User-Perceived Privacy in Blockchain

Simin Ghesmati[1,2], Walid Fdhila[2,3], and Edgar Weippl[2,3]

[1] Vienna University of Technology, Vienna, Austria
[2] University of Vienna, Vienna, Austria
[3] SBA research, Vienna, Austria
(firstletterfirstname)(lastname)@sba-research.org,

Abstract. This paper studies users' privacy perceptions of UTXO-based blockchains such as Bitcoin. In particular, it elaborates – based on interviews and questionnaires – on a mental model of employing privacy-preserving techniques for blockchain transactions. Furthermore, it evaluates users' awareness of blockchain privacy issues and examines their preferences towards existing privacy-enhancing solutions, i.e., add-on techniques to Bitcoin versus built-in techniques in privacy coins. Using Bitcoin as an example, we shed light on existing discrepancies between users' privacy perceptions and preferences as well as current implementations.

Keywords: blockchain · privacy · anonymity · Bitcoin · mixing · wallets.

1 Introduction

Blockchain is a disruptive technology that offers innovative solutions for distributed and secure transactions. By relying on a P2P network, blockchain technology offers the compelling properties necessary to develop new forms of distributed applications. However, despite the significant amount of research to address the challenges posed by such a new technology, several privacy and security issues remained partially unresolved. In particular, in a public blockchain where details about transactions are publicly available (e.g., senders' and receivers' addresses as well as transaction amounts), it becomes possible for an adversary to use such data in combination with heuristics and auxiliary information (e.g., address tags) to cluster and identify users and their transactions, and eventually, linking Bitcoin addresses to real identities [4, 10, 44, 55]. For example, common input ownership, change addresses detection, address reuse, side-channel attacks, tagging addressee by auxiliary information from the Internet, transaction graph are some of the most prominent techniques [6, 36] used for de-anonymization in the Bitcoin blockchain [4]. To overcome such privacy challenges, several solutions have been proposed, which provide users with mechanisms and techniques to hide their transactional data and preserve their anonymity. This includes i) add-on techniques that can be used on top of existing blockchain solutions such as

[4] See Appendix B for an explanation of de-anonymization as well as privacy-preserving techniques. Related works are also discussed in Appendix C

Bitcoin (e.g., mixing techniques such as CoinJoin), or ii) blockchain solutions with built-in privacy features such as privacy coins (e.g., Zcash or Monero).

Our research seeks to unravel the difference between users' expectations and the current implementation of such privacy solutions, raising intriguing questions regarding the effectiveness of proposed techniques when adopted in practice.
RQ 1: To what extent are users aware of privacy issues and privacy-enhancing technologies?
RQ 2: What preferences do the users have for privacy-enhancing technologies?
i. Do they prefer using add-on privacy techniques on top of Bitcoin or built-in features in privacy coins (e.g., Monero)?
ii. Are they willing to use privacy-preserving techniques despite the higher fees and longer transaction time?
iii. Do they trust third-party privacy-preserving services?
iv. Which privacy features interest users the most (e.g., hiding the source, hiding the destination, hiding the amount)?

The paper is structured as follows: In Section 2, we describe our quantitative and qualitative study, while in Section 3, we present the results and discussion. Finally Section 4 concludes the paper.

2 Study Design

We present both a qualitative and a quantitative evaluation of users' perception of privacy in UTXO-based blockchains such as Bitcoin.

2.1 Qualitative Research

Methodology In this subsection, we explain designing the questionnaire and the interview procedure. Recruitment, the coding methodology, limitation, and sampling are provided in Appendix D.1. For the questions, we conducted multiple rounds of pilot interviews and -discussions, including collecting the answers to the questionnaire in a Blockchain workshop with eleven participants, a think-aloud study with four blockchain experts, and consulting security- and privacy usability experts, a legal expert, and an English proofreader. We revised the questions to ensure that technical terms and questions were clear. The procedure for designing the questionnaire is illustrated in Figure E.1.

Interview Procedure Before the interview, participants were briefly informed about the research context and signed a consent form. Each interview lasted about 30 minutes. We conducted semi-structured interviews both in-person and via online meetings. The researchers used an interview guide with open-ended questions (Appendix A) to ensure consistency. The questions were revised and validated in two pilot rounds. All interviews were recorded and anonymized, and fully transcribed.

2.2 Quantitative Research

Methodology We conducted quantitative research to get a larger and geographically more distributed set of participants for the study. We hosted a survey on SurveyMonkey. The follow-up questions in the questionnaire were shown

according to the logic set to the answers. The overall logic is illustrated in Figure E.2. For the reliability of the answers, in the quantitative part, we did not show the questions regarding Bitcoin privacy attacks and privacy-enhancing solutions if the respondents selected Bitcoin is fully anonymous. Those respondents were redirected to questions specific to privacy unaware users. Additionally, those unaware respondents were informed about privacy issues and privacy-enhancing tools in Bitcoin and were asked if they value having better privacy despite the extra fees or longer transaction times. Sampling and ethical considerations are provided in Appendix D.2.

2.3 Validity and Reliability

In total, 101 participants took part in our survey in the quantitative part. After applying our exclusion criteria, we reached a final sample of n = 58 for our analysis. Interviews with non-users with absolute no knowledge about cryptocurrencies were omitted from the study. Our final dataset includes responses from 12 participants (cryptocurrency users) in the qualitative part and 58 participants in the quantitative part. We asked the respondents to specify if they studied or worked in an IT-related field in the demographic part. This was the case for 58.33% of the participants in the qualitative part and 65.52% of the respondents in the quantitative part. The questionnaire was distributed in English. Adding the "other" option allowed us to have unassisted answers. Re-submission was prevented by restricting one submission per device and IP. The respondents were not allowed to change their responses to the previous questions. We followed [39], and to ensure the reliability of the dataset, five exclusion criteria were considered:

- No knowledge of cryptocurrencies. 8 respondents who selected "not at all familiar" with cryptocurrencies were eliminated.
- Who partially replied to the questionnaire. 27 respondents were eliminated.
- Who wrongly answered the quality control question with shuffled options (they should select "Homophonic substitution cipher in one of the questions"). 7 respondents were eliminated.
- Who selected invalid answers (if they chose fake options in two questions, Dram, a fiat currency as a privacy coin, and MyMaps, a map application as a Bitcoin wallet), 1 participant, who selected invalid answers to two questions was eliminated.
- Who failed to successfully re-phrase the earlier questions (they should write their roles in an open-ended question, while they selected their roles in the earlier questions). None of the participants who passed the above criteria was eliminated by this criterion.

3 Results

3.1 Privacy Awareness

The Importance of Privacy in Transactions Half of the interviewees (PU1, PU2, PU4, PU7, PU10, PU11) specified that transaction privacy is very important to them. PU1 stated that "*Blockchain transparency creates a guard*

for some people to accept it as a monetary system. If you ask me to shift all of my traditional transactions to the blockchain, I would have a serious guard against that". PU2 and PU4 specified their expectations on being anonymous in blockchain transactions. PU2 said, "*I expect no one realizes my identity although everyone can see the transaction* [on the blockchain]", and PU4 specified "*I don't like anyone knowing my financial transactions either in traditional or crypto. It's completely a private thing.*"

PU11 said, "*anonymity in crypto transactions is useful when you want to be hidden from your government's eyes*". They stated that it is useful when the law prevents you from using new technologies while you are not working on the darknet or are not pursuing illicit activities.

While PU3, PU6, and PU9 considered the privacy of transactions at an intermediate level of importance. PU6 pointed out that "*on the one hand when I could pay by crypto rather than traditional systems to buy services or transfer money without specifying my identity, it's totally great. On the other hand, this anonymity makes it quite difficult to find a hacker who steals your crypto; you will lose it forever* [and you cannot find him], *it depends on who can know it. If they are my relatives or friends, it's a matter, but if it is the government, it's OK*". PU5 and PU12 asserted the privacy of transactions is not important to them. PU5 referred to his low investment in cryptocurrencies stating that "*at the moment my investment is too low, that's why the privacy is not that much important for me; however, I don't want anyone to know it as I'm afraid of future laws on taxing the crypto transactions or if the government bans the crypto transactions.*" In contrast, PU12 stated that privacy is important for those who do money laundering, "*I do not perform anything special or illegal, the privacy does not matter to me.* PU8 specified privacy is not important at all, although their answers to the following questions expressed privacy concerns. When asked about their contradicting answers to the following questions, they replied by "*privacy is not important at all to me as nothing happens if this information is disclosed, however, I prefer it not to be [disclosed]*".

QNT.[5] Most of the participants said that the anonymity of cryptocurrency transactions is extremely important (46.55%) or very important (24.14%), while a minority considered it less important (Somewhat important: 22.41%, Not so important: 5.17%, Not at all important:1.72%).

Bitcoin Anonymity While most of the interviewees categorized Bitcoin as not so anonymous (PU1, PU3, and PU8) or with moderate anonymity (PU4, PU9, PU7, and PU1), four out of twelve stated Bitcoin anonymity is high (PU5) or very high (PU6, PU11, and PU12).

PU1 and PU7 stated that the peer with whom they transacted knew them. PU2 and PU7 stated that it is not at all anonymous outside the network, but its anonymity is great at the Bitcoin network level. PU1 and PU3 mentioned privacy issues as a result of monitoring tools. PU1 explained "*transaction transparency makes it* [Bitcoin] *not so anonymous. There are monitoring tools, e.g. Crystal, that analyzes the network. I would say it is more transparent compared*

[5] We specified quantitative results by starting with **QNT** abbreviation.

to traditional banking systems." PU3 notified monitoring tools such as Cipher Trace and suggested that "*Bitcoin should find a solution for this issue, no idea if it should be handled by wallets! It's better not to use Bitcoin if you want to perform anonymous transactions; I'd suggest Monero or Zcash instead.*" PU8 and PU9 were also aware of the algorithms to find the relationship between accounts and tracing transactions. PU9 elaborated, "*it is possible to trace a specific transaction and recognize how it was funded, for instance in which exchange.*" PU8 also specified the privacy issues regarding wallets where "*the information about your e-mail, your mobile phone, your phone number are recognized.*" PU8 considered the wallets as mobile or web wallets, and their answers applied to the specific wallets that they experienced before. While, software wallets on desktop computers neither ask for e-mail nor can connect to mobile SIM cards. They also were unaware that full node wallets do not suffer from these privacy issues.

Some of the interviewees (PU2, PU4, PU5, PU7, and PU8 mentioned anonymity issues using exchanges or services accepting Bitcoin. PU2 mentioned, "*no anonymity in [using] exchanges*". However, the privacy issues with exchanges matter when users use centralized exchanges with know-your-customer (KYC). In this question, those interviewees did not mention decentralized exchanges, which do not ask for KYC. PU5 also stated the privacy issues with centralized exchanges where KYC applies; however, they believed "*Bitcoin is still more anonymous than traditional banking.*" PU4 stated that "*although users do not know the entities behind the addresses, the stories where police could find criminals who used Bitcoin indicates the possibility of tracing the transactions.*"

PU10 had a level of uncertainty about Bitcoin anonymity as they said, "*I've just heard Bitcoin anonymity is less than other cryptocurrencies, I'm not sure.*" Among those who considered Bitcoin anonymity very high. PU6 referred to the fact that "*the users don't know to whom the public key belongs, it's an alphanumeric phrase and all the identities are hidden in the network*". They were confident that no one could find the users who perform Bitcoin transactions as they had heard about the story of the Silk Road [marketplace] developer. They thought the Police had to investigate through sophisticated ways to find him, and the reason was using TOR and Bitcoin payment in designing the system. This caused a misconception that the user was unaware of the possibility of de-anonymization techniques applied in Bitcoin to map the addresses to real identities. PU11 and PU12 wrongly considered Bitcoin is fully anonymous since it uses addresses rather than real identities. PU11 has a misconception about privacy as they thought Bitcoin is based on encryption algorithms which makes it anonymous; they also referred to the fact that "*Bitcoin does not record identities in its blockchain.*" They stated, "*you can transfer coins from a wallet which is not recognized by an identity, you don't know the recipient, and the recipient does not know who the sender is.*"

QNT. The respondents reported Bitcoin anonymity as: Not at all anonymous: 15.52%, Not so anonymous: 27.59%, Somewhat anonymous: 36.21%, Very anonymous: 18.97%, Extremely anonymous:1.72%). One of the users who selected Bitcoin as extremely anonymous jumped into privacy unaware users' ques-

tion. We asked the unaware users why they believe Bitcoin is fully anonymous. This participant selected "there are no real identities in the transactions (neither names nor personally identifiable information (PII))."

Privacy Risks The reported risks varied among the interviewees. PU1, PU2, and PU3 specified monitoring tools. PU2, PU5, and PU8 mentioned [Centralized] exchanges and exchange hacks. PU3 and PU8 pointed out address reuse. PU5 reported possession of private keys by web wallets. PU5 and PU8 specified Bitcoin explorers; however, PU8 used that under the name "*crypto scanner*" and according to their explanation, we found that they meant what is known as "explorers". PU4 mentioned tracing transactions by, e.g. police.

PU2 stated, "*exchanges know the history of my transactions, and they are not secure; therefore, they can compromise my privacy. I bought or sold my crypto via the exchanges,* [thus,] *my identity can be identified, [and] along with tracking systems they can identify my behaviors.*" PU3 mentioned if the address is reused, it could be traced to find the source of other transactions. PU5 pointed out, "*if the exchanges are hacked, the hacker can find to whom these cryptocurrencies belong.* [Furthermore] *Web wallets such as Blockchain.com have your private key. So, they can access your assets*", by this, the interviewee meant the corrupted web wallet can spend money on behalf of users, compromising their privacy where it is interpreted that the user got involved in that transaction.

PU8 considered that privacy risks are only related to the wallets and exchanges "*as long as you are not trading and the wallet you are using are not related to you, privacy is OK. Privacy attacks are only implemented in academic papers; I haven't seen any implementation in practice.*" The participant was unaware of current monitoring tools and companies who are working in this context as their businesses. That is why they thought privacy attacks were not implemented in practice and are just proposed in the academic papers. Some of the interviewees (PU6, PU9, PU10, PU11, PU12) could not specify any privacy risks associated with Bitcoin. PU12 stated, "*I haven't heard it because the people around me haven't talked about it.*"

QNT. We provided an open-ended question to evaluate user awareness about privacy risks. The majority of participants (68.96%) stated Bitcoin risks they are aware. Among them, three participants misstated "losing money" and "password hack" as privacy risks. "Centralized exchanges (KYC)", "identity identification", "creating transaction graphs", "public and immutable database" were the most reported privacy risks.

Privacy Risk Measures We present different measures stated by users who answered the previous question. PU2 and PU3 suggested using various platforms and wallets, using Decentralized Finance (DeFi), decentralized exchanges. PU3 also proposed to not directly transfer from personal wallets to other addresses, using mixing, using TOR or VPN, using privacy coins such as Zcash or Monero. PU3 specified that "*monitoring systems are improved every year; thus, I may switch to Monero and Zcash if I want to be anonymous. They developed for this reason and I'm so confident using them for this purpose.*" PU2 proposed to use DeFi, where it is not required to disclose identities. But they mentioned that

"*they have higher risks, your wallet or your assets can be easily stolen* [in these non-prominent decentralized exchanges], *therefore, it is better to scatter your assets between different platforms if you have a large amount of money.*"

PU8 mentioned not using exchanges and trying to use wallets that require less identity information; however, as it was mentioned in the previous section, this was due to the unawareness of the participant from decentralized exchanges and desktop/full node wallets. PU5 mentioned that they did not apply any measures to mitigate privacy risks as they have not invested much in the market.

Awareness of De-anonymization Techniques Three out of twelve (PU1, PU2, and PU3) were aware of how monitoring tools flag the transactions; however, they did not know the algorithms and the techniques that the monitoring tools applied to flag the transactions and find suspicious transactions.

PU1 asserted, "*they* [monitoring tools] *find the suspicious transactions from for example gambling websites. They try to find transactions suspicious of money laundering. They find the suspicious UTXO and trace the UTXO to find the user or the exchange that the UTXO has been sent.*" PU2 specified "*they try to find mixers or ransom by finding different wallets. They can at least find a set of wallets belonging to a criminal group.*" PU3 mentioned, "*if they* [monitoring tools] *collaborate with some explorers they can also tag the transaction with the IP of the user who checked the transaction confirmation." They also clarified how the address reuse can be used to relate the transactions to each other.*" PU8 notified the issues with address reuse and the patterns achieved from the transactions with the same amounts. PU5 stated the transaction graphs. HOwever, more than half of the interviewees (PU4, PU6, PU7, PU9, PU10, PU11, and PU12) did not mention any techniques.

QNT. Address reuse 73.68% was the most reported de-anonymization technique that the participants were aware. More than half of the participants (64.91%) said that they are aware of tagging addresses through the information available on the Internet. Transaction graphs with 57.89% and change address detection with 54.39% ranked in the successive positions. In contrast, one-tenth was unaware of any techniques.

Awareness of Correlation Attacks PU1 and PU2 have heard about the correlation attacks, but they had no information about them. PU3 was aware of IP address mapping to the addresses and finding access patterns as network correlation. They also mentioned, "*it is better to be a full node rather than connecting to third party wallets.*" PU4 specified the time and amount correlation by services that users pay with Bitcoin, for instance, online shops; therefore, the service is able to provide the information regarding the identity of the users to map to the user's transaction. They also mentioned that "*it highly depends on privacy provided by the service.*" More than half of the interviewees (PU5, PU6, PU7, PU9, PU10, PU11, and PU12) were unaware of the correlation attacks.

QNT. 60% reported that they are aware of network, time, and amount correlation attacks, while 15.79% were unaware of any correlation attacks.

Awareness of Add-on Techniques While most of the interviewees (PU4, PU5, PU6, PU7, PU8, PU10, PU11, and PU12) were unaware of the add-on

techniques. PU1 was aware of mixers, "*I know they collect all the transactions from one side and randomly send them to another side to obfuscate the relationships* [between inputs and outputs]". By collecting transactions from one side, they probably meant the inputs. They also specified that they have heard of CoinJoin and CoinSwap but did not know how they work. They mentioned, "*analyzers can find CoinJoin transactions and flag them... I'm not convinced that CoinJoin can provide better privacy.*" PU3 was aware of mixers and CoinJoin, and they mentioned that "*we can also use exchanges as mixers.*" PU9 has seen CoinJoin and CoinSwap names, but they have not read about them.

QNT. Mixing websites (66.67%) were the popular add-on technique that the participants were aware. The participants' awareness of other techniques was reported as follows: CoinJoin-based techniques (49.12%), threshold signatures (43.86%), off-chain solutions (42.11%), and Fairexchange /Coinswap (31.58%). 17.54% were unaware of any of the techniques. Figure E.5 illustrates the awareness of add-on techniques.

Awareness and Usage of Privacy Coins Except for PU1, PU2, PU3, PU5, and PU8 who were aware of some of the privacy coins, others neither heard of them nor were aware that these coins were developed for privacy reasons. PU1 and PU2 have heard about Monero, but they did not know how it works. PU2 specified "*I just knew that Monero was developed specifically for this* [privacy]." PU1 stated, "*I just wanted to buy one of the privacy coins, just according to the market analysis, however, I didn't.*" PU3 was aware of Zcash and Monero, and they were the only one who owned Monero through the mining. "*I read a paper about Monero and* [I found that] *it could better implement privacy. . . .I also tested its mining as its mining was quite easy at that time.*" PU5 was aware of Monero as a privacy coin that provides strong anonymity. They also have heard of Zcash and Decred, but they were unaware that they are developed as privacy coins. PU8 specified that they know Zcash, "*... it uses Zero-knowledge proof to verify transactions, but I don't know how its transactions look like.*"

PU9 has heard there are some privacy coins in the market, but they could not remember their names. PU7, PU10, and PU11 have heard of the name of Zcash or Monero, but they were unaware they are privacy coins. PU4, PU6, and PU12 were unaware of privacy coins.

QNT. Monero (78.95%) and Zcash (70.18%) were the most prominent privacy coins that the participants were aware. Figure E.6 outlines the awareness of privacy coins. Monero and Zcash were the top coins that have been owned /bought /mined by the participants. Most of the participants selected, they owned privacy coins both for better anonymity and investment.

3.2 Privacy Preferences

Preference Between Bitcoin Add-on Techniques and Privacy Coins

Most of the interviewees (PU1, PU3, PU4, PU7, PU8, PU10, PU11, PU12) preferred privacy coins rather than Bitcoin to enhance their anonymity in cryptocurrency transactions. The reason for preferring privacy coins rather than Bitcoin add-on techniques varied from the better privacy in built-in techniques

to not getting involved in the adversity of using add-on techniques or relying on third-party services. PU1 specified the fear of making the transactions suspicious by using CoinJoin and CoinSwap. They were informed about the possibility of flagging CoinJoin transactions; however, at the time of writing, monitoring tools did not recognize CoinSwap transactions. They are similar to hash-time-locked contracts (HTLC) that are mostly used in payment channel funding transactions. The participant may be afraid of other add-on techniques being flagged by monitoring tools. PU3 specified that "*if privacy is the priority, I'll definitely prefer Monero. I don't like to do a tough task to improve privacy in Bitcoin. Monero has been developed exactly for this* [providing privacy], *its algorithms, its network... The only situation that forces me to perform a transaction* [where I need privacy] *with Bitcoin is when the destination does not support Monero and I have to pay in Bitcoin.*" They continued that in privacy coins, the developers thought about the privacy concerns, and they can rely on that, "*it does not get me in trouble of using add-on techniques.*"

PU9 preferred to use Bitcoin add-on techniques as they were more familiar with Bitcoin. PU2 and PU5 had different opinions; they preferred neither add-on nor privacy coins. PU2 did not desire to use privacy coins as they thought this anonymity is against the goal of using cryptocurrencies in real life. PU2 clarified their opinion by being against privacy coins with "*they* [privacy coins] *don't have any applications in real life, they are used either for illegal activities or investment, so they don't attract me*". They preferred to use Bitcoin as *"Bitcoin is the market leader. If it goes up, consequently, other coins go up. It's easily exchanged."* They also mentioned the problem with changing Monero in the exchanges "*Monero is not listed in most of the authorized exchanges, it may be listed in some unknown exchanges and it's risky to use those exchanges. At the moment, there are lots of risks* [in the crypto market]... *I can't add more risks.*" PU5 preferred using DeFi to provide better privacy rather than add-on techniques in Bitcoin or privacy coins. They noted that "*decentralized exchanges provide privacy in the level of trading, they went one step ahead of privacy coins.*" PU6 also preferred security rather than privacy. They mentioned that if the privacy-enhancing technology endangers security, they preferred not to use them.

QNT. More than half of the participants (63.16%) preferred using privacy coins rather than Bitcoin add-on techniques. Mandatory built-in privacy (91.67%) and stronger anonymity (83.33%) when the technique is considered in design were among the highest reasons for preferring privacy coins. Among those who preferred Bitcoin add-on techniques, Bitcoin's reputation (85.71%) and availability of Bitcoin tools (wallets, explorers, etc.) (71.43%), and Bitcoin market cap (71.43%) were the most selected options.

Preferences Between Bitcoin Built-in and Add-on Privacy Techniques More than half of the interviewees (PU4, PU7, PU8, PU9, PU10, PU11, and PU12) preferred applying mandatory built-in techniques in Bitcoin protocol, while PU1 and PU3 preferred using add-on techniques whenever they needed better privacy. PU2 preferred not to answer this question as they were not knowl-

edgeable in this context. PU5 suggested not to use Bitcoin for privacy reasons as it still requires improvement in too many other aspects.

PU1 and PU3 pointed out the negative consequence of applying mandatory built-in privacy techniques in Bitcoin. PU1 stated, "*I am afraid of bans by governments or exchanges once built-in techniques apply to the Bitcoin protocol*". PU3 continued, "*it's a difficult question, as it has personal benefit and public benefit, ... better not to implement mandatory privacy techniques in Bitcoin, there are dark web activities.... and we need some sort of monitoring in Bitcoin since it is the main cryptocurrency.*" For those who preferred using built-in techniques, PU4 referred to the HTTPS story, which became popular after HTTP, and they said, "*in future, we will reach the point that we have to consider privacy aspects in Bitcoin.*" PU9 explained their reason by "*if it* [built-in technique] *introduces a new risk. The risk would be for all the users* [while in add-on techniques it would be for those who use add-ons]." PU10, PU11, and PU12 had better feelings by using built-in techniques rather than add-on techniques.

QNT. While half of the participants preferred applying mandatory built-in privacy techniques in Bitcoin, 29.82% did not know, 12.28% preferred add-on techniques, and 8.77% had other opinions such as being too late to change Bitcoin or doubt about applying built-in privacy in Bitcoin. One of the participants also pointed out that this would cause a "complete crash of that ecosystem, bankruptcy for the grifters."

Preferred Privacy Features in Bitcoin We asked the interviewees to specify their preferred features of Bitcoin. We also provided them the options (hiding the source, destination, or amount) if they had no statements. Except for one interviewee (PU6) who was unaware of the probability of mapping the addresses to the real identities by stating that "*in my opinion, it is not important that the source and destination addresses are not hidden. They are not related to real identities.*", other interviewees prioritized hiding the source while they preferred hiding the amount, and hiding the destination, for better privacy.

Some of the interviewees added some other features. PU2, PU3, and PU5 mentioned to prevent mapping the addresses to the real identities while they knew that it is not related to the Bitcoin protocol. PU9 specified this feature; however, they did not mention that it is not specifically related to the Bitcoin protocol. PU5 continued *"I also don't like Bitcoin explorers where they trace the transactions, they can find and publicly show from which address to which address the coins have been transferred, and if one of the transactions can be mapped to my real identity other transactions can be revealed.*" PU8 also specified to make it impossible to create transaction graphs. PU2 suggested preventing the wallet from accessing one's mobile data (e-mail, location) in mobile wallets. Not to store IP addresses, and not to get informed which device is connected to the wallet, also suggested by PU2.

QNT. Hiding the source of the transaction (70.18%), hiding the amount (70.18%), and hiding the destination (63.16%) were selected, respectively.

Accepting Extra Fees Half of the interviewees (PU1, PU3, PU7, PU8, PU10, PU11) accepted paying extra fees for privacy, while the other half were not

willing to do so. We asked those who accepted to pay for privacy to specify the fees in a transaction worth $1000, and $31.25 was the acceptable fee on average.

PU1 and PU3 specified that they pay to the technique that they are confident about the level of privacy that can be achieved. PU1 noted that "*if it is, for instance, a special signature,* [which can provide better privacy] *yes, roughly $15-$16, but I never pay to mixers or CoinJoin technique.*" PU3 pointed out the high transaction fees in Bitcoin and its dependency on the size of the transaction. They agreed to pay $50. PU7 and PU10 also said they will pay 5% ($50). PU8 agreed on paying up to 10% of the transaction fee (which relates to the transaction size, therefore, we can not precisely estimate the fees in dollars), and PU11 stated they would pay 2% ($20).

PU4, PU6, and PU9 specified that the current Bitcoin privacy meets their expectations, and they would not pay extra for privacy. Others thought paying for privacy is for famous people, criminals, or those who invested lots of money in the crypto market. PU12 asserted, "*I am not a politician, I am not a big business person who wants to run away from taxes. I have no reason to be anonymous, so I prefer to pay lower fees and be non-anonymous.*" PU5 stated, "*I don't have much money in the crypto market to pay extra fees for its privacy, however, if I had, I wouldn't pay more than a dollar.*"

QNT. While almost half of the participants accepted to pay extra fees for better privacy (53.45%), 32.76% did not accept, and 13.79% did not know. Those who accepted to pay extra fees paid on average $18.13 for a transaction worth $1000 (max. = 200, min. = 0.1, median.=10). Those who did not accept to pay extra fees selected "current Bitcoin transaction fees are too high", "current level of Bitcoin privacy meets my expectation", "the volume of my investment in the crypto market is too low" as their reasons. Others specified that it would be a paywall for user privacy, or the privacy should be provided by default in a system not asking for more fees to offer it. The others preferred not to use Bitcoin, which is why they did not accept paying extra fees.

Accepting Extra Delays All of the interviewees (except PU6) accepted waiting longer for better privacy. We then asked those who accepted the delays to specify the time they could tolerate. PU1 agreed on less than a day. PU2 referred to the Bitcoin transaction confirmation time, which is too long at the moment. They continued that "*if I know the other party beforehand, let's say 1 to 2 days. If not, I prefer being non-anonymous rather than putting myself at such a risk... the price of Bitcoin changes a lot, and waiting for more than a day sounds unreasonable.*" PU4 noted that "*it highly depends on the recipient whether he accepts it or not, it also depends on the importance of that transaction for me, then I would say 4 to 5 hours.*" PU3, PU10, and PU12 stated 1 to 3 hours, 1 to 2 hours, and less than an hour, respectively. PU7 and PU9 could tolerate less than 30 minutes, while PU5 and PU8 stated less than 10 minutes, and PU11 could only tolerate if the delay was less than a minute. PU5 stated that "*nowadays, Bitcoin is considered as an asset rather than a currency for buying or selling* [products or services], *therefore, time is not that much important in Bitcoin... it's not that bad to tolerate extra delays for better privacy; 10 minutes would be tolerable.*"

PU6 was against extra delays; they noted that "*Bitcoin is a slow network compared to other networks. It's not interesting to make it even slower.*"

QNT. Accepting extra delays varied among the participants (22.41% less than a minute, 29.31% less than an hour, 15.52% less than a day, 5.17% less than a week, and 5.17% less than a month). In total, 77.58% accepted extra delays; Those who did not accept the delays (13.79%) referred to the delays in Bitcoin confirmation or preferring not to use Bitcoin as a privacy option.

3.3 Privacy Wallets

Awareness and Usage of Privacy Wallets Except for PU3, none of the interviewees were aware of Bitcoin privacy wallets. PU3 has heard of Samourai in a forum; they were also aware of Joinmarket, but they have not used them. They told us, "*it is better to perform ordinary transactions rather than CoinJoin transactions and being flagged by monitoring tools.*" PU8 was unaware of de-anonymization heuristics and add-on techniques such as CoinJoin or mixers; therefore, they thought the privacy wallets are the wallets that create a fresh address for each of the transactions (although this feature is also provided by privacy wallets, they are not the only option), their belief related to their misconception that "*the only way you can have privacy in Bitcoin network is to create a new address for* [each of your] *transactions.*"

QNT. Wasabi and Samourai were the most prominent privacy wallets among the participants. Figure E.7 indicates the awareness of the privacy wallets. 43.86% of the participants were unaware of privacy wallets.

Most wallets have not been used. Wasabi with 28.13% and Samourai with 12.50% were among the top ones. 9.38% also reported using JoinMarket wallet. The satisfaction of using the privacy wallet is demonstrated in Table E.2. We asked the wallet users to scale their satisfactions on a five Likert scale ("extremely satisfied" to "not at all satisfied"). 6 out of 9 were very satisfied with Wasabi, 3 out of 4 were very satisfied with Samourai, and 1 out of 3 was very satisfied with Joinmarket. 2 out of 9 and 2 out of 3 were somewhat satisfied with Wasabi and Joinmarket, respectively. While 1 out of 9 and 1 out of 4 reported being not at all satisfied with Wasabi and Samourai.

Trusting Third-party Wallets Except for PU8, who did not trust the wallets, other interviewees argued about which wallets they could trust. PU12 had no answer for the question as they were not familiar with the subject of privacy.

PU1, PU2, and PU3 mentioned being open-source as one of the items. PU1 continued that "*if the code is available on Github and can be checked, it gives me a sense of security.*" PU2, PU3, PU4, PU6, and PU7 pointed out being approved by a reliable person. PU3 clarified that "*I can rely on the reviews of the reliable experts with a good experience and background in this context.*" PU5 and PU10 pointed to the wallet reputation and the number of users; however, PU10 did not prefer to use third-party wallets. PU4 added recommendations by trusted websites. PU6 and PU7 also referred to users' reviews about the wallet. PU7 also pointed to the number of downloads. PU9 and PU11 specified they should first research to know the wallet. PU11 specified related papers and forums where they could check if the wallet's security and privacy have been approved.

PU8 explained that "*we cannot even trust hardware wallets, how can we trust software wallets. We don't know* [the technology] *behind them. How you can know the code behind them to trust. I cannot trust them, as I don't know the codes and mechanisms behind them.*" The interviewee did not know or did not specify the open-source code where the code can be checked. They exaggerated the untruthfulness of the wallets; they thought there is no way to check the technology and code behind the wallets. We asked them how they perform their transactions while they do not trust any wallets, and they replied, "*I have to do that as I don't have any alternatives. Therefore, I accept its risk.*"

QNT. More than half of the participants (55.17%) asserted they trust the privacy wallet if it is open-source and the code can be checked. In contrast, 22.41% stated that they do not trust third-party services. Trusting information available in forums or provided by friends was selected with the same rate (8.62%). 3.45% did not have any answer to the question. The participant who selected "other" mentioned the importance of "*surviving over a long period.*"

3.4 Discussion

Privacy Awareness In both quantitative and qualitative results, the majority of the users highlighted the importance of privacy. The numbers show that more people are now aware of Bitcoin anonymity compared to similar previous studies [31, 11]. The interviewees who considered Bitcoin is fully anonymous were asked questions about privacy attacks and respective solutions in Bitcoin. Most of them said that they never heard about these privacy issues, but if they knew about them, they would have researched possible solutions to mitigate them. While address reuse and auxiliary information (obtained from exchanges or services) have increased the attention among our participants in the quantitative part, most of the respondents were unaware of the most prominent heuristic in the de-anonymization techniques, namely common input ownership.

We noted that some of the participants in the qualitative study did not know the difference between custodial (e.g., exchanges) and non-custodial wallets. They were either unaware or did not care about the risks of using centralized exchanges to manage their coins. Although some of them were aware of past security hacks to well-renowned exchanges (e.g., Mt. Gox [53], Bitstamp [9], Binance [54]), they continued to use them. Taking this risk is mainly motivated by the ease of using such traditional systems to manage their funds against the complexity of managing the cryptographic keys by themselves. Indeed, recovering lost credentials for accessing exchanges is much easier than recovering cryptographic keys in such a distributed system, especially if no recovery mechanisms or tools are employed. Some participants still use exchanges because they were either actively trading or preferred to be able to react fast when they wanted to trade. Some participants realize the privacy concerns of relying on a custodial wallet (e.g., the exchange may require KYC and is also able to correlate transactions), others did not think about it or were unaware of such privacy issues.

Some participants assumed that blockchain is safe from a privacy perspective as they use addresses rather than real identities. Others considered privacy persevering tools/coins are most likely to be used by criminals or for tax evasion.

Both groups refrain from applying privacy-enhancing measures or tools. While privacy misconceptions about encryption of data on blockchain found by [33], our study supports this as there exist participants who had a similar belief that the blockchain uses encryption, the data is safely stored, and there is no way to trace the users on the blockchain. [33] suggested showing a notification to users through their wallets to inform them that the transaction will be publicly available in the network. Wallets are in a good position to educate the users regarding privacy by providing notifications or features. One feature that is applied by some wallets [28, 51, 45] are preventing users from address reuse. The wallets can notify users to prevent reusing the address once the address is created. The wallets can also remove the address and create a new one, once the address gets funded. Indexing the address is another measure to increase users' attention on preventing address reuse.

Most of the participants in the qualitative study were unaware of the add-on techniques (for improving privacy on Bitcoin) or existing privacy-by-design blockchains. In the quantitative study, mixing websites were more popular, while other techniques were selected by less than half of the participants. Even if we consider biased answers among the participants, more than half are still unaware of privacy-enhancing techniques in Bitcoin. A previous study [11] showed that coin mixing services are a popular measure to improve privacy and that more than half of participants were unaware of CoinJoin and ZeroCoin (now called Zcash). Our study considers additional add-on techniques and privacy coins. However, in the quantitative part, more than two-third of participants were aware of Monero and Zcash 78.95% and 70.18%, respectively.

Most participants have little to no understanding of privacy-enhancing techniques, neither how to use them nor the mechanism behind them, even if they have heard about them. They did not understand what kind of data these privacy techniques can hide. Some participants think that the privacy-enhancing techniques are too technical for novice users who only use cryptocurrencies for trading and investment purposes. Therefore, a negative understanding of using privacy tools (such as using them for criminal activities or tax evasion) as well as how blockchain public can be used for malicious actions needs to be educated either (i) through integration with wallets by providing meaningful notification and privacy features (e.g., generating a fresh address), or (ii) through documentation and social media.

Note that a distinction should be made between public privacy and private privacy. While in the former, the information publicly available on the blockchain is visible to everyone. In private privacy, the data is not public but solely available to governments, exchanges, or wallets. For formal research on collaborative deanonymization to achieve private privacy, the reader may refer to [30].

Privacy Preferences While more than half of the participants preferred to use privacy coins, most of those who chose to use add-on techniques on top of Bitcoin if needed, expected future built-in privacy improvements to Bitcoin. Although this does not seem realistic in the near future, it is instead implemented by wallets or layer two solutions. According to our study, users are willing to accept

longer transaction times to achieve better privacy, while half of them dismissed the idea of paying extra fees. Half of the participants were fine with paying extra fees. The interesting aspect here is that most current privacy solutions for Bitcoin (CoinJoin, CoinSwap) require more than one transaction fee, where additional transaction fees should be paid by users. Indeed, multiple CoinJoin rounds may be necessary to achieve adequate privacy. This entails additional transaction fees and consequently higher overall fees. Considering the high Bitcoin transaction fees at the time of writing, using privacy solutions seems relatively expensive. Therefore, privacy solutions should be implemented in a way that requires fewer fees, as it is unlikely that users will pay additional transaction fees for transactions with less value. Users who were aware of the distinguishability of CoinJoin transactions with the same output amount were not willing to use it. Instead, they favored alternative techniques that preserve indistinguishability, where the transactions cannot be flagged by monitoring tools. PayJoin, Wabisabi (Wasabi 2.0) [13], threshold signatures, and CoinSwap techniques can provide some level of indistinguishability; however, they have not been widely adopted in practice yet. The possibility of PayJoin transactions being flagged with unnecessary input heuristics has been investigated in [18].

Privacy Wallets Although their development started around 2015, privacy wallets still struggle to attract more users. Indeed, such wallets are complex and require a minimum understanding of privacy concepts and techniques [17]. On the one hand, current Bitcoin privacy wallets implemented CoinJoin with the same output amount suffer from distinguishability in the blockchain; on the other hand, the newly implemented indistinguishable techniques such as Wabisabi and PayJoin may be banned by governments. This would be a severe problem for the respective wallet developers and users. In the interviews, we found that users prefer to use wallets that support different coins; thus, we can not expect users to install different wallets for different coins and, even worse, install additional wallets for their privacy, as well as having to spend time to learn the wallet functions.

4 Conclusion

In this paper, we conducted a study on user perception and preference on Bitcoin privacy. We investigated different add-on privacy techniques in Bitcoin as well as their implementation in practice. We showed the difference between users' preferences and the implementation of privacy techniques in practice. Interestingly, most users preferred privacy coins rather than add-on techniques in Bitcoin. Our results show that participants are more likely to accept delays rather than extra fees to achieve anonymity in Bitcoin. The participants also preferred indistinguishable privacy techniques rather than being flagged by monitoring tools. Therefore, important questions are raised as current privacy wallets offer CoinJoin transactions with equal-sized output that are distinguishable in the blockchain. Overall, we show that users who prefer better privacy are not likely to use Bitcoin, and they favor embedding built-in privacy features in Bitcoin.

Acknowledgments

This research is based upon work partially supported by (1) SBA Research (SBA-K1); SBA Research is a COMET Center within the COMET – Competence Centers for Excellent Technologies Programme and funded by BMK, BMDW, and the federal state of Vienna. The COMET Programme is managed by FFG. (2) the FFG ICT of the Future project 874019 dIdentity & dApps. (3) the European Union's Horizon 2020 research and innovation programme under grant agreement No 826078 (FeatureCloud) (4) OEAD (Austria's agency for education and internationalization) Special Grant.

References

1. Bao, Z., Shi, W., Kumari, S., Kong, Z.y., Chen, C.M.: Lockmix: a secure and privacy-preserving mix service for bitcoin anonymity. International Journal of Information Security pp. 1–11 (2019)
2. Barber, S., Boyen, X., Shi, E., Uzun, E.: Bitter to better—how to make bitcoin a better currency. In: International conference on financial cryptography and data security. pp. 399–414. Springer (2012)
3. Belcher, C.: Design for a coinswap implementation for massively improving bitcoin privacy and fungibility. https:// gist.github. com/ chris-belcher/ 9144bd57a91c194e332fb5ca371d0964 (Last accessed 16 July 2020)
4. Biryukov, A., Tikhomirov, S.: Deanonymization and linkability of cryptocurrency transactions based on network analysis. In: 2019 IEEE European Symposium on Security and Privacy (EuroS&P). pp. 172–184. IEEE (2019)
5. Bojja Venkatakrishnan, S., Fanti, G., Viswanath, P.: Dandelion: Redesigning the bitcoin network for anonymity. Proceedings of the ACM on Measurement and Analysis of Computing Systems **1**(1), 1–34 (2017)
6. Bonneau, J., Narayanan, A., Miller, A., Clark, J., Kroll, J.A., Felten, E.W.: Mixcoin: Anonymity for bitcoin with accountable mixes. In: International Conference on Financial Cryptography and Data Security. pp. 486–504. Springer (2014)
7. caedesvvv: Darkwallet. https:// github.com/ darkwallet/ darkwallet/ releases/ tag/ 0.8.0 (2015)
8. Chaum, D.: Blind signatures for untraceable payments. In: Advances in cryptology. pp. 199–203. Springer (1983)
9. Coindesk: Details of $5 million bitstamp hack revealed. https://www.coindesk.com/markets/2015/07/01/details-of-5-million-bitstamp-hack-revealed/ (Last accessed 17 January 2022)
10. English, S.M., Nezhadian, E.: Conditions of full disclosure: The blockchain remuneration model. In: 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). pp. 64–67. IEEE (2017)
11. Fabian, B., Ermakova, T., Sander, U.: Anonymity in bitcoin?–the users' perspective (2016)
12. Ficsor, A.: Zerolink: The bitcoin fungibility framework. URL: https: //github.com/ nopara73/ZeroLink (2017)
13. Ficsór, , Kogman, Y., Seres, I.A.: Wabisabi. https://github.com/zkSNACKs/WabiSabi/releases/download/build-70d01424bbce06389d2f0536ba155776eb1d8344/WabiSabi.pdf (Last accessed 3 Feb 2021)

14. Filtz, E., Polleres, A., Karl, R., Haslhofer, B.: Evolution of the bitcoin address graph. In: Data science–Analytics and applications, pp. 77–82. Springer (2017)
15. Fleder, M., Kester, M.S., Pillai, S.: Bitcoin transaction graph analysis. arXiv preprint arXiv:1502.01657 (2015)
16. Ghesmati, S., Fdhila, W., Weippl, E.: Sok: How private is bitcoin? classification and evaluation of bitcoin mixing techniques. Cryptology ePrint Archive (2021)
17. Ghesmati, S., Fdhila, W., Weippl, E.: Usability of cryptocurrency wallets providing coinjoin transactions. Cryptology ePrint Archive (2022)
18. Ghesmati, S., Kern, A., Judmayer, A., Stifter, N., Weippl, E.: Unnecessary input heuristics and payjoin transactions. In: International Conference on Human-Computer Interaction. pp. 416–424. Springer (2021)
19. Gibson, A.: New coinswap. https:// joinmarket.me /blog /blog /coinswaps/ (2017 (Last accessed 23 August 2020))
20. Gibson, A.: Snicker - simple non-interactive coinjoin with keys for encryption reused. https://joinmarket.me /blog /blog/snicker/ (2017 (Last accessed 31 August 2020))
21. Gibson, A.: Payjoin. https:// joinmarket.me /blog /blog /payjoin/ (2018 (Last accessed 23 August 2020))
22. Gibson, A.: Coinjoinxt - a more flexible, extended approach to coinjoin. https://joinmarket.me /blog/blog /coinjoinxt/ (2018 (Last accessed 31 August 2020))
23. Harrigan, M., Fretter, C.: The unreasonable effectiveness of address clustering. In: 2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ ATC/ ScalCom/ CBDCom/ IoP/ SmartWorld). pp. 368–373. IEEE (2016)
24. Heilman, E., Alshenibr, L., Baldimtsi, F., Scafuro, A., Goldberg, S.: Tumblebit: An untrusted bitcoin-compatible anonymous payment hub. In: Network and Distributed System Security Symposium (2017)
25. Heilman, E., Baldimtsi, F., Goldberg, S.: Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions. In: International conference on financial cryptography and data security. pp. 43–60. Springer (2016)
26. Ibrahim, M.H.: Securecoin: A robust secure and efficient protocol for anonymous bitcoin ecosystem. IJ Network Security **19**(2), 295–312 (2017)
27. Jelurida: Nxt. https://nxtdocs.jelurida.com/ Coin Shuffling (Last accessed 11 August 2020)
28. Joinmarket: Joinmarket. URL: https://github.com/JoinMarket-Org/ joinmarket-clientserver (2015)
29. Kappos, G., Yousaf, H., Maller, M., Meiklejohn, S.: An empirical analysis of anonymity in zcash. In: 27th {USENIX} Security Symposium ({USENIX} Security 18). pp. 463–477 (2018)
30. Keller, P., Florian, M., Böhme, R.: Collaborative deanonymization. arXiv preprint arXiv:2005.03535 (2020)
31. Krombholz, K., Judmayer, A., Gusenbauer, M., Weippl, E.: The other side of the coin: User experiences with bitcoin security and privacy. In: International conference on financial cryptography and data security. pp. 555–580. Springer (2016)
32. Lazar, J., Feng, J.H., Hochheiser, H.: Research methods in human-computer interaction. Morgan Kaufmann (2017)
33. Mai, A., Pfeffer, K., Gusenbauer, M., Weippl, E., Krombholz, K.: User mental models of cryptocurrency systems-a grounded theory approach. In: Sixteenth Symposium on Usable Privacy and Security ({SOUPS} 2020). pp. 341–358 (2020)

34. Maxwell, G.: Coinjoin: Bitcoin privacy for the real world, 2013. URL: https:// bitcointalk. org/ index. php (2013)
35. Maxwell, G.: Coinswap: transaction graph disjoint trustless trading (2013). URL: https:// bitcointalk. org/ index. php (2013)
36. Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M., Savage, S.: A fistful of bitcoins: characterizing payments among men with no names. In: Proceedings of the 2013 conference on Internet measurement conference. pp. 127–140 (2013)
37. Moser, M.: Anonymity of bitcoin transactions (2013)
38. Nakamoto, S.: A peer-to-peer electronic cash system. URL: https:// bitcoin. org/ bitcoin. pdf (2008)
39. Pfeffer, K., Mai, A., Dabrowski, A., Gusenbauer, M., Schindler, P., Weippl, E., Franz, M., Krombholz, K.: On the usability of authenticity checks for hardware security tokens. In: 30th {USENIX} Security Symposium ({USENIX} Security 21) (2021)
40. Quesnelle, J.: On the linkability of zcash transactions. arXiv preprint arXiv:1712.01210 (2017)
41. Ruffing, T., Moreno-Sanchez, P.: Valueshuffle: Mixing confidential transactions for comprehensive transaction privacy in bitcoin. In: International Conference on Financial Cryptography and Data Security. pp. 133–154. Springer (2017)
42. Ruffing, T., Moreno-Sanchez, P., Kate, A.: Coinshuffle: Practical decentralized coin mixing for bitcoin. In: European Symposium on Research in Computer Security. pp. 345–364. Springer (2014)
43. Ruffing, T., Moreno-Sanchez, P., Kate, A.: P2p mixing and unlinkable bitcoin transactions. In: NDSS. pp. 1–15 (2017)
44. Sabry, F., Labda, W., Erbad, A., Al Jawaheri, H., Malluhi, Q.: Anonymity and privacy in bitcoin escrow trades. In: Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society. pp. 211–220 (2019)
45. Samourai: Samourai wallet. URL: https:// samouraiwallet.com/ whirlpool (2015)
46. Tran, M., Luu, L., Kang, M.S., Bentov, I., Saxena, P.: Obscuro: A bitcoin mixer using trusted execution environments. In: Proceedings of the 34th Annual Computer Security Applications Conference. pp. 692–701 (2018)
47. Valenta, L., Rowan, B.: Blindcoin: Blinded, accountable mixes for bitcoin. In: International Conference on Financial Cryptography and Data Security. pp. 112–126. Springer (2015)
48. Ver, R.: The discontinuation of shared send at blockchain.info was due to threats of violence made by strangers in government. https:// www.reddit.com/ r/ btc/ comments/ 50t0jf/ roger ver the discontinuation of shared send at/ (2016)
49. Voskobojnikov, A., Obada-Obieh, B., Huang, Y., Beznosov, K.: Surviving the cryptojungle: Perception and management of risk among north american cryptocurrency (non) users. In: International Conference on Financial Cryptography and Data Security. pp. 595–614. Springer (2020)
50. Wang, Q., Li, X., Yu, Y.: Anonymity for bitcoin from secure escrow address. IEEE Access **6**, 12336–12341 (2017)
51. Wasabi: Wasabiwallet. URL: https://wasabiwallet.io/ (2018)
52. Weigl, D.: Mycelium shufflepuff. https:// github.com/ DanielWeigl/ Shufflepuff (2016 (Last accessed 11 August 2020))
53. Wiki: Mt. gox. https:// en.wikipedia.org/wiki/Mt.$_{Gox}(Lastaccessed17January2022)$
54. Wired: Hack brief: Hackers stole $40 million from binance cryptocurrency exchange. https://www.wired.com/story/hack-binance-cryptocurrency-exchange/ (Last accessed 17 January 2022)

55. Yousaf, H., Kappos, G., Meiklejohn, S.: Tracing transactions across cryptocurrency ledgers. In: 28th {USENIX} Security Symposium ({USENIX} Security 19). pp. 837–850 (2019)
56. Ziegeldorf, J.H., Grossmann, F., Henze, M., Inden, N., Wehrle, K.: Coinparty: Secure multi-party mixing of bitcoins. In: Proceedings of the 5th ACM Conference on Data and Application Security and Privacy. pp. 75–86 (2015)

A Questionnaire

* 1. Please check the box.

☐ I read all the information about objective, the GDPR compliance, and incentives for participants.

2. How familiar are you with cryptocurrencies?

☐ Extremely familiar
☐ Very familiar
☐ Somewhat familiar
☐ Not so familiar
☐ Not at all familiar

3. Where do you get information about cryptocurrencies? (Check all that apply.)

☐ Word of mouth
☐ News
☐ Social media
☐ Websites
☐ Internet search
☐ Forums
☐ Books
☐ White papers
☐ Technical reports
☐ Research papers
☐ Other (please specify)
☐ None of the above

4. Have you ever owned/bought/mined cryptocurrencies?

☐ Yes ☐ No

5. Have you ever made a cryptocurrency transaction? Transaction: transferring cryptocurrency from one address to another.

☐ Yes ☐ No

6. Which of the following best describes your current role with regards to cryptocurrencies? (Check all that apply.)

☐ Miner
☐ Investor
☐ Trader
☐ Financial user (using cryptocurrencies for payments)
☐ Researcher
☐ Curious about the technology (using and following the technology but not technically researching it)

☐ Developer
☐ Advisor/Consultant
☐ Other (please specify)
☐ None of the above

7. Which of the following wallets have you used? (Check all that apply.)
☐ Desktop wallet
☐ Mobile wallet
☐ Web wallet
☐ Hardware wallet
☐ Paper wallet
☐ Other (please specify)
☐ None of the above

8. Have you ever used Bitcoin wallet software?
☐ Yes ☐ No

9. Which of the following Bitcoin wallets have you used? (Check all that apply.) [6]
☐ List of bitcoin.org wallets
☐ Other (please specify)

10. Why did you use MyMaps as your Bitcoin wallet? It was shown to whom that selected MyMaps in the previous question.

11. How important is the anonymity of cryptocurrency transactions for you? "The anonymity of a subject means that the subject is not identifiable within a set of subjects, the anonymity set." [Pfitzmann and Hansen, 2010]
☐ Extremely important
☐ Very important
☐ Somewhat important
☐ Not so important
☐ Not at all important

12. How do you define Bitcoin in terms of anonymity?
☐ Extremely anonymous
☐ Very anonymous
☐ Somewhat anonymous
☐ Not so anonymous
☐ Not at all anonymous

13. Are you aware of the anonymity risks associated with Bitcoin?
☐ Yes ☐ No

14. If yes, please list the anonymity risks you are aware of.

15. What measures do you apply to improve your anonymity in Bitcoin?

16. Which of the following de-anonymization techniques in Bitcoin are you aware of? (Check all that apply.)
This question contained an invalid answer (Relating the input and output).
☐ Address reuse (reusing the address in different transactions)

[6] The list was adopted from https://bitcoin.org/en/choose-your-wallet which contains invalid answer (MyMaps)

☐ Multi-input/common input ownership heuristic (all the inputs of a transaction are controlled by the same entity)

☐ Change address detection (finding the change address and relating it to the owner of the input(s))

☐ Relating the input and output in the transactions with the same output amount (same input index is related to the same output index)

☐ Single-input, single-output (considered as self-payment)

☐ Transaction graphs (analyzing the money flow by creating the transaction graph)

☐ Tagging addresses through the information available on the Internet (finding the owner of the address by searching social networks, forums, etc.)

☐ Cashing out in forks (cash-out in Bitcoin forks (e.g. Bitcoin Cash) which compromise the privacy of the entity in the Bitcoin blockchain)

☐ Other (please specify)

☐ None of the above

17. Which of the following correlation attacks in Bitcoin are you aware of? (Check all that apply.)

☐ Network correlation (mapping IP address to Bitcoin address/finding a user's access pattern)

☐ Time correlation (mapping the time of the transaction with the activities in other services such as trading services)

☐ Amount correlation (mapping the amount of the transaction with the activities in other services such as trading services)

☐ Other (please specify)

☐ None of the above

18. Which of the following add-on privacy techniques in Bitcoin are you aware of? (Check all that apply.)

☐ Mixing websites/centralized mixers

☐ CoinJoin-based techniques

☐ Fairexchange /CoinSwap

☐ Threshold signatures/Schnorr signatures

☐ Off-chain solutions

☐ Other (please specify)

☐ None of the above

19. Which of the following built-in privacy coins (using techniques such as Zero-knowledge proof, Ring signature, CoinJoin, etc. by design) are you aware of? (Check all that apply.)

☐ Monero

☐ Decred

☐ Zcash

☐ Horizen

☐ Dram

☐ Pirate Chain ARRR

☐ MobileCoin

☐ Dero

☐ Verge
☐ Other (please specify)
☐ None of the above

20. Which features make Dram a privacy coin? (Check all that apply.) It was shown to whom selected Dram as a privacy coin.

☐ Hiding the amount of the transaction
☐ Hiding the source of the transaction
☐ Hiding the destination of the transaction
☐ Other (please specify)
☐ None of the above

21. Which of the following built-in privacy coins have you owned/bought /mined? (Check all that apply.)

Answers from Q.19
☐ Other (please specify)
☐ None of the above

22. Why did you own/buy/mine privacy coins?

☐ For better anonymity
☐ For investment
☐ Both of the above
☐ Other (please specify)

23. Which of the following would you prefer to achieve better anonymity in the cryptocurrencies area?

☐ Using add-on techniques implemented by wallets and services in Bitcoin (e.g., mixing techniques such as CoinJoin)
☐ Using built-in techniques in privacy coins (Zcash, Monero, etc.)
☐ I do not know
☐ Other (please specify)

24. Why do you prefer using Bitcoin add-on privacy techniques rather than privacy coins? (Check all that apply.)

☐ Bitcoin market cap
☐ Bitcoin reputation
☐ Availability of Bitcoin tools (wallets, explorers, etc.)
☐ Bitcoin is listed in most exchanges.
☐ Transacting is not as complicated as some privacy coins.
☐ Other (please specify)

25. Why do you prefer using privacy coins rather than Bitcoin add-on privacy techniques? (Check all that apply.)

☐ Privacy-by-design provides stronger anonymity.
☐ I prefer using privacy coins that have mandatory built-in privacy which is used by all users and provides better anonymity amongst all users. (using privacy features in some coins is optional)
☐ Add-on techniques implemented by third-parties require trust in those tools/services.
☐ Other (please specify)

26. Which of the following would you prefer in Bitcoin?

☐ Adding mandatory built-in privacy techniques (such as Zero-knowledge proof, Ring signature, Confidential transactions, etc.) to the protocol

☐ Using add-on privacy techniques (such as mixing) whenever you need better anonymity

☐ I do not know

☐ Other (please specify)

27. Please explain in more detail why you chose that option.

28. Which privacy features are you interested in for Bitcoin? (Check all that apply.)

☐ Hiding the amount of the transaction

☐ Hiding the source of the transaction

☐ Hiding the destination of the transaction

☐ I do not know

☐ Other (please specify)

☐ None of the above

29. Which of the following Bitcoin privacy wallets are you aware of? (Check all that apply.)

☐ Dark wallet

☐ Sharedcoin

☐ Joinmarket wallet

☐ Wasabi wallet

☐ Samourai wallet

☐ Other (please specify)

☐ None of the above

30. Which of the following privacy wallets have you used? (Check all that apply.)

☐ Answers from Q.29

☐ Other (please specify)

☐ None of the above

31. How satisfied are you with the following privacy wallets?

☐ Selected wallets from Q.30.

☐ Extremely satisfied

☐ Very satisfied

☐ Somewhat satisfied

☐ Not so satisfied

☐ Not at all satisfied

32. Please tell us why you are satisfied/dissatisfied with each of the wallets.

33. Which of the following best describes your opinion to trust third-party privacy wallets to enhance your privacy in Bitcoin?

☐ I trust the privacy wallet if it is open-source and the code can be checked.

☐ I trust the privacy wallet if it is trusted on forums/websites that I trust.

☐ I trust the privacy wallet if it is trusted by my friends.

☐ I do not trust third-party services.

☐ I do not know.

☐ Other (please specify)

34. If you do not trust third-party privacy wallets, why not?

35. Why do you think Bitcoin is extremely anonymous? It was shown to whom selected Bitcoin as fully anonymous.

☐ The source address is hidden.

☐ The destination address is hidden.

☐ The transaction amount is hidden.

☐ There are no real identities in the transactions (neither names nor personally identifiable information (PII)).

☐ No one can track the transaction flow.

☐ I do not know.

☐ Other (please specify)

If we say there are some techniques to improve privacy in Bitcoin, how would you answer the fees and delays questions?

36. Would you pay extra fees in Bitcoin transactions to enhance your privacy?

☐ Yes (You will choose the preferred fees in the question.)

☐ No

☐ I do not know.

37. How much would you pay for Bitcoin transaction privacy if the transaction's value is $1,000? (Please enter a whole number. Enter the number of dollars you are willing to pay.)

38. If you are not likely to pay extra fees for privacy in Bitcoin transactions, why not?

☐ Privacy is not important for me.

☐ The volume of my investment in the crypto market is too low, therefore it does not seem reasonable to pay more for privacy.

☐ The current level of Bitcoin privacy meets my expectations.

☐ Current Bitcoin transaction fees are too high and I can not tolerate paying more for privacy.

☐ Other (please specify)

39. Would you accept delays in performing Bitcoin transactions to enhance your privacy?

☐ No

☐ Yes, if it is less than a minute.

☐ Yes, if it is less than an hour.

☐ Yes, if it is less than a day.

☐ Yes, if it is less than a week.

☐ Yes, if it is less than a month.

☐ I do not know.

40. If you are not likely to accept delays for privacy in Bitcoin transactions, why not?

☐ Privacy is not important for me.

☐ The current level of Bitcoin privacy meets my expectations.

☐ The delays in Bitcoin transaction confirmations are still too long.

☐ Other (please specify)
41. Please select "Homophonic substitution cipher".
It is a quality check. If you choose other than Homophonic substitution cipher, we cannot consider your responses, because you are either not paying attention and your answers are not valid, or you are a robot.
☐ Caesar cipher
☐ Monoalphabetic cipher
☐ Homophonic substitution cipher
☐ Polyalphabetic Cipher
☐ Playfair cipher
☐ Rail fence
42. Please tell us your current role(s) with regard to cryptocurrencies.
43. Please provide us with your Monero address; in case you win, we will pay the incentives to this address.
44. Please provide your gender
☐ Female ☐ Male ☐ Diverse ☐ Do not want to specify
45. What is your age?
☐ 18 to 24 ☐ 25 to 34 ☐ 35 to 44 ☐ 45 to 54 ☐ 55 to 64 ☐ 65 to 74 ☐ 75 or older
46. What is the highest level of education you have completed?
☐ Did Not Complete High School
☐ High School
☐ Did Not Complete College
☐ Bachelor's Degree
☐ Master's Degree
☐ Ph.D.
47. Do you work or study in an IT-related field?
☐ Yes ☐ No
48. On what continent do you currently reside?
☐ Africa ☐ America ☐ Asia ☐ Australia ☐ Europe ☐ Do not want to specify

B Background

B.1 De-anonymization Techniques

Common input ownership. One of the main heuristics, namely "common input ownership" links all input addresses to the same user [36]. This is based on the assumption that multiple inputs of a transaction are controlled by the same user [38], as the coins associated with an address can only be redeemed by providing the corresponding signature. According to [23], the heuristic is able to identify almost 69% of the addresses stored in the clients' wallets.
Change addresses detection. When the sum of transaction inputs is larger than the sum of outputs, a fresh address, namely a "change address" is created to return the remainder of the coins to the sender [14]. This heuristic assumes

that the change address is controlled by the owner of the input addresses [6].
Address reuse. Reusing the same address for multiple transactions may help link identities to transactions, e.g., using graph analysis.
Side-channel attacks. Side-channel attacks [6] such as time correlation, amount correlation, and network-layer [5] information can be used to identify relationships between transactions.
Auxiliary information Auxiliary information [6] from, e.g., forums, merchants, search engines can be used to tag the addresses.
Transaction graph. A transaction graph shows the flow of bitcoins between users, in which addresses are the nodes, and transactions linking input- to output addresses [15].

Since a transaction input is related to the output of a previous transaction, it becomes possible to identify relationships between them [37]. Moreover, a transaction often includes a change addresses that is usually controlled by the sender (input address) and, consequently, links to them in the transaction graph. When interacting with specific services, users might have to reveal information about their real identities. This may allow to associate identities to Bitcoin addresses, which – if reused – could reveal the transaction history of that identity by using the transaction graph.

B.2 Privacy-enhancing Techniques in Bitcoin

Centralized mixers. This type of mixing is performed by a central mixer that collects the coins from different parties and forwards them to the associated destination addresses. Mixing websites were the first version of such mixers, trying to obfuscate the relationships between senders and recipients. However, this relies on the trust assumption that the mixer will not steal the coins and reliably send them to the recipients. MixCoin [6] solves the theft problem with mixing websites using a warranty that contains the mixer's signature. If they misbehave, the sender may publish the warranty and harm the mixer's reputation. Although theft can be detected, it cannot be prevented. Furthermore, the mixer can still correlate input and output addresses. BlindCoin [47] adds Blind signatures [8] to Mixcoin. This allows the sender to blindly send the output to the mixer and prevents the mixer from linking inputs to outputs. However, this does not resolve the theft problem. LockMix [1] improved BlindCoin by using multi-signatures to prevent theft. Obscuro [46] is also a centralized mixer which uses trusted execution environments (TEE) to solve theft and transaction linkability.

Atomic swap. In Atomic swaps, two parties exchange coins in a decentralized manner, while ensuring that if one of them gets paid, the other will also get paid. Fairexchange [2] were the first to use this feature. Alice sends the coins to Bob's destination address, and Bob does the same for Alice. They lock their transactions by different hashes (a and a+b). The parties can either redeem the coins by providing both their signatures or one party's signature and a pre-image of the hash in their hash lock transaction. Subsequently, Xim used Fairexchange and proposed a way to find another party to create Fairexchange transactions. Parties use blockchain to advertise their intention to create Fairexchange and

then communicate via an Onion address or Bulletin board. Coinswap [35] creates Fairexchange transactions through an intermediary where the hash lock transactions lock the funds by the same pre-image (x). New CoinSwap [19] uses Check Lock Time Verify (CLTV) to create hash time locked transactions. PaySwap [3] improves NewCoinSwap by using two-party ECDSA to create 2-of-2 multi-signature addresses; thus, the multi-signature looks like regular single-signature addresses and provides better privacy. It also combines the idea of PayJoin ([21]) with CoinSwap to create PaySwap transactions. Blindly Signed Contract (BSC) [25] uses CoinSwap transactions while it uses the blind signature to redeem the transactions; however, using blind signature requires a Bitcoin soft-fork. The protocol was improved in TumbleBit [24] which uses a puzzle solution.

CoinJoin-based. CoinJoin-based mixings do not require third parties and can prevent coin theft by the mixer. CoinJoin [34] is a joint transaction by Bitcoin users to hide relationships between sender- and recipient addresses. In Bitcoin, a transaction may include multiple inputs, and each of them should be signed by the corresponding key. This property allows different users to jointly create a transaction and, eventually, define change addresses to get the remainder of the coins back. For privacy reasons, all the users should spend the same amount of coins to avoid correlating input- to output values. Once the transaction is created, the users separately sign their inputs, and one of them publishes it to the network. While CoinShuffle [42] improves on CoinJoin by preventing the peers involved in the mixing from tracing each other, CoinShuffle++ advances mixing performance by using DiceMix. ValueShuffle [41] improves on CoinShuffle++ by adding a stealth address (a unique one-time address) and confidential transactions (hiding the transaction amount). CoinJoinXT [22] introduces a form of CoinJoin transaction where the users lock their funds in a multi-signature address. While Snicker [20] introduces a new protocol for a non-interactive CoinJoin, PayJoin [21] tries to solve the distinguishability of CoinJoin transactions with the same output amount.

Threshold signatures In threshold signatures, the peers jointly sign a transaction from an address which is under their control. CoinParty [56] uses mixing peers where the input peers send their coins to the addresses under the control of mixing peers along with their desired destination addresses. Next, mixing peers create a transaction in which they send the coins from the joint control address to the destination addresses. Several improvements for threshold signature were presented in SecureCoin [26] and Secure Escrow Address (SEA) [50].

B.3 Privacy Coins

In this section, we present a selection of top privacy coins according to their market cap [7]. Monero, Zcash, and Decred, all of which provide built-in privacy techniques.

[7] https://coinmarketcap.com/view/privacy/

Monero is a UTXO-based cryptocurrency that was developed to provide anonymity. It applies stealth addresses, ring signatures, and RingCT. Stealth addresses create a one-time address for each transaction. Ring signatures allow to obfuscate the sender by creating a group of inputs for hiding the actual sender. Finally, RingCT enables confidential transactions by hiding the amounts as well as senders and receivers. RingCT is also known as Multi-layered Linkable Spontaneous Anonymous Group (MLSAG) signature.

Zcash is a Bitcoin fork that employs a type of zero-knowledge proof named ZK-SNARKS. In addition to most Bitcoin features, Zcash adds the possibility to shield transactions. Transactions between transparent addresses (t-address) are equivalent to Bitcoin transactions. Transactions which involve z-addresses are carried out in the JoinSplit format. A JoinSplit has three fields: (1) the number of coins entered the shielded pool, (2) the number of coins exiting from the shielded pool, and (3) a field to carry out zero-knowledge proofs to show the legitimacy of the transaction [40]. It is possible for coins to be transferred between the transparent and the shielded addresses. [40] and [29] found that most of the transactions are performed outside of the shielded pool, so it is also possible to apply Bitcoin de-anonymization heuristics on the Zcash transparent transactions.

Decred is a cryptocurrency which utilizes a hybrid Proof-of-Work/Proof-of-Stake consensus system. Decred applies the CoinShuffle++ protocol [43] and allows for pruning (i.e., dropping the used transactions from full nodes which effectively reduces the UTXO set size), compared to ring signature and ZK-SNARKS.

B.4 Bitcoin Privacy Wallets

The comparison of security, privacy, and usability criteria of the Bitcoin privacy techniques have been investigated in [16], indicating that CoinJoin-based techniques require less transactions, which consequently lowers the fees that should be paid to provide privacy. Most of the privacy-preserving techniques have not been commercially implemented. Most of the implementations are centralized mixing websites, which suffer from theft and exit scams. At the time of writing, Joinmarket [28], Wasabi [51], and Samourai [45] are the usual implementations of CoinJoin wallets. SharedCoin (a CoinJoin service by Blockchain.com until 02.09.2016) [48] and Darkwallet (until 23.01.2015) [7] were discontinued. BTCpay implemented PayJoin in 2020, letting merchants create their stores accepting PayJoin transactions. At the time of writing, Samourai, Joinmarket, Wasabi and Bluewallet support the sender side of PayJoin transactions. Samourai and Joinmarket also support the recipient side of PayJoin transactions. ShufflePuff [52] is an alpha version of CoinShuffle in Github (last updated in 2016), while Nxt [27] reported the activation of CoinShuffle since block 621,000; at the time of writing, the CoinShuffle feature has been eliminated from the wallet feature list. To the best of our knowledge, there is no commercial implementation of atomic swap techniques. Recently, [3] proposed to develop a new CoinSwap design/PaySwap

wallet. TumbleBit implementations on Github (NTumbleBit and Breeze) are also in their alpha versions.

CoinJoin Wallets. In what follows, we review the CoinJoin wallets and explain how they implement the CoinJoin technique.

JoinMarket wallet. Joinmarket [28] is a desktop wallet which applies a taker-make model to create CoinJoin transactions. A taker broadcasts her willingness to create a CoinJoin transaction on the IRC messaging channel. The makers listening to the IRC send their participation confirmations to the taker, including fees. The taker creates the transaction with the desired CoinJoin amount and sends it to the makers for signing. As the taker is the one who creates the CoinJoin transaction, she can put the desired recipient address among the outputs, without the makers knowing to which input the output is related. Thus, in JoinMarket, directly sending to the desired recipient address is possible.

Wasabi wallet. Wasabi [51] is a desktop wallet. It uses Chaumian CoinJoin [12] which is a blind signature [8] on outputs to create CoinJoin transactions. In Wasabi, the users register their inputs by sending the UTXO, the proof of the UTXO ownership, the change address to get the remainder, and their blinded output to the coordinator to prevent the correlation of inputs to outputs. Afterward, the coordinator verifies the inputs, signs the blinded output, and sends each of the outputs back to the senders. In the output registration phase, the senders unblind and send their outputs to the coordinator. If the latter finds his signature on the output, he creates a CoinJoin transaction with all the registered UTXOs as inputs and all the registered outputs and change addresses as the outputs of the transaction. In the signing phase, the coordinator sends the transaction inputs to be signed by the corresponding users, collects all transactions, combines the signatures, and broadcasts the transaction in the network [12].

Samourai wallet. Samourai [45] is a mobile wallet currently released as an Android application. It also offers Chaumian CoinJoin under the name "Whirlpool". At the time of writing, four pools (0.001, 0.01, 0.05, and 0.5 BTC) are available to join and create CoinJoin transactions. There is a flat fee rate for the pools. Users register their coins to one of the pools and wait for the required peers to create a CoinJoin transaction. In Samourai, the coins are first split into the selected pool amount in transaction 0 (TX0). These UTXOs are considered as pre-mix UTXO. Then they are registered to a coordinator who will create the CoinJoin transaction for the selected pool. Once the CoinJoin is created, the mixed UTXO appears in the post-mix wallet.

C Related work

Blockchain security and privacy from a user perspective has been studied in [31, 11, 33]. The studies demonstrated the lack of users' knowledge about blockchain privacy issues and showed that most users do not know why privacy techniques are required or how they could mitigate de-anonymization.

Krombholz et al. [31] conducted a user study on Bitcoin security and privacy and identified a large gap between different users' understandings on how to remain private and anonymous in Bitcoin. More than a third of their participants thought that Bitcoin is fully anonymous. Fabian and Ermakova [11] found that almost 18% of users were unaware of the risk of being de-anonymized on blockchain, and half of them knew about the risks and were concerned, while the remainder was aware of the risks but not concerned. They also investigated whether users are aware of mixing services, and half of the participants were not familiar with the CoinJoin technique. Besides improving users' knowledge, the usability of implemented privacy techniques has a significant role in their practical adoption. They found that coin mixing services are better known, and that the participants are more willing to use them, compared to CoinJoin and Zerocoin. 38% of the participants would use coin mixing services, while 38% would not use them, and 24% do not know about them at all. More than half of the participants are not familiar with CoinJoin (52%) and Zerocoin (58%). Even of those aware of the measures in both cases, 29% would not use them, even if the community implemented them.

Mai et al. [33] performed a qualitative user study on user mental models of cryptocurrency systems. They found that users assume that they are anonymous, and that blockchain transactions are encrypted and therefore, the data is not publicly readable. Most of the users pointed out address mapping as a privacy threat. Identity disclosure through the use of third-party services (exchanges or market services), has also been reported by the users. For prevention against privacy threats, participants specified mining cryptocurrencies rather than buying them, in this manner they could avoid disclosing identities.A few participants were aware of buying cryptocurrencies from specific third parties that do not employ know-your-customer processes.

In [49], risk management of cryptocurrencies has been studied through a series of interviews with 11 users and 9 non-users, indicating that the misunderstandings of users and non-users can effectively deviate the measures they apply to mitigate the risks.

Most of the previous studies [31, 33, 49] focused on both security and privacy aspects. With respect to privacy, they mainly investigated Bitcoin anonymity and network privacy aspects. In contrast to network de-anonymization heuristics (such as common input ownership, change address detection, etc.), timing and amount correlation as possible privacy attacks have not been addressed in the previous user studies. Besides, these studies did not investigate privacy wallets and users' preferences on additional fees and delays related to add-on privacy techniques.

D Methodology

D.1 Qualitative Research

Recruitment Participants were recruited via social media, universities, and companies with a focus on Blockchain technology. Those who (i) already have

little to basic knowledge about blockchain and cryptocurrencies, and (ii) used a cryptocurrency wallet and performed a transaction in the past, and (iii) were at least 18 years old. were eligible to participate as users. Non-users were recruited with different requirement, (i) not familiar at all with cryptocurrencies, and (ii) not used a cryptocurrency wallet and performed a transaction in the past, and (iii) were at least 18 years old.We did not specify that the interview is about privacy aspects of blockchain and Bitcoin to make sure that the users did not read related materials beforehand. This allowed us to learn about their privacy perception with their actual level of knowledge.

Coding Grounded Theory [32] was used for coding. Researchers coded the data and grouped statements related to the same concept. In each coding round, we discussed the relations between categories to define higher-level categories. With this method, we were able to revise or add the options to the questions in our quantitative analysis.

Sampling We selected the participants according to their reported level of knowledge and their usage of cryptocurrencies, ranging from expert to novice users. We interviewed 14 participants, 12 users (age: max. = 45, min. = 26) and 2 non-users (age: max. = 45, min. = 35). 7 out of the 12 users and 1 out of the 2 non-users were working in IT-related fields. Detailed demographics is provided in Table E.1 . All the user participants have owned /bought /mined cryptocurrencies and have already made a transaction.

Limitations We asked our participants about their knowledge level regarding cryptocurrencies, field of study/work, previous experience with transactions on blockchain, and gender, if they allowed it. Most participants had university degrees. With regards to age, we unfortunately had no participants in 18-24 and 55-64 age groups, and no participants with high school- or college level of education. However, our sample covers diverse knowledge levels, education/work backgrounds, and genders. Due to the Covid-19 situation, we performed the majority of the interviews online, however, in some cases we had to ask some of the questions several times or request the interviewees to repeat their answers as a result of poor or unstable Internet connections.

D.2 Quantitative Research

Sampling Our scope was Bitcoin users and UTXO-based privacy coins. Our questionnaire was distributed through different international channels. It was shared in the Bitcoin forums Bitcointalk.org on social media such as Reddit, Telegram, Facebook, Twitter, and LinkedIn. It was also sent to blockchain and cryptography mailing lists, the related international research centers, researchers, university students, and businesses in our country. In total, 101 participants took part in our survey. After applying our exclusion criteria, we reached a final sample of n = 58 for our analysis. Those 58 were eligible based on their self-reported knowledge, completely filled-out questionnaires and passed quality

control checks. Detailed demographics and cryptocurrency familiarity are provided in Table E.1. The majority of participants (91.38%) reported that they have owned /bought /mined cryptocurrencies. 81.03% made at least one transaction, and 62.96% have used Bitcoin wallet software. Figure E.3 demonstrates the self-reported role in cryptrocurrency, and Figure E.4 illustrates the wallet types that were used by the participants. The majority of the participants reported themselves as "investors" and "curious about the technology". Desktop wallets and mobile wallets were among the top selected wallet types that were used by participants.

D.3 Ethical Considerations

Our research center is located in (blinded), and is subject to the European General Data Protection Regulation (GDPR). Before the interview in the qualitative part, all participants were asked to sign consent forms in which we specified the goals of the study and the academic context the data will be used for. The consent forms do not include the participants' IDs we assigned for the analysis. To comply with the GDPR, we did not ask any questions that may disclose personally identifiable information (PII); the questions do not allow any inference to the participants' identities. The research objective, the GDPR- and ethical notice regarding the raffle were provided at the beginning of the questionnaire in the quantitative part.

E Figures and Tables

In this section, the charts and tables are provided. Figure E.1 indicates the process of designing our questionnaire. We first prepared a draft of our questionnaire. Then we conducted a Pilot in a Blockchain workshop with 11 participants. We could revise the questionnaire based on the answers and feedback. Next, we performed another Pilot as a think-aloud with 4 blockchain security and privacy experts. We again revise the questionnaire. We then consulted with our legaloffice to be compliant with GDPR and a usability researcher provided us with her comments on the questionnaire. We then conducted a qualitative interview with 14 participants (12 users and 2 non-users) with open-ended questions. For our quantitative part, we added multi-choice options to some of the questions and asked an editor to Proofread the questionnaire. We Finalized the questionnaire and options Logic and published the questionnaire on survey monkey.

The chart in Figure E.2 illustrates how we defined the questionnaire logic. Interviews with non-users showed that they were not able to answer the questions as answering required a basic knowledge of cryptocurrencies; hence we set the logic in a way that if the respondents select "not familiar at all" with the cryptocurrencies, they will jump into the end of the survey. In the following questions, we asked the user privacy awareness, and in the first question, we asked how they consider Bitcoin anonymity. If they selected Bitcoin as extremely anonymous, they jumped into privacy unaware users' question, where We asked

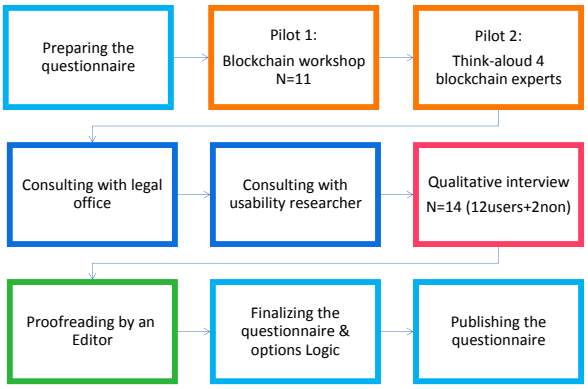

Fig. E.1. Designing the Questionnaire

them why they believe Bitcoin is extremely anonymous. Privacy-aware users could see the questions regarding De-anonymization attacks and add-ons techniques, privacy coins, privacy preferences, and privacy wallets. We asked both unaware and aware users about their willingness to pay extra fees or accept delays for better privacy. Before showing this to the unaware users we provided them about the privacy issues in the public blockchain. And finally, we asked them for demographics.

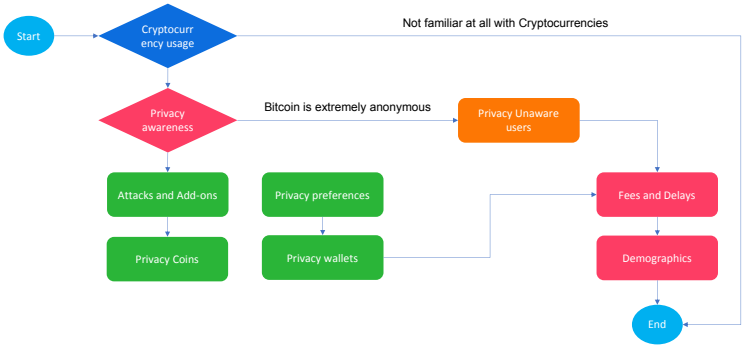

Fig. E.2. Questionnaire Overall Logic

Table E.1. Demographics and familiarity of participants

Demographichs	*Quantitative*	*%*	*Qualitative*	*%*
Gender				
Female	10	17.24%	4	28.57%
Male	40	68.97%	10	71.42%
Diverse	1	1.72%		
Do not want to specify	7	12.07%		
Age				
18 to 24	15	25.86%		
25 to 34	19	32.76%	2	14.28%
35 to 44	17	29.31%	10	71.42%
45 to 54	6	10.34%	2	14.28%
55 to 64	1	1.72%		
Highest level of education				
Did Not Complete High School	1	1.72%		
High School	6	10.34%		
Did Not Complete College	3	5.17%		
Bachelor's Degree	23	39.66%	4	28.57%
Master's Degree	21	36.21%	8	57.14%
Ph.D.	4	6.90%	2	14.28%
Continent of residence				
America	7	12.07%		
Asia	17	29.31%		
Australia	2	3.45%		
Europe	26	44.83%		
Do not want to specify	6	10.34%		
Self-reported cryptocurrency familiarity				
Extremely familiar	12	20.69%		
Very familiar	24	41.38%		
Somewhat familiar	17	29.31%		
Not so familiar	5	8.62%		

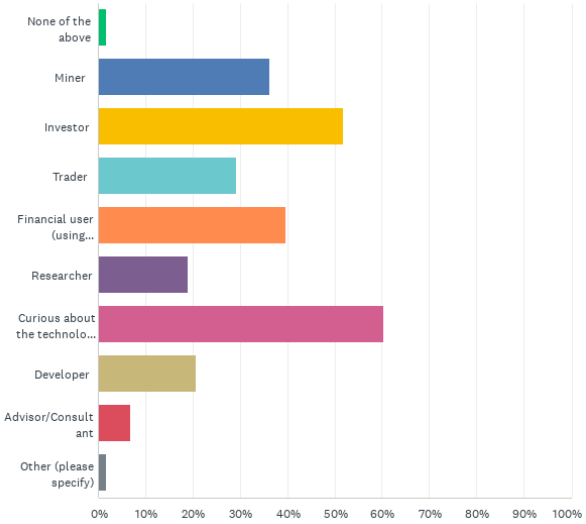

Fig. E.3. Current role in cryptrocurrency

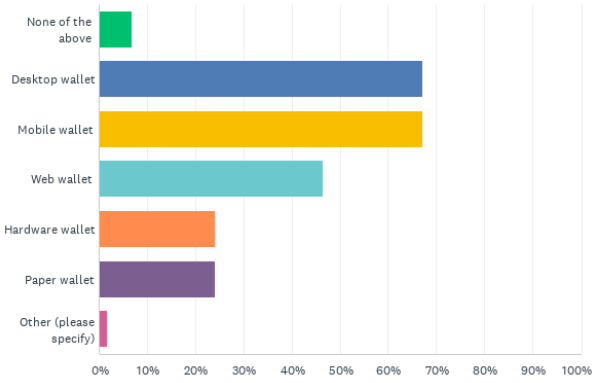

Fig. E.4. Wallet type used by participants

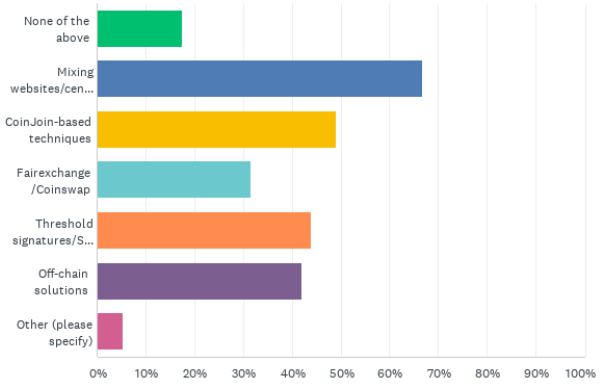

Fig. E.5. Awareness of Add-on Techniques

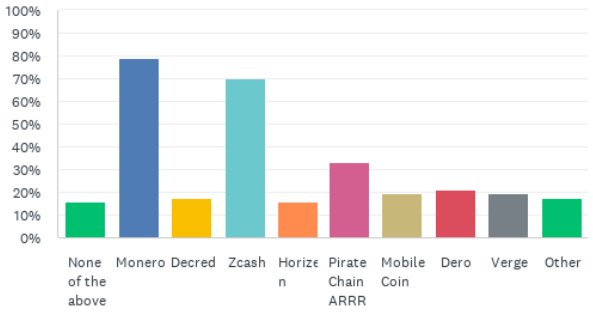

Fig. E.6. Privacy coins awareness

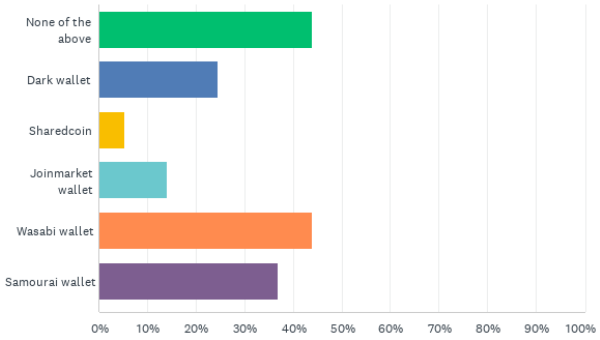

Fig. E.7. Privacy wallets awareness

Table E.2. Privacy wallets satisfaction

	Very satisfied		Somewhat satisfied		Not at all satisfied		Total
Dark wallet	100.00%	1	0.00%	0	0.00%	0	1
Sharedcoin	100.00%	1	0.00%	0	0.00%	0	1
Joinmarket wallet	33.33%	1	66.67%	2	0.00%	0	3
Wasabi wallet	66.67%	6	22.22%	2	11.11%	1	9
Samourai wallet	75.00%	3	0.00%	0	25.00%	1	4