Towards Understanding and Improving the Crypto-Asset User Experience

by

Artemij Voskobojnikov

B.Sc., Free University of Berlin, 2015

M.Sc., Free University of Berlin, 2017

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF

Doctor of Philosophy

in

THE FACULTY OF GRADUATE AND POSTDOCTORAL STUDIES

(Electrical and Computer Engineering)

The University of British Columbia

(Vancouver)

September 2021

© Artemij Voskobojnikov, 2021

The following individuals certify that they have read, and recommend to the Faculty of Graduate and Postdoctoral Studies for acceptance, the thesis entitled:

Towards Understanding and Improving the Crypto-Asset User Experience

submitted by **Artemij Voskobojnikov** in partial fulfillment of the requirements for the degree of **Doctor of Philosophy** in **Electrical and Computer Engineering**.

Examining Committee:

Konstantin Beznosov, Professor, Electrical and Computer Engineering, UBC
Supervisor

Victoria Lemieux, Associate Professor, School of Information, UBC
Supervisory Committee Member

Julia Rubin, Assistant Professor, School of Information, UBC
Supervisory Committee Member

Sidney Fels, Professor, Electrical and Computer Engineering, UBC
University Examiner

Ning Nan, Associate Professor, Sauder School of Business, UBC
University Examiner

Abstract

The crypto-asset domain has grown substantially over the past years, both in terms of overall market capitalization, available crypto-assets, and the number of users. While the underlying protocols are well-studied, little attention has been paid to the user behaviors.

This dissertation presents the results of mixed-methods research that investigated the motivations, behaviors, and user experience challenges of both users and non-users of crypto-assets. We found that crypto-asset usage is nuanced and is influenced by factors, such as the asset at hand, the amount invested, and the level of expertise of the respective user. This heterogeneity in behaviors was also confirmed through a cluster analysis. Through this analysis, we identified three distinct types of crypto-asset users, which we labeled as *cypherpunks*, *hodlers*, and rookies. While both *cypherpunks* and *hodlers* had high perceived self-efficacy (i.e., the ability to use crypto-assets and tools), they differed in their risk perceptions, with *hodlers* believing to be more vulnerable to potential risks, such as software wallet vulnerabilities. The rookies started to use crypto-assets recently and, unsurprisingly, had a lower self-efficacy when compared to the other two. They also owned fewer crypto-assets and used custodial wallets more often.

We also identified factors influencing the adoption intention and behavior and found self-efficacy to be a major deterrent. Besides the perceived high complexity of crypto-assets and, in turn, the perceived inability to use them, non-users also cited the high risks and lack of regulatory support as a reason for non-involvement.

Lastly, we investigated user experience complaints about the top five mobile crypto-wallets, i.e., mobile apps that allow users to manage their cryptographic keys for crypto-assets. We discovered that these wallets have severe usability is-

sues. While some of these issues (e.g., crashes and freezes) are commonly encountered in mobile apps in general, others are domain-specific, such as inadequate fee and key import settings. We found that such issues led to dangerous errors and offer design recommendations in order to reduce such risks. Our findings further the understanding of the crypto-asset users and non-users and can improve the user experience by informing the design of more effective and user-friendly key management.

Lay Summary

Cryptocurrencies and tokens (collectively referred to as crypto-assets) are new forms of cryptographically secured digital currencies that are used by millions all over the world. The research presented in this thesis explores the human factors associated with this new form of money and focuses both on users and non-users of crypto-assets. The results suggest that crypto-asset usage is nuanced and depends on various factors, such as the asset at hand or the amount invested. The user population also differs in their behaviors based on their intentions and level of expertise, with expert users being more conscious of their security decisions than rookies. We further found that current tools have severe usability issues that not only affect experienced users but also newcomers, potentially resulting in irreversible monetary losses. Addressing the identified challenges in this work could not only lead to more effective and user-friendly tools, but could also facilitate adoption.

Preface

This research was the product of a fruitful collaboration between the author of the dissertation and the following people: Konstantin Beznosov (supervisor), Masoud Mehrabi Koushki, Borke Obada-Obieh, and Yue Huang from the University of British Columbia, Svetlana Abramova and Rainer Böhme from the University of Innsbruck, and Oliver Wiese and Volker Roth from the Free University of Berlin. The work presented herein consists of research studies that have been published in peer-reviewed international conferences.

The qualitative user study presented in Chapter 3 and partly discussed in Chapter 6, is based on the following publication:

> A. Voskobojnikov, B. Obada-Obieh, Y. Huang, and K. 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.

I was responsible for the design of the interview study and conducted all interviews. Borke Obada-Obieh and Yue Huang participated in the qualitative analysis in order to reduce personal biases. Prior to conducting this study, I obtained ethics approval from the Behavioral Research Ethics Board (BREB) at UBC (H18-01456).

Next, in order to quantify and refine the findings of the qualitative study, an online survey was designed and deployed. The findings, which are presented in Chapter 4 and partly discussed in Chapter 6, are based on the following publications:

S. Abramova,* A. Voskobojnikov,* K. Beznosov, and R. Böhme. Bits Under the Mattress: Understanding Different Risk Perceptions and Security Behaviors of Crypto-Asset Users. In: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, 2021.

A. Voskobojnikov, S. Abramova, K. Beznosov, and R. Böhme. Non-Adoption of Crypto-Assets: Exploring the Role of Trust, Self-Efficacy, and Risk. In: Proceedings of the 29th European Conference on Information Systems (ECIS), 2021

** both authors contributed equally*

In the first project (first paper on the list above), the workload was split with the co-first author. Both Svetlana Abramova and myself designed the survey, ran the pilot study, and were responsible for the data collection. In particular, I ran the recruitment campaigns in North America. Both authors participated in the data analysis, with Svetlana Abramova being largely responsible for the clustering analysis and myself for the regression analyses presented in this thesis. Other co-authors also actively participated in the discussion of the instrument, results, and paper writing process.

In the second project, I developed the statistical model and ran the analysis. Other co-authors participated in the writing process.

The survey study, which was the basis for both publications, was approved by the ethics boards of both the University of Innsbruck and UBC (H18-01456).

Lastly, the empirical study, which is presented in Chapter 5 and partly discussed in Chapter 6, is based on the following publication:

A. Voskobojnikov, O. Wiese, M. Mehrabi-Koushki, V. Roth, and K. 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.

I was responsible for the design of the study and implementation of the underlying machine learning model. Masoud Mehrabi Koushki and Oliver Wiese participated in the qualitative analysis in order to reduce personal biases. All co-authors contributed to the paper writing process.

Table of Contents

List of Tables

List of Figures

Dedication

To Julia, Oleg, Rolf, Luisa, Alexandra, and Luka. To Kate, who has supported me throughout the journey and especially to my grandfather Sergei, who inspired me to start my PhD studies.

Chapter 1

Introduction

Crypto-assets[1] have experienced an explosive growth in the recent past. Over the last five years (2016-2021), thousands of new crypto-assets were created, tens of millions of new users entered the domain [145], and, as a consequence, the overall capitalization of the crypto-asset markets has increased from $7 billion to more than $1.5 trillion USD [44]. The resulting user base has also changed drastically when compared to the early days of bitcoin [115], [2] the very first cryptocurrency, and is no longer solely made up of cypherpunks and computer experts, but also people from various socio-economic backgrounds with varying levels of computer proficiency [73, 99, 180].

Limited attention, however, has been paid to this new population of users, their motivations, behaviors, as well as challenges that arise when using crypto-assets. The lion's share of research has been bitcoin-centric [73, 126, 193, 194] and it is unclear if other crypto-assets (e.g., utility tokens) bring the same or different challenges for its users. Similarly, it is also unknown what factors affect the corresponding usage behaviors.

Similarly, non-users of crypto-assets have been largely ignored by scholars. The first and only study of non-users was conducted by Gao et al. [73] where they interviewed bitcoin non-users. A key finding was that the non-users believed not to

[1] The term "crypto-assets" refers to both cryptocurrencies and tokens, where cryptocurrencies, contrary to tokens, have their own designated blockchain.

[2] Bitcoin refers to the protocol, whereas bitcoin refers to the cryptocurrency.

be able to use bitcoin because of their lack of understanding and knowledge about the underlying protocol. This lack of understanding, however, was also found to be prevalent among the user participants, and evidently, did not prevent them from engaging with bitcoin. The authors therefore hypothesize that there must be other reasons preventing non-users from getting involved with crypto-assets, which, thus far, have not been investigated any further.

In this dissertation, we analyze the experiences of both users and non-users of crypto-assets, including security and privacy behaviors, factors influencing adoption, as well as the user experience (UX) of crypto-asset management tools.

1.1 Problem Statement

The overreaching knowledge gap that this research seeks to fill is the lack of understanding of the challenges both users and non-users of crypto-assets perceive and experience. The work presented in this dissertation focuses on the Western world and their perceptions and is therefore limited in scope. We acknowledge that the findings might not be applicable to users in developing countries as they might use crypto-assets in a different way, e.g., as a hedge against inflation [125]. A future investigation and comparison between countries can therefore be of significant value as it will lead to a more complete understanding.

In the following, we define three smaller problems that this dissertation tries to address.

1.1.1 Lack of Understanding of the Risks Associated with Crypto-Assets

Empirical studies investigating user behaviors in the crypto-asset context have only targeted bitcoin users so far. In 2014, Bohr and Bashir [27] conducted the first exploratory analysis of bitcoin users based on publicly available data that was collected a year prior. Besides providing demographic information, the authors showed that certain variables, such as age and country of residence, have an effect on the perception of bitcoin and accumulation thereof. Other quantitative studies followed in the years after and explored the perception of risks that are associated with bitcoin [4, 126].

Qualitative studies have also explored the human-centered side of bitcoin in the past. Studies have investigated bitcoin users' motivations [117], risk perceptions [73], as well as trust challenges [116, 194], however, no work has looked beyond bitcoin and into the risks that arise for users of other crypto-assets.

Non-users have received far less attention than the counterpart. Gao et al. [73] conducted the first and only study of bitcoin non-users and showed that the perceived lack of understanding of the protocols was considered an entry barrier. There exists no work exploring other challenges, such as security and privacy risks, and we aim to fill this knowledge gap.

In summary, our goal is to explore crypto-assets beyond bitcoin in order to provide a more complete picture with regard to the risks users and non-users experience. Besides risks, we also investigate the motivations of users as well as their usage behaviors and the factors influencing them. For non-users, on the other hand, we investigate their perceptions of risks related to crypto-assets. Chapter 3 presents the corresponding qualitative study of both users and non-users, whereas the quantitative study of the security behaviors of users can be found in Section 4.1 of Chapter 4.

1.1.2 Lack of Understanding of the Adoption Behaviors in the Context of Crypto-Assets

There exists an extensive body of research investigating the adoption behaviors of various technologies. A technology acceptance model (TAM) was first proposed by Davis in 1989 [58] and included two constructs, *perceived usefulness* and *perceived ease of use*, which were both shown to have an effect on the intention to use a technology. Model extensions were also proposed in the years after [212, 214] and included other constructs, such as performance and effort expectancy or hedonic motivation, which all have been shown to have positive effects on the intention to adopt technologies. While these models and iterations thereof have been successfully applied in different contexts, including the fintech sector [86, 121, 131, 176], no work has investigated the factors influencing the adoption behaviors of actual crypto-asset users.

The only work on crypto-assets was conducted by Arias-Oliva et al. [15], who studied the usage intentions for cryptocurrencies by using an extended Unified The-

ory of Acceptance and Use of Technology (UTAUT) model [213]. The authors found that *performance expectancy*, i.e., the degree to which an individual believes that using a technology would enhance their performance [213], and *facilitating conditions*, i.e., the degree to which an individual believes that they have the required organizational and technical infrastructure to use a system [213], to have a significant effect on the intention to use cryptocurrencies. The participants in [15], however, were non-users that only had a general understanding of the internet and it therefore remains unknown what factors influence the adoption intentions of informed non-users and actual users of crypto-assets.

We aim to provide the first insights on the adoption behaviors of users as well as adoption intentions of non-users that have some understanding of crypto-assets. By shedding light on the factors influencing both users and non-users and comparing them between one another, one will be able to understand the key constructs that, potentially, could be leveraged to facilitate adoption. Section 4.2 in Chapter 4 presents the results of the corresponding survey study.

1.1.3 Lack of Understanding of the UX of Crypto-Asset Key Management Tools

Cryptography can be challenging for users and key management in the context of crypto-assets is no exception. Eskandari et al. [66] conducted cognitive walkthroughs with bitcoin wallets and identified UX challenges, such as complex metaphors and abstractions, that could lead to dangerous user errors. User errors were also confirmed in other studies, both for bitcoin [126, 194] and Ether [71], yet it remains unknown what types of UX issues exist in current tools, what effect they have on users, and how, if at all, they contribute to monetary losses.

In order to address this problem, we aim to study the user feedback for current crypto-asset wallets in order to shed light on some of the challenges users experience when managing their keys. By analyzing what specific features are poorly/well-received by the users, one would be able to provide recommendations on how to design more effective and user-friendly crypto-asset wallets.

1.2 Research Summary

As discussed in the previous section, the research presented in this thesis is geared towards a) understanding the risks associated with crypto-assets, b) investigating the factors influencing both the intention to adopt crypto-assets as well as actual adoption behavior, and c) understand the UX challenges that arise when using key management tools. In the following, we describe the corresponding projects that addressed these research questions.

1.2.1 Risks Associated with Crypto-Assets

As a first step towards understanding the existing risks with crypto-assets, we conducted an exploratory interview study with 20 participants. 11 of those were users and 9 informed non-users who had an understanding of crypto-assets, with some even having tried to purchase them. For users, we explored their motivations and use cases they used crypto-assets in as well as security and privacy challenges. For non-users, on the other hand, we explored their perceptions of crypto-assets and entry barriers they believe exist. The main findings are summarized below.

Main Findings of the Interview Study

- Crypto-asset usage appears to depend on factors, such as expertise, use case, crypto-asset at hand, and the amount invested.
- Crypto-assets other than bitcoin bring new risks and challenges for their users, e.g., in the case of decentralized applications where users have to use specific browser-based wallets or crypto-assets that have more than one pair of cryptographic keys.
- Risk, trust, and self-efficacy appeared to have an influence on the intention to adopt crypto-assets.
- We identify UX issues of current crypto-asset management tools and show that they can lead to monetary losses.

Next, we wanted to refine and quantify the findings related to the security practices explored in the qualitative study. Our results from the interview study suggest

that crypto-asset users are heterogeneous in their behaviors and in order to validate that, we conducted a survey with 395 users of crypto-assets and employed hierarchical clustering on five psychometric constructs: *perceived vulnerability*, *perceived severity*, *perceived self-efficacy*, *response cost*, and *perceived concern*. In the following, we summarize the main findings of the study.

Main Findings of the Survey Study

- We identify three clusters that differ in their characteristics and security behaviors: *cypherpunks*, *hodlers*, and *rookies* and show that the crypto-asset user population is indeed heterogeneous in their behaviors as conjectured in our prior work.
- These clusters differ in their risk perceptions, expertise, demographic characteristics, and motivations.
- We show that the amount invested has a statistically significant effect on the choice of storage, with higher holdings having a higher likelihood to be stored in hardware wallets.
- The choice of crypto-asset appears to have an effect on the severity of some perceived risks.
- We show that the crypto-asset held has an effect on the choice of wallet that stores the majority of a user's funds.
- We show that there exists a positive effect between the choice of custodial wallets and one's trust in custodians.

1.2.2 Crypto-Asset Adoption

Guided by our qualitative findings, we wanted to investigate the adoption behaviors next. For non-users, our results suggest that risk, trust, and self-efficacy all have an effect on the intention to adopt crypto-assets. However, besides only investigating the intention to adopt, we were also interested in the actual adoption behaviors of users and the influencing factors. For this reason, we recruited both users and informed non-users.

In total, we used responses from 404 participants, of which 200 were users and 204 informed non-users. We developed structural models for both the adoption intention and behavior and assessed their validity in a structural equation model analysis. The main findings are summarized in the following:

Main Findings

- We show that trust is a critical factor that affects the intention to adopt crypto-assets among non-users.
- We investigate the differences in construct means between users and non-users and show that non-users score significantly lower on the trust and self-efficacy constructs.
- We show that self-efficacy has a significant effect on the adoption behavior, suggesting that those participants that believe to have the necessary knowledge to use crypto-assets, tend to do so.
- We uncover the self-reported reasons of non-users that led to a decision against crypto-assets, amongst which, perceived software vulnerabilities of both crypto-assets and wallets as well as the possibility of falling victim to crime were mentioned the most.

1.2.3 Evaluating the UX of Mobile Wallets

Prior work has shown that UX challenges exist for both passwords [5] and cryptographic key management tools, such as PGP [223]. Similar findings have been reported for bitcoin wallets [66] and such UX issues were found to lead to user errors and losses of bitcoin [194]. In our qualitative study, we confirmed the prevalence of such issues and further showed that crypto-assets other than bitcoin and the corresponding tools bring novel challenges for its users.

Guided by these findings, we conducted a mixed-methods study of the UX issues of mobile wallets. We collected more than 45,000 mobile app reviews and then, through a combination of natural language processing (NLP) and machine learning (ML), were able to filter UX-relevant reviews. We then conducted a Thematic Analysis [30] of a random sample comprising 2,522 reviews and identified

five major types of issues, *domain-specific*, *general*, *security and privacy*, *trust*, and issues related to *misconceptions*. The major findings are summarized below:

Main Findings

- We provide a categorization of UX issues of crypto-asset mobile wallets and show that both domain-specific and general issues can result in dangerous errors and irreversible losses of crypto-assets.
- We show that some users have conventional payment systems in mind when using crypto-assets and are surprised when some of the known features, such as reversible transactions, do not exist for crypto-assets.
- We show that the user base has little trust in wallet developers and put the blame on them, even in cases where they can hardly do anything, such as with pending transactions or high transaction fees.

1.3 Contributions

In this section, we provide an overview of the most important contributions and discuss their potential impact on future work on crypto-assets.

1.3.1 Identification of Security Personas

Prior to our work, there has been very little understanding of the types of crypto-asset users that exist in the domain. Through a cluster analysis, which was partially informed by the results of the qualitative study, we were able to identify three distinct clusters that differed in their characteristics as well as security behaviors. Users had varying motivations for which they got involved in the domain and depending on their expertise, also differed in their needs, with rookies struggling with the onboarding processes and cypherpunks and hodlers putting an emphasis on security guarantees. We have also shown that the amount invested and the crypto-asset held are both significant predictors of the wallet choice. More details can be found in Chapter 3 and Section 4.2 in Chapter 4.

We also showed that crypto-assets other than bitcoin bring new challenges for the corresponding users, such as new tools and cryptographic principles. This ob-

servation shows that a focus on bitcoin, as it was the case in many of the prior studies, only provides a partial view of the challenges users nowadays experience.

The following are the key takeaways for future work:

- The crypto-asset user population is heterogeneous. Users differ in their level of expertise, motivations, as well as needs and future tools need to account for this heterogeneity.
- Future studies should focus on an even more diverse set of crypto-assets in order to further the understanding of the behaviors. This is particularly important in a domain such as the one of crypto-assets that evolves rapidly.

1.3.2 Factors Influencing the Adoption of Crypto-Assets

To the best of our knowledge, we conducted the first study of the adoption behaviors of users and non-users of crypto-assets. We showed the statistically significant effect of trust on the intention to adopt crypto-assets and further identified a mediating effect of self-efficacy. We also investigated the actual adoption behaviors of users and identified a statistically significant effect of self-efficacy. Lastly, we reported on the self-reported reasons against adoption and identified security risks as the major reason for which non-users have decided against crypto-assets. More details can be found in Section 4.2 of Chapter 4.

The following are the key takeaways for future work:

- Perceived self-efficacy was found to have effects in both structural models and future work can leverage this construct in order to facilitate adoption of crypto-assets.
- Our results also show the positive effect of trust on the intention to adopt crypto-assets. Guided by these findings, future work could also investigate effective regulatory policies in order to provide better support.

1.3.3 Identification of UX Issues of Crypto-Asset Management Tools

UX issues of crypto-asset tools have been reported by scholars in the past [73, 126, 194]. Yet, before our study, it was unknown how these issues can be grouped and

what effect they have on the users.

We identified five groups of issues during our review analysis. Besides domain-specific issues, such as inadequate transaction fees and outdated balances, general issues, such as crashes and freezes, also appeared to be very common. Both types of issues led to the inability to access the funds and caused great distress for the corresponding users. We also identified security and privacy issues, trust concerns, as well as misconceptions on the users' end. The latter, for example, were related to misunderstood principles of blockchains, such as irreversible transactions or variable transaction fees. More details can be found in Chapter 5.

The following are the key takeaways for future work:

- Mobile crypto-asset wallets do not only have domain-specific UX issues, but also general ones, with both potentially resulting in severe consequences for its users. A satisfying UX can therefore only be achieved if both types of issues are addressed.
- Some users have inadequate mental models when using wallets and have conventional payment systems in mind. Future wallet research should therefore focus on how to effectively communicate the key differences between crypto-assets and traditional systems.

1.4 Organization of the Thesis

Figure 1.1 provides an overview of the studies presented in this thesis. First, in Chapter 2, we provide the background and define the terms that are used throughout the thesis. Chapter 3 presents the results of the qualitative study on the perceived security and privacy risks. Next, informed by the qualitative findings, both quantitative studies are discussed in Chapter 4. Chapter 5 summarizes the results of the mixed-methods study investigating the UX of crypto-asset mobile wallets and Chapter 6 discusses the contributions and overarching takeaways from the research presented in this thesis.

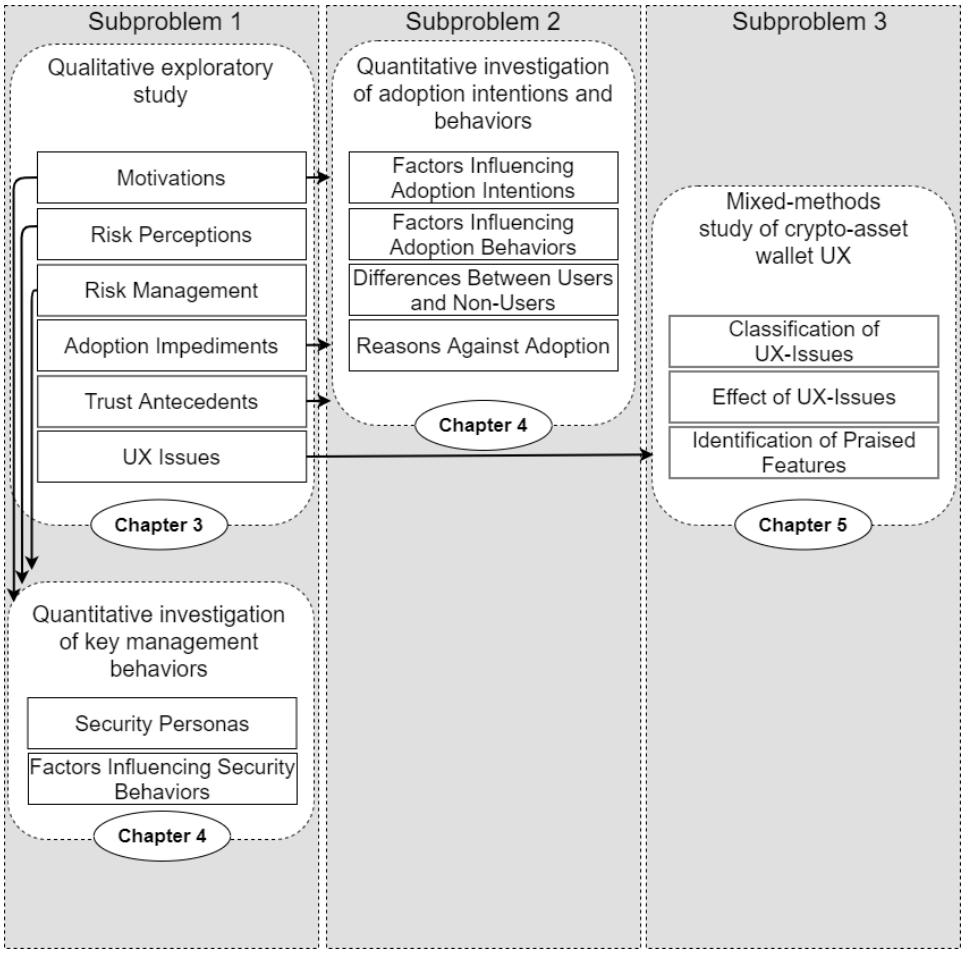


Figure 1.1: Overview of the studies and the relationships between them

Chapter 2

Background

2.1 Crypto-Assets

Throughout this thesis, we use the term crypto-assets to refer to both cryptocurrencies and tokens. According to Casey et al. [32], cryptocurrencies are generated by their own blockchains whereas tokens are not. In the following sections, we make distinctions where applicable and otherwise use the term *crypto-assets* when referring to both of them.

Over the past years, many cryptocurrencies other than bitcoin were created, some of which allow people to create their own tokens on top of the respective network. The Ethereum blockchain [225] is the most popular platform that allows the creation of tokens and contributed significantly to the now over 6,000 different crypto-assets [45]. These tokens are bound to that specific network, and whenever tokens are sent from one address to another, the transaction fees are paid in the cryptocurrency whose network the tokens exist on. These fees are paid to the miners, i.e., to the entities that process transactions and include them in the respective blockchain [13]. Here, transactions with higher fees are prioritized and are included more quickly than ones with lower fees.

Despite the large number of different cryptocurrencies, they all make use of public key cryptography. Addresses consist of cryptographic hashes of the public key (unless they are smart contract addresses), and private keys are needed to be able to transfer funds, as they are used to sign transactions [13].

Wallets, however, can also be accessed by using mnemonics, which consist of 12 to 24 words in the case of the BIP-39 standard [1] and are used to deterministically generate key pairs for a particular wallet. These words are also commonly used to recover wallets, e.g., when the encryption password is lost or forgotten. Overall, mnemonics are considered to be superior to conventional private keys and are supported by many wallet providers [25].

2.2 Coin Management Tools

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 (CMT) [126], 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 [56]. 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.

Further, there exist two types of wallets: *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 [159].

Non-custodial crypto 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.

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.

2.3 Grounded Theory

Grounded Theory is a research methodology that is often used in social sciences to construct a theory from data. It was first proposed by Glaser and Strauss [75] and is considered as a non-intrusive method that focuses on the construction of a theory rather than the description or confirmation of a pre-existing one. In the classic Grounded Theory, the researcher's role is passive and limited as an observer, whose goal is the generation of a theory through constant comparative methods [75]. The classic Grounded Theory follows a positivist perspective and therefore implies that there only exists one truth about the studied phenomenon.

This philosophical perspective, however, is not shared by all variations of Grounded Theory. Corbin and Strauss [51] question a researcher's ability to find the one underlying truth and accept potential subjective biases. In order to minimize these inevitable personal influences, the authors provide a clear outline on how to apply Grounded Theory in order to maximize objectivity on the researcher's end. The researcher plays a critical role and has to follow multiple steps, including open, axial, selective coding, and theoretic sampling. Throughout these stages, the researcher is guided by their experiences and beliefs, hence, why it is suggested that the Grounded Theory as it is outlined by Corbin and Strauss follows a interpretivist perspective [136].

Lastly, there also exist a constructivist perspective, which was first described by Charmaz [37]. Contrary to the other two approaches, the constructivist Grounded Theory fully integrates the researcher in the theory generation process and states that theory is constructed rather than discovered.

In this dissertation, we follow the Grounded Theory approach as outlined by Corbin and Strauss [51], as we found the outlined steps the most helpful. Fur-

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

ther, we believe that the role of the researcher is more realistic than in the classic Grounded Theory [75] as well as the constructivist Grounded Theory [37], where the constructed theory in the latter cannot stand without the researcher's view [195].

2.4 Thematic Analysis

In this dissertation, we also employed Thematic Analysis, which is described as method that allows to identify, analyze, and report patterns (themes) within data [211]. It was first proposed by Braun and Clarke [30] and consists out of six steps: familiarization with data, generating initial codes, searching for themes, reviewing themes, defining themes, and producing the final report.

Contrary to Grounded Theory, where philosophical underpinnings play a vital role, Braun and Clarke state that in Thematic Analysis researchers do not have to commit to theoretical intricacies if they do not wish to do so [30]. Further, Grounded Theory also follows an iterative process throughout the data collection, whereas in Thematic Analysis, the data analysis only begins when data has already been collected. The latter was the main reason for which we decided to use Thematic Analysis as the method to qualitatively analyze the UX issues of mobile wallets (see Chapter 5).

Chapter 3

Exploring the Risks Associated With Crypto-Assets

This chapter presents the results of an exploratory interview study investigating the behaviors of users and non-users of crypto-assets. In particular, an emphasis is put on the risk and trust perceptions as they emerged as the two dominant constructs during the investigation. First, in Section 3.1, we give an overview of the background and related work. Next, the methodological approach is described in Section 3.2, followed by the qualitative results, including both risk (Section 3.3.5) and trust (Section 3.3.6). The chapter concludes with a discussion of the results and an outline of future avenues for research.

3.1 Background and Related Work

3.1.1 Risks in the Crypto-Asset Domain

When users interact with blockchain-based technologies, they are directly or indirectly exposed to a significant number of risks. Here, we use the definition of risk as outlined by NIST [186]: *"a measure of the extent to which an entity is threatened by a potential circumstance or event."* Naturally, there exist a wide range of such circumstances, some of which were outlined by Bonneau et al. [28]. The authors survey the underlying security concerns in Bitcoin and possible attack vectors that

might compromise the distributed ledger. Most of these attack vectors, however, only indirectly affect the the users of crypto-assets.

To understand users' perception, one has to determine what risks affect them. Bitcoin's pseudonymity, for example, is considered one of its key features, but as research has shown, this pseudonymity can be used to track and identify users [10, 156].

Third-party sites can also pose a risk to users. Goldfeder et al. [76] showed that payment gateways may leak personally identifiable information, including the names, emails, and addresses of crypto-asset users.

Risks associated with the usage of Bitcoin are well documented, other crypto-assets, however, have not yet been investigated. For Bitcoin, both Böhme et al. [26] and Grant et al. [79] provide comprehensive overviews of risks, and Kiran et al. [122] further propose a grouping of these into *social risks*, *legal risks*, *economic risks*, *technological risks*, and *security risks*.

Besides identifying potential risks, qualitative investigations have been conducted providing insights into user experiences and perceptions. While users were asked to assess the severity of risk scenarios in [126], Abramova et al. [4] investigated factors influencing risk perception among bitcoin users. Results suggest that users are concerned with potential monetary losses, regulatory restrictions imposed by governments, and a general lack of adoption. However, it has yet to be determined what controls they personally apply for mitigation and what types of risks and challenges crypto-assets other than bitcoin bring for its users.

The population of non-users has been largely ignored by scholars. To the best of our knowledge, Gao et al. [73] conducted the only interview study on non-users of bitcoin. The focus of their work, however, was on the understanding of the underlying protocol, and not the potential risks associated with bitcoin. Our work fills this knowledge gap and further includes crypto-assets beyond bitcoin in order to provide a more complete picture.

3.1.2 Trust

Dishonest Actors in the Crypto-Asset Domain

The rapid market growth over the last years has attracted various actors, including some that operate in bad faith. BitConnect, a crypto-asset created in 2016, ended up being a $2.6 billion USD scam resulting in monetary losses for owners [157]. A more recent example of a fraudulent crypto-asset just ceased operation in 2019, resulting in estimated losses worth over $4 billion USD [174]. These are the two most prominent examples, but there have existed hundreds of documented scam coins over the years [46].

Besides crypto-assets created in bad faith, users can also fall victim to fraudulent exchanges. Mt. Gox, a bitcoin exchange operating between 2010 and 2014, reported to have lost bitcoin worth $450 million USD at the time [42]. Exchange shutdowns and hacks continue to happen, with one example being the missing crypto-assets worth $190 million USD on a Canadian exchange in 2019 [43]. The risk of falling victim to such exchanges is ever-present, with some breaches happening in late 2019 and even 2020 [2]. Similar to fraudulent crypto-assets, it is therefore of interest to understand what factors people consider when trusting an exchange.

Trust in Online Systems

There is no single notion of trust and definitions depend on the context and field of study. Beldad et al. [20] suggest that there exist two conceptualizations of trust with one being an expectation towards an interaction partner, and the other being seen as willingness to be vulnerable. The latter definition was proposed by Corritore et al. [52] for online systems and was later applied in the context of Bitcoin [193]. For this reason, we also use this definition in the general context of crypto-assets.

One major difference between online and offline trust is in regards to interaction partners. In the case of online systems, the object of trust can be a website or technology, whereas people or groups are considered trustors/trustees in traditional offline interactions [52]. Online transactions can therefore appear to be faceless or intangible [20], which also holds true for actors in the crypto-asset domain, e.g., in

the case of newly founded start-ups or exchanges.

For both offline and online systems, however, the trustor forms expectations based on the emitted signals of trustworthiness by the trustee. Riegelsberger et al. [183] developed a trust framework that distinguishes between *contextual properties* and *intrinsic properties* of the trustee. For first-time interactions, the contextual properties play an important role and include *temporal, social, and institutional embeddedness.* Temporal embeddedness refers to a transaction history between interaction partners and the trustee's willingness to operate in the market in the forseeable future. Social embeddedness relates to the reputation of the interaction partners that is at stake during every transaction and institutional embeddedness includes sanctions that parties could face in the case of dishonest actions.

Contrary to traditional online systems, such as e-commerce, where safety nets exist, there are none for crypto-assets due to the irreversible nature of transactions. In particular, this means that if a user assesses the trustworthiness of an interaction partner inadequately, monetary losses may occur. Therefore, the emitted trust cues and their interpretation become of utmost importance and yet, these cues have not been investigated in literature.

Trust in Crypto-Assets

Work on trust in the crypto-asset context has been very Bitcoin-centric. Studies investigating the implications of Bitcoin's characteristics, such as decentralization or anonymity, on trust can be found both in computer security [12, 73, 167, 191, 194] and finance literature [31, 165]. Sas and Khairuddin [193] created a Bitcoin trust framework spanning three dimensions, namely *technological*, *social*, and *institutional*, and were the first to shed light on the trust implications of Bitcoin's technological features [194].

Trust, however, is multi-faceted and goes beyond technology, which is evident in the proposed trust framework for Bitcoin [193] spanning three dimensions. Yet, *social* and *institutional* cues have been left unexplored thus far. By expanding the area of focus beyond Bitcoin's characteristics, we include antecedents in previously unexplored dimensions of trust and further identify novel technological cues that appear to foster trust formation in the crypto-asset domain.

Non-users of crypto-assets and their perceptions of trust have been ignored in literature. For traditional online systems, the initial formation of trust appears to be a key factor when it comes to adopting new technologies [137]. Similarly, Gao et al. [73] hypothesize that for non-users of bitcoin lack of trust might be one of the reasons leading to non-involvement. Guided by the proposed avenue of research in [73], this work sheds light on trust as perceived by non-users and provides first empirical evidence for the lack thereof when it comes to crypto-assets.

3.2 Methodology

3.2.1 Recruitment and Participants

We recruited participants aged 19 and older from the Vancouver metropolitan area. Users of crypto-assets were recruited through professional blockchain LinkedIn groups, a graduate reading seminar, a mailing list, and the community Slack channel of a blockchain club at UBC, as well as a meetup group focused on crypto-assets. The recruitment notice can be found in Appendix A.1. Non-users were recruited with the help of community managers of a local crypto-asset exchange platform and through personal contacts. There was no formal screening process; instead, we were in direct contact with all potential participants. This was especially necessary for non-users, whom we wanted to ensure had some prior familiarity with crypto-assets. We stopped recruiting once it became clear that we had reached code saturation and the last three interviews did not yield new codes.

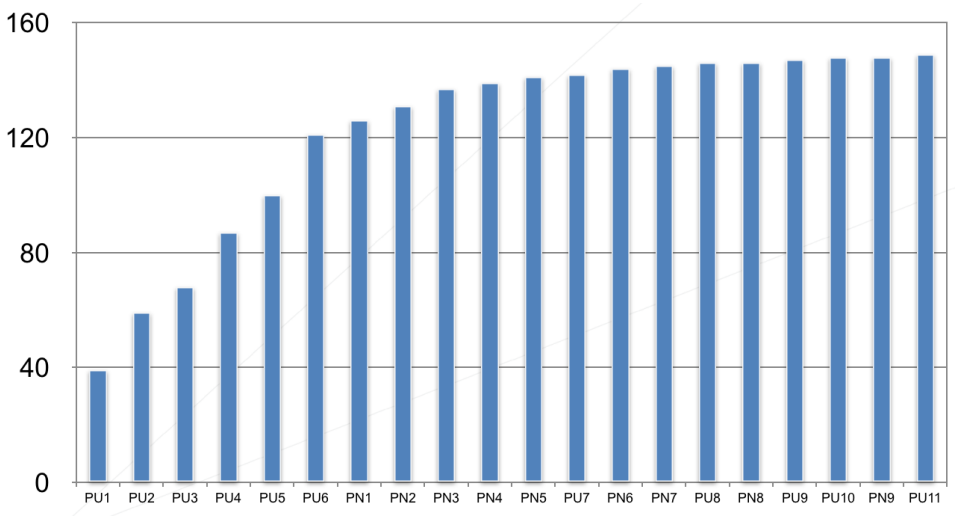


Figure 3.1: Number of codes after interviewing each participant

For the sake of clarity, we define users and non-users as follows:

- *User (PU):* A participant who owned crypto-assets at the time of the interview.
- *Non-user (PN):* A participant who did not own crypto-assets at the time of the interview, but had an understanding of crypto-assets or considered an involvement.

It is important to note that we did not differentiate between the levels of expertise of the users.

We conducted semi-structured interviews both in person and via telephone. The researchers followed an interview guide (Appendix A.2), ensuring consistency across participants. The following broad research questions were investigated.

- **RQ1:** What are the current usages of crypto-assets?
- **RQ2:** How do owners manage their crypto-assets?
- **RQ3:** What is the perception of crypto-asset-related risks?
- **RQ4:** How do owners manage the risks?

- **RQ5:** What factors influence users' security behavior?

Naturally, non-users could not answer some of these questions. We therefore focused on their perception of risks and how that influenced their decisions about crypto-assets. For both users and non-users, we validated the questions by conducting two pilot interviews and altered the questions, if needed. All interviews were recorded, transcribed, and anonymized. Each participant was compensated $15. The study got approved by UBC's Behavioural Research Ethics Board (H18-01456).

3.2.2 Data Analysis

An iterative coding approach based on Grounded Theory was applied [51]. Three researchers independently performed open coding of the interview transcripts, and the results were discussed and added to a shared codebook once the researchers converged on codes.

An axial coding followed, where concepts and relationships between the codes emerged. The resulting groups and themes were discussed among the same three researchers. During the selective coding process, the raw data was analyzed again to further enrich the results of the previous coding stages.

Lastly, a theory explaining the risk management for both users and non-users was formed, which is covered in detail in Section 3.3.5. During the analysis, however, trust was also identified as a prominent factor that appeared to have a direct influence on risk. In order to better understand the intricacies of that construct, we applied the Bitcoin trust framework by Sas and Khairuddin [193] to group our identified trust determinants. While the majority of identified trust cues during the coding process were covered by the *technological*, *social*, and *institutional* trust dimensions, others were not, which we refer to as *subjective antecedents*. We report on these findings in Section 3.3.6.

Throughout the study, we followed a reflexive approach and re-coded the interviews several times [51]. We do not report on inter-coder reliability, as codes are only an interim product in Grounded Theory and change throughout the data analysis [51]. Instead, in our study, agreements and disagreements were discussed among the researchers to ensure reliability.

3.2.3 Limitations

As with all qualitative investigations, the results of this study are not necessarily generalizable to the whole population of crypto-asset users and non-users. Our aim, however, was to interview a diverse sample. We ensured its diversity by recruiting through multiple channels and including participants from different backgrounds, including investors, miners, consultants, and blockchain developers. Since we investigated users' security and privacy behaviors, it is also possible that some participants decided against disclosing sensitive information such as monetary losses. Some potential participants might have chosen not to participate in our study because of privacy concerns.

All participants were also based in North America. While this geographical restriction might have impacted our results, we strove to recruit a diverse sample.

3.3 Results

3.3.1 Participants

We interviewed 20 participants, 11 of whom were users (age: max. = 43, mean = 28.8, median = 28, min. = 19) and 9 non-users (age: max. 57, mean = 32.4, median = 30, min. = 19). Seven of the 11 users had a technical background and 5 were active members of blockchain-related meetup groups. Detailed demographics can be found in Tables 3.1 and 3.2.

Table 3.1: User demographics

Participant	Age	Gender	Degree Achieved	Occupation	User Since	Number of Owned Crypto-Assets
PU1	21	M	Bachelor's	Looking for work	2016	2
PU2	28	F	Master's	News editor (blockchain domain)	2017	4
PU3	23	F	Bachelor's	Student	2016	1
PU4	22	M	Bachelor's	Entrepreneur (blockchain domain)	2016	12
PU5	40	-	College	Systems analyst (web technologies)	2013	3
PU6	30	M	No degree	Small business owner	2012	4
PU7	19	M	High school	Blockchain advisor	2014	50
PU8	21	M	High school	Student	2014	12
PU9	31	M	Bachelor's	Sales	2013	6
PU10	43	M	Master's	Software developer (energy)	2013	4
PU11	39	M	JD	Blockchain advisor (law)	2015	5

Table 3.2: Non-user demographics

Participant	Age	Gender	Degree Achieved	Occupation
PN1	23	F	Bachelor's	Student
PN2	53	F	No high school diploma	Asst. manager (money exchange)
PN3	57	M	College	Driver
PN4	30	F	ND	Naturopathic doctor
PN5	30	M	PhD	Research assistant
PN6	30	F	PhD	Financial advisor
PN7	25	M	Bachelor's	Teaching assistant
PN8	25	M	Bachelor's	Student
PN9	19	M	High school	Student

3.3.2 Motivation for Using Crypto-Assets

Addresses RQ1

A prevalent underlying theme in users' involvement with crypto-assets is investment. While potential monetary gains are regarded as one of the main reasons for involvement [73, 126], participants in our study broke this down into short-term and long-term investments. PU6[1] (a small business owner) considered crypto-assets, and bitcoins in particular, as a personal retirement plan: *"For me, I think [...] that's my retirement plan [...]. I don't see it necessarily as a store of value."* PU2, PU3, PU4, PU5, PU6, and PU9 referred to the investment strategy as "holding" crypto-assets, with PU9 (a salesman) explaining: *"I feel like I'm holding a lot of bags still [...] I own bitcoins, I own Ethereum, EOS, MakerDao [...] and Power Ledger."*

Participants also indicated having used crypto-assets to purchase goods. Some of these goods were physical and others digital. PU1 (unemployed) bought a ticket for a cryptocurrency convention, and PU6 mentioned a partial asset value transfer: *"I like to buy precious metals, so I get bullion with my bitcoins."* None of the participants indicated they had purchased illicit goods.

Everyday items were also purchased, as explained by PU10 (a software developer) : *"I have a friend who has a yoga studio who accepts [crypto-assets] as payment and another friend who has a restaurant that used to accept [crypto-assets as] payment."* Digital goods bought with crypto-assets also included video games. PU7 (a blockchain advisor) explained: *"So [I purchased video games from] Steam for example [...] not drugs."*

Unlike speculators, who deal mostly with exchanges, participants who use crypto-assets as a medium of exchange interact with various parties, such as merchants. Therefore, the risks also differ.

Some respondents used crypto-assets as alternatives to banks. PU1, PU4, and PU6 all reported instances where banks fell short in their eyes, with PU6 (a small business owner) saying: *"the one thing that intrigues me about cryptocurrencies is that you're your own bank."*

[1] We use the prefix "PU" when referring to those participants who used crypto-assets at the time of the interview.

A desire to learn more about crypto-assets was another motivation for some users. PU1, PU2, and PU7 cited curiosity as one of the main reasons for looking into the domain, with PU1 stating: *"Curiosity and learning. I'm in a time in my life where learning is very important. So I just want to learn more."*

Lastly, user participants reported owning utility tokens. The application areas of these tokens were wide ranging and included browsers, social media, betting platforms, and games. PU1, PU4, PU7, and PU8 all mentioned having used various platforms, with PU1 recalling placing a bet with Augur: *"I would scroll through a bunch of different markets, like sports, politics, and I clicked on things that were interesting and I said, 'Okay, Golden State is winning this year.'"*

For all the above-mentioned application areas of crypto-assets, the interaction partners appeared to differ depending on the area. PU1, PU7, and PU10 purchased goods and interacted with merchants that accepted crypto-assets, whereas others only interacted with exchanges (PU6 and PU8). Therefore, it is possible that the users would have been exposed to different risks, based on which crypto-assets they owned and how they used them.

3.3.3 Reasons for Not Using Crypto-Assets

Addresses RQ1

During interviews with non-users, several reasons for their non-involvement emerged. Negative views about crypto-assets were prevalent among non-users. PN1,[2] PN2, PN3, PN5, PN6, and PN8 associated crypto-assets with the drug trade and other illegal activities, with PN3 (a driver) saying: *"Somebody told me about the dark net [...] you know, selling drugs and guns and all kinds of illegal [stuff]."*

Non-users believed that some crypto-assets, bitcoin in particular, had reached their peak values and that this was a reason for not purchasing any. PN1, PN3, PN5, PN6, and PN8 expressed their concerns about investment in crypto-assets not making sense from a financial standpoint, with PN5 (a research assistant) stating the belief that the *"Bitcoin price was about $20,000 and there was not much room for an increase."*

[2]We use the prefix "PN" to refer to those participants who did not use crypto-assets at the time of the interview.

The ability of the government to trace all crypto-asset transactions was another stumbling block. PN3 stated they would consider getting crypto-assets *"if you actually had privacy and the government couldn't track it [back to me]."* This belief was not shared by all non-users, though, as PN8 (a student) trusted Bitcoin's anonymity: *"I feel like [Bitcoin] would be extremely private. I don't think it has been hacked at this point, like, there's no way to trace a payment."* Interestingly, although expressing opposing views, both of these statements hint at PN3's and PN8's inadequate mental models about crypto-assets.

On the other hand, the lack of government involvement in the domain was a deterrent for some non-users. PN2, PN4, PN5, PN6, and PN9 stated that regulations could potentially lead to more transparency, which could result in wider adoption. Such regulations could also reduce undesirable volatility, as PN4 (a naturopathic doctor) explained: *"Well, if it's not regulated, I just feel like it could be just so volatile."*

When trying to enter the domain, non-users had experienced barriers to entry. PN1 (a student) expressed displeasure with the verification processes of exchanges, saying, *"I think it takes a few weeks to get verified for the ID. And then, when you make a purchase, you have to do another type of verification."* This non-user had also considered getting crypto-assets through mining but faced challenges: *"I tried [mining] but I realized that all [...] the computers [are] specifically made for mining bitcoins. So maybe my personal computer is really good [but for mining] it doesn't really work."*

3.3.4 Handling of Crypto-Assets

Addresses RQ2

The following sections highlight how participants were storing their crypto-assets, what CMTs they were using, and why they were doing so. We also discuss the usability concerns about existing tools that many of the users brought up.

Storage

Hosted wallets were one of the most popular CMTs among our participants. All 11 users had used a crypto-asset exchange at some point. Coinbase, Binance, Bittrex, and QuadrigaCX were some of the exchanges they mentioned.

While all of the users interacted with an exchange, the nature of their interactions varied. PU1 only purchased Ethereum on Coinbase, just to transfer it over to his personal software wallet, whereas others kept most of their crypto-assets on exchanges. PU7, for example, said: *"I actually put a lot of funds on exchanges, as I think [keeping them in your own wallet is] the equivalent of keeping cash under your mattress [...]."*

Their method for storing crypto-assets appeared to be linked to the amount owned. PU1, PU2, PU10, and PU3 were all willing to consider different storing options, with PU2 (a news editor at a blockchain company) summing it up thus: *"If I store more, I'll think about storing it in a safer place."*

Software wallets were also a popular type of CMT. All of our user participants had used software wallets, such as Exodus, Parity, MetaMask, or Jaxx. PU4, PU6, PU7, and PU11 reported having used paper wallets, whereas hardware wallets were the least reported, used only by PU4, PU6, and PU11.

Options for storing crypto-assets also appeared to depend on the way they were used. PU4, PU5, and PU6 all reported storing bitcoins more securely than other crypto-assets. PU4 and PU6 stored bitcoins in hardware wallets, with PU4 (an entrepreneur) breaking down investments into two categories: *"Long-term holdings like bitcoins—I store offline. Small investments—I'm not necessarily super concerned about. A lot of them are utility tokens, and I'm not necessarily interested in a return."* Although using a software wallet, PU5 (a systems analyst) had additional tactics for increasing its security: *"I have a software wallet and then I hide my files on something else and then I encrypt."* Further, PU5 and PU6 reported having certain crypto-assets solely to trade them on exchanges to gather more bitcoins. For this purpose, PU5 used Litecoin, which has faster confirmation times ($\sim$ 2 minutes) than Bitcoin (10 minutes). PU6 reported storing so-called "shitcoins"[3] on exchanges, stating: *"Only my bitcoins [are stored in a hardware wallet]; shit-*

[3] A pejorative term for crypto-assets that have no intrinsic value.

coins all stay on the exchanges till they make me bitcoins and then [bitcoins] get sent back [to my hardware wallet].”

User Experience Issues with Existing CMTs

Several users reported usability concerns about existing CMTs. PU1, PU5, PU7, PU9, and PU11 all mentioned usability issues with current software. PU11 (a blockchain advisor) explained specific troubles with MetaMask: *“You have to enter a gas amount in some other currency that you have never heard called Gwei and then a lot of the times the recommended amount isn’t enough.”* PU7 described a long learning curve: *“I consider myself [...] decently tech-savvy, [but] it took me a while to kind of get used to it. [...] It’s not difficult but it’s not intuitive.”* PU1, talking about Augur, mentioned: *“I would scroll through a bunch of different markets [...] but I wasn’t able to post [the] transaction.”* PN1, although interested in purchasing crypto-assets, had not been able to do so: *“I had a really hard time learning [Ethereum]. [...] I spent a few days [...] and I just gave up, cause it is kind of too hard.”*

Several users had encountered too much friction in the onboarding phase at exchanges. PU1, PU2, PU4, PU5, PU7, and PU8 expressed dissatisfaction with the verification processes, with PU2 saying: *“Just too bothersome to get the KYC. At the beginning of the year, I KYCed Bitstamp; it took me 2 months to get approved.”*

When it came to ownership and the underlying technology, participants appeared to have misunderstandings. PU1 claimed to own the private key on Coinbase, which is not possible. PU2 stated that she did not understand the cryptographic principles: *“I haven’t figured out how they have the private key on the phone wallet [...] I still don’t understand the private and public key.”* This is in line with the findings [223, 224] and it is worthwhile to explore alternative metaphors that could improve the understanding [94].

3.3.5 Risks

Besides commonly known risks, such as volatility or lack of regulatory involvement, our participants also discussed risks that, to the best of our knowledge, have not yet been reported in the academic literature.

Perception of Risks

Addresses RQ3

High volatility was a concern for both users and non-users. Crypto-assets are strongly associated with opportunities for monetary gains. It is therefore not surprising that many of our participants (PU1, PU2, PN1, PN3, PN4, PN5, and PN6) considered volatility a risk, with PN4 saying: *"You could be paying into something, [it] either ends up worthless [...] It just seems so volatile. It could become worthless [...] It could be fake money."*

Directly associated with the volatile nature of most crypto-assets is the possibility of bubble formation.[4] PU4, PU6, and PU7 expressed their concerns, with PU4 saying: *"It's always way too much excitement [...] People get emotional, people change their strategy [to having] zero strategy at all."*

One of the reasons for bubble formation is the existence of crypto-assets with potentially no intrinsic value. PU1, PU3, PU4, PU5, PU6, and PU8 mentioned scam coins, and PU6 called them "shitcoins." This user went into detail, explaining how developers of these "shitcoins" sell them on the exchanges once they are released: *"they just get a certain amount of the coins right off the bat [...] I mean, it's just monopoly money, he's just collecting all this Bitcoin for all his shitcoin that he has built a website for over the weekend."*

Closely related to scam coins are pyramid schemes, some of which affect thousands of users. PU4 provided examples of pyramid schemes, stating: *"Pyramid schemes [are a risk]. Paying for parts of mining pools, referring family and friends."* One prominent example was BitConnect, which had a multilevel marketing structure. Investors were promised 1% interest compounded daily; after its shutdown in January 2018, investors holding the cryptocurrency ended up losing their entire investment.[5]

Scam ICOs were another risk cited by participants. ICOs are similar to initial public offerings, except that investors purchase coins of the new crypto-asset. PN5 mentioned that ICOs in particular can end up being scams and might lead to mon-

[4]Bubble formation describes unwarranted prices for a certain asset; the assigned market value exceeds the asset's intrinsic value.

[5]https://thenextweb.com/hardfork/2018/01/17/bitconnect-bitcoin-scam-cryptocurrency/

etary losses, saying: *"a lot of ICOs are just scams [...] they just get all the money and close the company."*

In discussions about securing assets, some participants brought up the possibility of losing the seed phrase. PN1 believed that a wallet is not accessible without a seed phrase. This is not the case, as the seed phrase is usually used to restore access to a wallet in case the password used for access is forgotten.

Some participants perceived the potential vulnerabilities of software wallets to be risks. PU4 recalled a multisignature vulnerability of the JAXX wallet. This vulnerability, however, could not have occurred, since multisignature wallets are not supported by JAXX. The wallet in question was actually Parity.

Phishing attacks in the form of incorrect URLs were reported by some participants. Here, PU4 hypothesized that phished users could access a malicious website and lose their assets: *"you can send, like, a fake phish email to your own mailing list [and wait] while they respond to it."*

Used hardware wallets were also considered risky. PU4 said they would not purchase used hardware wallets from third-party websites, as the seller might have altered the private key: *"they changed the private key and the person didn't keep the secret and once [the crypto-asset] appreciated a year later, the person could just take it back."* Such losses have been reported in the community,[6] and it is generally not advisable to purchase second-hand hardware wallets.

Providing credit card details and personal information to third parties was also brought up. When looking into crypto-assets, PN1 became concerned about providing personal information to third-party websites: *"I have to give my credit card information, personal information to other websites in order for me to buy it."*

As mentioned in earlier sections, negative beliefs were prevalent, including that involvement with crypto-assets could pose a social risk. PN6 (a financial advisor) mentioned that users of crypto-assets might be judged unfavorably: *"Cryptocurrency was initially used on the black markets, right, and if you tell people that you have some bitcoins or other cryptocurrencies, people will think that maybe you are buying something illegal."* PU6 also recalled a similar scenario before owning crypto-assets: *"A friend told me about it in 2012. He was a drug dealer and [...] I*

[6] https://cointelegraph.com/news/life-savings-stolen-from-second-hand-ledger-hardware-wallet

originally told him to stay away from [crypto-assets] because it is associated with all this, like, assassination [...].”

Personal safety associated with crypto-asset ownership was also considered a risk. PU6 stated: *“somebody could literally take a gun and put it against your head and say ‘give me your private key.’ It’s not like [they] can take you to the bank and say ‘give me all your money’.”*

The risk of inheritors not being able to access crypto-assets after the purchaser’s death was also brought up. PU11 explained: *“I think one risk that a lot of people don’t think about is what happens when you die—so making sure that there’s a way for whoever is going to be inheriting your cryptocurrency to actually access it.”*

While some users spoke favorably about crypto-asset adoption, others had concerns about what effects it might bring. PU11 explained how decentralization could be jeopardized by corporations: *“we’re starting to see that with Facebook talking about doing a stable coin, or Microsoft and Google and Amazon all kind of launching blockchain as a service type product, so potentially the benefits of decentralized systems could be lost.”* PU9 believed that rapid crypto-asset adoption might undermine governments: *“governments now have power that’s underpinned by their ability to control currency, and if they lost that, I’m concerned about how they would allocate capital and value to underpin some of the public needs of society [...].”* This user further explained how early adopters would have an unfair monetary advantage compared to the general public: *“if you own, say, 1 to 10 bitcoins now, you will be the 0.01% or 0.001% of the world’s wealthiest people in 20 years potentially [...] and I think in that sense [one] risk is a massive redistribution of wealth.”*

Risk perception appeared to be linked to the amount of money invested. PU1, PU2, PU10, and PU3 said that the severity of the risks would grow if they invested more, with PU1 saying: *“If I had multiple thousands, I’d consider it more, but I haven’t given [the risk of storing cryptocurrency on exchanges] too much thought.”*

Experienced Losses

Addresses RQ3

Losses were attributed to only a few risks, despite our participants mentioning many more. However, none of the participants reported having had their crypto-assets compromised. PU4, PU5, PU6, PU9, and PU11 had all experienced losses, each for different reasons. PU4 said that he had been phished after exposing and explaining a scam to others: *"I see an email request, you can tell the URL is wrong. Then, I close that MyEtherWallet. [...] Then I opened it up the next day, they happened to leave the scam tab open [and I used the phishing website to import my wallet file]."*

PU11 and PU5 had lost assets due to their own errors. PU11 explained: *"I definitely have one wallet with a small amount of bitcoins that I can't access—I lost the key."* PU9 also had lost a key, when using an ATM: *"[I] went to an ATM years ago [and] bought one bitcoin for like $100 or $200 like that, uh, and it stopped in a wallet I don't have the secret, I don't have a private key."* PU6 experienced an exchange shutdown, resulting in the loss of a substantial amount of cryptocurrency: *"I ended up losing a third of my portfolio that was on that exchange [...] it was over 100 Litecoins or something."*

Risk Management

Addresses RQ4 & RQ5

The risk-management techniques of our participants can be grouped into three categories: avoidance, reduction, and acceptance. Risk avoidance was most prevalent in non-users.

Volatility was a major concern for both user and non-user participants. The former reduced this risk through portfolio diversification. PU3 and PU4 reported counteracting volatility by purchasing multiple coin types instead of a single one, with PU3 (a student) saying: *"We like sort of started [...] dividing our assets. [...] so maybe we made sure we are safe from all sides in case the value falls."* Unlike the rest of the participants, PU6 enjoyed the volatility, explaining: *"it's very*

volatile [...] and that's when you gonna make the most money [...] So I personally love the volatility."

When it came to securing assets, some participants emphasized the importance of having a private key. This technique was mentioned by PU3, PU4, PU7, PU9, PU10, and PU11, with PU7 saying: *"Keep your own private key [...] When I say that, I know it's so difficult because it's not easy to operate."* PU2 and PU4 said that using multiple wallets and multiple devices prevents a single point of failure: *"In general, being across multiple devices, multiple wallets just helps protect [against] all those one-off dramas."*

The choice of wallets was influenced by whether or not users were able to access their private key. PU3, PU4, PU7, PU9, PU10, and PU11 preferred wallets with private key access, with PU7 equating key and ownership the following way: *"If you don't have the private key, it's not yours. It's that easy [...]."*

Fully insured storages were viewed as ultimate solutions. Both PU6 and PU9 explained how these solutions would provide the best security, with PU9 saying: *"it's these underground vaults in Switzerland—they're all over the world, you don't really know where they are, and it's a fully insured cold storage solution, but the thing is it's like multi-sig so [...] if they want to move your coins or your assets, they need your signature."*

One user considered seed phrases superior to key-based CMTs. PU1 argued that the seed phrase was a good alternative to the concept of private keys: *"The memorization of a seed phrase seems very plausible. I think people can memorize 12 words and then you could take it totally offline."*

Education was considered a possible mitigation technique by both users and non-users. PU4 stated that education is important and can be used as a way to prevent losses in the context of pyramid schemes: *"Education is very important. If there is a mining rig and you are getting paid day by day and everything works fine until one day it is not."* Similarly, PN4 stressed the importance of research for non-users, saying: *"I would have to do the research to understand it to be comfortable putting my money into something."*

One common theme among users was the acceptance of potential risks. PU4, PU5, PU6, and PU7 reported that when using exchanges, they knew they did not own the private key and everything would be gone in the case of an exchange

shutdown. PU6 summarized this sentiment well: *"It's just part of the game."* When talking about "shitcoins," the same user expressed a willingness to operate on questionable exchanges, stating that *"especially with a lot of these real shitcoins, they're on really [questionable] exchanges right? So [...] you kind of have to play in there, in the mud and get dirty."*

An overview of risks and mitigation techniques can be found in Figure 3.2.

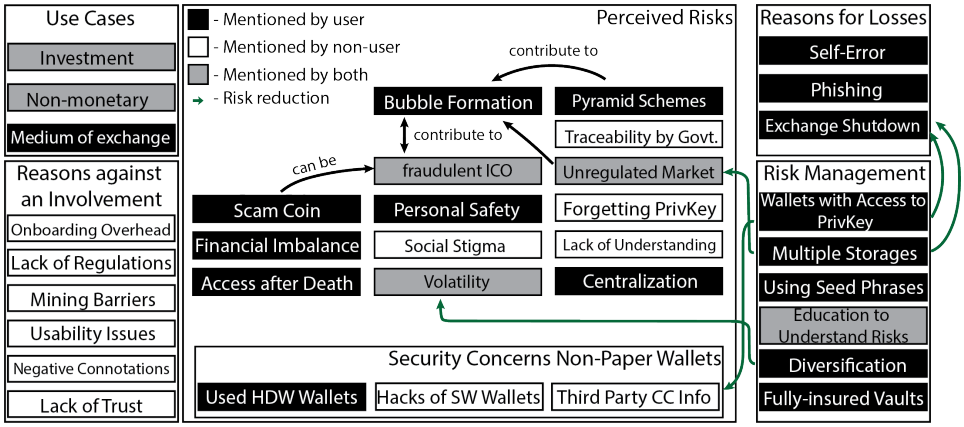


Figure 3.2: Overview of risks and risk management techniques

3.3.6 Trust

In the following sections we illustrate different trust dimensions and the identified cues. An overview of all trust antecedents can be found in Table 3.3.

Table 3.3: Trust antecedents of crypto-asset users and non-users. Antecedents marked with (–) inhibit the formation of trust.

Technological Antecedents	
Implementation:	decentralization, anonymity (–), immutability, cryptography, source code, software vulnerabilities (–), technology stack
Documentation:	books, academic papers, white papers, educational videos
Social Antecedents	
Interpersonal:	friends, family, coworkers, acquaintances, celebrities
Actor-specific:	news (–), team background, websites, social media presence, perceived size of exchanges and teams
Institutional Antecedents	
Structural Assurances:	lack of regulations (–), jurisdiction, location, compliance
Situational Normality:	exposure to alternative payment systems, perceived similarity of banks and exchanges, intangibility (–)
Subjective Antecedents	
Self-Efficacy:	lack of understanding (–), ability to conduct transactions

Subjective Antecedents of Trust

Self-Efficacy

Self-efficacy is the perceived ability to achieve certain goals. For crypto-assets, this includes the ability to conduct transactions successfully. Here, the familiarity with the respective system, which was shown to correlate with trust for e-commerce [74], online banking [188, 219], and mobile banking [138], becomes of importance. We also observed this in the context of crypto-assets.

Non-users had difficulties trusting crypto-assets because they did not understand the technology and were not even familiar enough with it. PN2 summarized her sentiment towards crypto-assets as follows: *"[...] what you know is comfortable, the unknown is uncomfortable and scary."* On a similar note, PN4 explained that crypto-assets in particular scare her, as she did not understand what exactly they were: *"[...] it seems like fake money and I feel [...] me not knowing much about it, I feel like it could just go under or become worthless or the fact that you don't have anything to show for it. That's what scares me."*

At the same time, those of our participants who did use crypto-assets, did not necessarily understand even the main building blocks of the underlying technology. PU2 did not understand public key cryptography, saying *"Oh, the private key I'm still confused with [...]."* This supports the findings by Gao et al. [73], who identified misconceptions for both users and non-users of Bitcoin. Therefore, it is possible that the familiarity with the wallets and platforms, and less so the protocols, is what results in a higher self-efficacy for users.

Technological Antecedents of Trust

Study participants reported on a variety of technology-related cues that can have an influence on their trust in crypto-assets. We present the findings in two groups, *implementation* (directly related to the technology or protocol) and *documentation* (descriptive reports or documents about the technology).

Implementation

Anonymity is often mentioned in the context of crypto-assets and it is therefore not surprising that it was brought up by both users and non-users. PU5 explained how Monero is *"a little bit dodgier [than Bitcoin], you can't quite see it unless you're the active participant [...] with two people trading which makes a lot of people happy because they can't be monitored."* This sentiment was however not shared by all users, as some raised concerns, such as PU11, because of potential illegitimate use cases: *"I like the idea of pseudonymous or totally anonymous payments [but anonymity] also really scares me so I think it's kind of a double-edged sword."*

Another reported characteristic was the *immutability* of the data published on the blockchain. PU7 believed that immutable data can help in holding transaction parties accountable: *"If we would have [...] some kind of blockchain-stored data that is just immutable and you know it's [...] the original data [...] we could solve [the accountability issue] pretty easily."*

Users seem to trust the underlying cryptographic protocols. PU3, PU6, and PU9 trusted the *cryptography*. PU3 explained that *"it all comes down to cryptography [...] how much do you really trust your mathematics."*

Closely related to the protocol is the actual *source code*. PU7 takes it upon

himself to verify the correctness of applications that can be viewed with the help of an app explorer: *"I taught myself Solidity so I can kind of get a good understanding of what their codebase is and can kind of see faults [...] in the actual source [...] Those are big red flags."*

Software *vulnerabilities* have a negative influence on trust. Such concerns, however, were expressed in regards to wallets, rather than crypto-assets. PU4 said to not use "anything that's been hacked" and then recalled a multi-signature vulnerability of a wallet.

Lastly, the *technology stack* used by companies was also a trust determinant. It was important for PU5's trust in crypto-asset exchanges which technologies those exchanges used: *"I feel, like, if [exchanges] are using banking level grade stuff [...] that feels very robust."*

Documentation

When it comes to newer crypto-assets and ICOs, all users reported to read *white papers*. In extreme cases, their judgments could be very superficial. For example, when PU1 was asked what factors he takes into consideration before purchasing a crypto-asset, he explained: *"Broadly, how many numbers are in the white paper. Are there formulas basically or is it just all writing."*

Users also reported to gather information from other sources. PU1 read *books* on crypto-assets, whereas PU3 explained that she read about Bitcoin in an *academic paper* and learned about *"[...] how it works, how it forms blocks, how there is a chain of [...] honest nodes [...]"*

While some non-users also referred to books, others preferred to gather information from less technical sources. For PN6, these were educational videos: *"I've seen some online lectures about the crypto coins, digital currencies [...] and I learned a little bit about the basics."*

Social Antecedents of Trust

Cues used by participants to develop trust towards other actors are discussed next. We identified two groups, *actor-specific* antecedents (i.e., characteristics of actors suggesting trustworthiness), and *interpersonal* antecedents (i.e., advice from the

social circle of the respective participants).

Actor-specific

Temporal embeddedness is an important factor in building trust among actors. In the crypto-asset domain, however, interactions with certain actors, such as newly-founded companies during ICOs, can be one-off events. As such, we wanted to understand how trust towards such actors is developed when there is no interaction history.

For non-users, one prevalent information source was the *news*. Similarly to the findings by Gao et al. [73], our data suggests that some non-users associate crypto-assets with illegal activities, with PN1 saying: *"The currency is used for totally buying guns, drugs, illegal stuff. That's why it became so popular and expensive."* It is therefore possible that information sources, the news being one of them, can negatively influence non-users' trust.

Contrary to non-users, owners of crypto-assets did not use traditional news sources, but gathered publicly available information to assess the trustworthiness of an actor. PU6 explained: *"[I research on] the person who is developing it [...] what's his background, what's his work history."* Similarly, PU8 believed that *"researching the people behind [the cryptocurrency]"* can help in understanding whether *"this person might run off with the money"* or not. his strategy, however, does not always work, as illustrated by PU5: *"Mt. Gox was a wake-up call to all of us [...] Cryptsy [24] was a big surprise. Cryptsy, I thought, would never go away [...]. They had a dedicated team, everybody was open, and to find that that was a scam too shocked me."*

Public presence of companies appears to influence trust in them. Sas and Khairuddin [194] suggest that *websites* are particularly important for bitcoin exchanges. Our data supports this in the general context of crypto-assets, as illustrated by PU5: *"I looked at the website and it looked pretty. I would've bought a few [coins], waited until it went up a bit and sold."* Besides websites, users reported to view *forums*, *Telegram channels*, and generally *social media* to assess a company's trustworthiness, with PU7 saying: *"[companies] usually have some sort of social media presence [...] you can go down a rabbit hole, see what people*

are up to, where they come from and if things don't match up, then it's a big red flag."

Telegram chat channels seem to be an information source about new crypto-assets. PU5 and PU6 mentioned the influence these channels might have, but also had concerns, as explained by PU6: *"it's all just nonsense [...]. You ever go to one of those Telegram chats for that new shitcoin that just came out. These guys are sitting there talking about how it's going to $100 [...] It's like they're so dumb that they'll keep putting their money into it."*

Social media can also influence trust of users. PU10 explained that communities, such as reddit, influence his decision making: *I didn't put a lot of thought into it [...] I went to what seemed like the the largest subreddit with the talks about Bitcoin or blockchains [and just used the wallet people promoted]."*

Besides the individuals behind an asset, the *perceived size* of exchanges and companies also influence the users. For companies, PU9 considered the size of development teams important, saying: *"[...] deploy capital where you have the most developers in the biggest communities [...] they'll probably succeed."* The size of exchanges on the other hand, and therefore the corresponding trust, was influenced by the *trading volume*. PU2, PU6, PU7, and PU8 considered the trading volume of exchanges before using them, with PU8 saying: *"Also trading volume is one of the indicators, if they're bigger they have more resources, I assume that to safely secure my portfolio."* PU7 further argued that bigger exchanges are more *transparent* in comparison to smaller ones: *"[...] the bigger exchanges [...] they're very transparent, you can see them. But the problem with smaller exchanges is that if they pull an exit scam, you can't trace them [...]"*

Closely related to the size is the *funding*, which was brought up for both exchanges and companies. PU2 believed that a start-up is trustworthy if *"they have a strong capital investment."* Similarly, PU4 argued the same for exchanges: *"You just kind of hope they are secure because they have so much funding [...] they are accountable."*

Interpersonal

Apart from publicly available trust cues, both users and non-users also rely on recommendations. PU3 explained that *"major sources comes from [...] friends and family who are already investing."* This was also prevalent for non-users, with PN4 saying that she heard about crypto-assets from friends first: *"Through friends [...] interestingly enough before I heard about it in the news."* When asked about how she decided what information to believe, she answered that *"[her] personal relationship with them and whether [she] thinks they are a credible person"* plays a major role.

Co-workers were another source of information. PU1, PU3, and PU11 purchased crypto-assets because of a recommendation by colleagues, with PU3 explaining: *"All the interns were sitting, and everyone was discussing about Bitcoin [...] I just decided to invest a little in bitcoin."* Prior to purchasing a crypto-asset, PU11 asked developers that he was working with: *"I like to talk to actual developers who I trust and get their opinions on it."*

Users also seem to trust people who seem to have more expertise than them. Participants took into account recommendation from acquaintances and even individuals that they have not met personally. For PU6 these were cryptographers and system analysts, whereas PU2 also trusted crypto-asset celebrities, saying: *"First thing for me is whether I hear about this token from a very famous person or a very experienced person. If this person tells me what to buy, I buy it."*

Institutional Antecedents of Trust

The last identified dimension of trust is institution-based. Gefen et al. [74] suggest two types of institutional antecedents of trust: *structural assurances* (including regulations and guarantees), and *situational normality*, as perceived by the user during an interaction. According to the data, it appears that both have an influence on people's trust in crypto-assets.

Structural Assurances

Signaling trustworthiness in the domain of crypto-assets is a complex issue. For e-commerce, trust badges are supposed to signal trustworthiness to the respective

end users. For crypto-assets it is however not clear how such guarantees can be made. Especially non-users found the lack of a regulatory involvement worrisome. PN5 suggested that regulations can help in reducing the risk of malicious actors in the form of ICOs: *"A lot of ICOs are just scams [...] the government should regulate that. [...] I think a similar [to IPO] process should be applied with ICOs."*

While users did not explicitly mention regulations, other factors played a role in their decision-making. The *jurisdiction*, under which the respective company or exchange is operating, as well as the *location* of the company appeared to influence trust of some participants. To illustrate, PU5 explained: *"Russian exchanges. I just don't trust them. I don't even know if I could get the money out."* In addition to that, PU8 pointed out the importance of start-ups meeting *regulatory compliance* in the respective country: *"If they say it's for investment then you have to be careful whether or not this project has compliance."* Users and non-users expressed different views on the institutional involvement, yet, both appeared to agree that assurances can help with criminal actors.

Situational Normality

The lack of situational normality for non-users appeared to be a hindrance. Contrary to *familiarity*, situational normality does not include knowledge [74], which, here, is about the underlying technology.

Non-users had difficulties dealing with the intangible nature of crypto-assets. This was a stumbling block for both PN2 and PN4, with PN2 saying: *"[...] it's all virtual. There's nothing real like you don't see anything [...] how do you know how much you have? [...] what happens if all of a sudden you wake up tomorrow morning and there's nothing showing you that you have any crypto."* Interestingly, this participant is working at a money exchange and it is therefore not surprising that strictly intangible interactions appeared abnormal.

PN9 (a student) further believed that crypto-assets and banks fundamentally differ: *"[...] there's hundreds of sites which say invest in this and that [...] so e-currency always seem like a scary thing [...] What if you ended up on a site which is not secure? [...] while banks have [...] a physical institution right in front of you if there is anything wrong."*

Some users, on the other hand, perceived crypto-assets and traditional banks to be alike. PU6 believed that trusting an exchange is not different to trusting a bank, saying: *"The bank machine only allows you to take out so much per day [...] these kinds of controls already exist, it wasn't really a big reach for me to trust another big institution [...]"*

Exposure to alternative forms of currency in the past appear to help adapting to crypto-assets. PU7 explained: *"[the store] had little paper money [...] and then similar things to those. I was exposed to [...] alternative forms of currency."*

These findings support the importance of situational normality for the development of trust. Gefen et al. [74] suggest that the perceived normality might indicate a successful transaction, and this appears to apply for crypto-assets.

3.4 Discussion

3.4.1 Misconceptions and Usability Barriers

Users had dangerous knowledge gaps and misconceptions when it came to the key building blocks of crypto-assets. Some users did not know the difference between public and private keys, and one incorrectly believed that they had access to their private key while using an exchange. Such a misconception could lead to a false sense of security and control over wallets, particularly nowadays when the crypto markets (and the exchanges that operate on them) are so volatile.

Non-users had their own set of misconceptions. Some believed that crypto-assets are mainly used to purchase illicit drugs. While this was one of the main uses of bitcoin in its early days [115], the applications nowadays are wide ranging. Non-users also discussed the notion of crypto-asset privacy. While some believed that transactions could be traced back to them by the government, others believed in their anonymity.

Current CMTs have usability problems. Combined with misconceptions about crypto-assets' building blocks, these UX problems result in barriers that are hard to overcome. Participants' usability concerns also seemed dependent on the respective crypto-asset. One participant explained having failed to use Augur, as they were not able to make a transaction using their application's interface. Another

found Monero harder to use than other crypto-assets because of the two pairs of keys: private and public. We therefore believe that findings on usability issues with Bitcoin key management tools [66] and the identified risks affecting Bitcoin usability [50] are not necessarily applicable to other crypto-assets and their applications.

3.4.2 Risks

Our results suggest that risk perception and management among crypto-asset (non) users goes beyond Bitcoin, as it depends on such factors as the application area, storage method, and amount invested. Our user participants stored their long-term holdings in the form of bitcoins in more secure ways and said they did not consider risks associated with short-term holdings a major concern. Similarly, four other users with smaller amounts said they would consider more secure storage options, but only if they had purchased more.

Design recommendations to combat some of the risks can be found in the literature. Authorized exchanges were proposed by Sas et al. [194] to combat dishonest traders through verification processes for buyers and sellers. Our data, however, suggests that both users and non-users consider such procedures bothersome and a significant barrier to entry. Since verification is mandatory, it should be in the interest of exchanges to optimize this process.

Public key cryptography appeared to still be a hindrance for many. Some participants considered keeping the private key private to avoid losses in potential shutdowns of exchanges. This, however, can only be done if the respective user understands the value of the private key. Some of our participants reported having accidentally deleted wallet files, while others did not understand what private and public keys were in the first place. One possible reason for this finding is that CMT providers do not convey the importance of keys clearly enough. While hosted wallets, such as exchanges, do not allow users access to private keys, others such as software wallets do. Therefore, depending on the CMT, users require a different level of understanding to ensure correct and secure handling.

3.4.3 Trust

Unreliable Information as Basis for Trust

Whenever information about the contextual properties of an actor is limited, users employ publicly available (unreliable) information to build and maintain trust. They research *blogs*, *websites*, as well as *white papers* and *forums* to assess whether a coin is worth purchasing. Learned mostly from public web pages, the *history of the development and operating team* (and its members), as well as the *jurisdiction* of the exchange or company behind it, play important roles. Yet, reliance on this type of information does not necessarily work. As a case in point, two exchanges, Mt. Gox and Cryptsy, ended up being scams, even though some of our participants were sure about their legitimacy. Some users also reported to consider the location of the exchange, with PU5 reporting to not use Russian exchanges. Stereotyping can lead to trust/distrust [192] and we encountered similar patterns for crypto-assets.

Further, when choosing a crypto-asset exchange, participants reported to take into account the *trading volume*, which was shown to be prone to manipulation. A report issued by the Blockchain Transparency Institute in 2019 suggests that the volumes of exchanges were being manipulated [107]. The report goes as far as claiming that some of the exchanges seemed to have inflated their trading volumes by over 90%. Thus, it is possible that users can be misled, if they take trading volumes into account.

Most importantly, crypto-asset markets appear to suffer from information asymmetry [23, 41]. Coin developers, exchange operators have an advantageous position, which can be easily abused. While users appear to do the best they can to mitigate this information asymmetry, unsurprisingly, they are very limited in their capabilities. Our results suggest that their practices of trust management rely on public information that can be either easily mimicked or faked by organizational actors (e.g., presence of formulas in white papers, records about prior projects of the developers, quality of the organization's web site) or otherwise unreliable (technology stack, advice of friends and celebrities).

If such information is used to distinguish between legitimate and fraudulent

parties, the amount of scams in the domain does not appear surprising any longer. While regulations might help reducing the amount of malicious actors, users preferred the unregulated and decentralized nature of crypto-assets. At the same time, however, users relied on regulators combating fraudulent ICOs and exchanges. This is clearly a paradox, and therefore, one of the biggest research and practical questions is who and how could aid users of crypto-assets in managing trust effectively.

Trust Impediments for Non-Users

We have revealed shortcomings in all four dimensions that appear to negatively influence the formation of trust, thus, eventually leading to a decision against crypto-assets. This is in line with the argument of Gao at al. [73] who suggest that the lack of trust in Bitcoin itself might be one of the concerns for non-users.

Non-users had a *low perceived self-efficacy* and believed to not have the required skill set to be using crypto-assets. Some said to not know where to purchase crypto-assets in the first place, whereas others explained to not understand the underlying technology well enough in order to be able to use it. The lack of understanding, however, was also shared by some users, who, despite all, were able to use crypto-assets and were confident in their abilities. Self-efficacy in the context of crypto-assets might therefore be tied to the familiarity with the respective CMT, and not the underlying technology.

Non-users also reported a poor user experience when interacting with tools and exchanges. Some participants did not know where to purchase crypto-assets, while others failed to do so because of high entry barriers. For example, one major issue (reported by users and non-users) was the bothersome KYC processes. Combined with the lack of guidance and the sheer number of available wallets and platforms to choose from, newcomers seemed to be overwhelmed. For online banking it has been shown that ease of use positively influences the initial formation of trust [203, 228] and we believe that an enhanced user experience can also foster trust in crypto-assets.

Structural assurances in the domain are limited. Non-users raised concerns and argued that they cannot trust a currency that is unregulated. The same holds

true for exchanges. Although, while regulated, QuadrigaCX was still shut down and millions of funds were lost [43]. Technology can therefore only do so much to combat bad actors and assurances have the potential to positively influence the development of trust.

Non-users perceived crypto-assets as abnormal, which hints at a *lack of situational normality*. In a study by Hernandez et al. [133] with unbanked participants in Mexico, informality was found to play a role in transactions because the participants were used to it. Similarly, our interviewees' experiences influenced their perception of trust when it came to crypto-assets. Some were familiar with alternative currencies, whereas others found purely virtual transactions abnormal.

Generally, it appears that the lack of guidance and institutional trust in the form of regulations and situational normality might lead to mistrust, and therefore to non-involvement.

3.4.4 Design Recommendations

Increase Situational Normality and Self-Efficacy

Both situational normality and self-efficacy appear to have an influence on the formation of trust in crypto-assets. Non-users found transactions abnormal and also believed to lack the necessary knowledge that would enable them to use the technology. Sandboxes and tutorials might help in increasing both situational normality and self-efficacy. Allowing newcomers to first familiarize themselves with the tools, terminology, and characteristics of transactions, such as irreversibility, can help in lowering the fears that were reported by some of our participants. This can be of importance for those people who are familiar with conventional payment systems, such as online banking, and might rely on safety nets that do not exist for crypto-assets.

Eliminate the Need to Trust Third Parties

Several users have reported to have lost crypto-assets in exchange shutdowns. In all cases these were custodial exchanges where users were not in possession of their private keys. While most participants understood the risk of using custodial

exchanges, some did not. As a case in point, PU1 believed to have access to his private keys on Coinbase, which is not the case in reality. Users of crypto-assets therefore, knowingly or unknowingly, put themselves at risk whenever they decide to transfer their holdings to exchanges. This risk, however, can be reduced or even eliminated by leveraging existing technology.

One possible way of improving the overall security is a seamless integration of wallets with custodial exchanges. This would provide a certain level of control for users and would further reduce the chances of falling victim to malicious actors. Crypto-asset exchanges have publicly available APIs to send and withdraw assets [14], however, most software wallets nowadays do not make use of these. By automatically sending assets to the exchanges and withdrawing directly after a successful trade, one would reduce the risk of monetary losses.

Another option would be to eliminate third parties all together through non-custodial solutions. Decentralized exchanges such as IDEX [105] or Uniswap [209] are based on smart contracts and eliminate middlemen in exchanges. In these cases, trust would shift from social to the technological dimension. While these exchanges are well-established and have existed for multiple years, none of the participants reported to be using them. An investigation of the usability/security trade-off in the context of custodial and non-custodial exchanges could be explored in future work.

3.5 Conclusion

We conducted semi-structured interviews to further an understanding of the behaviors of both users and non-users of crypto-assets. We identified that perceived risks and mitigation techniques are dependent on the specific crypto-asset, its storage options, and the amount being invested. Further, misunderstandings seemed to be prevalent in both users and non-users and could lead to dangerous errors, potentially resulting in monetary losses.

To truly understand risk perception and management in the domain, one therefore needs to study crypto-assets beyond bitcoin, as they expose users to new risks and challenges. We believe that to reduce risks, further public education is necessary, and government involvement is needed to combat pyramid schemes and

unregulated ICOs.

Perceived risk and trust further appear to be closely related. Both appear to have an effect on the willingness to get involved with crypto-assets. Users seemed to have enough trust in the ecosystem, even though unreliable cues might have been used to build said trust.

For non-users, on the other hand, various factors, such as the lack of structural assurances and low self-efficacy inhibit the formation of trust, thus, leading to decisions against crypto-assets. We therefore conclude that the development and maintenance of trust is a key factor for both existing and new users.

Chapter 4

Analyzing the Behaviors of Users and Non-Users of Crypto-Assets

Next, we wanted to validate and refine the qualitative findings presented in the previous chapter and for this reason, we conducted two quantitative studies. Section 4.1 reports on the findings on the security perceptions and practices of crypto-asset users, whereas Section 4.2 focuses on the adoption behaviors of both users and non-users and the factors influencing them.

4.1 Understanding the Security Behaviors of Crypto-Asset Users

4.1.1 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.

Empirical Studies on Crypto-Assets

Crypto-assets have received a fair share of attention from academia in recent years. Table 4.1 presents an overview of qualitative and quantitative user studies with additional sampling details. Sampling the hard-to-reach population of crypto-asset

Table 4.1: Overview of empirical studies on crypto-assets

Year	Qualitative studies	Quantitative studies
2020	Mai et al. (2020) Fröhlich et al. (2020)	
2019	Khairuddin and Sas (2019)	Arias-Oliva et al. (2019) Stix et al. (2019) *
2018		Rauchs et al. (2018) Henry et al. (2018) *
2017	Sas and Khairuddin (2017)	Rauchs et al. (2017)
2016	Gao et al. (2016) Khairuddin and Sas (2016)	Krombholz et al. (2016) Abramova and Böhme (2016)
2015	Baur et al. (2015)	
2014		Bohr and Bashir (2014) **

* Representative nationwide sample
** Use of secondary data collected on related Bitcoin sites

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 [169]. According to this classification, deep sampling involves such methods as snowball, respondent-driven, or targeted sampling [95], 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 [118], as well as challenges experienced during use [73, 216]. Besides trust [116, 194] and usability issues of wallets [19, 71], users are also found to have difficulties with the key management process [66]. Results show that some users have misconceptions related to the cryptographic principles [73, 146], while others, and novices in particular, often find the key management complicated [66, 73, 216]. 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 [194] or mistakenly deleted key pairs, which was reported by users in our interview study (Section 3.3.5).

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. [97] and Stix [199], whereas a series of global crypto-asset benchmarking studies [99, 180] attempted to characterize the crypto-asset population. Studies investigating risk perceptions and security practices of users can be found in literature [4, 126], 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 [180]. 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. As discussed in Chapter 3, this heterogeneity can be observed in their attitudes and experience toward crypto-assets, usage patterns, preferences over CMTs, risk profiles, and security behaviors. 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 security perceptions and practices.

Password and Key Management

There exists an extensive body of research on the challenges users face when managing their passwords. Adams and Sasse [5] 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 [69,

92, 220], sharing [206], and writing down passwords [200]. Pearman et al. [173] 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 [223] 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. [190]. Only 1 out of 10 pairs of users managed to exchange encrypted emails [190]. 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 [194] 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. Participants in our interview study reported to have faced challenges when managing their keys and we also found that newcomers were confused and overwhelmed by the underlying cryptography (Section 3.3.4). Often, they did not know where their keys were stored and even recalled instances of accidentally deleting keypairs. Inspired by these findings, 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.

4.1.2 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.

Approach

Over the years, more diverse individuals have become crypto-asset owners [99, 180]. As established in related work (Section 4.1.1), 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 [179]. 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 [55].

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) [185], which originated in individual health studies, and the Theory of Planned Behavior (ToPB) [6], 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) [58, 135] with its risk-augmented variant [171]. There are many examples of empirical computer security studies using these theories, including [29, 39, 54, 114, 144, 201, 202, 226].

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 [226] "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 B.29 in Appendix B.2 lists all scale items along with references to the sources from which they were adapted.

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. [118], 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 [126, 194], 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 Table 4.2). 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 [26, 79, 126] 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 [126, 194] and the results of our qualitative study (Chapter 3), 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 [4, 126], we collected basic demographic data. We inquired about their age, gender, occupation, degree, country of residence, and ethnicity.

Table 4.2: Wallet definitions

Crypto wallet type	Explanation note
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 authorise a transaction.

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[1] 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 [181]. 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 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 4.3.

Table 4.3: Demographics of the two 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%

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

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%
Doctorate 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	-	**57**	**29.2%**
Austria	0	-	23	11.8%
Germany	0	-	10	5.1%
Other	0	-	24	12.3%
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%

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[2] 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 both UBC and University of Innsbruck. 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 [53]. As reported in Table B.29 in Appendix B.2, all constructs have an alpha value greater than the rule-of-thumb threshold of 0.7 [205]. Also, the values do not improve after dropping an arbitrary item in any scale, which

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

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.

4.1.3 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.

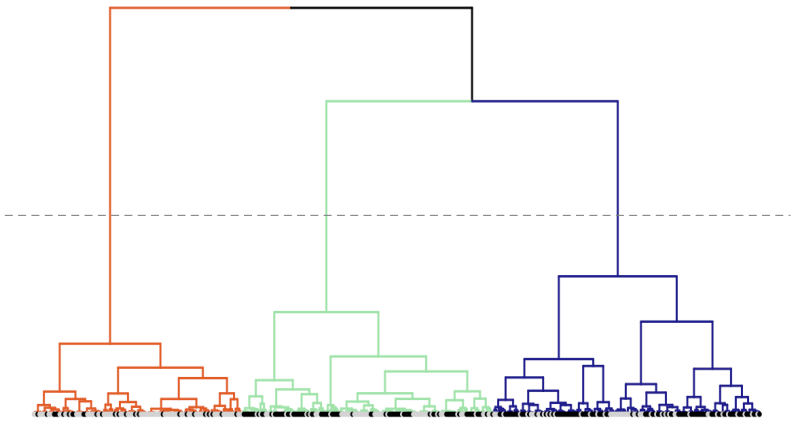
Typology of Crypto-Asset Users

Our data was categorical and we therefore employed Ward's hierarchical clustering with the Euclidean distance measure. The result was a dendrogram (shown in Figure 4.1a) suggesting three distinct clusters in the dataset.

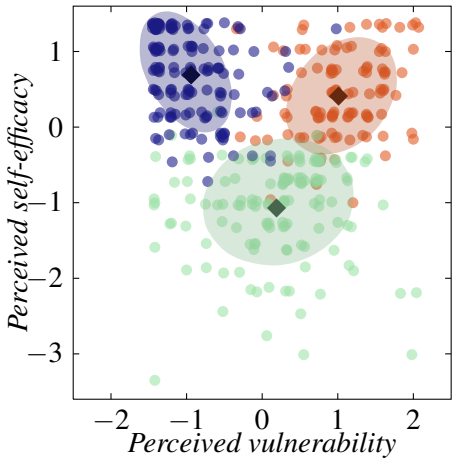
We tested the stability of this cluster solution by iteratively dropping one of the discriminating variables and rerunning the analysis. The resulting dendrograms, presented in Figure 4.2, reasonably support solutions with three clusters.

We visualize the cluster analysis results in Figure 4.1b 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 4.1b 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 4.3. At this point, we introduce the labels for the clusters



(a) Hierarchical cluster dendrogram



(b) Clusters and their centroids along two constructs

Figure 4.1: Cluster analysis results

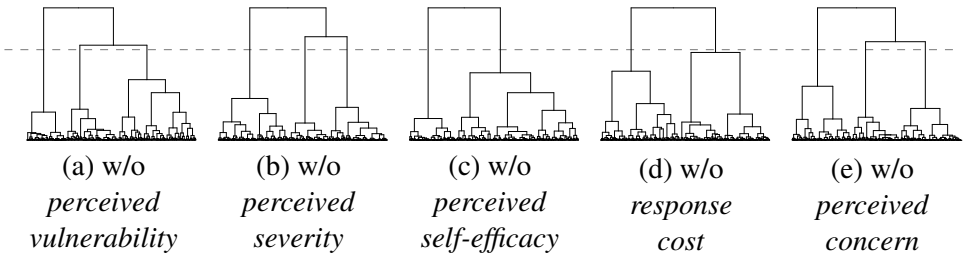


Figure 4.2: Dendrograms for the cluster analysis without (w/o) one of the five constructs

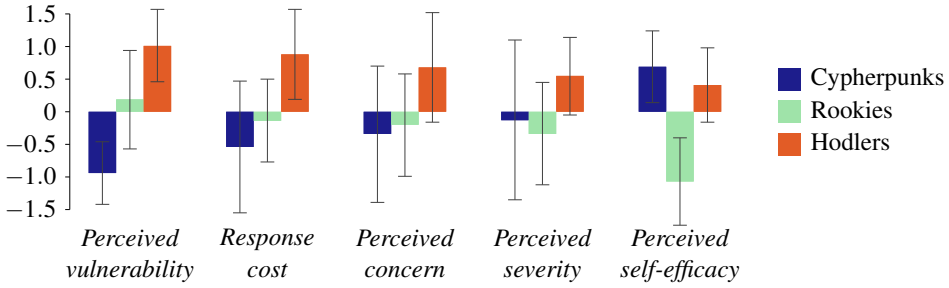


Figure 4.3: Construct means and ± 1 standard deviation per cluster, sorted by increasing values of the cypherpunks

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.

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 4.4), which is expected, considering their high scores on *perceived self-efficacy*. While hodlers scored lower than cypherpunks, they are more knowledgeable and

Table 4.4: 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

confident in their skills than rookies, who have the lowest scores throughout.

Below, we provide the profile description of each cluster and justify our hand-picked 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 4.5).

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 4.4a),
- "What factors influenced your decision when choosing a crypto wallet for storing your crypto-assets?" (Figure 4.4b).

Cypherpunks are technically savvy enthusiasts and early adopters who became obsessed by crypto-assets out of ideological and technological interest. As presented in Table 4.5, they are mostly men ($\sim$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. Moreover, digital tokens are held almost exclusively by cypherpunks (20%). Besides purely financial motives, cypherpunks rank the interest in the blockchain technol-

ogy itself and decentralization as the primary drivers of the crypto-asset usage (see Figure 4.4a). 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.

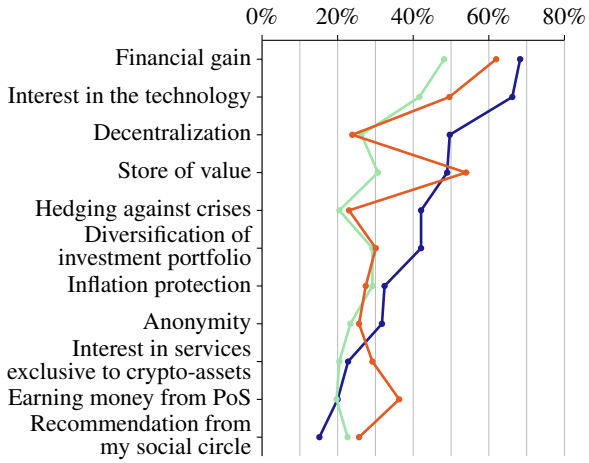
Rookies are casual users who joined the crypto market out of fear of missing out (FoMO). This is evidenced by the high fraction of rookies who are novices or who started to invest in crypto-assets 3–4 years ago, probably following the record surge in bitcoin's market price in 2017. While being curious about the technology, they seek long-term financial gains and profit opportunities (see Figure 4.4a). 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 4.4b).

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[3] in a misspelling by a bitcoin trader. Since then, hodlers are often associated with profit-oriented crypto-asset users, and this term therefore seems appropriate for the cluster.

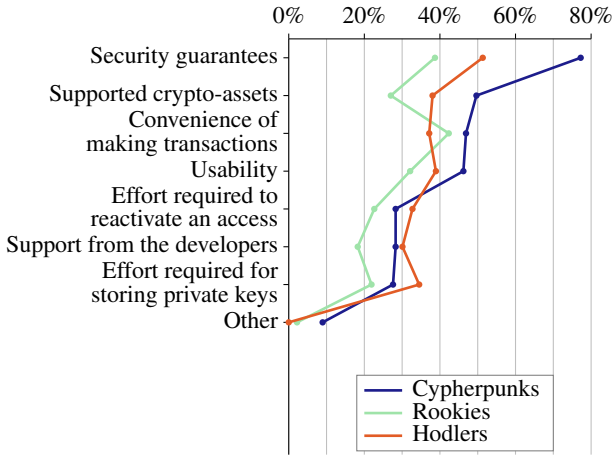
Besides trading crypto-assets, hodlers also trade on conventional stock markets more often (23% "regularly") than cypherpunks (18%) and rookies (13%). Interestingly, 25% of hodlers report owning more than US$100 000 of crypto-assets. As high-net-worth individuals, they are especially interested in proof-of-stake (PoS) protocols, perhaps to reap the benefits of the so-called compounding effect [67]. 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-

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



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



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

Figure 4.4: Self-reported factors in percentage of users per cluster, sorted by decreasing values of the cypherpunks

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 believe to know best what security in the context of crypto-assets means, whereas rookies perceived themselves as the 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

Table 4.5: 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%
1 000 – USD 5 000	18.6%	21.2%	15.9%	18.7%
5 000 – USD 10 000	13.1%	20.4%	20.4%	17.7%
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%

of their digital assets and devices.

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

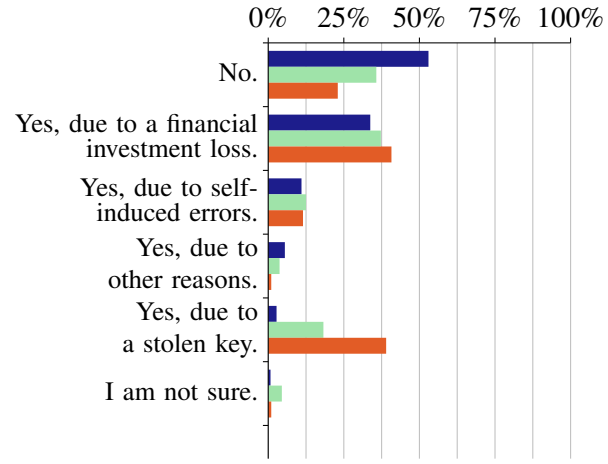
population level. In particular, all the three clusters appear in both samples and presumably in most populations of interest. The prevalence of each cluster may however vary between countries across the globe. Nevertheless, the user typology remains a strong tool to make more generalizable statements 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, as opposed to cypherpunks who mostly avoided this fate. Figure 4.5a provides an overview of the experienced losses and causes (including thefts of private keys) broken down by cluster.

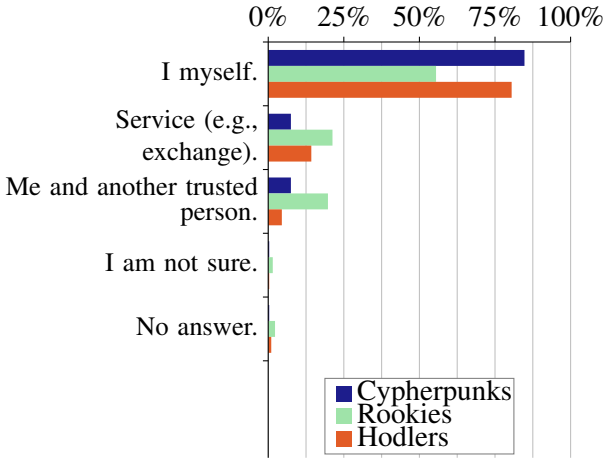
Rookies appear to refrain from managing their own private keys and often rely on third parties. This is not surprising, considering their low *perceived self-efficacy* and corresponding inability to self-control cryptographic keys. Close to half of rookies (see Figure 4.5b) also report sharing keys with 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 our interview study (Section 3.3.4). 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 4.6). 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 [111]. 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 4.6). 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.

Our qualitative findings presented in Section 3.3.4 suggest that individuals



(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)*

Figure 4.5: Self-reported monetary losses and control over private keys per cluster

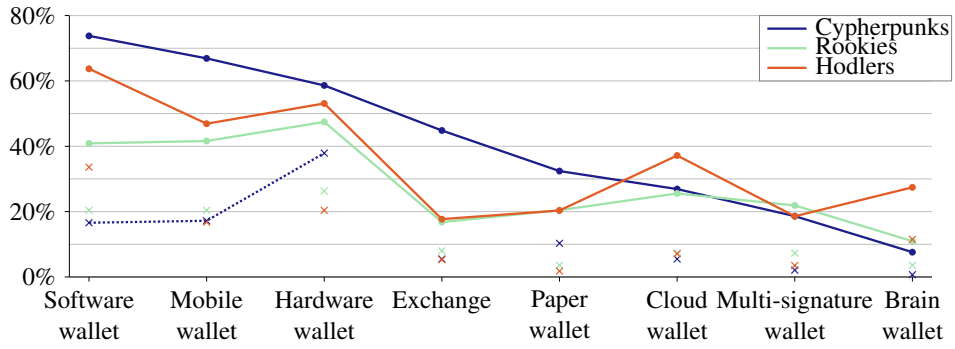


Figure 4.6: Self-reported usage of wallets in percentage of users per cluster. Cross symbols refer to the wallet type which holds the majority of the user's funds (*single-choice*).

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 4.6 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.

Table 4.6: 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

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 4.5) into a binary variable with a cut-off value of US$10,000. As for the dependent variables, we considered the 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 4.7.

Table 4.7: Results of the logistic regression models

	Hardware wallet	Software wallet	Mobile wallet	Other cold wallet	Custodial wallet	Custodial wallet
Value at risk						
$>$ \$10000 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: *** $p < 0.001$; ** $p < 0.01$; * $p < 0.05$

Among all the types considered, we quantitatively confirm, as conjectured in Section 3.3.4, 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.

Holding a particular crypto-asset also appears to have an effect on the wallet choice. The results of the logistic regressions (see Table 4.8) suggest that the ownership of privacy cryptocurrencies, such as Monero and Zcash, has a significant negative effect on the user's choice of mobile wallets. The ownership of bitcoin, on the other hand, has a positive effect on the choice of software wallets as one's

Table 4.8: Results of the logistic regressions with wallets as dependent variables

	Hardware wallet	Software wallet	Mobile wallet	Other cold wallet	Custodial wallet
Crypto-asset held					
Bitcoin	-0.583^{*}	1.276^{***}	-0.027	-1.314^{***}	0.459
	(0.286)	(0.382)	(0.339)	(0.386)	(0.413)
Ether	0.195	-0.163	0.231	-0.268	0.099
	(0.248)	(0.263)	(0.280)	(0.376)	(0.322)
Tokens	0.284	-0.573	-0.432	0.625	0.370
	(0.371)	(0.522)	(0.524)	(0.538)	(0.507)
Privacy cryptocurrencies	0.147	0.411	-0.731^{*}	0.232	-0.159
	(0.243)	(0.263)	(0.316)	(0.353)	(0.333)
Control variables					
Cypherpunks	-0.220	-2.704^{***}	-1.447^{***}	-1.053^{**}	-2.620^{***}
	(0.340)	(0.457)	(0.412)	(0.465)	(0.510)
Rookies	-0.860^{**}	-2.298^{***}	-1.205^{***}	-1.933^{***}	-2.010^{***}
	(0.279)	(0.388)	(0.325)	(0.401)	(0.401)
Hodlers	-1.061^{**}	-1.815^{***}	-1.451^{***}	-0.937^{**}	-2.341^{***}
	(0.342)	(0.413)	(0.395)	(0.419)	(0.482)
Observations	394	394	394	394	394
Log Likelihood	-228.009	-198.623	-183.284	-122.313	-149.903
Akaike Inf. Crit.	470.018	411.246	380.569	258.625	313.806
Significance level:	Significance level: $^{***}p < 0.001$; $^{**}p < 0.01$; $^{*}p < 0.05$				

preferred wallet type to store the majority of the funds. Therefore, we are able to confirm the hypothesized effect of crypto-assets themselves on the wallet choice as was discussed in Section 3.3.4.

We have also investigated whether the owned crypto-asset has an effect on the perceived severity of certain risks. Similar to the amount held, we also recoded the ordinal responses to the perceived risks into a binary variable. Here, we only consider high risks, i.e., a threshold of $\geq$4 (on a five-point Likert scale). For example, as can be seen in Table 4.9, owning privacy cryptocurrencies has a negative effect on the perceived severity of the risk to be extorted. In other words, this implies

that users owning privacy coins perceive themselves as less vulnerable to the risk of being extorted, which seems plausible. This, again, confirms our findings from the interview study, where we hypothesized that the perceived risk severity was dependant on the crypto-asset held.

Table 4.9: Results of the logistic regressions with risks as dependent variables

	Volatility risk	Extortion risk	Exchange vulnerabilities	Legal uncertainty
Crypto-asset held				
Bitcoin	0.575*	−0.468	0.101	0.254
	(0.286)	(0.289)	(0.266)	(0.283)
Ethereum	0.462	0.005	0.274	0.466*
	(0.239)	(0.242)	(0.225)	(0.238)
Tokens	−0.323	−0.782	0.454	−0.935*
	(0.384)	(0.459)	(0.374)	(0.424)
Privacy cryptocurrencies	−0.525*	−0.568*	−0.630**	−0.073
	(0.242)	(0.253)	(0.226)	(0.237)
Control variables				
Cypherpunks	−1.130**	−0.324	0.045	−0.995**
	(0.347)	(0.348)	(0.322)	(0.344)
Rookies	−0.997***	−0.352	−0.189	−1.112***
	(0.285)	(0.275)	(0.260)	(0.284)
Hodlers	0.728*	1.547***	0.753*	0.491
	(0.334)	(0.351)	(0.314)	(0.323)
Observations	393	391	392	392
Log Likelihood	−238.338	−227.514	−257.297	−240.725
Akaike Inf. Crit.	490.676	469.028	528.595	495.449
Significance level:	Significance level: *** $p < 0.001$; ** $p < 0.01$; * $p < 0.05$			

When it comes to security practices (see Table 4.10), rookies implement them less frequently than cypherpunks or hodlers. Similar discrepancies are found in the work of Ion et al. [108], 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 [166] 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 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 [36], 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.

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 4.6): 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 4.6) reveals that hodlers are 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 [124], 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 [11, 49, 160].

Table 4.10: 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.

4.1.4 Discussion

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 [106, 114, 226]. 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 [129] and comprise *fundamentalists* (highly concerned), *pragmatists* (somewhat concerned), and the *marginally concerned*. Dupree et al. [62] 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 being the most motivated and knowledgeable. For crypto-assets, the presence of different security personas was first suggested by Fröhlich et al. [71], 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 [204] or fitness trackers [72], 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 4.3).

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 [4, 126] or produced findings that were hard to generalize because of the small sample size [71, 73, 146, 194, 216]. Studies surveying the bitcoin user population were also predominantly of male users, with Bohr and Bashir [27] only finding 5% female users in 2014, and Krombholz et al. [126] 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.

4.1.5 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 custo-

dial solutions, such as Coinbase[4] or Binance,[5] 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. While the identified clusters might not be nuanced enough to give detailed design recommendations, they can still provide guidance in how to better address the different needs of the users. 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 [66, 216]. 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. Our findings from the interview study suggest that users are often not aware of where their private keys are being stored and this confusion leads to inadequate risk assessment (Section 3.3.4). To address this, wallet providers should be more transparent about the key management, particularly when it comes to the storage practices. Prior work [63, 182] 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. [71], 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

[4]Coinbase: www.coinbase.com
[5]Binance: www.binance.com

encrypted on the respective device and saved to a cloud service, similar to the beginner version of the Casa wallet.[6] 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,[7] 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 Central Bank Digital Currencies. 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.

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

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

men [90]. 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.

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* [222], 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 [97], 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 [39]. 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.

4.1.6 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.

4.2 Understanding the Adoption Behaviors in the Context of Crypto-Assets

There exists an extensive body of research investigating the factors that influence the adoption of information technology. Arguably, the most popular model is the Technology Acceptance Model (TAM) [58], which incorporates *perceived ease of use* and *perceived usefulness* as two constructs that influence an individual's

decision to adopt and use a new technology. This model and its extensions, such as the Unified Theory of Acceptance and Use of Technology (UTAUT) [212], have been successfully applied in various IS domains, including, but not limited to, the fintech sector [86, 121, 131, 176]. They have been shown to explain a significant proportion of the variance in the dependent variable, i.e., the behavioral intention to adopt the respective technology or software.

Since crypto-assets can be used as a digital currency, this study is guided by prior work on electronic payment systems. Hanafizadeh et al. [87] conducted a review of 165 studies between 1999 and 2012 that explored the factors influencing the adoption of Internet banking. They found that the vast majority of theory-driven publications employed the TAM or its extensions. The latter often included cultural or study-specific variables, but also constructs, such as *risk* and *trust*, that were shown to play a vital role. The first evidence of their significance was provided by Pavlou [172] and Gefen et al. [74] in the context of e-commerce, and was later confirmed for mobile banking [7, 120, 134, 141]. For example, Lee et al. [134] conducted a survey with 306 participants and studied the effect of risk and trust perceptions on the adoption of mobile banking in Korea. Both constructs comprised multiple dimensions, with trust being a significant predictor of the adoption.

Similarly, Luo et al. [141] investigated the effects of risk and trust on mobile banking adoption. Contrary to Lee et al. [134], however, the authors included more dimensions in their constructs and further investigated the interactions between them. Both constructs were found to be significant predictors, with risk having a negative and trust a positive effect on the behavioral intention.

More recent studies have also confirmed the importance of trust in adoption behaviors [9, 196]. Both Alalwan et al. [9] and Sharma and Sharma [196] extended the UTAUT2 and information systems success models [60] respectively by including trust dimensions, and provided empirical evidence for the hypothesized effects.

Another prominent construct influencing adoption behavior is *perceived self-efficacy* [8, 113, 140, 149, 161, 228]. It refers to an individual's perceived capabilities to achieve designated levels of performance in a given context [18]. Its importance has been confirmed by scholars for mobile banking, both for users [140, 228] and non-users [113]. Whereas Zhou [228] considered the moderating effect of

self-efficacy on the initial trust of mobile users, Luarn et al. [140] investigated the direct effects of self-efficacy on the behavioral intention. Among commonly included constructs in the TAM, self-efficacy was found to have a positive effect on the intention to use mobile banking services. Likewise, self-efficacy appears to have an impact on non-users. Jeong and Yoon [113] investigated the adoption behaviors of both users and non-users of mobile banking and identified self-efficacy as a significant predictor of adoption for non-users.

There exists an extensive body of empirical research on crypto-asset users. Their motivations, perceptions, and behaviors have been investigated in both qualitative and quantitative studies. However, contrary to the extensive research body on mobile banking, studies uncovering the reasons for or against the use of crypto-assets are scarce.

To date, motivations and reasons *against* an involvement with crypto-assets have been investigated only qualitatively. Gao et al. [73] interviewed non-users of bitcoin and found that perceived low self-efficacy associated with the use of bitcoin led to a decision against using it. Similarly, in the interview study presented in Chapter 3, we found that besides the low self-efficacy, non-users had little trust in crypto-assets due to the regulatory uncertainty and were concerned about risks associated with the adoption of crypto-assets. While the effect of perceived risk on the usage behavior has been empirically investigated for bitcoin users ([4]), its effect as well as the impact of trust and self-efficacy on the adoption intention of non-users have not been studied thus far.

It also remains unknown how non-users differ from users. While prior qualitative work has focused on the perceptions of both users and non-users ([73, 216]), no work comparing these two populations exists. Identifying differences in the key constructs may not only shed light on the previously undocumented reasons against adoption, but might further provide empirical evidence for the importance of certain constructs affecting the actual adoption behaviors, which, to the best of our knowledge, have been ignored in literature. This study therefore aims to fill these knowledge gaps.

4.2.1 Research Model

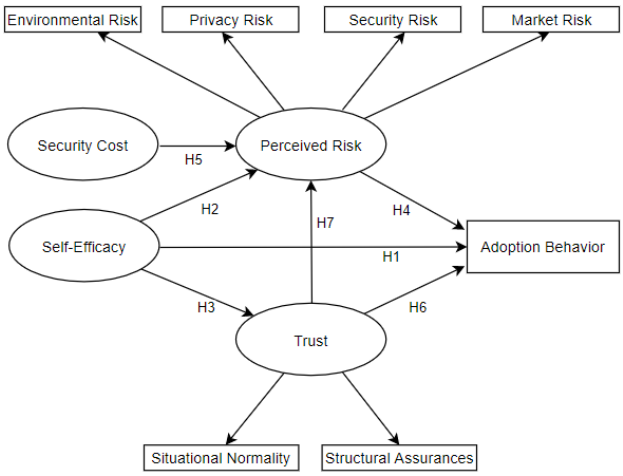


Figure 4.7: Research model

The following sections contextualize the theoretical constructs of perceived self-efficacy, trust, and risk, and reference relevant studies that show interactions between them. The hypotheses, shown in Figure 4.7, are based on prior findings in the fintech domain and qualitative studies of the populations of crypto-asset users and non-users. All items in the questionnaire were a stimulus to an unobservable latent variable and were therefore modeled as reflective.

Self-Efficacy

The effect of self-efficacy is well-documented in the fintech domain, both for online [8, 149] and mobile banking [113, 140, 228]. Exploratory qualitative studies have investigated its effect on both users and non-users of bitcoin and other crypto-assets. Gao et al. [73]) found that non-users believed to lack required skills that would enable them to use bitcoin and cited this as their main argument against an involvement. The users, on the other hand, were familiar with the ecosystem, knew the tools, and believed to understand the underlying technology well-enough to be comfortable to use it. These findings lead to our first hypothesis:

H1: The perceived self-efficacy has a positive effect on the non-users' inten-

tion to adopt crypto-assets.

Perceived self-efficacy was also shown to have an effect on both risk and trust. In the study of consumers' purchase intentions in e-commerce [121], the authors found that self-efficacy had a significant positive effect on trust, while also reducing the perceived risk. Zhou [228] confirmed the positive effect of self-efficacy on the initial trust formation for users of mobile banking as well.

In the context of crypto-assets, the interactions between these constructs were not investigated so far. Following the empirical results in related domains, we believe that similar effects might exist in the crypto-asset context:

> **H2:** The perceived self-efficacy has a negative effect on the non-users' perceived risk associated with crypto-assets.

> **H3:** The perceived self-efficacy has a positive effect on non-users' trust towards crypto-assets.

Perceived Risk

Perceived risk negatively affects users' intention to engage in online transactions. Its negative effect has been shown for e-commerce [40, 121, 184], Internet [151, 189] and mobile banking [7, 134, 141, 147]. These findings imply that consumers with high risk concerns are less likely to adopt the respective technology.

Overall, there exists a substantial number of risks that are associated with crypto-assets. Besides the possible attack vectors compromising the distributed ledger [28], self-errors [194, 216] and shutdowns of third-party services [159] such as exchanges are known to be prevalent and could lead to irreversible monetary losses. These and other risks have been documented in the crypto-asset literature [26, 79, 122], with Kiran and Stanett [122] suggesting a grouping into *social*, *legal*, *economic*, *technological*, and *security risks*.

Abramova and Böhme [4] were the first to shed light on the effect of the perceived risk on the behavior of bitcoin users. In their study, risk was considered as a multi-faceted construct, and included the legal, operational, adoption, and financial risks. The authors found that the perceived risk was a strongly significant indicator that negatively influenced the participants' willingness to transact with bitcoins.

The effect of risk on non-users has been only the object of qualitative studies thus far. Non-users were concerned about security vulnerabilities of crypto-assets, exchanges, tools, legal uncertainty, as well as privacy [216]. Another prevalent theme was the negative stigma surrounding crypto-assets. Non-users believed that crypto-assets were exploited for illicit activities, such as the drug trade, and viewed an involvement unsafe as they preferred not to be associated with such behaviors.

Similar to Abramova and Böhme [4], we consider the *perceived risk* as one's perception of the uncertainty and negative consequences associated with the adoption of crypto-assets, albeit from a non-user's perspective. Based on prior findings for both mobile banking [141] and crypto-assets [4, 216], we hypothesize the following:

> **H4:** The perceived risk associated with crypto-assets negatively affects non-users' adoption intention.

Security Cost

Prior qualitative studies have shown that both users and non-users of crypto-assets often find security practices complicated [71, 216]. Fröhlich et al. 2020 found that users were bothered by the secure key management and believed that a certain knowledge level is required in order to be able to successfully manage private keys. Similarly, we identified struggles of non-users related to keeping track of secure and trustworthy tools in our interview study (Section 3.3.4). Perceived security cost is closely related to the perceived security efficacy which captures an individual's belief in their ability to protect a system from threats or attacks [163]. Prior work has shown its effect on the risk perception of information system users. Nguyen and Kim [163] found a strongly significant negative effect of security efficacy on the perceived risk. Jansen [112] report similar findings for Internet banking, where the associated efficacy was found to have a negative effect on the perceived risk.

For non-users of crypto-assets, however, the associated cost of security measures is likely to have an opposite effect. Based on findings of prior interview studies [71, 216], non-users will likely perceive security measures as costly due to a lower perceived security efficacy. We believe that this assessment would lead to an increase in the perceived risk:

H5: The perceived cost of securing crypto-assets has a positive effect on the non-users' perceived risk.

Trust

In this work, we adapt the definition of trust known from prior work in the field of information systems (e.g., [74, 154]). Yet, there is debate on how accurate such definition is, such as for example by Hardin [89], who argues that literature on trust is truly about trustworthiness of a particular actor and that establishing trustworthiness itself then leads to trust. We acknowledge this, however, in order to remain consistent with regard to existing information systems literature, use "trust" throughout this chapter.

Trust was shown to be a significant predictor of technology adoption. Its positive effect for the adoption of mobile banking is well-documented [120, 134, 141]. For blockchain technology, there exists work conceptualizing trust (e.g., [59, 217, 221]), however, the interactions between trust, its dimensions and the adoption behavior in the context of crypto-assets are largely unexplored. Sas et al. [194] interviewed 20 bitcoin users and investigated the trust determinants in three dimensions: technological, social, and institutional. One of the major findings was that due to the unregulated and pseudonymous nature of Bitcoin, the institutional trust was limited and posed a risk to the users.

During the interview study, we also identified regulatory concerns as one of the major concerns of non-users that led to a decision against using crypto-assets (Section 3.3.3). Based on these findings, we investigate the effect of institutional trust on the intention to adopt crypto-assets. While other dimensions of trust can be found in literature [139, 207], we take a pragmatic perspective and focus on institutional trust, as we were able to provide first empirical evidence for its effect on non-adopters (Section 3.3.6).

Since institutional trust is multi-faceted, we consider its several dimensions. According to Gefen et al. [74], there exist two institution-based first-order constructs: *situational normality*, i.e., the perceived normality of a situation or a transaction in the context of crypto-assets, as well as *structual assurances*, i.e., existing safety nets that include guarantees and regulations. Yousafzai et al. [227] found that

both structural assurances and situational normality increased the participants' trust beliefs in online banks. Similar findings were also confirmed for mobile banking by Gu et al. [80], who found that both constructs significantly increased the perceived trust among users. Following these insights, we consider both constructs in our study and believe that those non-users who score higher on the latent construct of institutional trust are more likely to adopt crypto-assets.

> **H6:** Trust in crypto-assets will positively affect non-users' intention to adopt them.

Trust also has an effect on risk, as both are closely related. Das et al. [57] further suggest that both are mirror images of each other. Several scholars have investigated the effect of trust on risk and observed a negative effect. This has been shown for both e-commerce [121] and mobile banking [120, 134, 141]. For example, Luo et al. [141] showed that structural assurance has a negative effect on risk in mobile banking, implying that the belief in the institutional environment's safety leads to a reduction in the perceived risk. Thus, we hypothesize:

> **H7:** Trust in crypto-assets will negatively affect the non-users' perceived risk associated with them.

4.2.2 Research Methodology and Results

Instrument Design and Data Collection

An online survey was conducted in order to examine and test the proposed research model. The primary research objective of this work was to investigate non-users' perceptions and the factors influencing their decision not to adopt crypto-assets. Non-users did not own any crypto-assets at the point of the survey, however, had an understanding of the domain, which was a self-reported option *"No, I have never held [crypto-assets] but have some domain knowledge."*

However, we were also interested in comparing perceptions of non-adopters with those of actual users of crypto-assets. For this reason, we decided to further recruit current users. After conducting a pilot with 30 participants, both users

($N = 200$) and non-users ($N = 204$) were recruited through the commercial service provided by Qualtrics.[8] Crypto-asset ownership was predetermined by Qualtrics and both participant groups were recruited in June 2020 after the study was approved by the ethical boards of the involved institution. All participants resided in the U.S. and were over the age of 18. We used the same dataset as in the study investigating the security behaviors (see Section 4.1), however, excluded the users in the deep sample in order to reduce possible noise.

Table 4.11: Subsample demographics

Characteristic	Users	Non-Users
N	200 (100%)	204 (100%)
Gender		
Male	75.5%	37.3%
Female	24.5%	62.3%
Age		
18–24	11.5%	19.1%
25–34 years	26.5%	18.6%
35–44 years	46.5%	15.7%
45–54 years	13.0%	12.7%
55–64 years	2.5%	16.7%
65+	0.0%	17.2%
Education		
High school graduate (or an equivalent)	9.0%	25.0%
College or associate degree	9.0%	20.1%
Bachelor's degree	27.5%	33.3%
Master's degree	37.5%	14.7%
Doctorate degree	13.0%	2.9%
Other	4.0%	4.0%

[8] Qualtrics Panel: https://www.qualtrics.com/research-services/online-sample/

Measurement Model

The main objective of this study is the investigation of the adoption behaviors of crypto-asset non-users, with the dependent variable being operationalized as one's intention to purchase crypto-assets in 2020 (see *Adoption Intention* in Table 4.14). Here, a three-item nominal scale was used (*"Yes", "No", "I don't know"*).

However, as we also intended to compare non-users with current users of crypto-assets, we further tested a modified version of the model, in which the dependent binary variable is coded as the self-reported *Adoption Behavior*, i. e., whether an individual did or did not own crypto-assets at the time of the survey. The model of *Adoption Intention* depicted in Figure 4.7 is tested on data collected from the 204 non-users, whereas *Adoption Behavior* was analyzed using data from the combined sample of 404 participants.

Both models have the same risk construct, which, similar to prior work [4, 141], is modeled as multi-dimensional. As our study is the first quantitative investigation of risk perceptions of non-users of crypto-assets, we included a wide range of risks found in literature (e.g., [4, 26, 79]) in the survey and performed a separate exploratory factor analysis (with Varimax rotation) to identify the risk items that load together. For all risks, respondents were asked to rate the level of their concern on a five-point Likert scale.

Drawing upon the analysis, we differentiate between the four first-order constructs in our model: (1) *Environmental Risk (ER)* captures both regulatory and adoption uncertainty; (2) *Privacy Risk (PR)* captures the possibility of transactions being linked by parties to the individual user; (3) *Market Risk (MR)* reflects the possibility of experiencing losses due to the volatility of market prices; (4) *Security Risk (SR)* refers to potential security vulnerabilities in tools that could lead to losses. We excluded the risk items that did not load sufficiently on the first four components and considered only factor loadings that were 0.6 or higher. This cut-off is above the recommended 0.5 [85] and was used in the context of Bitcoin as well [4].

We assessed the measurement model by evaluating its internal consistency as well as convergent and discriminant validity. The composite reliability (CR) indicator was used to evaluate the internal consistency. As evident in Table 4.12,

two of our latent risk items are marginally below the suggested threshold of 0.6 for exploratory research [85]. One possible explanation is that we formed the risk constructs strictly based on the results of the exploratory factor analysis. Some risks, e. g., MR2, were phrased very broadly and could be interpreted differently by an individual respondent. However, based on the CR values of 0.58 for SR and 0.56 for MR respectively, we believe that the CR values are close enough for the constructs to be incorporated in our model.

Convergent validity was evaluated by assessing the factor loadings and the average variance extracted (AVE) [70]. The factor loadings for all indicators are above the recommended threshold of 0.5 [85]. The suggested threshold for AVE is 0.5 [70] and all constructs except for *MR* and *ER* are above this value. According to Fornell and Larcker [70], the convergent validity of items with an AVE lower than 0.5 and a CR higher than 0.6 are still considered adequate. Therefore, only MR is under the suggested threshold. The research model with *Adoption Behavior* as the dependent variable also satisfied the criteria for all constructs but MR.

Table 4.12: Reliability measures of first-order latent constructs

Item	Loading	Construct	CR	Mean	AVE	Item	Loading	Construct	CR	Mean	AVE
SE1	0.82	SE	0.87	2.41	0.68	ER1	0.72	ER	0.75	3.51	0.47
SE2	0.83					ER2	0.68				
SE3	0.80					ER3	0.62				
SE4	0.85					ER4	0.74				
SC1	0.78	SC	0.81	3.40	0.66	PR1	0.73	PR	0.79	3.33	0.61
SC2	0.88					PR2	0.81				
SC3	0.78					PR3	0.80				
SN1	0.93	SN	0.77	2.51	0.70	MR1	0.72	MR	0.57	3.81	0.45
SN2	0.74					MR2	0.61				
SA1	0.86	SA	0.88	2.70	0.78	SR1	0.65	SR	0.58	3.74	0.58
SA2	0.92					SR2	0.81				
SA3	0.87					SR3	0.82				

Lastly, we evaluated the discriminant validity of our research model. The Fornell-Larcker criterion is commonly used in literature and suggests that the square root of AVE of each construct should be greater than any of the bi-variate correlations involving the construct [85]. Table 4.13 shows that this criterion is met for all constructs, but MR, ER, and SN. The high correlation among SN and SA is

expected as both are measuring the institutional dimension of trust. We further applied the Heterotrait-Monotrait Ratio of Correlations (HTMT) criterion [98] and all our constructs were under the recommended value of 0.9. The model with *Adoption Behavior* as dependent variable satisfied this criterion for all constructs but the pair of SN-SA, where the score was marginally over 0.9. Overall, however, we believe that the discriminant validity is acceptable for both models.

Table 4.13: Fornell-Larcker criterion analysis

	SE	SC	SN	SA	ER	PR	SR	MR
SE	**0.83**							
SC	-0.06	**0.81**						
SN	0.70	0.02	**0.84**					
SA	0.75	-0.14	0.85	**0.88**				
ER	-0.41	0.29	-0.31	-0.39	**0.69**			
PR	-0.05	0.29	0.06	-0.05	0.44	**0.78**		
SR	-0.44	0.37	-0.34	-0.47	0.72	0.44	**0.76**	
MR	-0.39	0.43	-0.29	-0.45	0.67	0.26	0.70	**0.67**

We also compared the constructs between both samples in order to investigate statistical differences. The means of the indicators were compared using a two-sample t-test and the results can be found in Table 4.14.

The results of the two-sample t-tests suggest that there are significant differences between the two subsamples. Users have higher perceived *Self-Efficacy* with the differences for all four indicators being strongly significant. Similar results can also be observed for the two trust constructs. With regard to the risks, only the differences for the indicators of the *Security Risk* construct are significant.

We also questioned non-users about their specific reasons against the adoption of crypto-assets with the possibility to choose multiple options. The following Table 4.15 illustrates the responses in descending order.

Table 4.15: Reported reasons against using crypto-assets

Item	Frequency	Item	Frequency
Concern of falling victim to fraud or crime	95	Lack of regulatory support	62
Fear of possible security vulnerabilities in crypto-assets	85	Lack of incentives or use cases	42
Fear of possible security vulnerabilities in wallets	78	Negative stigma associated with crypto-assets	31
Volatile nature of crypto-assets	69	Negative experience with service providers, e. g., exchanges or wallets	17

Table 4.14: Results of two-sample t-tests between users and non-users

Question	Item	Users		Non-Users		p
		Mean	SD	Mean	SD	
How confident are you in the following skill areas in the context of crypto-assets?						
Purchasing crypto-assets.	SE1	3.88	1.11	2.51	1.16	***
Making payments with crypto-assets.	SE2	3.90	1.01	2.42	1.20	***
Explaining the difference between the private and public key.	SE3	3.68	1.10	2.22	1.20	***
Explaining the purpose of transaction fees.	SE4	3.83	1.01	2.50	1.19	***
Please indicate how costly are the following measures in terms of required time and money.						
Securing crypto-assets	SC1	3.40	1.17	3.37	0.94	n.s.
Keeping security measures for crypto-assets up-to-date	SC2	3.48	1.08	3.47	0.99	n.s.
Security investments into equipment	SC3	3.58	1.05	3.51	0.99	n.s.
Please indicate to what extent do you agree with the following statements.						
I feel confident that the technological features of crypto-assets make it safe for me to use them.	SA1	3.87	1.10	2.73	1.06	***
I feel that existing safeguards adequately protect me when using crypto-asset exchanges.	SA2	3.88	0.97	2.67	1.11	***
In general, the environment in which I can use crypto-assets is robust and safe.	SA3	3.84	1.06	2.71	1.13	***
Please indicate to what extent do you agree with the following statements.						
I feel that most crypto-asset exchanges act in their customers' best interest.	SN1	3.87	1.05	2.72	1.06	***
I feel that most merchants who accept crypto-assets act in their customers' best interest.	SN2	3.63	1.09	2.92	1.14	***
To what extent are you concerned about the following risks related to crypto-assets?						
I am concerned about						
the legal uncertainty for the users of crypto-assets and possible prosecution	ER1	3.38	1.15	3.66	1.11	*
the restricted crypto-asset usage because of regulatory involvement	ER2	3.43	1.08	3.39	0.99	n.s.
the lack of wide adoption of crypto-assets	ER3	3.50	1.14	3.51	1.12	n.s.
the lack of interoperability of crypto-assets with other services	ER4	3.42	1.08	3.50	1.05	n.s.
the traceability of transactions by governments	PR1	3.29	1.17	3.20	1.08	n.s.
the traceability of transactions by firms/private sector	PR2	3.33	1.16	3.30	1.11	n.s.
the traceability of transactions by individuals	PR3	3.42	1.14	3.38	1.18	n.s.
the theft of private keys	SR1	3.40	1.15	3.73	0.99	**
security vulnerabilities of wallets	SR2	3.52	1.10	3.73	0.96	*
security vulnerabilities of exchanges	SR3	3.5	1.11	3.77	1.02	*
the volatility of the market price	MR1	3.76	1.01	3.79	1.01	n.s.
I agree that the users of crypto-assets are risk-takers.	MR2	3.62	1.05	3.82	0.95	*
Are you considering purchasing crypto-assets in 2020?	AI					

Structural Model

To validate the theoretical models, structural equation models (SEM) were built using the lavaan (latent variable analysis) package [187] for the programming language R (version 4.0). The results of the analysis suggest that our models explain 25% of the variance in *Adoption Intention* and 62% of the variance in *Adoption Behavior*, respectively.

The fit of the structural models can be assessed by using a combination of fit measures. Following the suggestion of Kline [123], we report the ratio of the Chi-square value to the degrees of freedom (χ^2/df), Comparative Fit Index (CFI), Standardized Root Mean Square Residual (SRMR), and Root Mean Square Error of Approximation (RMSEA). Hu and Bentler (1999) suggest that a model is considered a good fit if the CFI is close to 0.95, SRMR – to 0.08, and RMSEA – to 0.06. There exists no consensus with regards to χ^2/df, where some suggest a value of less than 5 [150] and others considering a value between 2 and 3 as ac-

ceptable [153]. As reported in Figures 4.8 and 4.9, both our models satisfy these conditions and therefore have a reasonably good fit to the data.

The results of the structural equation model with *Adoption Intention* as the dependent variable (see Figure 4.8) suggest that several of our hypotheses are supported. *Trust* is the only construct that has a significant positive effect on *Adoption Intention* ($\beta = 0.39$, $p < 0.05$). Against our expectations, both *Perceived Risk* and *Self-Efficacy* have no significant effect on *Adoption Intention*. However, *Trust* acts as a mediator in the model: if the construct is removed, the positive effect of *Self-Efficacy* on *Adoption Intention* becomes strongly significant ($\beta = 0.49$, $p < 0.001$). *Self-Efficacy* has a significant positive effect on *Trust* ($\beta = 0.77$, $p < 0.001$), and *Trust* has a significant negative effect on *Perceived Risk* ($\beta = -0.25$, $p < 0.05$). Lastly, *Security Cost* is found to have a strongly significant positive effect on *Perceived Risk* ($\beta = 0.40$, $p < 0.001$). For the second structural model (Figure 4.9), only the positive effect of *Self-Efficacy* on *Adoption Behavior* is significant ($\beta = 0.75$, $p < 0.001$). *Self-Efficacy* further has a significant positive effect on *Trust* ($\beta = 0.90$, $p < 0.001$), whereas *Security Cost* has a significant positive effect on *Perceived Risk* ($\beta = 0.44$, $p < 0.001$).

We validated the results by running the analysis using PLS-SEM (SmartPLS). Both approaches produced comparable results, with PLS-SEM even identifying a significant effect of trust on adoption behavior, which is not the case for CB-SEM (see Figure 4.9). CB-SEM is further the more critical test [16] and our results and conclusions are therefore more conservative.

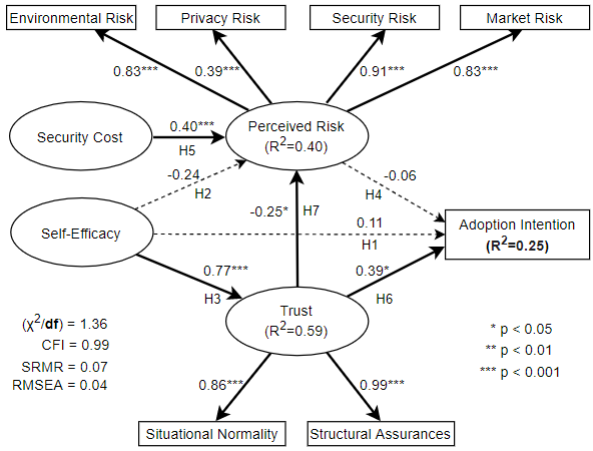


Figure 4.8: Results of the structural equation model with adoption intention as dependent variable (non-users only, $N = 204$)

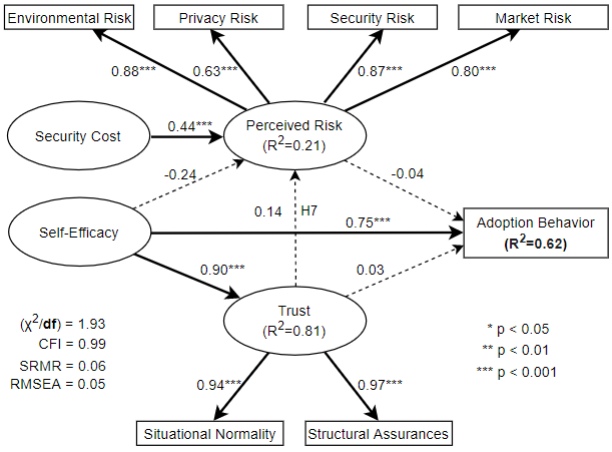


Figure 4.9: Results of the structural equation model with adoption behavior as dependent variable (combined sample, $N = 404$)

4.2.3 Discussion

Theoretical Implications

There only exists limited work that investigated interactions between the examined theoretical constructs in the context of crypto-assets. Abramova and Böhme [4]

were the first to apply a variation of the TAM on bitcoin users and found that perceived benefit and perceived ease of use had a positive effect on usage behavior, while perceived risk had a negative effect. Arias-Oliva et al. [15] employed a variation of the UTAUT and found performance expectancy and facilitating conditions to be significant predictors of behavioral intention. Based on the findings of prior work, the theoretical model in this study sheds light on the effects of trust, self-efficacy, and risk on the non-user's intention to adopt crypto-assets.

Thus far, non-users of crypto-assets have only been the subject of qualitative studies. Against this backdrop, our work provides the first empirical analysis of the factors influencing the adoption intention. Contrary to our original expectations, only *Trust* has a direct significant effect on *Adoption Intention*. Therefore, we are not able to confirm prior qualitative findings that suggest an effect of risk and self-efficacy [73, 216]. Yet, interestingly, *Self-Efficacy* has an indirect effect on *Adoption Intention*, suggesting that those participants who have higher perceived self-efficacy also score higher on the trust construct and hence, are more likely to adopt crypto-assets.

The importance of *Self-Efficacy* is even more evident in the second model (Figure 4.9), where *Self-Efficacy* has a strongly significant effect on *Adoption Behavior*. A reason for the different observations could be that non-users have difficulties in assessing their self-efficacy accurately, particularly if they only have limited knowledge. In this case, institutional trust acts as a full mediator.

We cannot confirm the negative effect of *Perceived Risk* on neither *Adoption Intention* nor *Adoption Behavior*. This finding is in stark contrast to prior work on crypto-assets [194, 216] and also other domains, such as mobile banking (e.g., [141]), where perceived risk was found to have a negative effect on the adoption behaviors. This is corroborated through the comparison of the first order risk constructs which did not yield a consistent picture. It appears that other constructs play a more vital role in technology adoption among informed non-adopters, such as *Self-Efficacy*, *Situational Normality*, and *Structural Assurances*, where the user subsample in our study scored significantly higher. These insights were only made possible through the investigation of both the user and non-user subsamples and we therefore believe that in order to understand the intricacies of technology adoption, one needs to go beyond the intention to adopt as it only provides a partial picture.

With regard to the different risks in the crypto-asset domain, *Security Risk* has the highest path coefficient. This matches the self-reported reasons of non-users for which they decided against adoption. The three most frequent reasons were all related to either falling victim to crime or software vulnerabilities (see Table 4.15), followed by the lack of regulatory support or the volatile nature, which are commonly reported in prior work [178, 218]. Overall, we conjecture that both users and informed non-users are aware of the most common risks, which explains the insignificant effect on both adoption intention and behavior. This is plausible as the adoption of crypto-assets itself does not pose any direct personal harm or financial loss on individuals, as opposed to the actual usage, which has been shown to be affected negatively by risk [4].

We also confirm the effects of *Trust* and *Security Cost* on *Perceived Risk* in the context of crypto-assets. Trust can therefore act as an important factor that can be leveraged to reduce the overall perceived risk. Lastly, *Security Cost* is also found to be a strongly significant predictor of *Perceived Risk*. This is not surprising, as poor user experience (UX) of crypto-asset tools, such as exchanges and wallets, is well-known and reported in literature [71, 194].

Crypto-asset users, however, are not necessarily confronted with those UX challenges. This is particularly true in the case of crypto-asset exchanges, which provide an abstraction layer and allow users to own crypto-assets without having to deal with the private key management and therefore the actual technology. Crypto-assets therefore show the limits of the traditional understanding of technology adoption as it is unclear whether one can truly speak of adoption in cases in which users are merely interacting on an abstraction layer and not with the technology itself. More work is needed in order to operationalize technology adoption in the context of crypto-assets.

Practical Implications

This study has several important implications for actors in the crypto-asset domain, such as regulators, blockchain start-ups, and tool developers. *Trust* was the only significant direct predictor of *Adoption Intention*, suggesting that participants who have more trust in the ecosystem surrounding crypto-assets are more likely to

adopt them. Improving both the *Situational Normality* and *Structural Assurances* could therefore have a positive effect on a participant's willingness to adopt crypto-assets. Situational normality is the degree to which a situation appears normal or customary [74]. Following our results, providers of crypto-asset services should try mimicking online banking or conventional payment systems that non-users are already familiar with. Attaining situational normality could also be achieved by introducing stable crypto-assets, so-called stable coins, to non-users, which, in turn, increase their trust due to the similarities to fiat currencies. Trust, however, could also be increased by providing more structural assurances that would protect potential newcomers. Regulatory uncertainty is often associated with crypto-assets and attracts malicious actors, such as exchanges that might disappear with users' funds [159] or fraudulent Initial Coin Offerings (ICOs) [47]. Non-users feel unsafe in such environment and need additional signals of trust. In e-commerce, trustworthiness is often signaled through trust badges, which could be introduced for operators of exchanges in this domain. These badges, however, have to be costly or hard to fake in order to avoid exploits by fraudulent parties [183]. Alternatively, similar to traditional banking, deposit insurances (e. g., by the Federal Deposit Insurance Corporation) could provide safety nets in the case of exchanges. However, crypto-asset deposits, contrary to the US dollar, are not yet insured, which calls for further regulatory involvement in order to facilitate adoption.

The results of the structural models have shown that *Self-Efficacy* has a significant positive effect on *Trust* and *Adoption Behavior*. Managerial attention should be therefore focused on the attainment of self-efficacy, which could be achieved in various ways. For example, training sessions could be used to let newcomers familiarize themselves with the terminology and technology prior to an actual engagement.

Better tool support could also increase self-efficacy among non-users. Prior work has identified challenges of crypto-asset tools, including, but not limited to, complex metaphors, wording, and a lack of guidance [66], which all lead to a poor overall UX. Understanding how to design usable crypto-asset tools is an open research topic and better tools could lead to an increase in trust, which in turn, could positively influence both *Adoption Intention* and *Adoption Behavior*.

4.2.4 Limitations

This work has limitations that are commonly found in empirical studies in general. Clearly, the results of this study are not generalizable to the entire population of informed non-users. Further, over 60% of the non-user sample are females, who, as prior research has shown, usually perceive their technological skills lower than males [90]. Therefore, it is possible that the scores on the construct of self-efficacy could change in a more balanced sample.

With regard to internal validity, some of the constructs in our measurement model do not meet all the recommended thresholds found in literature. This work is the first quantitative analysis of crypto-asset non-users and the measurement reliability could be significantly improved. The differences between users and non-users need to be closely observed and more research needs to be conducted in order to understand how well non-users understand the associated risks and what severity they associate with them.

In this work, we only explore the institutional dimension of trust. Its importance was shown in prior qualitative work [194, 216], however, other dimensions of trust, to the best of our knowledge, are left unexplored. Other trust constructs, including, but not limited to, *Dispositional Trust* [207], *Propensity to Trust* [155], and different *Trusting Bases* [137] have been shown to have an effect and could therefore also influence one's decision concerning the crypto-asset adoption.

The model could also potentially be improved by including constructs such as risk tolerance. In both our interview study (Chapter 3) we found that users have distinct risk profiles and this was also confirmed through the cluster analysis (Section 4.1). We did not include items exploring the risk tolerance of the respondents in the context of crypto-assets due to the length of the questionnaire, but believe that a financial risk tolerance instrument [77, 78] could provide a more nuanced understanding of the heterogeneous user population.

Lastly, all data was collected from participants residing in the U.S. Thus far, to the best of our knowledge, there exists no work highlighting the differences in crypto-asset usage behavior between countries. However, based on prior evidence suggesting that the cultural values play a role in technology acceptance [197], we believe that similar patterns might exist in the context of crypto-assets.

4.2.5 Conclusion

This study is the first empirical investigation of factors influencing the adoption behavior among non-users of crypto-assets. Drawing upon the results of the literature review, we have derived a theoretical model that explains the interactions between trust, self-efficacy, risk, and adoption intention.

Our results have showed a significant positive effect of trust on the adoption intention, and have further confirmed the interaction effects between the aforementioned constructs. We have provided recommendations on how to increase both self-efficacy and trust of non-users in order to lower the entry barriers and make the domain of crypto-assets more inclusive.

Chapter 5

Exploring the User Experience with Crypto-Asset Tools

In our interview study, we identified UX issues of crypto-asset tools to be a burden for its users. However, due to the small sample size, we were able to only uncover a small number of issues. To address this shortcoming, we conducted a mixed-methods research study on over 45,000 app reviews and report on the findings in the following. This chapter begins with an overview of the background and related work on crypto-assets and review analysis (Section 5.1). Next, we describe the methodology in Section 5.2 and results in Section 5.3. We conclude with a discussion of our findings and design implications that could be incorporated in future wallets (Section 5.4).

5.1 Background and Related Work

5.1.1 UX and Crypto-Assets

Crypto-asset users are known to struggle with the management of cryptographic keys. Studies have shown that users have inadequate mental models of the underlying cryptography [73, 146] and often employ poor security practices leading to

dangerous errors and, in the worst case, monetary losses [71, 126, 216].

Dangerous errors, however, can also occur as a result of poor wallet UX. Eskandari et al. [66] conducted the first and only usability study of crypto-asset wallets. Through a series of cognitive walkthroughs of six bitcoin wallets, the authors identified issues that could potentially affect users, including, but not limited to, complex metaphors, highly technical terminology, and a general lack of guidance. Due to the nature of the study, however, it remains unclear what effects such issues have on the UX.

Our contribution is twofold. Firstly, in a large body of app reviews of mobile wallets, we identify and categorize UX issues, and assess their severity and prevalence. Secondly, guided by the call for blockchain design patterns in the work of Elsden et al. [64], we propose design recommendations that address the identified issues. These recommendations can inform future design of wallets and can potentially contribute to an enhanced UX in the domain.

5.1.2 Review Analysis

App reviews provide rich, contextual information about an app as perceived by its users. Such information can include feature requests, bug reports, and functional error reports [84, 119], which, when analyzed, can help improve the app. Due to the sheer number of reviews, however, this analysis can become very tedious.

To reduce this burden, automated classification approaches have been proposed by scholars. Here, ML and NLP techniques were successfully applied to retrieve informative reviews related to general app maintenance [38], user feedback [81, 83], and UX [17, 96, 142, 152, 170]. For example, Hedegaard and Simonsen [96] proposed an approach to automatically classify reviews based on the dimensions of usability and user experience (UUX) found in literature. Results suggest that close to half of the reviews included information related to UUX, some of which could be used to improve the apps. Inspired by the previous work, we employ a combination of ML and NLP techniques to identify reviews that contain information about the UX in the context of crypto-assets. It needs to be emphasized that the classification approach presented in this chapter is not a contribution to the field of review classification, but merely serves as an intermediary step. In

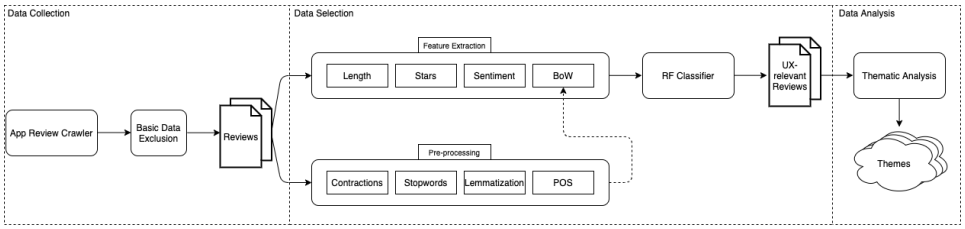


Figure 5.1: Overview of the data collection, selection, and analysis approach (POS = part of speech, BoW = bag of words, RF = random forests)

our case, these techniques are used to narrow down the review corpus to a humanly manageable size, which can then be analyzed qualitatively.

5.2 Methodology

We used a three-stage approach (see Figure 5.1) to investigate the shortcomings of crypto-asset wallets as perceived by the users. For data collection, we built a crawler to generate a list of reviews (and their metadata) from both the Apple App Store and Google Play Store. As review data is noisy [152] and only a subset of reviews is relevant to UX [96, 168], we decided to automate this selection process by using a combination of heuristics and an ML classifier. Lastly, we performed qualitative analysis of the subset of the reviews selected during the second stage. This third stage allowed us to provide a rich, contextual, in-depth analysis of the data. In the following sections, we describe each stage in detail.

5.2.1 Data Collection

App Selection

There exist two options when it comes to managing crypto-assets: custodial and non-custodial wallets. The latter allow its users to manage the cryptographic keys themselves, which, as prior work has found [71, 194, 216], users often struggle with. To investigate the underlying reasons for these struggles, we focused on non-custodial wallets and excluded custodial options, i.e., apps that only serve as an

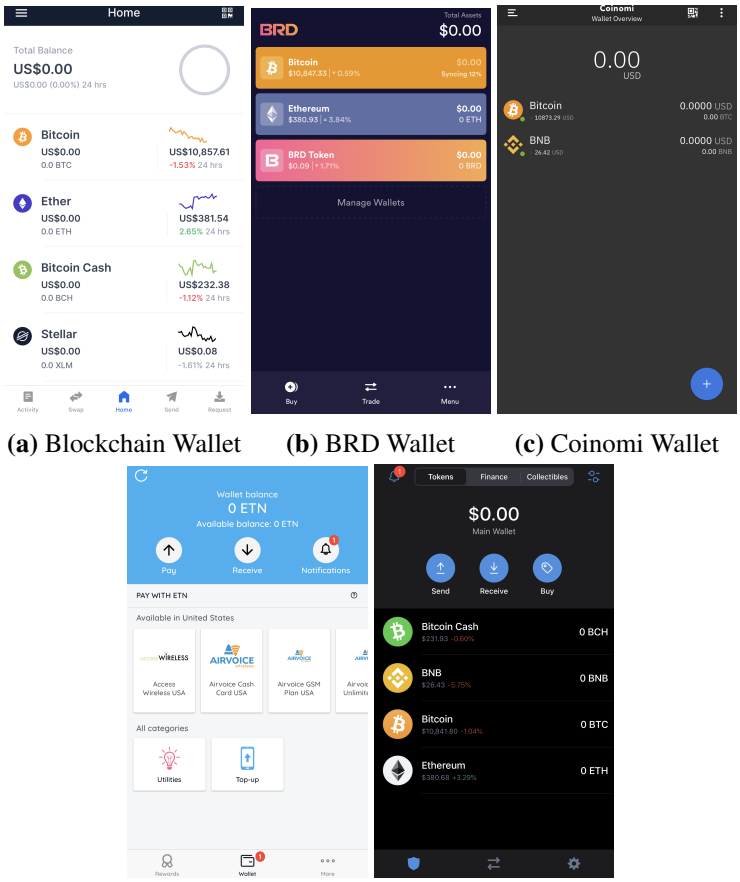
interface to a crypto-asset exchange, such as Coinbase[1] or Binance.[2] In particular, we decided to investigate mobile wallets, as we found them to be the second-most-popular wallet type in the survey study presented in Chapter 4, after desktop wallets, where reviews are scarce or non-existent.

The number of available mobile wallets, however, is overwhelming. In the Google Play Store alone, there are over 250 different apps with tens of thousands of reviews, which make it infeasible to analyze them manually, even after selecting only UX-relevant reviews. Therefore, we selected the top five mobile wallets in the Google Play Store, with the most reviews as of April 2020: Blockchain Wallet,[3] Trust Crypto Wallet,[4] Electroneum,[5] Coinomi Wallet,[6] and BRD Bitcoin Wallet.[7] We then selected the same applications and their corresponding reviews in the Apple App Store. Four of the top five wallets on Android were also among the top five wallets on iOS. The selected mobile wallets support a variety of different crypto-assets, such as bitcoin, Ether, and various tokens, and we believe that insights gained from analyzing these reviews will be transferable to other types of software wallets. Figure 5.2 depicts all the mobile wallets that were selected in this study.

Review Crawler

Similar to prior work [65, 215], we implemented a custom crawler that collected review data for a given app from both the Apple App and Google Play stores. The software adhered to the "ethical crawling" framework [208] by only downloading data from websites that permitted crawling according to the site *robots.txt* file, and by reducing the number of requests to minimize website traffic and prevent exorbitant operator costs. Besides reviews for any given application, the crawler also retrieved metadata associated with every collected review. This metadata includes the rating of the review, the date it was posted, and store-specific information in-

[1] Coinbase: www.coinbase.com
[2] Binance: www.binance.com
[3] Blockchain Wallet: https://www.blockchain.com/wallet
[4] Trust Crypto Wallet: https://trustwallet.com/
[5] Electroneum: https://electroneum.com/
[6] Coinomi Wallet: https://www.coinomi.com/en/
[7] BRD Bitcoin Wallet: https://brd.com/



(a) Blockchain Wallet **(b)** BRD Wallet **(c)** Coinomi Wallet

(d) Electroneum **(e)** Trust Wallet

Figure 5.2: User interfaces of current versions of the selected mobile wallets

cluding the number of times a review was rated as helpful in the Google Play Store and the review title in the Apple App Store. Overall, we collected 45,821 reviews for the five chosen mobile wallets.

Basic Data Exclusion

As with app reviews in general, our dataset had noisy data that reduced the overall quality [35, 83]. Guzman and Maalej [83] suggest that short reviews are often non-informative and might only include praise or dispraise. To improve the overall quality of our data set (similarly to McIlroy et al. [152]), we excluded those reviews

that had only three or fewer words.

While we only crawled reviews from the English versions of the Apple and Google Stores, some reviews turned out to be not written in English. To further reduce possible noise, we used the Google Cloud Translate API[8] to identify non-English reviews. We also excluded these from the final corpus. This reduced the review corpus further, to 26,109.

5.2.2 Data Selection

Prior work has shown that only a subset of all reviews is relevant to UX. The number of relevant reviews, however, can range and depends on the platform and application area. For example, Hedegaard and Simonsen [96] analyzed reviews on a dedicated review site epinions.com and found that up to 49% of all reviews contain information relevant to UX. A study of reviews in the App Store [168], on the other hand, only classified one-third as related to UX.

While these numbers differ significantly, they both suggest that only some reviews seem to be relevant to UX, whereas others are not. Therefore, our goal was to identify such relevant reviews for manual analysis from the selected corpus of 26,109 reviews. To assess how many reviews are relevant in our corpus, we manually labeled a random sample of 1,000 and found that only 37.5% of reviews were relevant to UX. Because of the high rate of irrelevant reviews, we sought ways to focus our efforts on analyzing relevant samples. To this end, we employed a combination of NLP and ML techniques and used the 1,000 reviews as a training set (Section 5.2.2). The following subsections explain our automated classification approach for the identification of UX-relevant reviews.

Pre-processing

Prior to building our machine learning model, the review corpus had to be pre-processed in order to further reduce noise. As a first step, we *expanded contractions* in each review, e.g., "isn't" was expanded to "is not" and "doesn't" to "does not". The app reviews in our corpus also included emoticons, numbers, and other symbols which were also all removed during pre-processing. These step allowed

[8] Google Cloud Translate: https://cloud.google.com/translate

Table 5.1: Features of a review

Raw Review	Pre-processed Review	Character Count	Rating	Sentiments
Horrible app! I haven't received my bitcoin money after a month of purchasing it. I emailed Blockchain and no one has gotten back to me yet. $200 down the drain! Thanks for nothing!	['horrible', 'receive', 'money', 'month', 'purchase', 'email', 'drain', 'thanks']	49	1	*neg* : 0.18 *neu* : 0.74 *pos* : 0.08 *compound* : −0.5684

Table 5.2: Examples of tagged reviews

Class	Review Text	Explanation
Relevant to Crypto-Asset UX	Takes at least 3 hours for the bitcoins to arrive in my bread wallet	User mentions dissatisfaction with bitcoin transactions being slow.
Relevant to General UX	The application does not open after upgrade! iPad Air 2 iOS 8.4	This review is not specific to crypto-asset wallets, but to apps in general.
Irrelevant to UX	The future of crypto instant payment!	No relevance to the app or UX.

us to reduce the vocabulary size and further made it easier to remove stopwords.

Stopwords are common words that rarely add any meaningful information. Such words include articles, pronouns, and prepositions. We used the stopword list from the gensim [9] package and expanded the list by adding words that are specific to our context, including the names of the apps as well as words such as "exchange" and "blockchain". Further, since our classification approach was intended to be cryptocurrency-agnostic, we also excluded names and abbreviations of cryptocurrencies. To accomplish this, we retrieved the top 3,500 cryptocurren-

[9]Gensim Package: https://radimrehurek.com/gensim/

Table 5.3: Number of classified/analyzed reviews per wallet and platform. Numbers from the training set are in parentheses.

	Automatically Classified Reviews			Analyzed Reviews		
	Play Store	App Store	Wallet Total	Play Store	App Store	Wallet Total
Blockchain Wallet	2,309	257	2,566	353 *(56)*	344 *(87)*	697 *(143)*
Electroneum	1,659	26	1,685	329 *(32)*	35 *(9)*	364 *(41)*
Coinomi Wallet	1,001	23	1,024	327 *(30)*	31 *(8)*	358 *(38)*
Trust Crypto Wallet	468	59	527	310 *(13)*	79 *(20)*	389 *(33)*
BRD Bitcoin Wallet	385	297	682	314 *(17)*	400 *(103)*	714 *(120)*
Store Total	5,822	662	6,484	1,633 *(148)*	889 *(227)*	2,522 *(375)*

cies and abbreviations through the Coingecko API [10] and treated these tuples the same way as stopwords. Words such as "bitcoin", "btc", "ethereum", and "eth" were all excluded in this step.

Next, we tokenized the filtered reviews and tagged every word according to its *part of speech (POS)*. For both steps, we used the Natural Language Toolkit (NLTK) [11] and only included nouns, verbs, adjectives, and adverbs. Based on these tags, we then *lemmatized* each word to reduce different forms of the same word to a common basic lemma. For example, the words "sending" and "sent" are reduced to the same term "send". This again lowers the number of overall words or features in our processed text corpus. An example in Table 5.1 shows a review before and after pre-processing.

Feature Selection

Similar to past studies on review classification [83, 96, 142, 162], we use the *bag-of-words* (BoW) model to represent the reviews. In BoW, all unique words in the text corpus are being added to a vocabulary and each document (= review) is being represented as a vector. This vector contains the word occurrences for the respective document and the length of this vector is equal to the vocabulary size [148]. We further employ the term frequency - inverse document frequency (TFIDF) as the weighting scheme, which decreases the weight of words that occur frequently in many documents, and increases the weight of words that occur frequently in a single document. In other words, TFIDF tries to capture the importance of a par-

[10] Coingecko: https://www.coingecko.com/en/api
[11] NLTK: https://www.nltk.org/

ticular word in a corpus by taking its occurrences per document into account. For each word *i*, the weight can be written as follows [148]:

$$weight(i,j) = \begin{cases} (1 + log(tf_{i,j}))log\frac{N}{df_i} & \text{if } tf_{i,j} \geq 1 \\ 0 & \text{if } tf_{i,j} = 0 \end{cases} \tag{5.1}$$

Where:

- $tf_{i,j}$: is the number of occurrences of the word *i* in document *j*
- N: is the number of overall documents
- df_j: is the number of documents that word *i* occurs in

According to the equation above, a word that occurred in only one document would get the full weight, whereas a word that occurred in all documents would get the weight 0 ($log N - log\, df_j = log N - log N = 0$). Words that appear only once in the whole corpus might however be misspellings and we therefore disregard such words. Moreover, we also exclude words that appear in more than 10% of the documents in order to eliminate very common words.

Occurrences of word sequences, instead of single words, can also be used as features. One commonly used approach in text classification are character [81, 162] and word [96, 142] *n-grams*. An n-gram feature is a sequence of n words or characters that commonly appear together. We have both experimented with character and word n-grams and word bi- and trigrams ($n = 2,3$) have yielded the best results. For example, some occurring n-grams in our corpus are *"zero balance"*, *"waste time money"* , and *"wallet scam"*.

Besides only taking the bag of words for each review, we have also included metadata in the classification approach. Past research has shown that the *rating* can indicate the type of information that is present in a particular review. For example, bug reports often have a lower rating, whereas user experiences are often found in higher rated reviews [168]. The *length* of a review can also be indicative of the data quality, with longer reviews being more informative than shorter ones [168]. Inspired by the findings in [168], we have therefore included both the rating (1 to 5) as well as the length of each review in characters.

Lastly, we also consider the associated sentiment for each review as a feature. Ratings and sentiments are closely related, however, the latter can provide more fine-grained information than a five-point scale. Prior work has also shown that sentiment scores can be effectively used to classify reviews containing UX information [83, 142]. In our approach, we employ VADER (Valence Aware Dictionary for Sentiment Reasoning) [103], a sentiment analysis tool created for social media text. The text on social media is often short and sparse, which also holds true in the case of app reviews.

VADER is a rule-based sentiment lexicon that includes information on both the polarity and intensity of sentiments. It takes the word order of texts into account as well as acronyms, slang terms, and emoticons. Each text is assigned a *positive*, *neutral*, and *negative* scores, who combined add up to 1. Moreover, these values can be also represented as the *compound* score, which is computed by summing up the scores for each word and then normalizing it to be in the interval from -1 (most negative) to +1 (most positive). For example, the review in Table 5.1 is assigned the following values: `'neg': 0.162, 'neu': 0.656, 'pos': 0.182, 'compound': -0.7141`. This particular review has therefore a very negative associated sentiment. A compound score between -1 and -0.05 indicates a negative sentiment, a score higher than -0.05 and lower than 0.05 a neutral sentiment, and a score between 0.05 and 1 indicates a positive sentiment [103]. We have both experimented with one (compound) and two sentiment scores (positive and negative) and present the results in Section 5.2.2.

Training Set

After defining the feature set, we proceeded with training the classifier. We randomly selected 1,000 reviews (500 for Android and 500 for iOS) from the set of 26,109 and manually classified them based on their relevance to UX. To ensure consistency, two researchers independently classified the 1,000 reviews and followed a coding guide (Appendix C.1) throughout the process. UX relevance was assessed based on definitions used in prior work [3, 91, 100, 109, 175] and a review was considered relevant only if it contained information about perceptions and experiences unique to wallets (and its features) or characteristics of crypto-

assets. During the manual classification process, we classified the reviews into three groups: *relevant to crypto-asset UX*, *relevant to general UX*, and *irrelevant to UX*.

We followed an iterative approach when manually classifying the 1,000 reviews. We split the reviews into three sets ($n_1 = 300, n_2 = 300, n_3 = 400$) and classified each set independently. After each set, Cohen's kappa was calculated to assess the inter-rater reliability (IRR) and disagreements, which were caused by the different levels of familiarity of the coders with crypto-assets and crypto wallets, were discussed and resolved. For n_1, IRR was $\kappa = 0.61$, for n_2, we achieved $\kappa = 0.62$, and for n_3, a value of $\kappa = 0.65$. All of these values indicate a substantial agreement among coders [132]. Table 5.2 shows examples of the three kinds of reviews that we encountered during the process.

The manual classification occurred on a review-based level, meaning that if a review had parts that were both relevant and irrelevant, it was classified as relevant. This classification is coarse; however, it was acceptable in our case, as it is only an intermediate step in our approach. This coarse classification might also be the reason for the high percentage of reviews classified as relevant to UX. Out of the 1,000 reviews, we classified 375 as *relevant to crypto-asset UX*, 557 as *relevant to general UX*, and 68 as *irrelevant to UX*. For our study, we were only interested in the UX issues particular to mobile wallets, and we therefore considered reviews containing only general UX comments as irrelevant. Overall, we manually classified 375 reviews as relevant to mobile wallet UX and the rest (625) as irrelevant. Cohen's kappa for these two classes of reviews was $\kappa = 0.69$.

Machine Learning Model

After finalizing the training set, a machine learning model had to be selected. There exist various models that have been successfully applied in the context of text classification, with some performing well for short text, such as reviews. Pranckevičius and Marcinkevičius [177] compared several classifiers and found that Logistic Regression (LR) outperformed models such as Support Vector Machines (SVM), Naive Bayes (NB), and Random Forests (RF). We have experimented with various models for binary classification (relevant vs irrelevant reviews) and report on

our findings for the three best performing ones, namely LR, SVM, and RF. We use *precision*, *recall*, and *f1* to report the performance of the classifiers. Precision is calculated by dividing the number of *true positives* by the sum of the *true positives* and *false positives*, whereas recall is calculated by dividing the number of *true positives* by the sum of *true positives* and *false negatives*. The f1 score is the harmonic mean of precision and recall. The following table presents the results of the top tree performing classifiers when trained using different feature combinations. We have adjusted the class weights inversely proportional to the class frequencies to account for the imbalance in the training set. The following values were the mean results of a 10-fold cross-validation.

Feature Combination	LR			SVM			RF		
	Precision	Recall	F1	Precision	Recall	F1	Precision	Recall	F1
BoW	0.82	0.54	0.65	0.77	0.67	0.72	0.8	0.69	0.74
BoW + 2 sentiments	0.74	0.61	0.67	0.74	0.67	0.7	0.8	0.72	0.76
BoW + 1 sentiment	0.77	0.55	0.64	0.76	0.66	0.71	0.79	0.69	0.74
BoW + 2 sentiments + metadata	0.78	0.63	0.7	0.76	0.7	0.73	0.79	0.78	0.78
BoW + 1 sentiment + metadata	0.78	0.60	0.68	0.77	0.7	0.73	**0.8**	**0.76**	**0.78**

Table 5.4: Accuracy of the classification depending on model and features

The combination of sentiment scores, BoW model, and metadata (length + rating) had an f1 score of 0.78 for the positive class (relevant UX reviews) and is comparable to prior work on binary classification of reviews relevant to UX [83, 96, 142].

Validation

We have also evaluated the performance of our binary classifier by measuring the area under the curve (AUC) for the receiver operating characteristic (ROC) [88]. The ROC curve is not sensitive to imbalanced data [93] and is therefore appropriate for evaluating our classification approach. A perfect classifier would have a corresponding AUC-ROC value of 1, whereas a binary classifier that operates by chance would have a value of 0.5. When we performed a 10-fold cross validation, our classifier achieved a mean AUC value of 0.90, which, according to Hosmer et al. [101], is indicative of an outstanding discrimination. The ROC curves can be found in Figure 5.3.

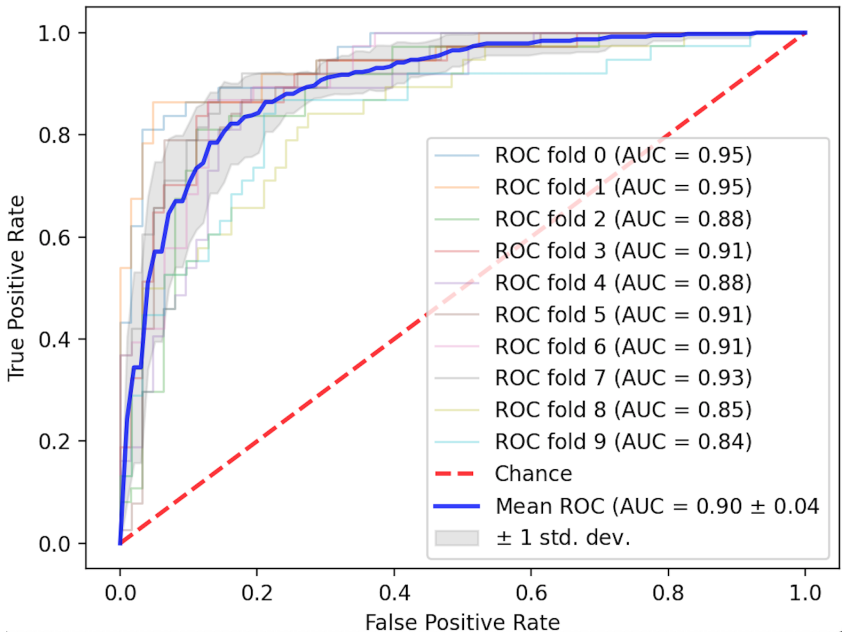


Figure 5.3: ROC curves of the 10-fold cross validation of our classification approach

We have also evaluated the performance of our binary classifier by plotting the area under the curve (AUC) for the receiver operating characteristic (ROC) [88]. The ROC curve is not sensitive to imbalanced data [93] and is therefore appropriate for evaluating our classification approach. A perfect classifier would have a corresponding AUC-ROC value of 1, whereas a classifier that operates by chance would have a value of 0.5. We apply a 10-fold cross validation and achieve a mean AUC value of 0.90, which is indicative of an outstanding discrimination [101].

5.2.3 Data Analysis

The final step in our approach was the qualitative analysis. From the 25,109 reviews, our classifier identified 6,484 (25.8%) as relevant to mobile wallet UX (see Table 5.3). Combined with the 375 relevant reviews from the training set, the overall number was 6,859. Similar to the Thematic Analysis approach described by Guest et al. [82], the lead analyst created an initial codebook. In our case, this resulted in 121 codes from the 375 relevant reviews of the training set.

We followed an iterative coding approach with two researchers. We selected the wallet with the lowest number of relevant reviews and randomly sampled the same number from each other wallet. As such, we selected 230 reviews ($10 * 23$ (# reviews for Coinomi iOS) $= 230$), and split them randomly between the two analysts. These reviews were split into equal-sized batches and were coded sequentially, i.e., one analyst waited until the other finished coding and then used the updated codebook to code their batch. We have not calculated the IRR, as it is suggested that in Thematic Analysis such measures do not indicate objective coding, but merely the fact that coders are able to code in the same subjective manner [211]. Instead, after every coding round, three researchers together discussed the codes, created code groups, and identified themes. Overall, after 17 review batches, 325 codes, 26 code groups, and five themes were identified. Out of the 2,522 classified reviews that we have coded, only 64 ($\sim 2.5\%$) were coded as false positives, which again is an indicator of the high accuracy of our classifier.

We stopped the analysis once it became clear that we had reached thematic saturation [82]. This occurred after 1,285 reviews. To ensure that this was truly the case, we coded another 1,237 reviews, and while there were new codes, no new themes were identified. The saturation graph can be found in Figure 5.4.

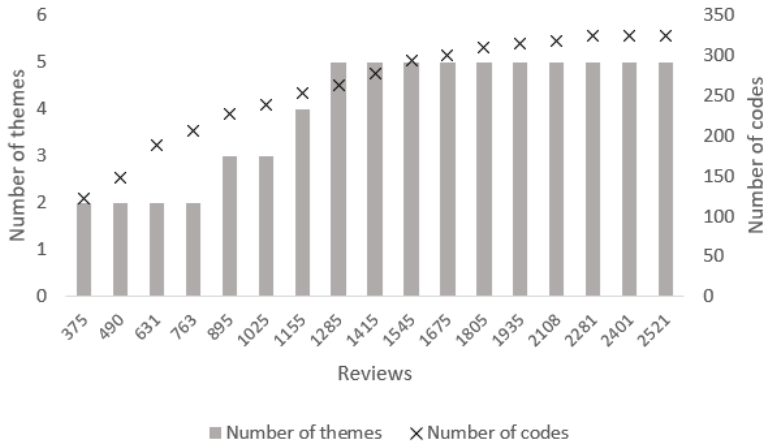


Figure 5.4: Number of codes and themes after each review batch

Table 5.5: Metadata for different types of reviews

Review Type		Word Count M	Word Count SD	Character Count M	Character Count SD	Rating M	Rating SD	Sentiment Neg	Sentiment Neu	Sentiment Pos
Relevant ($N = 6,859$)		33.12	28.24	178.13	153.3	2.36	1.52	17.5%	38.0%	44.5%
	Android ($N = 5,970$)	31.05	24.82	166.78	134.25	2.34	1.50	18.3%	38.5%	43.2%
	iOS ($N = 889$)	46.98	42.36	254.34	231.65	2.49	1.66	12.3%	34.5%	53.2%
Irrelevant ($N = 19,250$)		12.95	13.45	69.39	73.46	4.23	1.37	10.1%	14.3%	75.6%
All ($N = 26,109$)		18.25	20.53	97.96	111.54	3.74	1.63	15.2%	17.4%	67.4%

5.3 Results

In the following sections, we first briefly describe the metadata of the reviews that were classified as relevant by our approach and then present each identified theme. We include illustrative reviews where appropriate.

5.3.1 Review Corpus

The reviews that were classified as relevant to UX are longer and more detailed than the irrelevant reviews. They have more than twice as many words, with a standard deviation more than twice as large. The shortest relevant review is four words long and the longest 527 words. In Table 5.5, the relevant reviews are compared against the irrelevant ones. Other metadata, such as review age, can be found in Section C.2 in the supplementary material.

We performed an independent samples t-test on the lengths and ratings of the reviews. The results show that both the difference in length ($t(7992.5) = 56.79, p < 0.001$) and rating ($t(11020) = -89.47, p < 0.001$) between relevant and irrelevant reviews are statistically significant. The worse rating of relevant reviews is also reflected in the associated sentiments. The difference in negative sentiments between the relevant (M = 0.09, SD = 0.01) and irrelevant reviews (M = 0.04, SD = 0.01) was also statistically significant ($t(12162) = 35.17, p < 0.001$). Less than half (44.5%) of the relevant reviews have a positive sentiment, compared to the 75.6% of the irrelevant ones. The analysis was conducted using VADER [103], and discrete ratings were based on the compound score.

5.3.2 General UX Issues

Some reviews complained about shortcomings that are not unique to mobile wallets. Reviewers reported performance issues, including freezes and crashes that led to the inability to access funds in the worst case, e.g., *"[redacted wallet] is crashing every time I try to access it. Sometimes I can enter a number or two for my PIN before it crashes, but otherwise I cannot access my wallet at all [...]" (R6758).*

App updates also often resulted in negative effects for reviewers. Instances where an update led to a loss of functionality or access were reported for all wallets. In all such cases, reviewers appeared to be emotionally distressed, as illustrated in the following review: *"My app worked perfectly fine till you 'updated it' to 'fix crashes' now i can't even get the money out of my wallet. FIX THE APP ITS BEEN A WEEK ALREADY" (R522).* Some of these updates also occurred automatically and surprised some reviewers: *"[...] updating an app for security is not the same as completely changing what people get used to out of nowhere. being blindsided is not good [...]" (R1359).*

Common interface problems were also found in the reviews. Some issues were related to color schemes in the wallet interface, typos, or an inconsistent use of icons and were arguably merely an inconvenience, whereas others resulted in a direct functionality loss. Some examples for the latter were overlays that prevented reviewers from creating wallets or making transactions: *"[...] the app would not position the screen (lay out) properly...preventing me from touching the (APPROVE) button. Preventing the successful completion of the transaction. THIS APP IS FREEKING USELESS!!!!!!" (R440).* In this case, the reviewer did not lose crypto-assets; however, there were also cases where poor interface design led to monetary losses.[12] One example for this was double-spends, where reviewers sent a transaction multiple times by mistake. Because all transactions are irreversible by design, it resulted in a direct loss: *"This app is the worst. It just made me double send all my [crypto-assets] by not reacting to the Send button properly. Goodbye [redacted wallet], I trust you no more [...]" (R1086).*

Therefore, it appears that while the abovementioned issues are not unique to mobile wallets, they become more severe whenever money is at stake.

[12] Here, monetary losses do not include attacks or losses due to volatilty, but more so interface-related issues.

5.3.3 Domain-Specific UX Issues

We identified a variety of shortcomings unique to mobile wallets and present them in three groups: *before*, *during*, and *after* use.

Before Use

The wallet initialization process was found tedious by some reviewers. Some of the wallets that we investigated supported the option to purchase crypto-assets and therefore required reviewers to go through an identity verification procedure (also called know your customer) to prevent money laundering and fraud. This process, however, was reported to be cumbersome and sometimes involved downloading another application: *"Now I have download another app that is called Yoti. I have to put in MORE information about myself. I have to always take a selfie for any and every transaction. I don't want to have to use another app just to use another app [...]" (R1455)*. Even when downloading another app was not necessary and the verification was done in the respective wallet, it could often take up to multiple weeks to get verified, which resulted in reviewers getting frustrated: *"Since 4 months...Still showing verification under process...Your information is being reviewed...Am I going to be verified?" (R4105)*. This is in line with our qualitative findings where the verification process was identified as one of the entry barriers (Section 3.3.4).

Those reviewers who were able to get through the verification process also faced challenges. Reviews mentioned a lack of guidance during the setup that made it challenging to create a wallet in the first place. This was mostly reported by reviewers who considered themselves to be novices: *"I've been trying to learn about buying crypto, and even as an IT professional I've been a bit intimidated and confused. It took me several days of trying figure out how exactly to get money into the wallet [...]" (R382)*. This lack of guidance was also prevalent for specific functionalities of the wallet, such as the private key import/export: *"[...] Tutorials on how to import export would be nice and I'm a little nervous to try it out [...]" (R567)*.

During Use

Reviewers were unaware of which crypto-assets were supported by the wallet they were using. In the majority of cases when reviewers had installed a wallet without realizing that it did not support their particular crypto-asset, reviewers requested the support in a future version. However, there were also instances where reviewers sent an unsupported crypto-asset to their wallet, resulting in it getting stuck: *"I sent ICN tokens (300 of them) into my iconomi [...] wallet, and now [...] I can't send them out as it tells me it's an unambiguous address [...] but i need erc20*[13] *functionality not just storage" (R6334).*

Irrespective of the crypto-asset, reviewers also reported incorrect balances being displayed in their wallets. Some reviewers verified the transaction status with the help of blockchain explorers, such as Etherscan[14] or blockchain.com,[15] and found a mismatch between the actual status on the blockchain and the status in the wallet: *"We received a Bitcoin Cash transaction into this wallet 2 days ago, and the official blockchain shows that this transaction has received 76 confirmations. However, this app refuses to show the transaction as confirmed. It shows the transaction as pending with zero confirmations [...]" (R732).* Pending transactions were also often misunderstood, as illustrated by the following review: *"But it is still pending showing no confirmation and I am not able to transfer my ether to anybody these people have totally hijacked my wallet and I am on their mercy now" (R5542).* In this case, the user believed that by not being able to send their funds, a malicious party must have gained access to their wallet. In reality, however, pending transactions refer to transactions that have not been processed by the network yet.

One prominent reason for a transaction to stay in the pending state is the transaction fee (set by the user who initiates the transaction) being too small. For crypto-asset transactions, transaction fees can be set by the user and have a direct influence on how quickly a transaction is processed by the network – the higher the transaction fee, the more quickly a transaction is included in a block. Reviewers reported limited possibilities when it came to setting these fees in their wallets: *"Recom-*

[13] ERC-20 is the standard for tokens on Ethereum: https://eips.ethereum.org/EIPS/eip-20
[14] Ethereum blockchain explorer: https://etherscan.io/
[15] Bitcoin blockchain explorer: https://www.blockchain.com/explorer

mended fees are crazy one is too high the other is so low it would never process [...] I should have more than two fee options and should be allowed to set my own. Your [economy] fee would never get picked up by miners and your standard fee is crazy [...]" (R408). The main problem with inadequate fees is that even if a transaction fails, the fees are not refunded and this might result in a monetary loss: *"I've lost 40$ to unconfirmed transactions, my friends have lost 50$,70$, and 25$ [...]" (R873).*

High transaction fees were also caused by the apps' failure to support upgrades in the blockchain protocols. In the case of Bitcoin, one feature could have lowered the fees as explained in the following review: *"The fee for a bitcoin transaction on this app are ridiculous high, they have yet to add segwit*[16] *which will lower the fees and allow faster transaction times. If they would incorporate [segwit] these problems would not happen. I am very annoyed [...]" (R702).*

Moreover, the lack of transparency with regard to blockchain upgrades also resulted in functionality loss, with some reviewers not being able to send their transactions because of incompatible addresses: *"do you guys support the new bech32*[17] *format to send, keep getting incorrect bitcoin address error [...]" (R889).*

Inadequate transaction fees, however, were not the only problem, as some reviewers did not even know how to make transactions in the first place. Similar to the setup phase, some reviews mentioned an overall lack of guidance: *"I'm new at this but how do you add money to your wallet" (R608).* This lack of guidance was not only prevalent for transactions, but also for the recovery process. To recover a wallet, users need to input a 12-word seed phrase that was generated during the setup stage, and without such a phrase, a recovery is impossible. Some reviewers explained they had lost their phrases, whereas others did not understand how to use them: *"How can I recover my blockchain app [in case] I mistakenly delete it?" (R4127).* Reviewers also mentioned having difficulties with recovering access to their wallets in the case of new phones, or whenever they lost access otherwise: *"I recently uploaded some funds and now I can't even access them because [it keeps]*

[16] Segregated Witness (SegWit) was a protocol proposal improvement that, among other benefits, resulted in lower transaction fees: https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki

[17] Bech32 is a standard for wallet addresses that support SegWit: https://github.com/bitcoin/bips/blob/master/bip-0173.mediawiki

crashing I don't want to delete and reinstall because I've had this wallet for over a year and I don't [have] the [seed phrase] anymore [...]" (R405).

After Use

Some of the wallets required creating an account with the wallet provider, which some reviewers wanted to delete. In all such cases, however, they were not able to do so: *"I'm giving the 1 star would give it 0 if I could, I don't see any way to delete my account I don't use this anymore and trying to delete it so if anybody knows how to let me [know]" (R190).*

5.3.4 Misconceptions of Users

Some shortcomings can be attributed to reviewers' misconceptions of blockchain characteristics and crypto-asset building blocks, such as transactions. Reviewers attributed high fees, which were explained in Section 5.3.3, to wallet providers: *"I had around $30 worth of Bitcoin in my wallet. As I went to transfer the coin, I was charged a $10 transaction fee. That's 1/3 of my balance. Not only that, but I was charged a fee when I had my Bitcoin sent to Bread. I don't want to call them criminals or crooks because that's extreme. I just want to let everyone know how much in fees you will be charged if you use this service. Never again!" (R402).* Contrary to the reviewer's belief that the wallet provider is setting the transaction fees, the minimum required fees are determined by the network congestion and transaction size, and are received by the miners [13].

The fee structure was also not clear to some reviewers. To transfer tokens that are based on Ethereum, users have to pay the transaction fee in its currency, referred as Ether (often abbreviated as "ETH"), which was unclear to some: *"tries charging you ETH to make non-ETH trades and on top of that won't tell you how much ETH is even required. They are straight up extorting money from users! Avoid at all costs until they fix this and give us our money back [...]" (R3051).* Even after the developer responded to the review and explained the fee structure, the reviewer was still convinced they were correct: *"No exchange charges you coins that are not part of the 2 currencies being exchanged. Period. Fix your broken platform that locks people out of their $$."* This hints at the reviewer's belief that crypto-asset

exchanges operate in the same way as mobile wallets, which is not the case. Trades on a crypto-asset exchange are happening off-chain, i.e., are not incorporated into the blockchain, whereas transactions that are initiated from a mobile wallet are.

Reviewers were also confused about addresses. Some believed that their funds were tied to the mobile app: *"This app has deleted all my funds and account. DO NOT DOWNLOAD!!!" (R884)*. Such reviews hint at a misconception, as wallet addresses are immutable by design, with wallets being merely an interface to manage keys. Others believed that addresses were static and would not change, which is not the case for hierarchically deterministic wallets.[18] These wallets generate new addresses after every incoming payment, and in some instances, this led reviewers to believe that monetary losses have occurred: *"My Blockchain address was changed. I work for a company so they usually pay me in bitcoin every Friday. I usually receive the current weeks payment the next week. But due to the fact that my address was changed I couldn't see my payment on my wallet. I was shocked when I went to check and find out that my wallet address has been changed and my money for the week was lost" (R713)*.

Some reviewers also wanted to cancel transactions, which the design of the underlying blockchain does not allow. For example, this was reported in the context of transactions that were sent to a wrong address: *"[...] if i unfortunately sent any token on wrong [address] there [is] no cancel option! Add cancel option" (R928)*. A cancellation option was often requested, with some reviews mentioning conventional banking as an example: *"I never had an issue with Blockchain unlike Breadwallet but I [just] wish it was a way to stop payment [...] like you do a stop payment on a checking account" (R853)*. Recovery alternatives that were known from other payment systems were also requested: *"No way to restore your data and money once you lose your [seed] phrase. Please enter some other way of recovery like email backup" (R6271)*. Such recovery methods do not exist for non-custodial wallets, and using conventional systems as a reference point when dealing with crypto-assets could lead to errors and losses.

The comparison to conventional systems was also found in other contexts. Some reviewers were surprised by the transaction fees: *"Not user friendly. Al-*

[18] Deterministic wallets: https://en.bitcoin.it/wiki/Deterministic_wallet

ways wanting to get some sort of fee. I can't transfer funds without a cost. Just want to cash out and delete" (R3106). Others were taken by surprise when experienced fluctuations of the stored value, when expressed in fiat currency: *"I'm still new to the world of crypto currency, I thought this App is for storing value. But it looks my balance fluctuates with the Bitcoin price. I really need an urgent help before I lose all of my money" (R3096).*

A prevalent belief was also that the wallet providers have an influence on the transactions. Pending transactions were one example where reviewers asked for help from the developers: *"[...] Been 5 DAYS NOT ONE CONFIRMATION. I DONT CARE IF ITS THE MINERS THAT CONFIRM THE TRANSACTION THIS IS THEIR APP AND SHOULD HAVE SOME TYPE OF PROTOCOL FOR THIS [...]" (R90).* In case of failed transactions and lost fees, reviewers also expected help from the support team: *"Tried to exchange currency once it failed and I lost all of the [associated] fees, no help from support as to why it failed, I'll be using a different wallet from now on" (R5654).*

Support was also wanted in case of incorrectly displayed balances in the wallet. Some of these mismatching balances, however, were caused by syncing problems with the blockchain. Mobile wallets, and crypto-asset wallets in general, need to sync with the actual blockchain to display the newest transactions. Some reviewers did not know the purpose of the sync, whereas others were impatient and blamed the developer for coins that were not displayed: *"I do not recommend this app, they will steal your bitcoins and say that your wallet is out of sync, when you try to sync it, it just says the same thing. WALLET is a complete rip-off!!!!" (R3271).*

The majority of issues were believed to be the developer's fault, whereas in reality, the wallet had no influence whatsoever, as illustrated in the following review: *"Uninformed people are writing one star reviews because of high transaction fees and delays, when in reality [the wallet] has nothing to do with any of these issues" (R443).*

5.3.5 Security and Privacy

Issues related to security and privacy were brought up in app reviews. Mobile wallets allow anyone with the possession of the phone to transfer funds, and reviewers

expressed their concerns when it came to access to the app: *"This app is working very well except it opens straight into your send/receive function. A PIN would be nice to ensure only I can open the app" (R854)*. PIN codes, however, were viewed by some to be inferior to other authentication methods, such as biometrics: *"I was hoping they would finally include fingerprint authentication, but they still use pin and have a more dysfunctional app [...]" (R844)*. What's clear from our data is that reviewers were uncomfortable about their mobile wallets being accessible to anyone who opens them.

Measures to ensure that only the actual owners were able to send funds were also requested. For example, reviewers called for secondary protective measures, such as two-factor authentication: *"[...] security could be better (I'd like option to turn on 2FA when transacting on mobile app)" (R4497)*. Additional layers of access control, however, were not always welcomed, as illustrated by the following review: *"Forcing a screen lock = not cool. I keep my phone with me at all times, just like my physical wallet, and I don't want to turn on an annoying screen lock just for this app [...] Look, I get it, most people need to have their hand held through the process of securing their stuff, and adding an extra layer of security is covering your own behinds. [...] Just please don't force overbearing (and redundant) security features on users who don't want or need them" (R3333)*.

Reviewers were also worried about the security of their private keys. Wallets that allowed access to private keys were perceived to be more secure: *"This is only iOS wallet that puts you in control of your private keys (that I know of). Which makes it (potentially) one of the most secure mobile wallets" (R383)*. At the same time this potential single point of failure was also found worrisome, with some reviewers losing funds because of a stolen phone or a lost seed phrase: *"Some has stolen my phone and my blockchain wallet is inside the phone, I have so much money inside the bitcoin wallet but I've forgotten my password" (R720)*.

Physical safety was also considered to be a risk by some reviewers. This again relates to the fact that there is no centralized entity or safety net and in the case of losses, the funds are gone for good. Having a balance displayed in the wallet, for example, was found risky by some: *"[the wallet] should not display the accounts Total at first screen. Make you vulnerable to a $5 wrench*[19] *attack" (R6742)*. Sim-

[19] A hypothetical scenario where an attacker can physically force someone to give up information

ilarly, having to enter the PIN to accept transactions was seen as a physical risk as well: *"I have a background in law enforcement [...] I've investigated a quite a few robberies during my career and know how the future of robberies will happen [...] If I meet someone from craigslist to sell something [...] I have to enter my PIN to share my public key. So, let's say I'm meeting a stranger and now, I enter my pin and hold it up for them to scan... And WHAM! They snatch the phone out of my hand, run off with my phone and can now steal my bits cause I entered my pin for the bad guy. We don't need a PIN number to protect us from receiving money [...]" (R552).*

Lastly, privacy concerns were also found in the reviews. As previously mentioned, reviewers had to undergo a know your customer verification process to be able to purchase crypto-assets and found the sharing of personal data alarming: *"Need to disclose too much personal information [...] It just doesnt make any sense [...]" (R1837).* Deleting such personal information was found impossible, which resulted in distress for some: *"I am 17 years old and I'm trying to delete this app after an elderly man tried to trick me into opening an account. I'm scared because my Id information is on this app and I cannot delete it...can anyone help me?" (R770).* Questionable app permissions, such as the access to the contact list, microphone, or camera access also raised privacy concerns: *"Why do you need access to my microphone?? Can you [please] cite the international regulation you mentioned? What are 'localisation improvements?' Thanks. WHAT ARE LOCALISATION IMPROVEMENTS?? CITE THE INTERNATIONAL REGULATIONS???" (R99).* This is in line with prior work that identified the prevalence of overprivileged permissions in Android apps [68].

5.3.6 Trust

Reviews also included comments on factors that led reviewers to trust or distrust the wallets and their developers. Some reviewers explained they were using different types of wallets depending on the amount: *"If you're like me, you keep most of your BTC offline, or near offline, and transfer a little to [the Blockchain wallet] for some spending money [...]" (R836).* Others explicitly mentioned only trusting

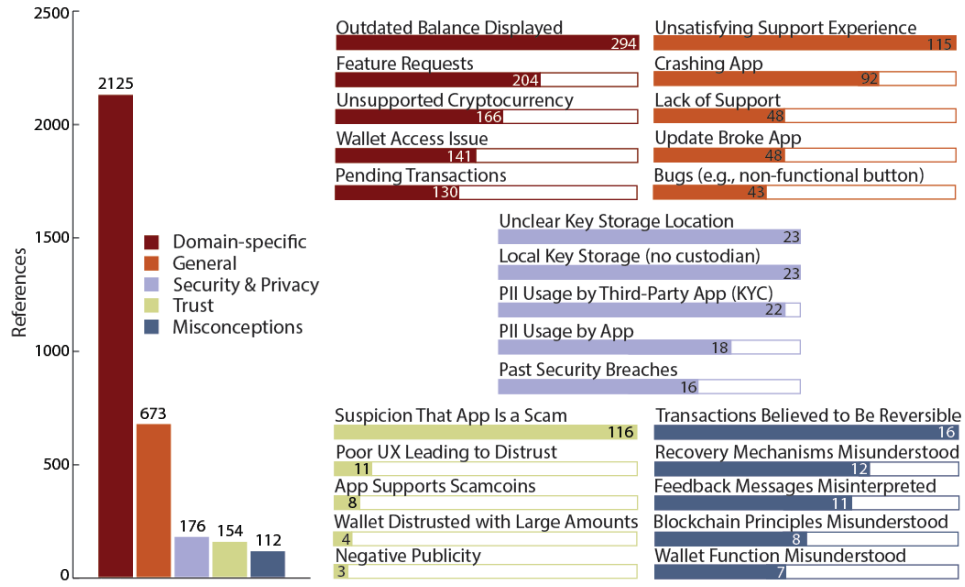
instead of breaking the underlying cryptography (https://xkcd.com/538/)

mobile wallets with small amounts, as illustrated in the following review: *"Just like any other wallet on a phone don't put all your funds here. It is just for small spending and transfers" (R6745).*

Some wallets were open source, which appeared to have an influence on trust. Reviewers valued the ability for the public to validate the source code: *"[...] the code is available to audit. It super important to feel safe using the app and this is the only one I trust" (R684).* However, whenever a wallet was closed source, such as the Coinomi wallet, some reviewers appeared to be hesitant: *"Coinomi's website lies by saying 'source-available.' They went close-source approx one year ago. This is not trustless. Who knows what they are now doing with your private keys" (R6319).* Bad publicity also appeared to influence the trust negatively: *"[...] the main reasons I don't trust this wallet is the defensive nature [that] the [developers] take towards negative comments, the fact that they leaked seeds [and] tried to threaten to cover it up [...]" (R5780).* This incident is well documented and was reported by multiple blockchain news outlets [130, 198].

Unsatisfying UX also led reviewers to question the motives of the developers and their apps. For example, missing transactions made reviewers believe that the wallet was a scam: *"[redacted wallet name] is a scam. The ceo needs to be arrested. I sent [crypto-assets] to Coinbase over a month ago and they have not arrive yet. This is one thing the president needs to look into, is not letting blockchain have any dealings in the USA" (R6660).* Various other reasons, such as the lack of a quick response from the customer service, high transaction fees, or even the volatility also led to some reviewers concluding that the app must be fraudulent: *"Beware of this scam application, it [is] deducting my money, from $155 to $89. What is deducting money from the account without any transaction. This app is totally scam scam scam scam" (R5569).*

Other prevalent issues that were presented in the previous sections also contributed to reviewers distrusting the apps. The inability to access the wallet or pending transactions, of which some might be attributed to unsynced wallets, were believed to be indicators of scams: *"Transferred a small amount from coinbase to this 12 hours ago, still nothing showing in the wallet. Has been confirmed sent but nothing on this end yet. [...] Think this is a scam of some kind" (R6071).* Even the most trivial things, such as accepting the terms and conditions, made some review-



(a) Number of referenced review segments per theme

(b) Five most frequent codes per theme (PII: personally identifiable information)

Figure 5.5: Theme statistics

ers question the legitimacy of the wallet: *"Would like allow me to accept terms and conditions. Wondering if it is a scam" (R6796).*

5.3.7 Theme Prevalence

Domain-specific issues were the most prevalent in our analysis. With 2,125 referenced review segments, these issues were more than three times as common as the next theme, i.e., general issues (see Figure 5.5a). Among domain-specific issues, outdated balances were the most prevalent, which, together with pending transactions, were found in over 400 reviews. For general issues, reviewers reported a poor (or nonexistent) support experience and further mentioned crashes and freezes that made it impossible for them to use the application in the first place. The other three themes were encountered less often (Figure 5.5b) but also appeared to influence the overall UX as outlined in Sections 5.3.4, 5.3.5, and 5.3.6.

5.3.8 Praised Features of Non-custodial Wallets

While the overwhelming majority of review segments were negative ($N = 3,104, \sim 96\%$), we also identified aspects about the wallets that were praised by the reviewers ($N = 136, \sim 4\%$). Pending transactions and outdated balances were among the most prevalent issues in the review corpus (see Figure 5.5b), which, as mentioned in Section 5.3.3, were sometimes caused by fixed transaction fees. Therefore, it is not surprising that some reviewers found customizable fees beneficial: *"I get to adjust the fees however I please, which has saved me a TON OF TIME AND MONEY when it comes to Price & Trx Spikes so i avoided being stuck on the blockchain [...]" (R6668)*.

Security features were also welcomed by reviewers. Some found it more secure that the app would lock itself after a time period, whereas others praised additional authentication measures, such as biometrics or PINs: *"Simple and easy way to send and receive bitcoin. Supports Touch ID and has a pin. I really love this app" (R857)*.

Reviewers also valued the non-custodial property of mobile wallets, as illustrated in the following review: *"[...] most other wallets are not wallets at all, they are just online banking apps for BTC. Not this! This is an actual wallet where you control the private keys. There is no central server, so you are responsible for your own security (this is a good thing) [...]" (R142)*. Similarly, the ability to import private keys into a wallet allowed users to seamlessly access their funds, leading to a better UX: *"Thanks so much! Had a few coins stuck in a wallet and instead of waiting for the wallet to sync I just imported my private key into [redacted wallet name]" (R6445)*. Such features could therefore have the potential to prevent access issues and stuck funds, which were both mentioned in hundreds of reviews.

5.4 Discussion

We have successfully applied a novel combination of automated review classification and manual, qualitative analysis to identify UX issues of mobile wallets. This hybrid methodology saved a considerable amount of time, as most reviews that were included in the qualitative analysis ($> 97.5\%$) were indeed relevant, compared to only 37.5% that were found relevant in a random sample. We identified

various issues that, while wide-ranging, can be assigned to one of two groups: *general* or *domain-specific*. All investigated wallets had these shortcomings, some of which resulted in dangerous errors or monetary losses for the reviewers. Our main contribution is the identification of previously unreported UX issues, both on the interface and conceptual levels, and their effects. In this section, we categorize these UX issues, discuss their implications, and outline possible design improvements that could alleviate them.

5.4.1 General UX Issues

Unsurprisingly, the investigated wallets had issues that are commonly found in mobile apps in general, both on Android and iOS. For example, reliability issues, such as crashes or freezes, are widely reported in the literature [83, 84, 119], yet their prevalence and impact in mobile wallets is unknown. For all mobile wallets that we investigated, the private keys are stored locally on the mobile device and are managed with the help of the app. For all apps, however, reviewers reported to have lost access to their funds because of apps crashing, slowing down, or not opening after new updates. Non-custodial wallets therefore present a unique case where user interface (UI) issues that would be harmless in many apps can have a disastrous impact on the UX and can lead to monetary losses.

To address this, wallet developers can clearly specify how to recover private keys in the case of non-functional applications. Mobile wallets, and non-custodial wallets in general, are interfaces that facilitate key management and are interchangeable as long as they support a particular crypto-asset. Often, reviewers did not know how to access or recover their assets without the mobile app. Providing more guidance and possibly technology support, e.g., in the form of key import/-export, could address this.

We have also encountered reviews mentioning common UI issues that led to a loss of functionality. For example, reviewers reported missing buttons that prevented them from sending transactions or instances where two transactions were sent because of an unresponsive interface. Similar to performance issues, these interface shortcomings can also have grave consequences. Following common usability guidelines or heuristics, such as the ones proposed by Nielsen and

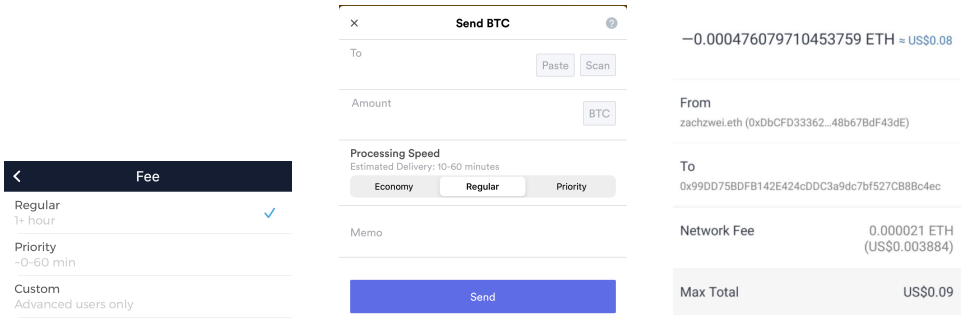
Molich [164], can help in reducing or even eliminating general issues, and can contribute to a better UX in the crypto-asset domain. Here, *error prevention (Heuristic 5)* is particularly important, because of the transaction irreversibility and the lack of a safety net for recovering from user-induced errors.

5.4.2 Domain-Specific UX Issues

The second group of identified issues is unique to the crypto-asset domain and needs special attention. Here, we differentiate between issues directly related to the UI and issues that are the result of users' misconceptions regarding crypto-assets. Two prominent examples of the former were incorrect wallet balances and unclear transactions statuses, some of which were caused by unsynced wallets. As a result, reviewers believed that losses had occurred, when in reality, the blockchain status displayed by the wallet was simply outdated. We recommend that wallets clearly display the current status of the blockchain and further state that syncing issues might be a reason for "incorrect" balances or "missing" transactions.

Transaction fees were another major problem encountered in reviews. The fees were perceived as either too high or too low, with reviewers rarely finding the fees appropriate. Transactions with low fees might not be processed by the miners at all, whereas users could overpay on transactions with too high fees. Mai et al. [146] further found that the implications of varying fees might be misunderstood by the users and suggest that wallets should provide preset fee options, as it is currently done in the Blockchain wallet and Coinomi. However, as our findings suggest, many reviewers found these options restricting and, at times, inadequate, especially when they could not be changed. We therefore recommend that wallets always allow users to customize their transaction fees based on a recommendation that averages the fees of the recently processed transactions that were included in the blockchain. Two of the five investigated wallets, BRD Bitcoin wallet and Trust Crypto wallet, did not (and still do not, as of December 2020) have a custom fee option, which was poorly received by their users. Figure 5.6 shows the fee options between the Blockchain Wallet, where custom fees are allowed, and the other two wallets, where pre-set fees are the only options.

Solving these domain-specific issues is not a trivial task, and one option could



(a) Blockchain Wallet **(b)** BRD Wallet **(c)** Trust Wallet

Figure 5.6: Comparison of transaction fee options between Blockchain, BRD, and Trust wallets

be the development of usability heuristics specific to the crypto-asset domain. Prior work has shown that domain-specific heuristics can help in identifying more severe usability issues unique to the domain (e.g., [21, 22, 48, 110, 127, 143]), and we believe that tailored heuristics can do the same for crypto-asset wallets. These heuristics could not only be used for discount usability testing, but also for informing the design of wallets.

Reviewers also had their fair share of misconceptions about the building blocks of crypto-assets that went beyond the interface. The most prevalent misconception of reviewers was that wallet developers are the ones who set and receive the transaction fees. This belief was particularly prevalent in those cases in which reviewers perceived the fees as very high, leading them to assume that the app was fraudulent. Others believed that transactions could also be canceled or reversed, which is also not the case in reality. Prior work has found that users do not understand the implications of varying fees on the processing speed [146], and our findings further suggest that the nature of transactions and fees in general might also be unclear for some. We do not report misconceptions regarding the underlying cryptography, as these are well documented [73, 146, 194, 216] and were confirmed in our study.

It further appears that traditional systems, such as online banking, serve as a reference point for some crypto-asset users who had these misconceptions. This can be problematic because of the vastly different natures of these two payment systems. Contrary to traditional currencies and systems, which allow the reversal

and cancellation of transactions in certain cases [34], it is impossible to do the same with crypto-assets. This lack of a safety net makes user errors, such as incorrectly addressed transactions, more costly. Crypto-assets also differ in other regards, such as inconsistent fees or dynamic addresses, and therefore clash with conventional payment systems [33].

Our results suggest that some users have these traditional systems in mind when using crypto-assets and are surprised when key characteristics or functionalities, such as the cancellation of payments, are not implemented. When using wallets, users also expected some type of recovery mechanisms that would allow them to regain access to their funds in case of lost seed phrases. Crypto-asset wallets should therefore try to mimic existing payment systems and features that users are already familiar with. Designing such systems is technically feasible, and we give detailed recommendations in Section 5.4.4 that could help in meeting some of the users' expectations.

Poor UX also led reviewers to question the intentions of the developers. Even the smallest errors or bugs, as well as the lack of customer support, made reviewers believe that the respective application was a scam. This is unsurprising considering the number of fraudulent crypto-asset exchanges and startups operating in the space [46]. Even in app reviews, we have identified several instances where reviewers tried to scam others, as illustrated in the following example: *"[...] please send some btc to my address I need to help some leprosy patients in my locality in Nigeria. All items and photos will be posted on all trust social network as a way trust is giving back to the society. [redacted bitcoin address]. Thank you in anticipation" (R1242)*. Fraudulent activities in the domain are prevalent [210] and make it particularly difficult for users to build trust. Losing trust, on the other hand, is easy and can be caused by common UX issues, such as a crashing app or a prompt asking the user to accept a set of terms and conditions. Therefore, it appears that trust in the crypto-asset domain not only includes social actors directly participating in transactions as suggested in prior work [193], but also the developers of tools that help users in managing their crypto-assets. A detailed investigation of factors influencing the choice of tools can be a subject for future studies.

Overall, it appears that the development of mobile wallets is a very difficult and unforgiving task. The developers have to consider not only common UX issues, but

also domain-specific ones, both of which can lead to irreversible damages for the respective users. Misconceptions on the users' side make it particularly difficult to design a wallet with a satisfying UX, as developers are blamed for every little mistake or bug, even though in many cases they can hardly be held responsible. Combined with the already distrustful user base due to the overwhelming number of scams and frauds in the domain, developers are fighting an uphill battle, as they have to address issues that are related to both UI and misunderstandings of technological intricacies of crypto-assets. We believe that providing functionality that is known from conventional systems and otherwise clearly stating the differences, such as transactions, addresses, and fees, can prevent future monetary losses and might further contribute to an improved overall UX.

5.4.3 Limitations

In this study, we have only investigated mobile wallets, and our findings are therefore not necessarily applicable to other wallet types. Similarly, the selected wallets do not support all crypto-assets in existence, and it is possible that some UX issues were therefore missed. However, we believe that while features might differ across crypto-assets and wallets, the key functionalities stay the same, and those include the management of cryptographic keys. A comparison of UX for different wallet types and crypto-assets could be an interesting avenue for future research.

Further, we have used an automated approach to filter non-relevant reviews. While our classifier has high accuracy, it is still possible that valuable reviews highlighting unreported UX issues were not included for manual analysis.

Some of the identified issues might have been version specific and may have been fixed in forthcoming updates. Due to the limited metadata in the app stores, however, we were not able to retrieve the version in which reviewers encountered these issues. Despite this limitation, we believe that the insights from this study provide a sufficiently accurate overview of the UX issues that are encountered in mobile wallets these days, especially since both general and domain-specific issues were found for all wallets and platforms.

5.4.4 Design Recommendations

Mimic Existing Payment Systems

Some users were surprised when features known from other payment systems were not implemented in mobile wallets. Certain features, such as reversible transactions, cannot be implemented as they clash with the fundamental principles of crypto-assets; others, however, can. A prevalent problem that was reported across all wallets in hundreds of reviews was pending transactions. Both Ethereum and Bitcoin allow users to "overwrite" an existing unconfirmed transaction that has not yet been processed by the network. For Bitcoin, this mechanism is called replace-by-fee[20] and allows users to send a modified transaction with a higher fee than the initial, possibly stuck, transaction. The miners would then process the newer transaction more quickly to maximize profits. Sending such transactions is relatively complex, and wallet developers could automate this process. Users could then replace "stuck" transactions with one click and would not have to wait days or even weeks just for a transaction to fail. One caveat of this approach, however, is that the user must pay the fees for both transactions. The wallet UI should therefore clearly communicate this prior to sending a replacement transaction.

Users also struggled with the recovery mechanism. Some had lost their seed phrase, whereas others had not saved it in the first place. Our work extends prior findings on self-errors of crypto-asset users [126, 194, 216] and shows the prevalence thereof during the wallet recovery phase. To alleviate this problem, encrypted cloud backups might be a viable option. During the setup, users could be given the option to encrypt their seed phrase with a password and store it in a cloud storage of their choice. In the case of lost seed phrases, users could then simply import their encrypted file and decrypt it in the wallet. Similarly, password managers could also be used to store seed phrases to ensure that funds could be recovered in case of non-functional apps or forgotten passwords. Both solutions, however, pose a potential new attack vector, as users would have to rely on a third party. To guarantee that such wallets remain non-custodial, the seed phrases would have to get encrypted on the user's device so that they were only stored by the service provider

[20] Replace-by-fee in Bitcoin: https://en.bitcoin.it/wiki/Replace_by_fee

in an encrypted form. Reliance on a third party in such "hybrid" approaches might be acceptable, particularly for newcomers with small amounts of crypto-assets. Alternatively, as a way to avoid storing seed phrases online at all, the wallets could provide backup reminders and ask users to enter their seed phrases periodically to ensure that they still have access.

Allow Wallet Personalization

Wallet personalization could also alleviate some of the identified issues. Users reported fixed transactions fees that led to pending transactions or lost funds. Customizable transaction fees, possibly with recommended values provided by the wallet, could have prevented some of these issues.

Distinguishing between advanced and new users could also be accomplished on the interface level. Personalized interfaces are known to enhance the overall UX [128] and we believe that different profiles for advanced versus new users can have the same effect for crypto-asset wallets. Newcomers could be shown only the default values, whereas experienced and expert users could have advanced options, such as custom transaction data, fees, and key import/export. Particularly the latter features should be communicated clearly, as our analysis has shown that some reviewers were confused or unsure of where the keys are located (see Figure 5.5b).

The security settings implemented by crypto-asset wallets were also found to be problematic. Shoulder surfing was perceived as a risk by users, with some being afraid of disclosing their wallet balance and others having the same concerns about their pin. A simple toggle option could be used to hide the wallet balance, whereas biometrics, e.g., a fingerprint, could be used to authenticate the wallet owner. Such features have to be implemented with caution, as some users complained about additional authentication measures being overbearing.

Improve Users' Understanding of Crypto-Assets

New users appeared to be overwhelmed when using crypto-asset wallets (Section 5.3.3). Blockchain characteristics were often unclear, particularly for users who used conventional payment systems as a reference point. Perhaps tutorials and sandboxes could help to familiarize newcomers with crypto-assets and could

potentially prevent costly user errors, which are known to be prevalent in the domain [126, 193, 216].

Users also often expected help from the developers whenever something went wrong. Often, however, the raised issues were the result of misconceptions on the users' end. Addressing these misconceptions is complicated, and there is no silver bullet. Yet guiding the users through their first transactions could improve their understanding. We believe that guiding users through a complex process safely, also referred to as *safe staging* [224], could be applied successfully to crypto-asset wallets. Embedded videos or animations could further be used to explain the most important elements and characteristics, such as private keys, addresses, and irreversibility of transactions. These guides could also explain the differences when compared to conventional systems and could not only help the users but also save time for the developers and their customer support teams.

5.5 Conclusion

We collected 45,821 app reviews of mobile crypto-asset wallets and employed ML and NLP techniques to select reviews relevant to UX. We then identified themes illustrating common UX issues as experienced by the users. These can be grouped into common and domain-specific UX issues, with both types leading to functional and monetary losses. Further, users appeared to rely on their understanding of traditional payment systems, such as online banking, when using crypto-assets and faced challenges when doing so. Security, privacy, and trust challenges were also uncovered that were caused by the UX shortcomings.

Our findings provide an overview of the challenges that crypto-asset users are facing and the underlying misconceptions prevalent among users. We suggest that to make the domain more usable, future wallets need to mimic conventional payment systems and users need to be more supported before and during use.

Chapter 6

Discussion and Conclusion

This thesis aims to create a better understanding of the challenges users and non-users of crypto-assets face and the factors influencing their behaviors and decisions. The findings for each of the four studies were discussed in their respective sections, hence, in the following, we focus on the overarching takeaways and discuss their implications.

6.1 Crypto-Asset Usage Is Nuanced

Prior to our work, few studies have looked beyond bitcoin and the understanding of the overall crypto-asset domain was therefore limited. Our qualitative study has revealed that, depending on crypto-asset, the implications for the users differ. For example, Ethereum and the corresponding tokens pose both a novel opportunity and risk for users. While smart contracts on Ethereum can be used to create decentralized applications, such as games and prediction markets, they also allow malicious actors to create fraudulent ICOs and scam coins which have been shown to lead to monetary losses [47, 174].

Participants also reported to store crypto-assets differently, depending on how they use them. Prior work has only focused on bitcoin key management [73, 126] and it was unknown what factors, and to what extent, affected users in their behaviors. Our results revealed that users distinguish between long- and short-term

holdings and store higher amounts of crypto-assets in more secure ways, such as hardware wallets. Crypto-assets that are traded, on the other hand, are oftentimes stored in custodial wallets, which can be more risky due to their centralized nature [158, 159].

We also found that this heterogeneity in behaviors goes beyond the storage practices. Prior qualitative work [27, 71], including our interview study, conjectured the existence of different user profiles, however, their existence was not empirically validated. The results of our clustering analysis suggest the existence of three crypto-asset user personas that differ in their motivations, perceptions, as well as security and privacy behaviors. Cypherpunks are expert users that are familiar with the tools and potential risks that an involvement with crypto-assets might bring. They got involved because of technological interest and an alignment of crypto-assets with their ideological principles. Hodlers, on the other hand, were driven mostly by financial incentives and this is reflected in their trust in custodians as well as prior trading experience. The last cluster are the rookies, i.e., novel users that got involved recently. They are less experienced and value convenience over security, contrary to the other two clusters.

Evidently, crypto-asset users differ in their characteristics and one can therefore hardly address their needs a whole and needs to narrow down the target population. This is critical, particularly in light of current key management tools that only offer a one-size-fits-all solution that is supposed to suit all users. Similarly, crypto-asset usage is also nuanced and goes beyond bitcoin and one needs to include other crypto-assets and use cases as they expose users to new challenges, such as security and privacy risks. We believe that more work is needed in order to understand how context is influencing crypto-asset users and one avenue for future work could be emerging application areas, such as decentralized finance and non-fungible tokens.

6.2 The Importance of Self-Efficacy

Throughout the research presented in this thesis, the perceived self-efficacy was found to be a key construct for both users and non-users. The non-users in our study believed to not be knowledgeable enough in order to be using crypto-assets, however, as it turns out, some users also had misunderstandings about the under-

lying protocols and cryptography. This is in line with the argument made by Gao et al. [73], who suggest that there must be other reasons preventing non-users from getting engaged with bitcoin and other crypto-assets, as they identified a lack of knowledge in both participant groups interviewed in their study, users and non-users of bitcoin. Based on our findings, one of these factors turns out to be the perceived self-efficacy.

The differences in self-efficacy, however, can also be observed within the population of crypto-asset users. As mentioned in the previous section, we identified three user personas, with cypherpunks being the expert users. Unsurprisingly, when looking at the perceived self-efficacy, cypherpunks also scored the highest amongst the three clusters, followed by hodlers and rookies. We discussed the heterogeneity of the user population in detail and the differences in the perceived self-efficacy again support our personas.

Self-efficacy also appears to have an effect on the adoption of crypto-assets. Guided by the findings of prior work suggesting the positive effect of self-efficacy on adoption behaviors [8, 113, 140, 149, 228], we were able to confirm the effects in the context of crypto-assets. Not only were we able to show its mediating effect on the intention to adopt crypto-assets, but it also had a strongly significant effect on the actual adoption behavior when we combined the samples of both users and non-users. Interestingly, self-efficacy was the only construct whose effect was statistically significant. This suggests that the perceived risk as well as institutional trust appear to not play a vital role in crypto-asset adoption.

Consequently, leveraging this construct could lead to an increased adoption of crypto-assets. While we have suggested ways of improving self-efficacy for both users and non-users, more work needs to be done in order identify effective ways of doing so. For example, enjoyment has been found to have a positive effect on the application-specific self-efficacy [104] and similar effects might also be observed for crypto-asset tools.

6.3 UX Shortcomings of Current Tools

Managing cryptographic keys is a challenge for end users. This was shown for PGP as early as in 1998 [223] and it is not surprising that this also holds true for

crypto-assets as well, due to both systems making use of public key cryptography. During our interviews, users reported usability issues for not only bitcoin wallets but crypto-asset wallets in general. For example, some users explained to have used tokens for non-monetary use cases, such as games or prediction markets, and recalled usability issues of browser-based wallets, decentralized applications, and mobile wallets.

The existence and prevalence of severe UX issues was then confirmed in our mixed-methods research study analyzing mobile wallet app reviews. Prior work has shown that wallets are difficult to use [66, 71], however, it was unclear what types of issues, and to what extent, affected the users. We addressed this knowledge gap by identifying five groups of issues, which, in the worst case, led to monetary losses and unusable applications.

Here, both domain-specific and general software engineering issues had these effects. For example, inadequate transaction fees preset by the applications led to pending transactions, which, eventually, failed and resulted in users losing the corresponding fees. Software bugs, such as crashes and freezes, also led to some users not being able to access their wallets and recover their keys. These issues, combined with the fact that users are solely responsible for the key management, put non-custodial wallets in a unique position where arguably harmless and common bugs could lead to severe, possibly irreversible, consequences.

Overall, it appears that cryptographic keys are still difficult to manage and not much has changed over the years. Ways of solving these issues in an effective manner is an open research question that could not only solve the challenges of existing users, but also lead to an increase in self-efficacy, thus, potentially facilitating adoption. Addressing the poor UX of current tools would therefore not only benefit users but also non-users and would make this avenue of research worth exploring in the future.

6.4 Conclusion

This dissertation investigates the behaviors of users and non-users of crypto-assets and identifies factors influencing them. We show that crypto-asset usage is nuanced and depends on factors such as the asset at hand, the amount invested, and the type

of user and their level of expertise. Current tools do not account for this heterogeneity and therefore only partially meet the users' needs and requirements, therefore, leading to a poor UX. In order to improve the overall UX, future tools need to account for contextual factors, such as the user personas and the way crypto-assets are used.

We also identified severe usability issues that appeared to contribute to the negative experience. These were found to lead to irreversible monetary losses and emotional distress for users and the perceived inability to use such tools further prevented non-users from getting involved. Addressing such issues could therefore not only improve the current UX but also lower the entry barriers and facilitate adoption.

Bibliography

[1] BIP 39 Standard. https://github.com/bitcoinbook/bitcoinbook/blob/f8b883dcd4e3d1b9adf40fed59b7e898fbd9241f/ch05.asciidoc, 2013. Accessed: 2019-09-19. → page 13

[2] A Comprehensive List of Cryptocurrency Exchange Hacks. https://selfkey.org/list-of-cryptocurrency-exchange-hacks/, 2020. Accessed: 2020-09-24. → page 18

[3] I. 9241-11. Ergonomics of human-system interaction — Part 11: Usability: Definitions and concepts. Standard, International Organization for Standardization, 2018. → page 111

[4] S. Abramova and R. 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*, 2016. → pages 2, 17, 51, 52, 57, 78, 84, 86, 87, 91, 96, 98

[5] A. Adams and M. A. Sasse. Users Are Not the Enemy. *Communications of the ACM*, 42(12):40–46, 1999. → pages 7, 52

[6] I. Ajzen. The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, 50(2):179–211, 1991. → page 54

[7] U. Akturan and N. Tezcan. Mobile banking adoption of the youth market. *Marketing Intelligence & Planning*, 2012. → pages 83, 86

[8] A. A. Alalwan, Y. K. Dwivedi, N. P. Rana, B. Lal, and M. D. Williams. Consumer adoption of Internet banking in Jordan: Examining the role of hedonic motivation, habit, self-efficacy and trust. *Journal of Financial Services Marketing*, 20(2):145–157, 2015. → pages 83, 85, 139

[9] A. A. Alalwan, Y. K. Dwivedi, and N. P. Rana. Factors influencing adoption of mobile banking by Jordanian bank customers: Extending UTAUT2 with trust. *International Journal of Information Management*, 37 (3):99–110, 2017. → page 83

[10] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun. Evaluating User Privacy in Bitcoin. In A.-R. Sadeghi, editor, *Financial Cryptography and Data Security*, pages 34–51, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg. → page 17

[11] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun. Evaluating User Privacy in Bitcoin. In *International Conference on Financial Cryptography and Data Security*, pages 34–51. Springer, 2013. → page 75

[12] A. Anjum, M. Sporny, and A. Sill. Blockchain standards for compliance and trust. *IEEE Cloud Computing*, 4(4):84–90, 2017. → page 19

[13] A. M. Antonopoulos. *Mastering Bitcoin: unlocking digital cryptocurrencies*. O'Reilly Media, Inc., 2014. → pages 12, 121

[14] C. API. Cryptocurrency exchange apis. https://www.coinapi.io/integration, 2019. Accessed: 2020-09-24. → page 48

[15] M. Arias-Oliva, J. Pelegrín-Borondo, and G. Matías-Clavero. Variables Influencing Cryptocurrency Use: A Technology Acceptance Model in Spain. *Frontiers in Psychology*, 10:475, 2019. → pages 3, 4, 51, 97

[16] C. B. Astrachan, V. K. Patel, and G. Wanzenried. A comparative study of cb-sem and pls-sem for theory development in family firm research. *Journal of Family Business Strategy*, 5(1):116–128, 2014. → page 95

[17] E. Bakiu and E. Guzman. Which feature is unusable? detecting usability and user experience issues from user reviews. In *2017 IEEE 25th International Requirements Engineering Conference Workshops (REW)*, pages 182–187. IEEE, 2017. → page 103

[18] A. Bandura. Self-efficacy. *The Corsini encyclopedia of psychology*, pages 1–3, 2010. → page 83

[19] A. W. Baur, J. Bühler, M. Bick, and C. S. Bonorden. Cryptocurrencies as a Disruption? Empirical Findings on User Adoption and Future Potential of Bitcoin and Co. In M. Janssen, M. Mäntymäki, J. Hidders, B. Klievink,

W. Lamersdorf, B. van Loenen, and A. Zuiderwijk, editors, *Conference on e-Business, e-Services and e-Society*, pages 63–80, Cham, 2015. Springer, Springer International Publishing. → page 51

[20] A. Beldad, M. De Jong, and M. Steehouder. How shall i trust the faceless and the intangible? a literature review on the antecedents of online trust. *Computers in human behavior*, 26(5):857–869, 2010. → page 18

[21] L. Benson, D. Elliott, M. Grant, D. Holschuh, B. Kim, H. Kim, E. Lauber, S. Loh, and T. C. Reeves. *Usability and Instructional Design Heuristics for E-Learning Evaluation*. Association for the Advancement of Computing in Education (AACE), 2002. → page 131

[22] E. Bertini, S. Gabrielli, S. Kimani, T. Catarci, and G. Santucci. Appropriating and assessing heuristics for mobile computing. In *Proceedings of the working conference on Advanced visual interfaces*, pages 119–126, 2006. → page 131

[23] D. Bianchi and A. Dickerson. Trading Volume in Cryptocurrency Markets. *SSRN Electronic Journal*, 01 2018. doi:10.2139/ssrn.3239670. → page 45

[24] Bitcoin News. Cryptsy exchange shuts down indefinitely. https://news.bitcoin.com/cryptsy-bitcoin-exchange-announces-massive-theft-shuts-indefinitely/, 2016. Accessed: 2019-04-27. → page 39

[25] Blockplate. The BIP39 (Mnemonic Seed) Wallet List. https://www.blockplate.com/blogs/blockplate/list-of-bip39-wallets-mnemonic-seed, 2019. Accessed: 2019-07-20. → page 13

[26] R. Böhme, N. Christin, B. Edelman, and T. Moore. Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives*, 29(2): 213–38, 2015. → pages 17, 56, 86, 91

[27] J. Bohr and M. 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. → pages 2, 51, 78, 138

[28] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In *2015 IEEE Symposium on Security and Privacy*, pages 104–121, May 2015. doi:10.1109/SP.2015.14. → pages 16, 86

[29] S. R. Boss, D. F. Galletta, P. B. Lowry, G. D. Moody, and P. 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. ISSN 0276-7783. → page 54

[30] V. Braun and V. Clarke. Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2):77–101, 2006. → pages 7, 15

[31] J. Bucko, D. Palová, and M. Vejacka. Security and trust in cryptocurrencies. In *Central European Conference in Finance and Economics*, pages 14–24, 2015. → page 19

[32] M. Casey, J. Crane, G. Gensler, S. Johnson, and N. Narula. The impact of blockchain technology on finance: A catalyst for change. 2018. → page 12

[33] V. Cermak. Can Bitcoin Become a Viable Alternative to Fiat Currencies? An Empirical Analysis of Bitcoin's Volatility Based on a GARCH Model. *An Empirical Analysis of Bitcoin's Volatility Based on a GARCH Model (May 2, 2017)*, 2017. → page 132

[34] P. Ceruleo. Bitcoin: a rival to fiat money or a speculative financial asset? *Master's Thesis*, 2014. → page 132

[35] R. Chandy and H. Gu. Identifying spam in the iOS app store. In *Proceedings of the 2nd Joint WICOW/AIRWeb Workshop on Web Quality*, pages 56–59, 2012. → page 106

[36] Chaos Computer Congress. Attacks on Hardware Wallets. https://wallet.fail/, 2020. Accessed: 2020-09-14. → page 75

[37] K. Charmaz. *Constructing grounded theory: A practical guide through qualitative analysis*. sage, 2006. → pages 14, 15

[38] N. Chen, J. Lin, S. C. Hoi, X. Xiao, and B. Zhang. Ar-miner: mining informative reviews for developers from mobile app marketplace. In *Proceedings of the 36th international conference on software engineering*, pages 767–778, 2014. → page 103

[39] Y. Chen and F. M. Zahedi. Individual's Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China. *MIS Quarterly*, 40(1):205–222, 2016. → pages 54, 81

[40] C.-M. Chiu, E. T. Wang, Y.-H. Fang, and H.-Y. Huang. Understanding customers' repeat purchase intentions in B2C e-commerce: the roles of

utilitarian value, hedonic value and perceived risk. *Information Systems Journal*, 24(1):85–114, 2014. → page 86

[41] P. Ciaian, M. Rajcaniova, and d. Kancs. The economics of BitCoin price formation. *Applied Economics*, 48(19):1799–1815, 2016. → page 45

[42] Coindesk. Mt. Gox Allegedly Loses $350 Million in Bitcoin (744,400 BTC), Rumoured to be Insolvent. https://www.coindesk.com/mt-gox-loses-340-million-bitcoin-rumoured-insolvent, 2014. Accessed: 2019-04-27. → page 18

[43] Coindesk. From Law to Lawlessness: Bits of the Untold QuadrigaCX Story. https://www.coindesk.com/from-law-to-lawlessness-bits-of-the-untold-quadrigacx-story, 2019. Accessed: 2019-04-27. → pages 18, 47

[44] Coingecko. Cryptocurrency Global Charts. https://www.coingecko.com/en/global_charts, 2021. Accessed: 2020-02-22. → page 1

[45] CoinMarketCap. Distinct Cryptocurrencies. https://coinmarketcap.com/all/views/all/, 2021. Accessed: 2020-01-09. → page 12

[46] D. Coins. Scam Coins Overview. https://deadcoins.com//, 2020. Accessed: 2020-08-10. → pages 18, 132

[47] CoinTelegraph. OneCoin: A deep dive into crypto's most notorious Ponzi scheme. https://cointelegraph.com/news/onecoin-a-deep-dive-into-crypto-s-most-notorious-ponzi-scheme, 2020. Accessed: 2020-11-11. → pages 99, 137

[48] T. Conte, J. Massolar, E. Mendes, and G. H. Travassos. Web usability inspection technique based on design perspectives. *IET software*, 3(2): 106–123, 2009. → page 131

[49] M. Conti, E. S. Kumar, C. Lal, and S. Ruj. A Survey on Security and Privacy Issues of Bitcoin. *IEEE Communications Surveys & Tutorials*, 20 (4):3416–3452, 2018. → page 75

[50] Conti, M., Sandeep Kumar, E., Lal, C., Ruj, S. A Survey on Security and Privacy Issues of Bitcoin. *IEEE Communications Surveys & Tutorials*, 20 (4):3416–3452, 2018. → page 44

[51] J. Corbin and A. Strauss. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. SAGE Publications, 2014. ISBN 9781483315683. URL https://books.google.ca/books?id=hZ6kBQAAQBAJ. → pages 14, 22

[52] C. L. Corritore, B. Kracher, and S. Wiedenbeck. On-line trust: concepts, evolving themes, a model. *International journal of human-computer studies*, 58(6):737–758, 2003. → page 18

[53] L. J. Cronbach. Coefficient Alpha and the Internal Structure of Tests. *Psychometrika*, 16(3):297–334, 1951. → page 60

[54] R. Crossler and F. 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. ISSN 0095-0033. → page 54

[55] W. A. Cunningham, K. J. Preacher, and M. R. Banaji. Implicit Attitude Measures: Consistency, Stability, and Convergent Validity. *Psychological science*, 12(2):163–170, 2001. → page 54

[56] P. Das, S. Faust, and J. 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. → page 13

[57] T. Das and B.-S. Teng. The risk-based view of trust: A conceptual framework. *journal of Business and Psychology*, 19(1):85–116, 2004. → page 89

[58] F. D. Davis. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, pages 319–340, 1989. → pages 3, 54, 82

[59] P. De Filippi, M. Mannan, and W. Reijers. Blockchain as a confidence machine: The problem of trust & challenges of governance. *Technology in Society*, 62:101284, 2020. → page 88

[60] W. H. Delone and E. R. McLean. The DeLone and McLean model of information systems success: a ten-year update. *Journal of management information systems*, 19(4):9–30, 2003. → page 83

[61] T. Dinev and P. Hart. An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, 17(1):61–80, 2006. → page 187

[62] J. L. Dupree, R. Devries, D. M. Berry, and E. 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. → page 77

[63] S. Egelman and S. Schechter. The Importance of Being Earnest [In Security Warnings]. In *International Conference on Financial Cryptography and Data Security*, pages 52–59. Springer, 2013. → page 79

[64] C. Elsden, A. Manohar, J. Briggs, M. Harding, C. Speed, and J. Vines. Making Sense of Blockchain Applications: A Typology for HCI. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2018. → page 103

[65] D. A. Epstein, N. B. Lee, J. H. Kang, E. Agapie, J. Schroeder, L. R. Pina, J. Fogarty, J. A. Kientz, and S. Munson. Examining Menstrual Tracking to Inform the Design of Personal Informatics Tools. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 6876–6888, 2017. → page 105

[66] S. Eskandari, J. Clark, D. Barrera, and E. Stobert. A First Look at the Usability of Bitcoin Key Management. *Proceedings 2015 Workshop on Usable Security, 2015*, 2015. → pages 4, 7, 44, 51, 79, 99, 103, 140

[67] G. Fanti, L. Kogan, S. Oh, K. Ruan, P. Viswanath, and G. Wang. Compounding of Wealth in Proof-of-Stake Cryptocurrencies. In *International Conference on Financial Cryptography and Data Security*, pages 42–61. Springer, 2019. → page 65

[68] A. P. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner. Android permissions demystified. In *Proceedings of the 18th ACM conference on Computer and communications security*, pages 627–638, 2011. → page 125

[69] D. Florencio and C. 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. ISBN 978-1-59593-654-7.

doi:10.1145/1242572.1242661. URL
http://portal.acm.org/citation.cfm?doid=1242572.1242661. → page 52

[70] C. Fornell and D. F. Larcker. Structural equation models with unobservable variables and measurement error: Algebra and statistics, 1981. → page 92

[71] M. Fröhlich, F. Gutjahr, and F. 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, 2020. → pages 4, 51, 77, 78, 79, 87, 98, 103, 104, 138, 140

[72] S. Gabriele and S. 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. → page 77

[73] X. Gao, G. D. Clark, and J. 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, 2016. → pages
1, 3, 9, 17, 19, 20, 25, 37, 39, 46, 51, 78, 84, 85, 97, 102, 131, 137, 139

[74] D. Gefen, E. Karahanna, and D. W. Straub. Trust and tam in online shopping: an integrated model. *MIS quarterly*, 27(1):51–90, 2003. → pages 36, 41, 42, 43, 83, 88, 99

[75] B. G. Glaser and A. L. Strauss. *Discovery of grounded theory: Strategies for qualitative research*. Routledge, 2017. → pages 14, 15

[76] S. Goldfeder, H. Kalodner, D. Reisman, and A. Narayanan. When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies. *Proceedings on Privacy Enhancing Technologies*, pages 179–199, 2018. → page 17

[77] J. Grable and R. H. Lytton. Financial risk tolerance revisited: the development of a risk assessment instrument. *Financial services review*, 8 (3):163–181, 1999. → page 100

[78] J. E. Grable and R. H. Lytton. The development of a risk assessment instrument: A follow-up study. *Financial services review*, 12(3), 2003. → page 100

[79] G. Grant and R. Hogan. Bitcoin: Risks and Controls. *Journal of Corporate Accounting & Finance*, 26(5):29–35, 2015. → pages 17, 56, 86, 91

[80] J.-C. Gu, S.-C. Lee, and Y.-H. Suh. Determinants of behavioral intention to mobile banking. *Expert Systems with Applications*, 36(9):11605–11616, 2009. → page 89

[81] X. Gu and S. Kim. "What Parts of Your Apps are Loved by Users?". In *2015 30th IEEE/ACM International Conference on Automated Software Engineering (ASE)*, pages 760–770. IEEE, 2015. → pages 103, 110

[82] G. Guest, A. Bunce, and L. Johnson. How many interviews are enough? an experiment with data saturation and variability. *Field methods*, 18(1): 59–82, 2006. → pages 114, 115

[83] E. Guzman and W. Maalej. How do users like this feature? a fine grained sentiment analysis of app reviews. In *2014 IEEE 22nd international requirements engineering conference (RE)*, pages 153–162. IEEE, 2014. → pages 103, 106, 109, 111, 113, 129

[84] E. Ha and D. Wagner. Do Android users write about electric sheep? Examining consumer reviews in Google Play. In *2013 IEEE 10th Consumer Communications and Networking Conference (CCNC)*, pages 149–157. IEEE, 2013. → pages 103, 129

[85] J. F. Hair, W. C. Black, B. J. Babin, R. E. Anderson, R. L. Tatham, et al. *Multivariate data analysis*, volume 5. Prentice hall Upper Saddle River, NJ, 1998. → pages 91, 92

[86] P. Hanafizadeh, M. Behboudi, A. A. Koshksaray, and M. J. S. Tabar. Mobile-banking adoption by Iranian bank clients. *Telematics and Informatics*, 31(1):62–78, 2014. → pages 3, 83

[87] P. Hanafizadeh, B. W. Keating, and H. R. Khedmatgozar. A systematic review of Internet banking adoption. *Telematics and informatics*, 31(3): 492–510, 2014. → page 83

[88] J. A. Hanley and B. J. McNeil. The meaning and use of the area under a receiver operating characteristic (roc) curve. *Radiology*, 143(1):29–36, 1982. → pages 113, 114

[89] R. Hardin. *Trust and trustworthiness*. Russell Sage Foundation, 2002. → page 88

[90] E. Hargittai and S. Shafer. Differences in Actual and Perceived Online Skills: The Role of Gender. *Social Science Quarterly*, 87(2):432–448, 2006. doi:10.1111/j.1540-6237.2006.00389.x. → pages 81, 100

[91] M. Hassenzahl and N. Tractinsky. User experience - a research agenda. *Behaviour & information technology*, 25(2):91–97, 2006. → page 111

[92] E. Hayashi and J. 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. ISBN 9781450302289. → page 53

[93] H. He and Y. Ma. *Imbalanced learning: foundations, algorithms, and applications*. John Wiley & Sons, 2013. → pages 113, 114

[94] P. Hecht, S. Fels, and J. Anacleto. Seamless and always-on security in a bring-your-own-application world. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*, pages 2019–2024, 2015. → page 29

[95] D. D. Heckathorn. Respondent-Driven Sampling: A New Approach to the Study of Hidden Populations. *Social Problems*, 44(2):174–199, 1997. → page 51

[96] S. Hedegaard and J. G. Simonsen. Extracting usability and user experience information from online user reviews. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2089–2098, 2013. → pages 103, 104, 107, 109, 110, 113

[97] C. S. Henry, K. Huynh, and G. Nicholls. Bitcoin Awareness and Usage in Canada. *Journal of Digital Banking*, 2(4):311–337, 2018. → pages 51, 52, 81

[98] J. Henseler, C. M. Ringle, and M. Sarstedt. A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the academy of marketing science*, 43(1):115–135, 2015. → page 93

[99] G. Hileman and M. Rauchs. Global Cryptocurrency Benchmarking Study. *Cambridge Centre for Alternative Finance*, 33:33–113, 2017. → pages 1, 51, 52, 54

[100] K. Hornbæk. Current practice in measuring usability: Challenges to usability studies and research. *International journal of human-computer studies*, 64(2):79–102, 2006. → page 111

[101] D. W. Hosmer Jr, S. Lemeshow, and R. X. Sturdivant. *Applied logistic regression*, volume 398. John Wiley & Sons, 2013. → pages 113, 114

[102] L.-t. Hu and P. M. Bentler. Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural equation modeling: a multidisciplinary journal*, 6(1):1–55, 1999. → page 94

[103] C. J. Hutto and E. Gilbert. Vader: A parsimonious rule-based model for sentiment analysis of social media text. In *Eighth international AAAI conference on weblogs and social media*, 2014. → pages 111, 116

[104] Y. Hwang and M. Yi. Predicting the use of web-based information systems: intrinsic motivation and self-efficacy. *AMCIS 2002 Proceedings*, page 149, 2002. → page 139

[105] IDEX. Decentralized Exchange. https://idex.market/, 2020. Accessed: 2020-09-24. → page 48

[106] P. 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. → pages 76, 186, 187

[107] B. T. Institute. Exchange Volumes Report. https://www.bti.live/bti-september-2019-wash-trade-report/, 2019. Accessed: 2020-09-24. → page 45

[108] I. Ion, R. Reeder, and S. 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. → page 74

[109] ISO9241-210. Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems. Standard, International Organization for Standardization, 2019. → pages 111, 188

[110] P. Jaferian, K. Hawkey, A. Sotirakopoulos, M. Velez-Rojas, and K. Beznosov. Heuristics for evaluating IT security management tools. In

Proceedings of the Seventh Symposium on Usable Privacy and Security, pages 1–20, 2011. → page 131

[111] S. Jain, E. Felten, and S. Goldfeder. Determining an Optimal Threshold on the Online Reserves of a Bitcoin Exchange. *Journal of Cybersecurity*, 4(1): 1–12, 2018. → page 68

[112] J. Jansen. Studying Safe Online Banking Behaviour: A Protection Motivation Theory Approach. In *HAISA*, pages 120–130, 2015. → page 87

[113] B. K. Jeong, T. E. Yoon, et al. An empirical investigation on consumer acceptance of mobile banking services. *Business and management research*, 2(1):31–40, 2013. → pages 83, 84, 85, 139

[114] A. C. Johnston and M. Warkentin. Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, 34(3):549–566, Sept. 2010. ISSN 0276-7783. → pages 54, 76, 186, 187

[115] Kevin Helms. Illegal Activity No Longer Dominant Use of Bitcoin: DEA Agent. https://news.bitcoin.com/illegal-activity-use-bitcoin-dea-agent/, 2019. Accessed: 2019-02-28. → pages 1, 43

[116] I. E. Khairuddin and C. 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*, page 629. ACM, 2019. → pages 3, 51

[117] I. E. Khairuddin, C. Sas, S. Clinch, and N. 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. ACM, 2016. → page 3

[118] I. E. Khairuddin, C. Sas, S. Clinch, and N. 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, 2016. → pages 51, 56

[119] H. Khalid. On identifying user complaints of iOS apps. In *2013 35th international conference on software engineering (ICSE)*, pages 1474–1476. IEEE, 2013. → pages 103, 129

[120] G. Kim, B. Shin, and H. G. Lee. Understanding dynamics between initial trust and usage intentions of mobile banking. *Information Systems Journal*, 19(3):283–311, 2009. → pages 83, 88, 89

[121] Y. H. Kim and D. J. Kim. A study of online transaction self-efficacy, consumer trust, and uncertainty reduction in electronic commerce transaction. In *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, pages 170c–170c. IEEE, 2005. → pages 3, 83, 86, 89

[122] M. Kiran and M. Stanett. Bitcoin Risk Analysis. *NEMODE Policy Paper*, 2015. → pages 17, 86

[123] R. B. Kline. *Principles and practice of structural equation modeling*. Guilford publications, 2015. → page 94

[124] M. Knittel, S. Pitts, and R. Wash. "The Most Trustworthy Coin": How Ideological Tensions Drive Trust in Bitcoin. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), 2019. doi:10.1145/3359138. URL https://doi.org/10.1145/3359138. → page 75

[125] M. Krause. Bitcoin: Implications for the developing world. 2016. → page 2

[126] K. Krombholz, A. Judmayer, M. Gusenbauer, and E. Weippl. The Other Side of the Coin: User Experiences with Bitcoin Security and Privacy. In J. Grossklags and B. Preneel, editors, *Financial Cryptography and Data Security*, pages 555–580, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg. → pages 1, 2, 4, 9, 13, 17, 25, 51, 52, 56, 57, 78, 103, 134, 136, 137

[127] B. A. Kumar and M. S. Goundar. Usability heuristics for mobile learning applications. *Education and Information Technologies*, 24(2):1819–1833, 2019. → page 131

[128] R. L. Kumar, M. A. Smith, and S. Bannerjee. User interface features influencing overall ease of use and personalization. *Information & Management*, 41(3):289–302, 2004. → page 135

[129] P. Kumaraguru and L. F. Cranor. *Privacy Indexes: A Survey of Westin's Studies*. Carnegie Mellon University, School of Computer Science, 2005. → page 77

[130] J. l Valenzuela. Coinomi Vulnerability Discovered, Developers React Harshly. https://dashnews.org/coinomi-vulnerability-discovered-developers-react-harshly/, Fall 2017. Accessed: 2020-08-10. → page 126

[131] V. S. Lai and H. Li. Technology acceptance model for internet banking: an invariance analysis. *Information & management*, 42(2):373–386, 2005. → pages 3, 83

[132] J. R. Landis and G. G. Koch. The measurement of observer agreement for categorical data. *biometrics*, pages 159–174, 1977. → page 112

[133] G. J. Larios-Hernández and A. Ortiz-de Zarate-Béjar. *Blockchain Entrepreneurship and the Struggle for Trust Among the Unbanked*, pages 259–283. Springer International Publishing, Cham, 2019. → page 47

[134] K. S. Lee, H. S. Lee, and S. Y. Kim. Factors influencing the adoption behavior of mobile banking: a South Korean perspective. *The Journal of Internet Banking and Commerce*, 12(2):1–9, 2007. → pages 83, 86, 88, 89

[135] Y. Lee, K. A. Kozar, and K. R. Larsen. The Technology Acceptance Model: Past, Present, and Future. *Communications of the Association for Information Systems*, 12(1):752–780, 2003. → page 54

[136] M.-J. D. Levers. Philosophical paradigms, grounded theory, and perspectives on emergence. *Sage Open*, 3(4):2158244013517243, 2013. → page 14

[137] X. Li, T. J. Hess, and J. S. Valacich. Why do we trust new technology? a study of initial trust formation with organizational information systems. *The Journal of Strategic Information Systems*, 17(1):39–71, 2008. → pages 20, 100

[138] H.-F. Lin. An empirical investigation of mobile banking adoption: The effect of innovation attributes and knowledge-based trust. *International journal of information management*, 31(3):252–260, 2011. → page 36

[139] Z. Liu, Q. Min, and S. Ji. An empirical study on mobile banking adoption: The role of trust. In *2009 Second International Symposium on Electronic Commerce and Security*, volume 2, pages 7–13. IEEE, 2009. → page 88

[140] P. Luarn and H.-H. Lin. Toward an understanding of the behavioral intention to use mobile banking. *Computers in human behavior*, 21(6): 873–891, 2005. → pages 83, 84, 85, 139

[141] X. Luo, H. Li, J. Zhang, and J. P. Shim. Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services. *Decision support systems*, 49 (2):222–234, 2010. → pages 83, 86, 87, 88, 89, 91, 97

[142] W. Maalej and H. Nabil. Bug report, feature request, or simply praise? on automatically classifying app reviews. In *2015 IEEE 23rd international requirements engineering conference (RE)*, pages 116–125. IEEE, 2015. → pages 103, 109, 110, 111, 113

[143] O. Machado Neto and M. D. G. Pimentel. Heuristics for the assessment of interfaces of mobile devices. In *Proceedings of the 19th Brazilian symposium on Multimedia and the web*, pages 93–96, 2013. → page 131

[144] D. Machuletz, S. Laube, and R. 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. → page 54

[145] P. H. Madore. Bitcoin Nation: 22 Million US Crypto Traders Dwarf Global Rivals. https://www.ccn.com/bitcoin-nation-22-million-us-crypto-traders-dwarf-global-rivals/, 2020. Accessed: 2020-08-16. → page 1

[146] A. Mai, K. Pfeffer, M. Gusenbauer, E. Weippl, and K. Krombholz. User Mental Models of Cryptocurrency Systems-A Grounded Theory Approach. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS) 2020)*, pages 341–358, 2020. → pages 51, 78, 102, 130, 131

[147] C. Makanyeza. Determinants of consumers' intention to adopt mobile banking services in Zimbabwe. *International Journal of Bank Marketing*, 2017. → page 86

[148] C. Manning and H. Schutze. *Foundations of statistical natural language processing*. MIT press, 1999. → pages 109, 110

[149] B. Marakarkandy, N. Yajnik, and C. Dasgupta. Enabling internet banking adoption. *Journal of Enterprise Information Management*, 2017. → pages 83, 85, 139

[150] H. W. Marsh and D. Hocevar. Application of confirmatory factor analysis to the study of self-concept: First-and higher order factor models and their invariance across groups. *Psychological bulletin*, 97(3):562, 1985. → page 94

[151] C. Martins, T. Oliveira, and A. Popovič. Understanding the Internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application. *International Journal of Information Management*, 34(1):1–13, 2014. → page 86

[152] S. McIlroy, N. Ali, H. Khalid, and A. E. Hassan. Analyzing and automatically labelling the types of user issues that are raised in mobile app reviews. *Empirical Software Engineering*, 21(3):1067–1106, 2016. → pages 103, 104, 106

[153] J. McIver and E. G. Carmines. *Unidimensional scaling*. Number 24. Sage, 1981. → page 95

[154] D. H. McKnight, V. Choudhury, and C. Kacmar. Developing and validating trust measures for e-commerce: An integrative typology. *Information systems research*, 13(3):334–359, 2002. → page 88

[155] D. H. Mcknight, M. Carter, J. B. Thatcher, and P. F. Clay. Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on management information systems (TMIS)*, 2(2):1–25, 2011. → page 100

[156] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage. A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. In *Proceedings of the 2013 Conference on Internet Measurement Conference*, IMC '13, pages 127–140, New York, NY, USA, 2013. ACM. ISBN 978-1-4503-1953-9. doi:10.1145/2504730.2504747. URL http://doi.acm.org/10.1145/2504730.2504747. → page 17

[157] Mix. How BitConnect pulled the biggest exit scheme in cryptocurrency. https://thenextweb.com/hardfork/2018/01/17/bitconnect-bitcoin-scam-cryptocurrency/, 2018. Accessed: 2020-08-10. → page 18

[158] T. Moore and N. Christin. Beware the middleman: Empirical analysis of bitcoin-exchange risk. In *International Conference on Financial Cryptography and Data Security*, pages 25–33. Springer, 2013. → page 138

[159] T. Moore, N. Christin, and J. Szurdi. Revisiting the risks of bitcoin currency exchange closure. *ACM Transactions on Internet Technology (TOIT)*, 18(4):1–18, 2018. → pages 13, 86, 99, 138

[160] M. Möser, K. Soska, E. Heilman, K. Lee, H. Heffan, S. Srivastava, K. Hogan, J. Hennessey, A. Miller, A. Narayanan, et al. An Empirical Analysis of Traceability in the Monero Blockchain. *Proceedings on Privacy Enhancing Technologies*, 2018(3):143–163, 2018. → page 75

[161] Y. Y. Mun and Y. Hwang. Predicting the use of web-based information systems: self-efficacy, enjoyment, learning goal orientation, and the technology acceptance model. *International journal of human-computer studies*, 59(4):431–449, 2003. → page 83

[162] D. C. Nguyen, E. Derr, M. Backes, and S. Bugiel. Short text, large effect: measuring the impact of user reviews on android app security & privacy. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 555–569. IEEE, 2019. → pages 109, 110

[163] Q. N. Nguyen and D. J. Kim. Enforcing Information Security Protection: Risk Propensity and Self-Efficacy Perspectives. In *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017. → page 87

[164] J. Nielsen and R. Molich. Heuristic evaluation of user interfaces. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 249–256, 1990. → page 130

[165] F. of Money Research Collaborative:, T. C. Nelms, B. Maurer, L. Swartz, and S. Mainwaring. Social payments: Innovation, trust, bitcoin, and the sharing economy. *Theory, Culture & Society*, 35(3):13–33, 2018. → page 19

[166] OpenZeppelin. The Parity Wallet Hack Explained. https://blog.openzeppelin.com/on-the-parity-wallet-multisig-hack-405a8c12e8f7/, 2020. Accessed: 2020-09-14. → page 75

[167] N. Ostern. Do you trust a trust-free transaction? toward a trust framework model for blockchain technology. In J. Pries-Heje, S. Ram, and M. Rosemann, editors, *Proceedings of the International Conference on Information Systems - Bridging the Internet of People, Data, and Things, ICIS 2018, San Francisco, CA, USA, December 13-16, 2018*. Association for Information Systems, 2018. URL https://aisel.aisnet.org/icis2018/crypto/Presentations/3. → page 19

[168] D. Pagano and W. Maalej. User feedback in the appstore: An empirical study. In *2013 21st IEEE international requirements engineering conference (RE)*, pages 125–134. IEEE, 2013. → pages 104, 107, 110

[169] L. A. Palinkas, S. M. Horwitz, C. A. Green, J. P. Wisdom, N. Duan, and K. 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. → page 51

[170] S. Panichella, A. Di Sorbo, E. Guzman, C. A. Visaggio, G. Canfora, and H. C. Gall. How Can I Improve My App? Classifying User Reviews for Software Maintenance and Evolution. In *2015 IEEE International Conference on Software Maintenance and Evolution (ICSME)*, pages 281–290. IEEE, 2015. → page 103

[171] P. 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. → page 54

[172] P. A. Pavlou. Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International journal of electronic commerce*, 7(3):101–134, 2003. → page 83

[173] S. Pearman, J. Thomas, P. E. Naeini, H. Habib, L. Bauer, N. Christin, L. F. Cranor, S. Egelman, and A. 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, Oct. 2017. Association for Computing Machinery. ISBN 978-1-4503-4946-8. doi:10.1145/3133956.3133973. URL https://dl.acm.org/doi/10.1145/3133956.3133973. → page 53

[174] Y. B. Perez. 2019's juiciest crypto drama: The saga of OneCoin's $4B 'cryptocurrency' scam. https://thenextweb.com/hardfork/2019/12/23/onecoin-cryptocurrency-scam-need-to-know/, 2019. Accessed: 2020-08-10. → pages 18, 137

[175] H. Petrie and N. Bevan. The Evaluation of Accessibility, Usability, and User Experience. *The universal access handbook*, 1:1–16, 2009. → page 111

[176] T. Pikkarainen, K. Pikkarainen, H. Karjaluoto, and S. Pahnila. Consumer acceptance of online banking: an extension of the technology acceptance model. *Internet research*, 2004. → pages 3, 83

[177] T. Pranckevičius and V. Marcinkevičius. Comparison of naive bayes, random forest, decision tree, support vector machines, and logistic regression classifiers for text reviews classification. *Baltic Journal of Modern Computing*, 5(2):221, 2017. → page 112

[178] W. Presthus and N. O. O'Malley. Motivations and barriers for end-user adoption of bitcoin as digital currency. *Procedia Computer Science*, 121: 89–97, 2017. → page 98

[179] B. D. Rapkin and D. A. Luke. Cluster analysis in Community Research: Epistemology and Practice. *American Journal of Community Psychology*, 21(2):247–277, 1993. → page 54

[180] M. Rauchs, A. Blandin, K. Klein, G. C. Pieters, M. Recanatini, and B. Z. Zhang. 2nd Global Cryptoasset Benchmarking Study. *Available at SSRN 3306125*, 2018. → pages 1, 51, 52, 54

[181] E. M. Redmiles, S. Kross, and M. 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. → page 58

[182] R. W. Reeder, A. P. Felt, S. Consolvo, N. Malkin, C. Thompson, and S. 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. → page 79

[183] J. Riegelsberger, M. A. Sasse, and J. D. McCarthy. The mechanics of trust: A framework for research and design. *International Journal of Human-Computer Studies*, 62(3):381–422, 2005. → pages 19, 99

[184] M. Riek, S. Abramova, and R. Böhme. Analyzing Persistent Impact of Cybercrime on the Societal Level: Evidence for Individual Security Behavior. In *ICIS*, 2017. → page 86

[185] R. W. Rogers. A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology*, 91(1):93–114, 1975. → page 54

[186] R. S. Ross. Guide for conducting risk assessments (nist sp-800-30rev1). *The National Institute of Standards and Technology (NIST), Gaithersburg*, 2012. → page 16

[187] Y. Rosseel. Lavaan: An R package for structural equation modeling and more. Version 0.5–12 (BETA). *Journal of statistical software*, 48(2):1–36, 2012. → page 94

[188] S. Rotchanakitumnuai and M. Speece. Barriers to internet banking adoption: a qualitative study among corporate customers in thailand. *International Journal of Bank Marketing*, 21(6/7):312–323, 2003. → page 36

[189] S. K. Roy, A. Kesharwani, and S. S. Bisht. The impact of trust and perceived risk on internet banking adoption in India. *International Journal of Bank Marketing*, 2012. → page 86

[190] S. Ruoti, J. Andersen, D. Zappala, and K. Seamons. Why Johnny Still, Still Can't Encrypt: Evaluating the Usability of a Modern PGP Client. *arXiv:1510.08555 [cs]*, Jan. 2016. URL http://arxiv.org/abs/1510.08555. arXiv: 1510.08555. → page 53

[191] V. Sadhya, H. Sadhya, R. Hirschheim, and E. Watson. Exploring technology trust in bitcoin: the blockchain exemplar. In P. M. Bednar, U. Frank, and K. Kautz, editors, *26th European Conference on Information Systems: Beyond Digitization - Facets of Socio-Technical Change, ECIS 2018, Portsmouth, UK, June 23-28, 2018*, page 5, 2018. URL https://aisel.aisnet.org/ecis2018_rp/5. → page 19

[192] S. Sarker, J. S. Valacich, and S. Sarker. Virtual team trust: Instrument development and validation in an is educational environment. *Information Resources Management Journal (IRMJ)*, 16(2):35–55, 2003. → page 45

[193] C. Sas and I. E. Khairuddin. Exploring trust in Bitcoin technology: a framework for HCI research. In *Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction*, pages 338–342, 2015. → pages 1, 18, 19, 22, 132, 136

[194] C. Sas and I. E. 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, 2017. → pages 1, 3, 4, 7, 9, 19, 39, 44, 51, 52, 53, 56, 78, 86, 88, 97, 98, 100, 104, 131, 134

[195] K. Sebastian. Distinguishing between the types of grounded theory: Classical, interpretive and constructivist. *Journal for Social Thought*, 3(1): 1–9, 2019. → page 15

[196] S. K. Sharma and M. Sharma. Examining the role of trust and quality dimensions in the actual usage of mobile banking services: An empirical

investigation. *International Journal of Information Management*, 44: 65–75, 2019. → page 83

[197] M. Srite and E. Karahanna. The role of espoused national cultural values in technology acceptance. *MIS quarterly*, pages 679–704, 2006. → page 100

[198] J. Sterling. Coinomi – disclosure, denial, and destructive PR. https://cryptoinsider.media/coinomi-wallet-disclosure-denial-destructive-pr/, Fall 2017. Accessed: 2020-08-10. → page 126

[199] H. Stix. Ownership and purchase intention of crypto-assets – survey results. Oesterreichische Nationalbank Working Papers (Austria), 2019. → pages 51, 52

[200] E. Stobert and R. Biddle. The Password Life Cycle. *ACM Transactions on Privacy and Security*, 21(3):13, 2018. → page 53

[201] P. Story, D. Smullen, A. Acquisti, L. F. Cranor, N. Sadeh, and F. Schaub. From Intent to Action: Nudging Users Towards Secure Mobile Payments. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS)*, pages 379–415, 2020. → page 54

[202] M. Suh and G. 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. → page 54

[203] A. Susanto, H. Lee, H. Zo, and A. P. Ciganek. User acceptance of internet banking in indonesia: initial trust formation. *Information Development*, 29 (4):309–322, 2013. → page 46

[204] M. Tabassum, J. Kropczynski, P. Wisniewski, and H. R. 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. → page 77

[205] K. 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. → page 60

[206] 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. ISSN 0144-929X, 1362-3001. doi:10.1080/01449290903121386. URL http://www.tandfonline.com/doi/abs/10.1080/01449290903121386. → page 53

[207] F. B. Tan and P. Sutherland. Online consumer trust: a multi-dimensional model. *Journal of Electronic Commerce in Organizations (JECO)*, 2(3): 40–58, 2004. → pages 88, 100

[208] M. Thelwall and D. Stuart. Web crawling ethics revisited: Cost, privacy, and denial of service. *Journal of the American Society for Information Science and Technology*, 57(13):1771–1779, 2006. → page 105

[209] Uniswap. Exchange. http://uniswap.exchange/, 2020. Accessed: 2020-09-24. → page 48

[210] M. H. ur Rehman, K. Salah, E. Damiani, and D. Svetinovic. Trust in blockchain cryptocurrency ecosystem. *IEEE Transactions on Engineering Management*, 2019. → page 132

[211] M. Vaismoradi, H. Turunen, and T. Bondas. Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing & health sciences*, 15(3):398–405, 2013. → pages 15, 115

[212] V. Venkatesh and F. D. Davis. A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management science*, 46 (2):186–204, 2000. → pages 3, 83

[213] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis. User acceptance of information technology: Toward a unified view. *MIS quarterly*, pages 425–478, 2003. → page 4

[214] V. Venkatesh, J. Y. Thong, and X. Xu. Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS quarterly*, pages 157–178, 2012. → page 3

[215] S. T. Völkel, R. Schödel, D. Buschek, C. Stachl, V. Winterhalter, M. Bühner, and H. Hussmann. Developing a Personality Model for Speech-based Conversational Agents Using the Psycholexical Approach. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2020. → page 105

[216] A. Voskobojnikov, B. Obada-Obieh, Y. Huang, and K. 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. → pages 51, 78, 79, 84, 86, 87, 97, 100, 103, 104, 131, 134, 136

[217] S. Wallbach, R. Lehner, K. Roethke, R. Elbert, and A. Benlian. Trust-building effects of blockchain features–an empirical analysis of immutability, traceability and anonymity. 2020. → page 88

[218] A. Walton and K. Johnston. Exploring perceptions of bitcoin adoption: the South African virtual community perspective. *Interdisciplinary Journal of Information, Knowledge & Management*, 13, 2018. → page 98

[219] S. W. Wang, W. Ngamsiriudom, and C.-H. Hsieh. Trust disposition, trust antecedents, trust, and behavioral intention. *The Service Industries Journal*, 35(10):555–572, 2015. → page 36

[220] R. Wash, E. Rader, R. Berman, and Z. 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. → page 53

[221] K. Werbach. *The blockchain and the new architecture of trust*. Mit Press, 2018. → page 88

[222] F. Westin and S. 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. ISBN 9781450376471. doi:10.1145/3368860.3368865. URL https://doi.org/10.1145/3368860.3368865. → page 81

[223] A. 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. → pages 7, 29, 53, 139

[224] A. Whitten and J. D. Tygar. Safe Staging for Computer Security. In *Workshop on Human-Computer Interaction and Security Systems*. Citeseer, 2003. → pages 29, 136

[225] G. Wood et al. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151(2014):1–32, 2014. → page 12

[226] H. yi Sandy Tsai, M. Jiang, S. Alhabash, R. LaRose, N. J. Rifon, and S. R. Cotten. Understanding Online Safety Behaviors: A Protection Motivation Theory Perspective. *Computers & Security*, 59:138 – 150, 2016. ISSN 0167-4048. → pages 54, 76, 186, 187

[227] S. Y. Yousafzai, J. G. Pallister, and G. R. Foxall. Strategies for building and communicating trust in electronic banking: A field experiment. *Psychology & Marketing*, 22(2):181–201, 2005. → page 88

[228] T. Zhou. Understanding users' initial trust in mobile banking: An elaboration likelihood perspective. *Computers in Human Behavior*, 28(4): 1518–1525, 2012. → pages 46, 83, 85, 86, 139

Appendix A

Interview Study

A.1 Recruitment Notice

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

Electrical and Computer Engineering
Vancouver Campus
Kaiser 5500 - 2332 Main Mall
Vancouver, BC Canada V6T 1Z4

www.ece.ubc.ca

Towards the Understanding of Security and Privacy Behavior of Cryptocurrency Users

The main objective of this study is to investigate users' behavior regarding security and privacy when using cryptocurrencies. We seek to understand what the current security/privacy risks are, how well aware users are of these risks and how these risks are mitigated.

Participants of the study will be involved in an interview lasting approximately **one** hour. The interview can be conducted either in-person or via a telephone call. During the interview, participants will be asked questions regarding their behavior when using cryptocurrencies and utility tokens.

Participants will be compensated with $15 in appreciation of their time.

If you are interested, please contact

Artemij Voskobojnikov

Figure A.1: Recruitment notice

A.2 Interview Questions

Interview guides for both users and non-users follow. Research questions that were addressed are in bold.

A.2.1 Users of Crypto-Assets

RQ1: What are the current usages of cryptocurrencies?

Q1. Please tell me about how you got into cryptocurrencies.

Q2. How much money have you spent?

Q3. What do you use cryptocurrencies for?

Q3.1 How many transactions do you perform?

Q4. How has this usage changed over time? If it did, why?

Q5. How many different currencies do you own?

Q5.1 What three currencies have you invested the most money in? Why?

Q5.2 Do you use these currencies for different use cases? Why?

Q6. What factors influence you when making a decision to invest in a currency?

Q6.1 How well do you research the currency prior to an investment?

Q6.2 How knowledgeable are you about currencies that you have invested in?

Q6.3 Can you explain the concept behind blockchain to me?

RQ2: How do holders manage their cryptocurrency?

Q.7 How do you store your cryptocurrencies?

Q7.1 Please name the wallets you personally use the most.

Q7.2 Why did you choose these wallets?

Q7.3 How many different wallets do you use?

Q7.4 For how many of these wallets do you own the private key?

Q7.5 Can you explain to me what a private key is?

Q7.6 What do you need the private key for?

Q7.8 How is a private key different from a public key?

Q7.9 Do you store different currencies in different wallets?

RQ3: What is the perception of cryptocurrency-related security risk?

Q8 Have you ever lost cryptocurrency?

Q8.1 How much money did you lose?

Q8.2 Were you able to recover the key(s)?

Q9 What risks are you personally aware of when it comes to cryptocurrencies?
Q9.1 What is the most severe one according to you? Why?
Q10 What measures do you use to mitigate those risks? (**RQ4**)
Q10.1 What measures worked and which ones did not? Why?
Q11. In what ways do you protect different cryptocurrencies? (**RQ5**)
Q11.1 What factors influence your decisions?

A.2.2 Non-Users of Crypto-Assets

RQ1: What are the current usages of cryptocurrencies?
Q1. What payment systems do you use in your daily life?
Q2. How did you hear about cryptocurrencies for the first time?
Q3. What cryptocurrencies have you heard of?
Q4. How do you view your understanding of cryptocurrencies?
Q4.1 And of the underlying technological background?
Q5. What do you think cryptocurrencies are used for?
Q6. Why do you believe people purchase cryptocurrencies?
Q7. Why did you choose not to purchase cryptocurrencies?
Q7.1 What would have to happen for you to reconsider?

RQ3: What is the perception of cryptocurrency-related security risk?
Q8. What risks come with the usage of cryptocurrencies?
Q8.1 What is the most severe one? Why?
Q9. Can you think of ways users can protect themselves? (RQ4)

Appendix B

Survey Study

B.1 Survey Questionnaire

INTRODUCTION

Dear visitor,

are cryptocurrencies secure? Please participate in our survey and help us to tackle this question in our research project. Your answers will inform us and the community of developers about your security needs and opinions on crypto-assets and will make a significant contribution towards providing a better experience for both cryptocurrency users and newcomers. Completing this survey is voluntary and will take about 25 minutes of your time. In appreciation of your time and efforts, you will have the choice to participate in a raffle to win 50 Euro. You have the choice to either receive 50 Euro (or its U.S. dollar equivalent) in the form of an Amazon gift card OR make us donate the amount to WWF, Red Cross, or Unicef on your behalf.

Please note that your anonymous responses will be analyzed and reported in an aggregate form and will be used for research purposes and by the involved academic partners only. If you have any questions or would like to get further information, you may contact [redacted]. By clicking Yes, you confirm to be over 19 years of age and consent to us collecting information about your opinions on crypto-assets and general demographic information. You may refuse to participate or withdraw from the study at any time without penalty.

Before you proceed to the survey, please complete the captcha below.

Q1 Do you consent to participating in this study?
() Yes, I consent.
() No, I do not consent.

We care about the quality of our survey data and hope to receive the most accurate measures of your opinions, so it is important to us that you thoughtfully provide your best answer to each question in the survey.

Q2 Do you commit to providing your thoughtful and honest answers to the questions in this survey?
() I will provide my best answers.
() I will not provide my best answers.
() I can't promise either way.

Q3 How old are you?
() Under 18 years
() 18–24 years
() 25–34 years
() 35–44 years
() 45–54 years
() 55–64 years
() 65+ years

() Prefer not to answer

Q4 In which country do you currently reside?
(drop-down list from Afghanistan ... Zimbabwe)

SECTION A: YOUR EXPERIENCE WITH CRYPTO-ASSETS

This survey is about cryptocurrencies and tokens. We use the term **"crypto-assets"** to refer to both of them. The survey is thematically structured into 6 sections.

Q5 Have you ever held crypto-assets?
() Yes, I'm currently holding them.
() Yes, I'm currently holding them but plan to stop using them in the next 6 month.
() Yes, I have held them in the past and stopped using them.
() No, I have never held them but have some domain knowledge.
() I have never heard of crypto-assets / only know them by name.

Q6 How many years of experience using crypto-assets do you have?
() Less than 1 year
() 1–2
() 3–4
() 5–6
() More than 6 years

Q7 Please select up to 5 factors that contributed to starting your use of crypto-assets.
() Decentralization
() Financial gain
() Store of value
() Anonymity

() Interest in the technology
() Interest in services exclusive to crypto-assets
() Recommendation from my social circle
() Earning money from Proof-Of-Stake
() Hedging against the next financial crises
() Inflation protection
() Diversification of my investment portfolio
() Other: _____

Q8 Please select all the areas where you have used crypto-assets.
() Payment method for goods or services
() Non-monetary case, e. g., use of platforms or services that support crypto-assets
() Investment
() Cross-border money transfer
() Other: _____

Q9 What services or products have you paid for with crypto-assets?
() Restaurants, cafés, bars
() Donations
() Virtual goods (e. g., videogames, hosting services)
() Travel
() Drugs
() Goods on underground marketplaces
() Other: _____

Q10 Please select all the factors that contributed to your decision against holding crypto-assets. *(Q5, items selected 3–5)*
() Volatile nature of crypto-assets
() Lack of regulatory support
() Lack of incentives or use cases
() Fear of possible security vulnerabilities in crypto-assets
() Fear of possible security vulnerabilities in wallets

() Negative experience with service providers, e. g., exchanges or wallets
() Negative stigma associated with crypto-assets
() Concern of falling victim to fraud or crime
() Other: _____

Q11 Are you considering purchasing crypto-assets in 2020? *(Q5, items selected 3–5)*
() Yes
() No
() I don't know.

Q12 In which context(s) do/did you use crypto-assets?
() For private purposes
() For business purposes
() For other purposes: _____

Q13 How confident are you in the following skill areas in the context of crypto-assets? *(1 - not confident at all, 5 - very confident)*

	1	2	3	4	5
Purchasing crypto-assets	()	()	()	()	()
Making payments with crypto-assets	()	()	()	()	()
Explaining the difference between the private and public key	()	()	()	()	()
Explaining the purpose of transaction fees	()	()	()	()	()
Finding support in the case of erroneous transactions	()	()	()	()	()

Q14 Which crypto-assets are you currently holding?
() Bitcoin
() Ethereum

() Ripple
() Bitcoin Cash
() Litecoin
() EOS
() Monero
() Dash
() Neo
() Cardano
() Z-cash
() Tokens
() Others: _____

Q15 Please list the names of crypto-tokens you are currently holding.

_____

Q16 How much, in terms of the market value, are you currently holding in crypto-assets?

() Less than USD 1,000
() USD 1,000 – USD 5,000
() USD 5,000 - USD 10,000
() USD 10,000 – USD 100,000
() USD 100,000 – USD 1,000,000
() More than USD 1,000,000
() Prefer not to tell

Q17 Please indicate to what extent do you agree with the following statements. *(1 - fully disagree, 5 - fully agree)*

	1	2	3	4	5
I am comfortable making transactions with crypto-assets.	()	()	()	()	()

I am comfortable using software that allows me to make crypto-asset transactions.	()	()	()	()	()
I feel that most crypto-asset exchanges act in their customers' best interest.	()	()	()	()	()
I feel that most merchants who accept crypto-assets act in their customers' best interest.	()	()	()	()	()
I am NOT comfortable making transactions with crypto-assets.	()	()	()	()	()
The application areas of crypto-assets are similar to those of other payment systems.	()	()	()	()	()

SECTION B: STORAGE OF CRYPTO-ASSETS

Q18 To what extent are you aware of the types of crypto wallets available for storing crypto-assets? *(1 - not aware at all, 5 - very aware)*

() 1
() 2
() 3
() 4
() 5

Q19 Please specify all type(s) of crypto wallets you are currently using.

() *Software wallet*: A software wallet is specialized software downloaded and installed on users' personal devices (e. g., Bitcoin Core client, Armory, Electrum, or Hive).

() *Offline kept paper wallet*: A paper wallet refers to the way of storing private keys offline on a physical document.

() *Hardware wallet*: A hardware wallet refers to the way of storing private keys on an external hardware device (e. g., Ledger or Trezor).

() *Cryptographic hardware storage device*: A cryptographic hardware storage device is a highly-secure physical device for safeguarding private keys (e. g., a smart card or HSM).

() *Brain wallet*: A brain wallet refers to the way of storing private keys in one's own mind by memorization of a passphrase.
() *Multi-signature wallet*: A multi-signature wallet requires more than one private key to authorise a transaction.
() *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.
() *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.
() *Exchange*
() I am not sure.
() Other: _____

Q20 Please specify which type of crypto wallet holds most of your funds.
() *Software wallet*
() *Offline kept paper wallet*
() *Hardware wallet*
() *Cryptographic hardware storage device*
() *Brain wallet*
() *Multi-signature wallet*
() *Mobile wallet*
() *Cloud/online wallet*
() *Exchange*
() I am not sure.
() Other: _____

Q21 What factors influence/influenced your decision when choosing a crypto wallet for storing your crypto-assets?
() Convenience of making transactions
() Effort required for storing private keys
() Effort required for reactivating an access
() Recommendation from friends and family
() Usability

() Support provided by the developers
() Security guarantees
() Supported crypto-assets
() Other: _____

Q22 Who has control over private keys for the majority of your crypto-assets (in terms of value)?
() I myself
() Service (e. g., exchange)
() Me and another trusted person
() I am not sure.

Q23 Have you also kept a significant deposit of conventional money (e. g., dollar or euro) on a crypto-exchange account?
() Yes, at the present
() Yes, in the past
() Never

Q24 Have you ever traded on conventional financial stock markets? If yes, how often?
() No, I haven't.
() Yes, I traded once or a few times.
() Yes, I trade occasionally.
() Yes, I trade regularly.

Q25 Please indicate to what extent do you agree with the following statements. *(1 - fully disagree, 5 - fully agree*)

	1	2	3	4	5
I feel confident that the technological features of crypto-assets make it safe for me to use them.	()	()	()	()	()

I feel that existing safeguards adequately protect me when using crypto-asset exchanges.	()	()	()	()	()
In general, the environment in which I can use crypto- assets is robust and safe.	()	()	()	()	()

Q26 Please select exchanges you are currently using for storing your fiat money and crypto-assets.

() Binance
() Bisq
() Bitbuy
() bitcoin.de
() Bitfinex
() Bitmex
() Bittrex
() cex.io
() Coinbase
() coinfinity
() Coinsquare
() Gemini
() Huobi
() Kraken
() Kucoin
() Localbitcoins
() OKEx
() Other: _____

Q27 Please select up to 5 factors that should be considered in general when choosing an online wallet provider or exchange?

() Official registration and location
() Terms of use
() Transaction fees
() Amount of personal data I need to provide

() Ease of opening an account
() Technical security features
() Reputation profile
() Supervision by a renowned authority
() Supported crypto-assets and services
() Recommendations from my social circle
() Transaction volume
() Others: _____

SECTION C: RISKS

Q28 Have you ever lost a substantial amount of crypto-assets at a time?
() Yes, due to a stolen key
() Yes, due to a financial investment loss (e. g., market price volatility, scams)
() Yes, due to self-induced errors (e. g., forgotten key/password)
() Yes, other: _____
() No
() I am not sure.

Q29 To what extent are you concerned about the following risks related to crypto-assets? *(1 - not concerned at all, 5 - very concerned)*

	1	2	3	4	5
Theft of private keys	()	()	()	()	()
Volatility of the market price	()	()	()	()	()
Risk of being extorted	()	()	()	()	()
Losing crypto-assets by my own mistakes	()	()	()	()	()
Security vulnerabilities of wallets	()	()	()	()	()
Security vulnerabilities of exchanges	()	()	()	()	()
Legal uncertainty for the users of crypto-assets and possible prosecution	()	()	()	()	()

Restricted crypto-asset usage because of regulatory involvement	()	()	()	()	()
Lack of wide adoption of crypto-assets	()	()	()	()	()
Lack of interoperability of crypto-assets with other services	()	()	()	()	()
Traceability of transactions by governments	()	()	()	()	()
Traceability of transactions by firms/private sector	()	()	()	()	()
Traceability of transactions by individuals	()	()	()	()	()
Leakage of personally identifiable information (e. g., e-mail addresses) by crypto-asset exchanges	()	()	()	()	()
Information sharing with national tax authorities	()	()	()	()	()

Q30 To what extent do you agree with the following statements?
(1 - do not agree at all, 5 - fully agree)

	1	2	3	4	5
The users of crypto-assets are risk-takers.	()	()	()	()	()
Using crypto-assets sidesteps regulated banking systems.	()	()	()	()	()
Using crypto-assets supports illicit ecosystems.	()	()	()	()	()
Using crypto-assets is bad for the environment.	()	()	()	()	()

Q31 Have you ever felt physically unsafe because of holding crypto-assets?

() Yes, I've experienced a real physical threat.

() Yes, however I have not experienced a real threat yet.

() No

() I am not sure.

SECTION D: SECURITY PRACTICES

Q32 Please specify how often you undertake (or undertook) the following security practices.

	never	**occassionally**	**regularly**
I store(d) my crypto- assets in a reputable online wallet or exchange.	()	()	()
I back(ed) up my crypto wallet.	()	()	()
I generate(d) multiple backups of my crypto wallet.	()	()	()
I encrypt(ed) backups for additional security.	()	()	()
I keep (kept) my hardware wallet and its backup key separately.	()	()	()
I enable(d) a multiple-factor authentication for my online account(s).	()	()	()
I disconnect(ed) from the Internet before creating private keys.	()	()	()
I use(d) a multi-signature crypto wallet out of security concerns.	()	()	()
I store(d) private keys differently depending on the purpose and amount of crypto-assets.	()	()	()
I create(d) backups for my crypto wallet.	()	()	()
A device I use(d) to access my crypto-assets has/had a unique password.	()	()	()
A device I use(d) to access my crypto-assets is/was equipped with the latest malware protection.	()	()	()
A device I use(d) to access my crypto-assets is/was not used by anyone else.	()	()	()
A device I use(d) to access my crypto-assets is/was not connected to the Internet.	()	()	()
A device I use(d) to access my crypto-assets is/was kept in a physically secured location.	()	()	()

SECTION E: SECURITY EFFICACY

Q33 Please indicate to what extent do you agree with the following statements. *(1 - fully disagree, 5 - fully agree)*

	1	2	3	4	5
I am able to protect my private keys from being stolen.	()	()	()	()	()
I am able to prevent unauthorized access to my crypto wallet.	()	()	()	()	()
I have technical skills and time to secure and prevent the theft of my crypto-assets.	()	()	()	()	()
I find it easy to secure my crypto wallet.	()	()	()	()	()

Q34 Please indicate how costly are the following measures in terms of required time and money. *(1 - not costly at all, 5 - very costly)*

	1	2	3	4	5
Securing crypto-assets	()	()	()	()	()
Keeping security measures for crypto-assets up-to-date	()	()	()	()	()
Security investments into equipment	()	()	()	()	()
Staying informed about secure crypto wallets	()	()	()	()	()
Spending crypto-assets from secure crypto wallets	()	()	()	()	()

SECTION F: SECURITY PERCEPTIONS

Q35 To what extent do you agree with the following statements?

(1 - fully disagree, 5 - fully agree)

	1	2	3	4	5
Losing crypto-assets would require serious efforts from me to compensate for the loss.	()	()	()	()	()
Losing crypto-assets would likely cause me severe stress.	()	()	()	()	()
Losing crypto-assets would likely negatively impact my daily life.	()	()	()	()	()
Losing crypto-assets would significantly compromise my financial situation.	()	()	()	()	()
My crypto wallet is at risk of being compromised.	()	()	()	()	()
The risk of my crypto wallet being compromised is high.	()	()	()	()	()
It is likely that someone abuses private keys of my crypto-assets.	()	()	()	()	()
It is likely that someone makes criminal transactions in my account.	()	()	()	()	()
Self-control of my private keys reduces the risk of losing crypto-assets.	()	()	()	()	()
A well-known and regulated exchange is capable of securing my crypto-assets.	()	()	()	()	()
An exchange that checks user identities is in a good position to secure my crypto-assets.	()	()	()	()	()
An exchange that monitors the origins of incoming transactions is in a good position to secure my crypto-assets.	()	()	()	()	()
Strong passwords help me to protect my online accounts better.	()	()	()	()	()
Not storing passwords in plain text helps me to protect my crypto-assets better.	()	()	()	()	()

Backups help me to reduce the risk of losing crypto-assets.	()	()	()	()	()
Multi-factor authentication reduces the risk of my online accounts being compromised.	()	()	()	()	()
Minimizing time my crypto-assets stay in online crypto wallets or exchanges helps me to reduce the risk of losing crypto-assets.	()	()	()	()	()
Separating long- and short-term crypto-assets (e. g., in cold and hot storages) helps me to reduce the risk of losing crypto-assets.	()	()	()	()	()

SECTION G: DEMOGRAPHICS

Q36 What is your gender?

() Male
() Female
() Non-binary/third gender
() Prefer to self-describe: _____
() Prefer not to answer

Q37 What is your current occupation?

() Student
() Skilled manual worker
() Employed position in a service job
() Self-employed/freelancer
() Unemployed or temporarily not working
() Retired or unable to work through illness
() Employed professional
() Other
() Prefer not to answer

Q38 What is the highest degree you have received or the highest level of education you have completed?

() Less than high school
() High school incomplete
() High school graduate (or an equivalent)
() College or associate degree
() Bachelor's degree
() Master's degree
() Doctorate degree
() Other postgraduate or professional degree
() Prefer not to answer

Q39 Which categories describe you? Please select all that apply to you.
() American Indian or Alaska Native
() Asian
() Black or African American
() Hispanic, Latino or Spanish Origin
() Middle Eastern or North African
() Native Hawaiian or Other Pacific Islander
() White
() Some other race, ethnicity, or origin, please specify: _____
() Prefer not to answer

Your opinion matters!

Thank you very much for completing our survey, you have really helped us a lot! If you choose to receive the Amazon gift card in the lottery, please provide your email address below. You can also indicate whether you are interested in a summary of the survey results or are willing to be contacted for a follow-up survey.

If you have any comments on the survey or want to provide additional information or feedback to us, please use this open text field:

_____

How would you like to be compensated in case you win the lottery?
() Amazon gift card
() Donation to WWF
() Donation to Red Cross
() Donation to Unicef

Would you be interested in being contacted?
() I am interested in the survey results.
() I am interested in a follow-up survey.

Please enter your email address for us to contact you:

_____

B.2 Construct scale items

Table B.29: 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.	[106, 114, 226]	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.	[114], 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.	[106, 114, 226]	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.	[61]	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.

Appendix C

UX Issues Investigation

C.1 Coding Guide

The following instructions were used during the manual classification:

> We will use three classes for the manual classification of reviews. Reviews that describe a detailed cryptocurrency wallet feature will be considered *relevant to cryptocurrency UX*, reviews that describe general UX without addressing a specific feature unique to cryptocurrencies will be considered *relevant to general UX*, and reviews that are not relevant to UX at all will be classified as *irrelevant to UX*. After having the classification output, we will then qualitatively code those reviews that are relevant to cryptocurrency UX. For clarification purposes, we use the following definition of UX [109]: "The extent to which a product can be used by specified users to achieve specific goals, with effectiveness, efficiency and satisfaction in a specified context of use."
>
> Examples of reviews that were found to be relevant/irrelevant:

Table C.1: Examples of classified reviews

Class	Review Text	Explanation
Relevant to Cryptocurrency UX	Uses biometrics, super secure, super fast, supports multiple wallets. Syncs easily with the desktop version. Great app overall.	Review mentions syncing with the desktop app and multiple wallets as good features.
Relevant to Cryptocurrency UX	Covers a ton of coin!	Review mentions the support of many cryptocurrencies.
Relevant to Cryptocurrency UX	The app looks nice and is pretty easy to navigate. Yet, I can receive ether, but cannot send ether no matter what changes I make to the gas sliders. Pointless to have something you cannot move.	Review mentions the inability to send transactions.
Relevant to General UX	Good App and Secured one	This review is not specific to cryptocurrency wallets, but to apps in general.
Relevant to General UX	The application does not open after upgrade! iPad Air 2 iOS 8.4	This review is not specific to cryptocurrency wallets, but to apps in general.
Irrelevant to UX	Bitcoin is the future.	No relevance to the app or UX.
Irrelevant to UX	Use referral code to get bonus mining reward [redacted]. Mine with IOS, Android or PC!.	No relevance to the app or UX.

For further rounds ensure that users mention specific features that are good/bad so we can derive guidelines on how to design future software wallets. Information that the app is just good/bad is not explicit enough. Generally, our goal is to identify features of apps that have a positive/negative effect on the UX. Ease of use can have a positive influence, whereas difficult onboarding will have a negative one.

C.2 Review Corpus Metadata

The following two plots show the distributions of the review age and lengths.

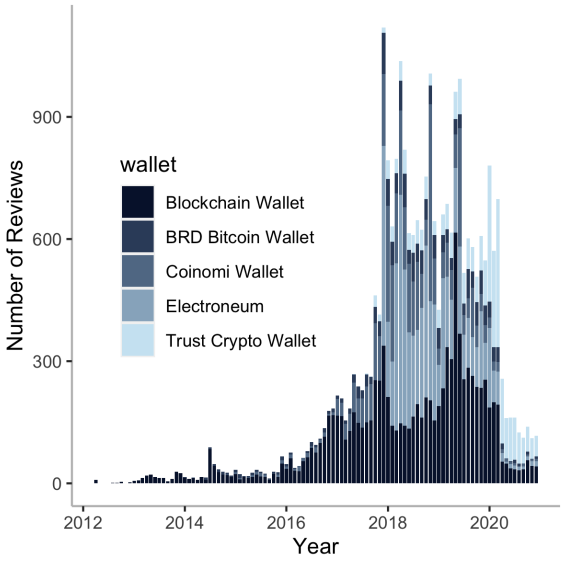


Figure C.1: Review age aggregated by month

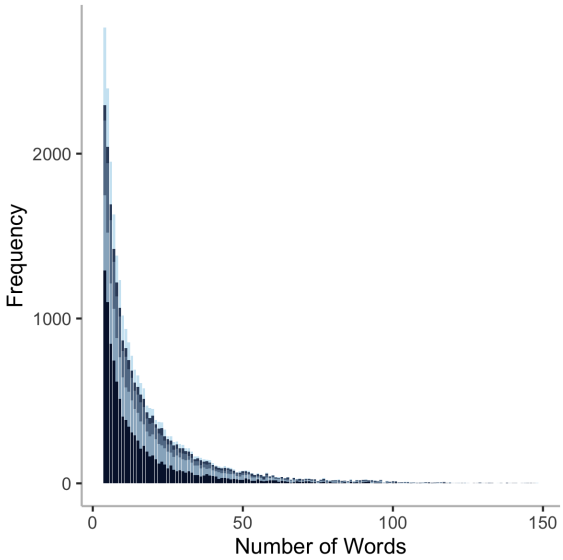


Figure C.2: Review length in words