Bits Under the Mattress: Understanding Different Risk Perceptions and Security Behaviors of Crypto-Asset Users

SVETLANA ABRAMOVA*, University of Innsbruck, Austria
ARTEMIJ VOSKOBOJNIKOV*, University of British Columbia, Canada
KONSTANTIN BEZNOSOV, University of British Columbia, Canada
RAINER BÖHME, University of Innsbruck, Austria

Crypto-assets are unique in tying financial wealth to the secrecy of private keys. Prior empirical work has attempted to study end-user security from both technical and organizational perspectives. However, the link between individuals' risk perceptions and security behavior was often obscured by the heterogeneity of the subjects in small samples. This paper contributes quantitative results from a survey of 395 crypto-asset users recruited by a novel combination of deep and broad sampling. The analysis accounts for heterogeneity with a new typology that partitions the sample in three robust clusters – cypherpunks, hodlers, and rookies – using five psychometric constructs. The constructs originate from established behavioral theories with items purposefully adapted to the domain. We demonstrate the utility of this typology in better understanding users' characteristics and security behaviors. These insights inform the design of crypto-asset solutions, guide risk communication, and suggest directions for future digital currencies.

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

Additional Key Words and Phrases: Crypto-asset, security, user behavior, cluster analysis

ACM Reference Format:
Svetlana Abramova, Artemij Voskobojnikov, Konstantin Beznosov, and Rainer Böhme. 2021. Bits Under the Mattress: Understanding Different Risk Perceptions and Security Behaviors of Crypto-Asset Users. In *CHI Conference on Human Factors in Computing Systems (CHI '21), May 8–13, 2021, Yokohama, Japan.* ACM, New York, NY, USA, 26 pages. https://doi.org/10.1145/3411764.3445679

1 INTRODUCTION

Money is widely recognized as a social construct whose value depends on subjective beliefs and expectations of individuals. Crypto-assets are described as a new type of money [27], and their adoption has continued to grow over the last years [33]. Increasingly, people of different backgrounds, interests, and socio-economic status are starting to invest and experiment with this novel form of digital value. However, adopting crypto-assets is not an easy task from the viewpoint of both users and non-users [27]. Prior qualitative studies [25, 27, 71] have found that users are burdened by secure key management and often find tools confusing and complex to use. Design choices leave users in a position where slight mistakes and security flaws can lead to irreversible damages, which are compounded by the lack of central authorities providing a safety net.

*Both authors contributed equally to this research.

Manuscript accepted for ACM CHI '21

Countless crypto-asset users, both experienced and novice, have already suffered monetary losses caused by the intricacy of key management, basic negligence, or security breaches [43]. Astonishingly, nearly 4 million bitcoins, worth tens of billions of dollars, are believed to be buried forever because of lost or forgotten keys [60].

In response to the complex nature of key management, centralized security solutions emerged on the crypto market as a viable alternative. Such solutions, while wide-ranging, include a custodian entrusted by the user to manage and secure their assets. These services, such as cryptocurrency exchanges, are deemed to provide a better user experience (UX) than self-managed options. However, they are also exposed to security threats [48], which in the worst case might lead to shutdowns and monetary losses for users.

Previous qualitative research has shown that crypto-asset users differ in their security decisions and employ various tactics to secure crypto-assets [25, 71]. These decisions are influenced by a variety of risk factors, such as the usage context or the amount at stake. Some users, in particular novice ones, resort to convenient custodial services to manage keys on their behalf. Conversely, more experienced and conservative users have little trust in virtual asset service providers (VASPs) and, therefore, strongly advocate for the self-management and safekeeping of keys [25, 71]. This variation in individual risk perceptions and security behaviors is likely to grow further in the future, as more people decide to adopt crypto-assets.

Moreover, the increased interest in central bank digital currencies (CBDCs) [4, 6, 51] broadens the scope of the heterogeneity issue even further. In fact, many topics of discussion on CBDCs link back to the fundamental trade-off between safety and convenience of managing digital assets. Should central banks leave the control of cryptographic keys in users' hands or shift this burden to third parties instead? How should VASPs be regulated to ensure their liability and full transparency with users about ownership, security risks, and protection measures?

This empirical paper aims to bring security research in this domain forward by providing an up-to-date picture of the current population of users and their preferences and practices in managing and securing crypto-assets. It also intends to overcome the major shortcomings of prior qualitative works (e.g., small samples and exploratory nature of research), which make generalizations of their results problematic. Against this backdrop, this paper contributes the first in-depth quantitative study of 395 crypto-asset users, documenting their different risk concerns and security behaviors. We apply a theory-guided approach to the instrument design and propose a new typology for characterizing the diverse and ever-growing population of crypto-asset users. The user typology is derived from cluster analysis using a number of context-specific psychometric constructs relevant to security, protection, and risk. Our analysis reveals that crypto-asset users can be broadly categorized into "cypherpunks" (experienced crypto-asset advocates and enthusiasts), "hodlers" (security-concerned and profit-oriented traders and investors), and "rookies" (inexperienced users motivated by fear of missing out). We provide a detailed characterization of each cluster along several dimensions, and we study differences and commonalities in individuals' perceptions, key management choices, and security practices on the cluster level.

We make a number of important contributions. Specific to this research area, our study is the first of its kind to complement the customary method of purposeful sampling with online crowdsourcing recruitment of crypto-asset users. The second innovation is that the survey design and data analysis are built on behavioral theories and constructs. We provide a set of adapted and newly developed scale items pertinent to security risks of crypto-assets. This approach enables us to account for the user heterogeneity and break down the mixed population of crypto-asset users into meaningful clusters. Third, we find that cypherpunks prefer offline storage devices for large-value assets and this choice is significantly correlated with the self-reported amount. Hodlers are found to be mostly affected by key thefts, whereas rookies perceive themselves as incapable of self-managing keys. Based on these findings, we suggest user-targeted practical design implications for crypto-asset security solutions.

The remainder of this paper is organized as follows. We first introduce the key terminology (Section 2) and review related work (Section 3). We describe our methodological approach in Section 4 and report empirical results in Section 5. Finally, we discuss the implications and limitations of our work from both research and practical perspectives in Section 6.

2 TERMINOLOGY

Throughout the paper, we use the term *crypto-assets* to refer to both cryptocurrencies and digital tokens. Cryptocurrencies are cryptographically secured digital currencies without a centralized governing or issuing party. The first modern cryptocurrency is Bitcoin, introduced in the working paper [50] and released in 2009. Since then, a plethora of other cryptocurrencies were created, allowing users to extend the underlying protocol (e.g., of Ethereum) with new functionality such as tokens. Digital tokens can represent almost any exchangeable asset, including a cryptocurrency, a conventional security (*security token*), or a consumptive right to a product or a service provided by the token's issuer (*utility token*) [35]. Though the functions of tokens go beyond those of cryptocurrencies, they share similar security mechanisms and risks. Therefore, we consider both in our study and refer to them as *crypto-assets*.

When it comes to the management of crypto-assets, there exists a wide range of tools for users to choose from. These coin management tools (CMTs), also known as crypto wallets, allow users to effectively manage their pairs of cryptographic keys and transact with crypto-assets. CMTs are commonly categorized into *hot* and *cold* wallets [17]. Hot wallets are directly connected to the Internet, which makes them an easier target for attacks. Common examples are software desktop applications, mobile wallets, or browser plug-ins. Cold wallets, on the contrary, are kept offline most of the time. Consequently, they provide better security, but are less convenient to use. Common examples are hardware, paper, or brain wallets.

In this paper, we further distinguish between *custodial* and *non-custodial* crypto wallets. Custodial wallets are third-party services that take care of the key management. They are known to be user-friendly as they create an abstraction layer and free the user from understanding the underlying cryptography. One prominent example for such third-party services are cryptocurrency exchanges. Here, users' funds are stored in an aggregated form in a combination of hot and cold wallets. Due to this aggregation, users never truly control crypto-assets, but are merely promised that they will be able to withdraw their crypto-assets if they decide to do so. Therefore, exchanges provide some of the functionality of conventional wallets and users can use them as such. Storing large amounts in exchanges, however, can be risky due to the associated permanent monetary losses that can occur in case of shutdowns or hacks [48].

Non-custodial wallets, on the other hand, allow users to manage and control the key pairs directly. While this supports customizability and freedom, it can also lead to mistakes that are difficult to recover from. Poor security practices of users tasked with the storage and protection of private keys could (and are known to) cause monetary losses [63, 71]. Therefore, while these wallets promise high security guarantees, they are also more burdensome to use. Software wallets, such as Electrum,[1] and mobile wallets, such as Trust Crypto wallet,[2] are some examples of non-custodial wallets.

3 RELATED WORK

We structure the discussion of related work into two main themes: empirical studies on crypto-assets and user studies on password and key management.

[1]Electrum wallet: www.electrum.org
[2]Trust wallet: www.trustwallet.com

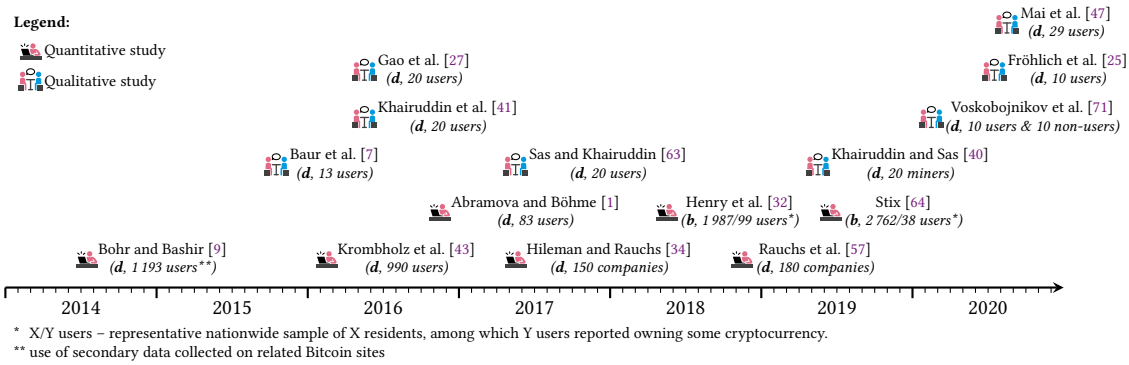


Fig. 1. Overview of empirical studies on crypto-assets (***d*** – deep sampling, ***b*** – broad sampling)

3.1 Empirical Studies on Crypto-Assets

Crypto-assets have received a fair share of attention from academia in recent years. Figure 1 presents an overview of qualitative and quantitative user studies with additional sampling details. Sampling the hard-to-reach population of crypto-asset users is deemed difficult due to its unknown size, its geographical dispersion, and the privacy concerns of its members. As a result, two distinct strategies dominate in prior empirical work: (a) *deep sampling*, which involves reaching out to crypto-asset users through personal referrals, local networks, or recruitment notices posted on dedicated discussion boards or distributed by companies operating in this field; (b) *broad sampling*, which includes traditional random sampling procedures with the aim to collect evidence on the awareness and ownership of crypto-assets by nationwide populations [53]. According to this classification, deep sampling involves such methods as snowball, respondent-driven, or targeted sampling [31], and is widely employed in this domain due to its cost and time efficiency.

Qualitative studies have closely investigated the behavior of crypto-asset users. They have shed light on users' underlying ideologies and motivations [41], as well as challenges experienced during use [27, 71]. Besides trust [40, 63] and usability issues of wallets [7, 25, 72], users are also found to have difficulties with the key management process [22]. Results show that some users have misconceptions related to the cryptographic principles [27, 47], while others, and novices in particular, often find the key management complicated [22, 27, 71]. These difficulties not only pose inconvenience for them, but can also lead to errors and monetary losses in extreme cases, e.g., due to forgotten passwords [63] or mistakenly deleted key pairs [71].

Quantitative work on crypto-assets, however, is scarce and has mainly focused on Bitcoin and its ecosystem. Attitudes toward Bitcoin were investigated by both Henry et al. [32] and Stix [64], whereas a series of global crypto-asset benchmarking studies [34, 57] attempted to characterize the crypto-asset population. Studies investigating risk perceptions and security practices of users can be found in literature [1, 43], yet, they present an either partial or outdated view. Over the past four years, the market capitalization of crypto-assets other than Bitcoin has grown from US$600 million to over US$140 billion, with millions of new users and investors joining the domain [57]. Our work not only includes these other crypto-assets, but also presents an updated overview of the crypto-asset user population.

Prior work relied on the crude distinction between users and non-users of crypto-assets. This view is very coarse, as crypto-asset users represent a remarkably heterogeneous group in their attitudes and experience toward cryptocurrencies, usage patterns, preferences over CMTs, risk profiles, and security behaviors [9, 25, 71]. While experienced and

skilled individuals usually have better control of private keys and devices, amateurs are in the early phase of their learning curve and hence more vulnerable to targeted attacks or accidental errors such as deleting wallet files. We adopt the cluster analysis approach to segment the diverse population of crypto-asset users, and provide new evidence about their perceptions and protection behaviors. To the best of our knowledge, our work is the first quantitative study of crypto-asset users that sheds light on their usage behavior, security perceptions, and practices.

3.2 Password and Key Management

There exists an extensive body of research on the challenges users face when managing their passwords. Adams and Sasse [2] were the first to point out that users experience significant cognitive load when trying to comply with security recommendations, particularly when managing multiple passwords. To lower this burden, users employ measures that they deem more convenient, such as re-using [24, 30, 73], sharing [70], and writing down passwords [65]. Pearman et al. [55] provided a first categorization of password practices. The authors applied hierarchical clustering on a sample of 154 participants. They found differences between the groups in terms of password strength and sharing behavior. Some users were security conscious and employed stronger passwords, whereas others chose weaker passwords and re-used them more often.

The aforementioned cognitive burden is, however, not exclusive to password management. In 1999, Whitten and Tygar [75] evaluated the usability of PGP 5.0 and found significant misunderstandings among users about public-key cryptography. More recent PGP tools bring similar challenges, as shown by Ruoti et al. [62]. Only 1 out of 10 pairs of users managed to exchange encrypted emails [62]. Mistakes were made by all the groups. Some tried to encrypt the email with their own public key, while others disclosed sensitive information, such as private keys, to the recipient.

In the context of crypto-assets, mishandling passwords or cryptographic keys can also have grave consequences. Sas and Khairuddin [63] interviewed 20 Bitcoin users on trust challenges and security practices. Among other findings, the authors report on monetary losses incurred either due to lost or weak passwords. The users of crypto-assets also have difficulties with managing cryptographic keys. Voskobojnikov et al. [71] conducted an interview study with crypto-asset users and found that newcomers were confused by the underlying cryptography. Often, they did not know where their keys were stored and even recalled instances of accidentally deleting keypairs. Inspired by these previous works, this study aims to examine security behaviors of crypto-asset users in relation to their risk concerns and levels of experience, thereby complementing former qualitative insights with robust data-driven inferences.

4 METHODOLOGY

This section presents our general approach and how it is reflected in the survey instrument. We also describe the data collection and quality assurance processes.

4.1 Approach

Over the years, more diverse individuals have become crypto-asset owners [34, 57]. As established in related work (Sect. 3), there is no single profile of a typical crypto-asset user. This heterogeneity complicates the empirical analysis of individual security behaviors. A canonical response to heterogeneous samples is cluster analysis, an exploratory method that finds more homogeneous subsamples (clusters) of individuals in a multivariate space [56]. The method assigns subjects to clusters such that the members of each cluster are as similar as possible and as different as possible from subjects in other clusters.

Cluster analysis depends heavily on which variables are included in the metric of (dis-)similarity between subjects. We considered reported behavior (e.g., the choice of wallets, transaction periodicity), socio-demographics (e.g., age, gender, occupation), and psychometric beliefs (e.g., risk perceptions, self-efficacy). We chose psychometric beliefs for their presumed convergence and stability at the individual and population level, which results from the redundancy of measuring a latent construct with multiple items [16].

We sought inspiration from well-established behavioral theories to define a set of constructs relevant to protection and risk. Specifically, we consider the Protection Motivation Theory (PMT) [61], which originated in individual health studies, and the Theory of Planned Behavior (ToPB) [3], a general theory of action. PMT has a calculus that trades off the likelihood and severity of a bad outcome versus the effort and efficiency of a preventive action. Both the PMT and ToPB emphasize the importance of self-efficacy, which is defined as the subjective belief of one's ability to successfully perform an action. Derivates of both theories have been successfully applied in literature to explain human–computer interaction, most prominently the Technology Acceptance Model (TAM) [18, 45] with its risk-augmented variant [54]. There are many examples of empirical computer security studies using these theories, including [10, 12, 15, 39, 46, 66, 67, 76].

All constructs in these theories were shortlisted as candidates for clustering. In adapting the scale items to the domain of our study, we interpreted the loss of crypto-assets as a bad outcome and related it to the user's key management decisions. For example, the original scale item of a PMT construct in [76] "I have the resources and the knowledge to take necessary security measures" is adapted to "I have technical skills and time to secure and prevent the theft of my crypto-assets." We included constructs by the ease of adapting the associated scale items, while keeping an eye on construct diversity and questionnaire length. This iterative process converged on five constructs.

The construct *perceived vulnerability* (4 scale items) reflects one's belief of the likelihood of private keys or user accounts being compromised. The statement "My crypto-wallet is at risk of being compromised" is an example of a scale item for this construct. *Perceived severity* (4 items) captures one's belief of the impact of financial distress or personal harm caused by the loss of crypto-assets. The construct is operationalized with scale items like "Losing crypto-assets would likely cause me severe stress." *Perceived self-efficacy* (4 items) is the belief in one's capability to secure keys and prevent the theft of crypto-assets. An example statement is "I am able to protect my private key from being stolen." *Response cost* (5 items) refers to the financial cost, time, effort, or inconvenience the user associates with securing crypto-assets. The scale items cover one-off (e.g., "Security investments into equipment are costly") as well as recurring costs (e.g., "Spending crypto-assets from secure crypto wallets is costly"). *Perceived concern* (5 items) measures the level of concern about broader security risks related to crypto-assets, including threat vectors through third parties, such as custodians. Example statements are "I am concerned about security vulnerabilities of wallets" or "I am concerned about security vulnerabilities of exchanges." All scale items are measured on five-point rating scales with end points labeled "strongly disagree" and "strongly agree," except for *perceived concern*, where the scale semantically ranges from "not concerned at all" to "very concerned." Table 5 in Appendix A lists all scale items along with references to the sources from which they were adapted.

4.2 Instrument

The online survey can be broadly structured into two parts: the scale items required to measure the constructs (discussed above), and a series of complementary questions about the ownership, storage, other risk factors related to crypto-assets, employed security practices, and demographics. Overall, the final instrument included 67 questions, with an estimated completion time of 25 minutes. We summarize below the blocks of questions, which served as entry points

for characterizing the clusters and understanding users' security behaviors. The complete questionnaire is available in the supplementary material.

[Crypto-Asset Ownership] This block of questions aimed to identify the *what*, *how*, and *what for* of the crypto-asset use. Specifically, we inquired about owned cryptocurrencies and tokens, the amount held, as well as services and products users pay for with crypto-assets. Similar to Khairuddin et al. [41], we asked about motives for the use of crypto-assets.

[Crypto-Asset Storage] This block of questions collected data on types of wallets used and on the reasons why they were chosen. Contrary to prior studies that focus on hosted wallets [43, 63], we provided an exhaustive list of eight wallet types, including non-custodial options (e.g., hardware, paper, or brain wallets). Each type was supplemented by a pop-up note providing an exhaustive explanation (presented in Appendix C). Those respondents who reported using more than one type were explicitly asked to specify which of the selected wallets stored **most** of their funds (in terms of value).

[Other Risk Concerns] Besides security risks, the survey included 10 additional risk scenarios, including, but not limited to, financial, adoption, and privacy risks. The items were adapted from prior work [8, 28, 43] and extended with self-developed scenarios to provide a more comprehensive coverage of concerns crypto-asset users may have nowadays.

[Security Practices] Little is known about security practices that users employ to protect their crypto-assets and devices. Based on the findings of prior studies [43, 63, 71], we constructed a list of 14 options and asked respondents how often they implement those practices. For instance, users were asked whether they use backups, two-factor authentication, encryption, or multi-signature wallets. The responses were reported on a 3-point ordinal scale (1 – rarely, 2 – occasionally, 3 – regularly).

[Demographics] Similar to prior studies [1, 43], we collected basic demographic data. We inquired about their age, gender, occupation, degree, country of residence, and ethnicity.

4.3 Data Collection

From the outset, we aimed to maintain both the breadth and depth of data to be collected (instead of representativeness, which is known to be challenging in this domain). The online survey (in English and German) with an optimized front end for both desktop and mobile browsers was hosted in early 2020 using the Qualtrics survey platform licensed by the participating institution. We surveyed crypto-asset users in both North America and Europe using a combination of the two sampling strategies. First, we recruited participants through a variety of direct communication channels, including pertinent communities on Reddit, cryptocurrency forums, and Twitter, as well as with the help of community managers of blockchain startups and cryptocurrency exchanges. To diversify this sample and target pragmatic users with less community engagement, we decided to further recruit participants through a Qualtrics[3] panel. The use of such online crowdsourcing services has become increasingly popular in security and privacy research. Furthermore, prior work has shown that samples recruited in the U.S. tend to be representative of the country-wide population [58]. Therefore, our survey was restricted to participants residing in the U.S. and predetermined by Qualtrics to be crypto-asset users over the age of 18.

In total, we collected reliable data from 395 crypto-asset users, 195 of which were recruited through our targeted campaigns and the rest (200 users) – through the commercial service. The average completion time of the questionnaire

[3]Qualtrics panel: https://www.qualtrics.com/research-services/online-sample/

was 16.5 and 9 minutes for the subsamples recruited by us and Qualtrics, respectively. We present the comparative analysis of the two subsamples along with the socio-demographic factors in Table 6 in Appendix B.

4.4 Quality Assurance, Ethics, and Privacy

We implemented a number of quality assurance measures and checks to avoid misinterpretation and reduce response bias in the data collection phase. First, we conducted a pilot survey with 30 participants to assess the clarity and translation quality of the instrument. The participants were a mix of domain experts, researchers, and crypto-asset users, whose valuable feedback led to several improvements. Specifically, we made adjustments related to incorrect randomization of questions or wording issues. Second, basic attention checks (e.g., repeated and reversed questions) were implemented in the survey itself to ensure that participants complete it with full attention.

In the Qualtrics subsample, we also excluded participants who reported using European exchanges, as non-European citizens would not be able to register and pass the Know-Your-Customer[4] check. Qualtrics further screened out respondents who completed the survey in less than 250 seconds. For the sake of consistency, we applied the same rule for the other subsample, too. Overall, we excluded 406 response sets (206 from the broad and 200 from the deep sample), which either failed quality or completion time checks, or were identified as straight-liners.

Prior to the data collection phase, the study was reviewed and approved by the research ethics boards of the involved institutions. Participants were asked for explicit consent to participate in the study and to use their anonymized data for research purposes. We arranged a raffle as an incentive and compensation for participation. Winners were able to choose between a 50 euro (or the equivalent amount in the currency of choice) Amazon gift card or a donation to UNICEF, WWF, or the Red Cross. The probability of winning was 1 out of 25 for our subsample. For the sake of fairness, it was adjusted for the other subsample based on the estimated value, since Qualtrics itself compensated respondents with US$4.

Upon completion of data collection and cleaning procedures, Cronbach's alpha was calculated for each construct as a measure of the internal consistency of the designed scale items [14]. As reported in Table 5 in Appendix A, all constructs have an alpha value greater than the rule-of-thumb threshold of 0.7 [69]. Also, the values do not improve after dropping an arbitrary item in any scale, which indicates a sufficient level of redundancy in the items. As expected, the construct *perceived concern* has the lowest Cronbach's alpha ($\alpha = 0.77$), since the items operationalize tangential types of security risk. We calculated the aggregate score of each construct by summing up the scores of all individual items and standardizing this sum to allow equal weighting of the inputs to the cluster analysis.

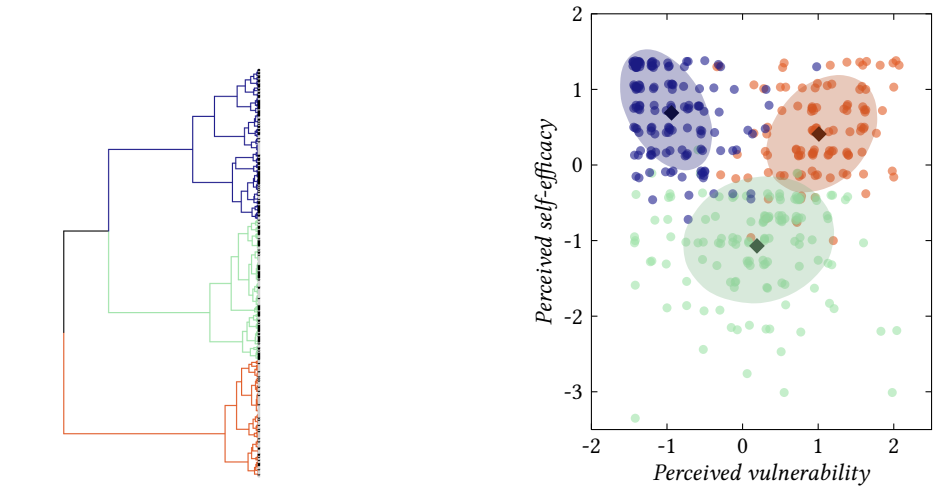
5 RESULTS

We first present the clustering results and describe the discovered user typology. Then, we examine users' security behaviors on the cluster level by looking at the users' choice of wallets and a number of security practices specific to the protection of crypto-assets.

5.1 Typology of Crypto-Asset Users

Ward's hierarchical clustering with the Euclidean distance measure yielded a dendrogram (shown in Figure 2a) suggesting three distinct clusters in the dataset. We tested the stability of this cluster solution by iteratively dropping one of the discriminating variables and rerunning the analysis. The resulting dendrograms, presented in Figure 7 in Appendix D,

[4]Know-Your-Customer (KYC): Practices carried out by (financial) service providers to verify their clients



(a) Hierarchical cluster dendrogram (b) Clusters and their centroids along two constructs

Fig. 2. Cluster analysis results

reasonably support solutions with three clusters. We visualize the cluster analysis results in Figure 2b by plotting the standardized scores of the constructs *perceived vulnerability* and *perceived self-efficacy* (with added noise of 5% to avoid the discreteness effects) of each individual respondent in the sample. From this plot, it appears that users within two clusters (marked in blue and orange) are homogeneous in their high scores on *perceived self-efficacy*, but differ in their self-evaluation of *perceived vulnerability* (rated as either low or high). Users within the third cluster (in green) perceive themselves as the least competent in taking protective measures and are distinguished by their heterogeneous opinions on the likelihood of their accounts or keys being compromised.

Since Figure 2b gives only a partial view of the cluster analysis results, we present the mean and plus or minus one standard deviation of all the constructs per each cluster in Figure 3. At this point, we introduce the labels for the clusters for the sake of convenience: cypherpunks, rookies, and hodlers. Cypherpunks (in blue) report being the least vulnerable to security threats and the most skilled in protecting keys and wallets on their own.

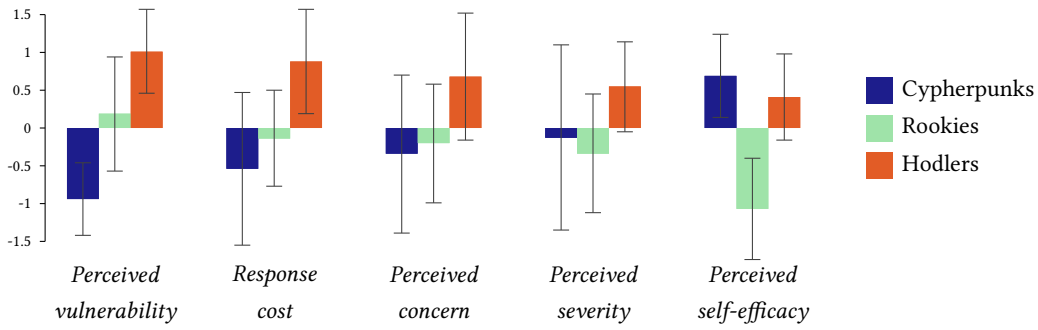


Fig. 3. Construct means and ±1 standard deviation per cluster, sorted by increasing values of the cypherpunks

Hodlers are also competent in digital self-protection; however, they are more security-concerned and cautious, as evidenced by the consistently high scores on *perceived vulnerability*, *perceived severity*, *response cost*, and *perceived concern*. With regard to rookies, the mean value of *perceived self-efficacy* is what makes this cluster stand out in our dataset. As for the rest of the psychometric constructs, this cluster has in-between means close to zero.

The differences between the clusters are evident in the level of self-reported confidence and literacy of their users. Cypherpunks are more confident in using crypto-assets and explaining the intricacies of the underlying technology (see Table 1), which is expected, considering their high scores on *perceived self-efficacy*. While hodlers scored lower than cypherpunks, they are more knowledgeable and confident in their skills than rookies, who have the lowest scores throughout.

Table 1. Mean and standard deviation of statements referring to the level of confidence in skill areas per cluster. Maximum in bold (mean) or italics (SD). Reported on a five-point rating scale: 1 – not confident at all, 5 – very confident.

Questionnaire item	Cypherpunks		Rookies		Hodlers	
	Mean	SD	Mean	SD	Mean	SD
How confident are you in the following skill areas in the context of crypto-assets?						
Purchasing crypto-assets.	**4.56**	0.73	3.42	0.99	4.04	*1.05*
Making payments with crypto-assets.	**4.46**	0.83	3.33	*1.03*	4.05	0.91
Explaining the difference between the private and public key.	**4.32**	0.92	3.20	*1.11*	3.99	0.96
Explaining the purpose of transaction fees.	**4.37**	0.87	3.41	*1.03*	4.01	0.96

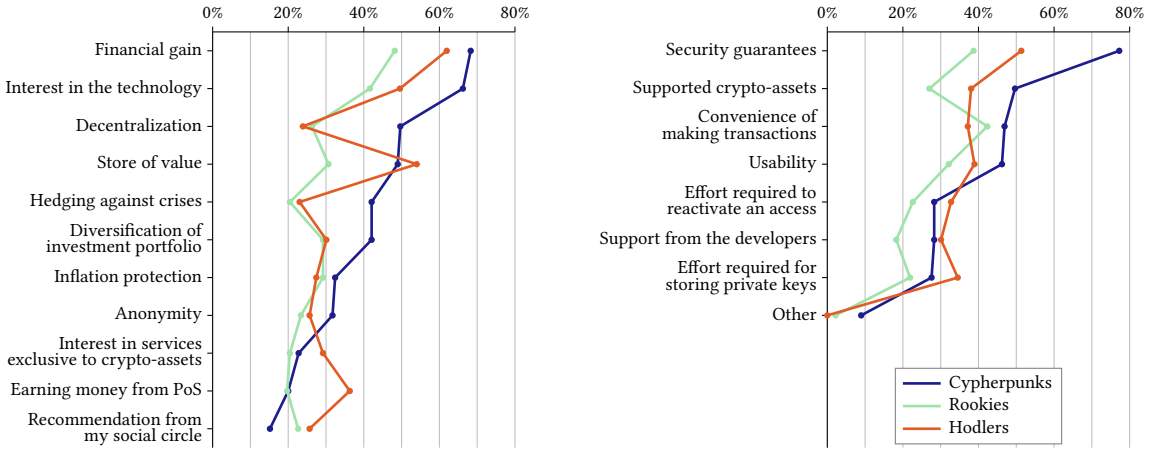
Below, we provide the profile description of each cluster and justify our handpicked labels. It is worth emphasizing that this characterization draws solely on the socio-demographic indicators (gender and age) and a number of self-reported facts related to the crypto-asset ownership (see Table 2).

In addition, we base our conclusions on users' responses to the following questions:

- "Please select up to 5 factors that contributed to starting your use of crypto-assets." (Figure 4a),
- "What factors influenced your decision when choosing a crypto wallet for storing your crypto-assets?" (Figure 4b).

Cypherpunks are technically savvy enthusiasts and early adopters who became obsessed by crypto-assets out of ideological and technological interest. As presented in Table 2, they are mostly men (~88%) around 25–44 years old with more than 3 years of experience. Almost 17% of cypherpunks report belonging to the true early adopters of cryptocurrencies with at least 6 years of experience. The majority of users report owning Bitcoin and Ethereum (see Table 7 in Appendix E). Moreover, digital tokens are held almost exclusively by cypherpunks (20%). Besides purely financial motives, cypherpunks rank the interest in the blockchain technology itself and decentralization as the primary drivers of the crypto-asset usage (see Figure 4a). All the above findings explain our decision to label this cluster as cypherpunks. Though they started to invest in crypto-assets probably long before the surge of the crypto market, only 14.5% report holding crypto-assets worth of more than US$100 000. Interestingly, ~17% of cypherpunks prefer not to disclose their financial status, as opposed to ~2% of users with the similar response in the other two clusters.

Rookies are casual users who joined the crypto market out of fear of missing out (FoMO). This is evidenced by the high fraction of rookies who are novices or who started to invest in crypto-assets 3–4 years ago, probably following the record surge in Bitcoin's market price in 2017. While being curious about the technology, they seek long-term financial



(a) Self-reported motives for the use of crypto-assets

(b) Self-reported decision factors for the choice of crypto wallets

Fig. 4. Self-reported factors in percentage of users per cluster, sorted by decreasing values of the cypherpunks

gains and profit opportunities (see Figure 4a). In contrast to the male-dominated cluster of young and medium-aged cypherpunks, rookies are characterized by the largest share of women (33%) and a significant share (25%) of the older population (over 45). With respect to coin management tools, rookies favor convenient, secure, and easy-to-use wallets (see Figure 4b).

Hodlers are middle-aged traders (with almost half being 35–44 years old) who started to use crypto-assets 3–4 years ago foremost out of financial motives. The term *hodler* originated on the Bitcointalk forums[5] in a misspelling by a Bitcoin trader. Since then, hodlers are often associated with greedy crypto-asset users, and this term therefore seems appropriate for the cluster.

Besides trading crypto-assets, hodlers also trade on conventional stock markets more often (23% "regularly") than cypherpunks (18%) and rookies (13%). Interestingly, 25% of hodlers report owning more than US$100 000 of crypto-assets. As high-net-worth individuals, they are especially interested in proof-of-stake (PoS) protocols, perhaps to reap the benefits of the so-called compounding effect [23]. The effect predicts that wealthier users will become even richer, as with the growing wealth they have higher chances of being elected as new block leaders and getting financially rewarded.

It is remarkable that this typology, derived from a purely data-driven approach, presents a plausible and fairly consistent view of the entire population of crypto-asset users. With the descriptive characteristics of the clusters at hand, we can now connect the dots back to the psychometric constructs and summarize the key facts. Cypherpunks know best what security in the context of crypto-assets means, whereas rookies are the least knowledgeable and experienced in this matter. Hodlers, in turn, trade and interact with large amounts of money and hence, face incentives to take special care of the security and protection of their digital assets and devices.

[5] I AM HODLING: https://bitcointalk.org/index.php?topic=375643.0

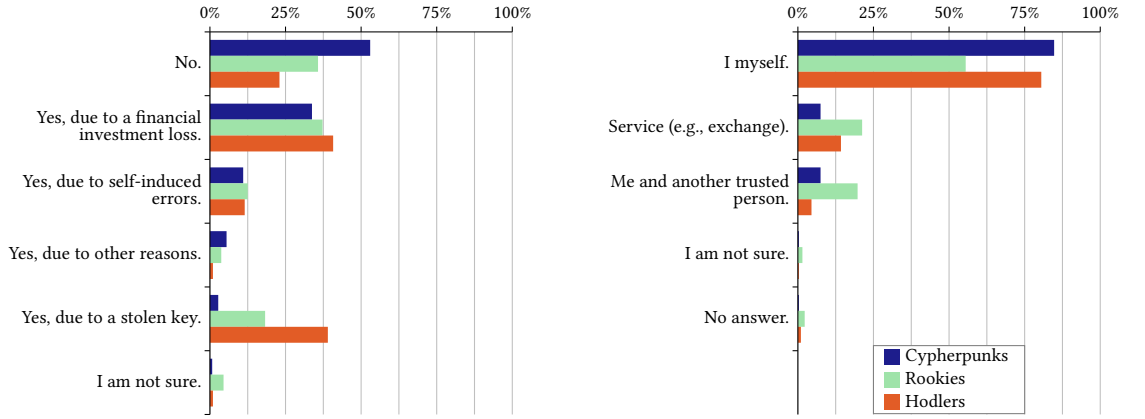
Table 2. Descriptive characteristics of the clusters

Characteristic	Cypherpunks	Rookies	Hodlers	Total
N	145 (36.7%)	137 (34.7%)	113 (28.6%)	395 (100.0%)
Gender				
Men	87.6%	64.2%	80.5%	77.5%
Women	9.7%	32.8%	17.7%	20.0%
Non-binary/third gender	0.0%	1.5%	0.0%	0.5%
Prefer not to answer	2.8%	1.5%	1.8%	2.0%
Age				
Younger than 25	15.2%	13.1%	9.7%	12.9%
25–34 years	35.2%	29.9%	34.5%	33.2%
35–44 years	33.1%	31.4%	46.0%	36.2%
45–54 years	12.4%	22.6%	8.0%	14.7%
55–64 years	2.8%	2.2%	0.9%	2.0%
Prefer not to answer	1.4%	0.7%	0.9%	1.0%
How many years of experience using crypto-assets do you have?				
Less than 1 year	10.3%	16.1%	6.2%	11.1%
1–2 years	17.2%	25.5%	26.5%	22.8%
3–4 years	42.1%	38.0%	43.4%	41.0%
5–6 years	13.8%	17.5%	16.8%	15.9%
More than 6 years	16.6%	2.9%	7.1%	9.1%
How much, in terms of the market value, are you currently holding in crypto-assets?				
Less than USD 1 000	7.6%	13.1%	7.1%	9.4%
USD 1 000 – USD 5 000	18.6%	21.2%	15.9%	18.7%
USD 5 000 – USD 10 000	13.1%	20.4%	20.4%	17.7%
USD 10 000 – USD 100 000	29.7%	29.9%	30.1%	29.9%
More than USD 100 000	14.5%	13.1%	24.8%	17.0%
Prefer not to tell	16.6%	2.2%	1.8%	7.3%
Have you ever traded on conventional financial stock markets? If yes, how often?				
No, I haven't.	31.0%	19.0%	12.4%	21.5%
Yes, I traded once or a few times.	22.1%	33.6%	32.7%	29.1%
Yes, I trade occasionally.	29.0%	33.6%	31.0%	31.1%
Yes, I trade regularly.	17.9%	13.1%	23.0%	17.7%
No answer	0.0%	0.7%	0.9%	0.5%

5.2 Understanding Security Behavior

The identified user typology allows us to study heterogeneous security perceptions and behaviors of crypto-asset users on the cluster level instead of the hard-to-define population level. In particular, all the three clusters appear in both samples and presumably in most populations of interest. The prevalence of each cluster may however vary between countries across the globe. Nevertheless, the user typology remains a strong tool to make more generalizable statements in a domain plagued with sampling difficulties. While we cannot claim that x% of the entire population uses a security practice, we can state that y% of users within a certain cluster report to use that practice.

Monetary losses in the crypto-asset domain are common, and hodlers experienced them more often than cypherpunks and rookies. Almost 40% of hodlers had already fallen victim to key thefts. This presumably explains their high concern about security risks and willingness to take precautions. A similar negative experience is observable for 18% of rookies,



(a) Have you ever lost a substantial amount of crypto-assets at a time? *(multiple choice)*

(b) Who has control over private keys for the majority of your crypto-assets (in terms of value)? *(single choice)*

Fig. 5. Self-reported monetary losses and control over private keys per cluster

as opposed to cypherpunks who mostly avoided this fate. Figure 5a provides an overview of the experienced losses and causes (including thefts of private keys) broken down by cluster.

Rookies appear to refrain from managing their own private keys and often rely on third parties. This is not surprising, considering their low *perceived self-efficacy* and corresponding inability to self-control cryptographic keys. Close to half of rookies (see Figure 5b) also report sharing keys with another trusted person or relying on custodians (e.g., exchanges), which, in both cases, reduces the burden of secure key management.

When it comes to the wallet types used, there is no clear preference among the clusters. This corroborates with the findings of earlier qualitative user studies [71]. In fact, almost 80% of the entire sample report using more than one type, among which the most popular are software, mobile, and hardware wallets (see Figure 6). Software and mobile wallets are usually chosen for their convenience and easy access, whereas hardware wallets are widely recommended for the secure, long-term storage of digital assets [38]. Since this great variety in wallet types was somewhat expected, we shifted our focus of the analysis to the single wallet that stored **most** of the user's funds (marked by a cross symbol in Figure 6). From this perspective, one can recognize an increased tendency toward the use of hardware wallets by cypherpunks, while rookies and hodlers remain consistent with their general wallet preferences.

Prior qualitative work [71] found that individuals choose wallets depending on the exact purpose and amount to be held. In simple terms, users seem to differentiate between cold (offline) storage for long-term, high-value funds and hot (online) storage for short-term, low-value funds. We explore individuals' perceptions in this regard and their effect on user behaviors, both descriptively and statistically. Table 3 shows the means and standard errors for the four perception-checking statements, labeled for brevity as self-control of keys, trust in custodians, reducing risk exposure, and a trade-off between cold and hot storage. Again, cypherpunks strongly endorse the self-management of keys, rookies appear to be the least confident about these storage tactics, while hodlers somewhat naively trust exchanges.

We ran a series of logistic regressions to examine more closely the relationship between the user's perceptions and their wallet choice (as a proxy of self-reported behavior). As for the explanatory variables, we considered the above statements and recoded ordinal responses to the question about the total amount of owned crypto-assets (see Table 2) into a binary variable with a cut-off value of US$10 000. As for the dependent variables, we considered the

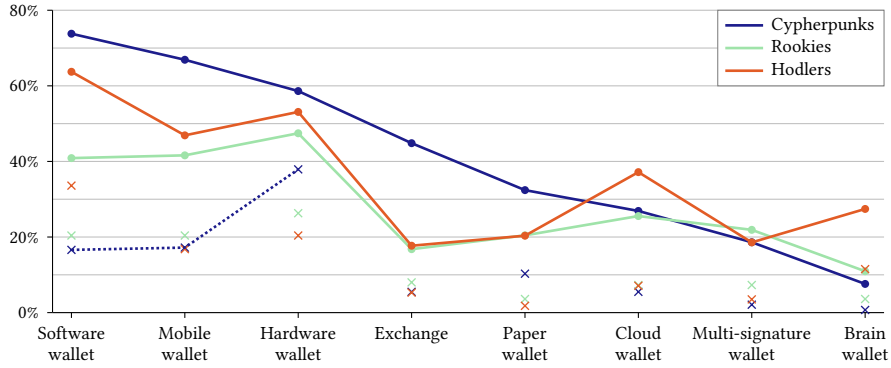


Fig. 6. Self-reported usage of wallets in percentage of users per cluster. Cross symbols refer to the wallet type which holds the majority of the user's funds (*single-choice*).

most common types (i.e., software, hardware, and mobile wallets), other cold (paper or brain wallets), and custodial wallets (i.e., exchanges and cloud wallets). The results of the regression models are presented in Table 8 in Appendix F. Among all the types considered, we quantitatively confirm, as conjectured in prior literature, a significant positive effect between higher holdings and the user's choice of hardware wallets. For each cluster, we estimated how the likelihood of choosing a hardware wallet changes when the total amount of user's funds exceeds the threshold of $10 000. According to the fitted model, this probability increases from 0.32 to 0.46 for cypherpunks, from 0.15 to 0.25 for hodlers, and from 0.21 to 0.33 for rookies. Regarding the perception statements, we find a significant positive correlation between the choice of custodial wallets and one's trust in custodians.

When it comes to security practices (see Table 4), rookies implement them less frequently than cypherpunks or hodlers. Similar discrepancies are found in the work of Ion et al. [37], who compare self-reported security practices of non-expert online users to those of experts. Particularly cypherpunks and hodlers, who are more security-aware and knowledgeable, adhere to best practices, such as backing up wallets and using multi-factor authentication. Conversely, cypherpunks are reluctant to use multi-signature wallets, which require multiple keys to authorize a transaction. Some critical bugs were found in such wallets [52] that likely formed a negative image of this feature, paradoxically introduced for better security control in the first place.

In terms of the protection of devices used to access crypto-assets, cypherpunks tend to take special care of physical security (e.g., by preventing a physical access to a device and protecting it with a unique password). Interestingly, hodlers are less concerned by physical security and, as opposed to cypherpunks, more attentive to online security measures, such as disconnecting devices from the Internet or installing the latest anti-malware software. Again, this is consistent with the fact that cypherpunks prefer hardware wallets for large holdings, as these types of wallets have one of the highest levels of security. The only known weak points to date are sophisticated side-channel attacks [11], which are an unlikely threat scenario for most users. Hodlers, on the contrary, resort more to software wallets, which are particularly exposed to online security threats, such as breaches and phishing [71].

Privacy concerns were prevalent among all clusters. Users were asked to rate their level of concern about the five domain-specific risk scenarios impacting user privacy (Table 3): transaction traceability by different parties (3 items), the leakage of personally identifiable information by exchanges, and information sharing with national tax authorities. The cross-cluster analysis of the mean and standard deviation values (see Table 3) reveals that hodlers are

Table 3. Mean and standard deviation of security and privacy perception statements per cluster. Row maximum in bold (mean) or italics (SD). Reported on a five-point rating scale: 1 – fully disagree/not concerned at all, 5 – fully agree/very concerned.

Questionnaire item	Cypherpunks		Rookies		Hodlers	
	Mean	SD	Mean	SD	Mean	SD
Self-control of my private keys reduces the risk of losing crypto-assets. *(self-control of keys)*	**4.07**	*1.25*	3.29	1.10	3.98	0.86
A well-known and well-regulated exchange is capable of securing my crypto-assets. *(trust in custodians)*	2.92	*1.27*	3.19	1.00	**3.92**	0.87
Minimizing the time my crypto-assets stay in online crypto wallets or exchanges helps me to reduce the risk of losing crypto-assets. *(reducing risk exposure)*	**4.10**	*1.11*	3.31	1.01	3.82	0.92
Separating long- and short-term crypto-assets (e.g., in cold and hot storages) helps me to reduce the risk of losing crypto-assets. *(cold vs. hot storage)*	**4.30**	0.99	3.40	*1.03*	3.97	0.89
To what extent are you concerned about …						
… traceability of transactions by governments?	2.9	*1.3*	3.0	1.0	**3.7**	1.1
… traceability of transactions by firms/private sector?	2.9	*1.4*	3.1	1.0	**3.8**	1.0
… traceability of transactions by individuals?	2.8	*1.3*	3.0	1.0	**3.9**	0.9
… the leakage of personally identifiable information (e.g., e-mail addresses) by crypto-asset exchanges?	3.4	*1.4*	3.0	1.0	**3.8**	1.0
… information sharing with national tax authorities?	2.9	*1.4*	2.8	1.0	**4.0**	1.0

most privacy-concerned and especially fear being taxed on their crypto-asset trading profits. Interestingly, cypherpunks are on average the least concerned by transaction traceability; however, the observed high variance suggests some disagreement within the cluster. Arguably, cypherpunks include "dreamers" or "true Bitcoiners," as defined in [42], who follow the concepts and ideas of Nakamoto's original working paper and truly believe in perfect anonymity and infallibility of the blockchain technology, and "pragmatists," who are aware of well-documented privacy deficiencies of many of the existing crypto-assets [5, 13, 49].

6 DISCUSSION

6.1 Implications for Research

Our study has several implications for usable security and privacy research on crypto-assets. First, we have proposed new domain-specific scale items, which extend established theoretical constructs defined in prior work [36, 39, 76]. The scales have shown high internal consistency and proved to be useful and robust in cluster analysis, compared with classical socio-economic variables. This is further supported by the fact that the discovered clusters are stable in both sampling frames (Qualtrics panel vs. other recruitment channels). We believe that the three emerging user personas – cypherpunks, rookies, and hodlers – present a sufficiently accurate categorization of the contemporary crypto-asset population.

Our findings further extend prior work on user personas in human-computer interaction research. Privacy personas were first defined in the work of Westin [44] and comprise *fundamentalists* (highly concerned), *pragmatists* (somewhat concerned), and the *marginally concerned*. Dupree et al. [20] extended this model to five personas and suggest that security and privacy behaviors differ based on the motivation and knowledge of the respective cluster, with fundamentalists

Table 4. Self-reported security practices in percentage of users within each cluster

Security practice	Cypherpunks	Rookies	Hodlers
Please specify how often you undertake (or undertook) the following security practices. Scale: rarely, occasionally, regularly.	%	%	%
Practices related to backups			
I back(ed) up my crypto wallet.	9 32 59	20 55 24	6 33 61
I generate(d) multiple backups of my crypto wallet.	17 43 41	23 46 31	6 45 49
I encrypt(ed) backups for additional security.	23 29 48	23 52 25	10 42 49
Practices related to secure wallets			
I keep (kept) my hardware wallet and its backup key separately.*	21 76	14 43 43	5 37 58
I use(d) a multi-signature crypto wallet out of security concerns.	43 33 23	34 38 28	5 58 37
Practices related to custodial wallets			
I store(d) my crypto-assets in a reputable online wallet or exchange.	17 38 46	11 56 33	46 50
I enable(d) a multi-factor authentication for my online account(s).	6 16 79	11 54 35	37 61
Practices related to key protection			
I disconnect(ed) from the Internet before creating private keys.	35 23 41	34 39 28	19 40 42
I store(d) private keys differently depending on the purpose and amount of crypto-assets.	23 34 43	24 51 25	6 50 44
Practices related to devices			
A device I use(d) to access my crypto-assets …			
… is/was not used by anyone else.	6 22 72	15 47 38	45 52
… has/had a unique password.	8 21 71	13 53 34	5 34 61
… is/was kept in a physically secured location.	12 34 53	23 45 31	53 43
… is/was equipped with the latest malware protection.	16 26 59	23 43 34	42 55
… is/was not connected to the Internet.	36 34 30	29 47 23	10 44 46

* Valid for the respondents who self-reported using hardware wallets.

being the most motivated and knowledgeable. For crypto-assets, the presence of different security personas was first suggested by Fröhlich et al. [25], who compared fundamentalists against the marginally concerned with regard to the use of custodial and non-custodial crypto wallets. The authors suggest that the fundamentalists value control over their private keys, whereas the marginally concerned trust websites and consider key management a burden. However, the characteristics of these user groups were not discussed by the authors any further due to the qualitative nature of the study.

This work fills this gap, confirms the key management dichotomy, and provides the in-depth characterization of the user groups based on empirical evidence. This is achieved through an integration of the psychometric and multidimensional data, with many of the analyzed variables being orthogonal to the construct variables.

We further employed a novel combination of the recruitment strategies, including the use of a commercial panel. Prior work has successfully shown that specific user populations, such as owners of smart home devices [68] or fitness trackers [26], can be recruited through such means. Our study gives some indications that crypto-asset users are not an exception. Employing both deep and broad sampling allowed us to target a more diverse crypto-asset user population, the heterogeneity of which is evident in the results of cluster analysis. The vast majority of users recruited through the panel were hodlers, with cypherpunks and rookies being underrepresented, whereas most cypherpunks, on the other hand, were recruited through our targeted campaigns (see Table 6 in Appendix B).

It should be emphasized, however, that each sampling strategy comes with its own share of trade-offs. In our case, the recruitment periods differed significantly, with the targeted campaigns running for four months and the broad sampling through Qualtrics only for three days. This striking divergence is due to difficulties that we experienced throughout the targeted deep campaigns, caused largely by security and privacy concerns of potential participants. Yet, the respondents who completed our online questionnaire provided quality responses and took nearly twice as long (16.5 vs. 9 minutes) when compared to the participants recruited through Qualtrics. In the latter case, we observed more low-quality responses, including straight-liners, very quick completion times, and failed attention checks. These measures contributed to the four iterations needed to reach the target of 200 quality responses. Despite the method-specific challenges we encountered, we strongly believe that the combination of both sampling strategies allowed us to gather responses from a broader spectrum of crypto-asset users, which has been unparalleled in published research in this emerging domain.

Consequently, this study also provides an updated and possibly more accurate overview of the current crypto-asset user population, including its security and privacy perceptions and behaviors. Prior work has either focused exclusively on Bitcoin [1, 43] or produced findings that were hard to generalize because of the small sample size [25, 27, 47, 63, 71]. Studies surveying the Bitcoin user population were also predominantly of male users, with Bohr and Bashir [9] only finding 5% female users in 2014, and Krombholz et al. [43] reporting 10% female users in 2015. In our study, 20% of participants are women. Arguably, this development hints at a trend of increasing diversity, particularly when considering the cluster of rookies. While this trend is promising, it is still an open research question how to make crypto-asset use more accessible to underrepresented groups.

6.2 Design Implications

Our results suggest that the crypto-asset user population is composed of homogeneous groups that differ in their security behaviors, motives, and backgrounds. Consequently, the decision for or against a specific crypto wallet depends on a variety of the user's idiosyncratic characteristics. An entry questionnaire could provide guidance for users in choosing the "right" wallet for depositing funds. For example, cypherpunks and hodlers are fairly knowledgeable and value the option of being solely responsible for their private keys, whereas rookies are not as confident in their abilities. Our scales could be used to assess the self-efficacy of individuals and refined to provide wallet recommendations. For rookies, these would be custodial solutions, such as Coinbase[6] or Binance,[7] and non-custodial solutions would be recommended for the more experienced users.

The requirements for tools also differ based on the group they are intended to support. Modern crypto wallets mostly provide a "one-size-fits-all" solution, which is impractical considering the varying levels of expertise among users. Prior work has shown that newcomers are often confused by the complex terminology and metaphors used in current wallets [22, 71]. While one cannot expect wallet providers to develop tailored solutions for each user group, the implementation of default user profiles seems feasible. Perhaps, a *novice user profile* would not provide advanced transactions options, custom fees, and the export of private keys, whereas an *expert user profile* would support these options. *Wallet personalization* would benefit all three of the identified clusters in this study, providing rookies with an abstraction layer while also supporting more advanced hodlers and cypherpunks.

Personalization could also go beyond the interface alone and be applied to more effective risk communication. Studies have shown that users are often not aware of where their private keys are being stored [71] and this confusion leads to

[6]Coinbase: www.coinbase.com
[7]Binance: www.binance.com

inadequate risk assessment. To address this, wallet providers should be more transparent about the key management, particularly when it comes to the storage practices. Prior work [21, 59] has shown that more transparent, comprehensible, and actionable security warnings can lead to better security practices, and we believe that similar enhancements could be made in the context of crypto-asset key management. Particularly cypherpunks and hodlers, who both understand the nature of keys, would be able to assess the risks and could make an educated decision about a key management solution at hand.

For rookies, a hybrid wallet approach, as defined by Fröhlich et al. [25], could be used to enhance the UX. The vast majority of crypto wallets nowadays are either custodial or non-custodial. Encrypted cloud backups could provide a viable option for new users with small amounts of crypto-assets. The private keys could be encrypted on the respective device and saved to a cloud service, similar to the beginner version of the Casa wallet.[8] Casa, however, only supports bitcoin, and we believe that similar approaches could also work for other crypto-assets.

Hodlers could also be supported by already existing technology. Hodlers are profit-oriented traders and have reported losing significant amounts in the past. Decentralized exchanges, such as Uniswap,[9] allow users to trade crypto-assets while being in sole possession of their keys at the same time. These exchanges would suit the needs of hodlers, and yet, overall, only 5 out of 395 participants have reported using such platforms. Understanding why these types of exchanges are not more popular could be the object of future studies.

Overall, our findings suggest that there is no silver bullet for crypto-asset key management practices because of the significant differences among the identified user groups. These groups and their needs have to be likewise considered when making design decisions for CBDCs. If the goal of such systems is inclusiveness, then they cannot offer only custodial or non-custodial solutions. Users should be given the choice to decide themselves and should be supported throughout to guarantee that an educated decision is being made. It is equally important that the risks are communicated effectively and that the users understand the benefits and dangers of custodial and non-custodial solutions. This becomes of utmost importance in light of the number of newcomers – potentially hundreds of millions – that a widespread adoption of CBDCs might bring and the grave consequences that could result from self-induced errors.

6.3 Limitations and Future Work

This work has a number of limitations typical for empirical studies of crypto-assets. In particular, our analysis is based on self-reports, which are potentially skewed toward socially desirable responses or biased due to cognitive influences or repeated survey participation. We also relied on self-reported claims in screening out users and non-users of crypto-assets, which could have affected an unobservable (to us) coverage error. Furthermore, prior research on gender and technology use has found that women appear to rank their technological skills lower than men [29]. This tendency to self-underestimation may have unwittingly biased the cluster analysis results, especially considering the higher proportion of women in the rookies cluster.

Using the general term "device" in the security practice statements may have confused some respondents. The "device to access crypto-assets" may take many forms, such as a computer, an external hardware storage device, or a mobile phone. Unfortunately, the question wording used allows us neither to distinguish between these devices nor to provide a more nuanced view of the ways they are protected by users. We also acknowledge that our study is limited in its focus on security practices. Future empirical research should explore which privacy practices crypto-asset users adopt, and for what reasons.

[8]Casa Wallet: https://decrypt.co/32448/casa-launches-free-private-crypto-wallet-for-bitcoin-beginners
[9]Uniswap: www.uniswap.org

From a theoretical perspective, future work is needed to validate some of our hypothesized observations about the user groups. Since cluster analysis was performed after the data collection, no a priori knowledge about the user typology was taken into consideration at the survey design stage. We therefore encourage further empirical research, for example, in the realm of *FoMO-centric design* [74], to study whether the psychometric construct *fear of missing out* may affect security and privacy behaviors of users, especially those of hodlers and rookies. Similarly, both research and practice will benefit from developing scale items for the objective measurement of user literacy about crypto-assets, cryptographic keys, and wallet types. The first attempt to this end was presented in a representative survey done by the Bank of Canada [32], which included 8 true/false statements testing the respondent's knowledge of Bitcoin and cryptocurrencies. Extending this to security- and privacy-related questions will provide additional insights about the self-reported efficacy of cypherpunks. Another potentially fruitful area of research is to investigate contrasts in risk perceptions and security behaviors of crypto-asset users in a cross-national context [12]. Our sample includes a large fraction of users from North America and Europe, thereby giving an opportunity for examining significant differences between these two regions.

From a practical perspective, it is desirable to reduce the number of scale items used to measure the psychometric constructs to a smaller set of checklist questions, while still striving for (at least) the same accuracy and robustness of the user profiling. Designers of coin management solutions would particularly benefit from a shorter list in providing more informed wallet recommendations to users. The expressiveness and reliability of these indicator questions could be first validated by a larger convenience sample or, ideally, in representative studies of national populations.

7 CONCLUSION

To the best of our knowledge, this study is the first to examine the relation between individuals' risk perceptions and security behavior in a stratified sample of crypto-asset users recruited through a mixed sampling strategy. We demonstrate that the use of a robust, theory-guided approach to scale construction together with cluster analysis renders the quantitative analysis of security behaviors more tractable and instructive. We offer a validated method for drawing fairly homogeneous groups of crypto-asset users from empirical data and present its utility in providing generalizable insights about the hard-to-reach population.

The key theme of our analyses is that crypto-asset users differ in their security and risk perceptions, and these heterogeneous beliefs affect their crypto wallet decisions and security practices. In spite of this heterogeneity, one can however distinguish between the three characteristic groups of users. Cypherpunks opt for self-managed security solutions, whereas hodlers and rookies appear to face a non-trivial dilemma between risk-prone but convenient custodial solutions and secure but more burdensome non-custodial wallets. Interestingly, this decision resembles the basic question of whether to stash money under the mattress or entrust banks with taking care of savings. We argue that there is no one-size-fits-all solution in this domain, and greater personalization of tools and informational and educational materials is required to address the idiosyncratic needs of different user groups.

ACKNOWLEDGMENTS

We would like to thank Martin Summer and Helmut Stix from the Austrian Central Bank (OeNB) for their valuable comments on the survey instrument, our colleagues Daniel W. Woods and Michael Fröwis for helpful comments and suggestions on the paper draft, and Bernhard Ertel for translating the questionnaire into German. We thank the anonymous reviewers for their valuable comments, and our research and industry partners for their help with recruiting participants. This work is funded by the Austrian security research programme KIRAS of the Federal Ministry of

Agriculture, Regions and Tourism (BMLRT) under project KRYPTOMONITOR (879686) and a gift from Scotiabank to the University of British Columbia.

REFERENCES

[1] Svetlana Abramova and Rainer Böhme. Perceived Benefit and Risk as Multidimensional Determinants of Bitcoin Use: A Quantitative Exploratory Study. In *Proceedings of the Thirty Seventh International Conference on Information Systems (ICIS)*, Dublin, Ireland, 2016.

[2] Anne Adams and Martina Angela Sasse. Users Are Not the Enemy. *Communications of the ACM*, 42(12):40–46, 1999.

[3] Icek Ajzen. The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, 50(2):179–211, 1991.

[4] Sarah Allen, Srđjan Čapkun, Ittay Eyal, Giulia Fanti, Bryan A Ford, James Grimmelmann, Ari Juels, Kari Kostiainen, Sarah Meiklejohn, Andrew Miller, et al. Design Choices for Central Bank Digital Currency: Policy and Technical Considerations. Technical report, National Bureau of Economic Research, 2020.

[5] Elli Androulaki, Ghassan O Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun. Evaluating User Privacy in Bitcoin. In *International Conference on Financial Cryptography and Data Security*, pages 34–51. Springer, 2013.

[6] Raphael Auer and Rainer Böhme. The Technology of Retail Central Bank Digital Currency. *BIS Quartely Review*, pages 85–100, March 2020.

[7] Aaron W. Baur, Julian Bühler, Markus Bick, and Charlotte S. Bonorden. Cryptocurrencies as a Disruption? Empirical Findings on User Adoption and Future Potential of Bitcoin and Co. In Marijn Janssen, Matti Mäntymäki, Jan Hidders, Bram Klievink, Winfried Lamersdorf, Bastiaan van Loenen, and Anneke Zuiderwijk, editors, *Conference on e-Business, e-Services and e-Society*, pages 63–80, Cham, 2015. Springer, Springer International Publishing.

[8] Rainer Böhme, Nicolas Christin, Benjamin Edelman, and Tyler Moore. Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives*, 29(2):213–238, 2015.

[9] Jeremiah Bohr and Masooda Bashir. Who Uses Bitcoin? An Exploration of the Bitcoin Community. In *Twelfth Annual International Conference on Privacy, Security and Trust*, pages 94–101, Toronto, Canada, 2014. IEEE.

[10] Scott R. Boss, Dennis F. Galletta, Paul Benjamin Lowry, Gregory D. Moody, and Peter Polak. What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors. *MIS Quarterly*, 39(4):837–864, 2015.

[11] Chaos Computer Congress. Attacks on Hardware Wallets. https://wallet.fail/, 2020. Accessed: 2020-09-14.

[12] Yan Chen and Fatemeh M. Zahedi. Individual's Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China. *MIS Quarterly*, 40(1):205–222, 2016.

[13] Mauro Conti, E Sandeep Kumar, Chhagan Lal, and Sushmita Ruj. A Survey on Security and Privacy Issues of Bitcoin. *IEEE Communications Surveys & Tutorials*, 20(4):3416–3452, 2018.

[14] Lee J. Cronbach. Coefficient Alpha and the Internal Structure of Tests. *Psychometrika*, 16(3):297–334, 1951.

[15] Robert Crossler and France Bélanger. An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, 45(4):51–71, 2014.

[16] William A. Cunningham, Kristopher J. Preacher, and Mahzarin R. Banaji. Implicit Attitude Measures: Consistency, Stability, and Convergent Validity. *Psychological science*, 12(2):163–170, 2001.

[17] Poulami Das, Sebastian Faust, and Julian Loss. A Formal Treatment of Deterministic Wallets. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, CCS '19, pages 651–668, New York, NY, USA, 2019. Association for Computing Machinery.

[18] Fred D. Davis. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, 13(3):319–340, 1989.

[19] Tamara Dinev and Paul Hart. An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, 17(1):61–80, 2006.

[20] Janna Lynn Dupree, Richard Devries, Daniel M. Berry, and Edward Lank. Privacy Personas: Clustering Users via Attitudes and Behaviors toward Security Practices. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 5228–5239, New York, NY, USA, 2016. Association for Computing Machinery.

[21] Serge Egelman and Stuart Schechter. The Importance of Being Earnest [In Security Warnings]. In *International Conference on Financial Cryptography and Data Security*, pages 52–59. Springer, 2013.

[22] Shayan Eskandari, Jeremy Clark, David Barrera, and Elizabeth Stobert. A First Look at the Usability of Bitcoin Key Management. *Proceedings of the 2015 Workshop on Usable Security (USEC)*, 2015.

[23] Giulia Fanti, Leonid Kogan, Sewoong Oh, Kathleen Ruan, Pramod Viswanath, and Gerui Wang. Compounding of Wealth in Proof-of-Stake Cryptocurrencies. In *International Conference on Financial Cryptography and Data Security*, pages 42–61. Springer, 2019.

[24] Dinei Florencio and Cormac Herley. A Large-Scale Study of Web Password Habits. In *Proceedings of the 16th International Conference on World Wide Web – WWW '07*, pages 657–666, New York, NY, USA, 2007. Association for Computing Machinery.

[25] Michael Fröhlich, Felix Gutjahr, and Florian Alt. Don't Lose Your Coin! Investigating Security Practices of Cryptocurrency Users. In *Proceedings of the 2020 ACM Designing Interactive Systems Conference*, pages 1751–1763. Association for Computing Machinery, 2020.

[26] Sandra Gabriele and Sonia Chiasson. Understanding Fitness Tracker Users' Security and Privacy Knowledge, Attitudes and Behaviours. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–12, New York, NY, USA, 2020. Association for Computing Machinery.

[27] Xianyi Gao, Gradeigh D. Clark, and Janne Lindqvist. Of Two Minds, Multiple Addresses, and One Ledger: Characterizing Opinions, Knowledge, and Perceptions of Bitcoin Across Users and Non-Users. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 1656–1668, New York, NY, USA, 2016. Association for Computing Machinery.

[28] Gerry Grant and Robert Hogan. Bitcoin: Risks and Controls. *Journal of Corporate Accounting & Finance*, 26(5):29–35, 2015.

[29] Eszter Hargittai and Steven Shafer. Differences in Actual and Perceived Online Skills: The Role of Gender. *Social Science Quarterly*, 87(2):432–448, 2006.

[30] Eiji Hayashi and Jason Hong. A Diary Study of Password Usage in Daily Life. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2627–2630, New York, NY, USA, 2011. Association for Computing Machinery.

[31] Douglas D. Heckathorn. Respondent-Driven Sampling: A New Approach to the Study of Hidden Populations. *Social Problems*, 44(2):174–199, 1997.

[32] Christopher S. Henry, Kim Huynh, and Gradon Nicholls. Bitcoin Awareness and Usage in Canada. *Journal of Digital Banking*, 2(4):311–337, 2018.

[33] Christopher S. Henry, Kim Huynh, Gradon Nicholls, and Mitchell Nicholson. 2018 Bitcoin Omnibus Survey: Awareness and Usage. Technical report, Bank of Canada, 2019.

[34] Garrick Hileman and Michel Rauchs. Global Cryptocurrency Benchmarking Study. *Cambridge Centre for Alternative Finance*, 33:33–113, 2017.

[35] Sabrina T. Howell, Marina Niessner, and David Yermack. Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sales. *The Review of Financial Studies*, 33(9):3925–3974, 2020.

[36] Princely Ifinedo. Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory. *Computers & Security*, 31(1):83–95, 2012.

[37] Iulia Ion, Rob Reeder, and Sunny Consolvo. "…No One Can Hack my Mind": Comparing Expert and Non-Expert Security Practices. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security*, SOUPS '15, pages 327–346, USA, 2015. USENIX Association.

[38] Samvit Jain, Edward Felten, and Steven Goldfeder. Determining an Optimal Threshold on the Online Reserves of a Bitcoin Exchange. *Journal of Cybersecurity*, 4(1):1–12, 2018.

[39] Allen C. Johnston and Merrill Warkentin. Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, 34(3):549–566, September 2010.

[40] Irni Eliana Khairuddin and Corina Sas. An Exploration of Bitcoin Mining Practices: Miners' Trust Challenges and Motivations. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–13, New York, NY, USA, 2019. Association for Computing Machinery.

[41] Irni Eliana Khairuddin, Corina Sas, Sarah Clinch, and Nigel Davies. Exploring Motivations for Bitcoin Technology Usage. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, pages 2872–2878, New York, NY, USA, 2016. Association for Computing Machinery.

[42] Megan Knittel, Shelby Pitts, and Rick Wash. "The Most Trustworthy Coin": How Ideological Tensions Drive Trust in Bitcoin. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), 2019.

[43] Katharina Krombholz, Aljosha Judmayer, Matthias Gusenbauer, and Edgar Weippl. The Other Side of the Coin: User Experiences with Bitcoin Security and Privacy. In Jens Grossklags and Bart Preneel, editors, *Financial Cryptography and Data Security*, pages 555–580, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.

[44] Ponnurangam Kumaraguru and Lorrie Faith Cranor. *Privacy Indexes: A Survey of Westin's Studies.* Carnegie Mellon University, School of Computer Science, 2005.

[45] Younghwa Lee, Kenneth A. Kozar, and Kai R.T. Larsen. The Technology Acceptance Model: Past, Present, and Future. *Communications of the Association for Information Systems*, 12(1):752–780, 2003.

[46] Dominique Machuletz, Stefan Laube, and Rainer Böhme. Webcam Covering as Planned Behavior. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–13, New York, NY, USA, 2018. Association for Computing Machinery.

[47] Alexandra Mai, Katharina Pfeffer, Matthias Gusenbauer, Edgar Weippl, and Katharina Krombholz. User Mental Models of Cryptocurrency Systems – A Grounded Theory Approach. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS)*, pages 341–358, 2020.

[48] Tyler Moore, Nicolas Christin, and Janos Szurdi. Revisiting the Risks of Bitcoin Currency Exchange Closure. *ACM Transactions on Internet Technology (TOIT)*, 18(4):1–18, 2018.

[49] Malte Möser, Kyle Soska, Ethan Heilman, Kevin Lee, Henry Heffan, Shashvat Srivastava, Kyle Hogan, Jason Hennessey, Andrew Miller, Arvind Narayanan, et al. An Empirical Analysis of Traceability in the Monero Blockchain. *Proceedings on Privacy Enhancing Technologies*, 2018(3):143–163, 2018.

[50] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

[51] Bank of England. Central Bank Digital Currency: Opportunities, Challenges and Design, 2020.

[52] OpenZeppelin. The Parity Wallet Hack Explained. https://blog.openzeppelin.com/on-the-parity-wallet-multisig-hack-405a8c12e8f7/, 2020. Accessed: 2020-09-14.

[53] Lawrence A. Palinkas, Sarah M. Horwitz, Carla A. Green, Jennifer P. Wisdom, Naihua Duan, and Kimberly Hoagwood. Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and policy in mental health and mental health services research*, 42(5):533–544, 2015.

[54] Paul A. Pavlou. Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. *International Journal of Electronic Commerce*, 7(3):69–103, 2003.

[55] Sarah Pearman, Jeremy Thomas, Pardis Emami Naeini, Hana Habib, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, and Alain Forget. Let's Go in for a Closer Look: Observing Passwords in Their Natural Habitat. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 295–310, Dallas Texas USA, October 2017. Association for Computing Machinery.

[56] Bruce D. Rapkin and Douglas A. Luke. Cluster analysis in Community Research: Epistemology and Practice. *American Journal of Community Psychology*, 21(2):247–277, 1993.

[57] Michel Rauchs, Apolline Blandin, Kristina Klein, Gina C. Pieters, Martino Recanatini, and Bryan Zheng Zhang. 2nd Global Cryptoasset Benchmarking Study. *Available at SSRN 3306125*, 2018.

[58] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. 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)*, pages 1326–1343, 2019.

[59] Robert W Reeder, Adrienne Porter Felt, Sunny Consolvo, Nathan Malkin, Christopher Thompson, and Serge Egelman. An Experience Sampling Study of User Reactions to Browser Warnings in the Field. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2018.

[60] Jeff John Roberts and Nicolas Rapp. Nearly 4 Million Bitcoins Lost Forever, New Study Says. Fortune, 2017. 25 November 2017.

[61] Ronald W. Rogers. A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology*, 91(1):93–114, 1975.

[62] Scott Ruoti, Jeff Andersen, Daniel Zappala, and Kent Seamons. Why Johnny Still, Still Can't Encrypt: Evaluating the Usability of a Modern PGP Client. *arXiv:1510.08555 [cs]*, January 2016. arXiv: 1510.08555.

[63] Corina Sas and Irni Eliana Khairuddin. Design for Trust: An Exploration of the Challenges and Opportunities of Bitcoin Users. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 6499–6510, New York, NY, USA, 2017. Association for Computing Machinery.

[64] Helmut Stix. Ownership and purchase intention of crypto-assets – survey results. Oesterreichische Nationalbank Working Papers (Austria), 2019.

[65] Elizabeth Stobert and Robert Biddle. The Password Life Cycle. *ACM Transactions on Privacy and Security*, 21(3):13, 2018.

[66] Peter Story, Daniel Smullen, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. From Intent to Action: Nudging Users Towards Secure Mobile Payments. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS)*, pages 379–415, 2020.

[67] Minhyang Suh and Gary Hsieh. Designing for Future Behaviors: Understanding the Effect of Temporal Distance on Planned Behaviors. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 1084–1096, New York, NY, USA, 2016. Association for Computing Machinery.

[68] Madiha Tabassum, Jess Kropczynski, Pamela Wisniewski, and Heather Richter Lipford. Smart Home Beyond the Home: A Case for Community-Based Access Control. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–12, New York, NY, USA, 2020. ACM.

[69] Keith S. Taber. The Use of Cronbach's Alpha when Developing and Reporting Research Instruments in Science Education. *Research in Science Education*, 48(6):1273–1296, 2018.

[70] L. Tam, M. Glassman, and M. Vandenwauver. The Psychology of Password Management: A Tradeoff Between Security and Convenience. *Behaviour & Information Technology*, 29(3):233–244, May 2010.

[71] Artemij Voskobojnikov, Borke Obada-Obieh, Yue Huang, and Konstantin Beznosov. Surviving the Cryptojungle: Perception and Management of Risk Among North American Cryptocurrency (Non) Users. In *International Conference on Financial Cryptography and Data Security*, pages 595–614. Springer, 2020.

[72] Artemij Voskobojnikov, Oliver Wiese, Masoud Mehrabi-Koushki, Volker Roth, and Konstantin Beznosov. The U in Crypto Stands for Usable: An Empirical Study of User Experience with Mobile Cryptocurrency Wallets. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021.

[73] Rick Wash, Emilee Rader, Ruthie Berman, and Zac Wellmer. Understanding Password Choices: How Frequently Entered Passwords are Re-used across Websites. In *Proceedings of the Twelfth USENIX Conference on Usable Privacy and Security*, page 175–188, USA, 2016. USENIX Association.

[74] Fiona Westin and Sonia Chiasson. Opt out of Privacy or "Go Home": Understanding Reluctant Privacy Behaviours through the FoMO-Centric Design Paradigm. In *Proceedings of the New Security Paradigms Workshop*, NSPW '19, page 57–67, New York, NY, USA, 2019. ACM.

[75] Alma Whitten and J D Tygar. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8*, page 15. USENIX Association, 1999.

[76] Hsin yi Sandy Tsai, Mengtian Jiang, Saleem Alhabash, Robert LaRose, Nora J. Rifon, and Shelia R. Cotten. Understanding Online Safety Behaviors: A Protection Motivation Theory Perspective. *Computers & Security*, 59:138 – 150, 2016.

Appendices

A CONSTRUCT SCALE ITEMS

Table 5. Proposed constructs, scale items,* and Cronbach's alpha

Scale item	Source(s)	Mean	SD
Perceived vulnerability	$\alpha = 0.90$		
My crypto wallet is at risk of being compromised.	[36, 39, 76]	2.8	1.3
The risk of my crypto wallet being compromised is high.		2.7	1.4
It is likely that someone abuses private keys of my crypto-assets.		2.6	1.4
It is likely that someone makes criminal transactions in my account.		2.5	1.4
Perceived severity	$\alpha = 0.79$		
Losing crypto-assets would require serious efforts from me to compensate for the loss.	[39], self-developed	3.6	1.1
Losing crypto-assets would likely cause me severe stress.		3.7	1.1
Losing crypto-assets would likely negatively impact my daily life.		3.4	1.2
Losing crypto-assets would significantly compromise my financial situation.		3.3	1.2
Perceived self-efficacy	$\alpha = 0.83$		
I am able to protect my private keys from being stolen.	[36, 39, 76]	3.9	1.0
I am able to prevent unauthorized access to my crypto wallet.		3.9	1.0
I have technical skills and time to secure and prevent the theft of my crypto-assets.		3.8	1.1
I find it easy to secure my crypto wallet.		3.8	1.1
Response cost	$\alpha = 0.84$		
Securing crypto-assets is costly.	self-developed	3.2	1.1
Keeping security measures for crypto-assets up-to-date is costly.		3.2	1.1
Security investments into equipment are costly.		3.3	1.2
Staying informed about secure crypto wallets is costly.		3.3	1.1
Spending crypto-assets from secure crypto wallets is costly.		3.1	1.2
Perceived concern	$\alpha = 0.77$		
I am concerned about the theft of private keys.	[19]	3.3	1.2
I am concerned about the risk of being extorted.		3.1	1.3
I am concerned about losing crypto-assets by my own mistakes.		3.2	1.2
I am concerned about security vulnerabilities of wallets.		3.3	1.1
I am concerned about security vulnerabilities of exchanges.		3.6	1.1

* Reported on a five-point rating scale: 1 – fully disagree/not concerned at all, 5 – fully agree/very concerned.

B COMPARISON OF SAMPLING FRAME DEMOGRAPHICS

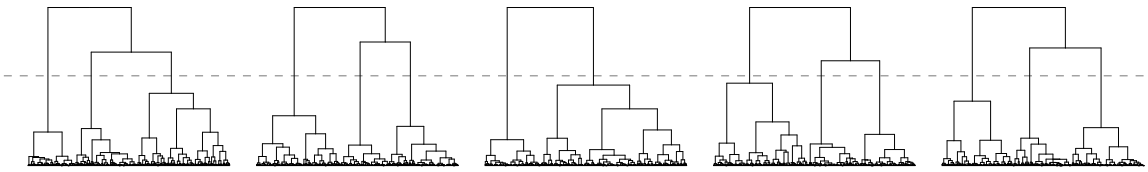
Table 6. Comparison of demographics between the subsamples

Characteristic	Qualtrics (June 2020)		Other channels (February–June 2020)	
	Absolute	Relative	Absolute	Relative
Size	200	100%	195	100%
Gender				
Male	151	75.5%	155	79.5%
Female	49	24.5%	30	15.4%
Non-binary/third gender	0	-	2	1.0%
Prefer not to answer	0	-	8	4.0%
Age				
Younger than 25	23	11.5%	28	14.4%
25–34 years	53	26.5%	78	40.0%
35–44 years	93	46.5%	50	25.6%
45–54 years	26	13.0%	32	16.4%
55–64 years	5	2.5%	3	1.5%
Prefer not to answer	0	-	4	2.0%
Education				
High school incomplete	5	2.5%	13	6.7%
High school graduate (or an equivalent)	18	9.0%	45	23.1%
College or associate degree	18	9.0%	36	18.5%
Bachelor's degree	55	27.5%	45	23.1%
Master's degree	75	37.5%	34	17.4%
Doctoral degree	26	13.0%	5	2.6%
Other postgraduate or professional degree	3	1.5%	8	4.1%
Prefer not to answer	0	-	9	4.6%
Occupation				
Student	7	3.5%	17	8.7%
Skilled manual worker	5	2.5%	10	5.1%
Employed position in a service job	51	25.5%	20	10.3%
Self-employed/freelancer	15	7.5%	49	25.1%
Unemployed or temporarily not working	3	1.5%	14	7.2%
Retired or unable to work through illness	3	1.5%	4	2.1%
Employed professional	111	55.5%	63	32.3%
Other	2	1.0%	8	4.1%
Prefer not to answer	3	1.5%	10	5.1%
Country of residence				
Americas	**200**	100%	**101**	**51.8%**
United States of America	200	100%	35	18.0%
Canada	0	-	61	31.3%
Other	0	-	5	2.6%
Europe	0	-	**56**	**28.7%**
Austria	0	-	23	11.8%
Germany	0	-	10	5.1%
Other	0	-	23	11.8%
Rest of the world	0	-	**7**	**3.6%**
Prefer not to answer	0	-	**31**	**15.9%**
Cluster				
Cypherpunks	53	26.5%	92	47.2%
Rookies	61	30.5%	76	39.0%
Hodlers	86	43.0%	27	13.8%

C CRYPTO WALLET TYPES

Crypto wallet type	Explanation
Software wallet	A software wallet is specialized software downloaded and installed on users' personal devices (e.g., Bitcoin Core client, Armory, Electrum, or Hive).
Mobile wallet	A mobile wallet is an online account with an external provider that keeps required files in a shared server with access via the phone apps.
Hardware wallet	A hardware wallet refers to the way of storing private keys on an external highly secure hardware device (e.g., Ledger or Trezor).
Paper wallet	A paper wallet refers to the way of storing private keys offline on a physical document.
Brain wallet	A brain wallet refers to the way of storing private keys in one's own mind by memorization of a pass-phrase.
Cloud/online wallet	A cloud/online wallet is an online account with an external provider that keeps required files in a shared server with access via the web.
Multi-signature wallet	A multi-signature wallet requires more than one private key to authorize a transaction.

D CLUSTER DENDROGRAMS



(a) w/o *perceived vulnerability* (b) w/o *perceived severity* (c) w/o *perceived self-efficacy* (d) w/o *response cost* (e) w/o *perceived concern*

Fig. 7. Dendrograms for the cluster analysis without (w/o) one of the five constructs

E CRYPTO-ASSETS USED

Table 7. Self-reported usage of crypto-assets in percentage of users within each cluster

Crypto-asset(s) used	Cypherpunks	Rookies	Hodlers
Color coding: ■ used exclusively, ■ used among other crypto-assets, ■ not used at all.	%	%	%
Bitcoin	10 79 11	14 48 38	11 70 19
Ethereum	70 30	38 60	44 56
Litecoin	33 66	25 74	43 56
Bitcoin Cash	33 67	30 68	44 56
Privacy cryptocurrencies (Monero, Dash, and Zcash)	32 66	5 36 59	42 55
Other cryptocurrencies	48 51	7 36 57	40 58
Digital tokens	21 79	96	97

F RESULTS OF LOGISTIC REGRESSION MODELS

Table 8. Results of the logistic regression models

	Hardware wallet	Software wallet	Mobile wallet	Other cold wallet	Custodial wallet	Custodial wallet
Value at risk						
> $10 000 of total funds	0.60^{**}	-0.40	-0.11	0.38	-0.26	
	(0.23)	(0.25)	(0.26)	(0.33)	(0.31)	
Security perceptions						
Self-control of keys						0.15
						(0.16)
Trust in custodians						0.33^{*}
						(0.15)
Reducing risk exposure						-0.14
						(0.16)
Cold vs. hot storage						0.09
						(0.18)
Control variables						
Cypherpunks	-0.77^{***}	-1.46^{***}	-1.52^{***}	-2.27^{***}	-1.98^{***}	-3.56^{***}
	(0.20)	(0.24)	(0.25)	(0.32)	(0.29)	(1.03)
Rookies	-1.31^{***}	-1.20^{***}	-1.31^{***}	-2.72^{***}	-1.60^{***}	-3.13^{***}
	(0.23)	(0.23)	(0.24)	(0.37)	(0.27)	(0.89)
Hodlers	-1.72^{***}	-0.47^{*}	-1.54^{***}	-2.10^{***}	-1.82^{***}	-3.71^{***}
	(0.28)	(0.24)	(0.29)	(0.35)	(0.32)	(1.06)
Log likelihood	−228.78	−205.32	−187.14	−129.75	−151.01	−147.38
McFadden's R^2	0.16	0.25	0.32	0.53	0.45	0.46
Number of total observations	395	395	395	395	395	395
… of which choose this wallet:	114	90	72	41	51	51

Significance level: $^{***}p < 0.001$; $^{**}p < 0.01$; $^{*}p < 0.05$