Surviving the Cryptojungle: Perception and Management of Risk Among North American Cryptocurrency (Non)Users

Artemij Voskobojnikov, Borke Obada-Obieh, Yue Huang, and Konstantin Beznosov

University of British Columbia, Vancouver, Canada
{voskart, borke, huang13i, beznosov}@ece.ubc.ca

Abstract. With the massive growth of cryptocurrency markets in recent years has come an influx of new users and investors, pushing the overall number of owners into the millions. At the same time, the number of distinct cryptocurrencies has exploded to over 4,900. In this burgeoning and chaotic "cryptojungle," new and unexplored incentives and risks drive the behavior of users and non-users of cryptocurrencies. While previous research has focused almost exclusively on Bitcoin, other cryptocurrencies and utility tokens have been ignored. This paper presents findings from an interview study of cryptocurrency users and non-users ($N = 20$). We specifically focus on their perceptions and management of cryptocurrency risks as well as their reasons for or against involvement with cryptocurrencies. Our results suggest that associated risks and mitigation strategies (among other factors) might be specific to a particular crypto-asset and its application area. Further, we identify misunderstandings of both users and non-users that might lead to skewed risk perceptions or dangerous errors. Lastly, we discuss ways of aiding users with managing risks, as well as design implications for coin management tools.

1 Introduction

Cryptocurrencies have come a long way since the introduction of Bitcoin in 2009 [24]. Emerging technologies, such as Ethereum or EOS, allow the issuance of tokens, and this was one of the reasons for the rapid expansion of the domain. Nowadays, the resulting "cryptojungle" entails close to 5,000 different cryptocurrencies and tokens [12] with wide-ranging application areas.

Despite prior research on security risks in the blockchain domain, little is known about users' perception and management of risk. The main focus in the literature has been on identifying potential attack vectors and risk scenarios [20, 18], without taking the respective end-users into account. While Sas et al. [25] present some risks experienced by Bitcoin users, risk management has not been investigated any further. Addressing this knowledge gap will inform the development of more effective technology support for the users of cryptocurrencies and tokens.

It is also vital to understand informed non-users' perceptions of the risks associated with cryptocurrencies. Gao et al. [16] were the first to study non-users of Bitcoin and identified *lack of perceived usefulness* and *lack of understanding* as two reasons for non-involvement. Unlike Gao et al., who interviewed participants with very limited knowledge about cryptocurrencies, our goal was to recruit *informed non-users* who had considered involvement with cryptocurrencies but had decided against it. Potential findings could then be leveraged by industry to ease the onboarding process and eventually facilitate adoption.

To investigate how cryptocurrency users and non-users perceive and manage risks, we conducted semi-structured interviews. We recruited 20 participants from the metropolitan area of Vancouver, Canada, comprising 11 users and 9 non-users. Some interviews were in person and others via telephone. An iterative coding approach based on Grounded Theory [14] was applied by three researchers, and data was collected until theoretical saturation was reached.

Several themes emerged when we probed our participants more deeply about risks in the cryptocurrency domain. User participants identified a variety of risks, such as scam coins and questionable exchanges, but only a few of those risks resulted in actual losses. Further, *risk acceptance* turned out to be a prominent risk-management technique employed by users. Non-users, on the other hand, were concerned with the potential implications of involvement with cryptocurrency. Amongst other concerns, our participants mentioned the possibility of being judged by their social circle, as well as the poor usability of exchanges and tools. Our findings suggest that perceived risks depend on the particular asset as well as the individual's reasons and motivations for using it. The perceived risk severity appears to be linked to the amount invested.

Lastly, we identified our participants' misunderstandings. Most were not knowledgeable about the underlying cryptography, including private and public keys, while some non-users had a skewed risk perception. For example, the latter were concerned with governments tracing potential cryptocurrency transactions back to them. While the implications of misperceptions differ, both users and non-users are affected. For users, misunderstandings can lead to monetary losses, and non-users might decide against any involvement at all because they have assessed the risks incorrectly.

One of the main issues to emerge was the usability of coin management tools (CMTs). In our study, both users and non-users reported having faced challenges when looking into purchasing or using cryptocurrencies, with some participants saying that the usability of current CMTs posed a significant risk and barrier to entry. Some users had addressed transactions incorrectly or failed to make them in the first place, and non-users reported being overwhelmed by the onboarding process of exchanges and the overall number of available CMTs.

To summarize, our contributions are as follows:

- We conducted the first investigation of risks perceived by users and informed non-users of cryptocurrencies.
- We identified factors linked to risk perception and mitigation in the cryptocurrency domain.

– We identified misunderstandings in both users and non-users that can lead to monetary losses or non-involvement, respectively.

2 Background

2.1 Cryptocurrencies and Utility Tokens

Bitcoin and cryptocurrencies in general make use of public-key cryptography and consequently force users to deal with this in one way or another. Traditionally, cryptocurrency wallets can be seen as means for storing one or more private and public cryptographic key pairs. Wallet addresses consist of hashes of the respective public cryptographic keys, and transactions are cryptographically signed transfers of funds from one public key to another. Unlike in centralized payment systems, however, the responsibility is shifted onto the user, and payments can only be successfully concluded by using a private key.

Besides private keys, wallets can also be accessed by using mnemonics. These consist of 12 to 24 words in the case of the BIP-39 standard [1], which are used to deterministically create key pairs for a cryptocurrency wallet. To further enhance the security, a passphrase can be used as a salt, thus guaranteeing that adversaries who know the mnemonic will still be denied access to the funds. This option is supported by many wallet providers [7].

Nowadays, the application areas of cryptocurrencies are wide-ranging and go beyond the initial vision of an alternative payment system. Emerging technologies, such as Ethereum, allow the issuance of tokens, which exist on the respective blockchain and are used within applications. Examples of such applications are social networks and games. Some participants in our study used the terms *cryptocurrencies* and *tokens* interchangeably. In the following sections, we make distinctions where applicable and otherwise use the term *crypto-assets* when referring to both of them.

2.2 Coin Management Tools

A wide range of options exist when it comes to storing crypto-assets. Such wallets, or coin management tools, as Krombholz et al. [21] defined them, emerged. In the case of hosted wallets, the responsibility is shifted from the users to the CMT providers. To use hosted wallets, users are often asked by providers to verify their identities in a so-called know-your-customer (KYC) process to combat money laundering and fraud. Prominent examples of hosted wallets are major exchanges, such as Binance, which do not give users access to the private keys. This abstraction, while arguably making the exchange more usable, poses a risk for users, as they might lose assets in the case of shutdowns or hacks, which has indeed happened (Mt.Gox [10], QuadrigaCX [11]).

Besides transferring funds to third parties, users also can choose to be solely responsible for the management of their crypto-assets. Here, two options exist: *hot wallets* and *cold wallets*. Hot wallets are connected to the internet and can

be mobile applications, desktop wallets, online wallets, or utility platforms run by blockchain start-ups. Compared to hot wallets, cold wallets can provide a better level of protection. Hardware wallets, which are specialized cold wallets, often store private keys in the secure key storage provided by microcontrollers. However, cold wallets are kept offline. Paper wallets with printed private and public keys, as well as USB sticks with key files, also fall under this category.

3 Related Work

3.1 Risks in the Cryptocurrency Domain

When users interact with blockchain-based technologies, they are directly or indirectly exposed to a significant number of risks. Bonneau et al. [9] 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 [23, 5]. Third-party sites can also pose a risk to users. Goldfeder et al. [17] 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. However, other crypto-assets have not yet been investigated. Both Böhme et al. [8] and Grant et al. [18] provide comprehensive overviews of Bitcoin risks, and Kiran et al. [20] 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. Here, Sas et al. [25] were the first to uncover some reasons for monetary losses.

Perception of risks associated with Bitcoin can be found in the literature [21, 4]. While users were asked to assess the severity of risk scenarios in [21], Abramova et al. [4] investigated factors influencing risk perception among Bitcoin users. Results suggest that Bitcoin 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 how well aware users are of these risks and what controls they personally apply for mitigation. We further believe that perceived risks and mitigation techniques depend on the crypto-asset and are influenced by factors unidentified in previous studies.

3.2 Concerns Regarding Usable Security and Privacy

In addition to crypto-assets being lost due to technological vulnerabilities, user-induced errors are very common. Bitcoin is theft resistant by design, and assets can only be compromised by private key leakages [13]. Eskandari et al. [15]

conducted a cognitive walkthrough for various Bitcoin key management systems. Their findings suggest that the metaphors being used can often be unclear for end-users, leading them to make dangerous errors.

Empirical evidence of users experiencing such dangerous errors was first offered by Krombholz et al. [21]. Out of the 990 participants in an online survey, almost 23% indicated they had lost Bitcoins. Of those who had, 43% indicated the loss had been their own fault.

Gao et al. [16] conducted the first purely qualitative study investigating the mental models of both users and non-users of Bitcoin. The main contributions of the study were to identify misconceptions about privacy and security properties, as well as a general lack of understanding in both users and non-users about the underlying technology.

Further investigating users' and non-users' mental models of risk should make it possible to address inconsistencies that could lead to dangerous errors. Such errors pose a risk and can lead to the loss of Bitcoins, as reported by Sas et al. [25]. It is therefore of interest to understand the behavior of users when it comes to the protection of their crypto-assets. By expanding the study beyond Bitcoin, and investigating security behaviors regarding crypto-assets in general, it should be possible to understand what factors influence users in their decision making.

4 Methodology

In this section we describe our recruitment process, the interview procedure itself, as well as the coding methodology and process.

4.1 Recruitment and Participants

We recruited participants aged 19 and older from the metropolitan region around our university. Users of crypto-assets were recruited through professional blockchain LinkedIn groups, our department's graduate reading seminar, a mailing list, and the community Slack channel of a blockchain club at our university, as well as a meetup group focused on decentralization. The recruitment notice can be found in Appendix A. Non-users were recruited with the help of community managers of a local cryptocurrency 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.

4.2 Interview Procedure

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

- **RQ1:** What are the current usages of cryptocurrencies?
- **RQ2:** How do owners manage their cryptocurrencies?
- **RQ3:** What is the perception of cryptocurrency-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 was approved by our university's research ethics board.

4.3 Coding Procedure

An iterative coding approach based on Grounded Theory [14] was applied. Three researchers independently performed open coding of the interview transcripts, and the results were discussed and added to a shared codebook once the researchers' codes converged. Axial coding followed, whereby themes and concepts emerged. Again, the resulting themes were discussed among the four researchers to ensure reliability. The percentage agreement for three raters was 90%, and we stopped recruiting once it became clear that we had reached code saturation (see Appendix C). Throughout the study, the interviews were recoded several times after our codes converged, and the interview guide was adjusted based on our intermediate findings [14].

4.4 Limitations

As with all qualitative investigations, the results of this study are not necessarily generalizable to the whole population of cryptocurrency users and informed non-users. Our aim, however, was to interview a diverse sample. We ensured its diversity by recruiting through multiple channels and including participants from diverse backgrounds, including investors, miners, consultants, and blockchain developers. Since we investigated users' security and privacy behaviors, it is 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 of our participants were in North America. While this geographical restriction might have impacted our results, we strove to recruit a diverse sample. Compared to previous qualitative studies [16, 25, 19], our sample was more diverse in terms of gender, education, occupation, and age.

5 Results

5.1 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 Appendix D.

5.2 Motivation for Using Crypto-Assets (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 [16, 21], participants in our study broke this down into short-term and long-term investments. PU6[1] considered crypto-assets, and Bitcoin 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 explaining: *"I feel like I'm holding a lot of bags still [...] I own Bitcoin, I own Ethereum, EOS, MakerDao [...] and Power Ledger."*

Participants also indicated having used cryptocurrencies to purchase goods. Some of these goods were physical and others digital. PU1 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 Bitcoin."* None of the participants indicated they had purchased illicit goods. One user described having gotten into the cryptocurrency space through a friend who was a drug dealer at the time and was using cryptocurrencies.

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

Unlike speculators, who deal mostly with exchanges, participants who use cryptocurrencies as a medium of exchange interact with various parties, such as merchants. Therefore, the risks also differ. Some respondents used cryptocurrencies as alternatives to banks. PU1, PU4, and PU6 all reported instances where banks fell short in their eyes, with PU6 saying: *"the one thing that intrigues me about cryptocurrencies is that you're your own bank."*

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.'"*

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

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 cryptocurrency, 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.

5.3 Reasons for Not Using Crypto-Assets (RQ1)

During interviews with non-users, several reasons for their non-involvement emerged. Negative views about cryptocurrencies were prevalent among non-users. PN1,[2] PN2, PN3, PN5, PN6, and PN8 associated cryptocurrencies with the drug trade and other illegal activities, with PN3 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 cryptocurrencies, 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 cryptocurrencies not making sense from a financial standpoint, with PN5 stating the belief that the *"Bitcoin price was about $20,000 and there was not much room for an increase."*

The ability of the government to trace all cryptocurrency transactions was another stumbling block. PN3 stated they would consider getting cryptocurrencies *"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 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 cryptocurrencies.

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 explained: *"Well, if it's not regulated, I just feel like it could be just so volatile."*

When trying to enter the cryptocurrency domain, non-users had experienced barriers to entry. PN1 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 cryptocurrencies through mining but faced challenges: *"I tried [mining] but I realized that all [...] the computers [are] specifically made for mining Bitcoin. So maybe my personal computer is really good [but for mining] it doesn't really work."*

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

5.4 Handling of Crypto-Assets (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 cryptocurrency 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 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 Bitcoin more securely than other crypto-assets. PU4 and PU6 stored Bitcoin in hardware wallets, with PU4 breaking down investments into two categories: *"Long-term holdings like Bitcoin—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 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 cryptocurrencies solely to trade them on exchanges to gather more Bitcoin. 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 Bitcoin [is stored in a hardware wallet]; shitcoins all stay on the exchanges till they make me Bitcoin and then [Bitcoins] get sent back [to my hardware wallet]."*

Users 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 explained specific troubles with MetaMask: *"You have to enter a gas amount in some other currency that*

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

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 cryptocurrencies, 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."*

5.5 Risks

Besides commonly known risks (see Appendix E), 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.

Perceived Risks (RQ3) Non-users were afraid of being judged by their social circle if they purchased cryptocurrency. PN6 explained: *"Cryptocurrency was initially used on the black markets, right, and if you tell people that you have some Bitcoin or other cryptocurrencies, people will think that maybe you are buying something illegal."*

Personal safety associated with cryptocurrency 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 cryptocurrency 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 cryptocurrency 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 cryptocurrency

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 Bitcoin 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 (RQ3) Losses were attributed to only a few risks, despite our participants mentioning many more. However, none of the participants reported having had their cryptocurrencies 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 cryptocurrency due to their own errors. PU11 explained: *"I definitely have one wallet with a small amount of Bitcoin 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 (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 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 Appendix F.

6 Discussion

Participants' three major reasons for using crypto-assets were speculation, exchange, and utility. Each particular application area exposes the respective user to new CMTs, such as software wallets, hardware wallets, payment processors, and utility platforms. User interfaces as well as underlying technological features differ according to the CMT and consequently expose users to different risks. Hosted wallets, such as exchanges, do not allow users to access their private keys, which in the case of a shutdown results in monetary loss. Cold wallets, on the other hand, while not affected by shutdowns are often more complex to

use, as reported by our participants. Our findings suggest that usage scenarios were important factors linked to the user experience (UX), as well as risk perception and management.

All user participants had used exchanges at some point during their involvement. One voiced a willingness to accept the risk of losing crypto-assets in order to make gains on questionable exchanges with so-called "shitcoins." Four users accepted the risk of storing their crypto-assets on exchanges without having direct access to their private key.

Risk perception also seemed to depend on how much participants valued the respective crypto-asset. Here, we consider the amount invested in the particular asset. Our user participants stored their long-term holdings in the form of Bitcoin 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.

6.1 Misconceptions and Usability Barriers

Users had dangerous knowledge gaps and misconceptions when it came to the key building blocks of cryptocurrencies. 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 cryptocurrencies are mainly used to purchase illicit drugs. While this was one of the main uses of Bitcoin in its early days [6], the applications nowadays are wide ranging. Non-users also discussed the notion of cryptocurrency 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 cryptocurrencies' 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 cryptocurrencies because of the two pairs of keys: private and public. We therefore believe that findings on usability issues with Bitcoin key management tools [15] and the identified risks affecting Bitcoin usability [13] are not necessarily applicable to other crypto-assets and their applications.

6.2 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. Further investigation is needed to

reveal other factors related to risk perception and to further our understanding of the risk-management practices among users and informed non-users.

New crypto-assets bring new risks for users. The vast majority of our user participants owned multiple crypto-assets, with PU7 owning as many as 50. Such variety can be dangerous, as different crypto-assets pose different risks and challenges for their respective users. For example, initial coin offerings (ICOs) are not always created in good faith [2], and utility tokens can end up being pyramid schemes [3], as reported by PU4, PU5, and PU6. While risks associated with Bitcoin are fairly well documented [18, 20, 15, 8], other crypto-assets have thus far been ignored by the research community.

Design recommendations to combat some of the risks can be found in the literature. Authorized exchanges were proposed by Sas et al. [25] 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. Sandboxes allowing newcomers to first get familiar with the terms and technology, as well as more guidance from CMT providers could especially help new users overcome existing fears of the unknown, as reported by many of our informed non-users and in previous research [16].

Personalization would be another way to support users [22]. Perhaps wallet providers could create separate user profiles for beginners and experts, allowing users to select a level of abstraction. For example, advanced transaction settings would only be displayed for experienced users, whereas new users would only see the bare minimum. Simpler terms—e.g., "transaction fees" instead of "gas price"—could further improve the user experience for newcomers, making involvement in the domain less foreign.

6.3 Implications for Theory and Practice

Our investigation of crypto-assets other than Bitcoin has revealed risks and usability concerns previously undocumented in the literature. Usability research on blockchain-based technologies has been Bitcoin-centric [21, 16, 25, 20]. While Bitcoin is still the most popular cryptocurrency, our results suggest that associated risks do depend on the application area and crypto-asset. Pyramid schemes

in the form of mining pools, unregulated ICOs, "shitcoins," and tokens all pose new risks to both existing and new users and can lead to monetary losses.

When looking at crypto-assets, one also has to consider CMTs, as they are vital to UX. Our participants reported owning as many as 50 different currencies, and while exchanges support a variety of tokens, not all software wallets do. Such wallets support different subsets of crypto-assets, and the included features are also wide ranging. Newcomers looking into purchasing cryptocurrency can easily be overwhelmed by the number of different wallets, as was the case for PN1.

Monetary losses due to self-induced errors were reported by multiple user participants. By creating more usable and intuitive software wallets, possibly employing terms from payment platforms already familiar to users, one might be able to decrease the chances of losing crypto-assets due to self-induced errors. By also adding two-factor authentication, similar to some online banking platforms, it would be possible to reduce the risk of users sending crypto-assets to an incorrect address, which some participants reported having done.

Some informed non-users seemed to hold negative beliefs about cryptocurrency use. Educating potential new users about other application areas for blockchain-based technologies could help reduce the negative views and social risks associated with cryptocurrency involvement.

7 Conclusion

We conducted semi-structured interviews to further an understanding of how users and non-users perceive and manage risks related to 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 skewed risk perceptions and 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.

Acknowledgements

This research has been supported in part by a gift from Scotiabank to UBC and by an NSERC Engage Grant (with Symetria), #EGP538930-19. We would like to thank members of the Laboratory for Education and Research in Secure Systems Engineering (LERSSE), who provided their feedback on the reported research and earlier versions of the paper. We thank our anonymous reviewers for all the feedback and suggestions they provided to improve the paper.

References

1. BIP 39 Standard. https://github.com/bitcoinbook/bitcoinbook/blob/
2. Cointelegraph: ICO Scams. https://cointelegraph.com/news/new-study-says-80-percent-of-icos-conducted-in-2017-were-scams (2018), accessed: 2019-09-23
3. Cointelegraph: Ponzi Schemes. https://cointelegraph.com/news/from-ponzi-schemes-to-ico-exits-ethereums-blockchain-has-been-the-platform-of-choice-for-scammers (2019), accessed: 2019-09-23
4. Abramova, S., Böhme, R.: 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)
5. Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T., Capkun, S.: Evaluating User Privacy in Bitcoin. In: Sadeghi, A.R. (ed.) Financial Cryptography and Data Security. pp. 34–51. Springer Berlin Heidelberg, Berlin, Heidelberg (2013)
6. Bitcoin.com: Illegal Activity No Longer Dominant Use of Bitcoin: DEA Agent. https://news.bitcoin.com/illegal-activity-use-bitcoin-dea-agent/, accessed: 2019-02-28
7. Blockplate: The BIP39 (Mnemonic Seed) Wallet List. https://www.blockplate.com/blogs/blockplate/list-of-bip39-wallets-mnemonic-seed (2019), accessed: 2019-07-20
8. Böhme, R., Christin, N., Edelman, B., Moore, T.: Bitcoin: Economics, Technology, and Governance. Journal of Economic Perspectives **29**(2), 213–38 (2015)
9. Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J.A., Felten, E.W.: SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In: 2015 IEEE Symposium on Security and Privacy. pp. 104–121 (May 2015). https://doi.org/10.1109/SP.2015.14
10. 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
11. 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
12. CoinMarketCap: Distinct Cryptocurrencies. https://coinmarketcap.com/all/views/all/ (2019), accessed: 2019-09-15
13. 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)
14. Corbin, J., Strauss, A.: Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory. SAGE Publications (2014), https://books.google.ca/books?id=hZ6kBQAAQBAJ
15. Eskandari, S., Barrera, D., Stobert, E., Clark, J.: A First Look at the Usability of Bitcoin Key Management. In: NDSS Symposium 2015. Internet Society (2015)
16. Gao, X., Clark, G.D., Lindqvist, J.: 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. pp. 1656–1668. CHI '16, ACM, New York, NY, USA (2016). https://doi.org/10.1145/2858036.2858049, http://doi.acm.org/10.1145/2858036.2858049

17. Goldfeder, S., Kalodner, H., Reisman, D., Narayanan, A.: When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies. Proceedings on Privacy Enhancing Technologies (4), 179–199 (2018)
18. Grant, G., Hogan, R.: Bitcoin: Risks and Controls. Journal of Corporate Accounting & Finance **26**(5), 29–35 (2015)
19. Khairuddin, I.E., Sas, C., Clinch, S., Davies, N.: Exploring Motivations for Bitcoin Technology Usage. In: Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems. pp. 2872–2878. ACM (2016)
20. Kiran, M., Stanett, M.: Bitcoin Risk Analysis. NEMODE Policy Paper (2015)
21. Krombholz, K., Judmayer, A., Gusenbauer, M., Weippl, E.: The Other Side of the Coin: User Experiences with Bitcoin Security and Privacy. In: Grossklags, J., Preneel, B. (eds.) Financial Cryptography and Data Security. pp. 555–580. Springer Berlin Heidelberg, Berlin, Heidelberg (2016)
22. Kumar, R.L., Smith, M.A., Bannerjee, S.: User interface features influencing overall ease of use and personalization. Information & Management **41**(3), 289–302 (2004)
23. Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M., Savage, S.: A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. In: Proceedings of the 2013 Conference on Internet Measurement Conference. pp. 127–140. IMC '13, ACM, New York, NY, USA (2013). https://doi.org/10.1145/2504730.2504747, http://doi.acm.org/10.1145/2504730.2504747
24. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System. http://bitcoin.org/bitcoin.pdf (2008), accessed: 2019-02-28
25. Sas, C., Khairuddin, I.E.: 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. pp. 6499–6510. CHI '17, ACM, New York, NY, USA (2017). https://doi.org/10.1145/3025453.3025886, http://doi.acm.org/10.1145/3025453.3025886

Appendices

A Recruitment Notice

Fig. 1. Recruitment notice

B Interview Questions

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

B.1 Users of Cryptocurrencies

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?

B.2 Non-Users of Cryptocurrencies

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)

C Coding Saturation Graph

The following graph presents the number of codes after each interviewed study participant. The last three interviews did not yield new codes.

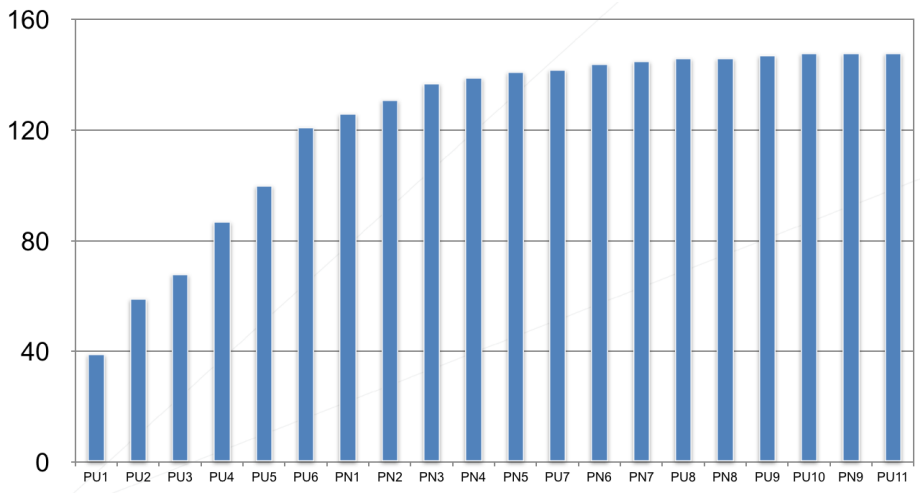

Fig. 2. Coding saturation

D Participant Demographics

Table 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 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

E Perception of Previously Documented Risks

High volatility was a concern for both users and non-users. Cryptocurrencies 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 cryptocurrencies 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 cryptocurrencies 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 cryptocurrency. PN5 mentioned that ICOs in particular can end up being scams and might lead to monetary 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.

The possibility of exchanges being shut down was a concern for those using them. Naturally, this may result in monetary losses, especially in the case of exit scams,[6] as happened with Mt.Gox and Bitgrail. PU5 summarized it as follows: *"Mt. Gox was a wake-up call to all of us. I didn't even see that coming. Thank*

[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/

[6] Exit scams are fraudulent practices that often include cryptocurrency founding teams or exchange operators stealing users' funds.

god they never approved my account. Uhm, I never saw that coming [...]. Cryptsy too was a surprise."

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 cryptocurrency] appreciated a year later, the person could just take it back."* Such losses have been reported in the community,[7] and it is generally not advisable to purchase second-hand hardware wallets.

Participants considered it risky to provide credit card details and personal information to third parties. When looking into cryptocurrencies, 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 cryptocurrencies could pose a social risk. PN6 mentioned that users of cryptocurrencies might be judged unfavorably: *"Cryptocurrency was initially used on the black markets, right, and if you tell people that you have some Bitcoin or other cryptocurrencies, people will think that maybe you are buying something illegal."* PU6 also recalled a similar scenario before owning cryptocurrencies: *"A friend told me about it in 2012. He was a drug dealer and [...] I originally told him to stay away from [cryptocurrencies] because it is associated with all this, like, assassination [...]."*

One user considered personal safety to be a risk associated with cryptocurrency ownership. 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."'*

Lastly, non-users presented their lack of understanding as a risk. PN2, PN3, and PN4 commented that by not understanding the technology, they would be putting themselves at risk, with PN4 saying: *"it seems like fake money, and I feel like it would be very risky to me, like, not knowing much about it."*

Interestingly, risk perception appeared to be linked to the amount of money invested. PU1, PU2, 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."*

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

F Schematic Overview of the Results

The following figure depicts the findings of the interview study. Based on our research questions we created five groups, *use cases*, *reasons against an involvement*, *perceived risks*, *reasons for losses*, and *risk management*. We use distinct colors for users and non-users and show relationships where appropriate.

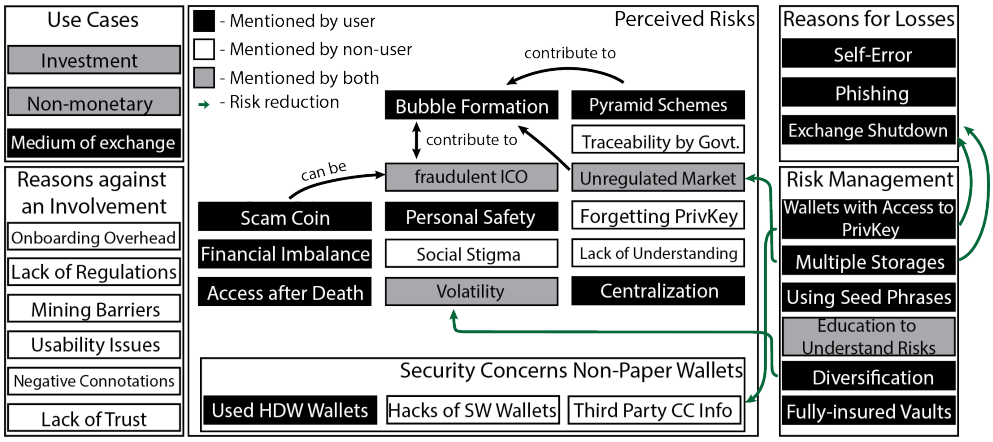

Fig. 3. Findings overview