User Mental Models of Cryptocurrency Systems - A Grounded Theory Approach

Alexandra Mai and Katharina Pfeffer, *SBA Research;* Matthias Gusenbauer, *Tokyo Institute of Technology, SBA Research;* Edgar Weippl, *University of Vienna;* Katharina Krombholz, *CISPA Helmholtz Center for Information Security*

https://www.usenix.org/conference/soups2020/presentation/mai

This paper is included in the Proceedings of the Sixteenth Symposium on Usable Privacy and Security.

August 10–11, 2020

978-1-939133-16-8

User Mental Models of Cryptocurrency Systems - A Grounded Theory Approach

Alexandra Mai
SBA Research

Katharina Pfeffer
SBA Research

Matthias Gusenbauer
Tokyo Institute of Technology,
SBA Research

Edgar Weippl
University of Vienna

Katharina Krombholz
CISPA Helmholtz Center
for Information Security

Abstract

Frequent reports of monetary loss, fraud, and user-caused security incidents in the context of cryptocurrencies emphasize the need for human-centered research in this domain. We contribute the first qualitative user study ($N = 29$) on user mental models of cryptocurrency systems and the associated threat landscape. Using Grounded Theory, we reveal misconceptions affecting users' security and privacy.

Our results suggest that current cryptocurrency tools (e.g., wallets and exchanges) are not capable of counteracting threats caused by these misconceptions. Hence, users frequently fail to securely manage their private keys or assume to be anonymous when they are not. Based on our findings, we contribute actionable advice, grounded in the mental models of users, to improve the usability and secure usage of cryptocurrency systems.

1 Introduction

More than ten years after the first Bitcoin transaction was performed [13], cryptocurrencies have gained popularity among different types of users, ranging from technology enthusiasts to investors, gamblers, and people who are simply curious. Media reports often contain anecdotes of negative user experiences with security and privacy in cryptocurrency systems. Cryptocurrencies obviate the need for central control by maintaining a decentralized public ledger. While technical aspects of cryptocurrencies have been heavily studied (e.g., [6], [17], [34], [3]), human-centered studies are still rare.

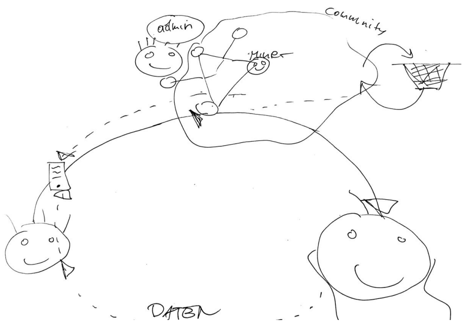


Figure 1: Drawing assignment of the transaction process (S8).

Gao et al. [16] used semi-structured interviews to explore specific aspects of the Bitcoin system out of context. Krombholz et al. [29] quantitatively examined user perceptions on Bitcoin security mainly based on closed-ended questions. However, so far no research investigated mental models which are based on users' *tacit knowledge*. Such knowledge consists of implicit and subjective assumptions that cannot easily be verbalized, but are heavily influencing human behavior [24].

We extend the state of the art by providing the first qualitative user study ($N = 29$) to learn about people's **mental models of cryptocurrencies**[1] **and associated security and privacy threats**. Therefore, we use drawing and card assignment tasks (see Figure 1). Our study methodology follows an inductive approach based on Grounded Theory (GT) [18, 31, 42].

Thereby, we answer the following research questions:

- **Q1** What mental models of cryptocurrency systems and their functional components do users have?
- **Q2** Which mental models interfere with a secure and privacy-preserving usage of cryptocurrency systems?
- **Q3** How can cryptocurrency tools prevent security and privacy threats caused by users' mental models?

[1] We focus on Bitcoin and Ethereum since they were the most prevalent cryptocurrency systems in terms of market capitalization [9] at the time of our study.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2020.
August 9–11, 2020, Virtual Conference.

Our work aims at explaining (some of) the reasons for user-caused security incidents. This is necessary in order to re-design tools and create effective strategies for behavior change. We argue that cryptocurrency tools (e.g., wallets, online exchanges) should be designed in a way to avoid security or privacy risks even when used by people with incorrect or incomplete mental models. This is in line with Wash et al. [43] claiming that instead of attempting to force users into more 'correct' mental models, technology should be shaped to work well with existing mental models.

Through our study we identify the gaps between the actual protocol functionality and users' mental representations. Although not all the incorrect or incomplete mental models found imply security pitfalls, some partly explain why users of current cryptocurrency tools fail to securely manage their digital assets and have wrong assumptions about privacy and anonymity. Mental models with negative consequences include an erroneous understanding of cryptocurrency systems with regards to (i) cryptographic keys, (ii) anonymity, and (iii) fees.

2 Related Work

Cryptocurrency systems differ from other public key systems (e.g., PGP and secure messaging), as keys are used to sign transactions which are transparently published in the blockchain, instead of ensuring confidentiality through encryption. The threat model is entirely different as well: losing a private key leads to severe problems in the context of cryptocurrency systems as monetary assets are involved. A plethora of research has been carried out to study security and privacy aspects of the Bitcoin system [45]. Nevertheless, several user-centric challenges remain, providing a breeding ground for security and privacy threats.

Only few studies have examined the usability and user perceptions of cryptocurrency systems, mainly focusing on Bitcoin. Baur et al. [4] found that users attribute a high potential to cryptocurrencies, but perceive the usefulness of current cryptocurrencies as low. According to Khairuddin et al. [25], the major motivation for users to buy Bitcoin is its potential for financial revolution, increased user empowerment, and its use as an investment. Sas and Khairuddin [40] as well as Lustig and Nardi [32] explored trust issues of Bitcoin users. Elsden et al. [11] proposed a typology of emerging blockchain applications making it easier for users to understand them. Gao et al. [16] conducted a qualitative study where they found that the major entry barrier for non-users is a perceived necessity for profound technical knowledge.

The first large-scale quantitative user study was presented by Krombholz et al. [29], revealing that many users neither understand nor use the security capabilities of coin management tools correctly. Although the authors also conducted a small number of qualitative interviews, those were only used to contextualize their quantitative findings, not to construct an inductive theory. Kazerani et al. [23] investigated the influence of (poor) usability of cryptocurrency management tools on the adoption of Bitcoin by lay people. Eskandari et al. [12] compared the usability of different cryptographic key management approaches.

However, these earlier studies either opted for a quantitative study design (e.g., [29]) or asked questions which the interviewees deemed too complex to answer given their background as non-users (e.g., [16]). To the best of our knowledge, our work is the first mental model study on cryptocurrencies that aims at discovering the tacit knowledge of the participants. Therewith, we answer open questions on why users commonly fail to manage private keys safely in the context of cryptocurrencies and which parts of current cryptocurrency tool interfaces put users with incorrect mental models at security or privacy risk. We give suggestions for future designs of cryptocurrency tools on how to ensure that user behavior does not compromise the users' security and privacy.

3 Methodology

The overall goal was to understand user perceptions and misconceptions of functional principles, and whether they prevent users from using cryptocurrencies in the most secure and privacy-preserving manner. We chose Bitcoin and Ethereum as examples of prevalent cryptocurrencies and excluded Ethereum's smart contract functionality to only focus on its native currency ether. Furthermore, payment channels are out of scope of our research. This allows us to make general assumptions about user perceptions with regard to the majority of cryptocurrencies that build on the same functional principles as Bitcoin and Ethereum (i.e., in relation to key generation and usage, transaction generation and confirmation, blockchain application, and mining operations). For the remainder of this paper, we will thus use the term *cryptocurrency* to refer to bitcoin, ether, and similar cryptocurrencies.

3.1 Grounded Theory

We follow an inductive approach and use Grounded Theory (GT) [18, 31, 42] to explore user perceptions based on qualitative data. GT is a set of systematic inductive methods to develop theories that are grounded in qualitative research data. A key characteristic is that it merges data collection and analysis in an iterative approach until (theoretical) saturation is reached [42]. Therefore, different phases of recruitment and coding are necessary (see below). By following a process during which we directly analyze the collected data, we generate descriptive theories that are as close to reality as possible. GT is traditionally used in social sciences and has gained popularity in human-computer interaction and usable security research [15, 20, 28].

3.2 Recruitment

Our goal was to recruit a diverse sample of current and potential future cryptocurrency users. We approached possible interviewees through Bitcoin mailing lists and social media as well as personal contacts, also to get in touch with organizations that work with blockchain technology.

We distributed a short description of our study and issued a questionnaire (Appendix A.1) for preselection. To prevent potential participants from reading up on the technical intricacies of blockchain technology, we did not disclose the concrete purpose of our study, only that it deals with cryptocurrencies. Then we selected a subset of participants fitting our recruitment criteria from the people who completed the questionnaire.

We chose the participants according to their self-reported level of knowledge about cryptocurrencies and information technology (ranging from lay users to experts) as well as to their usage of cryptocurrencies. We also chose to recruit participants with diverse exposure to and interaction with cryptocurrency. We recruited 7 people who were not actively using cryptocurrencies but who were working with cryptocurrencies in their professional life (e.g., organizing cryptocurrency meetups, conferences or projects with wallet/exchange operators). Further 10 participants considered cryptocurrencies mainly as an investment, 5 used them mainly for trading, and 7 actively used cryptocurrencies as a payment method.

While the self-reported data might not fully reflect the actual knowledge level of participants, we are confident that these measures are sufficiently accurate to reflect our inherently diverse target population and that a diverse sample was obtained.

3.3 Sampling

GT [42] requires to go back and forth between data collection and analysis in order to construct a theory which is derived from data and not chosen a priori (as it is the case in quantitative studies). Following GT, we conducted the selection of participants in two rounds (two weeks apart). First, we collected an initial sample of 18 cryptocurrency users (experts and non-experts) and then explored the obtained data through open coding.

Based on the concepts derived from our analysis, we extended our initial sample to people who are not actively using cryptocurrencies themselves, but work in institutions that use or deal with cryptocurrencies or blockchain technology (see Section 3.2). Since these people were confronted with cryptocurrency tools, at least at a superficial level, they have certain mental models but are not influenced by cryptocurrency tool interfaces. These mental models are particularly interesting as they represent perceptions of (potential future) first-time cryptocurrency users for whom cryptocurrency tools should be designed as well. By comparing non-users to users, we were able to explore how cryptocurrency tool interfaces might influence mental models (cryptocurrency tool bias) and also investigate biases of non-users (e.g., bank bias). For the second round of recruitment, we collected additional data, recruiting a sample of 11 participants based on the emerging theories.

Table 1: Participant demographics. Total N=29

Demographic	**Participants (%)**
Gender	
Male	19 (65.5%)
Female	10 (34.5%)
Age	
18 – 22	1 (3.4%)
23 – 27	12 (41.4%)
28 – 32	10 (34.5%)
33 – 37	4 (13.8%)
38 – 42	2 (6.9%)
Highest Completed Education	
High school	5 (17.2%)
Bachelor degree	10 (10.4%)
Master degree	14 (72.4%)

Hence, we had a final set of 29 participants (summarized in Table 1). In order to protect the privacy of our participants, we queried the age, beginning with 18 years, in intervals of five years.

3.4 Design and Procedure

As shown by Kearney and Kaplan [24], people commonly construct implicit knowledge maps to understand complex systems when the systems' functionality goes beyond their technical knowledge. They argue that such tacit knowledge influences people's decision-making and behavior in critical situations, although they are often not aware of it. We opted for a study design that encourages participants to expose their tacit knowledge and functional understanding by engaging them in drawing and card assignment exercises. During these exercises the participants had to assign cards with a function (e.g., "sign transaction") to the entities in their drawings.

Based on related work on human factors of Bitcoin [11, 12, 25, 35] and recent mental model studies in usable security [15, 16, 20, 37, 43, 46], we constructed an interview script for semi-structured interviews including a short pre-assessment questionnaire covering demographics and the participants' general cryptocurrency usage patterns, two drawing tasks, and a card assignment task. The complete study material can be found in the Appendix (Section A).

Our final dataset is based on 29 interviews which were conducted in person in two Austrian cities, namely Vienna and Graz. The interviews took place either in a room at our lab, the participants' workplace, or their home. The majority of the interviews were conducted by two researchers (one interviewer and one assistant taking notes). Two interviews were performed by only one interviewer due to scheduling conflicts.

With the informed consent of the participants, we recorded all interviews, fully transcribed them, and photographed all drawings and card assignments. The pictures (along with the transcribed verbal explanations) served as our baseline for coding.

3.4.1 Pilot Studies

We carried out three pilot studies to test the expressiveness and practicability of our interview script. At the end of each iteration, we requested feedback from the respective participant. We specifically asked the participants to explain their understanding of selected functional concepts and well-known buzzwords – e.g., blockchain, [de-]centralized system, miner – if the participants had not drawn or mentioned them during the interview. We modified the interview script only once (after the first interview). Therefore, we decided to include the remaining two interviews in our final sample.

3.4.2 Interview Procedure

Before the actual interview started, participants were briefed, they signed a consent form and received their compensation (20 Euro Amazon voucher). Each interview lasted roughly 30 minutes and consisted of semi-structured questions, two drawing tasks and one card assignment task. These tasks were based on a concrete scenario, namely transferring a certain amount of bitcoin or ether to a fictional friend called Alice.

In the course of the first drawing task, we asked participants to visualize and verbally express all components and actors involved in the transaction process, as well as their connections. We encouraged participants to think aloud while drawing to gather additional insights into their reasoning. Afterwards, we gave them 15 cards with short descriptions of selected functions (e.g., “generate private key”, “generate transaction”, “validate transaction”, etc.; see Appendix A.2). Depending on which cryptocurrency the participants were more familiar with (self-assessment), the cards reflected the terminologies from either bitcoin or ether. We told the participants to assign the cards to the components and actors in their drawings. We did not provide full definitions but asked the participants to verbalize their own understandings of these technical terms and the associated context.

We added the card assignment task to assist the participants in refining and contextualizing their tacit knowledge. In order to eliminate the possibility of misunderstood terms and random guessing during the interview, the participants were encouraged to provide detailed definitions as far as possible and the interviewers asked follow-up questions if further clarification was needed.

The second drawing task was used to elicit understandings of attackers and threats, and how specific security and privacy risks are contextualized in transaction processes.

3.5 Ethical Considerations

Our organization, which is located in Austria, has no institutional review board but a series of guidelines to be followed when conducting user studies. One of the fundamental requirements is to preserve the participants’ privacy and limit the collection of sensitive data as much as possible. Before the interview, all participants were asked to sign consent forms in which the goals of our study and data handling procedures were described. Those consent forms were stored securely and do not contain any links to the IDs we assigned to our participants. The study furthermore strictly followed the EU’s General Data Protection Regulation (GDPR).

3.6 Coding

3.6.1 Open and Axial Coding

We followed a GT-based approach to interpret our data. After the first 18 interviews, two researchers independently coded the data (initial *open coding*) with the aim to group recurring statements and assertions relating to the same phenomena (preliminary categories). We created codes based on the drawings and think-aloud protocols. We refrained from assigning codes based on single denotations or terms (e.g., verify, confirm, encrypt). Instead, we coded entire statements and hence included the context in which a term was used.

In line with the full GT approach and while discussing the results, we decided to extend our participant pool by including people who do not actively use Bitcoin, but work in a field related to cryptocurrencies. We are confident that the perceptions and opinions of those people add a new perspective to our study outcome since they have no practical experience in using Bitcoin or Ethereum – and, as such, are not influenced by interfaces of exchange platforms or wallets – but possess some (theoretical) knowledge about blockchain technology. Moreover, this sample’s knowledge structures are particularly relevant when thinking about the design of future technology for managing cryptocurrencies, since those people are either potential new users or decision makers in corporate environments.

Following the GT methodology, we performed a second round of open coding to refine the results of the first round. Three researchers independently coded the entire data-set in three rounds (Round 1: 10 interviews, Round 2: 10 interviews, Round 3: 9 interviews). In order to systematize the process, we applied *affinity mapping*, whereby we cut the interview transcripts into snippets and used sticky notes to label newly found categories that emerged from recurring or related statements. As we coded the interviews based on contextualized statements (instead of single terms), we generated a code book based on the participants’ mental representations and reasoning. After each round of individual coding we discussed the relations between the newly found categories and agreed upon a set of higher-level categories (*axial coding*). For instance, we decided to group the categories “public key generation external”, “key and address independent”, and “one public key for all” to the meta-category “address/key generation”. The categories of the third round of coding served as a baseline for *selective coding*.

The final sample size was determined through reaching saturation [19], i.e., no new insights could be gathered from the interviews. As we achieved saturation in the newly emerging categories, we stopped interviewing after 29 participants.

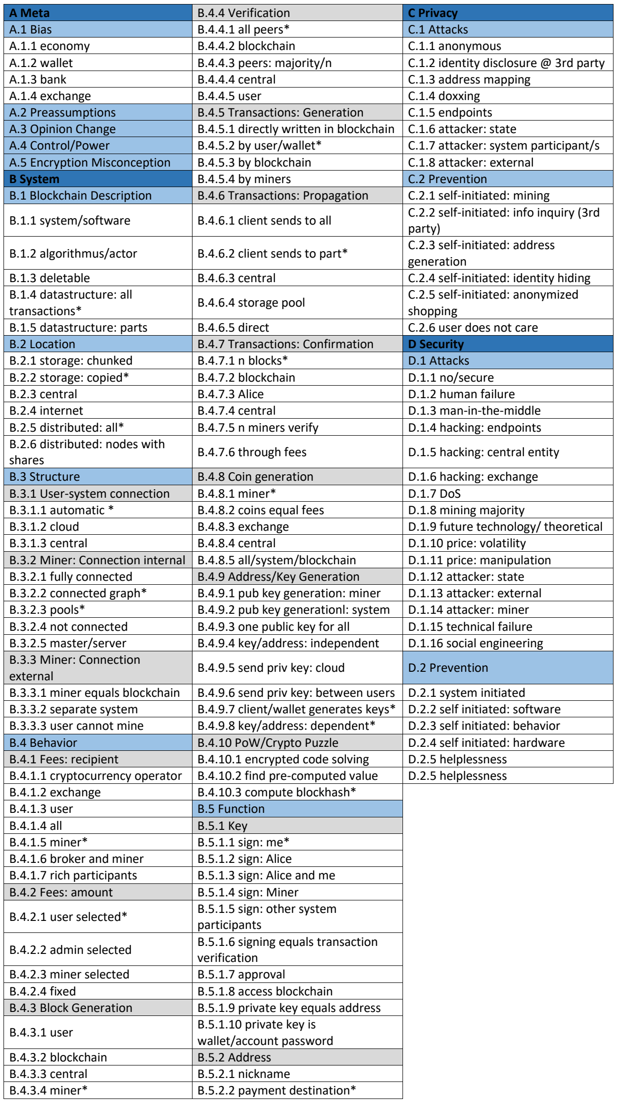
3.6.2 Selective Coding

During this process, three independent researchers agreed upon a set of final core categories centered around the identified misconceptions which might compromise the users' security and/or privacy. The misconceptions are grouped into the following four different top-level categories which consist of multiple subcategories (final codebook see Figure 2[2]):

- ***Meta*** – This category includes statements which were meaningful for building our theory, but are not directly related to cryptocurrency systems and their functionality. It comprises general opinion changes during the interviews, prerequisites, statements about the control or power of the system, biases which influenced participants' descriptions, and misconceptions related to encryption and hashing.
- ***System*** – The system category includes statements describing the blockchain (*Blockchain Description*) as well as where and how it is stored (*Location*). Additionally, this category is split into *Structure*, *Behavior*, and *Function*. *Structure* includes descriptions about the connection between users and miners. The category *Behavior* refers to the behavior of the system (e.g., who receives fees). *Function* on the other hand categorizes the tasks of the keys and the addresses.
- ***Privacy*** – This category codes all mentioned attacks and possible prevention mechanisms on users' privacy.
- ***Security*** – This category includes all attacks and possible prevention mechanisms specific to the users' security.

3.6.3 Final Coding

With a final set of codes grouped into categories, two researchers independently went through all 29 interviews and assigned one or multiple codes, thus generating a comprehensive codebook. Thereby, the transcripts, drawings, and outcome of the card assignment task served as a baseline. We report an inter-rater reliability with a Krippendorff's Alpha value [27] of $\alpha = 0.89$, indicating a high level of agreement among the coders. We claim that this relatively high number is fostered by the technical classification and the granularity of the codebook. Conflicts mostly appeared due to slightly different interpretations of the drawings, which sometimes conflicted with the think-aloud protocols. When we detected a conflict, we consulted the drawings and transcripts and discussed the results again. In these cases, we agreed that the verbal explanations should weigh more than the card assignments, since the latter were sometimes less expressive than the participants' verbal descriptions. All conflicts among the coders were resolved.



A Meta	B.4.4 Verification	**C Privacy**
A.1 Bias	B.4.4.1 all peers*	C.1 Attacks
A.1.1 economy	B.4.4.2 blockchain	C.1.1 anonymous
A.1.2 wallet	B.4.4.3 peers: majority/n	C.1.2 identity disclosure @ 3rd party
A.1.3 bank	B.4.4.4 central	C.1.3 address mapping
A.1.4 exchange	B.4.4.5 user	C.1.4 doxxing
A.2 Preassumptions	B.4.5 Transactions: Generation	C.1.5 endpoints
A.3 Opinion Change	B.4.5.1 directly written in blockchain	C.1.6 attacker: state
A.4 Control/Power	B.4.5.2 by user/wallet*	C.1.7 attacker: system participant/s
A.5 Encryption Misconception	B.4.5.3 by blockchain	C.1.8 attacker: external
B System	B.4.5.4 by miners	C.2 Prevention
B.1 Blockchain Description	B.4.6 Transactions: Propagation	C.2.1 self-initiated: mining
B.1.1 system/software	B.4.6.1 client sends to all	C.2.2 self-initiated: info inquiry (3rd party)
B.1.2 algorithmus/actor	B.4.6.2 client sends to part*	C.2.3 self-initiated: address generation
B.1.3 deletable	B.4.6.3 central	C.2.4 self-initiated: identity hiding
B.1.4 datastructure: all transactions*	B.4.6.4 storage pool	C.2.5 self-initiated: anonymized shopping
B.1.5 datastructure: parts	B.4.6.5 direct	C.2.6 user does not care
B.2 Location	B.4.7 Transactions: Confirmation	**D Security**
B.2.1 storage: chunked	B.4.7.1 n blocks*	D.1 Attacks
B.2.2 storage: copied*	B.4.7.2 blockchain	D.1.1 no/secure
B.2.3 central	B.4.7.3 Alice	D.1.2 human failure
B.2.4 internet	B.4.7.4 central	D.1.3 man-in-the-middle
B.2.5 distributed: all*	B.4.7.5 n miners verify	D.1.4 hacking: endpoints
B.2.6 distributed: nodes with shares	B.4.7.6 through fees	D.1.5 hacking: central entity
B.3 Structure	B.4.8 Coin generation	D.1.6 hacking: exchange
B.3.1 User-system connection	B.4.8.1 miner*	D.1.7 DoS
B.3.1.1 automatic *	B.4.8.2 coins equal fees	D.1.8 mining majority
B.3.1.2 cloud	B.4.8.3 exchange	D.1.9 future technology/ theoretical
B.3.1.3 central	B.4.8.4 central	D.1.10 price: volatility
B.3.2 Miner: Connection internal	B.4.8.5 all/system/blockchain	D.1.11 price: manipulation
B.3.2.1 fully connected	B.4.9 Address/Key Generation	D.1.12 attacker: state
B.3.2.2 connected graph*	B.4.9.1 pub key generation: miner	D.1.13 attacker: external
B.3.2.3 pools*	B.4.9.2 pub key generationl: system	D.1.14 attacker: miner
B.3.2.4 not connected	B.4.9.3 one public key for all	D.1.15 technical failure
B.3.2.5 master/server	B.4.9.4 key/address: independent	D.1.16 social engineering
B.3.3 Miner: Connection external	B.4.9.5 send priv key: cloud	D.2 Prevention
B.3.3.1 miner equals blockchain	B.4.9.6 send priv key: between users	D.2.1 system initiated
B.3.3.2 separate system	B.4.9.7 client/wallet generates keys*	D.2.2 self initiated: software
B.3.3.3 user cannot mine	B.4.9.8 key/address: dependent*	D.2.3 self initiated: behavior
B.4 Behavior	B.4.10 PoW/Crypto Puzzle	D.2.4 self initiated: hardware
B.4.1 Fees: recipient	B.4.10.1 encrypted code solving	D.2.5 helplessness
B.4.1.1 cryptocurrency operator	B.4.10.2 find pre-computed value	D.2.5 helplessness
B.4.1.2 exchange	B.4.10.3 compute blockhash*	
B.4.1.3 user	B.5 Function	
B.4.1.4 all	B.5.1 Key	
B.4.1.5 miner*	B.5.1.1 sign: me*	
B.4.1.6 broker and miner	B.5.1.2 sign: Alice	
B.4.1.7 rich participants	B.5.1.3 sign: Alice and me	
B.4.2 Fees: amount	B.5.1.4 sign: Miner	
B.4.2.1 user selected*	B.5.1.5 sign: other system participants	
B.4.2.2 admin selected	B.5.1.6 signing equals transaction verification	
B.4.2.3 miner selected	B.5.1.7 approval	
B.4.2.4 fixed	B.5.1.8 access blockchain	
B.4.3 Block Generation	B.5.1.9 private key equals address	
B.4.3.1 user	B.5.1.10 private key is wallet/account password	
B.4.3.2 blockchain	B.5.2 Address	
B.4.3.3 central	B.5.2.1 nickname	
B.4.3.4 miner*	B.5.2.2 payment destination*	

Figure 2: Final codebook

3.6.4 Theory and Mental Model Construction

The last step of our GT approach was to form theories including the overarching mental models which describe how our participants perceive cryptocurrency systems. First, two independent researchers generated two draft mental models:

[2] For category B all correct answers are marked with an asterisk *

one incomplete model and one inaccurate model for the structure, function, and behavior of components in cryptocurrency systems. We constructed the models based on our results, centered around those categories which resulted from our selective coding (codebook). Then, the two coders met in person to reach an agreement. We validated our constructed mental models through negative case analysis [7] by going through all interviews to check whether the participants' statements can be assigned to one of our draft mental models. If not, we sought to understand how they diverged from our draft and adopted it accordingly. In doing so, we iteratively refined our draft mental models until all statements could be assigned. A participants' mental model can contain aspects of the incorrect and incomplete mental model. In order to (i) construct our theory, (ii) examine whether the mental models interfere with secure and privacy-preserving usage of cryptocurrencies, and (iii) understand how resulting issues can be solved, we ran a focus group (Section 4.7) with four experts in the field of cryptocurrencies and blockchain technology. The two final models are presented in Section 4.2 and 4.3.

4 Mental Models of Cryptocurrency Systems

In this section, we first provide a simplified description of the Bitcoin and Ethereum system to provide the appraisal factors for the assessment of our data. Then, we present our participants' veritable mental models. These models represent incomplete and inaccurate descriptions of our participants in correspondence to the structure, functionality, and behavior of cryptocurrency systems. Direct participant quotes (translated to English) are provided for illustration. Since quantitative results (numbers) in qualitative research cannot be used to generalize findings, we will discuss all statements without providing numbers. Nonetheless, coding frequencies can be found in Appendix A.4.

4.1 Appraisal Factors

Before conducting the study, we constructed a ground truth model together with two cryptocurrency experts. These experts were also part of our focus group. We do not claim exhaustiveness of our expert mental models which can be incomplete and diverse as well. To increase the validity, we interviewed two experts and constructed one mental model incorporating both statements. Similar to the user interviews, we asked both experts to draw all components and actors involved in a transaction process and verbalize their thoughts. We then constructed a simplified representation of their mental models (see Figure 3). This model serves as a basis for the evaluation of user mental models and only focuses on important parts for user transactions. We found the participants' mental models to be consistently sparser than the expert mental model. The comparison of users' and expert mental models is purely illustrative and non-judgmental. We defined the assessment basis as follows:

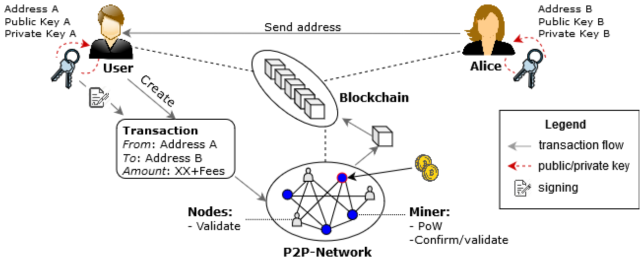


Figure 3: Ground truth of the transaction process of cryptocurrency systems based on blockchains.

Bitcoin and Ethereum are blockchain-based, peer-to-peer (P2P) networks which enable users to perform transactions with virtual (crypto-)currencies. The system consists of multiple participants (peers) that we group in four different roles: (i) sender, (ii) receiver, (iii) miner, and (iv) other users. Each participant can hold multiple roles.

The basic requirement to perform a transaction within a cryptocurrency system is that sender and receiver must have some kind of wallet, or are enrolled with an online exchange service. A wallet consists of public keys, private keys, and addresses. The private key is randomly generated and permits the user to spend cryptocurrency units. In the case of offline wallets, it is the user's responsibility to securely store and back up the private key. The address is a hashed version of the public key and acts as a public identifier of the asymmetric key pair.

Prior to performing a transaction, the receiving party communicates its address to the sending party. The sender creates the transaction which comprises the sending and receiving address as well as the transferred amount, including fees. The amount of the fees can be selected by the user and determines the processing speed of the transaction (transactions with higher fees are more likely to be included within the next block). Afterwards, the sender signs the transaction with the private key and broadcasts it to the P2P network. The verification – for both the transactions and the blocks – is performed by peers in the network. Thereby, not all peers necessarily perform full validation (e.g., SPV wallets or thin clients do not check whether transactions are valid, but they rather evaluate whether full nodes have validated them correctly).

A specific transaction t is considered to be confirmed when (i) a miner successfully constructed the Proof-of-Work (PoW) for a block b containing t, (ii) b ends up in the heaviest chain (i.e., the chain with the most cumulative PoWs), and (iii) a certain amount of blocks is succeeding b (as the blockchain gets longer, the confirmation can be considered to be more secure). The miner (or mining pool, i.e., a cluster of miners that work together) who solves the PoW first gets rewarded with newly created currency (a specific amount depending on the implementation of the system) and the transaction fees. As soon as the transaction is confirmed, the amount is credited from the sender's to the receiver's wallet.

4.2 Incomplete Mental Model

Figure 4 depicts the best-case mental model grounded in our qualitative analysis. It includes technically correct yet sparse perceptions compared to the ground truth (see Figure 3). We did not encounter poor decision-making as a result of incomplete mental models, hence the missing details are not crucial for secure usage of the cryptocurrency system.

Several users correctly stated that cryptocurrency systems are decentralized with annotations reflecting an outline of a peer-to-peer (P2P) system, and a transaction flow matching our ground truth (illustrated through lighter grey continuous lines in Figure 4). The majority correctly stated that the user's wallet software generates the public/private key pair (illustrated by a dotted red line in Figure 4). Some of them also knew that in order to send coins to another party, the sender has to sign the transaction with the generated keys. They correctly mentioned that an address is the payment destination in our proposed scenario. Many participants correctly understood that miners receive the transaction fees. However, only a few participants knew how fees are actually calculated and could give a correct explanation of the mining process.

4.3 Inaccurate Mental Model

The mental model presented in Figure 5 incorporates the participants' misconceptions of cryptocurrency systems. However, not all illustrated components are reflected in all mental models of our participants. Misconceptions related to the transaction flow are illustrated by a grey, continuous line, and those related to the key generation are shown through dashed, red lines in Figure 5. We found that many misconceptions do not jeopardize users' security or privacy. In the following we discuss which misconceptions are crucial and which are not.

Some participants assumed a central management entity as part of a cryptocurrency system, such as a server or broker. Others thought that a direct end-to-end connection existed between sender and receiver, via which transactions are performed.

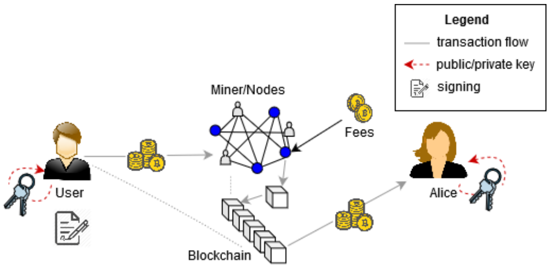


Figure 4: Incomplete mental model

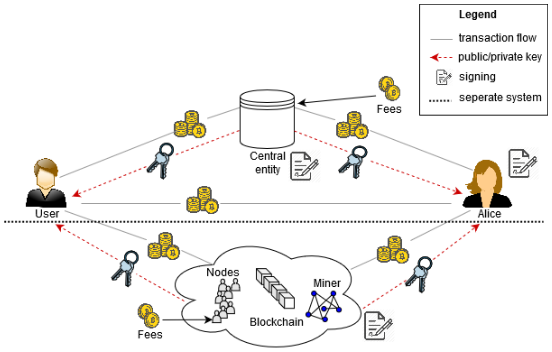


Figure 5: Inaccurate mental model

> *It is a de-centralized system because there is no pivotal element. Only the two accounts interact with each other directly without a third person interfering.* (S6)

One participant hypothesized that in addition to an end-to-end user connection, a further connection to a cloud exists through which users can get initial approval for transactions in order to afterwards send confirmed transactions directly to the receiver. Participants with incorrect mental models often described the blockchain, other nodes, and the miners either only through keywords without being able to explain them, or as a separate system or cloud. Therefore we depict them as a cloud and (partly) separated system (see bottom half in Figure 5). In the following sections, we discus these misconceptions and their impact on security and privacy in detail.

4.3.1 Cryptographic Keys

We identified many misconceptions related to the keys used in cryptocurrency systems. Although users' problems with cryptographic keys (and their management) have already been investigated for other application areas – for example secure messaging and PGP – the effects of mistakes from the users' perspective are different for cryptocurrency systems (e.g., direct monetary impact). In particular, we found that participants do not understand who generates the keys. Some participants claimed that the miners carry out key generation or expected the whole cryptocurrency system to generate keys.

> *Hmmm well, I don't generate my private keys myself, they are saved in my smartphone app. It is... generally the blockchain who generates it [the key] for me, or the network, the blockchain. It is floating in the air somehow. I don't know. It comes from the internet.* (S19)

One participant thought that all parties in the Bitcoin system share one common key. This would break cryptocurrency systems because everybody would have access to everybody else's funds. Other participants presumed that in order to send coins between two parties, the users' private keys have to be sent to "the cloud".

> *I generate my private key and send it to the cloud. Then I get back [from the cloud] a public key... I must be able to rely on the channel to be secure, e.g., encrypted, when I send my private key to the cloud.* (S22)

Through contextual information from this interview, we can deduce that S22 was not referring to storing a key in the cloud (which would be a correct mental model), but to sending it to the cloud in order for the blockchain to get decrypted.

One participant assumed that they have to send the private key directly to the recipient. This would crucially harm the user's security as it would enable the receiver to have access to the sender's account. As most of our participants were not aware of the fact that the private key is generated on their side, they also did not understand that the private key should never be exposed to external entities (such as miners, central entities, or other system participants).

Our participants also lacked understanding of the signing process. Some stated that the receiver has to sign the transaction. Others thought that both, the sender and the receiver have to sign. A few participants inaccurately stated that the miners have to sign transactions. Several participants assumed that other end users in the system are signing transactions in order to validate them. One participant stated that other end users as well as the miners have to sign a transaction. A participant claimed that a user's keys were necessary in order to access the blockchain. As a result, users frequently did not understand why and how they should keep their private key safe, given that they did not understand what a private key can be used for.

We observed many incorrect card assignments and descriptions not matching our ground truth model in relation to cryptocurrency addresses. It was unclear to many participants what a cryptocurrency address actually is. One participant thought that the private key is a user's Bitcoin address. This misconception is especially severe as it might encourage a participant to share the private key with other participants. Many participants assumed that the generated keys and cryptocurrency address are entirely independent. Some participants assumed that the address is a form of nickname, similar to a pseudonym which you choose on a message board.

Such misinterpretations of key generation and usage can have a major security impact if cryptocurrency tools delegate the responsibility of key generation or management to the users without providing guidelines. If, due to misconceptions, users make their keys accessible to others, they become susceptible to theft.

4.3.2 Fees

Our participants expressed many incorrect assumptions about how fees are calculated and what their purpose is. A few participants explicitly stated a lack of knowledge in this regard. One participant thought that fees are defined by an administrator, two said that the miners select the amount. Others stated that the amount of fees is fixed.

> *Miners ask for transaction fees, I don't know if I can choose the amount...If I want to send money and I am in a hurry, for example in the case of smart contracts, then it is possible that the miner knows that I am in a hurry and the miner adds an exorbitant amount of transaction fees [to my transaction].* (S20)

As a result of such misconceptions, users might pay transaction fees that are too high in comparison to the amount that would have been needed to fulfill their requirements, if no guidelines are provided by cryptocurrency tools.

4.3.3 Anonymity Misconceptions

During the coding process, further themes related to anonymity in cryptocurrency systems emerged from our collected data which are not directly related to our generated mental models. A few participants assumed that transactions stored in the blockchain are deleted after some time.

> *After 8 blocks one blockchain is ready and it becomes one instance...Then, the old one is deleted.* (S8)

This entails a wrong assessment of privacy features offered by the blockchain. Participant S8 perceived the blockchain as oblivious and drew a garbage can where old transactions are disposed/recycled (this is only correct within the Lightning network [1], which S8 was not referring to). S8 stated that it is not possible to store a too big amount of data in the blockchain. Many participants incorrectly assumed that the cryptocurrency system applies some form of encryption by default. The participants imagined that either the blockchain, the transaction, or the transaction channel between the end points is encrypted.

> *The transaction itself must be encrypted to ensure a secure connection between server and client.* (S29)

One participant argued that the cryptographic puzzle or hashing is an en-/decryption operation necessary to get access to the money which was sent.

> *Alice receives the cryptographic puzzle, but I don't know what happens if she can't solve it...Because, I mean the bottom line is, I encrypt it [some kind of transaction code] and she receives it.* (S17)

Furthermore, some participants thought about encryption as a major factor used for security purposes. However, those participants commonly also stated that it is necessary to have some kind of additional knowledge in order to pursue this kind of cryptographic task.

> *I guess you can encrypt them [the transactions], however I do not know how.* (S20)

These misconceptions violate participants' privacy as they incorrectly assume that information in the blockchain is unreadable by the public. Moreover, in line with the findings by Gao et al. [16], it might discourage people from using cryptocurrencies when they are under the assumption that only participants with cryptographic knowledge are able to correctly apply privacy or security measures (i.e., encrypting the blockchain).

4.4 Mental Models of Security Threats and Prevention

Most of our participants were able to explain a broad spectrum of (potential) security risks. The majority of our participants mentioned threats related to compromised end points (e.g., mobile phones), which are indeed present as shown in a Kaspersky [22] report. However, this threat is not limited to cryptocurrency applications. Furthermore, our participants named mining majority attacks (i.e., an attacker controlling more than 50% of the mining power in the network). No mining majority attack has yet been performed on Bitcoin or Ethereum, although Bitcoin Gold experienced a 51% attack in May 2018, and a theoretical approach of an Eclipse attack on Ethereum has been described by Yuval et al. [33]. Therefore, there is a possibility that such an attack could happen in a larger cryptocurrency system, especially when ownership and mining are increasingly concentrated on a small group of people [36].

Many participants referred to attacks related to human failure, such as people losing their private keys or failing to store keys in a secure way. This is in line with results from Krombholz et al. [29] and newspaper articles [21] providing evidence that key loss is often caused by the users themselves. Some mentioned the threat of online exchanges being hacked, which has indeed been reported frequently [30]. Others mentioned price fluctuations or intentional price manipulation (e.g., through fake news) as risk factors. Furthermore, some participants correctly stated that Denial-of-Service (DoS) attacks on cryptocurrency systems [8] pose a potential security risk.

In contrast, some participants revealed an incorrect understanding of the threat landscape in cryptocurrency systems and described attacks which are not feasible in a decentralized system. A few participants stated that hacking of central entities, such as the miners, full nodes, or (parts of) the P2P network is feasible. Some described Man-in-the-Middle attacks as a possibility, where an attacker interferes or manipulates the transaction process and possibly alters information (e.g., the recipient's address).

Other participants reported not to be aware of any security risks and to consider cryptocurrency systems to be secure by design. Some of our participants assumed theoretical threats such as broken or weak cryptography that might expose users to a security risk.

Related to *prevention mechanisms against security threats*, more than half of the participants mentioned self-initiated behavior (such as storing private keys securely). Moreover, many referred to the usage of specific hardware (e.g., hardware wallets) and mentioned software (e.g., secure wallets) as a remedy against security breaches. In relation to that, participants described possible prevention mechanisms initiated by the cryptocurrency system, thinking that users cannot influence their execution. Many participants described feeling helpless as they do not think that (technically non-adept) users can actively apply any measures to circumvent such threats.

> *Maybe I can keep a low profile and I shouldn't sit in the tram with the app because of shoulder-surfing... As a non-professional I cannot really do more.* (S22)

4.5 Mental Models of Privacy Threats and Prevention

Some participants assumed that they are anonymous when using cryptocurrencies. However, the majority mentioned address mapping as a possible privacy threat, which is indeed possible [2, 26]. The second biggest privacy threat people mentioned was identity disclosure through third parties, since it is often mandatory to provide identification when purchasing or exchanging cryptocurrencies. Doxxing (writing private data into the blockchain) and a privacy-threatening attack of the end points (e.g., hacking) were also mentioned. Notably, potential future attacks with the help of quantum computers or artificial intelligence were referred to by several participants. Some thought that the state might be a possible attacker or named external persons with bad intentions as relevant attackers. In contrast, others thought that the system participants themselves might carry out attacks on their privacy.

With respect to *prevention mechanisms against arising privacy threats*, participants referred to the possibility to mine themselves in order to prevent identity disclosure when buying cryptocurrencies. A few participants explained that it is possible to buy cryptocurrencies from a specific third party which does not require identity disclosure. One participant assumed that the usage of two-factor authentication would ensure privacy:

> *To secure myself against the threat that IP addresses can be mapped [to bitcoin addresses], I use two-factor authentication.* (S7)

Some explicitly stated not to care about the prevention of privacy threats as they do not consider them important or do not assume that privacy issues exist in decentralized systems.

4.6 Tool Bias

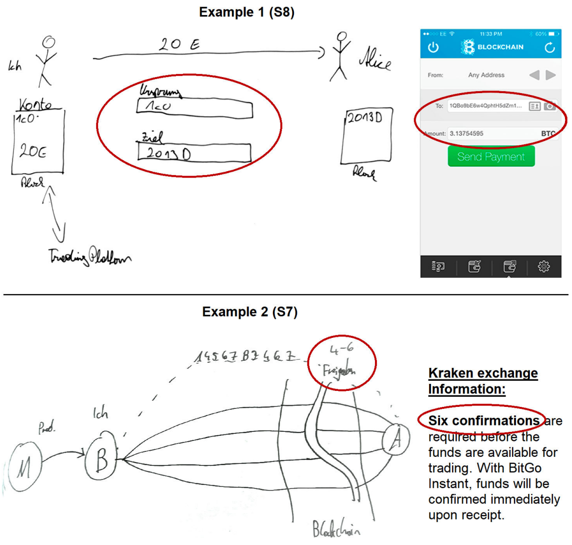
Many cryptocurrency users focused their explanations and drawings of the transaction process on the graphical user interface which they are exposed to when performing transactions, either via a mobile wallet, a PC wallet, or an online exchange. We observed that wallet interfaces shaped the way participants perceived the blockchain location (centralized vs. decentralized), its functionality (persistent, transparent), and the users' role within the cryptocurrency system.

Figure 6 shows a drawing (example 1) which is influenced by the interface displayed to users when carrying out transactions via mobile phone. In particular, we found that our participants were frequently influenced by a feature of the interfaces currently used by many online exchanges and wallets (Figure 6 example 2). Thereby, the current number of confirmations is displayed to show how many blocks are already successfully mined and incorporated in the heaviest chain of the blockchain. After a specific number of succeeding blocks the current transaction is marked as "accepted". However, we can deduce from our study that users commonly misinterpret these confirmations as a specific number of miners or peers who signed, approved, or validated their transaction. Even among experts, a specific fixed number of confirmations is assumed, although the security actually depends on the weight of the longest chain (see Sompolinsky and Zohar [41]).

In contrast to the cryptocurrency tool bias for cryptocurrency users, we discovered a **bank bias** for non-users. They often stated that the blockchain is centrally managed or that transactions are conducted directly between users.

4.7 Expert Focus Group

In order to construct our theory, we discussed the security and privacy impact of our participants' mental models in an expert focus group which consisted of four members from a different research group at our institution who are primarily researching blockchain technology. One researcher led the discussion and two researchers took notes and asked follow-up questions. First, we presented our incorrect model to all participants and provided printouts. Then, we discussed the incorrect model in three rounds based on the categories resulting from the selective coding (keys, fees, anonymity misconceptions). In each round we first presented the identified misconceptions and then asked our participants whether they think that these categories interfere with security and privacy. If the answer was yes, we asked for the experts' opinions on how these security problems could be prevented. Our discussion and improvement suggestions for cryptocurrency tools are based on the outcome of this focus group.



From: Any Address

To: 1QBo9bE6w4QphtH5dZm1...

Amount: 3.13754595 BTC

Kraken exchange Information:

Six confirmations are required before the funds are available for trading. With BitGo Instant, funds will be confirmed immediately upon receipt.

Figure 6: Illustrating cryptocurrency tool bias

We decided on a final set of categories which are important for our theory generation since they have a direct impact on users' security and privacy. These categories are (i) **keys**, (ii) misconceptions regarding **anonymity**, and (iii) **fees**. The resulting mental models are centered around these aspects of our participants' mental representations. The anonymity misconceptions only emerged from the participants' descriptions of the transaction process and were not reflected in their drawings.

Regarding the questions of how cryptocurrency tools could prevent security problems caused by incorrect mental models, the focus group brought up the challenge of designing tools which are adapted to the diverging mental models we found. There is a thin line between an easy-to-use system and a system that gives (expert) users the feeling of being too simple to be secure, and also provides too little information to evaluate the system. Therefore, the focus group proposed that the user interfaces of cryptocurrency tools should have options to switch between different levels of complexity, providing the user with the chance to interact with the system and obtain detailed information about it only if desired. This approach has been (partly) implemented by Coinomi [10] (see Appendix A.3) and should be a standard feature for all (future) wallets.

5 Discussion

Our results explain the roots of several misconceptions with impact on security and privacy found in related work [12, 16, 29] and can be directly linked to concrete improvement suggestions for cryptocurrency tools (e.g., wallets or exchanges).

We claim that modifications of the interface of cryptocurrency management tools can prevent security and privacy threats caused by incorrect mental models. We base this claim on our observation that there is a **cryptocurrency tool bias** of cryptocurrency users (see Section 4.6). Our results indicate that users' mental models are influenced by the interfaces of tools and technologies they use, which will be subject to further research.

5.1 Challenges and Improvement Suggestions

We found a wide range of mental models, from very detailed to sparse and from correct to incorrect. Hence, we suggest – in line with the outcome from our focus group – to design cryptocurrency tools adapted to diverging mental models and different user groups (e.g., experts and non-experts). Therefore, we suggest that cryptocurrency tool providers ought to offer **different levels of complexity**.

In the following, based on the results from our study and the experts focus group, we discuss how current cryptocurrency tools should be adapted to allow people to use them in a secure and privacy-preserving manner, irrespective of their (incorrect) mental models.

5.1.1 Anonymity

We noticed that about a quarter of our participants used the term "encryption" when describing a transaction process in cryptocurrency systems. Many participants stated that the blockchain is encrypted. We hypothesize that these users mixed up authentication/signing (which indeed takes place during a transaction process) and encryption. Most of these participants assumed that encryption is a safety measure against security- or privacy breaches. Moreover, many participants presumed that transactions cannot be tracked due to the encryption of the blockchain. We claim that such misconceptions jeopardize people's privacy as some participants were incorrectly assuming that their information is hidden from the public or that all information is deleted after some time. Our results suggest that people with these misconceptions refrain from taking measures to safeguard their privacy while believing that they are anonymous.

Furthermore, we revealed misconceptions about the persistence of the blockchain. We infer from discussions with industrial partner institutions that blockchain technologies are commonly applied in areas where it does not make sense, such as for ephemeral data. The mental models we found in the course of this study explain such a contradiction.

Recommendation: *Interfaces of cryptocurrency tools should illustrate the openness, persistence, and transparency of the blockchain. For example, a block explorer could be integrated, visualizing in which block a transaction is integrated and how many succeeding confirmed blocks currently exist. Some wallets (see Appendix A.3) provide access to textual block explorers as an additional feature; however, there is no graphical visualization integrated into the wallets. Furthermore, a pop-up could be shown before pursuing a transaction, stating that this transaction will be broadcasted in clear text to the cryptocurrency network and no information can be altered later on.*

5.1.2 Cryptographic Keys

Previous research on public key cryptography for e-mail encryption has shown that users have difficulties managing and understanding asymmetric keys [38, 44]. Our study supports this finding as less than half of our participants were able to correctly describe how keys are generated and used. Until the time of writing, no holistic solution has been proposed to solve these issues. Bitcoin and Ethereum use keys differently than for example PGP (i.e., it is only used to sign data instead of also encrypting it) and come with an unexplored and diverse user group. Nevertheless, no research has been conducted so far to examine how people understand the function of keys in the context of cryptocurrency systems.

The misconceptions about cryptographic keys, as found during our study, directly influence the way users manage their keys, thus putting them at risk for monetary loss and fraud.We observed that many users did not draw a connection between their private key and the ability to carry out transactions from their account. Moreover, we discovered misconceptions in relation to the key generation. We suppose that these incorrect perceptions interfere with a secure key management if users are not aware of the fact that private keys give access to their funds and should be known only to their owner, hence being kept safe locally.

In line with research on usable key management in other domains [38, 39], we suggest to automate tools as far as possible so that users do not have to deal with key generation or key back-ups, while still providing as much transparency and information as needed to not expose users to security or privacy risks (for a feature overview of key storage and back-up systems from popular wallets, see Appendix A.3).

For cryptocurrency systems this means that users must at least understand that their seed phrase (or private key) (i) should not be shared with anybody else, and (ii) can currently not be recovered in case of loss, leading to the loss of all funds. These facts should be emphasized to the user during wallet initialization and whenever the wallet is used, as discussed in the above sections.

Recommendation: *In order to avoid that users lose their seed phrases, wallets should enforce seed phrase back-ups by asking the users to input a certain number of words from their phrase after making a copy (e.g., writing it down on paper, taking a picture, copying it on a USB device). Furthermore, wallets should ask users to enter their seed phrases in specific time intervals to ensure that they maintain access. Most current wallets do not implement these features (see Appendix A.3). Alternatively, we suggest using automatic key recovery (e.g., similar to trusted friends [14]).*

5.1.3 Fees

Currently, many cryptocurrency tools only offer one fixed amount for fees. Our results show that due to this practice, the majority of participants do not know that users can actively select how much they want to pay as mining fees during the creation of a transaction. Therefore, users are not aware that it is in their power to select how quickly their transaction will be included in the blockchain. As a result, users might pay transaction fees that are too high in comparison to the actual amount needed for their requirements.

Recommendation: *User interfaces of cryptocurrency tools should remind users that by choosing the amount of transaction fees they can influence how quickly their transaction will be included in the next block. The amount of fees should be precomputed based on heuristics (leading to different amounts for each user and transaction) and labeled with understandable terms (e.g., "slow—low fees", "default" and "fast—high fees"). A comparable approach is provided by the Blockchain [5] and Coinomi [10] wallet (see Appendix A.3).*

5.1.4 Security and Privacy Threats and Prevention

We discovered that while our participants showed a basic understanding of the threat landscape in cryptocurrency systems, their knowledge about possible prevention mechanisms was poor and led to a feeling of helplessness among half of them. These participants either believed that users cannot take any measures, but need to rely on the system, or they assumed that prevention mechanisms (e.g., wallet encryption) can only be pursued by technologically knowledgeable users. This coincides with the results found by Krombholz et al. [29] which showed that many users do not apply security measures offered by state-of-the-art cryptocurrency tools.

Recommendation: *We suggest that cryptocurrency tools should perform encryption by default and inform the users about this safety measure (see Appendix A.3 for the status of popular wallets). Moreover, they should add cues and visualizations to explain to the users which security measures (e.g., encryption) are implemented so that users can make informed trust decisions.*

6 Limitations & Future Work

Participant recruitment via mailing lists, social media, and personal contacts provided us with a diverse sample regarding age and profession. However, our sample still has its limitations as it is biased towards a higher educated social stratum; also, non-users without any connection to cryptocurrencies were excluded. Furthermore, the recruiting area was limited to two cities in Austria. Therefore we cannot compare or evaluate cultural differences to other countries/continents, and the European legal landscape with regard to security and privacy (GDPR) also most likely influenced the participants.

The interviews were conducted in German, which is why language-specific expressions in direct participant quotes may have been lost in translation. However, all direct translations were double-checked by a translator, which is why we are confident that such issues have been kept to a minimum.

We followed an inductive approach for our qualitative study to gather insights into user perceptions of cryptocurrency systems. However, our methodology also has its limitations as the data is self-reported and, in comparison to quantitative studies, the sample size is fairly small. Still, we feel confident that our sample is sufficiently large to observe general tendencies.

This study provides the basis for future work to quantify our findings. We plan to examine the connection between mental models, experiences with cryptocurrency management tools, and security-critical errors. Moreover, usable cryptocurrency management tools can be designed and evaluated based on our findings.

7 Conclusions

We explored user perceptions and misconceptions of cryptocurrency users ($N = 29$) enriched with drawing and card assignment tasks. Although our study focused on Bitcoin and Ethereum, our findings can be further useful for improving the security and privacy of a large body of (existing or future) altcoins which also build on the blockchain technology.

We discovered that flaws and inconsistencies in user mental models of cryptocurrency systems expose users to security and privacy risks when using current cryptocurrency tools. These risks include money loss, fraud, or deanonymization. Most importantly, we revealed major misconceptions related to the functionality and management of cryptographic keys which are not compensated by the cryptocurrency tools. Our findings explain why cryptocurrency users fail to manage their private keys securely and, as a result, frequently fall victim to money loss and fraud. Furthermore, we revealed that users think that the blockchain is encrypted or oblivious, which prevents them from taking measures to safeguard their privacy. Another interesting result was that many participants were not aware of the fact that the amount of mining fees can be actively selected to influence the transaction speed.

We proposed several concrete enhancements to state-of-the-art cryptocurrency tools (e.g., wallets or exchanges) with the purpose of protecting users with misconceptions from security and privacy threats. Among others, we suggest to automate key generation, -management, and -back-up as much as possible. With our work, we lay the foundation for improving the usability of state-of-the-art cryptocurrency management tools to prevent security and privacy breaches.

8 Acknowledgments

We thank the anonymous reviewers, our shepherd, and Michael Schilling for their valuable feedback on our work. SBA Research (SBA-K1) is a COMET Centre within the framework of COMET – Competence Centers for Excellent Technologies Programme and funded by BMK, BMDW, and the federal state of Vienna. The COMET Programme is managed by FFG. The financial support by the Christian Doppler Research Association, the Austrian Federal Ministry for Digital and Economic Affairs and the National Foundation for Research, Technology and Development is gratefully acknowledged.

References

[1] Lightning network. https://lightning.network/, 2020. Accessed: 2020-01-31.

[2] Elli Androulaki, Ghassan O. Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun. Evaluating user privacy in bitcoin. *International Conference on Financial Cryptography and Data Security (FC'13)*, 2013.

[3] Maria Apostolaki, Aviv Zohar, and Laurent Vanbever. Hijacking bitcoin: Routing attacks on cryptocurrencies. *IEEE Symposium on Security and Privacy (S&P'17)*, 2017.

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

[5] Blockchain. Blockchain.com. https://www.blockchain.com/wallet. Accessed: 2020-05-26.

[6] Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A Kroll, and Edward W Felten. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. *IEEE Symposium on Security and Privacy (S&P'15)*, 2015.

[7] Anne E Brodsky. Negative case analysis. *The SAGE encyclopedia of qualitative research methods*, page 553, 2008.

[8] David Canellis. Crippling DoS vulnerability put the entire Bitcoin market at risk. https://thenextweb.com/hardfork/2018/09/20/bitcoin-core-vulnerability-blockchain-ddos/, 2018. Accessed: 2020-01-31.

[9] Coinmarketcap. Coinmarket. Cryptocurrency Market Capitalizations. https://coinmarketcap.com/coins/, Accessed: 2019-05-06.

[10] Coinomi. Coinomi. https://www.coinomi.com/en/. Accessed: 2020-05-26.

[11] Chris Elsden, Arthi Manohar, Jo Briggs, Mike Harding, Chris Speed, and John Vines. Making Sense of Blockchain Applications: A Typology for HCI. *SIGCHI Conference on Human Factors in Computing Systems (CHI'18)*, 2018.

[12] Shayan Eskandari, Jeremy Clark, David Barrera, and Elizabeth Stobert. A first look at the usability of bitcoin key management. *arXiv preprint arXiv:1802.04351*, 2018.

[13] Blockchain Explorer. Block #0. https://www.blockchain.com/btc/block-index/14849, 2019. Accessed: 2019-09-17.

[14] Facebook. How can I choose friends to help me log in if I ever get locked out of my account? https://www.facebook.com/help/119897751441086/, 2019. Accessed: 2019-08-27.

[15] Kevin Gallagher, Sameer Patil, and Nasir Memon. New Me: Understanding Expert and Non-Expert Perceptions and Usage of the Tor Anonymity Network. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS'17)*, pages 385–398. USENIX Association, 2017.

[16] Xianyi Gao, Gradeigh D. Clark, and Janne Lindqvist. Of Two Minds, Multiple Addresses, and One Ledger: Characterizing Opinions, Knowledge, and Perceptions of Bitcoin Across Users and Non-Users. *SIGCHI Conference on Human Factors in Computing Systems (CHI'16)*, 2016.

[17] Juan Garay, Aggelos Kiayias, and Nikos Leonardos. The bitcoin backbone protocol: Analysis and applications. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 281–310. Springer, 2015.

[18] Barney G Glaser and Anselm L Strauss. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Transaction publishers, 1967.

[19] Greg Guest, Arwen Bunce, and Laura Johnson. How many Interviews are enough? An Experiment with Data Saturation and Variability. *Field methods*, 18(1):59–82, 2006.

[20] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. My Data just goes Everywhere: User Mental Models of the Internet and Implications for privacy and security. In *Symposium on Usable Privacy and Security (SOUPS'15)*, pages 39–52. USENIX Association Berkeley, CA, 2015.

[21] Michael Kaplan. I accidentally threw away $60M worth of Bitcoin . https://nypost.com/2018/05/26/i-accidentally-threw-away-60m-worth-of-bitcoin/, 2019. Accessed: 2019-05-02.

[22] Kaspersky. The number of mobile malware attacks doubles in 2018. https://www.kaspersky.com/about/press-releases/2019_the-number-of-mobile-malware-attacks-doubles-in-2018-as-cybercriminals-sharpen-their-distribution-strategies, Accessed: 2019-05-06.

[23] Ali Kazerani, Domenic Rosati, and Brian Lesser. Determining the Usability of Bitcoin for Beginners Using Change Tip and Coinbase. pages 1–5. ACM Press, 2017.

[24] Anne R. Kearney and Stephen Kaplan. Toward a Methodology for the Measurement of Knowledge Structures of Ordinary People: The Conceptual Content Cognitive Map (3CM). *Environment and Behavior*, 29(5):579–617, 1997.

[25] Irni Eliana Khairuddin, Corina Sas, Sarah Clinch, and Nigel Davies. Exploring Motivations for Bitcoin Technology Usage, 2016.

[26] Philip Koshy, Diana Koshy, and Patrick McDaniel. An analysis of anonymity in bitcoin using p2p network traffic. *International Conference on Financial Cryptography and Data Security (FC'14)*, 2014.

[27] Klaus Krippendorff. Content Analysis: An Introduction to It's Methodology. pages 241–243. SAGE Publications, 2004.

[28] Katharina Krombholz, Karoline Busse, Katharina Pfeffer, Matthew Smith, and Emanuel von Zezschwitz. " if https were secure, i wouldn't need 2fa"-end user and administrator mental models of https. *IEEE Symposium on Security and Privacy (S&P'19)*, 2019.

[29] Katharina Krombholz, Aljosha Judmayer, Matthias Gusenbauer, and Edgar Weippl. The Other Side of the Coin: User Experiences with Bitcoin Security and Privacy. *International Conference on Financial Cryptography and Data Security (FC'16)*, 2016.

[30] Eric Larcheveque. 2018: A record-breaking year for crypto exchange hacks. https://www.coindesk.com/2018-a-record-breaking-year-for-crypto-exchange-hacks, Accessed: 2019-05-06.

[31] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. *Research Methods in Human-Computer Interaction*. Morgan Kaufmann, 2017.

[32] C. Lustig and B. Nardi. Algorithmic Authority: The Case of Bitcoin. In *2015 48th Hawaii International Conference on System Sciences*, pages 743–752, Jan 2015.

[33] Yuval Marcus, Ethan Heilman, and Sharon Goldberg. Low-resource eclipse attacks on ethereum's peer-to-peer network. *IACR Cryptology ePrint Archive*, 2018(236), 2018.

[34] Rafael Pass, Lior Seeman, and Abhi Shelat. Analysis of the blockchain protocol in asynchronous networks. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 643–673. Springer, 2017.

[35] Mark Perry and Jennifer Ferreira. Moneywork: Practices of Use and Social Interaction around Digital and Analog Money. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 24(6):41, 2018.

[36] Burgess Powell. Not Only Is A 51% Attack On Blockchain Possible, But It's Coming. https://blocklr.com/news/51-attack-blockchain-more-likely-than-you-think/, 2018. Accessed: 2019-04-24.

[37] Karen Renaud, Melanie Volkamer, and Arne Renkema-Padmos. Why doesn't Jane Protect her Privacy? In *International Symposium on Privacy Enhancing Technologies Symposium*, pages 244–262. Springer, 2014.

[38] Scott Ruoti, Jeff Andersen, Scott Heidbrink, Mark O'Neill, Elham Vaziripour, Justin Wu, Daniel Zappala, and Kent Seamons. "we're on the same page": A usability study of secure email using pairs of novice users. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, page 4298–4308, New York, NY, USA, 2016. Association for Computing Machinery.

[39] Scott Ruoti, Jeff Andersen, Tyler Monson, Daniel Zappala, and Kent Seamons. A comparative usability study of key management in secure email. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS'18)*, pages 375–394, 2018.

[40] Corina Sas and Irni Eliana Khairuddin. Design for Trust: An Exploration of the Challenges and Opportunities of Bitcoin Users. 2017.

[41] Yonatan Sompolinsky and Aviv Zohar. Bitcoin's Security Model Revisited. *arXiv preprint arXiv:1605.09193*, 2016.

[42] Anselm Strauss, Juliet Corbin, et al. *Basics of Qualitative Research*, volume 15. Newbury Park, CA: Sage, 1990.

[43] Rick Wash and Emilee Rader. Influencing Mental Models of security: A Research Agenda. In *Proceedings of the 2011 workshop on New security paradigms workshop*, pages 57–66. ACM, 2011.

[44] Alma Whitten and J Doug Tygar. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *USENIX Security Symposium*, volume 348, 1999.

[45] Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander. Where Is Current Research on Blockchain Technology? - A Systematic Review. *PLOS ONE*, 11(10), October 2016.

[46] Eric Zeng, Shrirang Mare, and Franziska Roesner. End User Security & Privacy Concerns with Smart Homes. In *Symposium on Usable Privacy and Security (SOUPS'17)*, 2017.

A Mental Model User Study

A.1 Demographics gathered via a pre-study questionnaire

- Age/ Gender
- Profession/ Highest completed level of education/ Recent professional status
- I have a good understanding of Computers and the Internet: Likert Scale from 5 (agree) - 1 (disagree)
- I often ask other people for help when I am having problems with my computer: Likert Scale from 5 (agree) - 1 (disagree)
- I am often asked for help when other people have problems with their computer. Likert Scale from 5 (agree) - 1 (disagree)
- Which cryptocurrencies have you heard of?
- Was the subject of cryptography and/or cryptocurrencies part of your education or your profession?
- If yes, briefly outline the topics you heard of.
- Do you use Bitcoin/Ethereum?
- For which matters do you mainly use Bitcoin/Ethereum?

A.2 Interview Protocol

General

- Which kind of education do you have and what is your current profession?
- When and how did you become aware of cryptocurrencies?
- How have you been dealing with cryptocurrencies so far?
- Why do you use Bitcoin/Ethereum? (just asked if the participant owns a cryptocurrency)
- What is in your opinion the cryptographic part of cryptocurrencies?

Mental Models

- **[Drawing Task 1]** Please draw a picture of how you think the transaction process works between you and a second person called Alice. Imagine you transfer BTC/ETH 20 to Alice. Remember to include all relevant persons and components into your drawing.
- **[Card Assignment Task]** We prepared some cards which describe various functionalities of a cryptocurrency system. Please assign these cards to the components you drew in Phase 1. If you feel you missed a component before, please draw them with green colour. The cards we provided during this task:
  - Generate address
  - Generate public key
  - Generate private key
  - Transaction confirmed
  - Generate transaction
  - Sign transaction
  - Broadcast transaction
  - Verify transaction
  - Generate block
  - Validate block
  - Perform Proof of Work
  - Solve cryptographic puzzle
  - Receive transaction fees
  - Generate coins
  - Only Bitcoin: Receive unspent transaction output (UTXO)
  - Only Ethereum: Receive balance

Attacker Models

- There are two words which are lately frequently used in the media in relation to cryptocurrencies, namely "security" and "privacy". What do these two words mean to you and what are the differences between them?

- **[Drawing Task 2]** Please have a look on the model you created during Phase 2. Take a red marker for drawing security risks and a blue marker for drawing privacy risks. While drawing, keep the following two questions in mind:

  - Where do you think the potential threats occur?
  - Who is causing those threats?

  After the participant has finished the drawing, ask: "What countermeasures do you know to prevent those risks?"

A.3 Wallet Feature Overview

Table 2: Feature overview of 4 popular software wallets at the time of our study

	Blockchain.com	Coinbase.com	Coinomi	Exodus
Founded	2011	2012	2013	2015
Supported Cryptocurrencies	BTC, ETH, BCH, XLM, USD-D	BTC, ETH, BCH, ETC, LTC, ERC-20 tokens	BTC, ETH, BCH, ETC, LTC, etc.	BTC, ETH, BCH, ETC, LTC, etc.
Type	wallet/exchange	wallet/exchange	wallet/exchange	wallet/exchange
Private key storage	local	local	local	local
Back-ups	user initiated (seed phrase)	user initiated (seed phrase, gdrive with PIN)	user initiated (seed phrase)	user initiated (seed phrase)
Force seed phrase back-up	yes	no	no	no
Transaction Fees	options (pre-calculated/custom)	no options	options (low/normal/high priority)	no options
Wallet encryption	password (forced)	fingerprint/ PIN (forced)	password (standard)/ biometric/ none	none (standard)/ PIN / fingerprint
Periodic seed phrase querying	no	no	no	no
Block explorer included	yes (textual)	yes (textual)	yes (textual)	no
Different complexity levels	no	no	yes (creation: "fast", "advanced")	no

A.4 Coding Frequencies

Table 3: Coding Frequencies

A	Total	K	LA	BA	B	Total	K	LA	BA		Total	K	LA	BA	C	Total	K	LA	BA
A.1					B.1					B.4.5					C.1				
A.1.1	1	0	0	1	B.1.1	10	4	2	4	B.4.5.1	2	1	0	1	C.1.1	3	1	2	0
A.1.2	6	3	3	0	B.1.2	4	1	2	1	B.4.5.2	25	9	9	7	C.1.2	14	2	8	4
A.1.3	6	2	2	2	B.1.3	2	0	1	1	B.4.5.3	1	0	1	0	C.1.3	18	7	7	4
A.1.4	1	1	0	0	B.1.4	14	5	7	2	B.4.5.4	2	0	1	1	C.1.4	2	1	1	0
A.2	7	3	3	1	B.1.5	2	0	2	0	nm	1	0	1	0	C.1.5	1	0	0	1
A.3	10	3	5	2	nm	4	1	1	2	LOK	0	0	0	0	C.1.6	5	1	3	1
A.4	2	0	0	2	LOK	0	0	0	0	B.4.6					C.1.7	2	0	1	1
A.5	7	1	2	4	B.2					B.4.6.1	1	0	0	1	C.1.8	5	2	1	2
					B.2.1	4	2	2	0	B.4.6.2	6	3	3	0	C.2				
					B.2.2	6	3	2	1	B.4.6.3	3	1	1	1	C.2.1	0	0	0	0
					B.2.3	3	0	3	0	B.4.6.4	3	0	2	1	C.2.2	4	1	2	1
					B.2.4	2	1	0	1	B.4.6.5	2	0	1	1	C.2.3	5	0	4	1
					B.2.5	20	8	10	2	nm	12	5	3	4	C.2.4	3	1	1	1
					B.2.6	1	0	0	1	LOK	4	1	3	0	C.2.5	5	1	1	3
					nm	6	1	1	4	B.4.7					C.2.6	3	2	1	0
					LOK	1	0	0	1	B.4.7.1	4	1	2	1	C.2.7	4	0	3	1
					B.3					B.4.7.2	3	2	1	0	nm	13	5	6	2
					B.3.1					B.4.7.3	3	1	2	0	**D**	**Total**	**K**	**LA**	**BA**
					B.3.1.1	6	0	5	1	B.4.7.4	1	0	1	0	D.1				
					B.3.1.2	1	1	0	0	B.4.7.5	6	3	1	2	D.1.1	2	0	2	0
					B.3.1.3	0	0	0	0	B.4.7.6	0	0	0		D.1.2	11	2	6	3
					B.3.1.4	5	2	2	1	nm	12	3	5	4	D.1.3	7	0	5	2
					nm	15	6	5	4	LOK	0	0	0	0	D.1.4	15	4	8	3
					LOK	5	1	2	2	B.4.8					D.1.5	5	1	3	1
					B.3.2					B.4.8.1	23	10	11	2	D.1.6	9	3	4	2
					B.3.2.1	1	0	0	1	B.4.8.2	1	1	0	0	D.1.7	4	2	1	1
					B.3.2.2	9	3	5	1	B.4.8.3	1	0	1	0	D.1.8	14	4	6	4
					B.3.2.3	7	2	1	4	B.4.8.4	3	0	1	2	D.1.9	7	2	4	1
					B.3.2.4	3	1	1	1	nm	1	0	0	1	D.1.10	2	1	1	0
					B.3.2.5	1	0	0	1	LOK	2	0	0	2	D.1.11	2	0	0	2
					nm	11	5	4	2	B.4.9					D.1.12	3	2	1	0
					LOK	0	0	0	0	B.4.9.1	2	1	0	1	D.1.13	10	2	7	1
					B.3.3					B.4.9.2	4	1	1	2	D.1.14	7	3	2	2
					B.3.3.1	2	2	0	0	B.4.9.3	1	0	0	1	D.1.15	3	1	1	1
					B.3.3.2	5	2	2	1	B.4.9.4	11	2	6	3	D.1.16	4	0	1	3
					B.3.3.3	1	0	0	1	B.4.9.5	2	0	0	2	D.2				
					nm	0	0	0	0	B.4.9.6	1	0	1	0	D.2.1	5	1	2	2
					LOK	0	0	0	0	B.4.9.7	18	8	8	2	D.2.2	7	2	4	1
					B.4					B.4.9.8	6	5	1	0	D.2.3	15	2	7	6
					B.4.1					nm	0	0	0	0	D.2.4	10	3	5	2
					B.4.1.1	1	0	1	0	LOK	4	0	2	2	D.2.5	13	4	4	5
					B.4.1.2	1	1	0	0	B.4.10					nm	2	0	2	0
					B.4.1.3	1	0	1	0	B.4.10.1	2	0	1	1					
					B.4.1.4	3	1	1	1	B.4.10.2	2	0	0	2					
					B.4.1.5	19	8	8	3	B.4.10.3	9	4	5	0					
					B.4.1.6	2	1	1	0	nm	11	4	2	5					
					B.4.1.7	1	0	0	1	LOK	5	1	4	0					
					nm	1	0	0	1	B.5									
					LOK	3	0	1	2	B.5.1									
					B.4.2					B.5.1.1	13	4	6	3					
					B.4.2.1	4	0	4	0	B.5.1.2	1	0	1	0					
					B.4.2.2	1	0	1	0	B.5.1.3	4	1	0	3					
					B.4.2.3	2	1	0	1	B.5.1.4	6	3	2	2					
					B.4.2.4	2	1	0	1	B.5.1.5	6	2	1	3					
					nm	17	8	6	3	B.5.1.6	2	0	0	2					
					LOK	3	0	1	2	B.5.1.7	2	2	0	0					
					B.4.3					B.5.1.8	1	0	0	1					
					B.4.3.1	4	0	0	4	B.5.1.9	1	0	1	0					
					B.4.3.2	3	1	1	1	B.5.1.10	2	2	0	0					
					B.4.3.3	1	0	1	0	nm	0	0	0	0					
					B.4.3.4	16	7	7	2	LOK	3	0	2	1					
					nm	3	1	1	1	B.5.2									
					LOK	3	0	2	1	B.5.2.1	2	0	0	2					
					B.4.4					B.5.2.2	8	4	4	0					
					B.4.4.1	8	3	4	1	nm	16	6	6	4					
					B.4.4.2	4	2	1	1	LOK	3	0	2	1					
					B.4.4.3	11	3	2	6										
					B.4.4.4	2	0	2	0										
					B.4.4.5	4	1	2	1										
					nm	1	0	1	0										
					LOK	1	1	0	0										

The table displays our resulting numbers of the interviews, categorized according out three participation groups (i) knowledgeable user (K) (ii) lay active user (LA) and (iii) blockchain activity (BA).