# The Other Side of the Coin: User Experiences with Bitcoin Security and Privacy

Katharina Krombholz(✉), Aljosha Judmayer,
Matthias Gusenbauer, and Edgar Weippl

SBA Research, Vienna, Austria
{kkrombholz,ajudmayer,mgusenbauer,eweippl}@sba-research.org

**Abstract.** We present the first large-scale survey to investigate how users experience the Bitcoin ecosystem in terms of security, privacy and anonymity. We surveyed 990 Bitcoin users to determine Bitcoin management strategies and identified how users deploy security measures to protect their keys and bitcoins. We found that about 46% of our participants use web-hosted solutions to manage at least some of their bitcoins, and about half of them use exclusively such solutions. We also found that many users do not use all security capabilities of their selected Bitcoin management tool and have significant misconceptions on how to remain anonymous and protect their privacy in the Bitcoin network. Also, 22% of our participants have already lost money due to security breaches or self-induced errors. To get a deeper understanding, we conducted qualitative interviews to explain some of the observed phenomena.

## 1 Introduction

With a current market capitalization of more than 3.5 billion USD, Bitcoin is the most successful cryptographic currency at this time. Bitcoin is utilized for roughly 130.000 transactions per day [6] and has gained significant news coverage. With the success of Bitcoin, several other cryptographic currencies were developed either based on Bitcoin or from scratch.

Although the popularity of cryptographic currencies is increasing, they are not yet a mass phenomenon. One of the reasons is that Bitcoin forces its users to deal with public key cryptography. Furthermore, Bitcoin shifts the responsibilities for most security measures to the end user compared to centralized monetary systems. Even though there is a great variety of software available for managing bitcoins, user-experience is still not obviating the need to deal with the technical fundamentals and to perform backups to recover their virtual monetary assets in case of a loss. Hence, these systems are not resilient to human errors. Reports from online forums and mailing-lists show that many Bitcoin users already lost money due to poor usability of key management and security breaches such as malicious exchanges and wallets. This motivates our research on human interactions with the Bitcoin ecosystem.

Bitcoin users have a huge variety of tools available to manage their virtual assets. These tools are commonly referred to as *wallets*. A wallet was originally


J. Grossklags and B. Preneel (Eds.): FC 2016, LNCS 9603, pp. 555–580, 2017.
DOI: 10.1007/978-3-662-54970-4_33

defined as a collection of private keys [8]. Hence, a piece of paper with a private key on it or even a mental representation can be considered a wallet. However, most of these tools provide functionality beyond storing keys, such as performing transactions. In contrary to other public key crypto-systems, e.g. PGP/GPG, Bitcoin is not fully communication channel agnostic. In case of Bitcoin the interaction with the Bitcoin network is an integral part to operate in the distributed system. In contrast to other signing systems, Bitcoin tools need to keep state information on performed transactions and account balances respectively.

As a first step to accommodate these misconceptions on Bitcoin wallets, we introduce the term *Coin Management Tool (CMT)* as an extension to the current narrow definition of a wallet. We define a CMT as a tool or a collection of tools which allows users to manage one or more core tasks of cryptocurrencies. Throughout this paper we are therefore referring to *Bitcoin management*, as it better describes user activities when interacting with the Bitcoin ecosystem. Bitcoin security and privacy aspects have already been studied in the research literature [7,10,14–16]. A first look on the usability of Bitcoin key management has been presented in [8]. However, we are the first to conduct a comprehensive user study to collect evidence on user experiences with Bitcoin security and privacy.

In this paper, we present a comprehensive user study ($n = 990$) to cover human-computer interaction aspects of the Bitcoin ecosystem. The goal was to understand how users interact with Bitcoin and how they manage their virtual assets. We furthermore studied experiences and perceptions related to security, privacy and anonymity in the Bitcoin network. To collect user-reported data, we conducted a comprehensive online survey with 990 participants and qualitative interviews with a subset of 10 participants. Additionally, we extended the evaluation criteria from [8] and provide a method to categorize CMTs depending on the level of control and verifiability a user can exercise with the respective client.

We gathered interesting insights on how users interact with the Bitcoin network and what privacy and security measures they deploy to protect their keys and coins. We found that the first- and third-most used CMTs (Coinbase, Xapo) are web-hosted tools where users shift security responsibilities to a third party. We also found that about a third of their users are not aware whether their CMT data is encrypted or backed-up. Among the participants who use a web-hosted solution, 50% indicated to use it exclusively while the other half used additional local clients to manage their coins. Regarding risk scenarios and their likelihood to occur, the second-highest risk was attributed to vulnerabilities in web-hosted CMTs (after value fluctuation and followed by theft via malware).

We also found that many users have misconceptions about how to remain anonymous. About 25% of our participants reported to use Bitcoin over Tor which has already shown to be disadvantageous in certain cases [1,3]. 22.5% of the participants reported to have lost their bitcoins due to security breaches. About half of them consider this loss as their own fault and the majority of them was not able to recover their bitcoins and lost money permanently. Our work contributes research on user-centric concerns of Bitcoin management, as according to Bonneau [7] Bitcoin is one of the cases where practice is ahead of theory.

The main contributions of this paper are **(1) a user study consisting of an online survey and qualitative interviews**, and **(2) a method for categorizing Bitcoin CMTs**.

## 2 Bitcoin Background

The Bitcoin currency is based on a distributed P2P system which synchronizes a public ledger of all transactions among all Bitcoin clients. As a consequence, every full client in the Bitcoin network is able to see the entire history containing all prior transactions. Thereby it is possible to determine the current balance of every account. The account information in Bitcoin basically consists of a hash over a public key which can be compared to an account number, the so-called *Bitcoin address*. The protocol does not require a link between account information and personal data. An individual can have more than one account, hence Bitcoin provides a certain degree of pseudonymity [1,9].

To transfer $n$ bitcoins from account $A$, which is under control of Alice, to another account $B$, which is under control of Bob, a new transaction is created by Alice. Thereby, Alice creates a transaction message with the amount of bitcoins she wants to send to Bob and includes the hash of the public key of Bobs account $B$ as a destination before signing it with her secret key $sk_A$. Alice publishes this transaction in the Bitcoin network so that every participant knows that Alice now has $n$ bitcoins less on her account $A$ and Bob has received the difference on his account $B$. When this transaction is successfully propagated in the network, Bob can create new transactions from his account $B$ to another account and spend the previously received bitcoins. This chaining mechanism works fine for passing over arbitrary amounts of bitcoins from one account to another, except in the special case of the first transaction in a chain, because this is where new bitcoins come into existence [20].

Bitcoins are created during the so-called *mining process*. In this procedure every miner collects transactions which have recently been propagated in the P2P network. Then they try to successfully create a new block out of all unconfirmed transactions that have not yet been included in a block of the block chain. A block essentially consists of a collection of valid transactions[1], a nonce value, and a proof of work. The proof of work is a partial pre-image attack on SHA-256 over the whole block as input. For the attack to succeed, the hash has to be a value smaller than the current difficulty in the Bitcoin network. In other words, the SHA-256 hash has to start with a certain number of zero bits. The number of zero bits is referred to as difficulty. Since SHA-256 is categorized as a cryptographic hash function [21], it is easy to verify a previously calculated SHA-256 sum of a block, but it is considered infeasible to generate a specific block that produces a given hash value. To achieve this, the nonce field is constantly incremented to search for a hash value that fulfils the described property. This brute-force process of searching is called *mining*. If one client in the Bitcoin network finds

[1] More precisely a Merkle-Tree Hash over those transactions, for details see the specifications [4,5,17].

such a combination of valid transactions and nonce that yields a desired result, he/she publishes this new block in the Bitcoin network and gets rewarded with newly created bitcoins.

The reward comes in form of a new transaction of (currently) 25 bitcoins that has no predecessor and is included as a special so-called *coinbase transaction* by the creator of the respective block. This coinbase transaction also includes the public key/bitcoin address of the creator and marks the first transaction of a new chain of Bitcoin transactions [4,5,17,20].

## 3 Related Work

We build upon already existing work by contributing the first user study with Bitcoin users. Eskandari et al. [8] presented a first look at the key management of Bitcoin by providing a set of evaluation criteria for Bitcoin wallets and a cognitive walkthrough [23] of selected wallets. The work by Eskandari et al. [8] can be considered a first look at the usability of Bitcoin.

Moore and Christin [19] conducted an empirical analysis of Bitcoin exchange risks. They examined the track record of 40 Bitcoin exchanges and found that 18 had been closed, with customer account balances often wiped out. They also found that popularity is a strong indicator to predict the lifetime of an exchange, i.e. popular exchanges have a longer lifespan.

Baur et al. [2] conducted exploratory interviews with individuals of distinct groups and found that most stakeholders perceived the ease of use still as rather low. They also found that the experienced usefulness varies according to the user group.

However, no empirical study has been performed to examine user perceptions of Bitcoin security, privacy and anonymity. For a cryptographic currency like Bitcoin, public key cryptography is required. Regarding the usability of key management and encryption in the context of e-mail various studies have shown that there are numerous usability issues regarding the successful usage of public key cryptography [11,12,22,24]. At this time, for neither domain a fully usable concept has been successful. Human aspects of key management have already been studied in other domains [11–13,22,24]. For the Bitcoin ecosystem however, secure key management alone is not sufficient, as communication is not channel-independent but an integral part of the security concept.

## 4 User Study Methodology

The goal of this study is to empirically investigate end user perceptions and behavior in the Bitcoin ecosystem with an emphasis on security practices as well as coin and key management with the involved security risks. We designed an online questionnaire and additionally conducted qualitative interviews. We derived specific research questions from already existing literature on Bitcoin (as discussed in Sect. 3) as well as from a qualitative content analysis of threads from online forums and mailing lists. Furthermore, we revised the available Bitcoin

wallets[2] and their capabilities and used them as inspiration for our questions and the design of the security and privacy risk scenarios. We focus on Bitcoin as it was by far the most popular cryptographic currency at the time we conducted this study (July 2015). While the online survey was intended to broadly measure self-reported Bitcoin management behavior and risk perception, the interviews were conducted to get a deeper understanding on key usability issues, causes of common security incidents and if and how they managed to recover their keys.

### 4.1 Research Questions

We sought answers to the following questions regarding users' perceptions of Bitcoin management and Bitcoin-associated security risks:

- *Q1: What are the main usage scenarios of Bitcoin?*
- *Q2: How do participants manage their Bitcoins? What are participants' current practices and how do they deal with security, privacy and anonymity?*
- *Q3: How do participants perceive Bitcoin-associated security risks?*
- *Q4: What security breaches have affected users and how did they recover their Bitcoin keys and bitcoins?*
- *Q5: What are the main usability challenges that users have to deal with when using Bitcoin?*

We were also interested in categorizing CMTs in a way that users can quickly make an informed decision based on the level of security, privacy and control they prefer? Our categorization can be found in Appendix A.

## 5 Online Survey

We conducted our online survey over July 8–15, 2015. Our survey consisted of both closed- and open-ended questions and covered the following topics: (1) Bitcoin usage and management, (2) CMT choice and usage, (3) security, privacy, anonymity and backup behavior, (4) risk perception, and (5) demographics. The full set of questions is presented in Appendix B. The open-ended questions were coded independently by two researchers independently. After agreeing on a final set of codes, we coded all answer segments for the final analysis. Coding refers to categorizing qualitative data to facilitate analysis [18] and is a common practice in human-computer interaction research.

### 5.1 Recruitment

We hosted our survey at *soscisurvey.de*[3]. To restrict our participants to Bitcoin users only, we deliberately designed our study to exclude all non-Bitcoin users. As it is difficult to construct such a restricted sample on platforms like

[2] bitcoin.org.
[3] https://www.soscisurvey.de/.

Amazon Mechanical Turk, we decided to use Bitcoin mailing lists and forums for recruiting. Furthermore, we compensated participants in Bitcoin. The reward for a completed questionnaire was 4.2 mɃ(= 0.0042 Ƀ ≈ 1.22 USD at that time) After completing the survey, the participants were instructed to enter a valid Bitcoin address to receive the payment. This ensured that everyone who wanted to receive bitcoins as a reward is a Bitcoin user and hence exactly our target audience. Even participants who had not used Bitcoin before had to create a Bitcoin address to receive the compensation.

To motivate participants to spread the word and thus recruit further participants, we displayed a link for re-distribution at the end of the survey. All participants that recruited others received an additional 1 mɃ (≈ 0.29 USD). Table 1 shows that this additional incentive scheme was successful since we received a high number of participants this way. As Table 1 shows, the top 5 re-distributors of the link recruited about one quarter of the overall sample. Initially we distributed the link to our survey over the following channels: *bitcointalk.org* forum[4], *bitcoin-list* mailing list[5], *twitter.com*[6] and an Austrian bitcoin mailing list[7]. We aimed for maximum transparency to avoid that our call for participation would be misinterpreted as scam. Therefore, we proved on the initial page of our survey that we indeed hold a respectable amount of bitcoins[8], by providing our Bitcoin address[9] together with a signature with the according private key (see Appendix C for the signature).

We recruited 1,265 participants over July 8–15, 2015 via these channels. The total sample size after filtering out 275 participants due to incomplete or duplicated submission, or invalid entries, was 990. Of these, 85.2% claimed to be male (m), 10.5% claimed to be female (f). 4.3% of our participants preferred not to provide their gender. Ages ranged from 15 to 72 (median = 28.56). About half of our participants reported to have an IT-related background. According to the collected IP addresses, most of our participants filled out the survey in the US, followed by the UK and Germany. 7.6% accessed the survey site over Tor (Fig. 1). These numbers can of course be biased by VPN usage.

### 5.2 Validity of Our Dataset

Since the survey was designed to be anonymous and we only required a valid Bitcoin address, we had to take special care to avoid abuse. We semi-automatically verified the authenticity of our dataset and were able to exclude 116 submissions we suspected to be fraudulent, and 160 incomplete submissions. Nevertheless, there is still a chance that we missed some manual double submissions. However, due to our deployed countermeasures and the high quality of submitted data (e.g., the open-text questions) we suspect that the overall number

[4] https://bitcointalk.org/index.php?topic=1114149.0.
[5] http://sourceforge.net/p/bitcoin/mailman/bitcoin-list/?viewmonth=201507.
[6] https://twitter.com/bit_use.
[7] http://bitcoin-austria.at/.
[8] We purchased our 6.3965 BTC at https://coinfinity.co/.
[9] https://blockchain.info/address/12yeU5ymM67SL5UWVSwErAgwVwwaTd1Nma.

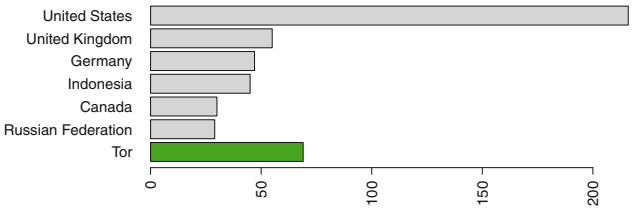


**Fig. 1.** Countries from which our participants accessed the survey site.

**Table 1.** Most refereed links.

| Reference | Occurrences | Reward in BTC/EUR/USD |
|---|---|---|
| 455975 | 91 | 0.0952/24.78/27.18 |
| 1295 | 58 | 0.0622/16.19/17.76 |
| 699324 | 51 | 0.0552/14.37/15.76 |
| 932181 | 28 | 0.0322/8.38/9.19 |
| 637623 | 21 | 0.0252/6.56/7.19 |

is negligible. Among other, we deployed the following countermeasure to make automation harder: ***reCAPTCHA:*** The last page of our survey contained a text box to enter a Bitcoin address for receiving the compensation and a Google reCAPTCHA. This together with the relatively low overall amount of compensations helped to mitigate fully automated submissions. Since reCAPTCHA adapts the difficulty depending on the source IP address, some Tor users complained about hard-to-solve CAPTCHAs. ***Meta data:*** The meta data like source IP address and information on the user's browser was used to pinpoint simple double submission attempts. ***Time:*** We considered submissions below a certain threshold fraudulent since it is impossible to provide reasonable answers under a certain lower bound. ***Open-text questions:*** In suspicious and borderline cases we manually checked the open-text questions to see if the user had meaningful contributions to the survey. ***Reference links:*** The reference links also provided a good insight when users attempted to submit multiple surveys and always referenced their initial survey. ***Bitcoin address:*** The uniqueness of a Bitcoin address was also an indicator for double submissions.

In case we detected double submissions, we accepted only the first submission for our dataset as well as for our compensation scheme. All subsequent submissions were excluded. In conclusion, we did not encounter fully automated submissions and that most fraudulent attempts can be attributed to simple manual double submissions. Moreover, the Bitcoin community has proven to be very forthcoming. There have been cases in which participants deliberately did not include Bitcoin addresses, and commenting that they would like to help by saving the reward in order to recruit more participants.

The demographics of our sample correspond with data on the general Bitcoin population[10].

## 6 Qualitative Interviews

To get a deeper understanding of the findings from our online survey, we conducted an additional field session with qualitative interviews.

### 6.1 Design and Recruitment

We recruited participants via a local Bitcoin mailing list and conducted a two-hour field session at a local bar that accepts bitcoins. All interviewees are regularly using Bitcoin and had previously completed our online questionnaire. Two researchers were present during the field session, one conducted the interview and the other one took notes. As all participants were very particular about preserving their privacy, we chose not to audio-record the interviews.

For the evaluation of our qualitative data, we focused on the exploration of ideas and insights of the participants. Some of the numbers gathered from the interviews will be used as rough indicators to discuss and complement the results from our quantitative survey. We interviewed 10 participants in total. All participants were male and frequent users of Bitcoin and other crypto-currencies. All of them reported to have an IT-related background. The purpose of the qualitative interviews was mainly to complement our quantitative results and to explain phenomena and trends from our online survey. After 10 participants, we reached saturation and little to no further insights were gained, so we concluded the study.

### 6.2 Coding

After the interviews, we went through the collected data and produced an initial set of codes. We traversed the data segments collected from each participant for each question and also included statements that did not directly evolve from a question. Two researchers performed the initial coding independently of each other to minimize the susceptibility of biased interpretation. After the initial coding process, we revised the retrieved codes and discussed recurring themes, patterns and interconnections. After agreeing on a final set of codes, we coded the entire interview data. We coded all data segments, regardless if they emerged directly from a question or a continuative discussion.

## 7 Results

In this section, we present an analysis of the participants' responses addressing our research questions defined in Sect. 4.1. At the beginning of each section we analyse the results from our online survey, whereas at the end we compare these results with our qualitative interviews and try to correlate and explain our findings.

[10] http://www.coindesk.com/new-coindesk-report-reveals-who-really-uses-bitcoin/.

### 7.1 General Bitcoin Usage (Q1)

Most participants reported to use Bitcoins for tips and donations (38.0%), followed by virtual goods, such as web hosting, online newspapers (33.3%), online shopping (27.5%), altcoins (26.5%), gambling (26.5%) and Bitcoin gift cards (19.9%). About 5% self-reported to buy or have bought drugs with bitcoins. 30.2% of our sample reported to use Bitcoin at least once a week, 25% stated that they use Bitcoin at least once a month and 19% at least once a day. The remainder of the participants indicated to use Bitcoin at least once a year or even less. These results suggest that the majority within our survey frequently uses Bitcoin.

We also asked our participants about the amount of bitcoins they are currently holding. About half of the participants did not want to specify. According to their reports, our sample holds approximately 8000 ฿ in total. The majority of users (70%) started to use Bitcoin between 2013 and 2015. 17% started between 2011 and 2012. 58.0% reported to use other crypto currencies in addition to Bitcoin, most frequently Dogecoin and Litecoin. The most popular Bitcoin exchanges in our sample are BTCE (20.9%), Bittrex (14.0%) and Bitstamp (13.0%). 11.4% of our participants are currently mining bitcoins. Most of them started mining after 2014. Many of those who started earlier have stopped mining as they currently consider it infeasible. 195 (19.7%) participants claimed to be running a full Bitcoin server that is reachable from the Internet. The top-mentioned reason for running a Bitcoin server was to support the Bitcoin network (60.5%), followed by fast transaction propagation (46.6%), network analysis (30.3%) and double-spending detection (26.1%).

All participants from our qualitative interviews are frequent Bitcoin users, and some of them are active in the local Bitcoin association. Most interviewees mentioned that the decentralized nature of Bitcoin was among the main reasons to start using Bitcoin. The second-most mentioned reason was simply curiosity. One participant who used to live in Crimea at the time the Ukrainian-Russian conflict started mentioned socio-political reasons. He used to work for a US company at that time and needed a safe and cheap option to receive his salary in Crimea. He furthermore wanted to make sure to not lose any money due to the annexation to the Russian Federation. In his opinion, Bitcoin was the best option and according to him, many people started using Bitcoin at that time in Crimea. Some participants also mined Bitcoins some years ago when it was still profitable to mine at small scale.

### 7.2 Practices of Bitcoin Management (Q2)

**Bitcoin Wallets and Backup Behavior.** Table 3 shows the most widely used Bitcoin wallets. The participants could mention multiple wallets as it is a common scenario that users use more than one wallet. The table also shows the number of participants from our sample who use a certain wallet as well as the percentage. Furthermore, Table 4 shows whether the users protect their wallets with a password and if these wallets are encrypted. Our findings show that the

majority of users protect their wallets with a password. In case of web clients, we observed a lack of background knowledge. For example, 47.7% of Coinbase users in our sample say that their wallet is encrypted and 34% claim that they do not know if it is encrypted. We observed a similar trend for Xapo which is the third-most used wallet in our sample. Just like Coinbase, it is also a web-hosted tool and, similarly to Coinbase, only about half of the users say it is encrypted and about a third does not know if it is encrypted. Regarding backups, only a third of Coinbase users and 43% of Xapo users backup their wallets. 33.9% of Coinbase and 28.5% of Xapo users do not know whether their wallet is backed up. We also found that Bitcoin users with more than 0.42฿ (100 USD) do not backup their CMT more often than users with less bitcoins. This effect is statistically significant in our sample ($\chi^2(1) = 5.1, p = 0.02$).

We also asked our participants whether they create additional backups in case their primary backup gets lost or stolen. In our sample, Bitcoin Core users have the highest rate of additional backups. 64% of them indicated to make a secondary backup of their wallet. Table 2 shows self-reported properties of wallet backups. According to our data, none of our participants stores a backup on an air-gapped computer. The most reported backup properties were encryption and password protection. According to our sample, 197 backups are stored in a cloud.

59.7% of our participants only use one wallet to manage their bitcoins. 22.7% use two, and 10.6% use three wallets. The remaining 7% use four or more wallets. The maximum number of wallets a participant reported to use was 14. This participant justified this high number by reporting that he wanted to try out the wallets before choosing those that met his requirements best. About half of our participants who used a web client did this exclusively to manage their bitcoins. The other half used a web client in addition to a local client. To our surprise our results show that most coins of our participants are stored in Armory[11]. The Armory users in our sample have about 3818 ฿ in their Armorys, where the top five users reported to have 2,000 ฿, 885 ฿, 300 ฿, 230 ฿ and 150 ฿. The highest reported number of bitcoins stored in a participant's web client was 100 ฿. The reported sum of all coins stored in Coinbase is 238 ฿, in Xapo it is 157 ฿. Figure 2 illustrates the accumulated bitcoins per wallet as reported by our participants.

**Anonymity.** We found that 32.3% of our participants think that Bitcoin is per-se anonymous while it is in fact only pseudonymous. 47% thinks that Bitcoin is not per-se anonymous but can be used anonymously. However, about 80% think that it is possible to follow their transactions. 25% reported to have used Bitcoin over Tor to preserve their anonymity.

We also asked participants if they take any additional steps to stay anonymous. 18% reported to frequently apply methods to stay anonymous on the Bitcoin network. Most of them reported to use Bitcoin over Tor followed by multiple addresses, mixing services, multiple wallets and VPN services. As shown

[11] https://bitcoinarmory.com/.

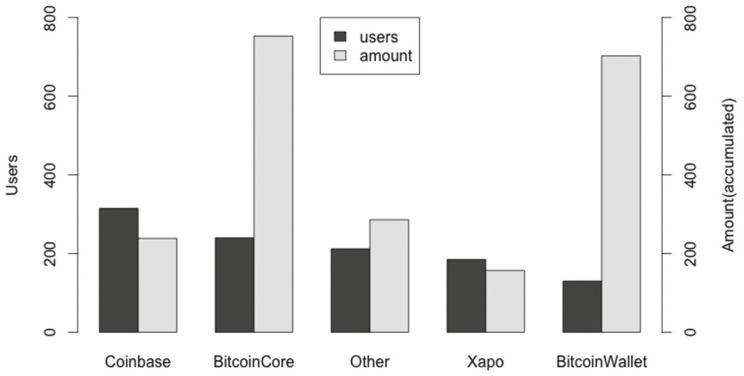


**Fig. 2.** Self-reported wallet usage and accumulated hosted bitcoins per wallet.

**Table 2.** Backup properties in absolute mentions in descending order; a user can have multiple wallets and multiple backups.

| Backup properties | Mentions |
|---|---|
| My backup is encrypted | 662 |
| My backup is password protected | 629 |
| My backup is stored on external storage (e.g. USB drive) | 430 |
| My backup is stored on paper | 334 |
| My backup is stored in the cloud (e.g. Dropbox) | 197 |
| My backup is stored on an air-gapped device | 0 |

**Table 3.** Properties of the most frequently used wallets mentioned by our participants.

| CMT | Number | Percent | ฿ |
|---|---|---|---|
| Coinbase | 314 | 31.7 | 238 |
| Bitcoin core | 236 | 23.8 | 752 |
| Xapo | 179 | 18.1 | 157 |
| Electrum | 125 | 12.6 | 226 |
| MyCelium | 97 | 9.8 | 62 |

by Biryukov et al. [1,3] using Bitcoin over Tor creates an attack vector for deterministic and stealthy man-in-the-middle attacks and fingerprinting.

### 7.3 Risk Perception (Q3)

We were also interested in user perceptions of risks associated with Bitcoin. We provided the participants with 11 risk scenarios. We selected the risk scenarios based on findings from scientific literature and evidence from online resources.

**Table 4.** Properties of the most mentioned CMTs. The three blocked columns contain information on whether the CMT is encrypted, if it is backed up, whether there exists an additional backup and the mentions in percent (Yes, No and I don't know (IDK)). The rightmost column contains the sum of bitcoins stored in a respective CMT by our participants.

| | Encrypted? | | | Backup? | | | Additional backup? | | |
|---|---|---|---|---|---|---|---|---|---|
| CMT | Yes | No | IDK | Yes | No | IDK | Yes | No | IDK |
| Coinbase | 47.5 | 18.5 | 34.0 | 35.5 | 30.6 | 33.9 | 30.3 | 66.9 | 2.8 |
| Bitcoin core | 72.8 | 16.1 | 11.1 | 76.3 | 14.0 | 9.7 | 64.0 | 32.2 | 3.8 |
| Xapo | 51.4 | 19.0 | 29.9 | 43.0 | 28.5 | 28.5 | 41.3 | 57.5 | 1.2 |
| Electrum | 72.8 | 15.2 | 22.0 | 77.6 | 16.0 | 6.4 | 55.2 | 44.0 | 0.8 |
| MyCelium | 61.9 | 21.6 | 16.5 | 83.5 | 12.4 | 4.1 | 52.6 | 47.2 | 0.2 |

For each risk scenario, we provided an easy-to-understand description and asked the participants whether they think the risk is likely or unlikely to occur. Figure 3 shows the participants' risk estimation. Our results show that the participants consider value fluctuation as the highest risk, followed by vulnerabilities in hosted wallets and Bitcoin theft via malware. Our participants estimated the risk for cryptographic flaws as the lowest, followed by double-spending attacks and DoS attacks on the Bitcoin network.

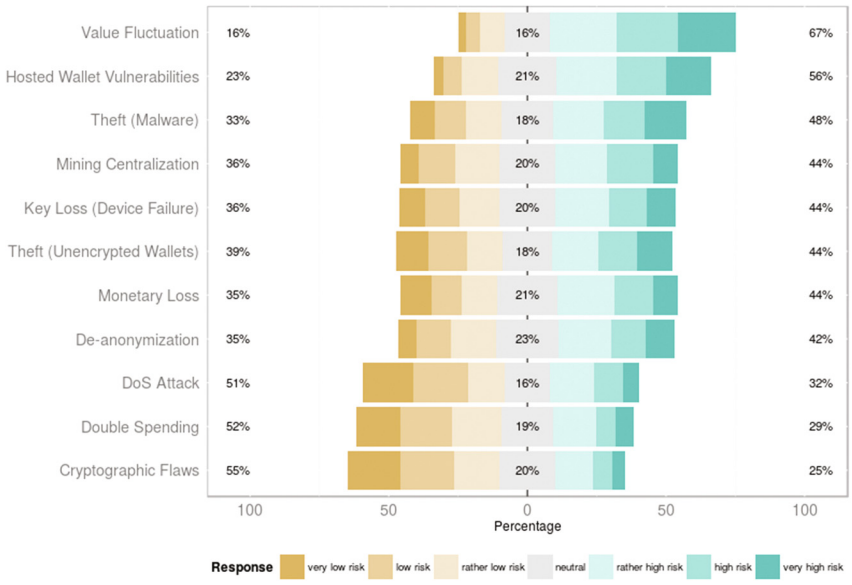


**Fig. 3.** User perceptions of risk scenarios in percentage of participants ($N = 990$).

### 7.4 Security Breaches (Q4)

About 22.5% indicated to have lost bitcoins or Bitcoin keys at least once. Of those, 43.2% mentioned that it was their own fault (e.g., formatted hard drive or lost a physical device with Bitcoin keys). 26.5% reported that their loss stemmed from a hardware failure (e.g., a broken hard drive), followed by software failure (24.4%; e.g. keyfile corruption) and security breaches (18% e.g., malware, hacker).

The majority (77.6%) among those who lost bitcoins did not want to indicate whether they were able to recover their keys. Of those who provided an answer, 65% were not able to recover their keys. Overall, our participants reported to have lost about 660.6873 bitcoins. However, it must be taken into account that we did not ask when the coins were lost. Hence, interpreting this result we must take into consideration that the Bitcoin exchange rate is highly volatile and it is therefore hard to provide an overall estimation in USD. About 40% of our participants reported to have lost money due to a self-classified major security breach. 13.1% of our overall sample reported to have lost bitcoins in HYIPS (high-yield investment programs) and pyramid schemes. 7.9% lost money at Mt. Gox.

We also gave our participants the opportunity to describe how they dealt with the incident. Most participants stated that they did not do anything to recover their keys and simply accepted the loss. Some argued that the financial loss was not worth the effort to take further steps or that they felt helpless as they didn't know what to do. Those who actually took action most frequently mentioned that they filed claims and contacted the exchange or online wallet provider. Those who lost money to a malicious online wallet reported to have moved to other types of wallets instead of hosted/online wallets. The participants who lost money in HYIPS mostly stated that they started to use less risky investments and learned from their previous mistakes. Irrespective of the security breach, many participants reported to have spread the word over forums on the Internet and shared their experiences with other affected users.

*Participant Statements*

- *"I follow the 'do not invest more than you're ready to lose' rule."* (P3848)
- *"I just had to accept that my money was stolen ... and that I learned my lesson to never use exchanges as wallets. Keep everything in your own hand."* (P3763)
- *"Just learned from it. It was exceedingly stupid on my part."* (P853)

Eight participants from our qualitative interviews reported that they have already experienced an intentional or accidental key and/or Bitcoin loss. Three participants were affected from the Mt. Gox security breach and two of them reported to have filed a claim on Kraken[12]. One participant reported to have lost a *physical* Casascius[13] Bitcoin but then stopped searching for it as it was

[12] https://www.kraken.com/.
[13] https://www.casascius.com/.

only worth about 9 USD at that time. Others also mentioned to have lost their keys due to device failure, corrupted HDDs, or software failure.

### 7.5 Perceptions of Usability (Q5)

Even though most participants of our qualitative interviews were very much concerned about security and privacy aspects of Bitcoin management, eight of them said that they would recommend web wallets and deterministic wallets to non-tech-savvy Bitcoin users. Convenience and easiness of use were highlighted as the main benefits. One participant said that he would definitely recommend a wallet where the private key is stored on a central server to make key recovery easier and to obviate the need for comprehensive backups as well as that mnemonics would help. Six participants also said that they would recommend MyCelium[14] as the most usable wallet. Those who had already used MyCelium consider the paper backup procedure as the most usable and secure way. To create a paper backup with MyCelium, the user has to print out a template that contains some parts of the key and then lets the user fill out the empty spots manually. Some participants expressed initial discomfort when they used paper wallets.

Most interviewees also highlighted the need for fundamental education in early years of childhood. P2 said that Bitcoin is inherently complex, that the fundamental idea of public key cryptography should be taught in school and monetary systems are a matter of culture.

Two participants also highlighted that user interfaces should be simplified and minimalized. Many participants stated that for a fast proliferation of Bitcoin, simple and intuitive UIs are more important than security. They argued that computers proliferated even though most people do not know how computers work and that security is not necessarily an argument for large-scale adoption. They provided examples such as cars in the 1940s, computers, credit cards and WhatsApp. They also said that the amount of money that is circulating in the Bitcoin network is low enough to take the risk of loosing it and compared this scenario to the risk of loosing cash. Some participants also proposed a dedicated device with an intuitive UI for key management and think that such an artifact would be the most secure and usable option.

*Participant Statements*

- *"It somehow didn't feel right for me to go out of the digital realm."* (P6 on paper wallets)
- *"Children learn about our monetary system in their very early days in primary school. This is why society knows how to use cash and credit cards. I'm sure it could be the same thing with a decentralized crypto-currency."* (P7)

[14] https://mycelium.com/.

## 8 Discussion

The goal of this paper was to answer the research questions provided in Sect. 4.1 in order to understand how users interact with the Bitcoin ecosystem. As this is the first-ever user study focused on user experiences with Bitcoin security and privacy, we gathered useful insights. In the following we discuss our results in the context of already existing works in the field.

Regarding Bitcoin management tools and practices (Q2), we found that two of the most widely used CMTs were web-hosted solutions that obviate the need for users to deal with key management and backups. Our results show that our participants had clear preferences regarding their choice of CMT. In contrary, this is not the case for Bitcoin exchanges. Our data shows that the Bitcoin exchanges chosen by our participants were almost evenly distributed. Even though our data reveals a clear tendency towards web-hosted solutions, these CMTs do not host the majority of our participants' bitcoins. According to our participants' self-reported data, the highest amount of accumulated bitcoins is hosted in Armory. At the time of writing, if used correctly, Armory is one of the most secure solutions.

For the two most widely used web-hosted CMTs, about a third of our participants are unaware of whether their wallet is encrypted or backed up. In such a scenario, users shift responsibilities to a third party. Even though this seems to be a convenient and usable solution for non-expert users, it implies that the user trusts these third parties to take care of their security. About 50% of web client users indicated to use an additional local client to store their virtual assets. According to our results, users that have a higher number of bitcoins do not necessarily back up their wallets more often. Also, MyCelium users back up their wallets more often than others. Hence we conclude that backup motivation and respectively fatigue depend highly on usability and not on the number of coins.

As the answer to Q4 indicates, participants have already lost money to malicious hosted-wallet providers. Also, our participants perceived vulnerabilities in hosted wallets as the second highest among our risk scenarios (Q5). Some participants from our qualitative interviews said that they would recommend inexperienced users to start with a hosted wallet due to the usability benefits as for most other solutions users are required to have at least a basic understanding of the underlying basics of Bitcoin and the blockchain.

Bitcoin is a pseudonymous system, whereas a wide-spread myth says that it is per-se anonymous. More than a third of our participants still believe in this myth and reported that they think that Bitcoin is fully anonymous. About half of our participants are aware that Bitcoin is not per-se anonymous, but that it can be used anonymously. Regarding anonymity measures, many users reported to use Bitcoin over Tor, which in fact creates an attack vector for deterministic and stealthy MITM attacks, as shown in [3].

Our results also suggest that our participants trust the cryptography behind Bitcoin and are aware of risks according to value fluctuation and software vulnerabilities. Poor usability and the lack of knowledge are major contributors to security failures. Almost a fourth of our participants indicated that they had

already lost bitcoins or Bitcoin keys at least once (Q5). To our surprise, almost half of those who lost bitcoins due to a self-induced error which indicates that state of the art CMTs are sometimes still difficult to use or require users to manually take care of security tasks, such as backups and encryption. Our results also indicate that the Bitcoin ecosystem is mostly utilized for tipping and donations as well as acquiring digital goods, but to some extend also for criminal activity and adventurous gambling.

## 9 Conclusion

In this work we presented the first user study to examine how users interact with the Bitcoin ecosystem in terms of security and privacy. We conducted an online survey with 990 Bitcoin users and qualitative interviews with a subset of 10 participants. Furthermore, we introduced the term *Coin Management Tools (CMTs)* to describe tools that let users manage their virtual assets (keys) and interact with the Bitcoin network. Additionally, we proposed a method for categorizing CMTs according to the degree of control and verifiability a user can exercise with this client.

We found that managing bitcoins is still a major challenge for many users, as many of them do not apply sufficient security measures such as encryption and backups. We found that many participants were not even aware of security features provided by their used CMT. Two of the most widely used CMTs among our participants were web-hosted solutions. About half of their users reported to use such solutions exclusively, while the other half also used local clients. Even though web clients ought to be a usable and convenient solution, they require a certain level of trust and shift the responsibilities of encryption and managing backups to a third party. We also found that 22.5% of our participants have already experienced security breaches and lost bitcoins. About half of them mentioned a self-induced error as the reason, which highlights that users find it still difficult to manage their bitcoins in a secure way.

We believe that our insights and suggestions are an important first step towards improving the usability of Bitcoin security. In order to guarantee secure interactions with the Bitcoin ecosystem to both expert and non-expert users, we must re-think the concept of Bitcoin management, since it is more than just the secure handling of secret keys. Bitcoin is a decentralized system where the interactions between peers and the propagation and verification of messages and data is important. If this aspect is ignored, Bitcoin would just consist of signed numbers without value.

**Acknowledgements.** This research was funded by COMET K1, FFG – Austrian Research Promotion Agency and by FFG Bridge Early Stage 846573 A2Bit. We would also like to thank Martin Mulazzani, Artemios G. Voyiatzis and Matthew Smith for their useful comments and feedback. Furthermore, we would like to thank Elizabeth Stobert for her valuable feedback and for her help in recruiting participants.

# A CMT Categorization

In this section we discuss the term *Coin Management Tool* and provide a methodology to categorize CMTs according to the degree of control and verifiability a user can exercise with his respective client. The proposed scheme is tailored to Bitcoin-like cryptocurrencies, but explicitly designed in an utmost generic way so that it can be applied to other derived cryptocurrencies as long as they are not fundamentally different in their design. Our approach used the evaluation framework from [8] as a starting point. A categorization according to our scheme allows users to quickly distinguish clients according to their underlying security model and hence allows users to make an informed decision on the level of confidence and trust they can put into an individual client.

## A.1 Definitions

When Bitcoin was in its infancy *bitcoind* was the only available Bitcoin client which performed all required tasks: *mining management*, *P2P network communication and blockchain management*, *key management* and *virtual asset management*. With the increased popularity of Bitcoin and cryptocurrencies in general, more and more software was developed which focused on a subset of individual tasks of the original implementation. Moreover, the design of Bitcoin allows users to use it even if they do not run mining software or a full P2P client (full node). As a result there exists software with varying feature sets where the handling of public-private key pairs is the most sensitive and hence the most common core feature. A Bitcoin wallet was originally defined as a collection of private keys[15]. Since this definition is very narrow, we introduced the broader definition of a *Coin Management Tool* (CMT) to account for the other areas without whom most cryptocurrencies would not work. Especially the network and blockchain layer of Bitcoin and other cryptocurrencies is not only important for the integrity of the system as a whole, but has a significant impact on the security and privacy of each and every end user.

## A.2 Categorization

To categorize CMTs, we first identified critical CMT tasks which are directly related to security and privacy issues. This covers aspects regarding key management like generating keys/addresses and signing transactions, as well as P2P network communication and blockchain management like handling connections as well as verifying and storing the blockchain. These core tasks can be used to divide CMTs into five different categories. A client can be in more than one category depending on its configuration.

– **cat. 0:** A client which runs on a user-controlled device and is able to perform key management operations, but cannot perform any P2P network

[15] https://en.bitcoin.it/wiki/Wallet.

communication. Therefore, it is not a stand-alone solution. This includes some dedicated *hardware clients/wallets* and *cold-storage* clients which require a second online device for transaction processing.

- **cat. I:** A client which runs on a user-controlled device and performs all P2P network communication and blockchain verification related tasks, keeps a copy of the full blockchain, is able to perform all key management related operations and executes the mining algorithm. In other words, this is a client which can perform all required tasks to operate a cryptographic currency (e.g., the Bitcoin core implementation *bitcoind* when the option *setgenerate true* is set).
- **cat. II:** A client which runs on a user-controlled device and performs all P2P tasks related to network communication and blockchain verification, keeps a copy of the full blockchain and is able to perform all key management related operations. This type of client is sometimes referred to as *thick-client* or *full-node*.
- **cat. III:** A client which runs on a user-controlled device and performs certain P2P tasks related to network communication and blockchain verification but does not keep a copy of the full blockchain, although, it is able to perform all key- management-related operations. This type of client is sometimes referred to as *thin-client* or *mobile-client/wallet* and includes so-called SPV-clients/wallets (Simplified Payment Verification) e.g., Electrum.
- **cat. IV:** A client which does not run on a user-controlled device and where all tasks are performed by a trusted third party on behalf of the user. This type of client is sometimes referred to as *hosted-* or *web-client/wallet*. Thereby it is not relevant if the key management is handled in the browser (e.g., via JavaScript) since this would require the user to download (and verify) the script code from the website of the third party every time he/she wants to use it.

## B Interview Questions

Questions with answer options as "( )" are multiple choice checkboxes whereas answer possibilities marked alphabetical e.g. "a)" are single selections.

### B.1 BTC Demographics

**Q1** Please input which year you started using Bitcoin:
a) 2009 *b*) 2010 *c*) 2011 *d*) 2012 *e*) 2013 *f*) 2014 *g*) 2015

**Q2** Select which main features are responsible for you using Bitcoin (multiple selections possible):
( ) The opportunity of financial gain
( ) Curiosity
( ) Anonymous nature
( ) Decentralized nature
( ) A friend/colleague suggested to me to start using Bitcoin

( ) The possibility to internationally transfer money with relatively low fee
( ) The possibility to accept bitcoins for my services or for my products
( ) Other:

**Q3** What is the estimated sum of bitcoins you are holding?
*a*) I hold approximately *b*) I do not want to specify

**Q4** Please provide what services or products you pay for with bitcoins (multiple selections possible):
( ) Bars, restaurants
( ) Bitcoin gift cards
( ) Donations, tipping
( ) Drugs
( ) Gambling sites
( ) Hotels, travel
( ) Online marketplaces and auctions
( ) Online shopping (Newegg, ...)
( ) Altcoin (e.g. Litecoin, ...)
( ) Physical stores that accept bitcoins
( ) Underground marketplaces
( ) Virtual goods (webhosting, online newspapers, ...)
( ) Medium for currency exchange
( ) Other:

**Q5** What do you think are the most likely risks associated with Bitcoin?

**Q6** Please select the crypto currencies you are holding or using besides Bitcoin (multiple selections possible):
( ) I do not use other crypto currencies
( ) BanxShares
( ) BitShares
( ) BlackCoin
( ) Bytecoin
( ) Counterparty
( ) Dash
( ) Dogecoin
( ) Litecoin
( ) MaidSafeCoin
( ) MonaCoin
( ) Monero
( ) Namecoin
( ) Nxt
( ) Peercoin
( ) Primecoin
( ) Ripple
( ) Startcoin
( ) Stellar
( ) SuperNET

( ) Vertcoin
( ) YbCoin
( ) Other

**Q7** Select the Bitcoin exchanges you have used in the past or you are using on regularly (multiple selections possible):
( ) None
( ) BanxIO
( ) Bitcoin Exchange Thailand
( ) Bittrex
( ) Bitcoin Indonesia
( ) bitcoin.de
( ) Bitfinex
( ) Bitstamp
( ) BitX South Africa
( ) BTC-e
( ) BTC38
( ) BTCChina
( ) CCEDK
( ) Cryptsy
( ) Gatecoin
( ) hibtc
( ) Kraken
( ) Mt. Gox
( ) OKCoin
( ) Poloniex
( ) QuadrigaCX
( ) The Rock Trading
( ) VirWox
( ) Other:

**Q8** What do you think are the greatest benefits of Bitcoin?
**Q9** How often do you perform Bitcoin transactions?
*a*) At least once a day *b*) At least once a week *c*) At least once a month *d*) At least once every six months *e)* At least once a year *f*) Less than once a year

### B.2 BTC Wallets

**Q10** Please tick which wallets you are currently using (multiple selections possible):
( ) Airbitz
( ) Armory
( ) Bitcoin Core
( ) Bitcoin Wallet (Schildbach Wallet)
( ) BitGo

( ) Bither
( ) breadwallet
( ) Circle
( ) Coinapult
( ) Coinbase
( ) Coinkite
( ) Coinomi
( ) Electrum
( ) Green Address
( ) Hive
( ) Ledger Nano
( ) mSIGNA
( ) MultiBit
( ) Mycelium
( ) Ninki
( ) TREZOR
( ) Xapo
( ) Not in list

**Q11** Why did you choose to use multiple wallets to manage your bitcoins?

### B.3 Wallet Usage

For every selected wallet in Q10 we asked the following questions.

**Q12** Why did you choose ⟨wallet-name⟩ to manage your Bitcoins?
**Q13** How many bitcoins do you have approximately in this wallet?
*a*) I hold approximately ⟨textfield⟩ bitcoins. *b*) I do not want to specify
**Q14** Is this wallet password protected?
*a*) Yes *b*) No *c*) I do not care *d*) I do not know
**Q15** Is this wallet encrypted?
*a*) Yes *b*) No *c*) I do not care *d*) I do not know
**Q16** Is this wallet backed up?
*a*) Yes *b*) No *c*) I do not know

### B.4 BTC Mining

**Q17** Are you currently mining bitcoins?
*a*) Yes, since *b*) No, but I have mined from-to *c*) No, I have never mined bitcoins
**Q18** How many bitcoins have you mined in total?
*a*) I mined approximately *b*) I do not want to specify
**Q19** Do you or have you participated in mining pools?
*a*) Yes *b*) No

**Q20** Please tick the names of the mining pools you have or are participating in (multiple mentions possible):
( ) 21 Inc.
( ) AntPool
( ) Bitcoin Affiliate Network
( ) BitFury
( ) BitMinter
( ) Bitsolo
( ) BTCChina Pool
( ) BTC Guild
( ) BTC Nuggets
( ) BW.COM
( ) EclipseMC
( ) Eligius
( ) F2Pool
( ) GHash.IO
( ) Kano CKPool
( ) KnCMiner
( ) MegaBigPower
( ) P2Pool
( ) Slush
( ) Telco 214
( ) Other:

### B.5 BTC Server

**Q21** Do you run a full Bitcoin server that is reachable for others from the Internet?
*a*) Yes *b*) No

**Q22** Please provide some reasons on why you operate a full Bitcoin server (multiple selections possible):
( ) Fast transaction propagation
( ) Double-spending detection
( ) Network analysis
( ) Support the Bitcoin network
( ) Other

### B.6 BTC Security Risks

**Q23** How would you estimate the risk of monetary loss for Bitcoin compared to credit cards?
(7 Point Likert-Scale from "High" to "Low")

**Q24** How high do you think is the risk of becoming a victim of a successful double spending attack?
(7 Point Likert-Scale from "High" to "Low")

**Q25** How high or low would you estimate the risk for malware that steals your Bitcoins?
(7 Point Likert-Scale from "High" to "Low")
**Q26** How would you estimate the risk of monetary theft in case the device with your wallet gets lost or stolen?
(7 Point Likert-Scale from "High" to "Low")
**Q27** How would you estimate the risk of de-anonymization?
(7 Point Likert-Scale from "High" to "Low")
**Q28** How high do you think the risk of cryptographic flaws is?
(7 Point Likert-Scale from "High" to "Low")
**Q29** How high do you think is the risk of security vulnerabilities in hosted/web wallets or Exchange services?
(7 Point Likert-Scale from "High" to "Low")
**Q30** How high do you think is the risk of key loss due to a device failure?
(7 Point Likert-Scale from "High" to "Low")
**Q31** How high do you think is the risk that the Bitcoin network is temporarily not available?
(7 Point Likert-Scale from "High" to "Low")
**Q32** How high do you think is the risk of a centralization of mining?
(7 Point Likert-Scale from "High" to "Low")
**Q33** How high do you think is the risk of a strong fluctuation in the Bitcoin exchange rate (e.g. BTC to USD and vice versa)?
(7 Point Likert-Scale from "High" to "Low")

### B.7 BTC Anonymity

**Q34** Do you think that Bitcoin usage is anonymous?
*a*) Yes, Bitcoin is fully anonymous *b*) No, Bitcoin is not anonymous *c*) Not per se, but it can be used in an anonymous manner
**Q35** Do you think it is possible to follow your transactions?
*a*) Yes *b*) No
**Q36** Have you ever used Bitcoin over Tor<b title = "Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security. More info at www.torproject.org"?
*a*) Yes *b*) No
**Q37** Do you take additional steps to ensure your privacy using Bitcoin?
*a*) Yes *b*) No

### B.8 BTC Security Breaches

**Q38** Have you ever lost your bitcoins or Bitcoin keys?
*a*) Yes *b*) No
**Q39** Please select the reason for your key/Bitcoin loss (multiple selections possible):
( ) Hardware failure (e.g. hard drive broke, etc.)
( ) Software failure (e.g. keyfile corruption, etc.)
( ) Self induced event (e.g. hard drive formatted, physical device lost, etc.)
( ) Malicious event (e.g. malware, hacker, etc.)
( ) Other

**Q40** Have you been able to recover your keys?
*a*) Yes, *b*) No,
**Q41** How many bitcoins did you loose due to this incident?
*a*) bitcoins *b*) I do not want to specify
**Q42** Please select the security incidents you have been affected by (multiple selections possible):
( ) None
( ) Mt. Gox incident
( ) Silk Road bust
( ) inputs.io hack
( ) Pony botnet malware
( ) Pyramid schemes/HYIPS (High yield investment programs)
( ) Mining hardware scams (Labcoin, Active Mining Corporation, Ice Drill, AsicMiningEquipment.com Dragon-Miner.com, ...)
( ) Mining pool scams
( ) Scam wallets
( ) Bitcoin exchange scam
( ) Other:

**Q43** How did you deal with the incident?
**Q44** What was the approximate value of your lost bitcoins in USD?
*a*) USD *b*) I do not want to specify *c*) I do not know

### B.9 Demographics

**Q45** Please provide your age:
**Q45** Please provide your gender:
*a*) Female *b*) Male *c*) Do not want to specify
**Q46** Please select your highest completed level of education:
*a*) Did Not Complete High School *b*) High School/GED *c*) Some College *d*) Bachelor's Degree *e)* Master's Degree *f*) Advanced Graduate work or Ph.D. *g*) Not Sure
**Q47** Do you work or study in a computer science related field?
*a*) Yes *b*) No

**Q48** How would you describe yourself in terms of privacy behaviour?
A continouos slider between "I am not concerned about my privacy" and "I would describe myself as a privacy fundamentalist"

### B.10 End

**Q49** You can enter your Bitcoin address in the textfield below. Please make sure that your address is correct in order to receive your incentive.
**Q49** This is the place where you can provide suggestions, complaints or any other information we may have forgotten to ask in the questionnaire.

## C Address Signature

```
./bitcoin-cli signmessage 12yeU5ymM67SL5UWVSwErAgwVwwaTd1Nma\
``https://www.soscisurvey.de/BTC_study/"
HzzNxFmeRhbhAwVZ4DsraBkXkW7JYjO0tAlIPAnHB2z5P12eddFilWXJmwGm\
PkgS/v8W0DNr0Z1qLwroPbWWMoE=
```

## D Reference link issue

We had a problem in our implementation of this last page of the survey which also showed the link to the survey containing a random reference which should identify this particular participant in our rewarding scheme. If the CAPTCHA was not solved successfully the side reloads itself and would also calculate and show a different reference link. The references link will only be stored and linked to this particular participant if the CAPTCHA is entered correctly. Therefore, all users which just copied the first link and then entered a wrong CAPTCHA distributed a link we where not able to attribute correctly at the end of the survey.

## References

1. Biryukov, A., Khovratovich, D., Pustogarov, I.: Deanonymisation of clients in Bitcoin P2P network. CoRR, abs/1405.7418 (2014)
2. Baur, A.W., Bühler, J., Bick, M., Bonorden, C.S.: Cryptocurrencies as a disruption? Empirical findings on user adoption and future potential of bitcoin and co. In: Janssen, M., Mäntymäki, M., Hidders, J., Klievink, B., Lamersdorf, W., Loenen, B., Zuiderwijk, A. (eds.) I3E 2015. LNCS, vol. 9373, pp. 63–80. Springer, Cham (2015). doi:10.1007/978-3-319-25013-7_6
3. Biryukov, A., Pustogarov, I.: Bitcoin over Tor isn't a good idea. arXiv preprint arXiv:1410.6079 (2014)
4. Bitcoin Community: Bitcoin developer guide, October 2014. Accessed 14 Oct 2014
5. Bitcoin Community: Bitcoin protocol specification, October 2014. Accessed 14 Oct 2014
6. Blockchain.info: Bitcoin currency statistics, April 2014. Accessed 05 Apr 2014

7. Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J.A., Felten, E.W.: SoK: research perspectives and challenges for Bitcoin and cryptocurrencies (2015)
8. Eskandari, S., Barrera, D., Stobert, E., Clark, J.: A first look at the usability of Bitcoin key management. In: Workshop on Usable Security (USEC) (2015)
9. Reid, F., Harrigan, M.: An analysis of anonymity in the Bitcoin system. In: 2011 IEEE International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing (2011)
10. Garay, J., Kiayias, A., Leonardos, N.: The Bitcoin backbone protocol: analysis and applications. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9057, pp. 281–310. Springer, Heidelberg (2015). doi:10.1007/978-3-662-46803-6_10
11. Garfinkel, S.L., Margrave, D., Schiller, J.I., Nordlander, E., Miller, R.C.: How to make secure email easier to use. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 701–710. ACM (2005)
12. Garfinkel, S.L., Miller, R.C.: Johnny 2: a user test of key continuity management with S/MIME and outlook express. In: Proceedings of the 2005 Symposium on Usable Privacy and Security, pp. 13–24. ACM (2005)
13. Gaw, S., Felten, E.W., Fernandez-Kelly, P.: Secrecy, flagging, and paranoia: adoption criteria in encrypted email. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 591–600. ACM (2006)
14. Gervais, A., Ritzdorf, H., Karame, G.O., Capkun, S.: Tampering with the delivery of blocks and transactions in Bitcoin. Technical report, Cryptology ePrint Archive, Report 2015/578 (2015). http://eprint.iacr.org
15. Goldfeder, S., Gennaro, R., Kalodner, H., Bonneau, J., Kroll, J., Felten, E.W., Narayanan, A.: Securing Bitcoin wallets via a new DSA/ECDSA threshold signature scheme. Accessed 09 June 2015
16. Heilman, E., Kendler, A., Zohar, A., Goldberg, S.: Eclipse attacks on Bitcoin's peer-to-peer network. In: 24th USENIX Security Symposium (USENIX Security 15), Washington, D.C., pp. 129–144. USENIX Association, August 2015
17. Okupski, K.: Bitcoin protocol specification, October 2014. Accessed 14 Oct 2014
18. Lazar, J., Feng, J.H., Hochheiser, H.: Research Methods in Human-Computer Interaction. Wiley, Hoboken (2010)
19. Moore, T., Christin, N.: Beware the middleman: empirical analysis of Bitcoin-exchange risk. In: Sadeghi, A.-R. (ed.) FC 2013. LNCS, vol. 7859, pp. 25–33. Springer, Heidelberg (2013). doi:10.1007/978-3-642-39884-1_3
20. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system, December 2008
21. NIST: FIPS 180–4: Secure Hash Standard (SHS), March 2012
22. Sheng, S., Broderick, L., Koranda, C.A., Hyland, J.J.: Why Johnny still can't encrypt: evaluating the usability of email encryption software. In: Symposium on Usable Privacy and Security (2006)
23. Wharton, C., Rieman, J., Lewis, C., Polson, P.: The cognitive walkthrough method: a practitioner's guide. In: Usability Inspection Methods, pp. 105–140. Wiley (1994)
24. Whitten, A., Tygar, J.D.: Why Johnny can't encrypt: a usability evaluation of PGP 5.0. In: Usenix Security, vol. 1999 (1999)