arXiv:1802.04351*, 2018.

[46] Ittay Eyal. On cryptocurrency wallet design. Cryptology ePrint Archive, Report 2021/1522, 2021. https://ia.cr/2021/1522.

[47] Matthias Fitzi, Martin Hirt, and Ueli M. Maurer. General adversaries in unconditional multi-party computation. In Kwok-Yan Lam, Eiji Okamoto, and Chaoping Xing, editors, *Advances in Cryptology - ASIACRYPT*, volume 1716 of *Lecture Notes in Computer Science*, pages 232–246. Springer, 1999.

[48] Michael Fröhlich, Felix Gutjahr, and Florian Alt. *Don't Lose Your Coin! Investigating Security Practices of Cryptocurrency Users*, page 1751–1763. Association for Computing Machinery, New York, NY, USA, 2020.

[49] Xianyi Gao, Gradeigh D. Clark, and Janne Lindqvist. *Of Two Minds, Multiple Addresses, and One Ledger: Characterizing Opinions, Knowledge, and Perceptions of Bitcoin Across Users and Non-Users*, page 1656–1668. Association for Computing Machinery, New York, NY, USA, 2016.

[50] Simson L. Garfinkel and Robert C. Miller. Johnny 2: A user test of key continuity management with s/mime and outlook express. In *Proceedings of the 2005 Symposium on Usable Privacy and Security*, SOUPS '05, page 13–24, New York, NY, USA, 2005. Association for Computing Machinery.

[51] Shirley Gaw, Edward W. Felten, and Patricia Fernandez-Kelly. Secrecy, flagging, and paranoia: Adoption criteria in encrypted email. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '06, page 591–600, New York, NY, USA, 2006. Association for Computing Machinery.

[52] Rosario Gennaro and Steven Goldfeder. Fast multiparty threshold ecdsa with fast trustless setup. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 1179–1194, 2018.

[53] Rosario Gennaro, Steven Goldfeder, and Arvind Narayanan. Threshold-optimal dsa/ecdsa signatures and an application to bitcoin wallet security. In *International Conference on Applied Cryptography and Network Security*, pages 156–174. Springer, 2016.

[54] Leonhard Glomann, Maximilian Schmid, and Nika Kitajewa. Improving the blockchain user experience - an approach to address blockchain mass adoption issues from a human-centred perspective. In Tareq Ahram, editor, *Advances in Artificial Intelligence, Software and Systems Engineering*, pages 608–616, Cham, 2020. Springer International Publishing.

[55] Xiaojian He, Jinfu Lin, Kangzi Li, and Ximeng Chen. A novel cryptocurrency wallet management scheme based on decentralized multi-constrained derangement. *IEEE Access*, 7:185250–185263, 2019.

[56] Martin E Hellman. An overview of public key cryptography. *IEEE Communications Magazine*, 40(5):42–49, 2002.

[57] Cormac Herley and Paul Van Oorschot. A research agenda acknowledging the persistence of passwords. *IEEE Security & privacy*, 10(1):28–36, 2011.

[58] Martin Hirt and Daniel Tschudi. Efficient general-adversary multi-party computation. In Kazue Sako and Palash Sarkar, editors, *Advances in Cryptology - ASIACRYPT*, volume 8270 of *Lecture Notes in Computer Science*, pages 181–200. Springer, 2013.

[59] Paul Hitlin. Turkers in this canvassing: young, well-educated and frequent users. In *Research in the Crowdsourcing Age, a Case Study*, 2016.

[60] Don Johnson, Alfred Menezes, and Scott Vanstone. The elliptic curve digital signature algorithm (ecdsa). *International journal of information security*, 1(1):36–63, 2001.

[61] Seoyoung Kim, Atulya Sarin, and Daljeet Virdi. Crypto-assets unencrypted. *Journal of Investment Management, Forthcoming*, 2018.

[62] Katharina Krombholz, Aljosha Judmayer, Matthias Gusenbauer, and Edgar Weippl. The other side of the coin: User experiences with bitcoin security and privacy. In Jens Grossklags and Bart Preneel, editors, *Financial Cryptography and Data Security*, pages 555–580, Berlin, Heidelberg, 2017. Springer Berlin Heidelberg.

[63] Joshua Lampkins and Rafail Ostrovsky. Communication-efficient MPC for general adversary structures. In Michel Abdalla and Roberto De Prisco, editors, *Security and Cryptography for Networks (SCN)*, volume 8642 of *Lecture Notes in Computer Science*, pages 155–174. Springer, 2014.

[64] Yehuda Lindell and Ariel Nof. Fast secure multiparty ecdsa with practical distributed key generation and applications to cryptocurrency custody. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, CCS '18, page 1837–1854, New York, NY, USA, 2018. Association for Computing Machinery.

[65] Thomas W. MacFarland and Jan M. Yates. *Mann–Whitney U Test*, pages 103–132. Springer International Publishing, Cham, 2016.

[66] Alexandra Mai, Katharina Pfeffer, Matthias Gusenbauer, E. Weippl, and Katharina Krombholz. User mental models of cryptocurrency systems - a grounded theory approach. In *SOUPS @ USENIX Security Symposium*, 2020.

[67] Antonio Marcedone, Rafael Pass, and Abhi Shelat. Minimizing trust in hardware wallets with two factor signatures. In Ian Goldberg and Tyler Moore, editors, *Financial Cryptography and Data Security*, pages 407–425, Cham, 2019. Springer International Publishing.

[68] Mary L McHugh. Interrater reliability: the kappa statistic. *Biochemia medica*, 22(3):276–282, 2012.

[69] Payman Mohassel and Yupeng Zhang. Secureml: A system for scalable privacy-preserving machine learning. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 19–38, 2017.

[70] R. L. Plackett. Karl pearson and the chi-squared test. *International Statistical Review / Revue Internationale de Statistique*, 51(1):59–72, 1983.

[71] Hossein Rezaeighaleh and Cliff C. Zou. Deterministic sub-wallet for cryptocurrencies. In *2019 IEEE International Conference on Blockchain (Blockchain)*, pages 419–424, 2019.

[72] G Rupert Jr et al. *Simultaneous statistical inference.* Springer Science & Business Media, 2012.

[73] C. Sas and Irni Eliana Khairuddin. Design for trust: An exploration of the challenges and opportunities of bitcoin users. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2017.

[74] Pablo Lamela Seijas, Simon J Thompson, and Darryl McAdams. Scripting smart contracts for distributed ledger technology. *IACR Cryptol. ePrint Arch.*, 2016:1156, 2016.

[75] Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, November 1979.

[76] Steve Sheng, Levi Broderick, Colleen Alison Koranda, and Jeremy J Hyland. Why johnny still can't encrypt: evaluating the usability of email encryption software. In *Symposium On Usable Privacy and Security*, pages 3–4. ACM, 2006.

[77] Victor Shoup. Practical threshold signatures. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 207–220. Springer, 2000.

[78] Marie Vasek, Joseph Bonneau, Ryan Castellucci, Cameron Keith, and Tyler Moore. The bitcoin brain drain: a short paper on the use and abuse of bitcoin brain wallets. *Financial Cryptography and Data Security, Lecture Notes in Computer Science. Springer*, 2016.

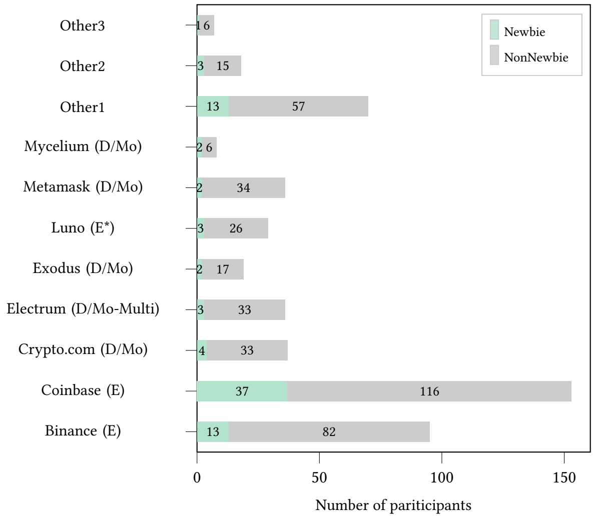


Figure 8: Currently used crypto-wallets. D/Mo- Desktop/Mobile, H - Hardware, Multi - Supports MultiSig, E* - Behaves like exchange wallet by maintaining keys.

[79] Artemij Voskobojnikov, Borke Obada-Obieh, Yue Huang, and K. Beznosov. Surviving the cryptojungle: Perception and management of risk among north american cryptocurrency (non)users. In *Financial Cryptography*, 2020.

[80] Artemij Voskobojnikov, Oliver Wiese, Masoud Mehrabi Koushki, Volker Roth, and Konstantin (Kosta) Beznosov. The u in crypto stands for usable: An empirical study of user experience with mobile cryptocurrency wallets. CHI '21, New York, NY, USA, 2021. Association for Computing Machinery.

A DIFFERENT SINGLE DEVICE WALLETS

- *Brain wallet*: In this, users choose to remember the passphrase or key associated with the wallet. This wallet is a single device wallet as the key is in a single location, the brain. If the user forgets the secret information, they can not access the funds.
- *Paper wallet*: The secret key of the wallet is placed on paper, typically as a QR code etc.
- *Desktop/Mobile wallet*: The wallet and the corresponding secret key are placed on the desktop or the mobile device of the user. The user can access the wallet only from that particular device. Eg: Electrum
- *Exchange wallet*: The secret key is placed at the exchange hosting the wallet. The exchange performs the transactions on behalf of the user. Eg: Coinbase.com, Binance
- *Web wallet*: The secret key is stored at the firm offering the wallet. This wallet is accessed through the web and hence is not device dependant.
- *Hardware wallet*: The secret key is stored on a particular hardware token. The client needs to plugin the hardware token every time a transaction is made. Eg: Trezor, Ledger Nano

Table 3: Participants' Demographics

	Newbie	Non-newbie	Total
	58 (22.74%)	197 (77.25%)	255 (100%)
Gender			
Female	26 (44.82%)	44 (22.33%)	70 (27.45%)
Male	32 (55.17%)	152(77.15%)	184 (72.15%)
Prefer not to answer	00 (00.00%)	01 (00.50%)	01 (00.39%)
Age			
18 - 24	16 (27.58%)	39 (19.79%)	55 (21.56%)
25 - 34	32 (55.17%)	101(51.26%)	133(52.15%)
35 - 44	08 (13.79%)	43 (21.82%)	51 (20.00%)
45 - 54	02 (03.44%)	08 (04.06%)	10 (03.92%)
55 - 64	00 (00.00%)	04 (02.03%)	04 (01.56%)
Prefer not to answer	00 (00.00%)	02 (01.01%)	02 (00.78%)
Education			
High school degree	04 (06.89%)	17 (08.06%)	21 (08.23%)
College degree	14 (24.13%)	31 (15.73%)	45 (17.64%)
Bachelor's degree	32 (55.17%)	72 (36.54%)	104(40.78%)
Master's degree	07 (12.06%)	57 (28.93%)	64 (25.09%)
Doctorate	01 (01.72%)	18 (09.13%)	19 (07.45%)
Prefer not to answer	00 (00.00%)	02 (01.01%)	02 (00.78%)
Employment status			
Full-time	41(70.68%)	146(74.11%)	187 (73.33%)
Part-time	03 (05.17%)	20 (10.15%)	23 (09.01%)
Unemployed	04 (06.89%)	08 (04.06%)	12 (04.70%)
Uncompensated	01 (01.72%)	06 (03.04%)	07 (02.74%)
Student	08 (13.79%)	10 (05.07%)	18 (07.05%)
Retired	00 (00.00%)	02 (01.01%)	02 (00.78%)
Other	00 (00.00%)	01 (00.51%)	01 (00.39%)
Prefer not to answer	01 (01.72%)	04 (02.03%)	05 (01.96%)
Background in IT			
Yes	12 (20.68%)	108(54.82%)	120 (47.05%)
No	46 (79.31%)	84 (42.63%)	130 (50.98%)
Prefer not to answer	00 (00.00%)	05 (02.53%)	05 (01.96%)

Table 4: U, p values for the Mann-Whitney U test. In the table we only present the variables that have significant p-values. The mean values for Newbie and Non-newbie groups are also presented.

Variable	U	p-value	μ-Newbie	μ-NonNewbie
Number of years	8619	7.40e-10 ***	1.43	2.34
% of savings invested	7992	7.50e-07***	16	32.7
Background in IT	8456	4.24e-10***	0.20	1.12
Usage - Trading	7541	1.90e-05***	0.25	0.57
Familiarity- Wallet				
Paper	7575	0.0001***	2.15	2.98
Exchange	8575	2.48e-09***	2.44	3.71
Desktop/Mobile	8161	2.61e-07***	2.93	3.90
Hardware	8962	1.78e-11***	1.87	3.24
Multisig	8121	2.73e-07***	1.44	2.38
Threshold	8033	4.46e-07***	1.34	2.14

Significance codes: $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

Table 5: p-values for the Mann-Whitney U test for 3 group classification — Newbie, Trader and Techie. In the table we only present the variables that had significant p-values for Newbie-Non newbie classification (in Table 4).

Variable	Newbie-Trader	Trader-Techie	Techie-Newbie
Number of years	9.12e-10***	0.4535	7.20e-05***
% of savings invested	2.90e-07***	0.1216	0.0152*
Background in IT	3.53e-09***	0.0177*	4.37e-05***
Usage - Trading	7.15e-06***	0.1250	0.0768
Familiarity- Wallet			
Paper	0.00016***	0.8471	0.0093**
Exchange	2.21e-09***	0.8114	0.00068***
Desktop/Mobile	7.40e-08***	0.0766	0.0370*
Hardware	3.22e-11***	0.9900	1.69e-05***
Multisig	1.39e-07***	0.3980	0.0059**
Threshold	2.51e-07***	0.2068	0.0043**

Significance codes: $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

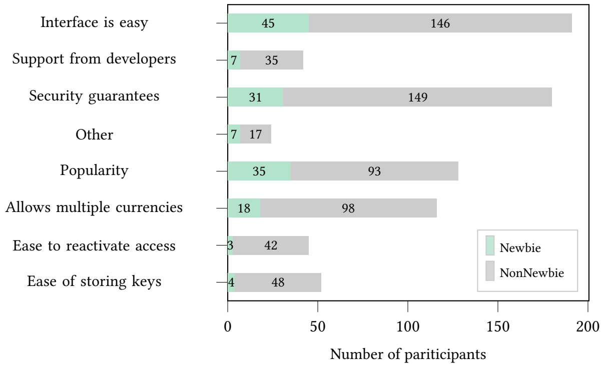


Figure 9: Reasons for choosing the most used crypto-wallets by the participants.

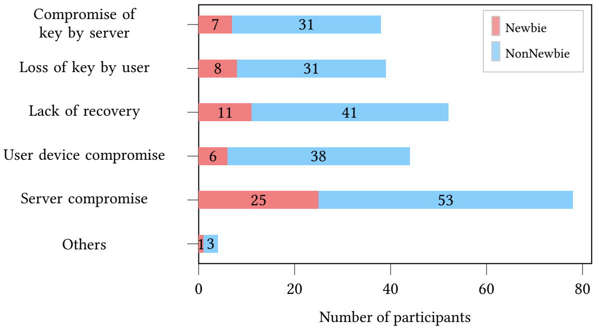


Figure 10: Biggest security concern of the participants when using a crypto-wallet.

B PREFERRED SETTINGS UNDER DIFFERENT GOVERNMENT CHARACTERISTICS

Settings for single-device wallets. For the single-device scenario, as long as the government can not block access to the server data, more than 56% of the Newbie group was willing to place the secret

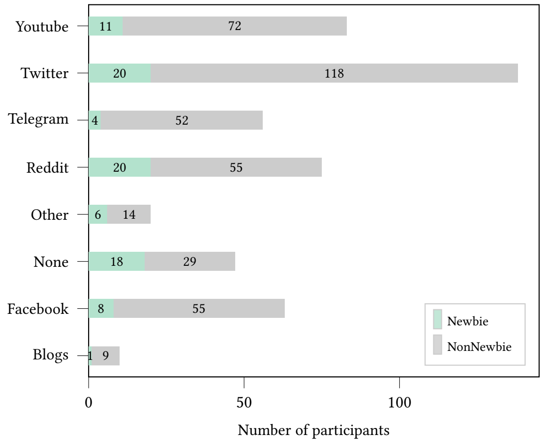


Figure 11: Followed social media for knowledge and information regarding crypto-wallets.

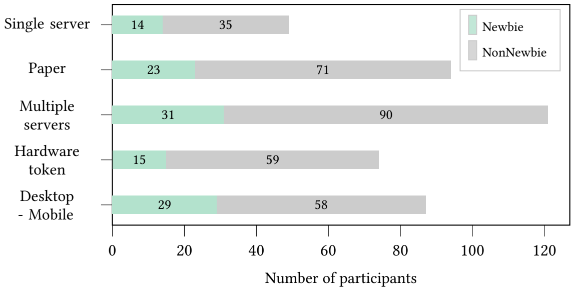


Figure 12: Key storage location preference under client device compromise scenario.

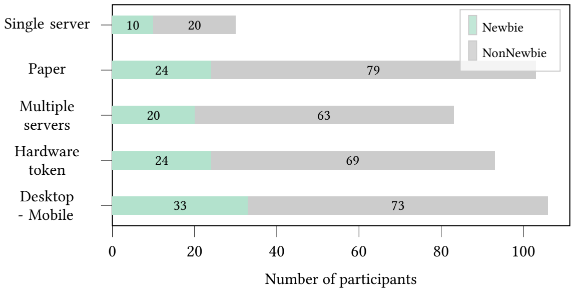


Figure 13: Key storage location preference under remote server compromise scenario.

information on multiple servers. However, when the government can deny data, this percentage is less than 36%. Among the Non-newbie group, when the government cannot view and deny data, 60.9% of participants were willing to place the secret shares on multiple servers while this drops to 41.6% when the government can view and deny data to the clients (see Figure 15). The p-value of 0.013 in the χ^2 test shows significant correlation of responses against the government characteristics.

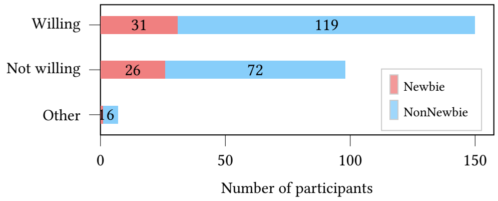
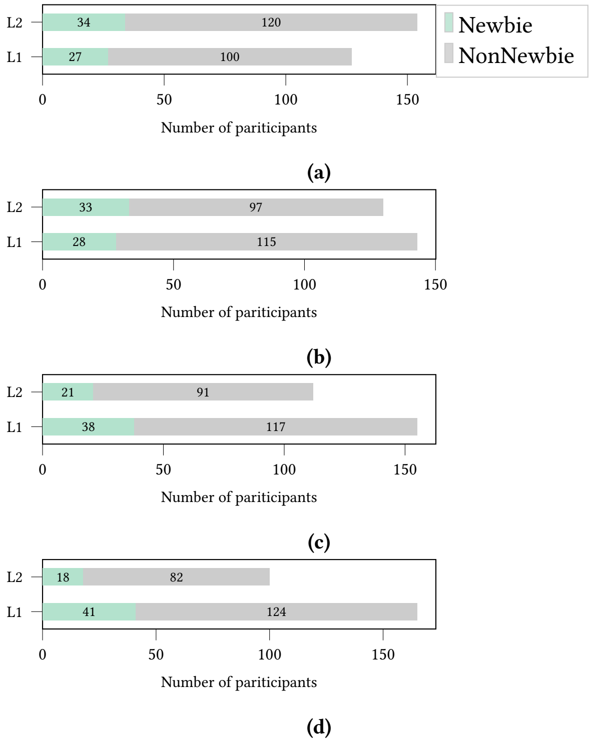


Figure 14: Willingness to increase T for a fixed N in a (N, T) multi-device wallet. It shows willingness of participants to distribute trust among higher (threshold) number of nodes.



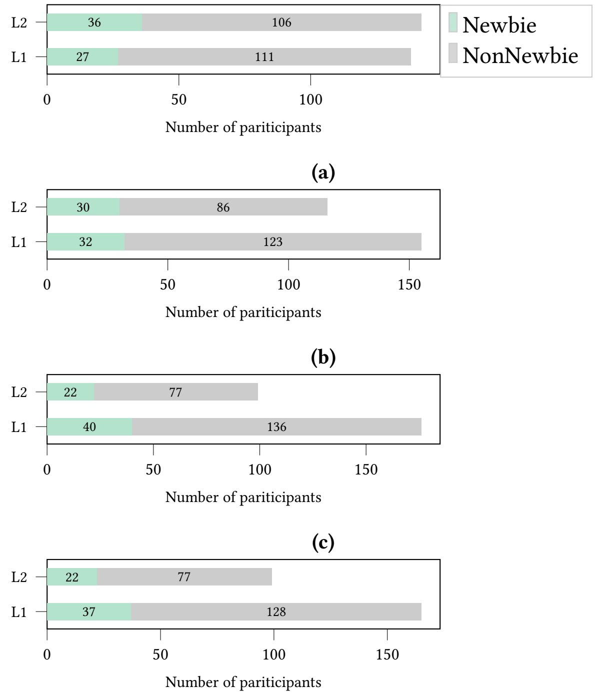
(a)

(b)

(c)

(d)

Figure 15: Single device wallet – user key location preference under different government characteristics regarding capabilities to view or deny access to secret (key) information. (a) Govt. can neither view nor deny access (b) Govt. can view but not deny access (c) Govt. can not view but can deny access (d) Govt. can both view and deny access. L2 - The key is on multiple remote servers across different countries (these countries do not share data). L1 -The key is on client desktop/mobile/hardware token.



(a)

(b)

(c)

(d)

Figure 16: Threshold Wallet – user key location preference under different government characteristics regarding capabilities to view or deny access to secret (key) information. (a) Govt. can neither view nor deny access (b) Govt. can view but not deny access (c) Govt. can not view but can deny access (d) Govt. can both view and deny access. L2 - Threshold-share the key among multiple servers. L1 - Divide the key into two parts. Place one part on the client-device. Threshold-share the other part among multiple-servers.

C 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 ○ 1-2 years ○ 2-4 years ○ > 4 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 crypto currency wallets? It tries to understand your preferences regarding usage and security models in wallets. You will be compensated appropriately.
○ Yes ○ No

D 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.

Section 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 ○1-2 years ○2-4 years ○ > 4 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 □ As an alternative to fiat/government issued currency - for daily 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.
□ Coinbase □ Electrum □ Ledger □ Trezor □ Metamask □ Exodus □ Mist □ Mycelium □ Bitso □ Binance □ Crypto.com □ Luno □ Robinhood □ 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 reactivate an access □ It is popular □ Other □

Q6: Do you follow any blogs/social media forums for learning about wallets? If yes, choose all the appropriate ones. If applicable please also tell us which blogs you do follow.
□ Twitter □ Reddit □ Telegram □ Facebook □ Youtube □ Quora □ Blogs □ None □ Other □ □ Other □

Q7: Did you choose your wallet solely based on ratings of the wallet from a crowd sourced platform like Play Store / AppStore / Reddit etc?
○ Yes ○ No

Q8: Did you choose your wallet solely based on reviews from a famous personality. If yes, kindly provide the name(s) of the personality(ies).
○ Yes □ ○ No

Q9: How important are ratings or reviews of the wallet when you choose?
○ Very important ○ Slightly important ○ Not at all important

Q10: 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.

Q11: Which one(s) did you lose?
□ Secret Key □ Password to the the interface

Q12: 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 □

Q13: Is it likely you might lose your wallet funds in the future?
○ Yes ○ No
If 'No' is selected skip to Q15.

Q14: Is there any reason that you are afraid of, regarding the future loss of wallet funds? □ Loss of the secret key or password □ A malicious entity/person stealing my funds □ Others □

Q15: Choose your biggest security concern in wallets among the listed ones. You can also add your own concern in the others field. In the choices below, a server is any remote server of a wallet firm on which 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 □

Q16: Kindly choose how far do you agree with the following statements.
Mark each on a Likert scale of 1 (Fully disagree) - 5 (Fully agree).
(a) My crypto wallet is at the risk of being compromised .
(b) The risk of my crypto wallet being compromised is high
(c) It is likely that someone abuses private keys of my crypto-assets
(d) It is likely that someone makes criminal transactions in my account
(e) I am able to protect my private keys from being stolen
(f) I am able to prevent unauthorized access to my crypto wallet
(g) I have technical skills and time to secure and prevent the theft of my crypto-assets
(h) I find it easy to secure my crypto wallet

Q17: How familiar are you with each of the wallet types below.
For each of the wallets below, choose the familiarity a Likert scale of 1 (Not familiar at all) - 5 (Very familiar).
(a) Paper wallet
(b) Exchange wallet
(c) Desktop/Mobile wallet
(d) Hardware wallet
(e) MultiSig wallet
(f) Threshold wallet

Q18: Choose the current month of the year.
○ April ○ December ○ September ○ August ○ March

Section 2 - Preference for different types of wallets and key storage. In this section, we briefly explain different types of in-use wallets today in two short videos. PLEASE WATCH THE TWO SHORT VIDEOS 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.

Q19: Please choose if the following statements are True or False
(a) Consider that you use an Exchange wallet. If the exchange server gets compromised, your funds may be lost.
○ True ○ False
(b) Consider that you use a desktop wallet. Your funds are safe even after the desktop is hacked/compromised.
○ True ○ False
(c) If you use a hardware wallet, anyone with your hardware token can transfer your money (assuming no other authentication is needed).
○ True ○ False

Q20: Please explain why you chose True/False for the above three questions. The questions have been reproduced as rows for your convenience.
(a) Consider that you use an Exchange wallet. If the exchange server gets compromised, your funds may be lost. □
(b) Consider that you use a desktop wallet. Your funds are safe even after the desktop is hacked/compromised. □
(c) If you use a hardware wallet, anyone with your hardware token can transfer your money (assuming no other authentication is needed). □

Q21: An exchange wallet (Eg: Coinbase.com) functions much like a bank account. Any key associated with the wallet is held by the crypto-exchange. Given a choice, where do you prefer the key to be stored?

○ Client device Eg: Phone ○ Remote server of the exchange ○ Copies at both client device and exchange's server ○ The location of storage does not matter ○ I am not sure

Q22: Explain your choice in the previous question in 1-4 sentences. □

Q23: "In a single device wallet, losing the only secret key is the same as forgetting a banking password, in-terms of accessing funds." Do you agree or disagree with the statement ?
○ Agree ○ Disagree ○ I am not sure ○ Other □

Q24: Consider a single device wallet. Which location(s) of key storage is vulnerable to funds being stolen if compromised ? You can choose more than one option.
□ Customer device Eg: Phone □ Remote server □ Hardware token □ I am not sure □ Other □

Q25: Kindly watch a short video on Multi-device wallets. Recall :

(a) Recall that a (N - device, T - threshold) multi-device wallet needs at-least T active devices to authorize the transaction.
(b) In a (N-device, T-threshold) Multi-Sig wallet N different keys are generated and placed on the devices. Signatures are collected and aggregated from any T (or more) of these devices. Anyone can find out the N and T values from the aggregate signature.
(c) In a (N-device, T-threshold) Threshold wallet a single key is divided into N shares and placed on the devices. Signatures are collected and aggregated from any T (or more) of these devices. No one can find out the N and T values from the aggregate signature. Example values for (N,T) are (5,3).

Please choose if the following statements are True or False.

(a) Consider a (4-device, 2-threshold) Threshold wallet. Towards creating a valid signature on a transaction, it is enough to collect signatures from 2 devices.
○ True ○ False
(b) Consider a (3-device, 2-threshold) Multi-Sig wallet with keys placed on Device1, Device2 and Device3. To authorize any transaction, Device3 should ALWAYS provide a signature.
○ True ○ False
(c) Consider a (10-device, 5-threshold) Threshold wallet. From a created/generated (threshold) signature, the threshold value being 5 can be determined/learnt.
○ True ○ False

Q26: Please explain why you chose True/False for the above three questions.The questions have been reproduced as rows for your convenience.

(a) Consider a (4-device, 2-threshold) Threshold wallet. Towards creating a valid signature on a transaction, it is enough to collect signatures from 2 devices. □
(b) Consider a (3-device, 2-threshold) Multi-Sig wallet with keys placed on Device1, Device2 and Device3. To authorize any transaction, Device3 should ALWAYS provide a signature. □
(c) Consider a (10-device, 5-threshold) Threshold wallet. From a created/generated (threshold) signature, the threshold value being 5 can be determined/learnt. □

Q27: Given a choice between single-device and multi-device wallets, which one do you prefer over the other ?
○ Multi-device wallets considering device/key storage compromise attacks in single-device wallets ○ Single-device wallets because I trust that the storage location will not get compromised easily ○ I prefer not to use any wallet, I want to control the entire key and do not want other entities holding my key ○ Other □

Q28: If you are currently using a single-device wallet, will you be willing to shift to a multi-device scheme if your current wallet provides it?
○ Yes ○ No ○ Not Applicable

Q29: Explain your choice in the previous question in 1-3 sentences. □

Q30: Recall that a (N - device, T - threshold) multi-device wallet needs at-least T active devices to authorize the transaction. Consider the N devices to be remote servers. For the given settings below, which one are you most comfortable with regarding safety of your funds? The N and T values presented here have been chosen randomly for a hypothetical scenario and do not pertain to any real deployment.
○ (10 - servers, 5 - threshold) wallet with servers hosted by well known reputed firms ○ (100 - servers, 5 - threshold) wallet with the servers chosen randomly across globe ○ (100 - servers, 50 - threshold) wallet with the servers chosen randomly across globe ○ Other setting □

Q31: Please briefly explain your choice in the previous question (1–3 sentences) □

Q32: Recall that in a (N - device, T - threshold) MultiSig wallet, any T or more customers/clients need to sign the transaction for it to be valid. Considering a (N - device, T - threshold) MultiSig wallet (for example N = 7, T = 2) will you be comfortable increasing the value of T i.e., increasing the number of clients that need to sign?
○ Yes - because I like to distribute trust among more devices/people ○ No - because for higher T, I need to collect more signatures ○ Other □

Q33: Recall:

(a) In a MultiSig wallet N different keys are generated and placed on the servers such that any T or more can be used to authenticate. N and T values can be found out from the aggregate signature

(b) In a Threshold wallet a single key is divided into N shares and placed on the servers such that any T or more can be used to authenticate. N and T values can not be found out from the aggregate signature

Given a choice between an (N-device, T-threshold) MultiSig and (N-device, T-threshold) Threshold wallets, which one would you prefer?
○ MultiSig wallet ○ Threshold wallet ○ Can not say

Q34: Explain your choice in the previous question in 1-3 sentences □

Section 3 - Desired preferences for different settings of crypto - wallets. Recall that the secret key of a wallet may be stored in a variety of locations including mobile phone, desktop etc on the client side or one or more servers at the wallet firm. The servers hosting the client's key may be located in different countries which apply a variety of privacy law on the content hosted by the servers. Now we ask you questions regarding your preferences for wallet settings which cover different client-server share distributions, threats from attackers and locations of servers supporting the crypto-wallets.

Single-device Wallet :

Q35: Imagine you are given an option to use a single-device wallet. Recall that they include desktop/mobile, paper, cold and hardware wallets. Considering that the *client (your) devices can be compromised*, which location(s) would you choose for your key. You can choose more than one option.
□ Client desktop or mobile □ Client hardware token □ Paper □ Single remote server □ Multiple remote servers (each storing the key)

Q36: Considering that the remote servers can be compromised, which location(s) would you choose for your key. You can choose more than one option.
□ Client desktop or mobile □ Client hardware token □ Paper □ Single remote server □ Multiple remote servers (each storing the key)

Q37: The wallet firm may host their servers in different countries with different privacy laws and characteristics. For the given government characteristics (as rows), which client-server share distribution setting would you choose.

(a) Govt. can neither view nor block access to server data in its jurisdiction
□ The key is on client desktop/mobile/hardware token. □ The key is on multiple remote servers across different countries (these countries do not share data)

(b) Govt. can view the server data but can not block access to server data in its jurisdiction
□ The key is on client desktop/mobile/hardware token. □ The key is on multiple remote servers across different countries (these countries do not share data)

(c) Govt. can not view but can block access to server data in its jurisdiction
□ The key is on client desktop/mobile/hardware token. □ The key is on multiple remote servers across different countries (these countries do not share data)

(d) Govt. can view and can block access to server data in its jurisdiction
□ The key is on client desktop/mobile/hardware token. □ The key is on multiple remote servers across different countries (these countries do not share data)

Multi-device Wallet :. Imagine you are given an option to use a Multi-device wallet. Recall that for a (N - device, T - threshold) setting, at least T devices should co-operate or sign the transaction for it to be valid. Multi-device wallets include MultiSig wallets and Threshold wallets. In the text below, threshold-sharing a key implies dividing a key into N parts such that any T of them can be used to authenticate.

Q38: Each row in the table below corresponds to a different client-server share distribution setting of a Threshold wallet. Considering that the *remote servers can collude* with one another, which setting(s) would you choose for your wallet. You can choose more than one option.
□ Threshold-share the key among multiple servers □ Threshold-share the key among multiple servers and the client-device. □ Threshold-share the key among multiple client-devices. □ Divide the key into two parts. Place one part on the client.-device Threshold-share the other part among multiple servers. □ Divide the key into two parts. Place one part on the server. Threshold-share the other part among multiple client-devices.

Q39: Consider a (N-device, T-threshold) Threshold wallet. Let the devices be all remote servers. The wallet firm may host their servers in different countries with different privacy laws and characteristics. For the given government characteristics (as rows), which client-server share distribution setting would you choose. Multiple servers indicates servers located across different countries that do not share data with each other.

(a) Govt. can neither view nor block access to server data in its jurisdiction
□ Threshold-share the key among multiple servers □ Divide the key into two parts. Place one part on the client-device. Threshold-share the other part among multiple-servers.

(b) Govt. can view the server data but can not block access to server data in its jurisdiction
□ Threshold-share the key among multiple servers □ Divide the key into two parts. Place one part on the client-device. Threshold-share the other part among multiple-servers.

(c) Govt. can not view but can block access to server data in its jurisdiction
□ Threshold-share the key among multiple servers □ Divide the key into two parts. Place one part on the client-device. Threshold-share the other part among multiple-servers.

(d) Govt. can view and can block access to server data in its jurisdiction
□ Threshold-share the key among multiple servers □ Divide the key into two parts. Place one part on the client-device. Threshold-share the other part among multiple-servers.

Section 4 : Demographics. In these final set of questions, we will ask you about your demographic details.

Q40: 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

Q41: Which gender do you identify with ?
○ Male ○ Female ○ Others ○ Prefer not to answer

Q42: 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

Q43: 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

Q44: 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

Q45: 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 a avenue for trade, buying and selling cryptocurrencies ○ I am a newbie, started using them for the fear of missing out the crypto boom