"I Tried to Buy Drugs Online Using Crypto but Failed": Understanding the Usability & Perceptions of Bitcoin

Chelse Swoopes
Carnegie Mellon University
cswoopes@andrew.cmu.edu

Daniel Stiffler
Carnegie Mellon University
dstiffle@andrew.cmu.edu

Saksham Chitkara
Carnegie Mellon University
schitkar@andrew.cmu.edu

David Edelstein
Carnegie Mellon University
dedelste@andrew.cmu.edu

Lorrie Cranor
Carnegie Mellon University
lorrie@cs.cmu.edu

Abstract

Cryptocurrencies such as Bitcoin have experienced explosive popularity growth over the last year - and some would say it is due to usability improvements. Unlike traditional currencies, cryptocurrency users interact with and control their assets using mathematically-related keys and a public ledger, which requires complex software to manage. The big question hidden in all of the hype is whether cryptocurrency is ready for the mainstream? Many wallets and exchanges claim to offer services that are indistinguishable from, say, online banking. However, there are notable, fundamental differences between owning a dollar and owning a Bitcoin that warrant further study. We were interested in exploring users' perceptions about the technology through an interview which consisted of (i) interviewee's explaining their actions in two hypothetical scenarios and (ii) providing background knowledge and confidence level on that knowledge. We found that participants mentioned security, privacy, and usability harms such as completing a transaction over a compromised network, being identified by unwanted actors, and experiencing wallets with a bad user interface. They also focused on Bitcoin specific considerations such as price fluctuation and verification issues.

Author Keywords

Bitcoin; cryptocurrencies; wallets; exchanges; usability; security; privacy

ACM Classification Keywords

H.1.2 User/Machine Systems: Human factors; K.6.5 Security and Protection: Authentication, Unauthorized access

1. Introduction

Cryptocurrencies such as Bitcoin [1] have exploded in popularity resulting in a huge surge in their demand. The price of Bitcoin increased by 1300% in 2017, peaking at nearly $20,000 in December 2017 [2]. In addition, the total number of cryptocurrencies has risen to more than 1600 as of May 2018 [3]. While there are mixed opinions regarding the destiny of cryptocurrencies, Bitcoin, the most famous of the lot, has garnered many supporters. Eric Schmidt, the ex-CEO of Google, stated "[Bitcoin] is a remarkable cryptographic achievement. The ability to create something which is not duplicable in the digital world has enormous value. Lots of people will build businesses on top of that," further fueling public interest in cryptocurrencies [5]. The growth of cryptocurrencies has been fueled by novel features like decentralization, as well as perception of user anonymity and control. However, anonymity is far from given in Bitcoin as all transactions are permanently recorded in a public ledger. Previous privacy and security research has found that users often relegate privacy and security to a secondary goal and perceive that security comes by default [4]. However, users' mental models are unclear in the domain of cryptocurrencies. We first try to understand the users' perceptions of Bitcoin and whether these match reality. Second, we study whether the users' misconceptions related to security translates to Bitcoin as well. To the best of our knowledge, both of these topics haven not been studied and are novel research contributions. Given the popularity, market share of more than 36% (the highest among all cryptocurrencies), market value and the originator status of Bitcoin, we restrict our evaluation on cryptocurrencies to Bitcoin [3]. In this paper we interview twelve novice and experienced cryptocurrency users. We walk through two hypothetical scenarios in which the participants attempt to transact using Bitcoin. First, the participants are instructed to tell us how they would pay for coffee using Bitcoin. Second, the participants are given the hypothetical scenario of donating to a charity using Bitcoin. We ask the participants to be specific and tell us how they would ensure speed, authenticity, integrity and confidentiality of the transaction. We also ask them to talk about the trade-offs involved in terms of achieving one of these goals by giving up the others. Finally, we ask the participants generic questions about Bitcoin wallets to further gauge their understanding of Bitcoin.

2. Methodology

To understand the perception of users on cryptocurrencies, we interviewed cryptocurrency enthusiasts. We conducted an interview because it is the best way to collect the in-depth data required by our study. We wanted a mix of novice and experienced users to avoid restricting our participants by requiring use of a wallet or exchange before. To be in the study, participants were required to be at least eighteen years old, answer "Yes" to having knowledge [either conceptual or applicable] on using a cryptocurrencies wallet or exchange, and capable of providing written consent. All the responses were kept anonymous and our study was approved by the Institutional Review Board of Carnegie Mellon University.

2.1 Interview

We recruited twelve participants by word-of-mouth, and qualified them if they were eighteen years or older, had used a cryptocurrency wallet, exchange or were cryptocurrency enthusiasts. To gauge the actual cryptocurrency knowledge of our participants, we included questions at the end of our interview where we asked participants generic cryptocurrency questions. In addition, we asked the participants to rate themselves on their knowledge about cryptocurrencies. This was done to understand participant's actual knowledge with their perceived knowledge. Our study included seven male and five female participants. We understand that our sample set is skewed as all participants were associated with Carnegie Mellon University. We wanted to understand some of the major misconceptions harbored by Bitcoin users. In addition, we wanted to understand users' perception regarding Bitcoin. Consequently, we designed our interview with these two goals in mind. We focused on the transaction properties of confidentiality, authenticity, integrity and speed. It is sometimes more relevant to trade one of the properties for the others based on the situation. Therefore, we designed two scenarios to focus on the contrasting properties of transactions. We conducted two pilot interviews where the interviewees walked through two hypothetical scenarios and rated their confidence on an array of Bitcoin related topics. In the first scenario, they were requested to imagine a scenario where they would pay for Coffee using Bitcoin and they were given a new wallet. This was done to alleviate concerns about privacy and security in this scenario and only focus on the speed and authenticity of the transaction. Our pilot interviews for this scenario went well and the interviewees focused on the intended topics, and provided us with interesting insight. In the second scenario, the participants were told that their entire salary would be paid in Bitcoin and they had to make transactions to protect their anonymity. The goal of this scenario was to focus on confidentiality, authenticity and integrity of transactions without going too much into speed. In this scenario, our pilot interviewees digressed into topics like price fluctuations in Bitcoin. They also mentioned that they would not be comfortable accepting their salary in Bitcoin. While these topics were interesting, they were not relevant to what we wanted to study. Therefore, for our actual study, we changed the second scenario to payment to a charity in Bitcoin. This scenario was more specific and the interviewees would be allowed to focus on the intended transactional properties of authenticity, integrity and confidentiality without focusing on the speed. The full interview script can be found in the Appendix of the full report.

2.2 Emergent Coding

After the twelve interviews were conducted, the responses were reviewed to develop a codebook for emergent coding. The reviewer looked for patterns of comments, concepts, and perceptions that interviewee's stated. These were then redefined into categories. Categories included security, privacy, and usability harms such as completing a transaction over a compromised network, being identified after using anonymization techniques such as using a pseudonym, and experiencing wallets with a bad user interface. An additional category focused on Bitcoin specific considerations such as price fluctuation and verification issues. The codebook also allowed coders to tag interviewee's thoughts on whether the two scenarios were compelling use cases. In addition, we coded responses to the user's background such as their duration of using/exploring Bitcoin. Quantitative analysis of these results are discussed below in the Results section. After reviewing the codebook, two coders separately coded a sample interview to practice using the codebook, gauge and correct misunderstandings with the codebook, and resolve any conflicts. After the sample was complete, 30% of the interviews were double coded and the remaining 70% was coded by one coder. The full codebook can be found in the Appendix of the full report.

3. Results

We received interesting comments from our interviewees. P6 mentioned, “blockchain will take care of security." This echoes the sentiment of prior security misconceptions where users feel that the device should take care of their security. Roughly 40% of participants were not concerned with security issues in scenario one where little money was involved. The top security concern in scenario one was possible verification issues with the possibility of the coffee shop not being able to verify the customers transaction whether due to network security issues or account compromise (see figure 1). Regarding the usability of Bitcoin, 75% of interviewees agreed that the transaction times are not yet fast enough for instantaneous transactions such as the coffee shop scenario, but would be okay for scenarios such as donating money where a return is not expected. In addition, usability remains a big hurdle before the mass adoption of cryptocurrencies. Participants mentioned usability problems such as price fluctuation (92%), the need for the recipients correct address (75%), transaction time (75%) and transaction fees (42%) which are persistent while using Bitcoin. One participant even claimed, “I tried to buy drugs online using cryptocurrency, but failed. The usability [of cryptocurrencies] sucks."

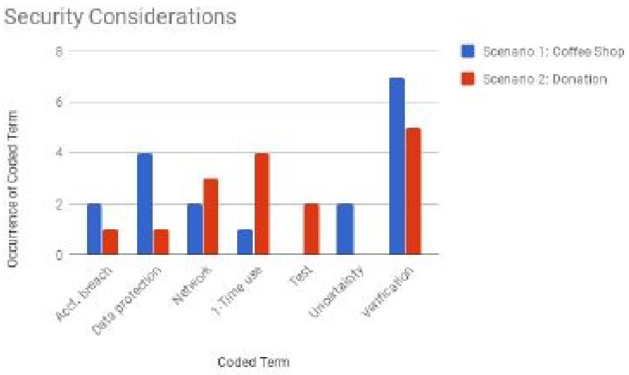

Figure 1: Security considerations per scenario

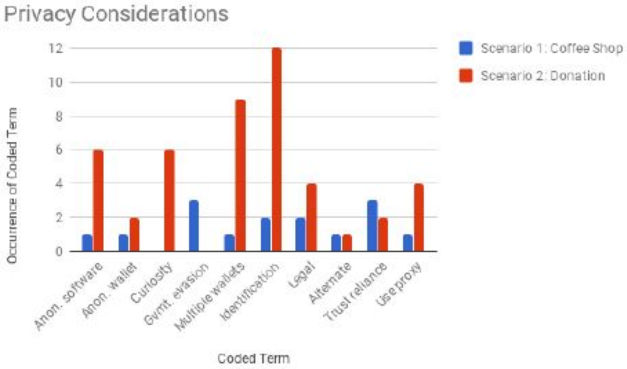

Figure 2: Privacy considerations per scenario

In terms of privacy, 50% of participants did not have concerns for scenario one, whereas roughly 16% did not have privacy concerns for scenario two. This is likely explicable by the lower stakes of buying coffee, similar to the gap for security. The concerns can be seen in Figure 2. For scenario one, 25% of participants were concerned about the government being able to retrieve data from the wallet/exchange companies. No participants voiced this concern for scenario two. The top privacy concern from all participants for scenario two was the possibility of being identified or traceable. Their solutions to this were to use multiple wallets for the transaction (75%) and utilize anonymizing software (50%). Some of the more skilled participants brought up mixing services. Overall, we found that participants have contrasting and sometimes dangerously incorrect mental models. While we do not have a qualitative measure to rank our participants (Limitations section in full paper), we noticed that the participants with little knowledge consistently overrated their expertise, whereas those who actually did have some understanding of cryptocurrencies took a more modest view of their abilities.

References

1. Bitcoin.org. Bitcoin. https://bitcoin.org/en/, 2018. [Online; accessed 10-May-2018].
2. BusinessInsider. Cryptocurrency price. http://markets.businessinsider.com/currencies/btc-usd, 2018. [Online; accessed 10-May-2018].
3. CoinMarketCap. CoinMarket Capital. https://coinmarketcap.com/, 2018. [Online; accessed 10-May-2018].
4. S. M. Furnell, A. Jusoh, and D. Katsabas. The challenges of understanding and using security: A survey of end-users. Computers & Security, 25(1):27{35, 2006.
5. Interview. Eric Schmidt on Bitcoin. https://www.youtube.com/watch?v=jRrEZbKm3m, 2018. [Online; accessed 10-May-2018].