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

Easwar Vivek Mangipudi
Supra Research
e.mangipudi@supraoracles.com

Udit Desai
IIT Kharagpur
uditdesai2206@gmail.com

Mohsen Minaei
Visa Research
mominaei@visa.com

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

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

ABSTRACT

Cryptocurrency users saw a sharp increase in different types of crypto wallets in the past decade. However, the emerging multi-device wallets, even with improved security guarantees over their single-device counterparts, are yet to receive proportionate adoption. This work presents a data-driven investigation into the perceptions of users towards multi-device wallets, using a survey of 357 crypto-wallet users. Our results revealed two significant groups among our participants—Newbies and Non-newbies. Our follow-up qualitative analysis, after educating revealed a gap between the mental model for these participants and actual security guarantees. Furthermore, we investigated preferred default settings for crypto-wallets across our participants over different key-share distribution settings of multi-device wallets—the threat model considerations affected user preferences, signifying a need for contextualizing default settings. We identified concrete, actionable design avenues for future multi-device wallet developers to improve adoption.

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**.

KEYWORDS

Cryptocurrency wallets, security, usability, multi-device wallets.

ACM Reference Format:
Easwar Vivek Mangipudi, Udit Desai, Mohsen Minaei, Mainack Mondal, and Aniket Kate. 2023. Uncovering Impact of Mental Models towards Adoption of Multi-device Crypto-Wallets. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS '23), November 26–30, 2023, Copenhagen, Denmark.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3576915.3623218

1 INTRODUCTION

The cryptocurrency boom has seen millions of people adopting digital assets; the recent economic successes [27, 29, 32] have enthused a broad population to explore them. 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[1] (or crypto-wallet) such as Coinbase [4, 5] and Binance [1, 3] indicate higher popularity of wallets that seem (cryptographically) weaker in the security model they offer. This popularity might be for reasons ranging from people trusting the wallet firms, and opting for wallets based on popular opinions to different security attitudes. These variations in knowledge, understanding of security models, and risk perception may also significantly affect the choice of wallets.

Recent studies [55, 59, 67, 74, 97] attempted to understand usability and challenges while performing transactions with crypto-wallets in use. They analyze the wallets using cognitive walk-through [53] and also study the common misconceptions by the users regarding the role of wallet firm [97]. The majority of prior research has concentrated on evaluating the *usability* and comprehension of conventional single-device wallets in use. There has been a lack of investigation into the emerging (and arguably more secure [54]) *multi-device wallets*. Specifically, there has been no exploration of users' mental models regarding the security and key management of multi-device wallets, which can be essential for comprehending the obstacles impeding 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. The single device wallets carry significant risk of key-compromise and loss of keys by the users through misplacement etc. It is estimated that roughly 4 million bitcoins (accounting for ∼20% of all mined bitcoins) were lost [8] through users losing access to their keys. On the other hand, storing the keys at exchanges (single device exchange wallets) creates single points of failure for large-scale thefts [9, 25, 28]. Roughly $2.6 Billion worth of cryptocurrency has been stolen since 2012 [28] from the exchanges through hacks. Owing to these increasing risks of key-compromise attacks [35, 95] and exchange hacks [9, 25, 28] on single-device wallets, one may expect a greater enthusiasm for the new and emerging multi-device wallets (e.g., Torus wallet [16], ZenGo [18]) which significantly mitigate these issues. However, in adoption,

[1] A cryptocurrency wallet is an app that allows cryptocurrency users to store and retrieve digital assets. They typically involve guarding an associated secret key with the assets.

CCS '23, November 26–30, 2023, Copenhagen, Denmark

ACM ISBN 979-8-4007-0050-7/23/11…$15.00
https://doi.org/10.1145/3576915.3623218

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? And, if the users are educated about the pitfalls of single-device wallets and the security advantages of the multi-device wallets and even provided a positive nudge, will the users opt for multi-device wallets (based on security)? Here, 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. The study is also the first to consider distributed cryptography [12, 48] – specifically, architectures for threshold and multi-sig signatures and their usability along with user preferences in wallets. Specifically, we conducted a survey-based study of 357 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 about their current cryptocurrency wallets, their usage, and 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 (self-reported by participants as presented in Section 5.1.1), 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 80% 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 groups are not very familiar with multi-device wallets.

RQ2: *Provided essential and sufficient information regarding different wallets 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. Our videos explain the basics of both the single-device and multi-device wallets. After the videos and knowledge check, we collected the preferences and feedback if the participants were willing to adopt multi-device wallets. Slightly less than 40% of all participants were unwilling to shift to multi-device wallets, though 54.7% of participants mentioned they were ready to shift.

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. 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. 60.8% of the participants preferred a small number of reputed servers compared to 34.6% 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.

The results and the answers to these questions offer interesting insights into the users' preferences and their implications to the developers. The existence of two definite groups with different experiences and utility indicates that both groups need to be educated and convinced by the developers using different approaches. It has been observed that both the groups, though having different usage requirements from the wallets, lack high familiarity with multi-device wallets. They can be educated to acknowledge that diverse requirements can be met, including ease of usage (typically by keeping multiple key shares on servers) or a high level of control (by placing key shares on multiple user devices). This can be done aside from explaining the security issues associated with single-device wallets, which multi-device wallets can address. Our results offer a few interesting insights and novel research directions for the threshold/distributed cryptography research and, specifically, signature scheme design itself.

Our participants desired far more control over their keys even while using multi-device wallets; future research can focus on models achieving the same—wallet architecture models that arise out of this are significantly different from traditional models adopted by the community and hence can be an area of study. The researchers should also consider more general adversary and access structures for multi-device wallets; however, the current distributed cryptographic systems literature and practice are pretty thin beyond the standard $(T-1)$-out-of-N adversary. The researchers may look into different weighted threshold structures where few devices are more trusted than others. The participants also identified a privacy-accountability trade-off between existing types of multi-device wallets, which presents an exciting research challenge.

Mental model of users: This work attempts to uncover *Mental model* of users for crypto-currency wallets. Wash et al. [98] defined a mental model as a "simplified representation of reality that allows people to interact with the world". Similarly, by 'mental model', we mean simplified rules of users about the security guarantees of cryptocurrency wallets. This work does not aim to uncover mental models about *how* cryptocurrency wallets work—which might necessitate interviews and drawing tasks (to uncover data flows). Rather we focus on how users, in their simplified understanding, perceive security properties offered by these systems and the resulting preferences. Previous works [64, 75, 76] leveraged similar surveys to uncover mental models. We are now set to classify crypto-wallets before uncovering users' mental models.

2 CLASSIFYING WALLETS

All cryptocurrency wallets today use paired secret keys and public keys [36, 69], 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 wallets to another.

Existing classifications of the cryptocurrency wallets. Several classes [26, 30, 46] of cryptocurrency wallets exist today depending on different dimensions—*hot and cold* wallets, *custodial and non-custodial* wallets [30, 55] etc. Hot wallets are connected to the internet, while cold wallets are not. To perform a transaction with a 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 wallets are notorious for loss or misplacement of keys and subsequent loss of funds—~20% of all mined bitcoin are lost this way [8]. In contrast, *custodial wallets* refer to ones where the secret key is not at the user (device) but at the firm that 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 the key at the user, it forces the user to trust the firm operating the wallet. A popular 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 [9, 20–22, 25, 28, 73]. Thus, it is quite evident that storing the keys at a single location is a security risk, irrespective of the user (client-side) or the firm (server-side). A relatively new type of wallet, which we call multi-device wallet, solves these issues—it distributes the secret keys into multiple shares [12, 94] and places them at different locations. These locations can be a combination of different firms/servers and devices owned by a single or multiple users.

Need for new security-focused classification. Note that the existing classifications 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 presented cases, whether at the user or the server, compromising the single key location compromises the funds; the multi-device wallets mitigate this security risk [54]. 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 wallets which is invariably related to the key location, we classify all the wallets into *single-device* and *multi-device* wallets.

2.1 Single- and Multi-device wallets

Single-device wallets store the keys at a single location, either on 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 shared across 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.

Security. In a single-device wallet, since the key is in a single location, it introduces a single point of failure. Loss of keys by the users and exchange hacks [8, 9, 20–22, 25, 28, 73] show that these wallets are highly vulnerable. In a multi-device wallet, since the key is distributed, the attackers need to compromise multiple devices/servers simultaneously to compromise the keys. Hence they are less prone to key loss or compromise.

Recently, Eyal [54] has shown that for a wallet, an increase in the number of associated heterogeneous keys improves security; the probability of users losing access and adversaries gaining access is lower for multi-device (multi-key) wallets. Hence, multi-device wallets are more *secure* than their single-device counterparts. Several different approaches [37, 54, 68, 81] 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. 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.

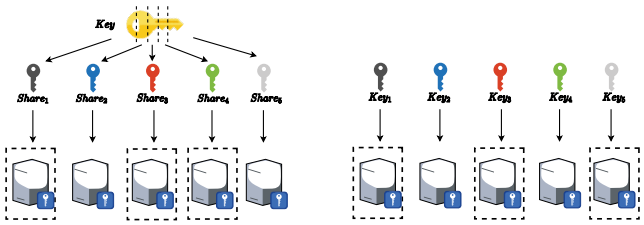
Trust and Usability. The trust and usability aspects of the wallets are more nuanced. For single-device wallets, the users need to trust the single location not to get compromised for the safety of their funds. For multi-device wallets, users need not trust a single entity like in exchange wallets since the secret information is distributed. Naturally, owing to this, they 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 [68] similar to the 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, in a scenario when the key is divided into two shares and one of the shares is placed on the client device, 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 [97], like participants' confusion regarding transaction and mining fees, cancellation of transactions, and lack of blockchain transparency regarding the transaction state is likely to be common between both single-device and multi-device wallets since they are not dependent on the location of the key. While this work focuses on the security model of different wallets and the users' perception, we uncover interesting mental models regarding usability aspects; the perceptions of usability affect the preferred settings (see 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 [23, 31, 51], N different keys are generated and placed on N devices such that signatures [39, 41, 71] from at least T devices are needed



(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.

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 on the board of a firm such that at least a subset of them need to provide the signature for the 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) distribute the secret information 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[14, 24], a single key is *secret-shared* [38, 91] among N devices out of which T or more provide a partial signature. The partial signatures are collected and aggregated into a single (threshold) signature [41, 63] to authorize the transaction. The signature generated as a threshold signature does not reveal [17, 63] the underlying access structure among the clients or which parties have signed. A threshold signature is similar to a single regular signature, unlike multisig, which is a concatenation of multiple signatures, so it offers better storage efficiency.

3 RELATED WORK

3.1 Usability and security of crypto-wallets

Many recent studies [10, 55, 59, 67, 96, 97] have focused on usability issues of cryptocurrency systems. Recently, Mai et al. [79] brought out the general misconceptions of users in using cryptocurrency systems regarding keys, anonymity, and fees. They investigate misconceptions about the generation of cryptographic keys, which may lead to their mishandling and loss of funds. Voskobojnikov et al. [96] 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. They observed that some non-users (non-crypto wallet users) are concerned that governments can trace the transactions back to them (loss of pseudonymity/anonymity). In contrast, we consider only participants who have used crypto-wallets. We aim to understand their preferences, e.g., under different government policy and capability scenarios where they can access or block the secret keys.

Usability. Blockchains and cryptocurrencies suffer from entry barriers and the perception of usability between users and non-users [59, 67, 96]. Voskobojnikov et al. [97] study the user experience of wallets by analyzing the ($> 45K$) ratings of famous cryptocurrency wallet applications. They reveal that users have several misconceptions regarding the features and interface, including how mining and transaction fees are collected, leading to grave errors in handling the secret keys and currency transfers. They [97] briefly observed that some of the users preferred access to the secret keys (like in iOS Apple devices) compared to custodial wallet settings. Furthermore, some of their participants were also concerned about losing the device and the secret keys. In contrast, we explore how participants wish to overcome such concerns if they wish to shift to multi-device wallets. For the multi-device wallets, we explore and understand user preferences among the varied settings offered by multi-device wallets differing in the levels of control, availability, and security of secret keys. In fact, our user study is the first of its kind for multi-party computation (MPC) or threshold cryptography.

Krombholz et al. [74] 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. [10] studied the usability problems in using crypto-wallets while achieving privacy through Tor and VPNs. They identify that most users find it difficult to set up wallets and integrate with anonymization tools . Frohlich et al. [55] 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. Abramova et al. [33] classified all the crypto-wallet users into three groups cypherpunks, hodlers, and rookies in a survey performed in 2020. 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. However, in this work, we analyze and observe that the participants behave as two groups - Newbies and Non-newbies in contrast with the previously observed three groups. These two groups are identified with self-reported segregation and have strong correlations among the different responses to the survey.

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.

Security and Privacy issues. Frolich et al. [56] presented a systematic overview of different threats faced by cryptocurrency users—accidental, privacy, physical, financial fraud, social, and technical threats. Among the physical threats, they observe the loss of cryptocurrency as a potential threat. As a possible countermeasure, they suggested backup mnemonics—divided and stored as separate parts on multiple devices. Furthermore, Ghesmati et al. [65] studied the privacy perceptions of (12 cryptocurrency users and 58 non-cryptocurrency users) about blockchains. They evaluated user perceptions about anonymity, privacy, and users' mitigation measures. They found that privacy concerns for a few of 12 users

were about exchanges having access to the secret information of the wallets and also exchange hacks. The authors observed that a majority of their participants preferred to use privacy coins with additional tools like CoinJoin, CoinSwap [57, 58, 88, 89]. Our work builds on and is complementary to these prior works—instead of threats and privacy-enhancing systems, we focus on (mis) conceptions about key management as well as user preferences regarding key management for better-perceived security of crypto-assets.

3.2 Key management in wallets

While passwords are used by many cryptocurrency wallets [1, 2, 4, 11, 15], the underlying cryptosystem authentication is through public-key cryptography using secret-key, public-key pairs. Usability issues of public-key cryptography in encrypted e-mail have been studied [60, 61, 92] 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. [53] conducted a cognitive walk-through of bitcoin applications, uncovered shortcomings, and provided a framework to evaluate such key management systems.
Vulnerabilities in wallets. Single devices wallets are vulnerable to several attacks; Vasek et al. [95] 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. [35] 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. [44] 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 secret information among many devices, they still can be vulnerable to attacks. Aumasson and Shlomovits [24] show ways to attack the implementations of schemes like threshold-ECDSA [62, 77].

Several works [45, 81, 87] 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. [45] suggest storing the seed of the secret key in a trusted part of the hardware such that no adversary can access it. Barber et al. [37] 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 [87] propose a deterministic sub wallet key generation from the super wallet seed. Marcedone et al. [81] proposed a two-factor signature generation mechanism in hardware wallets to be secure against malicious hardware vendors. He et al. [68] 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 [37, 54, 68, 81] 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.

Summary: Previous works [10, 53, 55, 59, 67, 74, 79, 96, 97] studied usability issues and challenges of cryptocurrency systems and wallets, including misconceptions regarding keys, anonymity, and fees, among users and non-users. They studied security practices, brought out perceptions in the usage of bitcoin wallets and clustered users into groups (depending on factors like perceived self-efficacy, etc.), and provided a framework to evaluate key management systems. They also study the different threats cryptocurrency users face and their privacy perceptions. Multiple works [35, 44, 45, 62, 81, 87, 95] study the vulnerabilities of wallets and some suggest multi-device wallets [37, 54, 68, 81] for mitigation of the attacks.

This work goes beyond, studying the participants who are already crypto-wallet users, and their preferences about key management for the security of their assets. We specifically educate the users about multi-device wallets and study their preferences about single-device and multi-device wallets, for different possible multi-device wallet settings and their reasons for shifting or not shifting to multi-device wallets. We also study their preferences under different government policy scenarios.

4 METHODOLOGY

4.1 Survey instrument

Our survey instrument had two parts. We asked questions regarding users' experiences with different crypto-wallets in part I. 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 them. We describe our full survey instrument in [80, Appendix F] . In our mixed-methods study, similar to Owens et al. [83], quantitative approaches uncovered user behavior, and qualitative methods uncovered mental models.
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 used by the participants 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, and 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 crypto-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 [33]. Finally, we asked the participants 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[2] discussed different

[2]Can be found at https://youtu.be/at5OHPYrc48

single-device wallets and their pros and cons. The second video[3] showed how multi-device wallets mitigate the single-device wallets problems and discussed the two multi-device types —threshold and multisig wallets. These videos have been designed after an extensive literature survey [6, 10, 17, 23, 26, 30, 31, 45, 46, 54, 68, 81, 87, 97] on different types of available wallets. The videos crisply explain the different types of wallets, their architectures, and the different devices that can be used to hold the keys for the wallets. Through the videos, we also explain the security issues of the wallets. For the multi-device wallets, we further explain the sub-categorization of multisig and threshold wallets and the privacy differences. We mention how the architectures can vary based on security requirements while being careful not to bias the users towards any specific architecture. Finally, we also mention the usability issues that may arise out of multi-device wallets. We present information that will let the participants think about and understand the security risks of the different settings of the wallets. Informing the participants 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 the multi-device wallets (see 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 their preferred settings. After showing the videos, first, we asked about 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 then 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 developer provided it. We also asked which one they prefer between threshold and multisig wallets and why.

To understand the participants' preferred settings for the multi-device wallets, we asked them to choose among three different settings (see Section 5.3, Figure 4) with a varied number 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 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 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 were 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 preferred settings for the multi-device wallets, including server setup under various government policies. Finally, we also included two questions on usability asking the participants if the single and multi-device wallets meet their usability needs and what they expect from these wallets.

[3]Can be found at https://youtu.be/4zx9loYQwYY

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 with six participants to test the comprehensibility of the 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 that asked to rank provided options—we converted 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 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 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 and enables us to uncover interesting user behaviors and attitudes using statistical analysis. However, one key challenge of our recruitment was to target crypto-wallet users and enthusiasts. To that end, following the approach of Abramova et al., [33], we recruited participants from the crowdsourcing platform Prolific.co. We recruited participants who have been using single-device and multi-device wallets; we do not restrict this study to only multi-device wallet users since we study the preferences of both single-device and multi-device wallet users and if single-device wallet users are willing to migrate to multi-device wallets. Restricting to only multi-device wallet users would not have been sufficient for our purpose.

Recruitment from Prolific: For Prolific, we chose participants from the US, UK[4], and Canada. We ensured that they had not taken our pilot studies. We selected them using a screening survey conducted before the entire 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

[4]Over 65% of the participants on Prolific are from the US and UK [13] who speak English and more than 18 years of age

instrument in [80, Appendix E]) . 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 on Prolific.co in multiple batches of $30-50$ participants on various days and times over one week. We did this for the distribution to counter any anomalous time dependencies due to the effect of events occurring at a specific time [34]. The median time of completion of the survey was 22 minutes, and the compensation was 4$ for each participant (indicating an hourly wage of 10.8$, comparable to prior studies [33]). 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.

Ethical Considerations. Before starting the survey, we informed participants about 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. Participants could abort and return the survey at any time during the study. Any identifying information like email ids, Twitter handles, etc., related to a participant is removed from the collected responses to preserve the participant's anonymity. 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). We consider only those participants who answered at least two out of three correctly in each subset. 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).

Knowledge-test after the videos. Few participants were already familiar with multi-device wallets (evident from "familiarity"-related responses); However, to bring all participants to a similar level of understanding, we developed two educational videos (Section 4.1).

We were careful not to offer any views on the settings of the different types of wallets. Note that a significant number of participants preferred single-device wallets (see Section 5.2) over multi-device wallets even after a positive narrative towards the multi-device wallets through the videos. Our approach, inspired by [66], quantized the utility of the videos with a total of six knowledge-test questions (and accompanying free-text explanations). We establish the validity of the videos in educating the users by comparing the knowledge-test responses of multi-device and single-device wallet users (see [80, Appendix B]).

4.5 Participant Demographics

A total of 524 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 357 valid responses. We present the demographics of our participants in Appendix Table 4. The samples from crowd platforms tend to be representative and workers from the platforms tend to reflect the population's security and privacy attitudes [86]. Thus, although we used a best-effort convenience sample from Prolific, we strongly believe our efforts capture the attitudes of an important part of the cryptocurrency user community.

In total, 70.3% of the participants identified themselves as male and 27.6% as female, while four participants preferred not to answer and two identified as others, indicating a male bias in our sample. Among the different age groups, the $25-34$ age group dominated the total population with 39.6% of the total, followed by the $35-44$ and $18-24$ age groups at 33.2% and 13.1%. 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 [7], with 62.5% of the participants having a Bachelor's degree or higher. While one expects the participants from crowdsourcing platforms like Prolific to be tech-savvy [70], more than half of the participants (58.9%) of our participants reported that they do not have any experience in the information technology field. Our participants are active users of different crypto-wallets, where they invest 29.56% of their savings on average in cryptocurrencies. See [80, Appendix Figure 6] for our participants' crypto-wallet usage pattern. They follow different social media and reputed personalities for ratings and reviews in choosing their wallets, as shown in [80, Appendix Figures 5 and 9] . Overall, a majority of our participants are young, well-educated, and have invested in cryptocurrencies.

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 [82] 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 of the participants. We used the Chi-Squared (χ^2) test [19, 84] for the different responses to all the questions to uncover correlations between groups of participants and their preferences. We also used the Mann-Whitney U test [78] 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 the Mann-Whitney U test are presented in [80, Appendix Table 2] . We used Mann-Whitney U (MWU) on Likert-scale responses and the Chi-squared (χ^2) test for checking the correlation between user groups and categorical preferences. Since the data is not from a normal distribution, we use non-parametric tests. For the analysis of the responses, visually, the

histograms do not show any characteristics of normal distribution. Hence we employ only non-parametric tests. For all the tests, the significance level α was 0.05, which was further adjusted using Bonferroni multiple-testing correction[90].

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 and 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.

The self-identified categories correlated well with the other independent 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 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 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.

Recall that Abramova et al. [33] categorize participants into three categories using multiple factors, of which perceived vulnerability and self-efficacy are significant. A similar investigation of the perceived vulnerability and self-efficacy using the same sets of four questions each, has *not* resulted in the same clustering. In our study, the responses to these questions highly correlate to only two groups, as shown in the extended version [80, Appendix Table 5] .

Initially, we were skeptical about the self-reported groups and classification based on them. However, these two groups significantly correlated with their other independent responses to other questions, indicated by the low p-values (see Tables 1 and 2, and the extended version [80, Table 5]). We categorized the users based on self-identification; however, this division was supported by statistical tests from other independent survey responses—usage, investment, and familiarity. Specifically, responses to the questions which significantly correlated with these two groups are in

Tables 1 and 2 (p-values are with Bonferroni correction). See the extended version [80, Table 5] for the Mann-Whitney U test results for perceived vulnerability and self-efficacy.

The key differences occurred in the usage of the crypto-wallets, the duration, and the purpose of usage viz trading, long-term investment or for collectibles like NFT. They also differ in their self-identification as knowledgeable in cryptographic tools, their background knowledge in information technology (IT), and employment. The other factor differentiating the two groups is familiarity with different wallet types. The groups' perceived vulnerability of their assets and self-efficacy of protecting them are also statistically significantly different.

We note that, Abramova et al. [33] identified three categories within participants from Prolific—cypherpunks, hodlers, and rookies. Whereas this work identified two—newbies and non-newbies. Since there is approximately a three-year gap (including the pandemic) between our and earlier work, this difference might hint at a temporal shift in crypto-wallet user characteristics over time, where the traders and techies show increasingly similar characteristics in terms of knowledge, duration, and usage of crypto-wallets.

Our survey also reveals that participants consider ratings to be important in choosing wallets and the majority of current users are recent adopters (62.5% of the participants started using them only in the last three years); Loss of keys either through server compromise or by the user are among the prominent security concerns of the participants. Social media is a source of knowledge for the participants regarding crypto-wallets, where Twitter, YouTube, and Reddit are among the prominent ones. We present all these results in detail in the extended version [80, Appendix C] .

Table 1: Chi-squared test results for different questions, including demographics for Newbies and Non-newbies. The number of samples is 357. The table only shows the variables that have significant p-values. df is degrees of freedom.

Variable	χ^2	df	p-value
Usage-Number of years	51.6278	3	3.5951e-11***
Usage-Trading	13.4790	1	24.1245e-5***
Usage-Longterm investment	4.0391	1	444.5521e-4*
Usage-NFT Collectibles	8.1084	1	44.0582e-4**
Wallet - Allows multiple currencies	9.7753	1	0.0017**
Wallet - Ease of storing keys	4.4327,	1	0.0352*
Knowledge on crypto mechanisms	35.3055	4	4.0201e-07***
Gender	28.4891	3	2.8671e-06 ***
Employment	16.7803	7	0.0186*
Background in IT	6.5629	2	0.0375*

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

Table 2: 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
Familiarity- Wallet				
Custodial	15532.5	1.8956e-06***	1.19	2.03
Non-custodial	15477.0	2.7011e-06***	1.11	1.91
Threshold	13261.5	0.0373*	0.64	0.94
MultiSig	13871.2	0.0042**	0.58	0.76

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

5.1.2 Most users use single-device wallets. Most of the participants use single-device wallets, including hardware wallets like Trezor (see [80, Appendix - Figure 10]). Coinbase, Metamask and Binance seem to be popular among the Newbie and Non-newbie groups. 66% of all the participants use Coinbase, whereas 39.3% use Metamask and Binance. The participants could enter up to 3 unlisted wallets in the 'Other' fields. The wallets listed by participants varied widely, including, Solar wallet, Guarda, Kraken, Robinhood. See [80, Appendix - Figure 11] for the reasons for choosing the different wallets and the corresponding number of participants. Among the various reasons, the one with the highest number of participants is the ease of use of the interface and the security guarantees offered. The other major factors are popularity, support for transactions in multiple currencies and ease of storing keys.

5.1.3 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 1.9% of all the participants claimed that they are 'very familiar' with the threshold wallet while 49.4% claimed to be "Not-familiar at all". The corresponding percentages for multisig wallets are 3.07%, and 48.6%. The means of familiarity across different wallet types can be found in Table 2. The mean familiarity across all users for the Threshold wallet in Newbie group is 0.64 and for the Non-newbie group is 0.94. The familiarity of the groups with the Multisig wallets is lower at 0.58 and 0.76, respectively. This corroborates with the names of different wallets reported to be used by the participants where single-device wallets dominate and shows that the participants are less familiar with multi-device wallets. While slightly better, the participants are not too familiar with the terms 'custodial' and 'non-custodial' wallets, as evident from the mean values. 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.

Overall, in our survey, we find that users behave in two specific patterns as Newbies and Non-newbies with different usage, investment characteristics, familiarity, and risk perception patterns. This specific behavior of the participants implies that these two groups need to be approached differently to provide them with services and address their requirements. However, neither of the groups is very familiar with the multi-device wallets.

The majority of the participants are recent adopters (< 3 years) and use wallets for long-term investments and tradings. They consider ratings to be important, with at least 72.5% claiming them to be important. They majorly use single-device wallets, with Coinbase, Metamask and Binance being popular among them. Loss of secret key at the user or through server compromise is one of their primary concerns. This behavior of participants indicates the areas to focus on while taking the security models to the users and convincing them of the risks and advantages.

Table 3: Reasons from our open coding and % of participants for their willingness and non-willingness to shift from single-device wallet to multi-device wallet.

	Reasons	%
Not willing	Single-device wallets are more secure	38.8%
	Single-device wallets are simple to use	24.8%
	I do not want to lose control of keys	15.6%
	Other reasons	19.8%
Willing	Multi-device wallets are more secure	79.7%
	Other reasons including availability	20.29%

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, 51.6% of all the participants chose multi-device wallets (see Figure 2a). The majority of participants wished to shift to them if their current firm offered it; at least 51.1% of each group wanted to shift (see Figure 2b). However, the remaining – close to 40% of each group were unwilling to use multi-device wallets even after the nudge through the videos. Table 3 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 between the Newbie and Non-newbie groups and their choices of shifting to multi-device wallets (indicated by high p values in the χ^2 analysis).

Reasons for shifting to multi-device wallets. Most participants who chose 'Yes' opted for it because multi-device wallets offer better security features like overcoming a single point of failure— P98 explained *"Breaking up the attack surface of a wallet is a good idea. This alleviates any single device being compromised and losing the wallet."* 79.7% of participants who chose to shift opted multi-device wallets for better security features (see Table 3). Around 20.2% 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. P140 wrote *"It gives you more options of access to your wallet and less chance of compromise"* In the case of multi-device wallets, the other parties can refresh the shares when a device is compromised. Some participants realized this and shifted to multi-device wallets for easier key recovery.

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

38.8% of the participants who stick to single-device wallets believe they are more secure than the multi-device wallets. They wrote *"A hardware wallet is secure enough for my individual use." (P63), "I prefer the single storage location. One location is easier to secure than multiple ones."(P107).* However, this is a flawed mental model of security since it is shown [54] that multi-device wallets are more

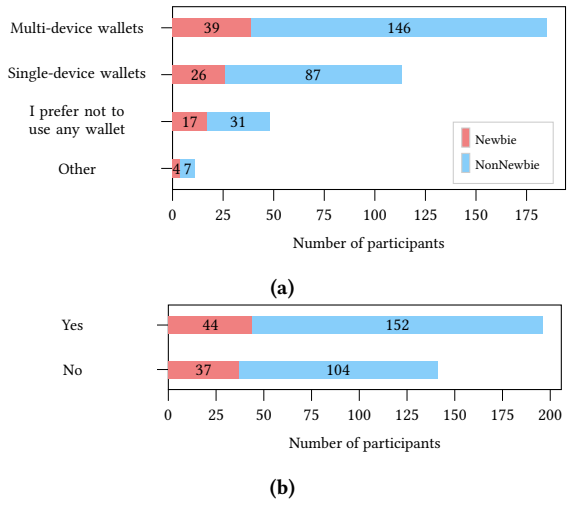


Figure 2: (a) Preference among single-device and multi-device wallets. (b) Willingness to shift to a multi-device wallet from the employed single-device wallet.

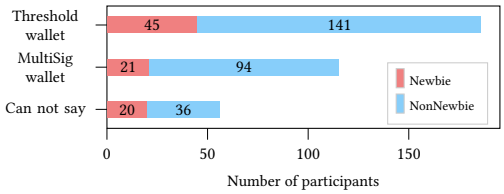


Figure 3: Preference among the multi-device wallets types – threshold and multisig wallets. The majority choose threshold wallets for offered privacy.

secure than single-device wallets. 15.6% participants wish to use single-device wallets since they want to hold on to the key themselves. Few answered, *"I want full control of my wallet/key"P(100), "I am happy to be in control of the key as I believe the risk is low"(P51).* Another participant, P57 preferred single-device wallets for their simplicity; they said *"I like to keep things simple, easy to access and without complexities."*.

While we group the participants choosing "single-device wallets are more secure", we note that users point out two related but separate reasons—"perceived sufficient security of single device wallets" and "perceived insufficient security of multi-device wallets compared to single device wallets." In the data, the second reason is the prominent one. Only four users (1.12%) refused to change to multi-device wallets due to "perceived sufficient security of single device wallets". However, note that in both cases, the mental model of participants unwilling to shift to multi-device wallets and putting keys in a single location for perceived better security is due to misunderstanding the security properties.

In multi-device wallets, devices must interact and aggregate the signature shares to compute the final signature. This may induce some delays and also affect availability. The other reasons included the availability of the keys, trusting themselves, having low funds, hence feeling that single-device wallet was enough etc. We further explore the usability perceptions of participants, including ease of use and if the wallets meet their requirements in [80, Appendix C] .

5.2.2 Users prefer threshold wallets for their privacy. In a threshold wallet, the threshold signature [41] generated to authenticate a transaction does not reveal the access structure, i.e., 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, 52.02% of the Non-newbie group and 52.3% of the Newbie group participants chose the threshold wallet over the multisig wallet as shown in Figure 3. These participants opted for threshold wallets for their privacy properties, like not revealing the access structure. On these lines, P15 commented, *"The fact that the N and T values cannot be found from the aggregate signature seems to add a layer of security. I would want that safeguard feature. It would make me feel more secure."*. 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 by the threshold signature.

34.6% of the Non-newbie group and 24.4% of the Newbie group chose multisig wallets. 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 less than the multisig signature, making it more space-efficient. While this is a technical aspect to grasp, some participants understand this and have opted for a threshold wallet. P232 commented *"I think that threshold wallet has lower transaction fees, cost efficiency is important."*, and P67 wrote *"threshold wallet is more efficient"*.

Participants chose multisig wallets for their simplicity and *because* it reveals the access structure (N, T). P40 commented *"This way, I can know which devices/people were used to provide signatures, so I can confirm with those devices/people if any suspicious activities occur."*. 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 accountability over not knowing who signed.

After familiarizing themselves through the presented videos, more than half 54.7% of participants were willing to shift to multi-device wallets. Among those who wish to use only single-device wallets, 37.5% (wrongly) believe they are more secure. 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's device, no entity can access the key and funds without the 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 wallets for the simplicity and accountability they impose. We further investigate the participants' attitudes 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 the key is preferred over the account compromise risk. 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 'Paper', followed by "Multiple remote servers (each storing the key)". This shows the users' mental model that they seem to trust themselves for holding the key on paper and keeping it safe.

Storing on multiple remote servers can be expected as one would expect users to opt for remote servers under the client compromise scenario. Hosting the key on multiple remote servers increases the availability of the key while also increasing the risk of being compromised. Following this, many participants in both groups opted for client devices, including hardware token and desktop/mobile as the preferred location for client storage (see extended version [Appendix - Figure 12][80]). This indicates that even under vulnerabilities and client device compromise, many wish to retain control over the secret key and thereby the agency over the funds. In the remote server compromise scenario, the three key storage locations chosen by the highest number of participants are paper, hardware token, and client desktop/mobile.

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, we asked the participants to pick among three choices — (i) a smaller number of reputed servers, (ii) a large number of servers with a much lower threshold, (iii) a large number of servers with a high threshold. Here, the threshold would refer to the value of T in (N,T) threshold wallet where the key is distributed among N devices, and any T devices can reconstruct the signature from partial signatures. A smaller number of reputed servers 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 a certain criterion) among many servers across the globe but with a lower threshold. Here the attacker is not sure which servers to attack even though the threshold is small. The last option has a higher threshold, indicating that the attacker must compromise many servers. We deliberately provided options with numbers starkly showing these differences to bring them to participants' attention.

More than 60% of the participants placed their trust in reputation rather than the inability of attackers to compromise a large number of servers distributed across the globe. 59.4% of Non-newbies and 66.2% of Newbies chose a small number of servers ($(10, 5)$ in Figure 4) 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 hosted by well-known reputed firms as they are likely to have stringent security measures to stop any breaches."* Few chose a smaller number of servers since maintaining and keeping track of a large number of them can be a complex task.

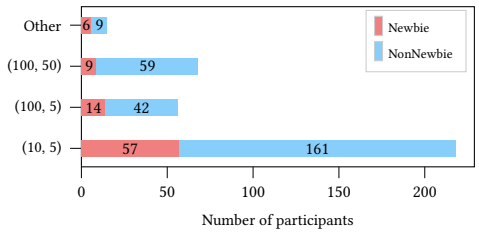


Figure 4: Preferred settings for (N, T) multi-device wallet. N is the total number of devices, and T is the minimum number of devices needed to generate the signature. $(10, 5)$ is with servers hosted by reputed firms. In other settings, servers are chosen randomly across the globe.

Among the parties who opted for choices with more 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, it is also harder to track them down"*. Another interesting aspect is that reputed firms can become centers for targeted attacks by adversaries. Given this one participant, P76 said *"I would prefer randomly chosen servers as they are less likely to be targeted than established companies"* while choosing the $(100, 50)$ setting. The participants who chose a larger number of servers and a 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. When asked if the participants were willing to increase the value of T (implying distributing the trust among more devices/people) for a fixed N, the majority of them opted for it (see the extended version [80, Appendix C] for details). . The participants were allowed to choose the 'Other' option followed by a text response, which we analyzed. Few of them who chose 'Other' indicated they did not wish to simply distribute the secret key among more parties but carefully tailor the threshold for the scenario. The participants prefer a smaller set of reputed servers, and given a choice, they prefer to have a higher threshold in the (N,T) structure of the wallet. This is significant in terms of the choice of default settings for the wallets.

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, the location of the hosted server is significant in terms of privacy and availability of keys to the users. Our survey explores users' preferences for the 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 in two

parts ($Share_1$ 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, when the government can not view or deny access to data, 52.2% of the participants were willing to place the shares only among multiple servers. This percentage decreases to 31.2% when the government can view and deny data. When the government can block access, irrespective of they can view the data, less than 36.5% chose to share among servers, with at least 67.8% choosing to share between the client device and the servers.

In the Non-newbie group, more than 51.1% always wanted to place a share on the client device, which went up to 68.6% when the government could deny access to the data. Thus government policies greatly affect the choice of location for the secret and the majority of users wish to have a share of the key on their devices when the government can deny access.

In short, in our study, most participants wish to retain control over the secret key despite its vulnerabilities. They prefer the keys distributed on a smaller number of servers hosted by reputed firms; they also like to increase the threshold for a fixed number of servers to distribute the trust further. The government's ability to view and block access to the secret affects their choices of key locations.

6 IMPLICATIONS

Our study offers the following valuable insights for different parties involved in the cryptocurrency ecosystem.

Need for educating and nudging the users. Our study shows that participants behave as two specific groups (see Section 5.1.1) Newbies and Non-newbies. These groups mainly defer in the duration of usage (Newbies being recent adopters), the amount of investments they make, their background in Information Technology, and their usage of the cryptocurrency. However, the participants from both groups are not too familiar with multi-device wallets. In reality, placing the key shares on multiple devices owned by multiple users provides an enhanced security feature where a committee or a group of people need to authorize a transaction; single-device wallets do not achieve this. Furthermore, placing the shares on different types of user devices (single user) makes it generally difficult for the adversary to compromise the system since the attacker must adopt different strategies for each device. However, even after educating through the videos, about 30% of the participants were unwilling to shift to multi-device wallets. More surprisingly, about 37% of these participants who were unwilling to shift to multi-device wallets believed that single-device wallets are more secure. About 20.5% of them wanted to stick to single-device wallets because they did not want to lose control over the keys. This flawed mental model needs to be addressed by educating the users about the security features of multi-device wallets. It can also be achieved by nudging the users towards better practices [49, 93] directly in crypto-wallet interfaces. This makes it imperative for the developers to educate and familiarize users with multi-device wallets and the security models that can be achieved and supported through them.

Customizing education and nudges focusing on security and availability trade-offs for different user groups. However, user education needs to be customized for each user group and their needs—different settings of multi-device wallets (with different (N, T) structures and key placements) provide different security and availability trade-offs. For example, a high N and a low T would indicate high availability of the keys, whereas a very high T (close to N) would indicate a higher number of total nodes that need to be compromised to compromise the key thereby implying better security. The users should be conveyed that the multi-device wallets indeed support giving control of the keys to the users while offering the advantage of not having a single key on a single device. The multiple settings under which this is possible, for example, keeping shares on multiple user devices, keeping a share on user devices while further dividing the other set of shares on servers, or further re-sharing the second share among servers, need to be explained. This should be done keeping the user preferences and usage characteristics in mind; the settings can be tuned specifically to each group's requirements and usage characteristics. These are significant because a user investing very little (e.g., newbies) may not want to go through the usage complexity of having the key shares on multiple devices and may prefer to distribute the key among reputed servers and vice-versa. These trade-offs need to be conveyed to the users by educating them (e.g., through blogs, videos, and FAQs) and also using nudges in the interface to help choose a setting that is most aligned with their needs.

Developing new cryptographic schemes for more user control. Since our participants indicated they want control over their keys, the researchers and developers may develop secret sharing schemes where greater weightage is provided to a client device than a server hosting the key. Such schemes would give the client greater control of the total key. This would involve complex access structures with uneven weights. Since no efficient schemes exist for uneven-weighted distributed key generation, the researchers can focus on developing efficient protocols to achieve the same. 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 [12]. The different access structures arising from the user preferences and signature schemes that support them can also be applied to multi-party computation protocols [52, 99]. 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 the keys in the wallets. The current threshold ECDSA protocols [50, 62, 63, 77] cannot securely realize users' control in the above-described setting where one of the two shares is re-shared among the servers.

Designing more usable settings in 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 more usable 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 the threshold wallet ZenGo [18] already follows this pattern with only one server share, while Torus [16] wallet offers no such control

to the users. While having two shares is a representative example, multiple share structures, including hierarchical structures among a subset of shares, are possible. These offer different privacy, security, and usability characteristics. It is important for the wallet firms to choose the proper default settings that cover most user preferences—most users just choose from the default settings [40, 47, 72, 85]. The users consider the location of the servers (see Section 5.3.3), so the wallet firms must also allow the users to choose the servers to host their secret shares.

Multi-device wallet users consider trade-offs of Threshold vs. Multisig wallets. Finally, Threshold and multisig wallets offer interesting trade-offs concerning accountability and privacy—our study shows that multi-device wallet users understand and consider these trade-offs. 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). For example, 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 motivates security researchers toward signature generation and wallet design to offer the best of both worlds, including privacy and accountability. [42, 43] Moreover, as participants are concerned about the space requirements of multi-signatures in wallets (see Section 5.2.2) developing space-efficient multi-signatures is an interesting issue to consider.

7 CONCLUSION

This study brings out a number of interesting behavioral 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 the interface and the popularity of the wallets. The Non-newbie group has relatively been using the crypto-wallets for a longer period; 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; they use their wallets for long-term investments and very little as an alternative to fiat currency. Key compromise is a common threat for both groups.

When educated and nudged about multi-device wallets that can mitigate both the issues of client-device or remote server compromise, most participants are willing to shift. Those who are not, have a false sense of security of single-device wallets. They also 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 government policies at locations where the servers containing secret information are hosted. Finally, the study offers specific insights into the users' expected multi-device wallet threat models. This 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] Bitgo. https://www.bitgo.com/.
[3] Coin ranking - binance exchange. https://coinranking.com/exchange/-zdvbieRdZ%2Bbinance.
[4] Coinbase. http://coinbase.com.
[5] Coinbase revenue and usage statistics (2021). https://www.businessofapps.com/data/coinbase-statistics/.
[6] Cryptocurrency wallets. https://www.gemini.com/cryptopedia/topic/cryptocurrency-wallets.
[7] Educational attainment in the united states: 2020. https://www.census.gov/data/tables/2020/demo/educational-attainment/cps-detailed-tables.html.
[8] Fortune - nearly 4 million bitcoins lost forever. https://fortune.com/2017/11/25/lost-bitcoins/.
[9] Hackers move 760 million from the 2016 bitfinex hack. https://therecord.media/hackers-move-760-million-from-the-2016-bitfinex-hack/.
[10] Holistic privacy and usability of a cryptocurrency wallet. https://arxiv.org/pdf/2105.02793.pdf/.
[11] Metamask wallet. https://metamask.io/.
[12] Nist- projects - multi-party threshold cryptography. https://csrc.nist.gov/Projects/threshold-cryptography.
[13] Prolific participants. https://www.prolific.co/#check-sample.
[14] Refresh when you wake up: Proactive threshold wallets with offline devices. https://arpa.medium.com/threshold-signature-explained-brining-exciting-apps-with-tss-8a75b43e19bf.
[15] Robinhood crypto. https://robinhood.com/us/en/about/crypto/.
[16] Torus wallet. https://tor.us.
[17] 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.
[18] Zengo wallet. https://zengo.com.
[19] Smooth tests of goodness of fit: An overview. *International Statistical Review / Revue Internationale de Statistique 58*, 1 (1990), 9–17.
[20] 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.
[21] Details of $5 million bitstamp hack revealed. https://www.coindesk.com/markets/2015/07/01/details-of-5-million-bitstamp-hack-revealed/, 2015.
[22] 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.
[23] Multisig wallets explained. https://medium.com/block-journal/multi-sig-wallets-explained-5544c122a1de, 2019.
[24] Attacking threshold wallet. https://eprint.iacr.org/2020/1052.pdf, 2020.
[25] A comprehensive list of cryptocurrency exchange hacks. https://selfkey.org/list-of-cryptocurrency-exchange-hacks/, 2020.
[26] Sok: A taxonomy of cryptocurrency wallets. https://eprint.iacr.org/2020/868.pdf, 2020.
[27] Bitcoin price history. https://www.investopedia.com/articles/forex/121815/bitcoins-price-history.asp, 2021.
[28] The complete list of crypto exchange hacks. https://www.hedgewithcrypto.com/cryptocurrency-exchange-hacks/, 2021.
[29] Crypto: A new asset class. https://www.goldmansachs.com/insights/pages/crypto-a-new-asset-class-f/report.pdf, 2021.
[30] Custodial vs. non-custodial wallets. https://www.gemini.com/cryptopedia/crypto-wallets-custodial-vs-noncustodial, 2021.
[31] Multisig wallet security. https://medium.com/the-capital/multisig-wallet-security-e2a1dee95cc0, 2021.
[32] Total cryptocurrency market cap, 2021. https://coinmarketcap.com/charts/, 2021.
[33] Abramova, S., Voskobojnikov, A., Beznosov, K., and Böhme, R. Bits under the mattress: Understanding different risk perceptions and security behaviors of crypto-asset users. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (2021), pp. 1–19.
[34] Albakry, S., Vaniea, K., and Wolters, M. K. What is this url's destination? empirical evaluation of users' url reading. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2020), CHI '20, Association for Computing Machinery, p. 1–12.
[35] Arapinis, M., Gkaniatsou, A., Karakostas, D., and Kiayias, A. A formal treatment of hardware wallets. In *Financial Cryptography and Data Security*

(Cham, 2019), I. Goldberg and T. Moore, Eds., Springer International Publishing, pp. 426–445.
[36] Atzei, N., Bartoletti, M., Lande, S., and Zunino, R. A formal model of bitcoin transactions. In *Financial Cryptography and Data Security* (Berlin, Heidelberg, 2018), S. Meiklejohn and K. Sako, Eds., Springer Berlin Heidelberg, pp. 541–560.
[37] Barber, S., Boyen, X., Shi, E., and Uzun, E. Bitter to better — how to make bitcoin a better currency. In *Financial Cryptography and Data Security* (Berlin, Heidelberg, 2012), A. D. Keromytis, Ed., Springer Berlin Heidelberg, pp. 399–414.
[38] Beimel, A. Secret-sharing schemes: A survey. In *International conference on coding and cryptology* (2011), Springer, pp. 11–46.
[39] Bellare, M., and Neven, G. Identity-based multi-signatures from rsa. In *Cryptographers' Track at the RSA Conference* (2007), Springer, pp. 145–162.
[40] Bellman, S., Johnson, E. J., and Lohse, G. L. On site: to opt-in or opt-out? it depends on the question. *Communications of the ACM 44*, 2 (2001), 25–27.
[41] Bleumer, G. *Threshold Signature*. Springer US, Boston, MA, 2005, pp. 611–614.
[42] Boneh, D., and Komlo, C. Threshold signatures with private accountability. In *Advances in Cryptology—CRYPTO* (2022), Y. Dodis and T. Shrimpton, Eds., pp. 551–581.
[43] Boneh, D., Partap, A., and Rotem, L. Accountable threshold signatures with proactive refresh. *IACR Cryptol. ePrint Arch.* (2022).
[44] Bui, T., Rao, S. P., Antikainen, M., and Aura, T. Pitfalls of open architecture: How friends can exploit your cryptocurrency wallet. In *Proceedings of the 12th European Workshop on Systems Security* (2019), pp. 1–6.
[45] Dai, W., Deng, J., Wang, Q., Cui, C., Zou, D., and Jin, H. Sblwt: A secure blockchain lightweight wallet based on trustzone. *IEEE Access 6* (2018), 40638–40648.
[46] Das, P., Faust, S., and Loss, J. A formal treatment of deterministic wallets. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (New York, NY, USA, 2019), CCS '19, Association for Computing Machinery, p. 651–668.
[47] Department of the Prime Minister and Cabinet, Australian Government. Harnessing the power of defaults. https://behaviouraleconomics.pmc.gov.au/sites/default/files/resources/harnessing-power-defaults.pdf.
[48] Desmedt, Y. *Threshold Cryptography*. Springer US, Boston, MA, 2011, pp. 1288–1293.
[49] di Prisco, D., and Strangio, D. Technology and financial inclusion: a case study to evaluate potential and limitations of blockchain in emerging countries. *Technology Analysis & Strategic Management 0*, 0 (2021), 1–14.
[50] Doerner, J., Kondi, Y., Lee, E., and Shelat, A. Threshold ecdsa from ecdsa assumptions: The multiparty case. In *2019 IEEE Symposium on Security and Privacy (SP)* (2019), pp. 1051–1066.
[51] Drijvers, M., Edalatnejad, K., Ford, B., Kiltz, E., Loss, J., Neven, G., and Stepanovs, I. On the security of two-round multi-signatures. In *2019 IEEE Symposium on Security and Privacy (SP)* (2019), pp. 1084–1101.
[52] Du, W., and Atallah, M. J. Secure multi-party computation problems and their applications: a review and open problems. In *Proceedings of the 2001 workshop on New security paradigms* (2001), pp. 13–22.
[53] Eskandari, S., Clark, J., Barrera, D., and Stobert, E. A first look at the usability of bitcoin key management. *arXiv preprint arXiv:1802.04351* (2018).
[54] Eyal, I. On cryptocurrency wallet design. In *Tokenomics 2021* (2021), vol. 97, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, pp. 4:1–4:16.
[55] Fröhlich, M., Gutjahr, F., and Alt, F. *Don't Lose Your Coin! Investigating Security Practices of Cryptocurrency Users*. Association for Computing Machinery, New York, NY, USA, 2020, p. 1751–1763.
[56] Fröhlich, M., Hulm, P., and Alt, F. Under pressure. a user-centered threat model for cryptocurrency owners.
[57] G, M. Coinjoin: Bitcoin privacy for the real world.
[58] G, M. Coinswap: transaction graph disjoint trustless trading.
[59] Gao, X., Clark, G. D., and Lindqvist, J. *Of Two Minds, Multiple Addresses, and One Ledger: Characterizing Opinions, Knowledge, and Perceptions of Bitcoin Across Users and Non-Users*. Association for Computing Machinery, New York, NY, USA, 2016, p. 1656–1668.
[60] Garfinkel, S. L., and Miller, R. C. 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* (New York, NY, USA, 2005), SOUPS '05, Association for Computing Machinery, p. 13–24.
[61] Gaw, S., Felten, E. W., and Fernandez-Kelly, P. Secrecy, flagging, and paranoia: Adoption criteria in encrypted email. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2006), CHI '06, Association for Computing Machinery, p. 591–600.
[62] Gennaro, R., and Goldfeder, S. Fast multiparty threshold ecdsa with fast trustless setup. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (2018), pp. 1179–1194.
[63] Gennaro, R., Goldfeder, S., and Narayanan, A. Threshold-optimal dsa/ecdsa signatures and an application to bitcoin wallet security. In *International Conference on Applied Cryptography and Network Security* (2016), Springer, pp. 156–174.
[64] Gero, K. I., Ashktorab, Z., Dugan, C., Pan, Q., Johnson, J., Geyer, W., Ruiz, M., Miller, S., Millen, D. R., Campbell, M., Kumaravel, S., and Zhang, W. Mental models of ai agents in a cooperative game setting. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (2020), CHI '20, p. 1–12.
[65] Ghesmati, S., Fdhila, W., and Weippl, E. User-perceived privacy in blockchain. *Cryptology ePrint Archive* (2022).
[66] Ghorbani Lyastani, S., Schilling, M., Neumayr, M., Backes, M., and Bugiel, S. Is fido2 the kingslayer of user authentication? a comparative usability study of fido2 passwordless authentication. In *2020 IEEE Symposium on Security and Privacy (SP)* (2020), pp. 268–285.
[67] Glomann, L., Schmid, M., and Kitajewa, N. Improving the blockchain user experience - an approach to address blockchain mass adoption issues from a human-centred perspective. In *Advances in Artificial Intelligence, Software and Systems Engineering* (Cham, 2020), T. Ahram, Ed., Springer International Publishing, pp. 608–616.
[68] He, X., Lin, J., Li, K., and Chen, X. A novel cryptocurrency wallet management scheme based on decentralized multi-constrained derangement. *IEEE Access 7* (2019), 185250–185263.
[69] Hellman, M. E. An overview of public key cryptography. *IEEE Communications Magazine 40*, 5 (2002), 42–49.
[70] Hitlin, P. Turkers in this canvassing: young, well-educated and frequent users. In *Research in the Crowdsourcing Age, a Case Study* (2016).
[71] Johnson, D., Menezes, A., and Vanstone, S. The elliptic curve digital signature algorithm (ecdsa). *International journal of information security 1*, 1 (2001), 36–63.
[72] Kesan, J. P., and Shah, R. C. Setting software defaults: Perspectives from law, computer science and behavioral economics. *Notre Dame L. Rev. 82* (2006), 583.
[73] Kim, S., Sarin, A., and Virdi, D. Crypto-assets unencrypted. *Journal of Investment Management, Forthcoming* (2018).
[74] Krombholz, K., Judmayer, A., Gusenbauer, M., and Weippl, E. The other side of the coin: User experiences with bitcoin security and privacy. In *Financial Cryptography and Data Security* (Berlin, Heidelberg, 2017), J. Grossklags and B. Preneel, Eds., Springer Berlin Heidelberg, pp. 555–580.
[75] Kulesza, T., Stumpf, S., Burnett, M., and Kwan, I. Tell me more? the effects of mental model soundness on personalizing an intelligent agent. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2012), CHI '12, p. 1–10.
[76] Lin, J., Amini, S., Hong, J. I., Sadeh, N., Lindqvist, J., and Zhang, J. Expectation and purpose: Understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing* (2012), UbiComp '12, p. 501–510.
[77] Lindell, Y., and Nof, A. 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* (New York, NY, USA, 2018), CCS '18, Association for Computing Machinery, p. 1837–1854.
[78] MacFarland, T. W., and Yates, J. M. *Mann–Whitney U Test*. Springer International Publishing, Cham, 2016, pp. 103–132.
[79] Mai, A., Pfeffer, K., Gusenbauer, M., Weippl, E., and Krombholz, K. User mental models of cryptocurrency systems - a grounded theory approach. In *SOUPS @ USENIX Security Symposium* (2020).
[80] Mangipudi, E. V., Desai, U., Minaei, M., Mondal, M., and Kate, A. Uncovering impact of mental models towards adoption of multi-device crypto-wallets. Cryptology ePrint Archive, Paper 2022/075, 2022. https://eprint.iacr.org/2022/075.
[81] Marcedone, A., Pass, R., and Shelat, A. Minimizing trust in hardware wallets with two factor signatures. In *Financial Cryptography and Data Security* (Cham, 2019), I. Goldberg and T. Moore, Eds., Springer International Publishing, pp. 407–425.
[82] McHugh, M. L. Interrater reliability: the kappa statistic. *Biochemia medica 22*, 3 (2012), 276–282.
[83] Owens, K., Anise, O., Krauss, A., and Ur, B. User perceptions of the usability and security of smartphones as {FIDO2} roaming authenticators. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)* (2021), pp. 57–76.
[84] Plackett, R. L. Karl pearson and the chi-squared test. *International Statistical Review / Revue Internationale de Statistique 51*, 1 (1983), 59–72.
[85] Ramokapane, K. M., Mazeli, A. C., and Rashid, A. Skip, skip, skip, accept!!!: A study on the usability of smartphone manufacturer provided default features and user privacy. *Proceedings on Privacy Enhancing Technologies 2019*, 2 (2019), 209–227.
[86] Redmiles, E. M., Kross, S., and Mazurek, M. L. How well do my results generalize? comparing security and privacy survey results from mturk, web, and telephone samples. In *2019 IEEE Symposium on Security and Privacy (SP)* (2019), pp. 1326–1343.
[87] Rezaeighaleh, H., and Zou, C. C. Deterministic sub-wallet for cryptocurrencies. In *2019 IEEE International Conference on Blockchain (Blockchain)* (2019), pp. 419–424.
[88] Ruffing, T., and Moreno-Sanchez, P. Valueshuffle: Mixing confidential transactions for comprehensive transaction privacy inÀ bitcoin. In *Financial Cryptography and Data Security* (2017).

Table 4: Participants' Demographics

	Newbie	Non-newbie	Total
	86	271	357
Gender			
Female	43	56	99
Male	42	210	252
Prefer not to answer	1	5	6
Age			
18 - 24	7	40	47
25 - 34	41	101	142
35 - 44	23	96	119
45 - 54	9	24	33
55 - 64	3	7	10
>65	2	0	2
Prefer not to answer	1	3	4
Education			
High school degree	18	56	74
College degree	11	43	54
Bachelor's degree	43	127	170
Master's degree	14	36	50
Doctorate	0	4	4
Prefer not to answer	0	5	5
Employment status			
Full-time	57	201	258
Part-time	14	30	44
Unemployed	7	11	18
Uncompensated	0	3	3
Student	1	13	14
Retired	3	0	3
Other	2	7	9
Prefer not to answer	2	6	8
Background in IT			
Yes	23	112	135
No	61	150	211
Prefer not to answer	2	9	11

[89] Ruffing, T., Moreno-Sanchez, P., Kate, A., and Vaidya, J. Coinshuffle: Practical decentralized coin mixing for bitcoin. In *Computer Security - ESORICS 2014* (2014).

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

[91] Shamir, A. How to share a secret. *Commun. ACM 22*, 11 (Nov. 1979), 612–613.

[92] Sheng, S., Broderick, L., Koranda, C. A., and Hyland, J. J. Why johnny still can't encrypt: evaluating the usability of email encryption software. In *Symposium On Usable Privacy and Security* (2006), ACM, pp. 3–4.

[93] Shin, D., and Bianco, W. T. In blockchain we trust: Does blockchain itself generate trust? *Social Science Quarterly 101*, 7 (2020), 2522–2538.

[94] Shoup, V. Practical threshold signatures. In *International Conference on the Theory and Applications of Cryptographic Techniques* (2000), Springer, pp. 207–220.

[95] Vasek, M., Bonneau, J., Castellucci, R., Keith, C., and Moore, T. 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).

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

[97] Voskobojnikov, A., Wiese, O., Mehrabi Koushki, M., Roth, V., and Beznosov, K. K. The u in crypto stands for usable: An empirical study of user experience with mobile cryptocurrency wallets. CHI '21, Association for Computing Machinery.

[98] Wash, R. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (New York, NY, USA, 2010), SOUPS '10, Association for Computing Machinery.

[99] Zhao, C., Zhao, S., Zhao, M., Chen, Z., Gao, C.-Z., Li, H., and Tan, Y.-a. Secure multi-party computation: theory, practice and applications. *Information Sciences 476* (2019), 357–372.

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