Anonymity in Bitcoin? – The Users’ Perspective

Conference Paper · December 2016

3 authors, including:

Benjamin Fabian
Hochschule für Telekommunikation Leipzig
95 PUBLICATIONS 640 CITATIONS

Tatiana Ermakova
Universität Potsdam
22 PUBLICATIONS 108 CITATIONS

Some of the authors of this publication are also working on these related projects:

- E-Mail and Web Tracking – Empirical Analysis, Privacy Impact, Countermeasures View project
- Privacy Policies – Readability, Content, Impact View project

All in-text references underlined in blue are linked to publications on ResearchGate, letting you access and read them immediately.

Available from: Benjamin Fabian
Retrieved on: 10 November 2016
Anonymity in Bitcoin – The Users’ Perspective

(Draft Version)

Research-in-Progress

Benjamin Fabian
Chair of Business Intelligence and Data Science, Hochschule für Telekommunikation Leipzig (HfTL)
Gustav-Freytag-Str. 43–45
04277 Leipzig, Germany
fabian@hft-leipzig.de

Tatiana Ermakova
Chair of Business Informatics, esp. Social Media and Data Science University of Potsdam
August-Bebel-Str. 89
14482 Potsdam, Germany
tatiana.ermakova@uni-potsdam.de

Ulrike Sander
Institute of Information Systems Humboldt-Universität zu Berlin
Spandauer Str. 1
10178 Berlin, Germany
uli-sander@web.de

Abstract

This article analyzes how users perceive the degree of anonymity provided by the Bitcoin network, to what extent they are concerned about anonymity when using Bitcoin, whether they are knowledgeable of and concerned about specific de-anonymization attacks, and if they are aware of and adopt privacy-preserving countermeasures.

A user survey with 125 active Bitcoin users reveals that 70% associate a medium or high level of anonymity with the Bitcoin network and rate their concerns as either low or medium. But almost every fifth user has already considered abandoning Bitcoin because of being concerned about anonymity. Though one third are aware of the risk of de-anonymizing the Blockchain but are not concerned, another almost 50% indeed feel concerned.

Our findings have implications for users and developers, suggesting that actions should be undertaken to increase privacy awareness and the level of anonymity provided by the Blockchain and the Bitcoin network.

Keywords: Bitcoin, Blockchain, Privacy, Anonymity, User Requirements

Introduction

Bitcoin (BTC) is a convertible virtual currency based on a decentralized peer-to-peer network. In 2009, Bitcoin was launched by a person known as Satoshi Nakamoto (Nakamoto, 2008) and has gained a large amount of controversial media and government attention since its introduction. Due to Bitcoin’s decentralization, there are lower transaction costs and fees, no financial institute acting as an intermediary, and financial freedom as accounts cannot be frozen (Mullan, 2014).
However, in contrast to popular belief that another benefit associated with Bitcoin is its full anonymity, Bitcoin is not per se anonymous. All confirmed transactions with the corresponding Bitcoin addresses as pseudonyms are publicly announced in the Blockchain (Meiklejohn et al., 2013).

In our research project, we aim to investigate the privacy awareness and potential concerns of users of peer-to-peer applications based on the Blockchain technology, with Bitcoin as a starting point. By conducting a study among active Bitcoin users, the present research study analyzes how users assess the level of anonymity provided by the Bitcoin network and to what degree they are concerned about their anonymity when using Bitcoin. It further examines Bitcoin users' awareness and concerns regarding the general risk of de-anonymizing the Blockchain in general and based on specific de-anonymization techniques. Finally, this study investigates Bitcoin users’ knowledge and adoption of various currently existing countermeasures.

Our article is structured as follows. The next section provides background on privacy concerns and their impact on adoption and usage of online technologies. It further discusses the different methods of attacking Bitcoin users' anonymity and their potential impact. Existing as well as potential improvement measures together with their benefits and drawbacks are contrasted as well. After that, we proceed with the main contribution of this paper, presenting the results of a survey of 125 active Bitcoin users about Bitcoin anonymity. Finally, limitations and future work directions are given, followed by concluding remarks including resulting implications.

**Background**

**Privacy Concerns**

In the management information systems (MIS) research, information privacy is subject of intense research (Smith et al., 2011; Bélanger and Crossler, 2011; Pavlou, 2011; Li, 2011, 2012). Scholars define information privacy concerns as the degree to which individuals are concerned about online companies' practices with respect to the collection and use of their personal information (Smith et al., 1996). Especially due to companies tracking online users and sharing their personal information with third parties, online users feel increasingly concerned about their information privacy (TRUSTe, 2015).

Empirical studies repeatedly confirmed the negative effect of information privacy concerns on individuals' attitudes towards online services (Angst and Agarwal, 2009; Dinev et al., 2012), behavioral intention to use online services (Angst and Agarwal, 2009; Li, 2013; Dinev and Hart, 2006b), behavioral intention to reveal information for online transactions (Smith et al., 1996; Bansal et al., 2010; Korzaan and Boswell, 2008; Dinev and Hart, 2006a), and actual behavior (Son and Kim, 2008). Practice similarly shows that almost ninety percent of Internet users avoid companies that do not protect their privacy (TRUSTe, 2015).

Based on this theoretical background, it is our hypothesis that privacy concerns could also constitute a major obstacle to the adoption of Bitcoin and other Blockchain applications.

**Anonymity in Bitcoin**

Although some MIS scholars do not differentiate between information privacy and information control (Smith et al., 1996; Malhotra et al., 2004; Hong and Thong, 2013), others argue that information control rather plays a key role in the formation of information privacy (Dinev et al., 2012, 2013; Xu et al., 2011, 2012). A recent study by Dinev et al. (2013) further shows that, mediated through perceived information control, a critical aspect of perceived privacy is the ability to stay anonymous when using an online service.

Based on a classical definition of anonymity (Pfitzmann and Hansen, 2010), the Bitcoin network should be regarded as anonymous for a payer or payee, if and only if an attacker is not able to sufficiently identify the payer or payee within the Bitcoin user community. The media’s popular belief that Bitcoin is fully anonymous stems from a misunderstanding of the currency (Brito and Castillo, 2013). In fact, anonymity was not a primary design goal of the Bitcoin system (Reid and Harrigan, 2011). All Bitcoin transactions are publicly visible in the Blockchain; however, instead of the user's name, his or her public address occurs as a pseudonym. Therefore, all transactions are pseudonymous (Ober et al., 2013).

---

**Anonymity in Bitcoin – The Users’ Perspective**
Androulaki et al. (2013) determine unlinkability as a measure to quantify privacy in Bitcoin. Privacy is stronger, the less personal data of the real identity can be linked to the pseudonym, and the less often the same pseudonyms are used and the less linkable different pseudonyms of one identity are. According to Nakamoto (2008), some linking is not avoidable in the Bitcoin network, because multi-input transactions reveal that their inputs were held by the same owner. The risk for anonymity emerges when the owner of one public key is revealed, as linking could result in exposing other transactions that belong to the same user as well.

Among the first ones, Reid and Harrigan (2011) argued that the inherent limits of anonymity largely stem from the Blockchain technology. This publicly visible ledger of all confirmed transactions is necessary to avoid double spending since there is no central authority in the network. However, all addresses used as an input for a single transaction can be grouped to one identity, as a user needs to possess all of those addresses for such multi-input transactions. Then one can cluster all those addresses, which are considered to belong to the same person, into a user network. This heuristic is used as a foundation by many other scholars to de-anonymize the Bitcoin network (Ober et al., 2013; Androulaki et al., 2013; Meiklejohn et al., 2014; Ron and Shamir, 2013). Spagnuolo et al. (2014) developed BitIndoine, a modular, semi-automatic framework that clusters addresses, labels the classified addresses and visualizes them.

Another approach to de-anonymize the Bitcoin network is the mapping of Bitcoin addresses to Internet Protocol (IP) addresses. This technique does not rely on the links between the transactions (Koshy et al., 2014). Its aim is rather to associate an IP address with a specific Bitcoin address, which is taken from the Blockchain. Possessing information about the device which a Bitcoin address originated from would be a major breach of anonymity. Inspired by Kaminsky (2011), Koshy et al. (2014) analyzed the possible risk of mapping Bitcoin addresses directly to IP data. They built a Bitcoin client, which they called CoinSeer, to actively collect the data of 5.6 million transactions. Lischke and Fabian (2016) used such mapping techniques to study the evolution of the Bitcoin economy. One can argue that IP addresses could remain untraceable when proxy or anonymity services such as Tor are used. However, Biryukov et al. (2014) showed that Tor users could be de-anonymized as well. Moreover, according to a more recent study by Biryukov and Pustogarov (2015), due to man-in-the-middle attacks, combing Tor and Bitcoins results in an even greater risk of being de-anonymized than by not using Tor.

Summarizing the challenges for privacy, anonymity of Bitcoin users can be eroded. Most of the researchers conducted their analysis by not only using the Blockchain, but also availing themselves of external information from the Internet. While some measures for improving anonymity in Bitcoin are already partially adapted, others are still fiercely discussed, trading off advantages versus disadvantages.

Concerning measures for increasing security and privacy, Bitcoin experts generally agree on advocating specific best practices regarding storage of Bitcoins. One major aspect involves the secure storage of private keys. In order to communicate with the network, the wallet is usually held by a device, which is connected to the Internet (Franco, 2015). This storage method is known either as an online, Web or hot wallet. Due to the fact that over the Internet connection many attacks can be conducted, it is recommended to store only small amounts of Bitcoins in a hot wallet (Franco, 2015; Barski and Wilmer, 2015). A Web wallet is less secure because an external provider manages the funds (Franco, 2015). Implications for privacy are on the one hand the increased anonymity, as for instance, Koshy et al. (2014) were not able to identify Bitcoin addresses controlled by a Web wallet with their method. On the other hand, the anonymity is decreased, since Web wallet providers have personal information and usually keep a record of all transactions (Franco, 2015).

A safer but not so convenient way to store Bitcoins is the cold storage, a place that is not accessible via the Internet. That is recommended for large amounts of Bitcoins (Barski and Wilmer, 2015). Cold storage devices are, for example, USB flash drives, paper wallets and hardware wallets. Hardware wallets store private keys on an offline computer, but can also sign transactions by plugging it into an online computer, which actually makes them a secure and convenient storage method (Barski and Wilmer, 2015). Although hardware wallets have higher purchase costs, experts expect this type of storage will become the predominant method (Antonopoulos, 2015).

Meiklejohn et al. (2013) and Barcelo (2014) further argue that reusing public addresses is not advisable. Nakamoto (2008) suggested using a new key pair for each transaction to limit linkability to some extent. Antonopoulos (2015) describes a convenient way to create a new key for each transaction: the hierarchical...
deterministic (HD) wallets. This way keys are derived in a tree structure, such that a master key can derive a sequence of child keys, those can derive a sequence of grandchild keys, and so forth. The advantage is that public keys can be created without having access to the private key. Therefore, HD wallets can also be installed on an unsafe server. Todd (2014) developed a technique that makes it possible for payees to publish one single Bitcoin address, the so-called stealth address (SX), which payers can send funds to, while at the same time providing anonymity, as payers and other third parties cannot learn what other payment have been made to that stealth address.

High anonymity within the Bitcoin network is also promised by (coin) mixing services. The concept behind mixers is that the Bitcoins pass a mixing service before entering into possession of the payee. The central mixing service draws profit in form of a 1-3% mixing fee for making the transactions unlinkable, and thus reaching a higher level of anonymity. Möser et al. (2013) used reverse-engineering to test the actual effectiveness of three money laundering tools. However, it must be differentiated between central and decentralized mixing services. Central mixing services, for instance, Bitcoin Fog, are trusted third parties, whereas Nakamoto (2008) actually intended to create a currency that does not rely on trust. The problem with trust is that service providers could steal funds, track coins or just become insolvent (Miers et al., 2013).

A decentralized way of mixing is known as CoinJoin. In 2013, the Bitcoin developer Gregory Maxwell proposed a way for joint payments, meaning that at least two users make a multi-input and multiple output transaction (Maxwell, 2013). The probably most serious issue with CoinJoin as an anonymity improvement measure is that it only works impeccably if the payments are of similar amounts (Barcelo, 2014). In other words, with the aid of the transaction amounts, input and output addresses might still be linkable. Consequently, cluster analysis could work successfully if the payments do not differ in their amounts. On the other hand, CoinJoin has the crucial benefit, compared to central mixing services, of being independent of trusted third party services, meaning that the risk of theft is minimized. That is the reason for its implementation in, for example, SharedCoin.com, the currently implemented mixing service from Blockchain.info. In order to improve CoinJoin’s problem of linkability though the transaction amounts, Maxwell (2015) recently proposed confidential transactions based on homomorphic encryption. All these mixing services can be easily integrated into the current Bitcoin Blockchain and do not require any modifications of the core protocol.

A different approach that would require changing the protocol is Zerocoin (Miers et al., 2013). Zerocoin is not a mixing service per se, but it also operates as a decentralized mixer (Franco, 2015). Like CoinJoin, Zerocoin aims to provide unlinkability without any trusted parties. The general idea behind the concept is to mint Zerocoins out of Bitcoins. These Zerocoins can be redeemed at a later point in time into Bitcoins, which cannot be linked with the previous Bitcoins. Thus, unlinkability in the transaction graph can be attained. Compared to CoinJoin, Zerocoin’s main disadvantages are the scaling limits leading to uncertainty if the theoretical approach would actually work in practice, as well as the required change of the Bitcoin protocol (Maxwell, 2013).

Concluding, there are several approaches for improving anonymity in Bitcoin, which include various benefits and drawbacks. Our main research questions are: (i) To what degree do Bitcoin users perceive anonymity on Bitcoin? (ii) To what degree are Bitcoin users concerned of anonymity risks? (ii) Are Bitcoin users aware of and how do they regard usage of potential anonymity improvements?

**User Survey on Bitcoin Anonymity**

**Procedure**

The persons of primary interest for our user study are all Bitcoin users located in the United States of America and in Europe. Bohr and Bashir (2014) as well as Yelowitz and Wilson (2015) argue that surveying a random sample of Bitcoin users is nearly impossible. This limitation also applies to our survey. The participation was voluntary, and because no central authority is involved in the Bitcoin network, there is no complete overview of who is using Bitcoin. However, our questionnaire was made accessible to many active Bitcoin users through the distribution of the survey’s link on several international channels. It was shared in various Bitcoin groups on the social media networks Facebook, LinkedIn and Xing, as well as in the Bitcoin forums Bitcointalk.org and Reddit.com/r/Bitcoin.
This seems to be a very effective way to reach Bitcoin users, as Bohr and Bashir (2014) as well as Smyth (2013) found that Bitcointalk, Reddit and Facebook are the three most popular platforms to discuss Bitcoin with others. Furthermore, emails drawing attention to the survey and requesting participation were sent to all students of a major university in Germany, as well as to all 195 businesses listed on coinmap.org in Germany whose email addresses were accessible via their homepage, to 150 randomly selected businesses in the United States of America and to 150 randomly selected businesses in the United Kingdom. Therefore, it can be assumed that for an initial pilot study, a relatively comprehensive data set was delivered. That was confirmed when comparing the user demographics of this study to Smyth (2013) with one thousand responses, Bohr and Bashir (2014), and CoinDesk (2015) with four thousand responses.

The respondents were first asked to rate how much anonymity Bitcoin provides in their opinion in general and in combination with third-party services. They were further expected to answer how high they rate their concerns about their anonymity when using Bitcoin in general and compared with cash, credit cards, and PayPal. Both questions could be responded with one of the following options: no, little, medium, a lot, no opinion. The next question focused on whether they have ever considered not using Bitcoin because of anonymity concerns, which could be answered with either yes or no. Then, they were asked to only fill-in if applicable whether they store their large and small Bitcoin amounts in an online-hosted wallet, online personal wallet, personal hot wallet, paper wallet, metal coins, and hardware storage.

Next, we asked the participants to state the degree of concern associated with the risk of de-anonymizing the Blockchain in general and based on the de-anonymizing techniques such as cluster analysis and revealing the IP address via the Bitcoin address. Here, we were interested whether they are unaware of the risk, aware but not concerned, slightly concerned, moderately concerned, or highly concerned. After that, they had to respond whether they are aware of not reusing public addresses and using stealth addresses as anonymity improvement measures and adopt them, as well as whether they were aware of Zerocoins, CoinJoin and would use them for increased anonymity if they were implemented by the Bitcoin community. Finally, they were asked to provide information regarding their country, age and gender. The detailed text of the questionnaire and sources for data collection will be made publicly available in an online companion document. The 129 received completed questionnaires were reduced to a sample size of 125, as it became apparent that four respondents do not use Bitcoin and consequently are not of interest to this survey.

Demographics

The most frequent respondent in this survey is a self-reported male (95%) German (54%) aged between 20 and 29 years (35%) or between 30 and 39 years (32%) (see Table 1).

While Bohr and Bashir’s (2014) predominant recorded nationality was American (44%), most participants (54.1%) in our study are Germans, followed by EU citizens except Germans (19.67%), and Americans (14.75%). With slightly over half of all full respondents being of German nationality, our empirical study has a special focus on Germany. We argue that this limitation also has benefits for our research questions, since German-speaking countries are often considered very privacy-aware (Bellman et al., 2004). Furthermore, in our earlier work (Lischke & Fabian, 2016) that empirically analyzes the Bitcoin transaction graph and applies geolocation methods, we show that Europe (and in particular Germany) is one of the two hotspot areas of Bitcoin activity. Moreover, Germany is an important global economic power and market (Audretsch and Lehmann, 2016), which is very relevant for studying the acceptance of a cryptocurrency.

Concerning the representativeness of gender, a similar, very high percentage of male respondents has also been discovered by Bohr and Bashir (2014) and Smyth (2013), who reported 95% of male participation. CoinDesk (2015) speak about over 90%. There are various attempted explanations for the apparent current dominance of men in the Bitcoin network. Scott’s (2014) most reasonable suggestion might be an inherent masculinity of Bitcoin. In this regard, he means, on one hand, a certain biological propensity of men to enjoy technology rather more than women do. This view can be supported by some empirical studies. For instance, Venkatesh and Morris (2000) have already shown by reference to the technology acceptance model (TAM) that there are gender differences for accepting new technology, such as that the perceived ease of use influences behavioral intention to use a system more strongly for women than for
men. On the other hand, Scott (2014) alludes to women’s assumed higher risk aversion, since Bitcoin is highly volatile.

<table>
<thead>
<tr>
<th>Table 1. Survey Demographics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
</tr>
<tr>
<td>Nationality</td>
</tr>
<tr>
<td>American</td>
</tr>
<tr>
<td>European</td>
</tr>
<tr>
<td>European (German)</td>
</tr>
<tr>
<td>European (not German)</td>
</tr>
<tr>
<td>Other</td>
</tr>
<tr>
<td>Gender</td>
</tr>
<tr>
<td>Female</td>
</tr>
<tr>
<td>Male</td>
</tr>
<tr>
<td>Age</td>
</tr>
<tr>
<td>&lt; 20 years</td>
</tr>
<tr>
<td>20-29 years</td>
</tr>
<tr>
<td>30-39 years</td>
</tr>
<tr>
<td>40-49 years</td>
</tr>
<tr>
<td>≥ 50 years</td>
</tr>
</tbody>
</table>

It is noticeable that nearly three-quarters are aged 39 or younger. CoinDesk (2015) also found almost 60% under 35 years, with 39.4% people aged between 25 and 34 years and 22% aged between 35 and 44 years. Smyth (2013) further revealed the age groups between 25 and 29 years and 30 and 34 years as two peaks in the age distribution of the Bitcoin community.

Therefore, the relatively young and mainly male respondents seem to be representative.

**Results and Discussion**

**Section 1: Anonymity Concerns**

Respondents were first asked about how much anonymity Bitcoin provides in their opinion (Figure 1, Left). The term anonymity was explained as the state of a person/group not being able to be identified. Overall, almost 40% associated a medium level of anonymity with the platform, followed by 30% who rated the level of anonymity as high. However, another one-quarter of the participants believed that Bitcoin provided little (14%) or no (12%) anonymity.

Interestingly, when asked about anonymity on Bitcoin combined with third party services, the proportion of those who attributed either no (7%) or medium (25%) anonymity to the platform almost halved, whereas the proportion of those who rated the anonymity as little (26%) almost doubled. It seems that participants could have had different kind of third party services in mind, general services around Bitcoin or privacy-enhancing services. Therefore, in future work, we would like to investigate specifically if Bitcoin and Blockchain users would consider third-party anonymity services trustworthy.
The survey showed that more than 1 out of 5 (22%) has already considered abandoning Bitcoin due to anonymity concerns. Therefore, respondents were next asked about their anonymity concerns on Bitcoin, and this in general, compared to cash, credit cards, and PayPal (Figure 1, Right). Most people rated their concerns as either low or medium (each 36%). Highly concerned ones were less present (15%). Only the remaining 8% had no concerns in general. Participants rated their concerns quite similarly when they compared Bitcoin with cash (no: 10%, low: 30%, medium: 26%, high: 23%): The proportion of highly concerned Bitcoin users increased and those with low or medium concerns got smaller.

The picture completely changed when Bitcoin was compared with credit cards or PayPal (no: 28%, low: 25% and 26%, medium: 9% and 8%, high: 24% and 26%, respectively). The proportion of those who were not worried at all was over three times as high as in general, whereas the proportion of those who rated their anonymity concerns as medium was four times as low as in general. Credit cards’ potential lack of anonymity was recently analyzed by de Montjoye et al. (2015). They were able to re-identify uniquely 90% of users with only four pieces of external information, such as a tweet about a restaurant he/she was having lunch. Therefore, the users’ assessment seems to be reasonable.

The next question asked participants to state the degree of their concerns associated with the risk of de-anonymizing the Blockchain, cluster analysis, and finding out the IP address via the Bitcoin address (Figure 2, Left). 35% were aware of the risk of de-anonymizing the Blockchain, but were not concerned. Almost 50% were, however, concerned in some way: either slightly (21%), or moderately (17%), or highly (10%). But almost one fifth (18%) were not aware of the risk.

Furthermore, to achieve a deeper understanding of what exactly worries users, the participants separately rated the concerns regarding cluster analysis and finding out the IP address via the Bitcoin address. Cluster analysis was explained as an attempt to group those public addresses in one cluster, which belong...
to the same entity. The most frequent answer to cluster analysis was “unaware of the risk” (34%). For finding out the IP address via the Bitcoin address, “unaware” was also a relatively frequent answer (30%). Currently, mainly academic research papers address those possible attacks. This could be the reason why they are still relatively unknown. Whereas 32% state that they are aware but not concerned about mapping Bitcoin addresses to IP addresses, only 18% are aware but not concerned about the cluster analysis. Correspondingly, more participants are slightly concerned about the cluster analysis (29%) than about mapping IP addresses (22%) as well as moderately concerned (cluster analysis: 14%, mapping IP addresses: 9%). Therefore, the cluster analysis seems to be a more unknown and more concerning technique. However, only 5% are highly concerned about it, in contrary to 8% who find mapping IP addresses a highly concerning method. In addition, from the feedback on Bitcointalk.org, some participants could not imagine that it is possible to track the IP address by the aid of the Bitcoin address. All in all, approximately one-third of the participants are unaware of the specific de-anonymizing techniques, and those who are conscious of the fact are on average slightly concerned.

Section 2: Improvement Measures

Most participants store Bitcoins in less secure hot wallets. However, the results also indicate that most participants act according to the recommendations (Figure 2, Right). 44% store small amounts of Bitcoins in an online hosted wallet. Only 9% use this storage method for large amounts. Similarly, 26% store small amounts and only 7% large amounts in online personal wallets, and 37% store small amounts and 18% large amounts in personal hot wallets. Cold storage methods are not only less popular but also less known, most probably due to the inconvenience. However, at least 18% follow the recommendation to use paper wallets for large amounts of Bitcoins. Metal coins are in general quite unknown. 23% are not aware of this storage method. Although similarly 22% do not know hardware storage, 12% of the participants already use it for large amounts. This demonstrates the users’ potential to behave more consciously with respect to security and privacy.

Further previously discussed best practices include not reusing public addresses and implementing stealth addresses (Figure 3, Left). Nearly half of the participants (47%) do not know that they are able to use stealth addresses. Another 46% are aware but do not adopt them, and only 7% use stealth addresses. This concurs with the theoretical findings that this technique is particularly beneficial for businesses that wish to publish one single address on their website that payers can send their funds to, for these businesses are a minority group among Bitcoin users. The result was considerably different when it was asked about single use of public addresses. Only 18% are not aware that single use of public addresses is an anonymity improvement measure. 35% are aware but do not adopt it, and 47% adopt it. Therefore, it seems to be a well-established technique, which most users deliberately chose to take or not to take.

Analyzing Figure 3 (Right) makes obvious that coin mixing services are better known and the participants are more willing to use them, compared to the other two measures. 38% of the participants would actually use coin mixing services. Another 38% would not use them, and 24% do not know the method. More than...
half of the participants are not familiar with CoinJoin (52%) and Zerocoins (58%). Even of those aware of the measures in both cases, 29% would not use them if the community implemented them.

**Limitations and Future Work**

Concerning limitations of our initial study, we would like to extend the audience of our questionnaire beyond its current (de facto) focus on Europe and Germany. This work has an explorative character and opens new avenues for conducting future studies. First, due to the absolute dominance of men in the Bitcoin network (Bohr and Bashir, 2014; Smyth, 2013; CoinDesk, 2015), which was also confirmed in our study, it would be interesting to explore the reasons why female online users avoid the Bitcoin platform and how they could be engaged into the Bitcoin community. Second, further insights can be gained through examining the dependencies between the aspects considered in this study. For example, our study demonstrates that a great majority of people has concerns when using Bitcoin (87%), and this in the presence of relatively large lack of awareness about potential anonymity-improvement measures such as not reusing public addresses (18%), using stealth addresses (47%), CoinJoin (52%) and Zerocoins (58%). In light of these findings, further research could examine the effect of awareness and adoption of these privacy-preserving countermeasures on reducing Bitcoin members' anonymity concerns, as suggested by prior literature (Dinev and Hart, 2006b). Third, a comparison between perceived anonymity on Bitcoin in general and perceived anonymity combined with third party services provides rather non-conclusive results so far. We assume that participants could have thought of different third party services, which could be general services around Bitcoin or privacy-enhancing services. Another reason might be that Bitcoin and Blockchain users generally consider third party services as untrustworthy. None of these issues are explored in the present study and are thus definitely warrant future research.

Finally, as previously reviewed, mitigating privacy concerns is essential for the success of online services. Improving privacy in the Bitcoin ecosystem can be regarded as a very important opportunity for future research. The role of user privacy and anonymity in the adoption of other cryptocurrencies and novel emerging Blockchain applications (Christidis and Devetsikiotis, 2016; Yue et al., 2016; Yuan and Wang, 2016; Ølnes, 2016; Ferrer, 2016; Weber et al., 2016; Kim and Laskowski, 2016) should be further part of future investigations.

**Conclusion**

The present research examines how users perceive anonymity provided by the Bitcoin network, to what degree they are concerned about their anonymity there, whether they are aware of and concerned about de-anonymization risks, and whether they are aware of and adopt potential privacy-preserving measures. A user survey with 125 active Bitcoin users revealed that seven out of ten associate a medium or high level of anonymity with the Bitcoin network and rate their concerns as either low or medium. But almost every 5th user has already considered abandoning Bitcoin because of being concerned about her or his anonymity. 35% are aware of the risk of de-anonymizing the Blockchain, but are not concerned, and another almost 50% are, however, concerned in some way.

Participants mostly act according to the recommendations when storing different amounts of Bitcoins in different types of wallets. Although cluster analyses and mapping Bitcoin addresses to IP addresses can effectively de-anonymize the Blockchain, approximately one-third of the participants are unaware of those specific de-anonymizing techniques. Nearly half of the participants (47%) do not know that they are able to use stealth addresses. Another 46% are aware but do not adopt them. Only 18% are not aware that single use of public addresses is an anonymity improvement measure, and 35% are aware but do not adopt it. Finally, coin mixing services are better known and the participants are more willing to use them, compared to measures CoinJoin and Zerocoins.

The findings of this research have implications for both Bitcoin developers and Bitcoin users. Specifically, they show that Bitcoin developers need to undertake efforts to increase the level of anonymity provided by the Blockchain technology and the Bitcoin network. Among others, they should refine the existing improvement measures for privacy, since these have weaknesses in guaranteeing full anonymity. Furthermore, Bitcoin users’ privacy-awareness with respect to the Blockchain technology needs to be increased. Not least, Bitcoin users can take this article as a starting point to better inform themselves about options for more secure and anonymous transactions.
References


