Don't Lose Your Coin! Investigating Security Practices of Cryptocurrency Users

Michael Fröhlich
CDTM
Munich, Germany
froehlich@cdtm.de

Felix Gutjahr
LMU
Munich, Germany
felix.gutjahr@campus.lmu.de

Florian Alt
Bundeswehr University
Munich, Germany
florian.alt@unibw.de

ABSTRACT

In recent years, cryptocurrencies have increasingly gained interest. The underlying technology, Blockchain, shifts the responsibility for securing assets to the end-user and requires them to manage their (private) keys. Little attention has been given to how cryptocurrency users handle the challenges of key management in practice and how they select the tools to do so. To close this gap, we conducted semi-structured interviews (N=10). Our thematic analysis revealed prominent themes surrounding motivation, risk assessment, and coin management tool usage in practice. We found that the choice of tools is driven by how users assess and balance the key risks that can lead to loss: the risk of (1) human error, (2) betrayal, and (3) malicious attacks. We derive a model, explaining how risk assessment and intended usage drive the decision which tools to use. Our work is complemented by discussing design implications for building systems for the crypto economy.

Author Keywords

usable security, blockchain, cryptocurrency, key management

CCS Concepts

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

INTRODUCTION

Driven by the rise in popularity of cryptocurrencies, Blockchain technology is receiving increased interest from practitioners and researchers alike. By the end of 2019, the number of wallet users has grown to exceed 42 million [49]. A total of 4993 cryptocurrencies are tracked on http://coinmarketcap.com/, with a combined market capitalization exceeding 195 billion USD. Despite the large body of alternative coins, Bitcoin [42] remains by far the most widespread cryptocurrency, with a market capitalization of 130 billion USD [15].

While cryptocurrencies remain the predominant application of Blockchain technology, there is considerable ongoing development in both industry and research. Advocates of blockchain view the technology as potentially transformative [21]. Swan discusses three stages of blockchain evolution: Blockchain 1.0 as digital currency, Blockchain 2.0 as digital economy, and Blockchain 3.0 as digital society [48]. Efanov and Roschin discuss the all-pervasive impact of blockchain technology and propose use cases in the fields of art, science, education, public goods, culture, and communication [18]. Elsden et al. provide the first topology of Blockchain applications for HCI, identify seven overarching 'families' of Blockchain applications – underlying infrastructure, currency, financial services, proof-as-a-service, property and ownership, identity management and governance – and argue for an active role of the HCI community in the Blockchain domain [21].

At the same time, cryptocurrencies users still face major unsolved challenges: user interfaces suffer from usability issues [8, 22, 27, 37], there remain fundamental trust challenges [6, 26, 34, 44, 45], cryptocurrencies are complex to understand [21, 22] and have a high entry-barrier for people with less technical knowledge [31]. With more blockchain-based services emerging, it is important to understand which challenges people face – to ultimately design solutions around them and facilitate the development of more inclusive systems that allow users without deep technical knowledge to participate in the crypto economy of tomorrow.

A large part of the complexity originates from private / public key cryptography Blockchain builds on. It shifts the responsibility to securely manage private keys to the end-user. Cryptocurrencies today offer a valuable opportunity to investigate how users manage arising security challenges in practice. Previous research of key management in the context of cryptocurrencies focused on the available tools [3, 22] and providing a quantitative macro view of security practices of Bitcoin users [37]. However, there remains a lack of qualitative insight into the security practices of cryptocurrency users.

To address this, we conducted semi-structured interviews with 10 users, investigating their experiences and security practices using cryptocurrencies. We identified 3 themes through thematic analysis concerning (1) motivation, (2) risk assessment and (3) coin management tool (CMT) usage.

We found that users' knowledge and understanding of security practices influence the choice of CMTs, as does the intent to use as an asset or as a currency. Not all users have either the motivation or knowledge to securely manage their keys on their own. Custodial CMTs, abstracting key management away from the end-user, are seen as a convenient alternative

DIS2020, July 06–10, 2020, Eindhoven, NL
ACM 978-1-4503-6974-9/20/07…$15.00
DOI: http://dx.doi.org/10.1145/3357236.3395535

to self-managed solutions for some, while others categorically advise against them. Those managing their keys themselves go to great length to secure their backups resorting to redundancy and also more traditional means, such as bank deposit boxes. Contrary to previous research, financial interest revealed itself to be the predominant motivator of users. This indicates that cryptocurrencies have started to move beyond the early adopters (who did so out of ideological and technological interest) to a broader audience (who does so out of utility). From our findings, we distill a model explaining how the dynamics can be used to better understand cryptocurrency users and explore design implications for research and practice.

Contribution Statement: The main contributions of this work are (1) a qualitative investigation of current cryptocurrency users' security practices; (2) a model explaining how risk assessment and intended usage influence users' tool choice; and (3) design implications for designing future systems.

BACKGROUND AND RELATED WORK

Our work draws from several strands of research, most notably research on blockchain applications from an HCI perspective as well as research on security and privacy practices of users.

Blockchain: Terms and Concepts

Bitcoin is a digital currency introduced by pseudonymous identity Satoshi Nakamoto in 2008 as 'a Peer-to-Peer Electronic Cash System' [42]. Bitcoin allocates units of value by maintaining a public distributed ledger of all transactions, making use of a technology known as Blockchain. This ledger is maintained by a decentralized network and makes use of a novel method to reach consensus on the valid state of the ledger, without the need for a trusted central authority. The transaction validation within the system is called mining. Participating actors compete for transaction fees and a reward for being the first to validate a block of transactions [34].

A critical component for this to work is private / public key cryptography. Bitcoin addresses are pseudonymous and derived from the public key of an account. To prove ownership, transactions are signed with the private key of the sending account to be accepted by the system. Knowledge of a private key grants access to the associated funds. Loss of a private key results in loss of access to those funds. Owning cryptocurrency in reality means, owning private keys to specific accounts on the public blockchain. Consequently, it is a critical task for users to maintain and secure these keys. This is done with cryptocurrency clients, commonly known as wallets [22].

Since the introduction of Bitcoin, a substantial number of alternative cryptocurrencies have been introduced. Bonneau et al. provide a first systematic exposition of these second-generation cryptocurrencies [10]. Initially, mining was the only way to obtain cryptocurrencies. Today, there are many exchanges that allow users to buy, sell, and exchange these cryptocurrencies. Some of these cryptocurrencies aim to provide additional functionality, enabling 'Smart Contracts' and ultimately 'Decentralized Autonomous Organizations (DAOs)'. Ethereum, one of the most advanced projects, aims to 'to provide a blockchain with a built-in fully fledged Turing-complete programming language' [14].

There is a growing body of research surrounding Blockchain technology, investigating the potential impact it could have on future use cases. Swan's discussion on the stages of blockchain development – Blockchain 1.0 as digital currency, Blockchain 2.0 as digital economy, and Blockchain 3.0 as digital society – is picked up by Elsden et al. and Efanov and Roschin [18, 21, 48]. In an aim to create the first topology of Blockchain applications for the HCI community, Elsden et al. cataloged over 200 applications of Blockchain and identified 7 overarching 'families': Underlying Infrastructure, Currency, Financial Services, Proof-As-A-Service, Property and Ownership, Identity Management and Governance. They base their topology on applications available or in development today and discuss specific use cases in depth, including examples [21]. Efanov an Roschin describe application use cases beyond currency and financial use i.e. in the fields of art, science, education, public goods, culture and communication and expand on M2M interactions in the context of the Internet of Things (IoT) and Digital Identity [18].

While the concept of a blockchain-based 'Digital Economy' may seem like in a distant future, the concept of a machine-to-machine (M2M) electrical market is already being explored [2, 47]. Wu et al. showed the feasibility of using smart contracts to manage the demand side of a grid by simulation [51].

Blockchain and HCI

There is an emerging body of research dealing with blockchain in HCI. Elsden et al. provide the first broader summary on Blockchain research in the HCI community [21].

Experiences and Motivation

Several publications report on the experiences and motivations of Bitcoin users [27, 36, 37, 44]. Sas and Khairuddin focused on Bitcoin-related practices in the context of a developing country at the example of Malaysian Bitcoin users [36, 44]. Gao interviewed both users and non-users of Bitcoin in the US [27]. Krombholz presents a survey of 990 Bitcoin users, complemented by interviews with frequent users [37].

While the motivation of users is reported in most instances, results are difficult to compare as there is no common taxonomy. Khairuddin et al. report the 'Oncoming Monetary Revolution', 'Empowerment Associated With the Use of a Decentralized Cryptocurrency' and 'Perceived (Material) Value' [36]. Later, Sas and Khairuddin reduce motivation to 'Economic Rationale', subsuming 'distrust in financial institutions', 'security' and 'speculation' [45]. Krombholz et al. identified 'Decentralized nature' and 'curiosity' as main motivators [37].

Trust an Values

Sas and Khairuddin further explore the role of trust in the context of Bitcoin, arguing for research into technological, social and institutional trust as well as stakeholder groups (miners, users, exchanges, merchants, governments) in the context of Bitcoin [44]. They identified 'the risk of insecure transactions' dealing with 'dishonest traders' as the main trust challenge for Bitcoin users [45] and further explore the trust challenges of miners [35]. Auinger and Riedl argue that Blockchain systems, such as Bitcoin, are not purely technical systems, but socio-technical systems and thus not trust-free technologies.

They propose a trust framework similar to the one by Sas and Khairuddin, with focus on the trust questions users have to consider when using, buying, selling and owning Bitcoin [6]. Lustig and Nardi explored the concept of algorithmic authority in Bitcoin online communities, identifying considerable variance in how participants viewed the cryptocurrency and what they valued it for. They concluded that trust in algorithms cannot entirely substitute trust in humans [39].

Key Management

Key management has been a topic of interest in usable security research since Whitten and Tygar first investigated the usability of PGP 5.0 in 1999, revealing significant challenges users faced with regards to key management [50]. More than 20 years later 'Johnny' has found his way into the title of many publications dealing with usable key management and email encryption as the topic remains unsolved [5].

Eskandri et al. present the first review of key management in the context of Bitcoin in 2015. They remark that users are challenged to ensure their keys be simultaneously accessible, resistant to digital theft and resilient to loss. While they conclude that Bitcoin key management shares fundamental challenges of key management in general, they emphasize their observations that 'developers in the Bitcoin ecosystem are making innovative attempts to solve decades-old problems of usable key management', calling for further investigation user- behavior [22].

Krombholz et al. report on practices of Bitcoin management. They found most users resort to a password-protected wallet. Users of web clients have less background knowledge and are less likely to have backed up their wallets. 22.5% of users had to face a loss of Bitcoin, half of which were attributed to self-induced errors. They conclude that managing Bitcoins remains a major challenge for users [37].

Bonneau et al. identified strategies developers of Bitcoin software deployed to mask the complexities of key management: keys stored on device, password protected wallets, offline storage, air-gapped and hardware storage and hosted wallets [10]. Eskandari et al. propose an evaluation framework for key management approaches [22]. Krombholz et al. propose a methodology to categorize wallets based on their degree of control over key management operations. They introduce the term Coin Management Tool (CMT) as a name, capturing the functionality Bitcoin clients offer, as the term 'wallet' was defined as a 'collection of private keys' originally [32, 37].

We build on the proposed categorization approaches and differentiate between **self-managed** and **custodial** CMTs. Self-Managed CMTs require the user to manage their keys. Custodial CMTs take over key management for end users.

User Attitudes Towards Security And Privacy

An important part of building secure systems is to understand how users actually engage with those. This holds true for cryptocurrency systems especially, given that they delegate security-related tasks to the end user. Security and privacy researchers have found that end users differ in their willingness to deploy and use tools to secure themselves [1, 9, 16]. Barth and De Jong describe the privacy paradox: While users claim to be concerned about their privacy, they undertake but little to protect it. They identify the risk-benefit calculation as major decision-making process and discuss it through the different lenses offered by the surveyed publications [7]. To better understand users, different measurement instruments have been proposed to assess the attitude of users toward privacy [13] and security [19, 20].

There have been also efforts to cluster users based on their attitude towards security and privacy and identify common types of users. Research from Westin [38] distinguishes three types of users: (1) The Marginally Concerned, (2) the Fundamentalists and the (3) Pragmatic Majority. However, these categories were shown to be bad predictors of user behavior. Dupree et al. extend Westin's model to 5 privacy personas that differ in their knowledge of and motivation toward security and privacy [17].

- Fundamentalists (High Knowledge, High Motivation)
- Lazy Experts (High Knowledge, Low Motivation)
- Technicians (Medium Knowledge, High Motivation)
- Amateurs (Medium Knowledge, Medium Motivation)
- Marginally Concerned (Low Knowledge, Low Motivation)

In the context of cryptocurrency it is interesting to consider that users may differ in the motivation and ability to protect themselves. Research indicates that cryptocurrency users are not a homogeneous group, but that their perceptions of security and risk differ substantially [37, 39].

Summary

From previous work, we can extract several learnings for the context of this paper. Blockchain and cryptocurrencies remain a complex topic to understand, primarily because they suffer from the same challenges as key management in general. Several accounts of Bitcoin users' experiences provide insight into their behavior and motivation, yet a thorough qualitative account of how they manage security challenges is missing. These reports have also come to age, exploring findings from 2016 and earlier, before the 'run on cryptocurrencies' in 2017 – this may have led to a different composition of cryptocurrency users as well as a change in their behavior today. The work of Dupree et al. shows that knowledge and motivation on how security differs between people, something worth also exploring among cryptocurrency users. Eskandari et al. emphasized the innovative approaches of developers in the Bitcoin ecosystem back in 2015. Five years later, we think it is worth looking at how users manage their cryptocurrency today.

METHOD

In this section, we describe our research approach, the apparatus of questions guiding the semi-structured interviews and the coding and analysis process.

Approach

We conducted semi-structured interviews via Skype[1] between September 4th and 28th, 2019. The interviews lasted between 37 and 54 minutes (in total 451 minutes), were conducted in German language, audio-recorded and fully transcribed.

[1] https://skype.com

Apparatus

The interviews explored the challenges users face when managing cryptocurrencies in practice. The question catalogue was derived based on a qualitative analysis of posts and discussion in online forums (reddit.com/r/bitcoin, bitcoin.stackexchange.com and blockchainjournal.news) dealing with challenges of managing cryptocurrencies securely, collected during August 2019. We inquired about the following topics during the interviews and probed deeper when interesting topics emerged.

- Cryptocurrency ownership: Which cryptocurrencies do you own? Why did you start to get involved with cryptocurrencies? How to you manage / use your cryptocurrencies?
- Wallet Usage: Which wallets do you use? How do you use them? Why did you decide for these wallets? Can you remember problems you encountered while using wallets?
- Backup Behavior: How do you approach backups in general? How do you store mnemonics? Can you remember a time, when you had to use your backup(s)? Do you think your backups are stored securely?
- Demographic Information: Age, Gender, Highest Finished Education, Affinity for Technology Interaction (ATI) scale [4, 25], self-assessed experience with Blockchain (5-item Likert scale)

Recruiting

For this study, we recruited 10 cryptocurrency users between 19 and 36 (mean 27.2) years old. Participants were recruited using local networks in Munich, Germany. An initial outreach to identify participants was shared via the local blockchain meetup group and a university Slack[2] channel. From initially 16 responses, 10 participants scheduled the interview.

Data Analysis

For data analysis, we used thematic analysis following the 6-step process described by Braun and Clark, using an inductive approach [11]. The initial data set consisted of the transcribed interviews. To freely explore and organize emerging codes and themes we performed the initial three steps with printed versions of the transcript, before digitizing the codes and themes in subsequent iterations. As themes started to emerge during the iterative process, we included the previously collected dataset of online discussion to validate the identified themes. Figure 1 provides a snapshot of the process.

FINDINGS

From 10 participants, 9 were male. 5 participants are students, 5 participants are employed or work in their own company. Their highest finished education are High School (2), Bachelor Degree (3), Masters Degree (5). Participants are all located in Germany and Switzerland and have 3 different nationalities: 8 German, 1 Swiss and 1 US American. 5 participants are from business administration related fields, 5 from IT-related fields. 5 participants have worked with Blockchain technology during their studies or current employment already.

[2] https://slack.com

Figure 1. We used thematic analysis to analyze data collected from interviews and from online forums. To freely explore the data sets the initial steps were performed with printed transcripts.

The Affinity for Technology Interaction (ATI) score describes a person's tendency to actively engage in intensive technology interaction, or to avoid it. A score of 6 represents a high affinity for technology interaction and a score of 1 the opposite. Our participants rank between 1.56 and 5.78 (mean 4.76), showing a broad range of scores among the interviewees. [4, 25].

The participants have between 2 and 6 years (mean 3.6) of experience with cryptocurrencies (two participants did not disclose their experience in years). We asked participants to self-select experience with cryptocurrencies on a Likert-Scale from 1-5. The self-assessments range from 1 to 5 (mean 3.8).

All participants owned cryptocurrencies themselves. 7 participants disclosed which cryptocurrencies they owned. The number of different crypocurrencies listed per participant varied between 2 and 15. All of them listed Bitcoin and Ethereum. We further asked participants to provide a valuation in Euros of their cryptocurrencies at the current point in time. 8 participants agreed to do so, providing estimates between EUR 50 and EUR 25.000 (mean EUR 10.534).

Through the interview process and subsequent analysis, prominent themes emerged surrounding motivation, risks, and tool usage. Interviewee statements are denoted with "P" and statements from users in online forums with "W". Interview statements (P) were translated into English. Statements from online forums (W) were re-written to preserve their privacy [24, 12].

Motivation

The motivation to engage with cryptocurrencies varies between participants, though all of them could be attributed to either (1) financial interest, (2) ideological interest or (3) technical interest. These motivators are not mutually exclusive and most interviewees are motivated by a combination of them.

Financial Interest

We found financial interest to be the most frequently mentioned motivator for why people engage with cryptocurrencies – 8 of the 10 mentioned it. P1 stated, "*I view it as an investment, i.e. I expect an increase in value.*" and P7 shared that he engaged with cryptocurrencies for "*speculation*". However, they are not just seen as an investment opportunity, but also as a means for value preservation. P4 stated that he asked himself, "*How can I make sure that I don't lose what I have earned?*".

While it sounds trivial that people are motivated by financial interest to engage with cryptocurrencies, this contradicts earlier findings by Krombholz et al. who identified the "*decentralized nature"* and *"simple curiosity"* as primary motivators [37].

Research indicates that cryptocurrencies are used primarily as an asset and not as currency [27, 30, 45]. Our analysis indicates the desire of practitioners to use it as a currency: P4 stated, "*I would like to use it on a day-to-day basis*" and P10, "*I would like to spend it in the real world*". However, practitioners agree that a lack of options to spend cryptocurrency is holding them back from doing so.

Ideological Interest

Some participants are motivated by ideology, i.e. the "decentralized nature" of cryptocurrencies. However, nobody mentioned ideological reasons as sole motivation. P2 stated, *"I do believe in the technology [. . .] but I also think the ideological idea behind the movement is very interesting. Thus, a mix of curiosity of ideology and technical and economic conviction."*. P4 added an interesting perspective by sharing, "*I am from Bulgaria. I know what could happen there. There was a hyperinflation. The people lost their entire savings [. . .] I have been very sceptical about central banks since the financial crisis.*".

Krombholz et al. reported a similar case in their sample of qualitative interviews. For one participant, Bitcoin presented it as a secure alternative to receive money in Crimea during the Ukrainian-Russian conflict [37]. Similarly, a 2019 report on cryptocurrencies by the Dutch Bank ING surveying close to 15.000 people in 15 countries found that 61% of respondents from Turkey were most positive about the future of cryptocurrencies. In comparison, only 20% of participants from Germany and 31% from the US showed positive attitudes towards the future of cryptocurrencies [33]. The socio-political environment people find themselves in may have a significant impact on their motivation and intent to use cryptocurrencies.

Technological Interest

Curiosity in the technology was the third motivator we identified. P10 explained, "*[...] to try it out. To better understand the technology. And especially with Ethereum to play around with Smart Contracts*". P2 stated, "*I think it is exciting to be at the technological frontline*" and P8, "*Mainly technical interest. I started engaging with cryptos in practice. So, not just with cryptocurrencies but with fundamental blockchain and distributed ledger technology.*". These statements are in line with earlier findings. Krombolz et al. identified "curiosity" as the second strongest motivator in their sample [37].

Risk Assessment

Krombholz et al. found that 22.5% of their sample had lost cryptocurrencies. Of these incidents, 43.2% were account to the fault of the user, 26.5% to a hardware failure, 24.4% to a software failure and 18% to security breaches [37]. The questions on how to best secure crypto assets and minimize the risk of losing them are therefore vivid discussion points.

Our analysis identified three essential sources of risk that can lead to the loss of cryptocurrency. Users have to deal with the (1) Risk of Human Error, the (2) Risk of Betrayal and the (3) Risk of Malicious Attacks. Previous research by Sas and Kahiruddin interviewing 20 Malaysian Bitcoin users similarly identified risks with the specific focus on transactions: (R1) *Risks due to User's Challenges of Handling Passwords*, (R2) *Risks Due to Hackers' Malicious Attack*, (R3) *Risks due to Failure to Recover from Human Error of Malice*, (R4) *Risks from Dishonest Partner of a Transaction* [45]. Our definitions differ in that they are not limited to transactions, but apply to cryptocurrency usage in general. Risk of Human Error encompasses all risk rooted in user behavior, including R1 and R3. Risk of Trust includes all stakeholders involved directly or indirectly with buying, selling and managing cryptocurrencies. Risk of Malicious Attacks extended beyond the digital realm and the risk of physical attacks as well.

Risk of Human Error

The decentralized nature of cryptocurrencies does not only shift the control over assets but also the responsibility for securing them to the end-user. Mistakes made by users can, therefore, lead to the loss (of access) to the managed crypto assets. Practitioners are generally aware of this, as P10 put it, "*If you lost your private key, your are f*cked"*.

P2 was generally afraid to not adequately handle technology. He described his feeling when using his mnemonic recovery key: "*Whenever I do something with mnemonics, I have a weird feeling even though there is not much that can go wrong. It always feels just like there is this pressure, like, 'Oh God, if you do something wrong now, in the worst case everything is gone'. You cannot call anyone. You cannot reset anything.*".

There is a fear of forgetting critical information to access crypto assets, such as passwords, private keys or physical backup location: "*Memorization is not the best idea. I wrote my seed phrase on paper and now I can't remember where I hid it.*" (W1).

Finally, there are the fears of inadequately storing or losing critical information. Examples are losing the seed phrase, misspelling the seed phrase, selecting the wrong storage medium or location ultimately leading to breakdown or destruction of the stored information. On how to store backup phrases (mnemomics) P4 remarked: "*Paper is sort of safe until you think about what would happen if the apartment burnt down*".

Risk Betrayal

While blockchain enables trustless consensus, social trust between stakeholders is still necessary [6, 44, 45]: "*You always need a gateway into the decentral system. So there will always be someone*" (P3). Placing one's trust into a third party carries an inherent risk that this third party may not act according to expectations and ultimately betray one's trust. This risk is not necessarily unique to cryptocurrencies.

Custodial CMTs provide a way to participate in the crypto economy without the need to deal with key management. However, for this to work there is the need to trust the custody provider to handle one's keys. Some participants expressed distrust of these services, best captured by the phrase *"not your keys, not your crypto"* (P1, P2, P8, P10). This sentiment is rooted in a fear of placing trust in the wrong guardian. Using a centralized service to manage assets is for some in direct

conflict with the decentralized nature of blockchain technology. P8 said, *"Custodial wallets are pure fiction [. . .] If they are bankrupt or they want to betray you, they just take the real hardware wallet and run away*". However, this risk is not limited to custodial CMTs, but more generally applies to all third parties involved directly or indirectly with buying, selling and managing cryptocurrencies. P10 illustrated this point with the example of a cloud storage provider: "*If I put the private key of my decentral cryptocurrency into a Google Drive, I should expect that someone looks at it.*" , adding "*What if Google cooperates with the government and they hand out some data . . . Therefore, I would never store it in Cloud Storage.*".

Risk of Malicious Attack

Discussions regarding malicious attacks revolve around three core topics: the self-managed CMT getting compromised, the custodial CMT getting compromised, and physical attacks.

A common fear of users is that the self-managed CMT could get compromised, allowing attackers to gain access to their funds. Digital storage methods of keys and mnemonics are viewed as less secure than physical storage. W4 stated, *"Do not store mnemonics digitally - you are asking for hacker attacks."* and W3 confirmed, *"If you store your seed phrase digitally, you increase your attack surface enormously."*. As a result, some recommend the use of hardware wallets that are not connected to the internet and thus less susceptible to attacks. P1 said, "*In my opinion, hardware wallets take away the majority of errors users can make [. . .] In the end, my PC could be infested with 5 viruses but my private key would not be stolen.*". P10 shared this view, "*I can use hardware wallets on virus-infested computers without my money being stolen*".

W2 made an interesting point stating, *"I think those who can handle the complexity of cold storage and hardware wallets do so anyway. Because when it comes to security against external attackers, these solutions are more secure. However, when all causes of Bitcoin loss are considered, the probability of loss is more likely to be due to user errors than to device hacks."*. This notion is not unfounded – it coincides with the findings of Krombholz et al. that listed security breaches as the least common reason of Bitcoin loss. Bitcoin loss was caused by user mistakes twice as often as by security breaches [37].

Practitioners also fear that custodial CMTs, such as exchanges, are an attractive target for attackers. This fear is rooted in a rich history of incidents in the past, most notably the infamous hack of the at the time largest Bitcoin exchange mt.gox in 2014 during which Bitcoin worth USD 460 million were stolen [40, 41]. P1 concluded, "*We have seen it more than once that Exchanges were hacked or that the founders ran off with the funds of their customers*".

Malicious Attacks are not neccesarily confined to the digital realm. Physical attacks can take two forms: (1) theft of credentials and backups and (2) attacks on the owner forcing them to provide access to their CMT. W5 summarized his thoughts on theft as follows: *"I can imagine that in the future, a burglar will know exactly what to do if he opens a drawer (or safe) and finds a laminated piece of paper with a seed phrase on it. In 1950 a thief would not have bothered to find a plastic card with a bunch of numbers in a wallet. But by 1960, every criminal knew exactly how to use a credit card."*. With regards to robbery, P1 said, *"Even if I was kidnapped and tortured, I could never give away my private key."*. W11 suggests a different approach for the event of robbery, *"Put an amount large enough that a thief cannot resist, into your wallet without password and the rest into a password protected wallet."*.

Coin Management Tool (CMT) Usage

The choice of Coin Management Tools by practitioners emerged as the third theme. Our findings indicate that there is no "silver bullet", no "one-size-fits-all solution" that works for all users and use cases. Rather, practitioners use both self-managed and custodial CMTs in parallel. They store backups redundantly and are aware of the challenges current CMTs brings about.

Use of Multiple CMTs

More than half of the participants reported to use both self-managed and custodial CMTs. The reasons behind choosing to use either type are consistent between participants. Users opting to use self-managed CMTs emphasise that only ownership of the private keys ensures ownership of cryptocurrency. This mindset is captured by the commonly used phrase *"not your keys, not your crypto"* (P1, P2, P8, P10). Users of custodial platforms value the usability and convenience they provide. Asked for his motivation, P3 explained, "*Because it has a lot of convenience. Honestly, does one really need to know one's keys? Do I really need to have access to them?*". P7 further argued that using a custodial CMT is a feature, as he is not solely responsible in case of a problem. He said, *"Do I trust the producer of the hardware wallet that the system will work in the future? As with Coinbase, other people have interest in it. Meaning, if there are problems, there will be a solution. If my personal hardware wallet breaks down, there is only me who has an interest in it. Worst case there will be not solution and my money is gone."*.

Participants using both self-managed and custodial CMTs do so for different use cases. Custodial wallets are used for spending and acquiring cryptocurrencies, whereas self-managed CMTs, specifically HW wallets, are seen as long-term storage for larger sums. P4 explained, "*There is not necessarily the need for one perfect thing for everything [. . .] The safe securely back home and a wallet of third parties for everyday use*". P8 claimed to use custodial CMTs only for buying: "*I use custodial wallets only to buy cryptocurrencies*", as did P2: "*On Coinbase I only buy and sell and then send it directly to my ledger . . . except for smaller sums*". This approach is similar to what Eskandari et al. propose: keeping small ready-to-spend amounts in online wallets and larger sums in more secure and difficult to access storage [22].

CMTs are not necessarily digital, either. Examples are services by banks, offering to handle the investment and storage of cryptocurrencies. P6 mentioned, "*There are already several private banks here which offer good solutions. These would be the Bank von Tovel und Bank Frick, who have been doing this for a long time now*.".

Backups Stored Redundantly

Backup of the private keys or the seed phrases are well discussed topics. We found that redundant backup storage is common practice among all users with self-managed CMTs. Most users store backups in the form of mnemonics: 12 or 24 letter sentences that encode the seed phrase used to generate the master key of a wallet [52, 43]. They store multiple copies, in multiple locations and combine different methods to do so. P1 explained his rational for redundant locations as safeguard against environmental threats: "*In my opinion, the best protection against environmental damage is redundancy. This means to not store my keys at one location, but to create maybe two backups and store them at geographically different places.*". Using multiple locations is also commonly recommended in online forums. W8 for example recommended, "*The most reliable way to keep your seed/secret key safe is to have numerous instances in different locations, perhaps in various formats, and even better if the keys are split.*".

These comments suggest that most users store these backups redundantly to avoid accidental loss or destruction. This naturally increases the probability a third party could gain access. To mitigate this, users employ additional strategies. P2 stores his backup in a safe, "*The ones for my Ledger Nano S are lying in a safe*" and P8 splits his backup and stores the parts in two fireproof safes, "*[. . .] just splitting the key in two parts. And then physically transport it in two fireproof safes*". Some users combine digital solutions with offline storage. P2 stated he additionally stores his backups, "*Having it encrypted on my laptop, deposit box in a bank and additionally some metal box lying around somewhere at home*". Some tech-savvy participants resort to the use of encryption. W10 for example stated to use PGP: *"I encrypt the keys of my wallet with PGP and send an email to my own account and someone I trust. Voila."*.

The collected data indicates that for backup storage there is no one-size-fits-all solution as well, causing users to resort to a combination of them: "*Every storage technique has its shortcomings. The optimum is always to diversify*" (P10).

Awareness of Usability Challenges

Another characteristic of interviewees is their awareness and acknowledgement of current issues with cryptocurrencies.

Many users perceive dealing with key management as a burden and bad usability. This is in line with prior usable security research [22, 28, 29, 50]. Not having to deal with keys is perceived as better usability. P3 said, "*The best usage for me would be to never see a private key or public key again. Optimal usage would be as simple as N26 banking today*". For these users, custodial CMTs, which shield them from having to deal with key management, are convenient. P8 explained the advantage of custodial CMTs, "*The usability of such wallets is far better. Because it is easier. Because you do not have to take care of any key management.*". P7 is convinced that key management is not the best solution, "*At the same time, I do not believe that local management is the best solution for all people*". He added, "*I believe, there is a large customer group for whom it makes a lot of sense to trust a central entity instead of managing it themselves*". P8 concluded that there could be different groups of CMTs for different users, "*There may be several groups. The first group has exceptional usability. The middle group is maybe encrypted – here MetaMask is very successful, but requires a lot of knowledge. And then there are things like Hardware wallets that are much more technical and more secure, but less convenient*".

Self-managed CMTs largely expose the underlying technology, blockchain, to the user. P4 is convinced that security needs to be at a level where the majority of people can use it: "*There will not be something like absolute security as long as humans are involved [. . .] Rather, the point is how can we provide the best security for most people so that most people can use it*". Several users suggested forms of biometric authentification as one solution (P3, P4, P8, P9). P3 thought, "*Maybe a fingerprint or retina scan will suffice in the future*".

Established naming concepts are perceived as bad metaphors that do not translate well to the concepts behind them. This makes it difficult for new users to asses possible consequences of these concepts. P10 said, "*I think a wallet has nothing to do with a wallet in which I put my bills. It is rather a box where I put my keys. This was simply a poor choice of labeling to understand what it really does*." and continued, "*The choice of words regarding 'wallets' is wrong [. . .] Recovery phrase sounds nothing like something private. It does not imply that, if you lose it, all your crypto might be gone*". From evaluating 6 Bitcoin key management clients Eskandari et al. concluded that "tasks involving key management can be mired in complex metaphors and confusing abstractions" [22].

There is a high technical entry-barrier new users need to clear before starting with cryptocurrencies. The complexity of the topic and the required technical knowledge make it difficult to use self-managed CMTs and provide many pitfalls for new users (increasing the **Risk of Human Error).** P1 stated, "*Creating a wallet is quite complicated for someone doing it the first time. At this point nobody is aware of the consequences of what they are doing*". P10 argued, "*The best entry point is to engage with the topic on a technical level*" and further explained, "*As non-technical user one should know that from the mnemonic the private key is created and that it has to be treated even more confidential*". P8 feels onboarding needs to be improved, "*I think that onboarding has to be improved everywhere*". Also Glomann et al. identified "The Onboarding Challenge" as one of the problems slowing down mainstream adoption of blockchain-based systems [31].

THEORETICAL IMPLICATIONS

We discuss the implications of our findings for HCI research on cryptocurrencies and blockchain systems. These are mostly valid for cryptocurrency users, but may be valuable to understand users interacting with other blockchain technologies.

Our findings indicate that all users are aware of the importance of keeping their cryptocurrency secure. Their strategies on how to achieve this, however, differ. Some users opt for a strict "not your keys, not your crypto" strategy, using only self-managed solutions while others choose to delegate key management all together to a custodial service. Some users advocate for offline storage in hardware wallets, while others manage them on internet-connected devices or web-based systems.

In choosing their tools, users need to balance the different sources of risk – **Risk of Human Error, Risk of Betrayal, Risk of Malicious Attack**. This happens largely along two dimensions. Firstly, users need to decide between self-managed and custodial CMTs. Secondly, users need to decide between CMTs disconnected from or connected to the internet.

Self-Managed CMT vs Custodial CMT

The decision to choose either self-managed or custodial services translates to balancing the **Risk of Human Error** against the **Risk of Betrayal**. For every individual user, this balance is different as it is influenced by their attitude toward security. As both motivation and knowledge of how to deploy security mechanisms influence this balance, Dupree et al.'s model of Privacy Personas lends itself as a valuable tool. Figure 2 exhibits this tension by showing two Privacy Personas on opposite sides of the spectrum. To illustrate this point we chose the extreme positions of the Privacy Personas [17].

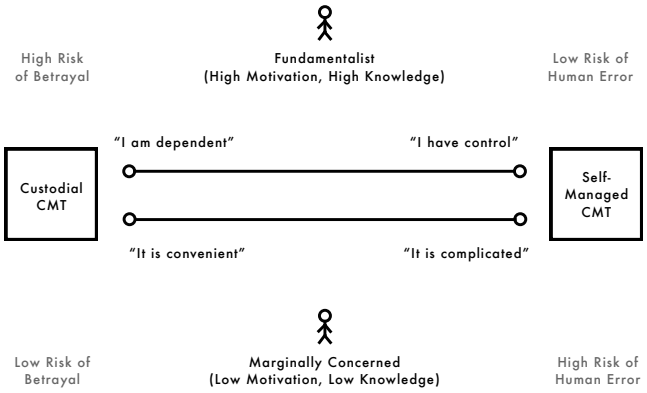

Figure 2. Motivation and Knowledge of security influences how users choose between self-managed and custodial CMTs.

Fundamentalists are characterized by a high motivation to and high knowledge of how to employ security. They value fine-grained access to security settings and generally view others as uneducated and insecure [17]. Consequently, they value the control over security self-managed CMTs offer. They know how to securely manage their keys and view it as unlikely that they will lose cryptocurrency through their own mistakes – they assess the **Risk of Human Error** to be low. From their perspective moving towards custodial CMTs is seen as giving up control and becoming dependent on a potentially insecure third party, ultimately increasing the **Risk of Betrayal**.

The Marginally Concerned have low motivation and knowledge about security concepts. They generally trust websites claiming to be secure. They know threats exist, but view it as unlikely that something will happen to them [17]. For them having to deal with key management is a burden. It is complicated. At best it is bad usability and at worst the source of mistakes that lead to the loss of their cryptocurrency. Custodial CMTs shield them from the technical complexity of key management and provide a familiar and convenient way to engage with cryptocurrencies. They trust the custodial service to provide better security than they could and assess the **Risk of Betrayal** as low. For them, moving from Custodial CMTs to Self-Managed CMTs is seen as a loss of convenience through additional complexity, increasing the **Risk of Human Error**.

Isolated CMT vs Connected CMT

The decision of whether to use a CMT isolated from or connected to the internet relates back to how users assess the **Risk of Malicious Attack**. To understand the decision process of users along this dimension, we review it through the lense of how cryptocurrency is being used. Previous research noted the dualism of cryptocurrencies – they are both an asset and a currency [27, 30, 45]. Assets and currencies exhibit different characteristics. The European Central Bank defines money as (1) a medium of exchange, (2) a store of value or (3) a unit of account to compare values of different goods or services [23]. Glaser et al. demarcate the use of Bitcoin as an asset from the use as a currency by whether users' intention is trade or a store of value [30]. Our findings indicate that this tension remains to exist. Users tend to use different strategies and tools next to each other to cope with the different use cases.

Figure 3 depicts how users' intention to use cryptocurrency as either asset (store of value) or currency (means to trade) influences their decision to use internet connected or isolated CMTs. Offline usage decreases the attack surface, but limits how fast users can access it.

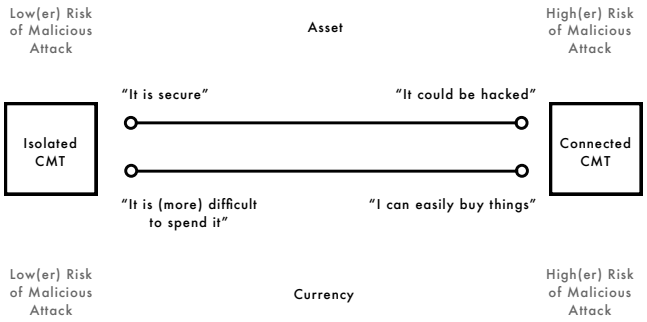

Figure 3. The intention to use cryptocurrencies as Assets or Currency influences decisions between online and offline CMTs.

We distinguish **Isolated CMT** and **Connected CMT** at each end of the spectrum. Connected CMTs are directly connected with the internet. Isolated CMTs are strictly disconnected from any network. These extremes define a scale on which any CMT can be placed based on how connected it is to the internet.

Managing cryptocurrencies with a connected CMT exposes it to potential digital attacks. Isolated CMTs are perceived to be more secure by users, as they decrease the attack surface. However, offline management limits how quickly users can spend cryptocurrencies. From the perspective of an asset – storing value over a long period of time – the time to access the funds is not as important as securing it from potential attackers. For the use as currency – to trade it for goods and services – the time needed to access them and complete a transaction is, however, crucial.

Depending on how users will use their cryptocurrencies, they will opt for isolated CMTs, connected CMTs or a combination.

A Model to Understand Coin Management Tool Usage

Understanding these fields of tension is important to develop better user-centric CMTs. We propose a conceptual model, which integrates these dimensions to enable researchers and practitioners to evaluate CMTs. Figure 4 depicts the model.

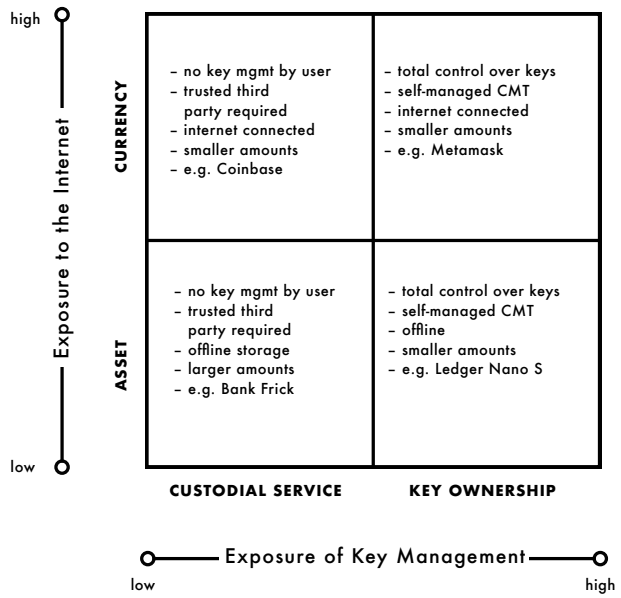

Figure 4. A model to explore how exposure to the internet and exposure of key management characterizes CMTs.

The vertical axis represents the degree to which the CMT is connected to the internet. The horizontal axis shows the degree to which public key cryptography is exposed to the end-user.

The key decision practitioners need to make with regards to how, i.e. with which tools, they want to participate in the crypto economy is dependent on how they assess the likelihood of the fundamental risks that can lead to a loss.

Different levels of key management enable control but also impose responsibility. Choosing between self-managed CMTs and custodial CMTs translates to balancing the **Risk of Human Error** against the **Risk of Betrayal** by a third party. Users with high motivation and knowledge about security mechanisms and key management will assess the risk to make mistakes themselves as low. Consequently, they see the usage of a custodial service as one that cause loss of control and independence. Users with low motivation and/or knowledge of key management will likely tend to choose a custodial CMT to abstract the key management away from them. For them, self-managed CMTs would reduce convenience and usability, while increasing the risk of loss through their own mistakes.

Choosing between connected and disconnected CMTs translates to the assessment of the **Risk of Malicious Attacks** by the practitioner. Managing one's crypto assets on an internet-enabled device, in the browser albeit, offers high mobility – that is the speed at which they can buy goods or sell their cryptocurrency. This naturally opens up an attack vector for potential malicious attackers. To reduce this attack surface, offline CMTs could be resorted to – at the cost of mobility. For example, storing one's hardware wallet in a bank safe may greatly reduce the attack surface, but limit the mobility of the assets to the time it takes to physically gain access through the processes of the bank. Depending on whether users' intent is value storage (use as an asset) or means of trade (currency), they are likely to choose a tool increasing mobility or security.

Each quadrant contains a short description of the features CMTs in this category would exhibit, including one example available today. These examples were chosen, because they were mentioned during the interviews and are explained below.

CMTs connected to the internet allow users to treat their cryptocurrencies as digital cash and use it to buy and sell goods. Metamask[3], for example is a wallet in the form of a browser-extension for the cryptocurrency Ethereum. It runs directly in the browser and allows websites to interact with by integrating the web3.js library. It stores keys password protected in the local browser, but requires users to protect and store the master private key of the wallet themselves.

Coinbase[4] is a web-based wallet and exchange that allows users to buy and sell a wide array of different cryptocurrencies. While also connected to the internet, it abstracts all key management tasks. Users can authenticate via familiar username/password and 2-factor authentication mechanism. Since the service takes over the key management, users need to trust that Coinbase does so with the necessary care.

Such custodial services also exist disconnected from the internet. The Liechtenstein based bank Bank Frick[5]offers custodial coin management through a traditional bank. Customers can delegate the acquisition and secure storage of cryptocurrencies entirely to the bank. The complete offline storage makes this method inapplicable for using cryptocurrencies to trade. However, it greatly reduces the attack surface through which potential attackers would gain access to them.

Users eager to maintain complete control over their keys without dependence on any third party may also opt out of offline storage methods. Besides, simple paper wallets, the Ledger Nano S[6] is a password protected hardware wallet enabling offline key management. The thumbdrive-sized device is supported by a wide range of digital wallets (mobile apps) and can be used to sign transactions for compatible cryptocurrencies.

DESIGN IMPLICATIONS

Based on the theoretical implications and our findings, we derive three design implications [46] for researchers and practitioners. CMTs should be developed with a clear target group in mind and focused on either the use as an asset or currency. Finally, a better understanding of cryptocurrency non-users is needed to address impediments and challenges that keep them from engaging with the technology.

Pick Your Target Group

The conversation around cryptocurrency security is largely led by tech-savvy people with high knowledge and motivation to deploy security. However, not all users have either the motivation or knowledge to securely manage cryptocurrencies on their own. Getting started with cryptocurrencies itself is perceived as a complicated process and key management remains a major challenge for non-technical users [31, 22].

[3] https://metamask.io
[4] https://www.coinbase.com
[5] https://www.bankfrick.li/en
[6] https://www.ledger.com

As the adoption of blockchain technology continues, it is important to design for inclusiveness. We argue that there is a need to lower the technological entry barrier to engage with the cryptocurrencies – and in extension, blockchain technology – to allow people without deep technical insight to participate in the crypto economy. Custodial CMTs (e.g. coinbase.com) are one product category where this already happens. At their example, one can see that people are willing to engage with the technology if they are provided with the right tools. Designers of CMT services should consider which audience they are building their product for and understand how balancing the **Risk of Human Error** and **Risk of Betrayal** influence their choice of tools.

Key management remains a challenge for users and current CMTs are either entirely self-managed or custodial. Using the proposed model, we hope that practitioners can go forward, envisioning hybrid CMTs that serve new audiences.

Design for Assets or for Currency

Cryptocurrencies exhibit a dualist nature, being both an asset and a currency. Depending on the reason users engage with the technology, different user needs should be considered. Developers should be aware that services for either assets or currencies have different requirements, especially regarding mobility and attack surface and design services accordingly.

Thinking through the lens of these different use cases should also be reflected in the communication towards users. Practitioners should aim to develop best practices specific for each use case and find meaningful analogies to convey them to non-technical users. For large investments emphasizing secure and redundant offline storage following a "not your keys, not your crypto" mindset is justified. Similarly to carrying cash in your pocket, smaller amounts of cryptocurrency can be managed with little downside risk in digital, custodial CMTs that allow for quick access when spending them.

As positive real-world example with focus on enabling spending of cryptocurrency in a currency-like way is the Lightning Network project[7], enabling real-time transactions of Bitcoin. The project decisively focuses on using cryptocurrency as a means to trade and makes use of metaphors taken from everyday life on their website to explain the technical concept behind it (last accessed April 18th 2020). They write, "*This is similar to how one makes many legal contracts with others, but one does not go to court every time a contract is made. [...] Only in the event of non-cooperation is the court involved – but with the blockchain, the result is deterministic.*"

Despite these efforts, cryptocurrencies today are, contrary to their name, predominantly used as an asset and not like a currency. Our findings indicate that this is not due to a lack of interest, but rather a lack of supply -– users would like to use them as currency, but cannot because of a lack of services accepting them. As technical limitations disappear, future research should investigate why merchants refrain from accepting cryptocurrency and explore how to "make cryptocurrencies as easy as online banking".

[7] https://lightning.network/

Seek Understanding of Non-Users

Arguably, the composition of cryptocurrency users has changed over the past 12 years. Current HCI research on cryptocurrencies is, however, primarily focused on practitioners. Findings from these studies ultimately help to understand and improve services for those that already use them. We argue that understanding why people are held back from engaging with cryptocurrencies in the first place is equally important to enabling more inclusive design.

The challenges non-users have to face might be very different from those that have become familiar with the terms and concepts. Glomann et al. stress the difficulty to find a "starting point" to learn basic concepts as one issue for potentially interested users [31]. Given the complexity of cryptocurrencies, it would be interesting to understand how novel users work around this issue and obtain their initial knowledge base.

The research community would further benefit from a deeper understanding of security and privacy behavior [17, 7] in the context of cryptocurrencies. Understanding how non-users attitudes towards privacy and security differ from those of current users would be valuable for researchers and practitioners alike.

Elsden et al. argue for the role of HCI in *Engaging Participants with Blockchain*, both for knowledge exchange and participatory design [21]. Future research should strive to include non-users in this process. Their perspective might lead to different types of applications, such as Gateway Services [21] mediating interactions with blockchain services, potentially opening them up to a broader audience overall.

CONCLUSION

This paper explores users' practices of engaging with cryptocurrencies and identifies prominent themes regarding motivation, risk assessment, and CMTs usage. We discuss how motivation and risk assessment influence CMT usage, introduce a conceptual model and derive design implications. While rooted in findings from CMT usage, we hope that this model provides a valuable lens through which HCI researchers and practitioners can view and understand user behavior in the wider area of emerging blockchain-based applications.

ACKNOWLEDGMENTS

This work was supported by the Deutsche Forschungsgemeinschaft (DFG) (grant no. 316457582 and 425869382).

REFERENCES

[1] Anne Adams and Martina Angela Sasse. 1999. Users Are Not the Enemy. *Commun. ACM* 42, 12 (Dec. 1999), 40–46. DOI:http://dx.doi.org/10.1145/322796.322806

[2] Amanda Ahl, Masaru Yarime, Kenji Tanaka, and Daishi Sagawa. 2019. Review of blockchain-based distributed energy: Implications for institutional development. *Renewable and Sustainable Energy Reviews* 107 (2019), 200 – 211. DOI:http://dx.doi.org/https://doi.org/10.1016/j.rser.2019.03.002

[3] E. Almutairi and S. Al-Megren. 2019. Usability and Security Analysis of the KeepKey Wallet. In *2019 IEEE International Conference on Blockchain and*

Cryptocurrency (ICBC). 149–153. DOI: http://dx.doi.org/10.1109/BLOC.2019.8751451

[4] Christiane Attig, Daniel Wessel, and Thomas Franke. 2017. Assessing Personality Differences in Human-Technology Interaction: An Overview of Key Self-report Scales to Predict Successful Interaction. In *HCI International 2017 – Posters' Extended Abstracts*, Constantine Stephanidis (Ed.). Springer International Publishing, Cham, 19–29.

[5] Erinn Atwater, Cecylia Bocovich, Urs Hengartner, Ed Lank, and Ian Goldberg. 2015. Leading Johnny to Water: Designing for Usability and Trust. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 69–88. https://www.usenix.org/conference/soups2015/proceedings/presentation/atwater

[6] Andreas Auinger and René Riedl. 2018. Blockchain and Trust: Refuting Some Widely-held Misconceptions. In *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*. https://aisel.aisnet.org/icis2018/crypto/Presentations/2

[7] Susanne Barth and Menno D.T. de Jong. 2017. The Privacy Paradox Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior A Systematic Literature Review. *Telemat. Inf.* 34, 7 (Nov. 2017), 1038–1058. DOI: http://dx.doi.org/10.1016/j.tele.2017.04.013

[8] Aaron W Baur, Julian Bühler, Markus Bick, and Charlotte S Bonorden. 2015. Cryptocurrencies as a disruption? empirical findings on user adoption and future potential of bitcoin and co. In *Conference on e-Business, e-Services and e-Society*. Springer, 63–80.

[9] Bettina Berendt, Oliver Günther, and Sarah Spiekermann. 2005. Privacy in E-Commerce: Stated Preferences vs. Actual Behavior. *Commun. ACM* 48, 4 (April 2005), 101–106. DOI: http://dx.doi.org/10.1145/1053291.1053295

[10] Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A Kroll, and Edward W Felten. 2015. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In *IEEE Symposium on Security and Privacy*. http://www.ieee-security.org/TC/SP2015/papers-archived/6949a104.pdf

[11] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (2006), 77–101. DOI: http://dx.doi.org/10.1191/1478088706qp063oa

[12] Amy Bruckman. 2002. Studying the amateur artist: A perspective on disguising data collected in human subjects research on the Internet. *Ethics and Information Technology* 4, 3 (2002), 217–231. DOI: http://dx.doi.org/10.1023/A:1021316409277

[13] Tom Buchanan, Carina Paine, Adam N. Joinson, and Ulf-Dietrich Reips. 2007. Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology* 58, 2 (2007), 157–165. DOI:http://dx.doi.org/10.1002/asi.20459

[14] Vitalik Buterin. 2014. A Next-Generation Smart Contract and Decentralized Application Platform. (Sep 2014). Retrieved Jan 28, 2020 from https://github.com/ethereum/wiki/wiki/white-paper/

[15] Coinmarketcap. 2020. Top 100 Cryptocurrencies by Market Capitalization. (Jan 2020). Retrieved Jan 4, 2020 from https://coinmarketcap.com/

[16] Paul Dourish and Ken Anderson. 2006. Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena. *Human–Computer Interaction* 21, 3 (2006), 319–342. DOI: http://dx.doi.org/10.1207/s15327051hci2103_2

[17] Janna Lynn Dupree, Richard Devries, Daniel M. Berry, and Edward Lank. 2016. Privacy Personas: Clustering Users via Attitudes and Behaviors toward Security Practices. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. Association for Computing Machinery, New York, NY, USA, 5228–5239. DOI: http://dx.doi.org/10.1145/2858036.2858214

[18] Dmitry Efanov and Pavel Roschin. 2018. The all-pervasiveness of the blockchain technology. *Procedia Computer Science* 123 (2018), 116–121. DOI: http://dx.doi.org/10.1016/j.procs.2018.01.019

[19] Serge Egelman and Eyal Peer. 2015a. Predicting Privacy and Security Attitudes. *SIGCAS Comput. Soc.* 45, 1 (Feb. 2015), 22–28. DOI: http://dx.doi.org/10.1145/2738210.2738215

[20] Serge Egelman and Eyal Peer. 2015b. Scaling the security wall : Developing a security behavior intentions scale (SeBIS). *Conference on Human Factors in Computing Systems - Proceedings* 2015-April (2015), 2873–2882. DOI: http://dx.doi.org/10.1145/2702123.2702249

[21] Chris Elsden, Arthi Manohar, Jo Briggs, Mike Harding, Chris Speed, and John Vines. 2018. Making Sense of Blockchain Applications: A Typology for HCI. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. Association for Computing Machinery, New York, NY, USA, Article Paper 458, 14 pages. DOI: http://dx.doi.org/10.1145/3173574.3174032

[22] Shayan Eskandari, David Barrera, Elizabeth Stobert, and Jeremy Clark. 2015. A First Look at the Usability of Bitcoin Key Management. *Proceedings 2015 Workshop on Usable Security* (2015). DOI: http://dx.doi.org/10.14722/usec.2015.23015

[23] Europe Central Bank. 2012. *Virtual Currency Schemes*. 55 pages. http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

[24] Casey Fiesler and Nicholas Proferes. 2018. "Participant" Perceptions of Twitter Research Ethics. *Social Media + Society* 4, 1 (2018), 2056305118763366. DOI: http://dx.doi.org/10.1177/2056305118763366

[25] Thomas Franke, Christiane Attig, and Daniel Wessel. 2019. A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (ATI) Scale. *International Journal of Human–Computer Interaction* 35, 6 (2019), 456–467. DOI: http://dx.doi.org/10.1080/10447318.2018.1456150

[26] Andrea Gaggioli, Shayan Eskandari, Pietro Cipresso, and Edoardo Lozza. 2019. The Middleman Is Dead, Long Live the Middleman: The "Trust Factor" and the Psycho-Social Implications of Blockchain. *Frontiers in Blockchain* 2 (2019), 20. DOI: http://dx.doi.org/10.3389/fbloc.2019.00020

[27] Xianyi Gao, Gradeigh D. Clark, and Janne Lindqvist. 2016. 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 (CHI '16)*. Association for Computing Machinery, New York, NY, USA, 1656–1668. DOI: http://dx.doi.org/10.1145/2858036.2858049

[28] Simson L. Garfinkel, David Margrave, Jeffrey I. Schiller, Erik Nordlander, and Robert C. Miller. 2005. How to Make Secure Email Easier to Use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '05)*. Association for Computing Machinery, New York, NY, USA, 701–710. DOI: http://dx.doi.org/10.1145/1054972.1055069

[29] Shirley Gaw, Edward W. Felten, and Patricia Fernandez-Kelly. 2006. Secrecy, Flagging, and Paranoia: Adoption Criteria in Encrypted Email. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '06)*. Association for Computing Machinery, New York, NY, USA, 591–600. DOI:http://dx.doi.org/10.1145/1124772.1124862

[30] Florian Glaser, Kai Zimmermann, Martin Haferkorn, Moritz Christian Weber, and Michael Siering. 2014. Bitcoin - Asset or currency? Revealing users' hidden intentions. *ECIS 2014 Proceedings - 22nd European Conference on Information Systems* January (2014).

[31] Leonhard Glomann, Maximilian Schmid, and Nika Kitajewa. 2020. Improving the Blockchain User Experience - An Approach to Address Blockchain Mass Adoption Issues from a Human-Centred Perspective. In *Advances in Artificial Intelligence, Software and Systems Engineering*, Tareq Ahram (Ed.). Springer International Publishing, Cham, 608–616.

[32] Steven Goldfeder, Rosario Gennaro, Harry Kalodner, Joseph Bonneau, Joshua Kroll, Edward W. Felten, and Arvind Narayanan. 2015. Securing Bitcoin wallets via a new DSA/ECDSA threshold signature scheme. (2015). http://www.cs.princeton.edu/~stevenag/threshold_sigs.pdf Accessed: 2015-07-13.

[33] ING Bank N.V. 2019. *ING From cash to crypto: the money revolution*. https://think.ing.com/uploads/reports/IIS

[34] Irni Eliana Khairuddin and Corina Sas. 2019a. An Exploration of Bitcoin Mining Practices: Miners' Trust Challenges and Motivations. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Association for Computing Machinery, New York, NY, USA, Article Paper 629, 13 pages. DOI:http://dx.doi.org/10.1145/3290605.3300859

[35] Irni Eliana Khairuddin and Corina Sas. 2019b. An Exploration of Bitcoin Mining Practices: Miners' Trust Challenges and Motivations. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Association for Computing Machinery, New York, NY, USA, Article Paper 629, 13 pages. DOI:http://dx.doi.org/10.1145/3290605.3300859

[36] Irni Eliana Khairuddin, Corina Sas, Sarah Clinch, and Nigel Davies. 2016. Exploring Motivations for Bitcoin Technology Usage. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '16)*. Association for Computing Machinery, New York, NY, USA, 2872–2878. DOI: http://dx.doi.org/10.1145/2851581.2892500

[37] Katharina Krombholz, Aljosha Judmayer, Matthias Gusenbauer, and Edgar Weippl. 2017. The other side of the coin: User experiences with bitcoin security and privacy. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 9603 LNCS (2017), 555–580. DOI: http://dx.doi.org/10.1007/978-3-662-54970-4_33

[38] Ponnurangam Kumaraguru and Lf Cranor. 2005. Privacy indexes: A survey of westin's studies. *School of Computer Science, Carnegie Mellon University* Tech. rep., December (2005), 1–22.

[39] C. Lustig and B. Nardi. 2015. Algorithmic Authority: The Case of Bitcoin. In *2015 48th Hawaii International Conference on System Sciences*. 743–752. DOI: http://dx.doi.org/10.1109/HICSS.2015.95

[40] Patrick McCorry, Malte Möser, and Syed Taha Ali. 2018. Why Preventing a Cryptocurrency Exchange Heist Isn't Good Enough. In *Security Protocols XXVI*, Vashek Matyáš, Petr Švenda, Frank Stajano, Bruce Christianson, and Jonathan Anderson (Eds.). Springer International Publishing, Cham, 225–233.

[41] Aleksander Murko and Simon L. R. Vrhovec. 2019. Bitcoin Adoption: Scams and Anonymity May Not Matter but Trust into Bitcoin Security Does. In *Proceedings of the Third Central European Cybersecurity Conference (CECC 2019)*. Association

for Computing Machinery, New York, NY, USA, Article Article 15, 6 pages. DOI: http://dx.doi.org/10.1145/3360664.3360679

[42] Satoshi Nakamoto. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. *bitcoin.org* (2008).

[43] Sean Palatinus, Marek, Rusnak, Pavlov, Voisine, Aaron, Bowe. 2013. BIP 39: Mnemonic code for generating deterministic keys. (2013). https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki

[44] Corina Sas and Irni Eliana Khairuddin. 2015. 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 (OzCHI '15)*. Association for Computing Machinery, New York, NY, USA, 338–342. DOI: http://dx.doi.org/10.1145/2838739.2838821

[45] Corina Sas and Irni Eliana Khairuddin. 2017. 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 (CHI '17)*. Association for Computing Machinery, New York, NY, USA, 6499–6510. DOI: http://dx.doi.org/10.1145/3025453.3025886

[46] Corina Sas, Steve Whittaker, Steven Dow, Jodi Forlizzi, and John Zimmerman. 2014. Generating Implications for Design through Design Research. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. Association for Computing Machinery, New York, NY, USA, 1971–1980. DOI: http://dx.doi.org/10.1145/2556288.2557357

[47] Janusz J. Sikorski, Joy Haughton, and Markus Kraft. 2017. Blockchain technology in the chemical industry: Machine-to-machine electricity market. *Applied Energy* 195 (2017), 234 – 246. DOI:http://dx.doi.org/https://doi.org/10.1016/j.apenergy.2017.03.039

[48] Melanie Swan. 2015. *Blockchain: Blueprint for a New Economy* (1st ed.). O'Reilly Media, Inc.

[49] M. Szmigiera. 2019. Number of Blockchain wallet users worldwide from 3rd quarter 2016 to 3rd quarter 2019. (Oct 2019). Retrieved Jan 4, 2020 from https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/

[50] Alma Whitten and J. D. Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8 (SSYM'99)*. USENIX Association, USA, 14.

[51] X. Wu, B. Duan, Y. Yan, and Y. Zhong. 2017. M2M Blockchain: The Case of Demand Side Management of Smart Grid. In *2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS)*. 810–813. DOI: http://dx.doi.org/10.1109/ICPADS.2017.00113

[52] Pieter Wuille. 2013. BIP32: Hierarchical Deterministic Wallets. (2013). https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki