TU WIEN Informatics

Privacy and Usability Aspects of Public Blockchains

DISSERTATION

submitted in partial fulfillment of the requirements for the degree of

Doktorin der Technischen Wissenschaften

by

Simin Ghesmati
Registration Number 11848747

to the Faculty of Informatics

at the TU Wien

Advisor: Univ.-Prof. Dipl.-Ing. Mag. Dr. techn. Edgar Weippl

The dissertation has been reviewed by:

Tomáš Pitner	Katharina Krombholz

Vienna, 7th May, 2024

Simin Ghesmati

Technische Universität Wien
A-1040 Wien ▪ Karlsplatz 13 ▪ Tel. +43-1-58801-0 ▪ www.tuwien.at

Erklärung zur Verfassung der Arbeit

Simin Ghesmati

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 7. Mai 2024

Simin Ghesmati

Acknowledgements

Edgar, I want to thank you for allowing me to start this journey. I gained insights not only into my thesis topic but also into handling challenges during my Ph.D. This would not have been possible without your support over the past years.

Walid, I am grateful for your support in my research, your feedback, and your assistance during the times I waited for paper notifications.

I would also like to extend my appreciation to Katharina Engel and the OEAD regional office team for assisting me in living in Austria and with visa-related matters.

A special thanks to the blockchain and usability researchers at SBA. Your feedback has significantly contributed to the improvement of my research.

I would also like to thank my family for their support during these years.

Thank you all once again for your support.

Abstract

The widespread adoption of blockchain technology (BT) has brought significant attention to concerns surrounding user privacy. As a decentralized and distributed system, BT enables users to store and transfer information securely and transparently. However, its public nature also means that anyone can access its data, potentially resulting in privacy breaches. To address these concerns, several privacy-preserving techniques have emerged to mitigate the risks associated with the public blockchain and safeguard user privacy.

This thesis[1] focuses on privacy concerns specific to the Bitcoin blockchain. Its primary objective is to assess the efficiency of the existing privacy-preserving techniques within the Bitcoin blockchain, highlighting their limitations and identifying emerging challenges. Moreover, the thesis investigates users' mental models in employing privacy-preserving techniques for the blockchain through interviews and questionnaires. By gaining insights into users' perspectives and expectations regarding privacy-preserving techniques, this approach contributes to a comprehensive understanding of users' perceptions.

A key challenge in the adoption of privacy-preserving techniques in BT is their usability for ordinary users. To overcome this challenge, the thesis conducts a comprehensive usability study of wallets that integrate add-on privacy techniques. This study incorporates a cognitive walkthrough and a user study based on usability and design criteria. The resulting findings provide insights and guidance to developers on enhancing the usability of these wallets and making them more user-friendly.

This thesis aims to advance the comprehension and enhancement of user privacy within BT, with a specific focus on the Bitcoin blockchain. The research findings have the potential to guide the development of novel, effective, and efficient privacy-preserving techniques for protecting user privacy. Moreover, the study's insights on the usability aspects of privacy wallets can assist developers in creating user-friendly and accessible privacy-preserving techniques for blockchain transactions.

[1]Some parts of this thesis are based on the published papers of the doctoral student about Studying Bitcoin Privacy Attacks and Their Impact on Bitcoin-Based Identity Methods (BPM 2021), Classification and Evaluation of Bitcoin Privacy Techniques (ARES 2022), User-Perceived Privacy in Blockchain (CoDecFin, FC 2022), Usability of cryptocurrency wallets providing CoinJoin transactions (USEC, NDSS2022) and use passages from these works verbatim and/or with little modifications.

Contents

CHAPTER 1

Introduction

Over the past years, there has been a remarkable surge in the popularity and curiosity surrounding blockchain technology. Since the publication of the Bitcoin whitepaper by Satoshi Nakamoto in 2008, blockchain technology has evolved beyond its initial application in cryptocurrencies and emerged as a powerful and transformative technology with numerous potential use cases. Industries such as supply chain management, Industry 4.0, healthcare, and identity management have recognized the value and potential of blockchain technology.

While traditional systems rely on centralized entities to facilitate and validate transactions, blockchain technology operates on a decentralized and distributed ledger that records and stores transactions transparently and immutably. This decentralized nature eliminates the need for intermediaries and enables secure, peer-to-peer transactions. However, the transparency of the blockchain poses a significant challenge to participant privacy, particularly in financial transactions.

Although blockchain transactions are pseudonymous, meaning that users are identified by their alphanumeric addresses (generated from public keys) rather than their real-world identities, the information within these transactions can still be analyzed and linked to reveal user identities and financial activities. Studies have shown that by analyzing multiple transactions and linking them together, adversaries can uncover sensitive information about users, including their interactions, and financial data. This lack of privacy in blockchain transactions can have severe consequences, such as exposing users to potential risks, enabling discrimination or extortion, and providing valuable insights to competitors.

To address these privacy concerns, it is imperative to develop and implement privacy-preserving techniques for blockchain transactions. Privacy-enhancing technologies aim to protect the confidentiality and anonymity of users while still maintaining the transparency and integrity of the blockchain. These techniques can help prevent the misuse of personal

information, safeguard financial privacy, and promote a more secure and user-centric blockchain ecosystem.

1.1 Aims

The blockchain technology of Bitcoin has gained significant attention for its potential to provide secure and decentralized monetary transactions. However, the public nature of the Bitcoin blockchain raises concerns regarding the privacy of users' financial transactions. Several studies [1, 2, 3, 4] have revealed that users' real identities can be exposed through the analysis of their interactions on the blockchain. This privacy vulnerability has led to the development of various proposals for privacy solutions, including built-in and add-on approaches [5].

This PhD thesis aims to delve into the different approaches to privacy in Bitcoin, with a specific focus on usability aspects and user experience of privacy wallets. While privacy-preserving techniques have emerged for coin mixing and preserving privacy in Bitcoin transactions, it is crucial to understand how users perceive the current implementation of such privacy solutions and the disparities between their expectations and the actual effectiveness of the proposed techniques when adopted in practice. The thesis investigates the misconceptions that users have about blockchain privacy, as the flawed understanding of the privacy guarantees provided by blockchain-based systems is prevalent. By analyzing the factors contributing to these misconceptions, this research aims to develop potential strategies for addressing them, ultimately enhancing the trust and adoption of blockchain technology.

Furthermore, this thesis aims to explore methods for improving the adoption of privacy wallets by both technical and non-technical users, emphasizing usability aspects and user experience. Since having a large user base is important to achieve the desired level of anonymity in these wallets, designing a user-friendly and informative privacy wallet becomes crucial. Unusable system design can become a significant obstacle, hindering the adoption and effectiveness of privacy-preserving techniques. Therefore, this research focuses on designing privacy wallets that offer improved user experiences, providing intuitive interfaces, clear explanations of risks associated with specific actions, and seamless integration with existing financial systems.

Generally, this thesis seeks to contribute to the understanding of the monetary aspects of Unspent transaction output (UTXO)-based blockchains such as Bitcoin, with a specific focus on privacy-preserving techniques and the usability of privacy wallets. By addressing the challenges related to privacy and usability, this research aims to pave the way for developing more user-friendly and privacy-enhanced blockchain-based financial systems.

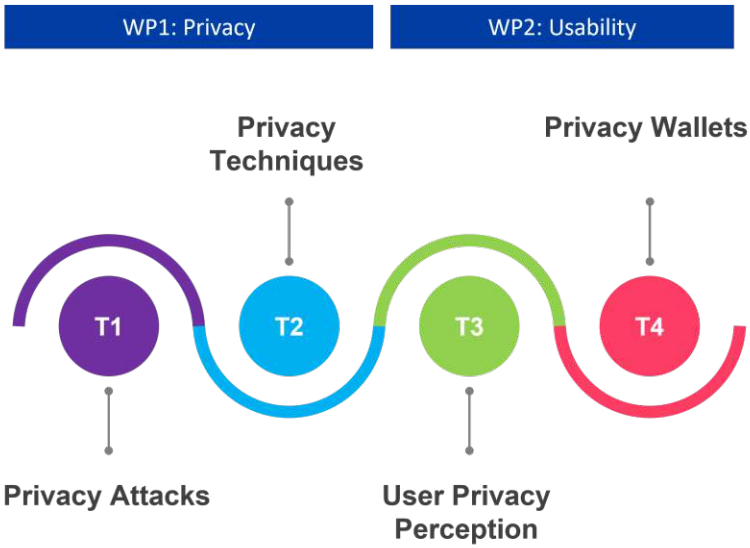


Figure 1.1: Thesis methodology

1.2 Methodology

The methodology for this thesis is structured into two main work packages, the privacy work package, and the usability work package. Each work package includes specific tasks, as illustrated in Figure 1.1. The four defined tasks are classification of privacy attacks, classification of privacy techniques, user privacy perception, and usability of privacy wallets.

1.2.1 Classification of Privacy Attacks and Privacy Techniques

To classify privacy attacks and privacy techniques, we followed the widely recognized Prisma methodology [6], the methodology consists of four main steps:

Research Question Identification: The first step involved formulating clear research questions to guide the literature search and analysis.

Literature Search: To ensure comprehensive coverage of relevant literature, a triangulation approach was adopted, combining various search methods. Manual searches were conducted in scientific databases.

Literature Selection: The papers were then screened based on their titles and abstracts to exclude irrelevant ones. Subsequently, a fast screening process was conducted to further filter the remaining papers.

Analysis and synthesis of extracted data: In the final step, we analyzed and synthesized the data obtained from the selected papers.

The research questions addressed in the privacy work package are as follows.

RQ 1: What are the different categories of Bitcoin privacy attacks, and how can they be classified based on their methods?

RQ 2: What are the potential ramifications of Bitcoin privacy attacks on the security and reliability of digital identity systems, specifically in the case of did:btcr (Decentralized Identifiers over Bitcoin)?

RQ 3: What are the potential countermeasures that can be implemented to protect users from privacy attacks in the context of did:btcr identity applications?

RQ 4: How do existing privacy techniques compare privacy measures, including the anonymity set, unlinkability, untraceability, and transaction value privacy?

RQ 5: To what extent are privacy techniques resilient against security attacks, including theft, denial-of-service (DoS), and Sybil attacks?

RQ 6: How do existing privacy techniques compare in terms of efficiency, considering factors such as the number of interactions with input users, the number of interactions with the recipient, Bitcoin compatibility, direct coin transfer to the recipient, the number of transactions involved, and the minimum required blocks?

1.2.2 User Privacy Perception and Usability of Privacy Wallets

For the investigation of user privacy perception and the usability of privacy wallets, we employed a mixed-method approach that integrated interviews, online questionnaires, and usability testing:

Interviews have been utilized as a research tool, allowing researchers to elicit valuable responses from participants by asking well-crafted questions [7]. Through interviews, deep insights into participants' thoughts, experiences, and needs can be gained, contributing to a comprehensive understanding of user perspectives.

Questionnaires have proven to be effective in gathering large amounts of user data. They involve the collection of information through written forms, which can be administered using traditional paper-based or digital formats [7].

Usability testing, focuses on identifying design flaws by evaluating the ease of use and user experience of a product or service [7].

The research questions addressed in the usability work package are as follows.

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?

RQ 3: How do the selected privacy wallets differ in terms of anonymity set and CoinJoin creation time, and how do these differences impact their overall effectiveness in enhancing transaction privacy?

RQ 4: What are the specific usability issues [8] identified during the cognitive walkthrough and user study in the context of coin mixing within the selected privacy wallets, and how do these issues vary among the wallets?

RQ 5: What are the fundamental design criteria [9] outlined in the learnability walkthrough, and how well do the selected privacy wallets adhere to these criteria in terms of their coin-mixing functionality?

RQ 6: What specific improvements or design changes can be recommended for each wallet based on the results of the cognitive walkthrough and user study?

1.3 Results

The thesis presents an evaluation of the privacy and usability of UTXO-based blockchain, which is essential for improving users' privacy in the context of public blockchains.

In [10], we delved into privacy attacks, establishing a framework to understand the limitations of existing techniques and to identify emerging challenges. This is essential for researchers and developers in their efforts to improve the design and resilience of new privacy techniques. By applying these attacks to blockchain-based applications like decentralized identifiers (DIDs), the thesis uncovers six potential privacy threats. Notably, it was demonstrated how combining Bitcoin public records with auxiliary information, enables advanced heuristics to reveal connections between transactions, identities, and users' addresses. Such information can be valuable for malicious actors or cybercriminals to conduct nefarious activities like ransomware or extortion attacks.

In [11], the comparison of privacy-preserving techniques based on criteria such as privacy, security, and efficiency provides insights into the strengths and weaknesses of each technique, guiding developers to improve their design. In addition, we examined the real-world implementation and practical adoption of these privacy techniques. While the primary aim is to enhance privacy against malicious actors, it is crucial to develop methods that distinguish between illicit transactions and legitimate mixing, ensuring financial privacy without aiding unlawful activities.

In [12], through the study on user perception and preferences for Bitcoin privacy and various add-on privacy techniques, we identified user preferences and priorities when it comes to privacy. The results highlight the importance of developing built-in privacy techniques within blockchain protocols rather than relying on add-on solutions. Furthermore, the results show that users prefer indistinguishable privacy techniques over being flagged by monitoring tools, which is an essential consideration for developers in designing future privacy-preserving techniques.

In [13] a cognitive walkthrough that evaluates the usability of three leading wallets supporting CoinJoin transactions was performed. This is important as it sheds light on the challenges of designing user-friendly wallets, particularly for novice users. The study highlights the need for an intuitive interface that informs users of risks associated with

specific actions. These findings can guide the development of new privacy wallets with improved usability.

The results of this thesis contribute to the understanding and improvement of users' privacy in the context of blockchain technology, particularly on the Bitcoin blockchain. The findings provide insights for researchers and developers to improve the design of privacy-preserving techniques and enhance the user experience of privacy wallets, ultimately leading to greater adoption of privacy-enhancing technologies.

1.4 Structure

The structure of this thesis is organized as follows:

Chapter 2 provides the necessary background and context for the research conducted throughout the thesis. This chapter delves into the main concepts and principles of blockchain technology, particularly UTXO-based blockchains such as Bitcoin. It also reviews the existing literature and state of the art regarding privacy-preserving techniques for blockchain transactions.

Chapter 3 investigates the privacy issues associated with one of the Bitcoin-based applications. The chapter specifically focuses on identifying and evaluating the risks of exposing user identities through the use of a Bitcoin-based DID method. By analyzing Bitcoin privacy attacks and the characteristics of the method, the chapter identifies potential privacy vulnerabilities and suggests possible solutions.

Chapter 4 presents and evaluates various privacy techniques based on predefined criteria. The chapter focuses on evaluating the effectiveness of these techniques in preserving privacy and anonymity in blockchain transactions. It analyzes the techniques' strengths and limitations and provides insights into security, privacy, and efficiency aspects.

Chapter 5 presents users' perception of blockchain privacy. The chapter explores the attitudes, beliefs, and concerns of users regarding the privacy of their blockchain transactions. It also investigates the factors that influence user behavior when making decisions about privacy and anonymity.

Chapter 6 evaluates the usability of wallets that offer CoinJoin transactions, which is one of the most promising privacy-preserving techniques. The chapter examines the usability of these wallets, including ease of use, user experience, and user interface design. By evaluating the usability of these wallets, the chapter provides insights into how to design more user-friendly and intuitive wallets that can increase adoption.

Finally, Chapter 7 summarizes the key findings of the thesis, discusses their implications, and provides recommendations for future research in the field of blockchain privacy and usability. This research emphasizes the need for interdisciplinary approaches to address the challenges and limitations of existing privacy-preserving techniques.

CHAPTER 2

Background and State of the Art

2.1 Introduction

In December 2008, Satoshi Nakamoto [14] published the Bitcoin white paper, which introduced a groundbreaking concept: a peer-to-peer (P2P) electronic cash system. Bitcoin revolutionized the way individuals transact, enabling direct communication and asset exchange without the need for a trusted third party. The system's core currency, bitcoin, is virtual and is associated with cryptographic addresses. Transactions are authorized by digital signatures which are generated using the private keys [15].

Bitcoin operates on a decentralized network where participants are responsible for validating and verifying transaction authenticity. Transactions are grouped into blocks, each identified by a block header and referencing a previous block, creating a chain of interconnected blocks. This sequential linking of blocks forms the blockchain, with the initial block known as the "genesis block" [15]. Figure 2.1 provides a simplified visualization of the blockchain structure.

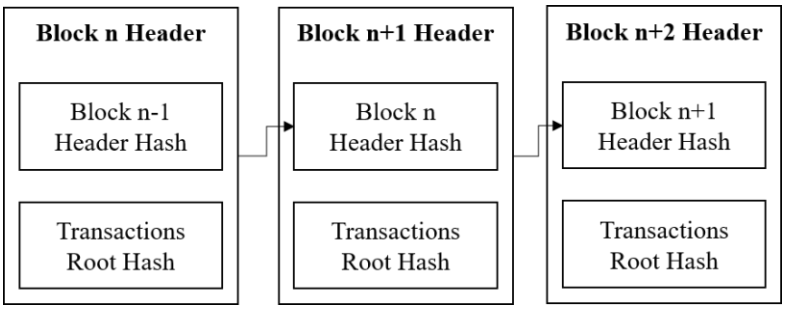


Figure 2.1: Simplified representation of a blockchain

The consensus mechanism, such as the Nakamoto consensus, is crucial for maintaining the consistency and security of the blockchain ledger [16, 17]. To establish a distributed

timestamp server on a peer-to-peer network, in the Nakamoto consensus the concept of proof-of-work is employed. This involves the search for a value that, upon being hashed, starts with a specified number of zero bits. The effort required for this task grows exponentially as the number of zero bits increases, yet a single hash is sufficient for verification [18]. Miners play a vital role in this process by collecting, verifying, and adding transactions to a block. All participants in the network are expected to adhere to the consensus mechanism, which ensures agreement on the order and validity of transactions.

Transactions recorded on a blockchain are distributed, permanent, and verifiable. Once recorded, they become practically immutable, meaning that they cannot be easily altered or removed without significant effort and costs. This immutability ensures the integrity and transparency of the ledger, providing a reliable tamper-resistance record of transactions over time.

2.2 Blockchain fundamentals

2.2.1 Digital signature

In the Bitcoin blockchain, digital signatures play a crucial role in ensuring the authenticity and integrity of transactions. Bitcoin utilizes the Elliptic Curve Digital Signature Algorithm (ECDSA) [19] for generating key pairs, which consist of a private key and the corresponding public key. In this algorithm, the private key is used to create digital signatures, while the public key is used to verify the authenticity and integrity of these signatures.

Public key cryptography, which forms the basis of digital signatures, was first introduced by Diffie and Hellman in 1976 [20]. It ensures that computing the secret key from a public key is computationally infeasible.

Creating a Digital Signature

To create a digital signature for a message (transaction) using the private key, a random public key (K) and private key (k) are generated. This process is similar to address generation. The public key is computed as $K = kG$, where K represents a point on the elliptic curve, denoted as (x, y).

The x coordinate of the public key is considered as r, and the value of s is calculated using the following equation:

$$s = k^{-1}(e + dr) \mod p \tag{2.1}$$

In the equation, k represents the random private key, e is the hash of the message, d is the address's private key, r denotes the x coordinate of the random public key, and p represents the prime order of the base point G.

To verify the signature, the following function is used:

$$(x_1, y_1) = s^{-1}(eG + rQ) \tag{2.2}$$

Here, s and r correspond to the signature pair, G represents the generation point, and Q denotes the public key associated with the address. The signature is considered valid if x_1 is equal to r.

2.2.2 Address

Bitcoin employs asymmetric cryptography, which involves the use of public and private keys. Bitcoin addresses are derived from the hash of the public keys. Users can unlock the coins associated with an address by providing a digital signature computed using the corresponding private key.

In addition to standard addresses based on public key hashes, Bitcoin also supports script hash addresses, also known as Pay-to-Script-Hash (P2SH) addresses. These addresses involve the use of scripts that define the conditions under which the transaction outputs can be spent [15]. The script hash addresses provide enhanced flexibility in defining complex spending conditions.

The use of the ECDSA [21] ensures the security and integrity of the address generation process, enabling secure ownership and control of bitcoins within the blockchain system.

Creating a Bitcoin address

To generate a Bitcoin address in Base58Check format, a random number is chosen as the private key (d). This private key is multiplied by a generator point G on the secp256k1 elliptic curve, which is the standard curve used in Bitcoin [22]. The result is a point (x, y) on the curve, representing the public key (Q) associated with the address [15].

$$Q = dG \tag{2.3}$$

The conversion of the elliptic curve public key to a Bitcoin address involves multiple steps. In Step 1, two one-way hash functions are applied to the public key, i.e., the Secure Hash Algorithm (SHA) and the RACE Integrity Primitives Evaluation Message Digest (RIPEMD). The public key is first hashed using SHA256 [23], and then RIPEMD160 [24] is applied to generate a 160-bit number (20 bytes), known as the HASH160 in the Bitcoin script.

In Step 2, a version prefix is added to the hash result. The version prefix identifies the type of Bitcoin address. Table 2.1 demonstrates some of the Bitcoin version prefixes for different address types.

In Step 3, a 4-byte checksum is appended to the result obtained from Step 2. The checksum is computed by applying the SHA256 hash function twice to the Step 2 result

Table 2.1: Bitcoin address version prefixes

Type	Prefix in Hex	Prefix in Base58
Pubkey hash (P2PKH address)	00	1
Script hash (P2SH address)	05	3
Private key (WIF, uncompressed pubkey)	80	5
Private key (WIF, compressed pubkey)	80	K or L
BIP32 pubkey	0488B21E	xpub
BIP32 private key	0488ADE4	xprv
Bech32 pubkey hash or script hash		bc1

and selecting the first 4 bytes. To enhance human readability and prevent errors during address entry [15], the 25-byte binary address obtained from Step 3 is encoded using the Base58Check encoding scheme [25].

Finally, in Step 4, the Base58Check encoding is applied to the 25-byte binary address, resulting in a Bitcoin address typically represented by 26-35 alphanumeric characters (e.g., 1FtmFgk83NudNmjnCQpv8ss4eHXLmzeUoh). The process of generating a Bitcoin address is illustrated in Figure 2.2. It is worth noting that users can create any number of addresses for free within the Bitcoin system [26, 27].

2.2.3 Transaction

Bitcoin employs a graph-based ledger model centered around unspent transaction outputs (UTXOs). This approach aligns effectively with the concurrent and distributed nature of blockchains [29]. A transaction in Bitcoin involves the transfer of value from address(es) to another [17]. It utilizes UTXOs owned by the sender as input(s) and assigns the recipient's address(s) as the output(s). Additionally, a new address, referred to as a "change address", is created to receive any remaining coins and is also included as an output in the transaction. A transaction comprises various attributes, including a transaction ID, version number, inputs, outputs, and nLockTime (a parameter specifying the time before which the transaction cannot be accepted into a block). Each input references the output of a previous transaction. To prevent double-spending [30], Bitcoin maintains a list of UTXOs [31]. Once an output is spent, it is automatically removed from the list.

Transaction Fee

In order to deter flooding attacks, which have been widely employed by attackers as a conventional method for denying services [32], Bitcoin introduces transaction fees to

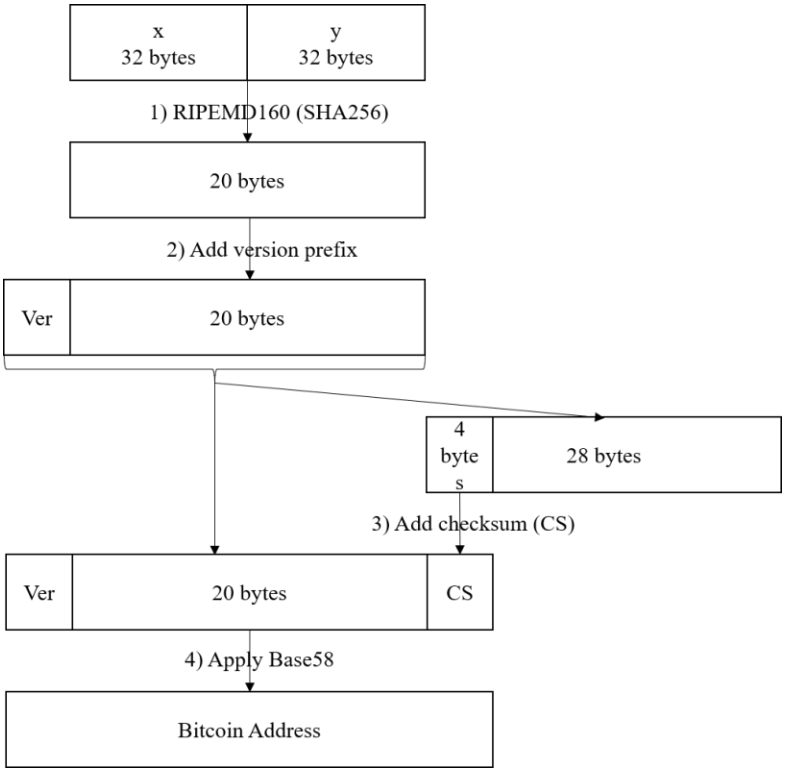


Figure 2.2: Bitcoin address generation, adapted from [28]

miners for the transaction to be included in a block. This fee is calculated by subtracting the sum of the input values from the sum of the output values [27]. It is important to note that larger transactions often necessitate higher fees in order to be confirmed promptly [33].

Transaction Scripts

The Bitcoin script [34] is a stack-based language called Script, resembling Forth [35]. Script words, also known as "operation codes" (opcodes), are prefixed with "OP_". A comprehensive list of opcodes can be found in [34]. The design of Bitcoin script emphasizes simplicity and efficient execution on most hardware platforms, requiring minimal processing [15]. Transactions utilize scripts to specify the conditions under which the coins can be spent [33]. The majority of Bitcoin transactions employ a pay-to-public-key-hash (P2PKH) script [36]. However, Bitcoin supports other script types that enable more complex spending conditions, such as pay-to-script-hash (P2SH) [37] and multi-signature [38, 39].

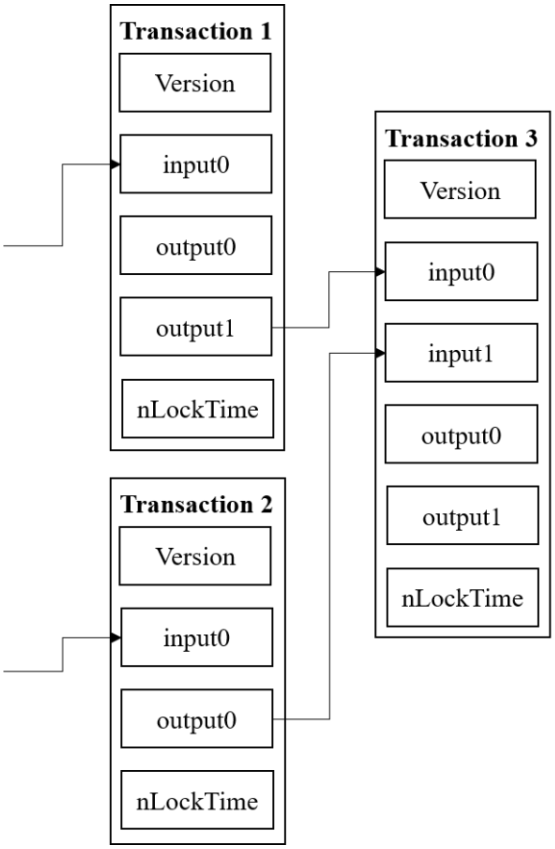


Figure 2.3: The relationship between transaction inputs and outputs [28]

Pay-to-Public-Key-Hash (P2PKH)

P2PKH [36] locks the output of a transaction to a public key hash, which serves as the recipient's address. When the recipient receives coins in her address, she can spend them by providing the public key and a valid digital signature of her address. This process is commonly known as spending the coins. A sample P2PKH script is demonstrated below, illustrating how Alice can unlock the coins she previously received in her Bitcoin address. The locking script of the output takes the following form:

```
OP_DUP OP_HASH160 <A pubkey Hash>
OP_EQUALVERIFY OP_CHECKSIG
```

To unlock the script, Alice's signature and Alice's public key are added to the beginning of the locking script, resulting in the following:

```
<A sig> <A pubkey> OP_DUP OP_HASH160
<A pubkey Hash> OP_EQUALVERIFY OP_CHECKSIG
```

If Alice provides a valid signature, the script will evaluate to be true. In other words, P2PKH is a script that requires the recipient to provide a valid signature over the public key to unlock the coins associated with that public key [15]. The execution of this script follows the steps outlined below:

1. Alice's signature (<A sig>) is pushed onto the stack.
2. Alice's public key (<A pubkey>) is pushed onto the stack, on top of <A sig>.
3. OP_DUP duplicates <A pubkey>, pushing two identical public keys onto the stack.
4. OP_HASH160 takes the top item from the stack, computes the RIPEMD160 hash of the SHA256 hash of <A pubkey>, and pushes the resulting hash onto the stack.
5. <A pubkey Hash>is pushed onto the stack.
6. OP_EQUALVERIFY compares the top two items on the stack, removing them if they are equal.
7. OP_CHECKSIG verifies whether <A sig>is a valid signature for <A pubkey>. If the check is successful, both <A sig>and <A pubkey>are popped from the stack, and TRUE is pushed onto the stack.

The P2PKH unlock script is illustrated in Figure 2.4.

Pay-to-Script-Hash (P2SH)

P2SH [37] facilitates payments involving complex scripts by utilizing a hash of a more complex script in the locking script. P2SH makes transactions as easy as P2PKH by enabling users to pay to a script that matches a hash of the script, which serves as a condition to unlock the output. The complex script that is replaced by a hash in P2SH is commonly referred to as the redeem script [15].

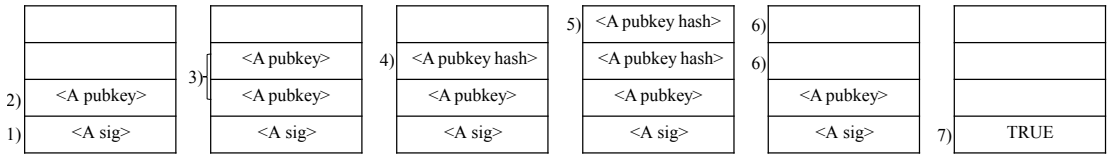


Figure 2.4: P2PKH unlock script

Multi-Signature Transaction (Multisig)

A multisig transaction [38, 39] is a type of P2SH transaction that requires multiple signatures to be performed. It is also known as M-of-N multi-signature transaction. The script of a multisig transaction includes N public keys, and the transaction can be spent if at least M signatures corresponding to these public keys are provided [40]. Some use cases for multisig transactions include shared wallets, escrow services, and corporate accounts [38].

Using a P2SH script which involves a larger number of participants typically requires higher fees, and is formed as follows:

Redeem script:

```
<OP_2> <A pubkey> <B pubkey> <C pubkey> <D pubkey>
<E pubkey> <OP_5> OP_CHECKMULTISIG
```

Lock script:

```
OP_HASH160 <Hash160(redeemScript)> OP_EQUAL
```

Unlock script:

```
OP_0 <A sig> <C sig> <redeemScript>
```

The presence of OP_0 at the beginning of the unlock script is related to a bug in the execution of CHECKMULTISIG. To resolve this bug, OP_0 is included at the beginning of multisig scripts [15].

Including multiple signatures in a multisig transaction adds an extra layer of security and allows for shared control over the funds, mitigating the risk of a single point of failure. Additionally, multisig transactions provide protection against the loss of coins in case one of the keys is lost.

Timelock Transaction

A timelock transaction [41] imposes a restriction on spending the coins until a specified time, making it useful for refund purposes. The specified time can be defined either in terms of block height or a specific point in time.

Hashlock Transaction

A hashlock transaction [42] is locked by a hash and can only be spent by providing the pre-image of the hash. The pre-image refers to the original data that was hashed and included in the unlocking output condition. It is important to note that multiple transactions can be locked by the same hash. These transactions are not publicly disclosed

unless a user acts maliciously. Once one of the transactions is unlocked, revealing the hash on the blockchain, all transactions locked with that hash can be redeemed [40]. By combining a signature and a pre-image of the hash, the hashlock transaction provides an additional layer of security and prevents unauthorized redemption of the locked coins.

The condition of a Hashlock transaction is typically represented as:

Lock script:

```
<data> OP_HASH256 <data_hash> OP_EQUAL
```

Hash-Time-Locked Contracts (HTLC)

Hash-Time-Locked Contract (HTLC) [43] provides a mechanism for creating conditional payments in cryptocurrency transactions, enabling secure and trustless operations between parties, even in the presence of time delays or other predetermined conditions. HTLC utilizes both hashlock [42] and timelock [41] transactions. In an HTLC, the output is locked by a hash, and if the recipient fails to unlock it within a specific period, the coins are automatically returned to the sender.

A simplified form of HTLC, adapted from [44], is as follows:

```
OP_IF
OP_HASH160 <data_hash> OP_EQUALVERIFY
OP_DUP OP_HASH160 <recipient_pubkey_hash>
OP_ELSE
<locktime> OP_CHECKLOCKTIMEVERIFY OP_DROP
OP_DUP OP_HASH160 <sender_pubkey_hash>
OP_ENDIF
OP_EQUALVERIFY
OP_CHECKSIG
```

The first part of the script unlocks the output by providing data that matches the data hash, while the second part allows for a refund to the sender after a specified lock time.

Figure 2.5 illustrates an example of an HTLC transaction. In this scenario, Bob can fulfill the transaction by providing the pre-image (x) and his signature, while Alice can initiate a refund via the refund transaction T_R after the locktime expires.

In Figure 2.5, σ_A represents Alice's signature, σ_B represents Bob's signature, T_O represents the offer transaction, T_R represents the refund transaction, and T_F represents the fulfill transaction.

2.2.4 Bitcoin Network

In the context of blockchain-based systems like Bitcoin, there are three key participants: mining nodes, full nodes, and clients. Full nodes play a crucial role in storing and

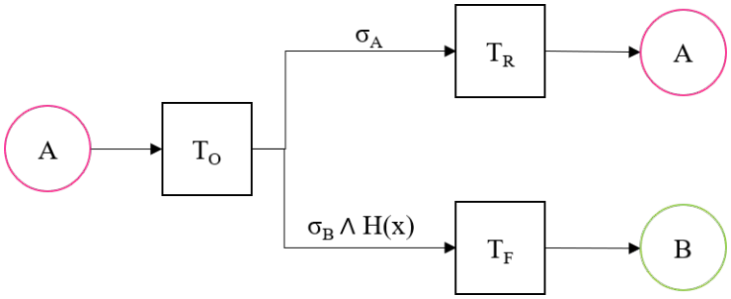


Figure 2.5: Hash Time Locked Contracts (HTLC)

transmitting blockchain data. They maintain a complete copy of the blockchain and validate transactions, thereby ensuring the integrity of the system. On the other hand, clients interact with the Bitcoin network by submitting queries and transactions. However, clients with limited resources may rely on full nodes to verify the accuracy of the blockchain. In the early stages of Bitcoin, these roles were not distinct, but later, the introduction of the Simplified Payment Verification (SPV) protocol [18] allowed less powerful clients to participate in the network. Despite the benefits of SPV, it still requires significant resources and introduces additional trust assumptions and potential attack vectors [45]. To add transactions to the blockchain, specialized nodes, known as miners, compete to mine new blocks. These blocks contain validated transactions along with the hash of the previous block. On average, miners generate a new block approximately every 10 minutes. Once a miner successfully mines a block, it propagates the block data across the permissionless peer-to-peer network, disseminating it to all other nodes.

The process of block propagation involves nodes quickly validating and transmitting new blocks to their peers, who, in turn, validate and propagate the blocks further. This continues until the entire network is updated with the latest block. Efficient block propagation is crucial for the scalability and performance of the Bitcoin network.

To address the challenge of block propagation latency, the Bitcoin protocol introduced a mechanism called compact block relaying [46] in 2016. This mechanism aims to reduce the time it takes to propagate blocks across the network by minimizing the amount of data that needs to be transmitted. By employing efficient data compression techniques and transmitting only the necessary information, compact block relaying significantly improves block propagation efficiency [47]. This optimization is crucial in enabling faster synchronization of nodes and enhancing the overall efficiency of the Bitcoin network.

2.2.5 Bitcoin Wallet

A Bitcoin wallet, whether hardware or software-based, plays a crucial role in facilitating users to effectively manage their cryptographic keys and addresses, as well as interact with the blockchain to execute and authorize transactions [15]. While the primary function of a wallet is to facilitate the sending and receiving of bitcoin to and from other

users, the concept of a privacy wallet takes it a step further by incorporating advanced privacy-enhancing techniques to protect user privacy and anonymity.

A multitude of Bitcoin wallets were created. The leading desktop wallets adhering to privacy criteria as outlined on the bitcoin.org wallets page were sought after. The results are visually represented in Figure 2.6. Remarkably, identical outcomes were produced for the selection of Windows and privacy criteria. In our search, wallets that had received a "Good" ranking in the majority of features were specifically opted for. As a result, the top desktop wallets listed on bitcoin.org were Bitcoin Core, Bitcoin Knots, Armory, Specter, Sparrow, and Wasabi.

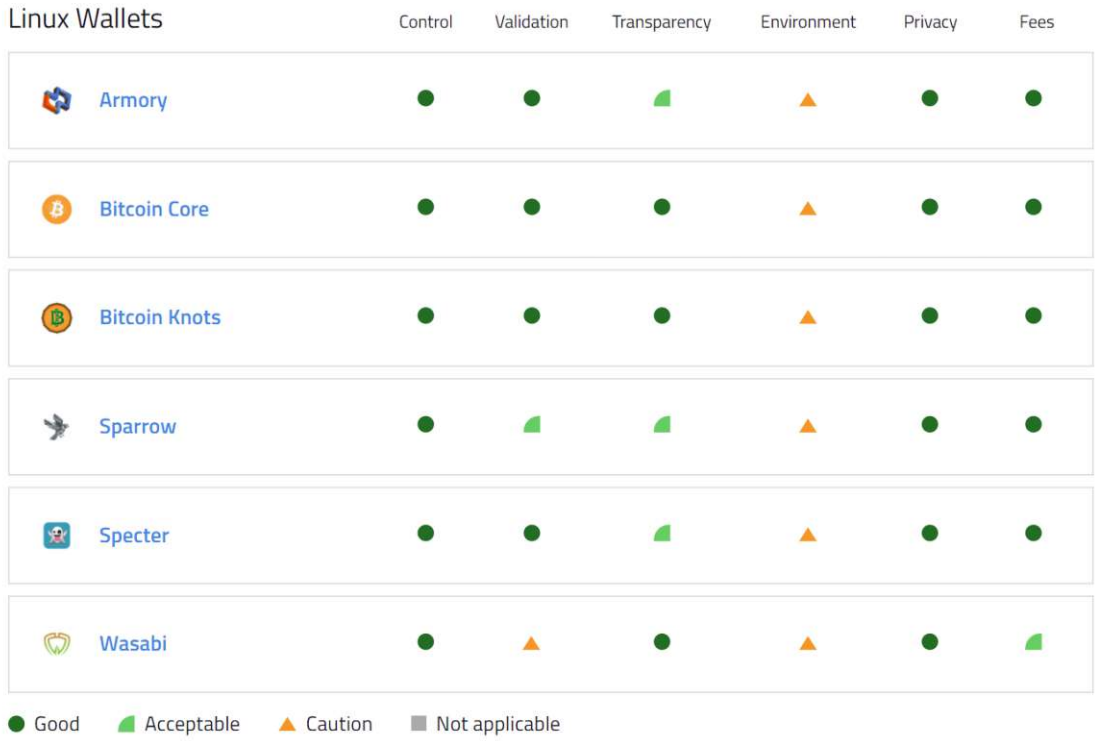


Figure 2.6: Bitcoin Desktop Wallets with Good Privacy Criteria
https://bitcoin.org/en/choose-your-wallet

2.3 Bitcoin Privacy

The public nature of the Bitcoin blockchain raises concerns about privacy for its users. By employing a combination of heuristics and information from external sources such as forums and online shops, transactions can be clustered, potentially revealing the identities of the involved users.

The concept of “anonymity” in the context of blockchain is subject to interpretation and

uncertainty. Pfitzmann and Hansen [48] proposed a definition of anonymity as the state where a subject cannot be identified within a set of subjects, known as the anonymity set. It is important to note that Bitcoin does not provide complete anonymity, as numerous studies [1, 2, 3, 49, 4] have demonstrated successful de-anonymization by linking Bitcoin addresses to real-world entities.

In recent years, several research works have focused on de-anonymizing users on the Bitcoin blockchain. Meiklejohn et al. [2] clustered Bitcoin wallets based on evidence of shared authority and employed re-identification attacks to classify users within these clusters. They concluded that the information collected by Bitcoin businesses, such as exchanges, combined with the ability to trace monetary flows to these entities, discourages illicit activities involving Bitcoin. Reid and Harrigan [1] analyzed anonymity in Bitcoin by examining the topological structure of two networks derived from Bitcoin's public transaction history. Their study revealed various forms of information leakage that contribute to de-anonymizing Bitcoin users, utilizing flow and temporal analysis to visualize and identify over 60% of the users and their relationships. Harrigan and Fretter [3] investigated the factors contributing to the effectiveness of simple heuristics in Bitcoin, including address reuse, avoidable merging, super-clusters with high centrality, and the growth of address clusters. Ermilov et al. [49] incorporated off-chain information as votes for address separation and combined it with blockchain data in their clustering model. They applied blockchain-based heuristics such as "common input ownership" and detected change addresses, alongside off-chain information, for address clustering. Jourdan et al. [4] proposed features for classifying entities on the Bitcoin blockchain based on a graph neighborhood perspective, including centrality and temporal features. Their approach successfully classified addresses into categories such as exchanges, gambling services, general services, and darknet-related entities.

Moser et al. [50] emphasized the significance of accurate address clustering in blockchain technology for several key applications. First, law enforcement agencies require reliable heuristics to identify relevant transactions. Second, accurate determination of user transactions is crucial for preserving privacy. Third, complete clustering of all addresses on the blockchain is necessary for aggregate analyses. Fourth, address clustering is valuable for machine learning research, as it presents unique challenges and serves as a benchmarking application.

The findings of the aforementioned research underscore the importance of enhancing privacy on the Bitcoin blockchain through effective techniques.

Various privacy-enhancing techniques have been proposed for Bitcoin, including centralized mixers, atomic swaps, CoinJoin-based mixing, and threshold signatures. Centralized mixers rely on a trusted third party to facilitate transaction mixing. Atomic swaps enable decentralized coin exchanges between two parties. CoinJoin-based mixing techniques allow users to jointly participate in a transaction, effectively obfuscating the relationship between sender and recipient addresses. Threshold signatures enable multiple peers to collaboratively sign a transaction from a shared address under their control.

In the subsequent chapters, we will delve into a detailed exploration of privacy attacks on the Bitcoin blockchain and examine various privacy-preserving techniques that have been proposed to address these concerns.

2.4 Usability in Blockchain

User research plays a crucial role in informing the design process, ensuring that products and services meet the needs and expectations of their intended users. In the context of evaluating blockchain security and privacy, as well as wallet usability, several user research methods have been employed. The researchers applied methods such as interviews, questionnaires, and usability testing.

2.4.1 Understanding User Perspectives

The usability of blockchain systems, particularly in relation to security and privacy, has garnered significant attention in previous research [51, 52, 53]. These studies have shed light on the limited understanding of users regarding blockchain privacy issues, revealing a lack of awareness regarding the necessity of privacy techniques and the means to mitigate de-anonymization risks.

Krombholz et al. [51] conducted a user study focused on Bitcoin security and privacy, unveiling a substantial gap in users' comprehension of how to maintain privacy and anonymity while using Bitcoin. Surprisingly, over one-third of the participants believed that Bitcoin provided complete anonymity. Similarly, Fabian and Ermakova [52] found that approximately 18% of users were oblivious to the risk of being de-anonymized on the blockchain, while half of the participants were aware of the risks and expressed concern. Additionally, they investigated users' familiarity with privacy-preserving techniques such as CoinJoin and discovered that half of the participants were unfamiliar with it.

Mai et al. [53] conducted a qualitative user study on the mental models of cryptocurrency systems. The findings indicated that users generally assume their transactions are anonymous and encrypted, leading them to believe that the data is not publicly readable. However, users expressed concerns about address mapping as a potential privacy threat, and identity disclosure through third-party services was also reported. Another study by Voskobojnikov et al. [54] investigated the risk management of cryptocurrencies through interviews with both cryptocurrency users and non-users. The research revealed that misunderstandings among both groups can influence the effectiveness of risk mitigation strategies.

While previous studies [51, 53, 54] primarily focused on security and privacy aspects, they primarily examined Bitcoin's anonymity and network privacy aspects. However, they overlooked potential privacy attacks such as timing and amount correlation. Furthermore, these studies did not explore privacy wallets and users' preferences regarding additional fees and delays associated with privacy-enhancing techniques.

2.4.2 Evaluating Usability of Cryptocurrency Wallets

Usability research in key management [55, 56] has established a clear methodology for evaluating systems usability. This approach involves defining specific tasks and conducting expert cognitive walkthroughs to assess interfaces' learnability. For instance, Eskandari et al. [56] performed usability research on Bitcoin key management, employing an evaluation framework and cognitive walkthroughs to compare different key management approaches based on their usability criteria. Ljunggren [9] defined evaluation criteria inspired by Norman [57] to assess the top five Ethereum mobile wallets. They conducted a user study to evaluate these wallets and provided an application structure to enhance them based on their findings. The usability of the Zcash wallet was examined in [58], revealing that many users struggled to purchase real items using the wallet due to installation complexities and challenges in integrating the wallet with network-level protection tools. Additionally, an analysis of the top five mobile cryptocurrency wallet reviews in [59] highlighted significant user experience (UX) shortcomings and misconceptions that can result in critical errors and fund loss.

In the subsequent chapters of this thesis, We will explore the usability aspects of blockchain systems with a focus on addressing privacy concerns.

In the next chapter, we examine various privacy attacks on Bitcoin and evaluate their privacy impact on one of the Bitcoin-based applications such as decentralized identities DIDs. We categorize the attacks and analyze their implications for the privacy of a DID method, namely did:btcr, and discuss its overall privacy properties.

CHAPTER 3

Privacy Attacks in Bitcoin: Implications for Bitcoin-based Identity Methods

3.1 Introduction

The introduction of the Bitcoin blockchain has revolutionized distributed ledger systems, offering a transparent platform for accessing and verifying historical data by anyone. This openness has led to new applications, transforming traditional systems to meet modern business needs, such as transparency, censorship resistance, and decentralization. One groundbreaking application is the use of blockchain for decentralized and self-sovereign identities, allowing innovative identity management in a trustless environment.

However, the transparency of the Bitcoin blockchain comes with privacy risks, exposing users to potential privacy breaches and identity de-anonymization. This has resulted in sophisticated privacy attacks that exploit the system's openness. As a result, safeguarding confidentiality and anonymity in Bitcoin-based identity systems has become a critical challenge in the blockchain landscape.

In this chapter, we extensively explore privacy attacks targeting the Bitcoin blockchain. We aim to understand the methods employed by these attacks and their potential impact on Bitcoin-based identity applications, with a specific focus on the did:btcr (Decentralized Identifiers over Bitcoin) identity method. This widely-used approach for creating decentralized and self-sovereign identities serves as a valuable case study to analyze the effects of privacy attacks on digital identity systems.

To conduct a thorough analysis, we will use a structured framework to shed light on the complexities of these attacks and their implications for the security and privacy

of digital identities within the blockchain ecosystem. Our goal is to pave the way for stronger privacy measures and robust identity management solutions in the ever-evolving landscape of blockchain technology.

The research questions addressed in this chapter are as follows.

RQ 1: What are the different categories of Bitcoin privacy attacks, and how can they be classified based on their methods?

RQ 2: What are the potential ramifications of Bitcoin privacy attacks on the security and reliability of digital identity systems, specifically in the case of did:btcr (Decentralized Identifiers over Bitcoin)?

RQ 3: What are the potential countermeasures that can be implemented to protect users from privacy attacks in the context of did:btcr identity applications?

In Chapter 2, we briefly discussed the utilization of sophisticated heuristics and auxiliary information, such as address tag databases, to correlate Bitcoin addresses with real-world identities, thereby compromising user privacy. In Section 3.3, we categorize privacy attacks on the Bitcoin blockchain that can expose the links between addresses and real-world identities, as well as correlate different identities. We specifically investigate the impact of these attacks on the did:btcr blockchain application. To achieve this, we adopt the terminology outlined in RFC 6973 [60].

This chapter is structured as follows: Section 3.2 presents the methodology employed in this research. Section 3.3 categorizes the privacy attacks discussed in the relevant research papers. Section 3.4 evaluates Bitcoin privacy threats and proposes possible mitigation. Section 3.5 provides an overview of the main concepts related to decentralized identifiers (DIDs). Subsequently, Section 3.6 delves into the investigation of privacy issues specific to the did:btcr method. Finally, Section 3.7 concludes the chapter by summarizing the key findings and providing suggestions for future research directions.

3.2 Methodology

In this section, we outline the methodology employed to collect and select relevant literature on categorizing privacy attacks. The research followed the PRISMA methodology [6], a widely recognized set of instructions for carrying out systematic reviews and meta-analyses. The methodology consisted of four main steps illustrated in Figure 3.1 : (i) planning and identifying research questions, (ii) conducting a literature search, (iii) selecting relevant literature, and (iv) analyzing and synthesizing extracted data.

3.2.1 Planning:

The first step involved formulating clear research questions to guide the literature search and analysis. The research questions specified in 3.1 aimed to explore privacy attacks in the context of blockchain technology, specifically focusing on the Bitcoin blockchain.

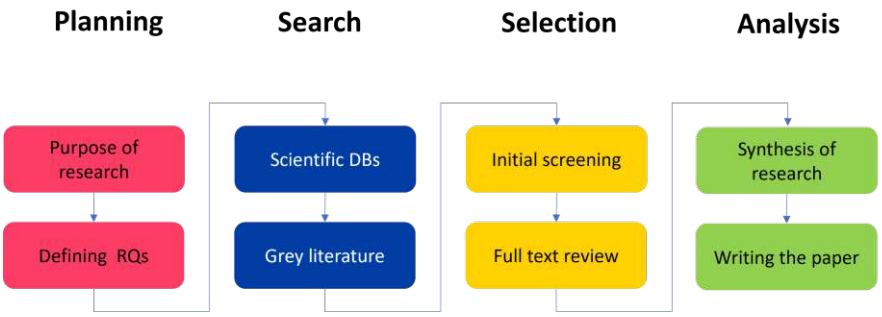


Figure 3.1: Methodology

3.2.2 Literature Search:

To ensure comprehensive coverage of relevant literature manual searches were conducted in scientific databases. Additionally, citation searches were performed to identify additional sources. The search focused on top conferences and journals in the fields of Distributed Ledger Technology and decentralized identity.

Search Query: In total, we gathered four terms related to blockchain and six terms associated with privacy attacks. The search query incorporated various keywords, such as "Bitcoin," "blockchain," "distributed ledger technology," "DLT," "privacy," "attack(s)," "anonymity," "deanonymization," "correlation," and "linkability." To ensure meaningful results, the search was confined to the title, abstract, and keywords. The search query was as follows: "Bitcoin" OR "blockchain" OR "distributed ledger technology" OR "DLT" AND "privacy attack" OR "anonymity" OR "deanonymization" OR "correlation" OR "linkability".

Inclusion criteria: We utilized various scientific and engineering databases and libraries, including IEEE Xplore, ACM, Elsevier, Usenix, NDSS, and Springer. Only peer-reviewed scientific research papers published in the top 20 computer security and cryptography publications, determined by h5-index and h5-median, were included.

Table 3.1 presents a list of the identified venues, ordered by their h5-index and h5-median. These venues represent prominent conferences and journals in the field, ensuring the inclusion of high-quality research publications.

3.2.3 Literature Selection:

Exclusion criteria: We limited our research to the papers published after 2009, as Bitcoin was implemented in 2009. As this survey was conducted in 2021, the search was then limited to papers published between 2009 and 2021, ensuring the inclusion of recent research. We did not consider an article if the title, abstract, or keywords did not relate to the Bitcoin blockchain.

Quality assessment: We considered works that satisfy the following assessment criteria:

	Publication	h5-index	h5-median	Publisher
1	ACM Symposium on Computer and Communications Security	88	140	ACM
2	IEEE Transactions on Information Forensics and Security	86	118	IEEE
3	USENIX Security Symposium	80	129	USENIX
4	IEEE Symposium on Security and Privacy	74	142	IEEE
5	Network and Distributed System Security Symposium (NDSS)	71	111	NDSS
6	International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT)	61	89	SPRINGER
7	Computers & Security	59	90	ELSEVIER
8	IEEE Transactions on Dependable and Secure Computing	54	77	IEEE
9	International Cryptology Conference (CRYPTO)	52	87	SPRINGER
10	International Conference on Financial Cryptography and Data Security	46	74	SPRINGER
11	International Conference on The Theory and Application of Cryptology and Information Security (ASIACRYPT)	42	61	SPRINGER
12	Security and Communication Networks	40	51	Wiley
13	Theory of Cryptography	38	58	SPRINGER
14	ACM on Asia Conference on Computer and Communications Security	37	55	ACM
15	Proceedings on Privacy Enhancing Technologies	35	55	
16	IEEE European Symposium on Security and Privacy	34	74	IEEE
17	Designs, Codes and Cryptography	34	50	SPRINGER
18	European Conference on Research in Computer Security	34	43	SPRINGER
19	IEEE Security & Privacy	31	53	IEEE
20	Journal of Information Security and Applications	31	40	ELSEVIER

Table 3.1: Computer security and cryptography top publications

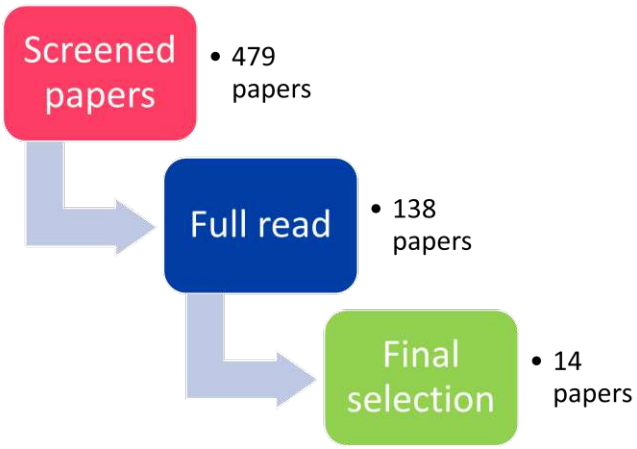


Figure 3.2: Literature selection

- Identification of privacy attacks or de-anonymization heuristics
- Inclusion of implementation and data analysis

The initial search yielded a total of 479 papers. These papers were then screened based on their titles and abstracts in order to exclude irrelevant items and 136 papers were selected. Subsequently, a fast screening process was conducted to further filter the remaining papers. Through this iterative selection process, 14 papers were identified that specifically focused on privacy attacks on the Bitcoin blockchain.

A number of the selected studies have identified privacy attacks that could potentially reveal links between identities and Bitcoin addresses. In the following sections, we categorize and explain the various possible attacks that have been discussed in the selected papers (see Table 3.2). Based on the purposes outlined in the papers, we have classified them into five categories: privacy challenges, classification, illicit activities (tracking Bitcoin usage on the dark web, ransomware, and Ponzi schemes), linking

Category	Paper	Year	Publication	Purpose	Blockchain
Privacy challenges	[61]	2018	IEEE S&P	Access privacy challenges	BTC, ZEC
Classification	[62]	2014	FC	User classification	BTC
	[63]	2020	USENIX	Analysis tool	BTC, BCH, BSV, LTC, and ZEC
Illicit activites	[64]	2018	Computer & Security	Tracking ransomware	
	[65]	2018	IEEE S&P	Tracking ransomware	BTC
	[66]	2019	NDSS	Crypto in dark web	BTC
	[67]	2020	Asia CCS	MMM ponzi detection	BTC
Link Pseudonyms to IPs	[68]	2014	FC	Link Pseudonyms to IPs	BTC
	[69]	2014	CCS	Link Pseudonyms to IPS	BTC
	[70]	2017	FC	Clustering heuristics+network layer info	BTC
	[71]	2019	EuroS&P	Link Pseudonyms to IPs	BTC, ZEC, XMR, Dash
Pattern detection	[72]	2017	EuroS&P	Remuneration detection	BTC
	[73]	2019	CCS	Tracing trading transactions	BTC
	[74]	2019	USENIX	Tracing trading transactions	ETH, BTC, LTC, BCH, Doge, Dash, ETC, ZEC

Table 3.2: Selected papers

pseudonyms to IPs, and pattern detection (identifying specific patterns related to user behavior in trading systems and remuneration patterns).

3.2.4 Analysis and synthesis of extracted data:

In the final step, we analyzed and synthesized the data obtained from the selected papers.

After finding the privacy attacks, we classified the identified privacy attacks into distinct privacy threat classes. We not only outline the associated risks but also offer mitigation strategies and countermeasures (refer to 3.4, for more details). Our categorization scheme closely aligns with the six principal threat categories of LINDDUN GO. We adopted the definitions for these categories from [75], encompassing concepts such as linkability, identifiability, non-repudiation, detectability, unawareness, and non-compliance."

3.3 Bitcoin privacy attacks

In this section, we provide an overview of the heuristics and de-anonymization techniques utilized to compromise privacy on the Bitcoin blockchain.

3.3.1 Bitcoin Blockchain Heuristics

Bitcoin blockchain heuristics are methods applied to the Bitcoin blockchain data to identify relationships between addresses. These heuristics leverage patterns and characteristics of transactions to make inferences about address ownership. In the following, we present the commonly employed heuristics on the Bitcoin blockchain, including common input ownership, change address detection, address reuse, single input-single output, and specific patterns.

Multi/Common Input Ownership

In Bitcoin, it is possible to add and combine multi inputs in a transaction. The multi/common input ownership heuristic assumes that the inputs of a transaction are controlled by the same entity and associates all the inputs to one entity. Since the inputs of a transaction can only be redeemed by providing their signatures, it is unlikely that

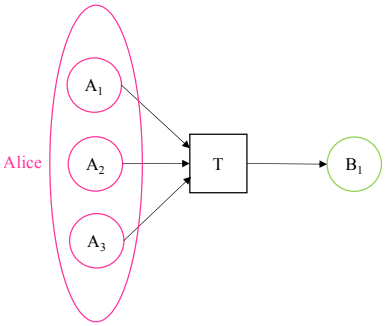


Figure 3.3: Multi/common input ownership heuristic

different users collaborate to create a transaction [26]. Figure 3.3 illustrates this heuristic, assuming that all the addresses (A_1, A_2, A_3) are controlled by one entity (Alice).

To prevent false positives, CoinJoin transactions are excluded from the analysis [63]. CoinJoin [76] is one of the most prominent mixing techniques adopted in practice. In mixing techniques, users combine their unspent transaction outputs (UTXOs) with those of other users to obscure the relationships between inputs and outputs. In CoinJoin, users collaborate to create and sign transactions, blurring the common input ownership heuristic. CoinJoin transactions should be structured with equal-size outputs to prevent linking input and output addresses.

Change address

In Bitcoin, a fresh address, referred to as a "change address", is created to receive any remaining coins from the sender of the transaction. This heuristic assumes that the owner of the inputs controls the change address of a transaction [2]. The following is a list of common heuristics that are employed to identify change addresses.

- *Fresh address:* A fresh address output can be considered a change address if the other output has been observed previously in the blockchain [2].
- *Script types:* If all the inputs have similar scripts (e.g., Pay-to-PubkeyHash (P2PKH), Pay-to-Script-Hash (P2SH)), the only output with a similar script can be identified as a change address [77].
- *Same input and output:* An input address that is also an output address of the transaction can be flagged as a change address [77].
- *UIH1 (Optimal change address):* The *optimal change* heuristic was introduced to detect the change address of a transaction with multiple inputs and outputs. It has been implemented by blockchain analysis tools such as blocksci [63] to cluster addresses. This heuristic flags the smallest output as a change address if it is smaller than the smallest input [63].

  - **BlockSci UIH1** [63]: *"If there exists an output that is smaller than any of the inputs it is likely the change."*[1]
  - **BlockStream UIH1**[2]: *"This heuristic gives an indication that one output is more likely to be a change because some inputs would have been unnecessary if it was the payment."*
  - **Gibson UIH1** [78]: *"One output is smaller than any input. This heuristically implies that output is not a payment, and must therefore be a change output."*

- *UIH2 (Unnecessary Input):* This heuristic identifies transactions as abnormal compared to the typical payment transactions when the largest output could be covered without the need for the smallest input.
  - **BlockSci UIH2** [63]: *"If a change output was larger than the smallest input, then the coin selection algorithm would not need to add the input in the first place."*[3]
  - **BlockStream UIH2**: *"If the sum of the inputs minus minimum input covers the larger output and transaction fee, the transaction has seemingly unnecessary inputs that are not typically added by consumer wallet software with a less sophisticated coin selection algorithm."*
  - **Gibson UIH2** [78]: *"One input is larger than any output. This heuristically implies that this is not a normal wallet-created payment."*

- *Round numbers:* Non-round number output values can be considered change addresses since payment amounts are typically rounded [77, 79].

- *Wallet fingerprinting:* Different wallets create transactions in a distinct manner, which can be used to reveal change addresses [79]. For example, characteristics such as the change output index or using lock time can be matched to identify the change address [77]. When arranging the inputs and outputs of a transaction, some wallets position the change output in the final index, simplifying the process of identifying the change.

- *Peeling chain:* In peeling chain transactions, where a single address with large amounts pays small amounts to other addresses, the output that continues the peeling process can be identified as a change address [77].

Address Reuse

Address reuse occurs when the same address is used in multiple transactions. This practice can lead to a correlation between all transactions associated with the reused

[1] We consider the BlockSci definition in a simpler form, ignoring the transaction fee for data categorization.

[2] https://github.com/Blockstream/esplora/blob/cbed66ecee9f468802cf1f073c204718beac30d7/client/src/lib/privacy-analysis.js#L47-L70

[3] A comprehensive definition can be considered as $(sum(in) - min(in) >= sum(out) - min(out) + TX.fee)$

address, potentially compromising the privacy of the user [80]. When an address is reused, it becomes possible to link all the transactions in which the address has previously appeared. This linkage creates a potential vulnerability for privacy, as it enables the tracing and analysis of transactions related to the same address.

Forced address reuse is another technique that attackers can employ to uncover additional UTXOs (Unspent Transaction Outputs) belonging to a user. In this scenario, the attacker pays a small amount of bitcoin to an address associated with the target user and then tracks the address in the blockchain to identify other UTXOs controlled by the same user. If the target combines this newly received UTXO with their other UTXOs in subsequent transactions, it becomes possible to associate them with the user as well [79]. This forced address reuse technique further threatens users' privacy by potentially revealing more of their transaction history.

Single Input-Single Output

Transactions that involve only one input and one output are often referred to as self-payments. In such transactions, the input and output addresses can be associated with the same entity. However, it is important to note that most payment transactions typically involve multiple inputs and outputs, making it more difficult to directly link the addresses to a single user or entity [63].

Specific patterns

In addition to the previously discussed heuristics, specific patterns extracted from user and transaction behaviors can be utilized to identify relationships and potentially compromise privacy on the Bitcoin blockchain.

Researchers have explored various patterns to uncover associations among addresses. For example, in [72], remuneration patterns were identified through the analysis of ground truth data. This analysis revealed patterns in how users receive payments and provided insights into address correlations. Similarly, in [74], common relationships between addresses within trading services were discovered. Receiving coins from the same address or sending coins to the same address can indicate a social relationship or connection among users involved in trading activities.

Table 3.3 summarizes the aforementioned heuristics on the Bitcoin blockchain. As can be seen in the table, the most frequently used heuristics in the papers are common input ownership and change address detection.

3.3.2 Side Channel Attacks

Side channel attacks leverage additional information beyond the blockchain itself to reveal users or transaction behaviors. These attacks exploit correlations in time, amount, network information, or user behavior within forked blockchains.

Table 3.3: Bitcoin blockchain heuristics

	Multi-input	Change address	Address-reuse	Single in-single out	Patterns
[62]	✓	✓			
[61]					
[63]	✓(excluding CoinJoin)	✓		✓	
[64]	✓	✓			
[65]	✓(excluding CoinJoin)				
[66]	✓(excluding CoinJoin)	✓			
[67]					
[68]					
[69]					
[70]	✓	✓			
[71]					
[72]					✓Remuneration profile
[73]	✓				
[74]	✓		✓		✓Common relationship

Time Correlation

By correlating the time when a transaction is confirmed with the time a user interacts with other services, attackers can potentially link transactions to specific users. Researchers in [73, 74] used this attack to identify transactions within trading services and correlated them with blockchain data to find related transactions.

Amount Correlation

The amount transferred in a blockchain transaction can be correlated with the amount paid in other services, such as fiat currencies or other cryptocurrencies. Publicly available trade amounts in trading services were used in [73, 74] to find corresponding transactions on the blockchain. Additionally, exchange rates of fiat currency at the time of transaction confirmation can be used to further correlate payment amounts.

Network Layer Information

The propagation of transactions between nodes in the Bitcoin network can reveal network layer data. Researchers in [69, 68, 70, 71] demonstrated the possibility of linking IP addresses to transactions by connecting to Bitcoin nodes and monitoring network activity. Access patterns can also be exploited to link IP addresses to specific transactions. For example, visiting a webpage with a donation address, performing a transaction, and then checking the confirmation using a block explorer can provide an access pattern that links the IP address to that transaction [61].

Cashing Out on Forks

Cashing out on forks is an attack that exploits cross-chain clustering to link addresses in one chain based on their activities in a forked chain. By combining information from different chains, a single-chain clustering can be created, thus revealing connections

and potentially compromising privacy. In [63], researchers demonstrated this attack by combining Bitcoin and Bitcoin Cash clusters. The cash-out behaviors of Bitcoin users in Bitcoin Cash posed a privacy risk to approximately 5% of the Bitcoin transactions.

This attack highlights the importance of considering cross-chain activity and the potential impact it can have on the privacy of users' transactions.

3.3.3 Flow Analysis

Flow analysis techniques enable attackers to track the flow of money through transaction graphs, user graphs, and taint analysis. These methods provide attackers with insights into the relationships between addresses and transactions.

Transaction Graph

The transaction graph represents addresses as nodes and transactions as edges. By analyzing this graph, an attacker can identify predecessors and successors of addresses, revealing patterns and connections [62].

Taint Analysis

Taint analysis tracks the flow of money from one address to another. It determines the percentage of the balance of an output address that comes from a specific input address, providing insights into fund's origin [2, 26].

User Graph

The user graph represents users as nodes and transactions as edges. By applying clustering techniques or heuristics, relationships between different users can be identified. This graph analysis helps uncover connections and associations among users in the blockchain [62].

Table 3.4 provides a summary of papers employing side-channel attacks or flow analysis. It is evident that amount correlation and IP address mapping are frequently employed side-channel attacks. Additionally, a significant number of papers used transaction graphs or user graphs to de-anonymize transactions.

3.3.4 Auxiliary Information

In addition to the techniques and analyses discussed earlier, attackers can utilize auxiliary information to enhance their understanding of addresses and their associated entities. By tagging addresses and gathering additional details about them, the attacker can gain insights into the identity, location, online presence, and other related information of the users.

Table 3.4: Side channel attacks and flow analysis

	Time correlation	Amount correlation	Network layer		Cashing out on forks	TX graph/ User graph	Taint analysis
			Map IP to pseudonyms	*Access pattern/ User behavior pattern*			
[62]						✓	
[61]			✓	✓			
[63]					✓(Combining BCH&BTC)	✓	
[64]						✓	
[65]		✓				✓	
[66]						✓	✓
[67]							
[68]			✓				
[69]			✓				
[70]			✓			✓	
[71]			✓				
[72]		✓(BTC in $)					
[73]	✓	✓				✓	
[74]	✓	✓					

Address Tagging

Attackers can tag addresses using various methods and sources of information. They may conduct internet searches, interact with target individuals or services, and utilize service APIs to gather relevant data. By tagging one address, the attacker can potentially extend the tagging to other addresses that are connected to or associated with it. This allows for a broader understanding of the network and relationships between different addresses.

Information Sources

Several resources have been employed in research papers to tag addresses and gather auxiliary information. Here are some commonly used sources:

- **Forums and Social Networks:** Platforms like Bitcointalk, Reddit, and Twitter have been used to identify and associate Bitcoin addresses [73, 62, 64]. Users often publish their addresses in these online communities, enabling the attacker to link addresses with specific individuals or entities.
- **Websites and Search Engines:** Addresses published on websites and those that can be queried through search engines provide valuable information. By examining the content associated with these addresses, the attacker can gather insights into the identity and activities of the address owners.
- **Service APIs:** Trading services such as LocalBitcoins, Changelly, and Shapeshift expose APIs that can be used to obtain additional information related to addresses [73, 74, 62]. This information may include transaction history, trading patterns, and other relevant details.
- **Interactions with Services:** In some cases, attackers may directly interact with specific services to obtain addresses associated with those services. This approach, often referred to as “mystery shopper payment” or “mystery shopping,” involves

Table 3.5: Auxiliary information resources

	Forums	Websites	Search engines	Social networks	Service APIs	Interacting	Address tags DB	others
[62]	✓BitcoinTalk, Bitcoin-OTC	✓Casascius physical coins	✓Google	✓Reddit	✓Mt.Gox		✓blockchain.info	
[61]								
[63]								
[64]		✓BleepingComputer, MalwareTips, 2-spyware	✓Google, Yahoo	✓Reddit				✓†
[65]	✓BleepingComputer‡‡	✓ID ransomware				✓**	✓Chainalysis	✓Synthetic addr ††
[66]			✓Ahmia, FreshOnions, Google				✓Walletexplorer,	
[67]	✓BitcoinTalk *						✓Walletexplorer, blockchain.info	
[68]								
[69]								
[70]								
[71]								
[72]								
[73]	✓BitcoinTalk	✓Localbitcoins		✓Twitter	✓Localbitcoins ✓Changelly, Shapeshift		✓Walletexplorer, ✓Walletexplorer, researchers data,	
[74]								

‡‡Ransom addresses in Bleeping computer forum.
† Ransomware knowledge base, YouTube videos, reports from Counter Threat Units (CTU), Incident Responses (IR), and Security Operations Centers (SOC).
†† By running ransomware binaries.
* Extracting Ponzi addresses, profile information, age, gender, location, ...
** Paying a small amount to ransom addresses.

making a small payment and tracking the address associated with the service in the blockchain [65, 79].

- **Address Tagging Databases:** Both non-commercial and commercial databases exist that provide address tags based on their own research and ground truth. Examples of such databases include Walletexplorer, Chainalysis, blockchain.info, as well as address tags published by individual researchers [74, 65, 67]. These databases offer pre-existing knowledge about addresses, enabling the attacker to associate them with specific entities or activities.

By leveraging these auxiliary information sources, attackers can enhance their understanding of the addresses and entities involved in the blockchain network, potentially compromising privacy and anonymity. In table 3.5 the resources that the previous research utilized to tag the addresses are provided.

3.4 Bitcoin Privacy Threat Categories

In a previous section, we identified a series of privacy attacks on the Bitcoin blockchain. This section categorizes these attacks into privacy threat classes, presents associated risks, and provides mitigation and countermeasures. Our classification aligns with the six main threat categories of LINDDUN GO. We adopted the definitions for these categories from [75].

Linkability (L): This category refers to the ability to determine whether two items of interest (IOI) are connected without knowing the genuine identity of the subject of the linkable IOI.

Identifiability (I): This category refers to the ability to identify the subject within a set of subjects.

Non-repudiation (Nr): This category refers to the inability of a subject to deny knowledge, action, or statements.

Detectability (D): This category refers to the ability to determine whether an IOI exists.

Unawareness (U): This category refers to a subject's unconsciousness or incapability to mediate within the collection and processing of their individual data.

Non-compliance (Nc): This category refers to the system's failure to comply with data protection principles.

We followed the threat categories of LINDDUN GO to assess privacy threats on the Bitcoin blockchain. We eliminated privacy threats related to external parties' services. Table 3.6 to Table 3.13 illustrate privacy threats and possible mitigation. We did not provide mitigation for threat U3 that arises from blockchain fundamentals such as public availability, immutability, and decentralization.

Table 3.6: Bitcoin Privacy Threats and Mitigation for Linkability

ID	Src*	Threat	Threat description	Mitigation
L1	B	Linkability of Addresses	Address reuse poses a privacy risk as it allows for the correlation of transactions associated with the same address. An attacker can exploit this to trace other transactions belonging to the same user [10].	**Address Diversity:** It is important to encourage the use of new addresses for each transaction. By generating a fresh address for every transaction, users can prevent linking their transactions and make it more challenging for attackers to trace their activities. Wallet software and services should emphasize the importance of address hygiene and provide clear instructions on how to generate new addresses easily. Additionally, educational initiatives can raise awareness among users about the risks associated with address reuse and promote best practices for maintaining privacy on the Bitcoin blockchain.
L2	B	Linkability of Addresses	Forced address reuse is a privacy threat where an attacker intentionally transfers a small amount of Bitcoin to a used address belonging to a target user. The attacker then monitors the blockchain for the subsequent use of the corresponding unspent transaction output (UTXO) in conjunction with other UTXOs associated with the same target. This method enables the identification of additional UTXOs belonging to the target user [79].	**Address Diversity:** Users should be encouraged to generate new addresses for each transaction and avoid reusing addresses. **Coin Control:** Wallet software should offer features that allow users to exercise control over which UTXOs are selected for spending in a transaction. **Privacy-Focused Wallets**: Wallets designed with privacy as a priority can incorporate built-in mechanisms to mitigate forced address reuse. This may include features like automatic address generation for each transaction and advanced coin selection algorithms that minimize UTXO linkage. **Education and Awareness:** Users should be educated about the risks of forced address reuse and the importance of maintaining address hygiene. Clear guidelines and instructions on address management should be provided to ensure users understand how to protect their privacy effectively.
L3	B	Linkability of Addresses	Threat: Common/Multi-Input Heuristic The common/multi-input heuristic is a privacy threat that relies on the assumption that all inputs of a transaction are controlled by the same entity. It associates all the inputs to a single user [26].	**Privacy-enhancing techniques**: Users can leverage privacy-enhancing techniques such as CoinJoin, CoinSwap, and Mixing Services. These services allow multiple users to combine their transactions, making it difficult for the common/multi-input heuristic to associate inputs to a single user. By obfuscating the transaction inputs, the privacy and anonymity of the participants can be preserved. **Use of Privacy-Focused Wallets:** Users should opt for wallets that prioritize privacy and incorporate features to counter the common/multi-input heuristic. Privacy-focused wallets can implement mechanisms like automatic coin selection and transaction mixing to break the deterministic link between transaction inputs and individual users. **Education and Awareness**: It is important to educate users about the common/multi-input heuristic and its implications for privacy. By raising awareness about this threat, users can make informed decisions and adopt privacy-enhancing practices when conducting Bitcoin transactions.

* Src: Source, B: Blockchain, B/E: Blockchain/External

Table 3.7: Bitcoin Privacy Threat and Mitigation for Linkability

ID	Src*	Threat	Threat description	Mitigation
L4	B	Linkability of Addresses	The change address detection heuristic is a privacy threat that operates under the assumption that the change address used in a transaction is controlled by the owner of the inputs. It associates the change address with the same user as the input addresses [2].	**Pay to New Addresses:** Instead of reusing addresses for receiving change, users should use new addresses for each transaction. By adopting this practice, the link between the input addresses and the change address is severed, making it difficult for the heuristic to determine ownership. **Privacy-Focused Wallets**: Choose wallets that prioritize privacy and implement features to counter the change address detection heuristic. Privacy-focused wallets may provide built-in functionalities like automatic address generation and change address obfuscation, ensuring that change addresses are not easily associated with input addresses. **Education and Best Practices**: Educate users about the risks associated with the change address detection heuristic and promote best practices for maintaining privacy.
L5	B/E	Linkability of Address with real identities	Bitcoin addresses can be associated or mapped to the real-world identities of individuals. This linkage can be achieved by gathering information from exchanges, services, merchants, forums, and social networks[2].	**Use of Privacy-Focused Wallets**: Opt for privacy-focused wallets that prioritize user anonymity. These wallets often implement techniques such as address and transaction obfuscation to prevent the direct linkage between Bitcoin addresses and real identities. **Decentralized Exchanges:**Utilize decentralized exchanges (DEX) that do not require users to provide personal information during the trading process. DEX platforms that prioritize user privacy can help minimize the risk of mapping Bitcoin addresses to real identities. **Avoid Sharing Personal Information:** Be cautious when sharing personal information online, especially on forums, social networks, or platforms associated with Bitcoin transactions. Limit the disclosure of personal details that could potentially link Bitcoin addresses to real identities. **Coin Mixing Services:** Employ the use of coin mixing services to obfuscate the transaction history and make it more difficult to trace the linkage between Bitcoin addresses and real identities. **Education and Privacy Awareness**: Educate Bitcoin users about the risks of linking addresses to real identities and the importance of safeguarding personal information. Promote privacy-conscious behavior and encourage users to be vigilant about protecting their identities when engaging in Bitcoin-related activities.
L6	B/E	Linkable User Actions	The access patterns associated with cryptocurrency addresses pose a privacy threat as they can be exploited to link a user to a specific cryptocurrency address. By analyzing specific search queries, such as checking a transaction in blockchain explorers shortly after broadcasting a transaction, it becomes possible to establish a connection between a user's IP address and a Bitcoin address.	**Utilize Privacy-Enhancing Tools:** Use privacy-enhancing tools such as Virtual Private Networks (VPN) or the Tor network to obfuscate IP addresses. These tools route network traffic through encrypted and anonymous channels, making it difficult to link a user's IP address to their cryptocurrency addresses. **Delayed Exploration**: Avoid immediately searching for a transaction in blockchain explorers after broadcasting it. Delaying the exploration reduces the association between the user's IP address and the specific transaction, making it harder for adversaries to link the user to their cryptocurrency address. **Utilize Wallet Software with Built-in Privacy Features:** Choose wallet software that incorporates privacy features, such as built-in transaction broadcasting services or coin mixing functionalities. **Educate Users on Best Practices**: Educate users about the potential risks associated with access pattern linkage and provide guidelines on best practices. Users should be aware of the importance of maintaining privacy while interacting with cryptocurrencies and understand the potential consequences of exposing their IP addresses.

Table 3.8: Bitcoin Privacy Threat and Mitigation for Linkability

ID	Src*	Threat	Threat description	Mitigation
L7	B/E	Linkability of context	Contextual information obtained from websites or services poses a privacy threat as it can be used to link users to their actions. For example, when a user visits a web page containing a Bitcoin address (e.g., for donation purposes) and subsequently performs a transaction, the access pattern created can be utilized to associate the user's IP address with that specific transaction [61].	**Use Privacy-Enhancing Browsers or Extensions:** Employ privacy-enhancing browsers or browser extensions that offer features like ad-blockers, anti-tracking mechanisms, and IP address obfuscation. These tools help prevent websites from gathering user information and reduce the likelihood of linking actions to specific IP addresses. **Utilize Transaction Mixing Services:** Utilize transaction mixing services that obfuscate the transaction history by mixing it with other transactions. These services make it difficult to trace the link between a user's IP address and their specific transactions, thereby enhancing privacy. **Opt for Disposable or Temporary IP Addresses**: Consider using disposable or temporary IP addresses, such as through the use of (VPN) or proxy servers. By rotating IP addresses, it becomes more challenging to link a specific IP address to a user's transactions. **Educate Users on Privacy Best Practices:** Educate users about the potential risks associated with linking contextual information to their actions on websites or services. Provide guidance on privacy best practices, such as being mindful of the websites visited, avoiding unnecessary exposure of personal information, and considering the potential consequences of publicly associating Bitcoin addresses with their real-world identity.

Table 3.9: Bitcoin Privacy Threat and Mitigation for Identifiability

ID	Src*	Threat	Threat description	Mitigation
I1	B/E	Identifying context	Merchants or services tracking users' transactions on the Bitcoin blockchain can gather information about the source of the user's funds and how they spend the remaining amount (in the change address) in subsequent transactions.	**Use of Multiple Wallets:** Users can utilize multiple Bitcoin wallets to segregate their funds and transactions. By using separate wallets for different purposes, such as one for online purchases and another for personal transactions, users can minimize the risk of linking their activities across different contexts. **Mixing Change Address Coins**: Users should mix the coins received in the change address when conducting transactions with merchants or services. By including the change address coins in mixing transactions, users can further obscure the link between the source of funds and subsequent spending activities. This makes it harder for merchants or services to trace the flow of coins and associate them with specific users. **Adoption of Privacy Coins**: Users can consider using privacy-focused cryptocurrencies that provide built-in privacy features, such as confidential transactions or ring signatures. These privacy coins offer enhanced transaction privacy by default, making it harder for merchants or services to trace and link transactions to specific users. **Educational Awareness**: Promoting user education and awareness regarding privacy risks associated with Bitcoin transactions is crucial. By understanding the potential privacy implications and adopting best practices, users can make informed decisions to protect their privacy when transacting on the Bitcoin blockchain.

Table 3.10: Bitcoin Privacy Threat and Mitigation for Non-repudiation

ID	Src*	Threat	Threat description	Mitigation
Nr1	B	Private key non-repudiation	When participating in a transaction, individuals cannot deny their involvement because the coins associated with an address can only be redeemed using the corresponding private key. This lack of deniability can have privacy implications, as it removes the ability to disassociate oneself from certain transactions.	**Implement Multi-Signature/Threshold Transactions**: Multi-signature or Threshold transactions Signature involve the use of multiple private keys to authorize a transaction. By requiring multiple parties to sign off on a transaction, it introduces a level of shared responsibility and reduces the ability to attribute the transaction solely to a single individual. This can provide increased deniability and privacy for participants involved in the transaction. **Utilize Privacy Coins**: Privacy-focused cryptocurrencies or privacy coins offer enhanced privacy features built into their protocols. These coins employ techniques such as ring signatures, zero-knowledge proofs, or confidential transactions to obfuscate transaction details and provide stronger privacy guarantees. By utilizing privacy coins, individuals can benefit from improved privacy and reduce the risk of non-repudiation. **Exercise Caution and Confidentiality**: Individuals should be mindful of protecting their private keys and exercising caution when sharing them. Private keys should be securely stored and not shared with unauthorized parties. By maintaining the confidentiality of private keys, individuals can reduce the likelihood of unauthorized access and potential non-repudiation issues.
Nr2	B	Non-repudiation of sending	When sending coins associated with a UTXO, it is not possible to deny the transaction because the information about the transaction is stored and publicly available in the blockchain. It removes the ability to disassociate oneself from specific transactions.	**Use Coin Mixing Services:** Coin mixing can be utilized to enhance privacy and break the link between the sender and recipient addresses. **Employ Privacy Coins**: Consider using cryptocurrencies that prioritize privacy as their core feature. **Use Payment Channels or Off-Chain Solutions**: Payment channels or off-chain solutions, such as the Lightning Network, allow for the execution of multiple private transactions before settling the final outcome on the blockchain. These mechanisms enable individuals to conduct off-chain transactions that are not publicly visible on the blockchain, providing a higher level of privacy. By leveraging payment channels, individuals can minimize the exposure of their transactions and enhance deniability.
Nr3	B	Non-repudiation of receipts	When receiving coins associated with a UTXO, it is not possible to deny the receipt of those coins because the information about the transaction is stored and publicly available in the blockchain. It removes the ability to disassociate oneself from specific incoming transactions.	**Use Different Addresses for Each Transaction**: Use a new and unique address for each transaction. By generating a fresh address for every incoming transaction, it becomes more difficult to link multiple transactions to a single identity. **Utilize Privacy-Enhancing Technologies**: Consider using privacy coins or technologies that provide stronger privacy guarantees. Cryptocurrencies employing techniques such as stealth addresses, or ring signatures, can help obfuscate transaction details and protect the privacy of the recipient. By leveraging these technologies, it becomes more challenging to associate received coins with a specific individual. **Implement Payment Channels or Off-Chain Solutions:** By using these solutions, transactions can be executed privately without publicly exposing the details of the received coins. **Consider Coin Mixing Services**: Coin mixing services can be utilized to further enhance privacy when receiving coins. These services mix transactions from multiple sources, making it difficult to trace the flow of coins.
Nr4	B	Non-reputable Storage	The data recorded on the Bitcoin blockchain is immutable, meaning it cannot be denied or altered once it has been confirmed and added to the blockchain. This lack of denial can pose privacy and security concerns, as it eliminates the ability to retract or modify sensitive information stored on the blockchain.	**Implement Off-Chain Solutions:** To protect sensitive data from being permanently stored on the blockchain, explore the use of off-chain solutions. This provides more flexibility and control over the data while maintaining privacy. **Employ Encryption and Hashing Techniques**: Prior to storing data on the blockchain, apply encryption and hashing techniques to protect its confidentiality and integrity. Encrypting sensitive data ensures that even if it is publicly accessible, it remains unreadable without the corresponding decryption keys.

Table 3.11: Bitcoin Privacy Threat and Mitigation for Detectability

ID	Src*	Threat	Threat description	Mitigation
D1	B/E	Detectable communication	An attacker can exploit public information, such as transaction amount and transaction time obtained from services like trading platforms, to correlate it with blockchain data and identify related transactions.	**Implement Transaction Fragmentation:** Consider splitting the transaction amount into smaller parts and submitting these sub-transactions at different times. By breaking down the transaction into multiple smaller transactions with varying amounts and time intervals, it becomes more challenging for an attacker to link them together and identify the original transaction. **Utilize Coin Mixing Services:** Leverage reputable coin mixing services. Coin mixing adds an additional layer of obfuscation to the transaction history, making it more difficult for an attacker to correlate transactions based on publicly available information. **Employ Privacy Enhancing Tools**: Utilize privacy-enhancing tools and technologies, such as wallet software that supports coin control features. Coin control allows users to manually select which inputs are used for a transaction, enabling more precise control over transaction amounts and improving privacy by avoiding the combination of inputs that may reveal correlation patterns.
D2	B/E	Detectable communication	If an individual has knowledge of the transaction time and amount, they can search the blockchain and potentially identify related transactions.	**Limit Information Sharing**: Avoid sharing specific details about your transactions, such as transaction time and amount, with friends, relatives, or other individuals who might inadvertently or intentionally disclose this information. By limiting the exposure of transaction details, you reduce the likelihood of someone being able to link your transactions through publicly available blockchain data. **Utilize Privacy-Centric Wallets**: Consider using wallets specifically designed to enhance privacy.
D3	B	Detectable outliers	There is a risk of detecting abnormal transaction behaviors and user patterns on the blockchain. Analyzing these patterns, such as consistent remuneration patterns, can reveal sensitive information about users. [72].	**Vary Transaction Amounts and Timing:** To avoid creating consistent patterns, it is advisable to vary the transaction amounts and timing whenever possible. Avoid using the same exact amount or conducting transactions at fixed intervals, as this can make it easier for external observers to link your transactions. **Utilize Multiple Inputs and Outputs:** Instead of using transactions with a single input and single output [63], consider utilizing transactions with multiple inputs and outputs. This helps add complexity and makes it more challenging for analysts to associate all inputs or outputs with a single entity. **Employ Coin Mixing Services**: Utilize reputable coin-mixing services that offer coin-mixing functionality. **Implement Payment Channels:** These solutions can provide additional privacy features and make it more challenging for pattern analysis to reveal transaction behaviors.

3.5 Unraveling the privacy implications for Bitcoin-based applications: A case study on Decentralized identity methods

Entities, including users and organizations, rely on global unique identifiers for various purposes such as telephone numbers, ID numbers, or URLs. Traditionally, these identifiers are issued and managed by central authorities. However, previous data breaches and concerns over centralized architecture have highlighted the need for decentralized management of identities, where users become their own identity providers. In response to this demand, blockchain-based DIDs have been proposed, leveraging blockchain technology and cryptographic techniques to establish ownership of identifiers without relying on a trusted entity [81].

Table 3.12: Bitcoin Privacy Threat and Mitigation for Unawareness

ID	Src	Threat	Threat description	Mitigation
U1	B/E	No user-friendly privacy control	Transacting with the Bitcoin blockchain does not offer convenient and user-friendly mechanisms for controlling privacy. This can result in the exposure of sensitive information.	**Utilize Privacy-Centric Wallets**: Use cryptocurrency wallets that prioritize privacy features. Look for wallets that offer advanced privacy settings. **Stay Informed about Privacy Best Practices**: Keep up-to-date with the latest privacy best practices in the Bitcoin community. Stay informed about new tools, techniques, and developments that can improve transactional privacy. Engage with privacy-focused communities and forums to learn from experienced users and experts. **Use Third-Party Privacy Services:** Consider utilizing third-party privacy services or tools that aim to enhance privacy in Bitcoin transactions. These services can provide additional layers of privacy protection by obfuscating transactional metadata or by offering alternative transaction routing methods that mitigate the risk of deanonymization. **Educate Users about Privacy Risks**: Raise awareness among users about the privacy risks associated with Bitcoin transactions. Educate them about the importance of privacy control and provide guidance on how to implement privacy-enhancing practices. Encourage users to be cautious and proactive in protecting their privacy when transacting with Bitcoin.
U2	B	No erasure or rectification	The data stored on the Bitcoin blockchain is permanent and cannot be erased or rectified once it is recorded.	**Be Mindful of Personal Information:** Avoid including personal information or identifiable details in transaction messages or metadata. This includes avoiding the use of usernames, email addresses, or any other PII that can potentially link your transactions to your real-world identity.
U3	B/E	Insufficient consent support	The decentralized nature of the Bitcoin blockchain means there is no central authority governing data processing. The blockchain is publicly accessible, and information extracted from its data can be published by third parties without the consent of the individuals involved.	-

Table 3.13: Bitcoin Privacy Threat and Mitigation for Non-compliance

ID	Src	Threat	Threat description	Mitigation
Nc1	B/E	Unlawful processing	The processing of data on the blockchain lacks a lawful basis, as it operates independently of traditional legal frameworks. Third-party services employ heuristics to cluster addresses and map them to real-world identities.	**Address Confidentiality**: Avoid publishing blockchain addresses on publicly accessible platforms such as websites, forums, or social media. By keeping the addresses private, the likelihood of them being linked to the real-world identity is reduced. **Privacy-Enhancing Solutions**: Utilize privacy-enhancing solutions that obfuscate heuristics used by third-party services. Techniques such as coin mixing or transaction obfuscation can help break the traceability of transactions, making it harder to link addresses to specific individuals. **Use TOR or VPN**: Utilize Tor or a VPN to add an extra layer of anonymity when accessing blockchain-related services. These tools can help mask the IP address and prevent third parties from easily correlating the online activities with the real-world identity.

A **decentralized identifier (DID)** is a string that consists of three main parts: the scheme, the DID method, and the DID method identifier. The syntax, as defined by the W3C recommendation [82], is as follows:

$$Scheme : DID\ method : DID - method - identifier$$

DIDs are typically associated with **DID documents**, which contain information about verification methods (such as cryptographic public keys) and service endpoints required to interact with the identified entity. The entity identified by a DID is referred to as the DID subject, which can represent a person, an object, or an organization.

In addition to the underlying infrastructure (e.g., Bitcoin, Ethereum), a **DID method** defines the procedures for creating, resolving, updating, and revoking DIDs. Each DID method has its own set of governance mechanisms and consensus models, ensuring the integrity and reliability of the identifiers.

While DIDs, in conjunction with DID documents, enable trustworthy communications and interactions with identity owners, **verifiable credentials (VCs)** represent information and claims about identity owners, such as name, age, or diplomas [83]. These credentials can be issued by different issuers, such as universities or employers, and can be cryptographically verified by third parties without the need to directly contact the corresponding issuers. This decentralized verification process enhances privacy, security, and efficiency in identity verification scenarios.

By combining the power of blockchain technology, cryptographic techniques, and decentralized identifiers, individuals and organizations gain greater control over their identities, reducing reliance on centralized authorities.

3.5.1 BTCR: Bitcoin-based Decentralized Identifiers

The BTCR (Bitcoin Reference) method [84] utilizes the Bitcoin blockchain to manage DIDs. In the did:btcr scheme, DIDs are created using transaction references ($TXRef$), which are only known once transactions are confirmed and recorded on the blockchain. Here is an example of a did:btcr (adapted from [84]), where "did" represents the scheme, "btcr" represents the DID method, and "xyv2-xzpq-q9wa-p7t" represents the identifier, which is the transaction reference. The transaction reference follows the BIP 0136 standard, which encodes transaction positions (including chain, block height, and transaction index) on the Bitcoin blockchain:

$$did : btcr : xyv2 - xzpq - q9wa - p7t$$

As mentioned earlier, creating a DID using did:btcr is as simple as creating a Bitcoin transaction. Figure 3.4 provides a simplified representation of Bitcoin transactions. In the first transaction, Alice (A_1) sends bitcoins to Bob (B_1) and receives the remaining

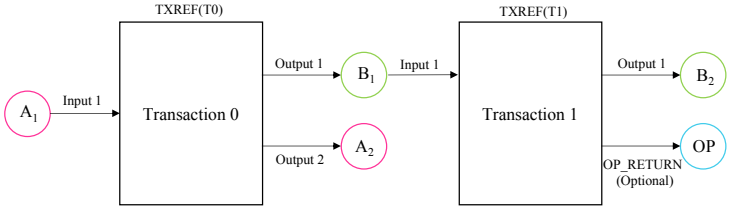


Figure 3.4: Simplified representation of Bitcoin transactions.

bitcoins back to her change address (A_2). In the subsequent transaction, Bob sends bitcoins from his address (B_1) to another address (B_2), while optionally specifying an OP_RETURN output. OP_RETURN is an opcode that enables embedding a small amount of data within a transaction.

The DID creation transaction may include a reference to a URL that holds a DID document using the OP_RETURN construct. However, at the time of writing, InterPlanetary File System (IPFS) was not supported, so the DID document might be stored on a separate storage, such as a third-party server. In cases where the first transaction does not specify an OP_RETURN, a DID document is created by default based on the information available in the transaction itself.

Subsequent operations on the DID, such as update transactions, must include the OP_RETURN construct; otherwise, the DID is considered revoked [85]. An update operation involves updating the DID document and creating a new transaction that consumes all previous UTXOs and embeds the new link to the updated DID document in the OP_RETURN output.

A DID document contains cryptographic materials and methods required to establish communication with the DID controller. For example, a verifiable credential issuer, such as a university, can publish their DID and use it to sign credentials, like diplomas. A verifier, such as an employer, can then check the authenticity of the verifiable credential by resolving the DID that issued the credential and verifying that it has not been revoked using the Bitcoin blockchain.

3.6 Evaluation of did:btcr Privacy

In this section, we evaluate the privacy of the did:btcr method by applying the criteria outlined in RFC 6973 [60]. These criteria include surveillance, misattribution, correlation, identification, secondary use, and disclosure.

3.6.1 Surveillance

Surveillance refers to any type of observation or monitoring of users, which can compromise their privacy, whether or not they are aware of it [60]. When it comes to did:btcr, there is a risk of surveillance due to the nature of the Bitcoin blockchain. As discussed in section

3.3, users' real-world identities can potentially be linked to their Bitcoin addresses, which can expose their activities and economic situations. Surveillance of DIDs on the Bitcoin blockchain can be examined from various perspectives. When users interact with services using DIDs, auxiliary information can be obtained, allowing the service to track the users' activities and money flow in the blockchain by exploiting Bitcoin privacy attacks.

For example, a payment service that requires users to authenticate using a DID and then makes payments using a different Bitcoin address that belongs to the user may link the DID to that Bitcoin address. Additionally, privacy concerns related to using an immutable blockchain for creating DIDs should be taken into account.

To mitigate surveillance risks, users can implement privacy-preserving techniques. Previous research [53, 51] has highlighted a misunderstanding of the privacy implications of the Bitcoin blockchain, leading to significant issues for blockchain-based applications. Possible countermeasures to surveillance in did:btcr include using Tor services [81], mixing the UTXOs before using them for did:btcr [11] to unlink the relationship between the did:btcr UTXOs and other UTXOs belonging to the user, and preventing the combined use of revoked did:btcr with other UTXOs in the future when spending the associated amount.

3.6.2 Misattribution

Misattribution occurs when a user's data or communications are wrongly attributed to someone else, which can have a negative impact on the user's reputation [60]. In the case of did:btcr, misattribution can arise due to indistinguishable mixing techniques, such as PayJoin [86]. PayJoin is a technique that creates a CoinJoin transaction, where the recipient adds their coins as an input to the transaction, increasing the payment amount without requiring equal-size outputs. This technique is indistinguishable in the blockchain but can cause privacy issues for users who are not aware of it when using PayJoin as a privacy technique or interacting with a service that implements PayJoin (e.g., merchants, exchanges).

To address this privacy issue, users should be provided with information to help them identify possible misattribution caused by the use of specific mixing techniques, such as PayJoin, for the UTXOs used in did:btcr. Awareness and education about such techniques can help users understand the privacy risks and take appropriate measures to protect their identities and reputations.

3.6.3 Correlation

Correlation refers to the linking of distinct pieces of information related to a single user [60]. In the context of did:btcr, we explore correlation across three distinct aspects: DID and DID document correlation, time correlation, and network correlation.

i) DID and DID Document Correlation. Using the same DID or DID document to engage with various services can make it easier to trace and correlate user activities

[87, 81, 88]. Additionally, employing the same public keys across different DID documents can expose links between corresponding DIDs, revealing interactions with diverse services under the same DID while displaying different VCs. Conversely, if distinct DIDs are used for each service but the same DID document is used, these services can associate multiple DIDs with the same user. To address this concern, the use of pairwise-unique DIDs issued for specific relationships or single-use identifiers that are discarded after use can be effective [89]. By employing these techniques, the correlation between a user's various services and activities can be minimized.

Moreover, the DID document incorporates methods for verifying the DID and its attributes, including the "also known as" and "controller" properties [81]. The "also known as" property enables the specification of another identifier associated with the same user. While this can be beneficial for businesses employing multiple DIDs for their services, unnecessary correlation should be avoided when not required. The "controller" property allows specification of another entity permitted to modify the DID document or authenticate. Caution is advised when utilizing the "controller" property to prevent exposing relationships between the subject and the controller DID if they belong to distinct entities.

ii) Network layer correlation. Network layer correlation has the potential to compromise DID privacy. An attacker might deduce links between different DIDs based on clients' IP addresses [89]. Moreover, traffic analysis, which examines access histories of DID documents, could aid in correlating IP addresses with DID documents. To bolster privacy concerning network correlation, users can use TOR or a proxy to obscure their IP addresses, thwarting easy identification.

iii) Time correlation. Time correlation can be leveraged to identify relationships of common controls [89]. For instance, timing analysis can correlate users' activities whenever the same service endpoint is utilized in DID documents. To mitigate this form of correlation, users can distribute service endpoints across an array of DIDs controlled by different entities [81], making it more complex to establish direct links between activities and a specific user.

3.6.4 Identification

Identification involves linking information to a specific user to derive their identity [60]. However, storing any personally identifiable information (PII) on the blockchain, even if it is encrypted or hashed, can put users' privacy at risk. This is because the data can be publicly accessible and potentially broken, as shown by various studies [87, 84, 81, 88].

In the case of did:btcr, despite the support for DID revocation, the immutability property of the blockchain prevents the deletion of existing BTCR DIDs logs. As a result, if a Bitcoin address associated with a DID is later spent with other inputs without using mixing techniques, it can link the DID address to other addresses owned by the user, based on the common input ownership heuristic. Furthermore, if a BTCR transaction contains a change address, it can be linked to the owner of the inputs. To prevent these

privacy leaks, it is suggested to create transactions without a change address, thereby reducing the chances of linking multiple addresses to a single user.

Blockchain analysis techniques can not only identify real-world identities and relate them to DIDs but also enable metadata tracing in the DID documents, which can provide information to identify entities [90]. For instance, an attacker can query the Bitcoin blockchain to identify all transactions with OP_RETURN that specify a link to a DID document, thereby gaining access to metadata and associated service endpoints. To prevent privacy leaks in this context, it is important to ensure that URLs to service endpoints do not include any personal information, such as usernames, that could potentially identify the users.

Additionally, the storage of DID documents on servers introduces further privacy considerations. If a third-party server stores the DID document, it may have the ability to identify the real DID owner. On the other hand, if the DID document is stored on the user's server, it becomes possible to correlate the user's IP address with the DID document. To mitigate these risks, the use of technologies like IPFS can be employed as a countermeasure, providing decentralized and distributed storage for DID documents.

3.6.5 Secondary Use

Secondary use refers to collecting information about a user without their consent and using it for purposes other than the ones for which the information was originally collected [60]. In the context of did:btcr, we can investigate secondary use in three aspects.

First, the read/resolve feature of did:btcr allows third-party services to access and resolve the DIDs. If these services are accessed by an attacker, they can trace the usage patterns of the DIDs and potentially identify the individuals associated with them. To mitigate the risk of third-party services collecting information about users, organizations may choose to employ their own Bitcoin full nodes to resolve DIDs internally, reducing reliance on external services.

Second, a verifier of a did:btcr DID can trace the transaction flow, check the history of theUTXOs, monitor subsequent transactions' flow if they are spent, and see all the amounts associated with the address. This high level of transparency may raise privacy concerns for users, as their transaction history can be easily tracked and analyzed, potentially revealing sensitive financial information.

Third, if a did:btcr DID is used in services that require additional information about the user or their activities, such as social networks, there is a risk of compromising the real identity behind the DID. The information provided in these services can be associated with the DID, potentially exposing the user's activities, preferences, and personal details.

To address these privacy risks related to secondary use, users should be cautious about the services they interact with and the information they provide. It is important for service providers to adopt privacy-preserving practices and clearly communicate their data usage policies to users. Additionally, individuals can explore the use of privacy-enhancing

techniques, such as obfuscation methods or privacy-preserving protocols, to mitigate the risks associated with secondary use.

3.6.6 Disclosure

Disclosure refers to the exposure of user information that violates the confidentiality of shared data [60]. In the context of did:btcr, all privacy attacks mentioned in the previous sections can be applied to the addresses associated with DIDs. Users who are not familiar with privacy issues on the Bitcoin blockchain may face significant problems if their DID addresses link to their other addresses in the blockchain. This can result in a loss of privacy in their economic activities for services authenticated by DIDs.

When creating the first DID in did:btcr, the user is required to provide an address from which they can buy cryptocurrency from an exchange. The exchange typically has access to information related to the owner, such as email address or, in some cases, the owner's real identity if Know Your Customer (KYC) procedures are applied. To enhance privacy, users can employ mixing techniques before associating their addresses with the did:btcr, obfuscating the relationship between the UTXOs used in did:btcr and their other UTXOs.

However, it is important to note that did:btcr updates require the use of the OP_RETURN field in Bitcoin transactions, which means that current mixing techniques cannot provide better privacy for the associated addresses. This makes did:btcr updates traceable on the Bitcoin blockchain. As a result, every update in did:btcr reveals not only the public key of the previous DID but also indicates the update or change of the access control, potentially allowing for the identification of the entities involved.

3.7 Conclusion

In this chapter, we reviewed Bitcoin privacy attacks and categorized them into four main categories. We then specifically investigated and analyzed six potential privacy threats to the did:btcr DID method. Through our analysis, we demonstrated how data analysis of Bitcoin's public records, in combination with auxiliary information, can be leveraged using sophisticated heuristics to uncover or correlate user transactions, identities, or addresses. Malicious actors and cybercriminals can exploit this information for various malicious purposes, including extortion or ransomware attacks.

While did:btcr offers advantages such as protection against censorship, data integrity, controlled access, and a degree of decentralization, it still faces challenges in addressing the privacy issues identified in this paper. The identified threats highlight the importance of considering privacy concerns when designing and implementing decentralized identity systems.

To mitigate these privacy issues, future research efforts should focus on developing new methods or utilizing existing privacy-enhancing techniques. For example, mixing techniques and zero-knowledge proofs can be explored to enhance privacy in the context of did:btcr. Mixing techniques can help obfuscate transaction histories and break

the traceability of Bitcoin addresses, making it more difficult to correlate them with DIDs. Zero-knowledge proofs can enable the verification of cryptographic statements without revealing any underlying sensitive information, providing a higher level of privacy assurance.

By incorporating these privacy-enhancing techniques and continuously exploring novel approaches, the did:btcr method can evolve to address the privacy challenges identified in this study. It is crucial to strike a balance between maintaining the desired properties of a decentralized identity system while ensuring robust privacy protections for individuals and organizations leveraging the technology.

In the next chapter, we assess and contrast different privacy techniques by examining their privacy, security, and efficiency, and assessing their suitability for the Bitcoin blockchain.

CHAPTER 4

Classification and Evaluation of Privacy-Preserving Techniques

4.1 Introduction

Unlike traditional systems, Bitcoin transactions are publicly and permanently recorded, and anyone can access the complete history of these records. Despite the use of pseudonymous identities, adversaries can undermine users' financial privacy and reveal their actual identities by employing advanced heuristics and techniques to identify potential links between transactions, senders, receivers, and consumed services (e.g., online purchases). Therefore, a multitude of approaches has been proposed to reduce financial transparency and enhance users' anonymity. These techniques range from mixing services to off-chain transactions, addressing various privacy concerns.

This chapter focuses on the classification and evaluation of privacy-preserving techniques specifically designed for Bitcoin, with a particular emphasis on mixing techniques [91]. The objective is to assess and compare existing privacy approaches by examining their efficacy in terms of privacy, security, and efficiency, while also considering their applicability to the Bitcoin blockchain. The research questions addressed in this chapter are as follows.

RQ 1: How do existing privacy techniques compare privacy measures, including the anonymity set, unlinkability, untraceability, and transaction value privacy?

RQ 2: To what extent are privacy techniques resilient against security attacks, including theft, denial-of-service (DoS), and Sybil attacks?

RQ 3: How do existing privacy techniques compare in terms of efficiency, considering factors such as the number of interactions with input users, the number of interactions with the recipient, Bitcoin compatibility, direct coin transfer to the recipient, the number of transactions involved, and the minimum required blocks?

To answer these research questions comprehensively, an in-depth analysis of various privacy-preserving techniques proposed for Bitcoin is conducted in this chapter. The evaluation criteria encompass privacy aspects, security considerations, and efficiency metrics. The results of this analysis contribute to a better understanding of the strengths and weaknesses of different approaches, ultimately aiding in the development of more effective privacy-preserving mechanisms for the Bitcoin ecosystem.

Section 4.2 presents the methodology used to classify the privacy-preserving techniques, which are then discussed in detail in section 4.3. Section 4.4 establishes a set of predefined evaluation criteria, which are then used to assess the techniques in Section 4.5. Finally, Section 4.6 concludes the work by summarizing the identified challenges and presenting a synthesis of the findings.

4.2 Methodology

The methodology used in this research involved a systematic approach to categorize privacy-preserving techniques. The study followed the PRISMA methodology [6], which is a well-known guideline for conducting systematic reviews and meta-analyses. The PRISMA methodology provides a thorough and structured framework to ensure a transparent and reproducible method for conducting systematic reviews. The approach involves a rigorous process of searching, screening, and analyzing pertinent literature to offer comprehensive insight into a particular research topic. The methodology is illustrated in Figure 4.1 and can be broken down into four main steps:

- **Planning:** The first step involved formulating research questions to guide the systematic review. These questions helped to identify the scope and purpose of the review.
- **Literature search** The second step involved searching various databases such as IEEE Xplore, Springer, and Science Direct, as well as unpublished papers on arxiv.org and eprint.iacr.org. Additionally, we conducted a direct search on GitHub to find real-world implementations of privacy techniques.
  - **Search Query:** The search query incorporated various keywords, such as “Bitcoin,” “blockchain,” “distributed ledger technology,” “DLT,” “privacy,” “privacy-preserving,” “mixing,” “tumbling,” “tumbler,” and “anonymity,”. To ensure meaningful results, the search was confined to the title, abstract, and keywords. The search query was as follows: “Bitcoin” OR “blockchain” OR “distributed ledger technology” OR “DLT” AND “privacy” OR “privacy-preserving” OR “mixing” OR “tumbling” OR “tumbler” OR “anonymity”.
- **Literature Selection:** We obtained 869 research papers.
  - **Exclusion criteria:** We limited our research to the papers published after 2009, as Bitcoin was implemented in 2009. As this survey was conducted in

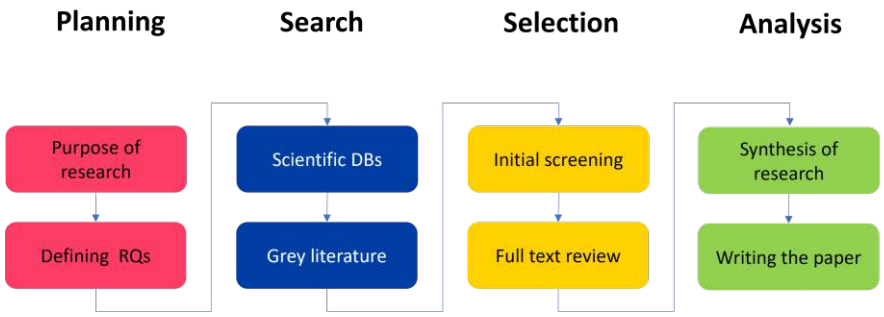


Figure 4.1: Methodology

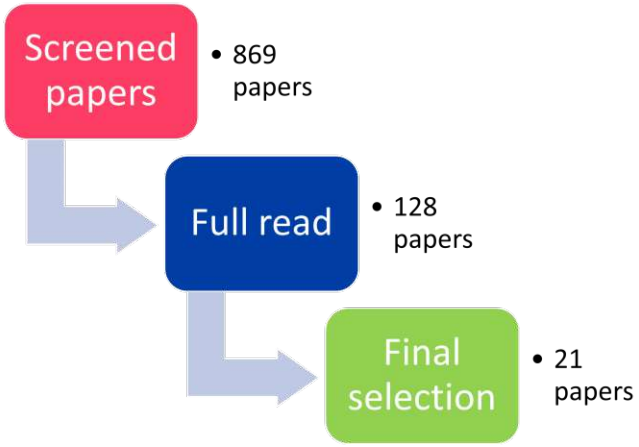


Figure 4.2: Literature selection

2020, the search was then limited to papers published between 2009 and 2020, ensuring the inclusion of recent research. We did not consider an article if the title, abstract, or keywords did not relate to the Bitcoin blockchain.

– **Quality assessment:** We considered works that proposed a privacy-preserving technique applicable to the Bitcoin blockchain.

The papers obtained were then screened based on their titles and abstracts to exclude papers that were not relevant to the research questions. We then fully read 128 papers and finally, 21 privacy techniques were selected for the study. The process of literature selection is indicated in Figure 4.2.

- **Analysis and synthesis of extracted data:** In the final step, we analyzed and synthesized the data obtained from the selected papers. The selected papers were evaluated based on their scope, disruption, and merit, following the criteria from [92].

4.3 Privacy-Preserving Techniques

Transactions within the Bitcoin blockchain consist of multiple inputs and outputs, each of which can be traced using sophisticated analytical tools. However, privacy-preserving techniques aim to obfuscate these links, preventing attackers from tracing inputs and maintaining the confidentiality of recipient addresses and transaction values. Various privacy techniques exist, differing in terms of their privacy guarantees, security characteristics, and efficiency. In this section, we categorize these techniques into centralized mixers, atomic swaps, CoinJoin-based methods, and threshold signatures, providing a comprehensive discussion of each.

4.3.1 Centralized Mixers

In this subsection, we explore privacy methods that rely on a centralized party, where senders forward their coins to a central mixer that performs the mixing process before forwarding the coins to the intended recipients.

Mixing Websites

The concept of mixing was initially proposed by Chaum in 1981 [93] to achieve anonymous email communication without the need for a universally trusted authority. This idea has been adapted for the blockchain to address anonymity concerns by employing mixing networks, such as mixing websites, to obscure the links between senders and receivers. For instance, suppose Alice, Bob, and Carol wish to send their coins to recipients A', B', and C', respectively. They collectively utilize a mixer for their transactions (Figure 4.3). The mixer receives equal amounts of coins from the senders, mixes them, and forwards them to the respective recipient addresses. By examining the published transactions, it becomes challenging to distinguish whether Alice sent her coins to A', B', or C'. On most mixing websites, users are typically required to fill out a form, providing the recipient's address and selecting the desired mixing delay. Subsequently, the mixer generates a fresh address to receive the coins from the sender, along with details such as the mixing fee, transaction fee, and user conditions. However, one of the drawbacks of mixing websites is that the mixer may steal the coins and never forward the coins to the destination.

It is worth noting that exchanges can also serve as centralized mixers. However, utilizing exchanges for mixing purposes comes with a significant drawback. In the case of KYC, the exchange can easily link the coin owners to their real identities.

MixCoin

MixCoin, proposed by Bonneau et al. [26], serves as a Bitcoin mixer designed to prevent theft in mixing services by leveraging the mixer signature as a warranty against malicious behavior. In this protocol, the mixer is required to sign the sender's mixing parameters, including the recipient address, preferred transfer deadlines, transaction value, and mixing fee. If the mixer fails to forward the coins to the intended recipient, the sender can

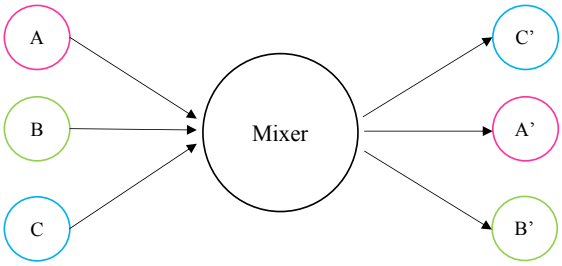


Figure 4.3: Mixing websites

publicly publish the warranty. This enables anyone to verify the mixer's malicious actions, thereby tarnishing its reputation.

In MixCoin, the mixing fee paid to the mixer is an all-or-nothing concept, as a constant mixing fee can potentially reveal sequential mixing transactions. To enhance anonymity, mixing transactions adopt a standardized chunk size, promoting uniformity in the resulting transactions. By chaining multiple mixing operations together, improved anonymity can be achieved.

BlindCoin

BlindCoin [94] incorporates blind signatures into the MixCoin protocol. Blind signatures, originally introduced by Chaum [95], enable the signing of a message without revealing its content to the signer. By integrating blind signatures into BlindCoin, the relationship between inputs and outputs is concealed from the mixer itself. The mixer provides its warranty by blindly signing the recipient's address. Subsequently, the sender anonymously submits the unblinded recipient's address to the mixer using a new identity. As the mixer recognizes its own signature on the recipient's address, it proceeds to send the coins to the designated recipient.

The inclusion of blind signatures in BlindCoin strengthens privacy by preventing the mixer from linking the sender's input to the recipient's address, enhancing the overall anonymity of the transaction.

LockMix

LockMix [96] represents a central mixer that builds upon the BlindCoin protocol [94] by incorporating multi-signature functionality to prevent the mixer from engaging in coin theft. In this protocol, the mixer publicly announces various parameters in the network, including user deposit, transaction value, waiting blocks, and mixing fee.

To initiate the LockMix protocol, Alice combines her desired deadlines for the protocol's steps, the blinded recipient's address, and her own address K_A to create a multi-signature address. The mixer then generates a 2-of-2 multi-signature address (K_{AM}) using Alice's address (K_A) and its own address (K_M). The mixer includes the multi-signature address and its escrow address, signs all the parameters, and sends the signed data back to Alice.

Subsequently, Alice deposits an amount larger than the intended mixing value to the multi-signature address K_{AM} as collateral. She then unblinds the recipient's address and sends it to the mixer. The mixer proceeds to send the coins to the designated recipient. Alice waits for the agreed-upon number of confirmation blocks to be mined and subsequently sends the coins to the mixer's escrow address.

Finally, Alice creates a transaction that transfers the mixing fee to the mixer and the remaining coins to herself from the 2-of-2 multi-signature transaction. To receive the coins, both Alice and the mixer must sign the transaction. It is important to note that during each step of the protocol, both Alice and the mixer have the option to abort. However, this does not benefit either party, as they may lose their coins or any potential benefits, resulting in a lose-lose scenario.

By utilizing multi-signature addresses and collateral deposits, LockMix enhances the security of BlindCoin by mitigating the risk of coin theft by the mixer. The protocol establishes a trustless environment where misbehavior by either party would result in potential losses, thus incentivizing honest behavior.

Obscuro

Obscuro [97] is a central mixer that leverages a trusted execution environment (TEE) to enhance privacy and security. The TEE is a secure processing environment that operates on a separate kernel, ensuring the authenticity of executed code and the integrity of runtime states. It provides strong guarantees for the confidentiality of stored code, data, and runtime states on persistent memory [98].

In the Obscuro protocol, the mixer generates a key within the TEE and publishes the corresponding public key and Bitcoin address. All participating users send their coins to a single address controlled by the mixer and publish their respective transactions in the network. These transactions include encrypted recipient addresses and a transaction refund script, which allows users to retrieve their coins in case they remain unspent by the lock time.

Obscuro scans the blockchain to extract these transactions and proceeds with the mixing process. The mixer decrypts the encrypted recipient addresses, shuffles them to obfuscate their original order, and transfers the coins to the corresponding recipients' addresses. A mixing transaction is created, which includes all users' deposit transactions as inputs and the shuffled list of recipient addresses as outputs.

To ensure the effectiveness and efficiency of the protocol, certain parameters are specified. These include the maximum and minimum number of participants in the mixing set, as well as the number of blocks to wait before performing the mixing transaction. By specifying a minimum number of participants, users are assured of the desired mixing set size before they decide to participate in the protocol. This helps maintain the anonymity and privacy guarantees of the mixing process.

The integration of a trusted execution environment in Obscuro enhances the security and privacy of the mixing process by providing a secure environment for key generation and execution of critical operations. This mitigates the risk of malicious behavior and preserves the confidentiality of sensitive information throughout the protocol.

4.3.2 Atomic Swaps

Atomic swap techniques enable users to exchange their coins with each other in a secure and trustless manner. The key idea behind atomic swaps is that if one party is paid, the other party is also paid, ensuring fairness and preventing the possibility of one party cheating or backing out of the transaction.

FairExchange

FairExchange, proposed by Barber et al. [99], is a protocol that facilitates the exchange of coins between two users. The protocol ensures that both parties can securely swap their coins without the risk of fraud or double-spending.

The FairExchange protocol operates as follows: Alice and Bob first generate two key pairs to be used in different transactions. They then generate secret values, denoted as a_i and b_i, and derive the hashes $H(a_i+b_i)$ and $H(b_i)$, which will be included in the offer transactions.

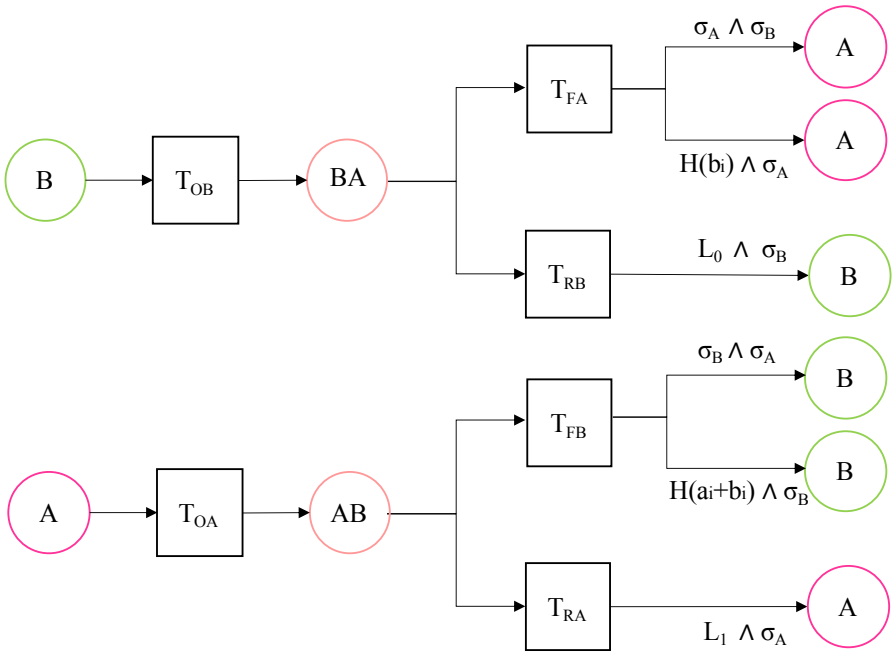
Figure 4.4 provides an overview of the FairExchange protocol. To initiate the exchange, Bob creates an offer transaction, denoted as T_{OB}, that can be redeemed by either Alice's and Bob's signatures or Alice's signature and b_i. Additionally, Bob creates a transaction refund, denoted as T_{RB}, which allows him to retrieve his coin if the protocol is aborted. Bob then waits for Alice to sign T_{RB} and publishes both T_{OB} and T_{RB}.

Similarly, Alice creates her own offer transaction, T_{OA}, which can be redeemed by both Bob's and Alice's signatures or Bob's signature and $a_i + b_i$. Alice also creates a transaction refund, T_{RA}, as a safeguard. Bob fulfills Alice's transaction by providing his signature and a_i+b_i. Alice then subtracts a_i from the obtained value to retrieve b_i and fulfills Bob's transaction, denoted as T_{FA}, using Bob's signature and b_i.

By following the steps of the FairExchange protocol, Alice and Bob can securely and fairly exchange their coins without the need for a trusted third party. The protocol ensures that the transactions are atomic, meaning that either both parties successfully complete the exchange or the process is rolled back, preventing any potential loss or unfairness in the transaction.

Xim

Xim, proposed by Bissias et al. [100], introduces a novel approach for facilitating FairExchange transactions (4.3.2) by leveraging the blockchain as a platform for advertising mixing requests. The protocol addresses the challenge of finding a trustworthy participant to engage in the exchange process.



σ_A: Alice's signature. σ_B: Bob's signature. T_{RA} & T_{RB}: Refund transactions.
T_{OA} & T_{OB}: Offer transactions. T_{FA} & T_{FB}: Fulfill transactions.
L_0 & L_1: Lock times.

Figure 4.4: FairExchange

In the Xim protocol, Alice initiates the process by paying a fee of $\frac{\tau}{2}$ coins to a miner in order to have her mixing request advertisement included in a block on the blockchain. The advertisement contains relevant information such as Alice's location, which can be an Onion address or a Bulletin board. By leveraging the blockchain's public nature, the advertisement becomes visible to potential participants who can contact Alice for further engagement.

Multiple participants may reach out to Alice in response to the advertisement, and Alice has the freedom to choose one of them as a partner for the FairExchange transaction. However, before proceeding with the partnership, the selected participant is required to pay a fee of τ coins to the miner. This fee serves as a preventive measure against Sybil and Denial-of-Service (DoS) attacks, ensuring that participants have a genuine and committed intention to engage in the transaction. If a participant fails to make the payment, Alice can select another participant who is willing to meet the required fee.

Once the participant pays the fee, Alice confirms the partnership by paying an additional $\frac{\tau}{2}$ coins, solidifying their commitment to the FairExchange process. With the partnership established, Alice and the participant can proceed with swapping their coins to their respective recipients' addresses using the FairExchange protocol (4.3.2).

The Xim protocol introduces a novel approach to address the challenge of finding

trustworthy participants for FairExchange transactions. By utilizing the blockchain as a medium for advertising and verifying participants.

CoinSwap

CoinSwap, proposed by Maxwell [101], is a protocol designed to prevent the theft of transferred coins by intermediaries. The protocol utilizes a series of transactions involving multiple parties to ensure secure and reliable transfers from the sender (Alice) to the recipient (Bob), while protecting against potential theft by the intermediary (Carol).

The CoinSwap protocol consists of four transactions: two for payments and two for releases. To initiate the protocol, Alice creates a 2-of-2 multi-signature transaction, denoted as T_0, which requires both Alice's and Carol's signatures ($\sigma_A \wedge \sigma_C$) to spend the coins (Figure 4.5). Simultaneously, Carol creates a multi-signature transaction, T_1, that requires both Carol's and Bob's signatures ($\sigma_C \wedge \sigma_B$).

To ensure fairness and protect against potential protocol abandonment, refund transactions, T_{0R} and T_{1R}, are created by Carol and Bob, respectively. These refund transactions guarantee that the coins will be sent back to Alice and Carol if the protocol is aborted. Notably, the timelock of T_{0R} should be set to a longer duration than that of T_{1R} to ensure fairness.

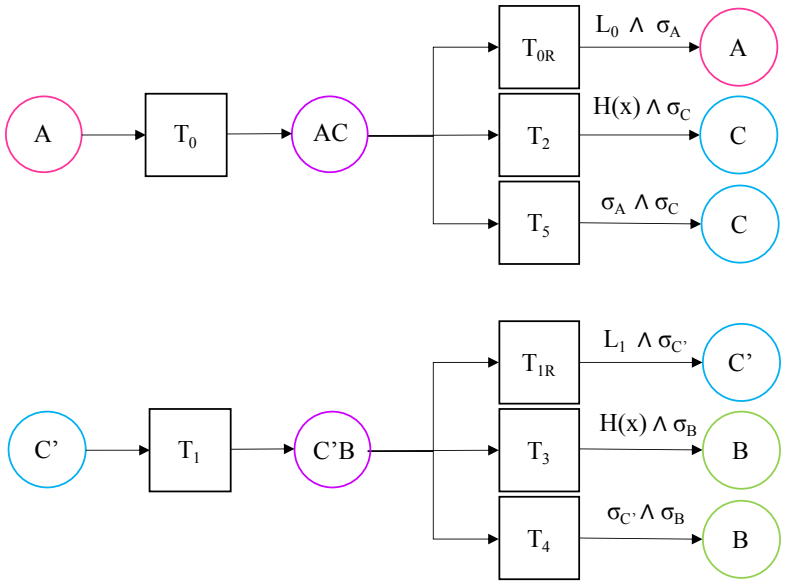
To prevent theft and ensure the integrity of the process, CoinSwap employs hashlock transactions. Bob chooses a random value, x, computes the hash of x (H(x)), and shares the hash with both Alice and Carol. Alice then creates a hashlock transaction, T_2, which can be redeemed by Carol's signature and x. Similarly, Carol creates a hashlock transaction, T_3, that can be redeemed by Bob's signature and x. It is crucial that x is not revealed unless there is misbehavior by one of the participants, as its publication would disclose the link between these transactions in the blockchain.

Subsequently, Carol waits to receive x from Bob. Once she receives it, she creates T_4, a transaction to send the coins to Bob. Carol sends T_4 to Bob for his signature and then publishes it to the blockchain. After T_4 is confirmed, Alice creates T_5, a transaction to send the coins to Carol, and sends it to Carol for her signature. Finally, Alice publishes T_5 to the blockchain.

If Bob fails to provide x to Carol, Carol has the option to redeem the coins from T_{1R} before the expiry of T_{0R}. In this case, Alice can retrieve her coins from T_{0R}, while Bob can simultaneously redeem the coins from the hashlock. It is worth noting that Carol should use a different identifier for the transactions between herself and Bob, as recommended in [102]. This ensures an added layer of anonymity and prevents linkability of the transactions.

A key feature of CoinSwap is the ability to operate across different blockchains that support timelock- and hashlock transactions. This allows the transactions to occur in separate paths, potentially involving different cryptocurrencies (e.g., Bitcoin and LiteCoin) [103].

CoinSwap provides a robust mechanism for secure and trustless coin transfers, minimizing the risk of theft by intermediaries.



σ_A: Alice's signature. σ_B: Bob's signature. σ_C: Carol's signature.
T_{0R} and T_{1R}: Refund transactions. L_0 & L_1: Lock times.

Figure 4.5: CoinSwap

New CoinSwap

The New CoinSwap protocol, introduced by Gibson [103], represents an enhanced version of the original CoinSwap that takes advantage of the Check Lock Time Verify (CLTV) [104] and Check Sequence Verify (CSV)) [105] opcodes. Additionally, it leverages segwit to address transaction malleability [106], resulting in a theft-resistant protocol.

Unlike the original CoinSwap, where Alice played the role of the sender and Bob was the recipient, in the New CoinSwap protocol, Alice assumes the role of Bob. This modification eliminates the need for direct interaction with the recipient. Instead, Alice initially sends the coins to her own fresh address and subsequently utilizes mixed coins to transfer them to the actual recipient.

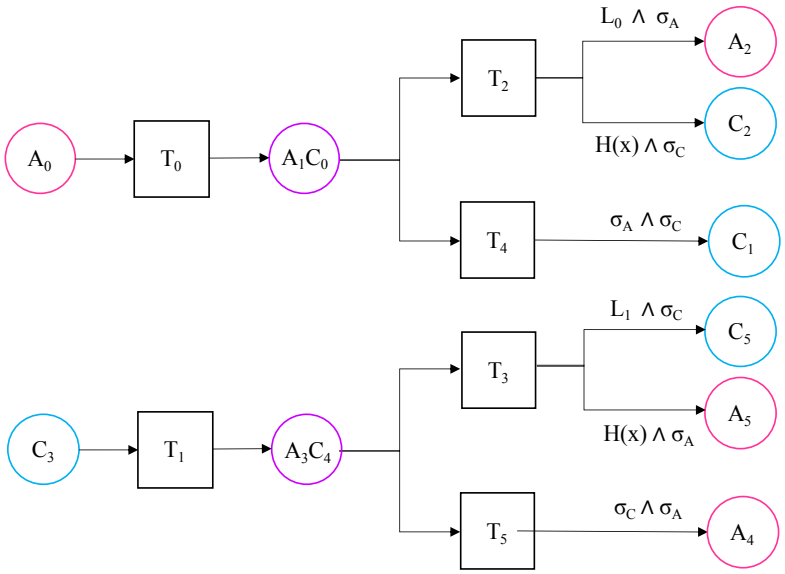
The introduction of CLTV and segwit brings significant improvements to the protocol. CLTV allows the creation of hash time-locked transactions, replacing the previous reliance on nLockTime for refund transactions. By utilizing CLTV, participants can specify time-based conditions that must be met before certain transactions can be redeemed. This enhances the security and flexibility of the protocol.

Furthermore, the integration of segwit addresses the issue of transaction malleability, which can potentially enable third-party interference or modification of transactions.

Segwit separates transaction signatures from the transaction data, preventing malleability and ensuring the integrity of the protocol.

In terms of the transaction flow, the New CoinSwap protocol follows a similar structure to the original CoinSwap. Alice initiates the process by sending the coins to her own fresh address. From there, she can utilize mixed coins to transfer the funds to the intended recipient. The protocol ensures that the coins are protected throughout the process by employing hashlock transactions and time-based locking mechanisms.

Figure 4.6 illustrates the transaction flow in the New CoinSwap protocol. It showcases the interaction between Alice, Carol, and Bob, and demonstrates the use of signatures (σ_A, σ_B, σ_C) and lock times (L_0, L_1) to secure the transactions.



σ_A: Alice's signature. σ_B: Bob's signature. σ_C: Carol's signature.
L_0 & L_1: Lock times.

Figure 4.6: New CoinSwap

PaySwap / Design for a CoinSwap Implementation

PaySwap, introduced by Belcher [107], represents a notable improvement upon the CoinSwap protocol. PaySwap leverages two-party ECDSA to create 2-of-2 multi-signature addresses, which function similarly to regular single-signature addresses. This advancement enhances the privacy of the protocol.

In PaySwap, the transaction flow involves Alice1 paying Bob1 and Bob2 paying Alice2 through CoinSwap transactions. Here, Alice1 and Alice2 represent different addresses of Alice, while Bob1 and Bob2 represent different addresses of Bob. The protocol introduces the concept of market takers and market makers, akin to the Joinmarket wallet [108].

Alice, as the market taker, pays a fee to Bob, who acts as the market maker. This fee compensates Bob for providing the service of facilitating the transaction.

To address potential amount correlation attacks, where an attacker could identify Alice2 based on transaction values, PaySwap introduces multi-transactions. This means that Alice sends the coins to Bob and, in return, receives multiple transactions with varying amounts that sum up to the original total amount. By employing multi-transactions, PaySwap enhances privacy and prevents adversaries from linking transaction values to specific individuals.

PaySwap also tackles internal traceability concerns, where Bob could potentially trace the flow of Alice's coins. To mitigate this risk, Alice can reroute her coins through multiple market makers, such as Bob, Carol, and Dave. Each market maker only knows the previous and next address in the transaction chain. Alice informs every market maker of the CoinSwap incoming and outgoing addresses, making it impossible for any individual market maker to distinguish whether the incoming address belongs to Alice or the previous market maker. This routing mechanism enhances privacy by obfuscating the coin flow and making it difficult to trace.

Furthermore, PaySwap suggests combining multi-transactions with routing to further strengthen the privacy of transactions. By integrating these techniques, the protocol achieves a higher level of anonymity and confidentiality during coin transfers.

PaySwap also explores the potential synergy between CoinSwap and PayJoin (discussed in Section 4.3.3). The combination of these two protocols offers a promising solution to break the "common input ownership" heuristic. By incorporating Bob's input into Alice's inputs in the transaction, the protocol confuses transaction analysis and further protects the privacy of the participants.

Blindly Signed Contract (BSC)

The Blindly Signed Contract (BSC) protocol, proposed by Heilman et al. [109], introduces two schemes for executing secure transactions: (i) an on-chain scheme and (ii) an off-chain scheme. The on-chain scheme utilizes untrusted intermediaries, while the off-chain scheme leverages micro-payment channel networks, enabling off-chain transactions with on-chain confirmations.

In the on-chain scheme, the BSC protocol involves two FairExchange transactions, requiring a total of four transactions to be submitted on the blockchain. The goal is to enable Alice to securely transfer coins to Bob, with the assistance of an intermediary, Carol. The protocol begins with Carol posting public parameters on the blockchain, including blind signature parameters, a transaction fee, a reward value (commonly denoted as 'w' and considered a mixing fee in the protocol), and transaction time windows.

To initiate the protocol, Bob selects a fresh address to receive the coins, while Alice selects a serial number and sends its hash to Bob. Bob then forwards this hash to Carol and requests her to create a transaction ($TO_{C->B}$) in which Carol offers one coin to Bob

if she receives a voucher $V = (sn, \sigma)$. This voucher contains a serial number that matches the hash provided by Bob. Carol proceeds to post $\mathrm{TO}_{\mathrm{C->B}}$ on the blockchain.

In order to enhance privacy and security, Alice blinds the serial number ($\overline{sn}$) and creates a transaction that offers 1+w coins to Carol if Carol provides a blind signature on ($\overline{sn}$). Once this transaction is confirmed on the blockchain, Carol fulfills the transaction $\mathrm{TF}_{\mathrm{A->C}}$ by providing a blind signature ($\overline{\sigma}$) on ($\overline{sn}$), thus enabling Alice to obtain the unblinded signature (σ). Alice can then send the voucher ($V = (sn, \sigma)$) to Bob to fulfill the transaction $\mathrm{TF}_{\mathrm{C->B}}$, which transfers the coins from Carol to Bob.

The BSC protocol provides a secure and efficient mechanism for conducting on-chain transactions using FairExchange. By leveraging blind signatures and the involvement of an intermediary, the protocol ensures that both Alice and Bob can trust the transaction process. The protocol's design addresses privacy concerns by utilizing blind serial numbers and blind signatures, making it difficult for external parties to link the transactions and identify the participants involved.

However, the successful implementation of the BSC protocol relies on the requirement of a Soft-fork on the Bitcoin blockchain. A Soft-fork is a backward-compatible protocol upgrade where new rules are added to the existing consensus rules of the blockchain. This implies that the BSC protocol introduces changes that can be adopted by a majority of the Bitcoin network's participants without causing a split in the blockchain. Therefore, it is essential to assess the feasibility and practicality of the BSC protocol's Soft-fork requirement. This evaluation should consider the potential benefits offered by the protocol, the willingness of the Bitcoin community to adopt the proposed changes, and the technical considerations necessary for a successful implementation.

It is worth noting that the BSC protocol also introduces an off-chain scheme that utilizes micro-payment channel networks. In this scheme, transactions are performed off-chain, and only the final settlement is recorded on the blockchain. This alternative scheme offers improved scalability and reduced transaction fees, making it suitable for frequent and rapid transactions between trusted parties.

TumbleBit

TumbleBit [33] is a privacy-enhancing protocol that utilizes the concept of puzzle solutions to achieve privacy in the presence of an untrusted central tumbler. The protocol involves a series of transactions, requiring four transactions to be confirmed within two blocks.

At a high level, TumbleBit operates as follows: The tumbler, acting as the intermediary, transfers the coins to Bob on the condition that he solves a specific puzzle. Subsequently, the tumbler sells the puzzle solution to Alice for the same amount of coins. This process ensures that the tumbler cannot link the input and output transactions, thereby preserving privacy.

To initiate the protocol, the tumbler generates a Rivest–Shamir–Adleman (RSA) [110] puzzle with the solution denoted as ϵ. The tumbler then takes an ECDSA signature

encrypted under the solution to the RSA puzzle and creates a ciphertext c. This encrypted signature represents a transaction signature that allows Bob to spend one bitcoin from the transaction escrow.

As depicted in Figure 4.7, the tumbler sends the puzzle z and ciphertext c to Bob. Bob, in turn, blinds the puzzle by applying a blinding factor to obtain z and forwards it to Alice. Alice, desiring to obtain the blinded solution, creates FairExchange transactions with the tumbler, where she pays the tumbler the desired amount. Alice sends the blinded puzzle z to the tumbler, who possesses the capability to solve the puzzle and obtain ϵ. Alice then receives ϵ from the tumbler.

Subsequently, Alice sends ϵ^* to Bob, who unblinds it to obtain ϵ. Finally, Bob can claim the coins from the transaction T_{F2} using the obtained solution ϵ.

The use of puzzle solutions in TumbleBit ensures that the tumbler does not have knowledge of the actual transactions taking place between Alice and Bob. By utilizing blind signatures, encrypted solutions, and blinding factors, TumbleBit maintains privacy and anonymity for the participants involved.

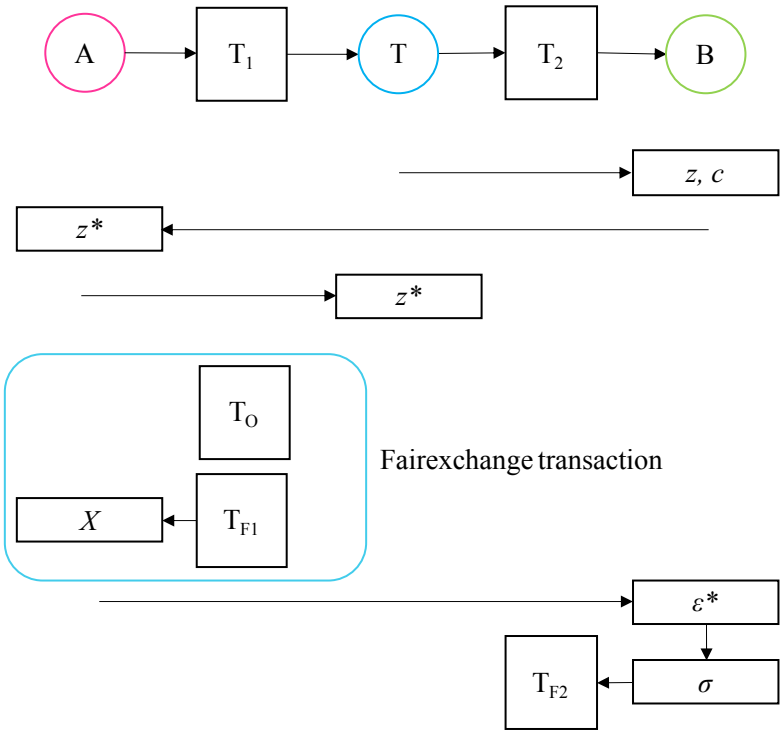


Figure 4.7: TumbleBit

4.3.3 CoinJoin-based Techniques

CoinJoin-based techniques leverage the collaborative nature of Bitcoin transactions to enhance privacy and anonymity. By allowing multiple users to jointly create a single

transaction with their inputs, CoinJoin techniques enable the breaking of the "common input ownership" heuristic and help conceal the relationships between sender and recipient addresses. These techniques offer several advantages, including the elimination of a single point of failure by removing the need for trusted third parties, as well as the prevention of theft and the removal of mixing fees in most cases.

CoinJoin

CoinJoin [76] is a specific implementation of a CoinJoin-based technique. It enables users to participate in a joint transaction where multiple inputs from different users (e.g., inputs A, B, and C) are combined with corresponding outputs (e.g., outputs A', B', and C') to create a single transaction. One notable feature of Bitcoin is that each input must be signed independently using the associated private key. Exploiting this property, users can collaborate and contribute their inputs and outputs to create a CoinJoin transaction.

Users may include change addresses (Ch_A, Ch_B, and Ch_C) to receive any remaining coins from the transaction (see Figure 4.8). It is crucial that all users spend the same amount of coins to avoid revealing any relationships based on different input and output values. Once the joint transaction is constructed, each participant signs the transaction independently, and one user then broadcasts the signed transaction to the Bitcoin network.

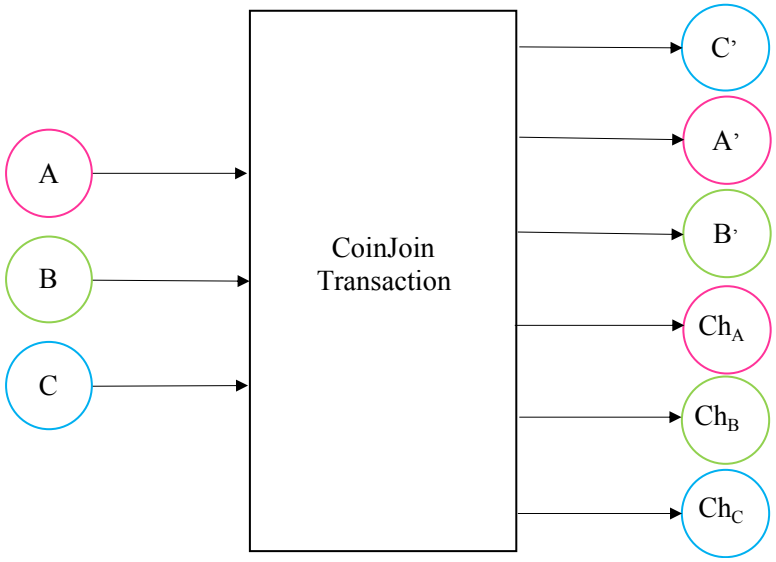


Figure 4.8: CoinJoin Transaction

CoinJoin offers a practical way for users to collaborate and obfuscate the connections between their inputs and outputs. By jointly participating in a CoinJoin transaction, users can significantly enhance their transactional privacy and make it more difficult for external observers to link specific inputs to corresponding outputs. This technique achieves privacy without the need for a trusted intermediary, empowering users to directly collaborate and take control of their own privacy.

CoinShuffle

CoinShuffle [111] is an enhanced version of CoinJoin that incorporates the Dissent protocol[112] to provide untraceability against mixing users. By leveraging peer-to-peer communication, CoinShuffle allows users to discover each other and collaborate in a privacy-preserving manner. The protocol ensures that the mixing process is resistant to tracing and manipulation, making it difficult for external observers to link inputs and outputs.

To initiate a CoinShuffle transaction, users first establish a network among themselves using a peer-to-peer protocol. Each user, except for the initial user (Alice), generates a fresh encryption-decryption key pair and announces the corresponding public encryption key. Alice takes her output address A' and encrypts it with layered encryption using the encryption keys of all the participating users. She then sends the encrypted output to Bob (see Figure 4.9). Bob decrypts the received message using his own encryption key and encrypts his output address B' with the remaining encryption keys. He shuffles the encrypted outputs and forwards them to the next user in the protocol.

This process continues as each user in the network decrypts the received message, adds their own encrypted output address, shuffles the list, and passes it to the subsequent user. The final user in the protocol receives all the shuffled encrypted outputs, adds their own output address, shuffles the entire list once more, and sends it back to all users. Each user can then verify if their own output address is present in the shuffled list.

Once the list of shuffled encrypted outputs is finalized, each user constructs a transaction that includes all the inputs from the participants and maps them to the corresponding shuffled outputs. The users sign their individual transactions and broadcast the signatures to one another. One of the participants can then aggregate the signatures and create a fully signed transaction, which can be published to the Bitcoin network. It is important to note that in case of a malicious user, the protocol enters a blame phase where the malicious user is identified, excluded from the process, and the protocol restarts to ensure the integrity of the mixing.

CoinShuffle++

CoinShuffle++ is an advanced iteration of CoinShuffle that incorporates the DiceMix protocol to achieve parallel processing of mixing transactions [113]. While its predecessor, CoinShuffle, required a linear number of communication rounds and was dependent on the number of users, CoinShuffle++ leverages DiceMix to perform mixing in parallel, regardless of the number of participants. This parallel processing approach significantly reduces the time required for mixing transactions. For example, even with 50 users, CoinShuffle++ can complete a mixing transaction within eight seconds.

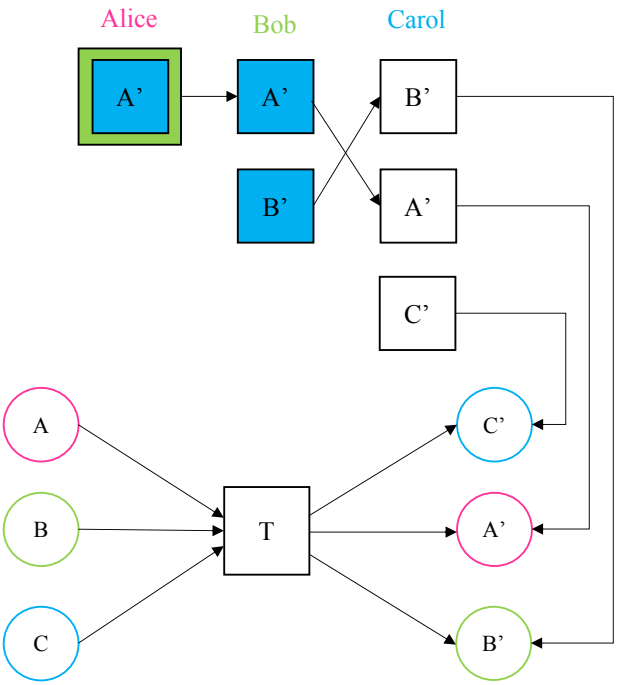


Figure 4.9: CoinShuffle

ValueShuffle

ValueShuffle extends the capabilities of CoinShuffle++ by combining it with confidential transactions ((CT)) and stealth addresses [114]. By incorporating confidential transactions, ValueShuffle introduces transaction value privacy, which represents a significant improvement over previous protocols. With CT, the transaction amounts are hidden from external observers, enabling users to mix different amounts of coins together while preserving privacy. However, it is important to note that the use of confidential transactions requires a soft-fork of the existing Bitcoin protocol.

In addition to confidential transactions, ValueShuffle incorporates the concept of stealth addresses to enhance recipient anonymity, which is often referred to as "unlinkability." Stealth addresses enable the sender to directly send the coins to the recipient's address while improving the recipient's privacy. A stealth address is a unique one-time address generated by the sender specifically for the recipient, ensuring that the recipient's identity remains protected.

CoinJoinXT

CoinJoinXT introduces a novel approach to CoinJoin transactions, offering enhanced privacy and flexibility [115]. In this protocol, users collaborate to create a joint funding address through the use of multi-signatures. This funding address serves as a centralized pool of funds that are jointly controlled by the participants.

To initiate the CoinJoinXT process, users collectively sign a set of spending transactions from the funding address in advance. These spending transactions are designed to disburse the funds to their intended recipients. Importantly, each spending transaction is assigned a specific timelock, preventing all transactions from being published simultaneously. The spending transactions can be structured as a chain or a tree, depending on the desired transaction flow. In either case, the transactions require the signatures of all participating parties for validation.

Once the participants have verified the signatures on the spending transactions, they can proceed to broadcast the funding address. Additionally, participants have the option to include their own unspent transaction outputs (UTXOs) in the subsequent transactions, further consolidating their funds. However, to mitigate the risk of double-spending, participants must also create and pre-sign a backout transaction for each round, which includes a specified timelock.

To enhance privacy and prevent subset-sum attacks, CoinJoinXT participants can leverage off-chain techniques such as the Lightning network. By utilizing a payment channel within the Lightning network, participants can route a portion of the transaction outputs to the channel, gradually shifting the balance over time. This off-chain privacy measure adds an additional layer of security and anonymity to the CoinJoinXT process.

Furthermore, CoinJoinXT addresses the distinguishability issue that arises from multi-signatures in a Pay-to-Script-Hash (P2SH) script. This is achieved through the adoption of Schnorr signatures [116] or Scriptless ECDSA-based Construction [117]. By utilizing these advanced cryptographic techniques, CoinJoinXT can construct 2-of-2 multi-signature transactions, similar to Pay-to-Public-Key-Hash (P2PKH) transactions, without revealing the underlying multi-signature nature of the transactions.

Snicker

Snicker is a non-interactive CoinJoin protocol introduced by Gibson [118]. It offers a convenient method for achieving CoinJoin transactions without the need for a centralized server or direct interaction between participants. Snicker is particularly well-suited for CoinJoin transactions involving two parties, where one participant (Alice) encrypts the transaction proposal using the public key of the other participant (Bob).

To initiate a Snicker CoinJoin, Alice scans the blockchain to identify potential participants based on the criteria of their UTXOs, such as the amount and age of the UTXOs. This scanning process can be facilitated by blockchain explorers, and Alice only needs to download the relevant data to identify active users. Once potential participants are identified, Alice creates a CoinJoin proposal, which includes various elements such as her own UTXO, the desired recipient address, the transaction amount, the transaction fee, and a transaction template that combines the UTXOs of both Alice and Bob.

To ensure the security and privacy of the proposal, Alice encrypts the message using Bob's public key. The encrypted message contains additional crucial information, such

as Alice's signature on the transaction and a recipient address for Bob that is generated by adding a value (k'G) to either Bob's existing reused public key (Version-1) or the R value in one of Bob's signatures (Version-2). Notably, Alice also includes the value k' within the encrypted message, enabling Bob to derive the private key corresponding to the newly generated public key.

Once the encrypted message is created, Alice can share it with Bob via a public network, such as a bulletin board or other suitable communication channels. Bob, upon receiving the encrypted message, decrypts it using his private key, verifying the ownership of the newly proposed public key. Bob can then sign the transaction and broadcast it to the Bitcoin network.

PayJoin

PayJoin, also known as Pay-to-EndPoint (P2EP), is a privacy-enhancing technique for Bitcoin transactions that was introduced in a blog post by Blockstream [119]. The concept was further developed and refined in subsequent proposals such as BustaPay [120] and PayJoin [78].

The primary objective of PayJoin is to mitigate the distinguishability of equal-sized CoinJoin transactions, which could potentially be exploited to flag transactions that have used a mixing technique. PayJoin achieves this by incorporating at least one UTXO from the recipient into the UTXO inputs of the transaction. This inclusion of the recipient's UTXO provides plausible deniability and breaks the common input ownership heuristic.

In simple terms, PayJoin can be seen as performing a CoinJoin transaction while simultaneously making a payment to another party. By doing so, the PayJoin protocol not only enhances the privacy of the participants involved in the PayJoin transaction but also provides privacy benefits to other Bitcoin users.

One of the key privacy features of PayJoin is the ability to hide the true payment amount. In a PayJoin transaction, the total output of the transaction is the sum of the payment amount and the recipient's input amounts. This ensures that outside observers cannot easily distinguish the actual payment amount being transferred.

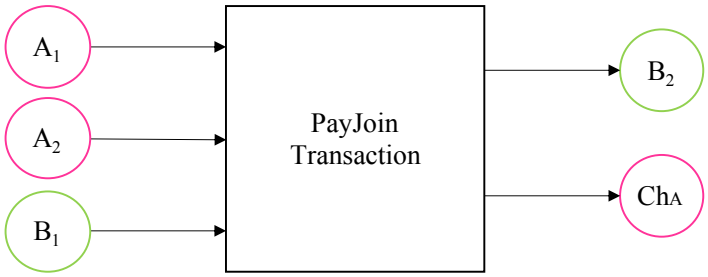
The PayJoin protocol follows a specific set of steps for its execution, as outlined in BIP (Bitcoin Improvement Proposal) 78 [121]. The protocol involves two parties: the sender (Alice) and the recipient (Bob). To initiate the protocol, Bob sends his address and the payment amount to Alice using a BIP21 URI. Alice then creates and signs an initial transaction, referred to as the original transaction, in which she sends the specified payment amount to Bob's address. Alice also provides her change address to receive any remaining funds and sends the transaction to Bob for verification.

Upon receiving the original transaction, Bob examines it and creates a new transaction known as the PayJoin proposal. In this proposal, Bob appends his own inputs to the transaction created by Alice. He then adjusts the output amount by adding his input

amounts to the transaction. Bob signs his inputs and sends the PayJoin proposal back to Alice.

Alice reviews the PayJoin proposal, verifies its correctness, and signs the transaction if everything is in order. Once the transaction is signed by Alice, she broadcasts it to the Bitcoin network. If any issues arise during the creation of the PayJoin transaction, Bob still has the option to broadcast the original transaction.

However, a naive implementation of the protocol, particularly in relation to participant coin selection, has the potential to trigger the identification of these transactions as involving unnecessary inputs (referred to as UHI2, as seen in 3.3.1). One potential countermeasure to prevent UHI2 in PayJoin transactions involves the recipient adding an input that surpasses the change address of the sender (represented as Ch_A in Figure 4.10). This adjustment ensures that the minimum output is lower than the minimum input, effectively categorizing the transaction as a regular payment transaction.



Ch_A: Alice's change address.

Figure 4.10: PayJoin

4.3.4 Threshold Signature

Threshold signature techniques introduce the concept of joint signatures, which require a specified threshold of signatures to redeem a transaction. These techniques provide enhanced security and resilience by distributing signing authority among multiple participants.

CoinParty

CoinParty, proposed by Ziegeldorf et al. in [27], is a protocol that utilizes mixing peers to achieve plausible deniability in transaction mixing. It introduces a threshold variant of the Elliptic Curve Digital Signature Algorithm (ECDSA) (inspired by [122]) based on Secure Multi-party Computation (SMC).

The protocol can be divided into two main phases: the escrow phase and the shuffling phase. In the escrow phase, mixing peers generate a set of escrow addresses (T_1, T_2, and T_3) using the threshold ECDSA scheme. These escrow addresses are jointly controlled by the mixing peers, and each input peer is assigned a different escrow address. The input

peers commit their coins to the escrow addresses, ensuring that the coins can only be redeemed if a majority of the mixing peers sign the transactions.

In the shuffling phase, input peers employ layered encryption to encrypt their output addresses using the public keys of the mixing peers. They broadcast the encrypted outputs along with the hash of their outputs to the mixing peers, which is used for verification purposes. Each mixing peer decrypts the received outputs, shuffles the addresses, and forwards them to the next peer in the sequence. The last mixing peer shuffles the output addresses and broadcasts them to all the mixing peers. At this stage, the mixing peers verify the shuffled addresses and seed a pseudo-random number generator (PRNG) to obtain a final permutation of the outputs. This ensures that the final peer in the shuffling process cannot manipulate the permutation and guarantees a random shuffling of addresses. Finally, the mixing peers send the coins to the respective output addresses.

To enable the joint signing of transactions, the private keys of the escrow addresses are shared among the mixing peers. This allows for the application of a threshold variant of ECDSA, where each transaction is created and signed collaboratively.

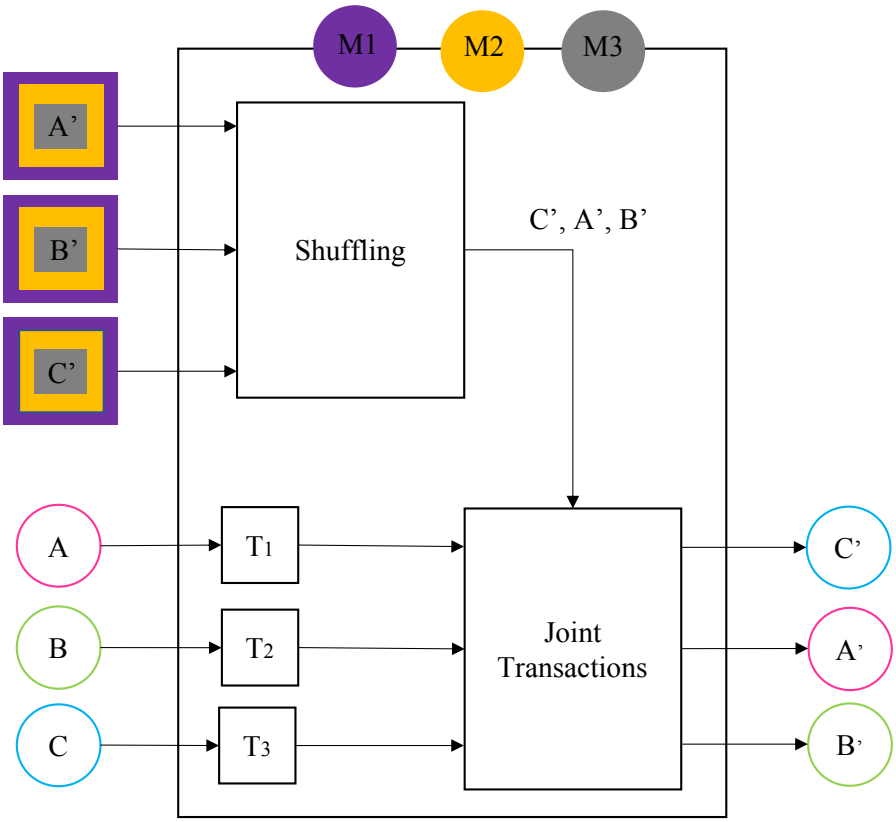


Figure 4.11: CoinParty, inspired by [27]

SecureCoin

SecureCoin, proposed by Ibrahim et al. in [123], is a protocol that leverages threshold digital signatures to achieve coin mixing. The protocol aims to enhance privacy and security by ensuring that transactions are jointly signed by a specified threshold of users.

The protocol begins with the generation of a joint address (J) in a threshold manner. To achieve this, the participating users collectively compute a public key that corresponds to the joint address. Once the joint address is generated, the users collaboratively initiate a transaction (T_1) in which they send their coins to address J (Figure 4.12).

In the next step, the users generate fresh recipient addresses and perform address shuffling to obfuscate the link between input and output addresses. This shuffling process and the handling of misbehaving users follow a similar approach to CoinShuffle. Each user encrypts their recipient address and sends it to the next user in the sequence, who decrypts the message and adds their own recipient address. If any user is found to be behaving maliciously, the protocol enters the accusation phase, during which the malicious user is excluded, and the shuffling process is repeated by the remaining honest users. This ensures that the mixing process remains secure and prevents malicious users from compromising the privacy and integrity of the protocol.

In the final step, the users collectively create a transaction (T_2) that transfers the coins from address J to the recipient addresses of the honest users, as well as the input addresses of users who were excluded during the accusation phase. This ensures that each user can retrieve their coins, even if they were previously involved in malicious behavior. For the transaction to be considered valid and complete the protocol, a threshold majority of the users must jointly sign the transaction, thereby ensuring that the transaction is authorized by a trusted subset of the participants.

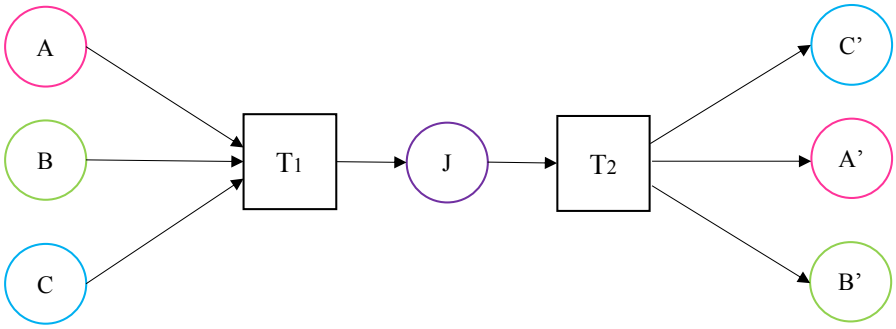


Figure 4.12: Securecoin

Secure Escrow Address (SEA)

Secure Escrow Address (SEA), proposed by Wang et al. in [124], is a decentralized protocol that utilizes distributed key generation and address shuffling techniques to enhance the privacy and security of coin transactions. The protocol aims to create a

temporary address, jointly controlled by the users, where the coins are initially sent before being transferred to the recipients' addresses.

The protocol begins by employing distributed key generation, based on the approach proposed by Gennaro et al. in [125], to collectively create a public key associated with the joint address (J). This joint address is used as a temporary holding location for the coins. Each user involved in the protocol possesses a share of the secret required to redeem the coins from address J, ensuring that no single user has complete control over the transaction.

Following the joint address generation, each user independently generates their own encryption-decryption key pair, similar to the process used in CoinShuffle [111]. The users then perform address shuffling by employing layered encryption techniques. This shuffling process obfuscates the link between the original sender and the intended recipients. The final user in the shuffling sequence broadcasts the shuffled list of recipient addresses.

Each user participating in the protocol checks the shuffled list to verify if their recipient's address is included. This verification step ensures that the intended recipients are correctly identified and prevents any tampering or unauthorized changes to the address list. If the verification is successful and all the addresses are in order, the users proceed to create a transaction that transfers the coins from address J to the respective recipients' addresses.

To redeem the coins from the temporary address J, each user must sign the transaction using their individual share of the secret obtained during the distributed key generation phase. This ensures that the transaction is authorized and authenticated by the collective agreement of the participating users, providing a robust level of security and preventing unauthorized access to the coins.

It is important to note that the proposed SEA protocol in the research paper has not been implemented, and there are no specific test results or evaluations provided to demonstrate the functionality and performance of the distributed key generation scheme within the ECDSA scheme. Further research and experimentation would be required to assess the practicality and effectiveness of SEA in real-world scenarios.

4.4 Evaluation criteria

This section focuses on evaluating the privacy, security, and efficiency properties of the selected mixing techniques. The evaluation criteria used in this study are based on commonly employed metrics found in recent research.

Figure 4.13 presents a comprehensive selection of criteria that have been extensively addressed in the literature and will be used to evaluate the mixing techniques.

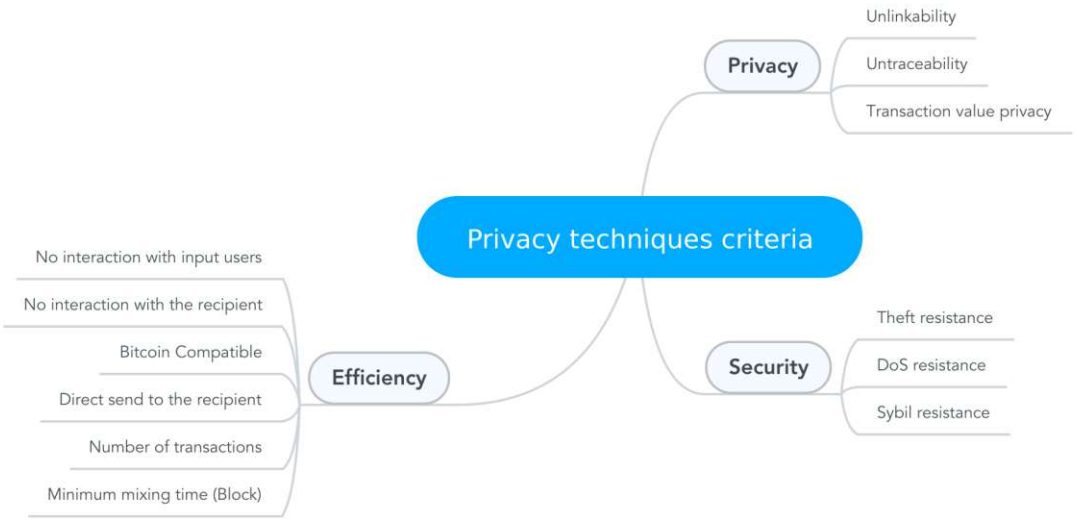


Figure 4.13: Privacy techniques criteria

4.4.1 Privacy criteria

Anonymity Set: The anonymity set refers to the number of participants involved in a mixing transaction. A larger anonymity set provides greater anonymity and makes it more difficult to link transactions to specific participants.

Unlinkability: *"Unlinkability ensures that given two transactions with recipients X and Y, it is computationally infeasible to determine if X=Y"*[126].

Untraceability. "*Untraceability guarantees that within a transaction involving multiple input addresses, it is impossible to identify the specific sender. All senders appear equiprobable, making it challenging to distinguish the true sender among the input addresses.*" [126].

Transaction Value Privacy: Transaction value privacy aims to protect the privacy of transaction amounts from blockchain data analysis. It ensures that the transaction value remains confidential and cannot be easily inferred by analyzing the transaction data.

These privacy criteria provide a comprehensive evaluation framework for assessing the effectiveness and robustness of mixing techniques in preserving user privacy. By analyzing and comparing these criteria across different techniques, the strengths and weaknesses of each approach can be identified, enabling researchers to make informed decisions about their selection and potential improvements.

4.4.2 Security Criteria

Theft Resistance: Theft resistance ensures that the coins involved in the mixing protocol cannot be stolen during the execution of the protocol. The protocol should be

designed in such a way that it prevents unauthorized parties from gaining control over participants' funds or manipulating the transaction process to steal coins.

DoS Resistance: DoS resistance refers to the ability of the protocol to withstand Denial-of-Service (DoS) attacks. Participants should not be able to refuse or disrupt the computation of the transaction, particularly in decentralized peering scenarios. Robust measures should be in place to prevent malicious participants from intentionally obstructing or delaying the protocol execution.

Sybil Resistance: Sybil resistance ensures that an attacker cannot participate in the protocol using multiple identities or accounts. By preventing Sybil attacks, the protocol maintains the privacy and security of the participants by making it difficult for an attacker to identify the relationship between sender and recipient addresses.

These security criteria play a vital role in assessing the effectiveness of the mixing techniques in providing a secure environment for participants. By evaluating the techniques against these criteria, their ability to protect against theft, resist DoS attacks, and prevent Sybil attacks can be assessed. It is crucial to ensure that the selected techniques offer robust security measures to safeguard participants' assets and prevent any unauthorized access or malicious activities.

4.4.3 Efficiency Criteria

No Interaction with Input Users: This criterion evaluates whether the mixing technique requires interaction with other participants during the peering process to create a transaction. Techniques that minimize or eliminate the need for direct interaction between input users enhance efficiency by reducing the communication overhead and complexity of the protocol.

No Interaction with the Recipient: Similar to the previous criterion, this criterion assesses whether the mixing technique necessitates direct interaction with the recipient to create the mixing transaction. Minimizing the interaction with the recipient streamlines the process and simplifies the user experience.

Bitcoin-Compatible: Bitcoin compatibility refers to the extent to which the mixing technique is compatible with the existing Bitcoin blockchain. Techniques that align well with the underlying Bitcoin infrastructure enable seamless integration and facilitate compatibility with features such as blockchain pruning, where unnecessary data is pruned from the blockchain to reduce storage requirements.

Direct Send to the Recipient: Direct send to the recipient evaluates the technique's ability to send the mixed coins directly to the recipient's address, bypassing the need to send them first to a new address of the sender and then to the recipient. This criterion assesses the efficiency and convenience of the technique by reducing the number of intermediary steps involved in the transaction.

Number of Transactions: The number of transactions criterion evaluates the minimum number of transactions required to complete the mixing protocol. Techniques that

Table 4.1: Evaluation of privacy techniques

		Anonymity set*	Unlinkability	Untraceability	Value privacy	Theft resistance	DoS resistance	Sybil resistance	No interact-input	No interact-recipient	BTC-compatible	Direct send	no. of Trx	no. of Block
		Privacy				Security			Efficiency					
Centralized mixers	Mixing websites	Large/ -	○	◑±	○	○	●	●	●	●	●	●	2	2
	MixCoin [26]	Large/ -	○	◑±	○	○×	●	●	●	●	●	●	2	2
	BlindCoin [94]	Large/ -	○	●	○	○×	●	●	●	●	●	●	2	4△
	LockMix [96]	Large/ 1000 in 143s	○	●	○	◑•	●	●	●	●	●	●	4	6
	Obscuro [97]	Large/ 430 in 1s	○	◑±	○	●	●	●	●	○	◑	●	2	2
Atomic swap	FairExchange [99]	Large/ -	○	◑±	○	●	●	○	○	●	●	●	4	3
	Xim [100]	Large/ -	○	◑±	○	●	●	●	○	●	●	●	7	X *
	CoinSwap [101]	Large/ -	○	◑±	○	◑◇	●	●	●	○	●	●	4	2
	New CoinSwap [103]	Large/ -	○	◑±	○	●	●	●	●	●	●	○	4	2
	PaySwap [107]	Large/ -	○	●	◑	●	●	●	●	●	●	○	4	2
	BSC [109]	Large/ -	○	●	○	●	●	●	●	○	◑◇	●	4	3
	TumbleBit[33]	Large/ 800 in 0.6s	○	●	○	●	●	●	●	○	●	●	4	2
CoinJoin-based	CoinJoin [76]	Small/ -	○	◑±	○	●	○	○	○	●	●	○	1	1
	CoinShuffle [111]	Small/ 50 in 3m	○	●	○	●	◑‡	○	○	●	●	○	1	2
	Coinshuffle++ [113]	Moderate/ 50 in 8s	○	●	○	●	◑‡	○	○	●	●	○	1	2
	ValueShuffle [114]	Moderate/ 50 in 8s	●	●	●	●	◑‡	○	○	●	◑◇	●	1	1
	CoinJoinXT [115]	Large/ -	○	◑±	◑	●	●††	●	○	●	●	●	X*	X*
	Snicker [118]	Small/ -	○	◑±	○	●	○	○	●	●	●	○	1	1
	PayJoin [86]	Large/ -	○	◑±	◑	●	●	●	○	○	●	●	1	1
Thres-holdsig	CoinParty [27]	Large/ 50 + 15 MP◇◇ in 30s	○	●	○	◑⊕	◑‡	○	○	●	●	○	2	2
	SecureCoin [123]	Moderate/ 31 in 1s	○	●	○	◑⊕	◑‡	●	○	●	●	○	2	2
	SEA [124]	Moderate/ -	○	●	○	◑	◑‡	●	○	●	●	○	2	2

●Full coverage◑Partial coverage○No coverage

* Test results from the papers are also provided.
± Internal traceability.
× Theft is detected, but it is not prevented.
• It is possible in lose-lose or get nothing-scenarios.
◦ In the case of the malleability of initial transactions.
†† In two-party cases.
⊕ If 2/3 of users are honest.
◇◇ Mixing peers.
‡ Prevented by finding and excluding the malicious participant.
◇ Soft-fork is required.
△ Two blocks for public log messages plus two blocks for two transactions.
* It is a two-party transaction,
so it needs many mixing transactions to achieve a large anonymity set.

minimize the number of transactions reduce transaction fees, blockchain bloat, and computational overhead, leading to increased efficiency and cost-effectiveness.

Required Blocks: This criterion assesses the minimum number of blocks needed to complete the mixing protocol. Given that the average time to mine a block in Bitcoin is around 10 minutes, reducing the required number of blocks ensures the protocol's timely completion. Techniques that can achieve efficient mixing within a shorter timeframe contribute to better transaction speed efficiency.

By evaluating the mixing techniques against these efficiency criteria, their practicality and usability can be assessed. Techniques that minimize user interactions, are compatible with the Bitcoin blockchain, and achieve efficient mixing with fewer transactions and blocks contribute to a more streamlined and user-friendly experience.

4.5 Evaluation of the Techniques

In table 4.1 we evaluate the techniques (centralized mixers, atomic swap, CoinJoin-based, and threshold signatures), which illustrates the comparison of the techniques in terms of privacy, security, and efficiency. It also includes a review of their practical implementation

and explores potential areas for future research. In what follows, we investigate the techniques in detail, according to the defined criteria.

4.5.1 Privacy

Anonymity set.

Most of the evaluated techniques, except for some CoinJoin-based techniques, can provide a large anonymity set and be hidden among other transactions in the blockchain. In the case of CoinJoin-based techniques, the size of the anonymity set is influenced by the transaction size. Combining multiple transactions into a single CoinJoin transaction can provide a larger anonymity set, but coordinating a large number of participants to create such a transaction can be challenging in practice. This is due to the increased risk of DoS and Sybil attacks, as well as the communication overhead involved. However, advancements in protocols like CoinShuffle++ and ValueShuffle, which leverage techniques like Dicemix to enhance peering among participants, have made it possible to achieve reasonable anonymity sets with a moderate number of participants. For example, CoinShuffle++ and ValueShuffle can facilitate the creation of a transaction with 50 participants in just 8 seconds, ensuring a reasonable level of anonymity within this set size.

Coinswap techniques, on the other hand, aim to achieve anonymity by hiding transactions among others with the same value. By implementing two-party ECDSA and making multi-signature transactions appear as single-signature transactions, coinswap techniques effectively provide anonymity for these transactions. The anonymity set in atomic swap techniques can also be large, although the use of timelock transactions in these techniques may limit the size of the anonymity set, as discussed by Moser and Bohme. [102].

Considering the evaluation of anonymity sets, it is important to strike a balance between achieving a sufficiently large set to enhance privacy while also addressing the practical challenges associated with coordination, scalability, and potential vulnerabilities related to anonymity set size.

Unlinkability.

In all techniques, users should create fresh addresses to receive mixed coins. However, there is no guarantee that these addresses will not be used in the future. Therefore, those addresses and their transactions can be linked to each other, which consequently can be used in a transaction graph analysis.

ValueShuffle stands out as a technique that specifically addresses unlinkability by utilizing stealth addresses as one-time-use payment addresses. By employing stealth addresses, ValueShuffle ensures that the receiver's address used in a transaction is ephemeral and cannot be linked to subsequent transactions. The concept of stealth addresses can be applied to other mixing techniques to enhance unlinkability as well. For instance, Darkwallet, an implementation of CoinJoin, integrated stealth addresses into its design. However, it is worth noting that Darkwallet has not received updates since 2015 [127],

and further research and development are needed to explore the full potential of stealth addresses in improving unlinkability across various mixing techniques.

It is important to recognize that the effectiveness of unlinkability achieved through stealth addresses is confined to the subset of users who employ them [102]. In other words, the unlinkability of transactions utilizing stealth addresses is limited to interactions within the specific group of users utilizing this feature. Therefore, the overall privacy provided by mixing techniques should consider the extent of adoption and usage of advanced features like stealth addresses, as their effectiveness relies on a critical mass of users incorporating them into their transactions.

To enhance unlinkability further, continuous efforts should focus on promoting best practices for address management, encouraging users to consistently generate fresh addresses and avoid address reuse. Additionally, the development of novel techniques and mechanisms that go beyond the traditional address-based models could offer new avenues to strengthen unlinkability and protect users' privacy in mixing transactions.

Untraceability.

The enhancement of untraceability in transactions is a common goal across all the evaluated techniques. However, it is important to note that some techniques offer partial coverage of this feature, which introduces internal traceability. The latter refers to the ability to trace the relationship between the inputs and outputs among the participants involved in a specific mixing transaction. In such cases, participants have access to the data of other users, which can potentially result in information leakage and compromise privacy.

While internally traceable techniques allow for traceability among the participants, they still provide privacy against blockchain analysts. This means that even though internal traceability exists, the techniques effectively safeguard transactions from being traced or linked by external entities analyzing the blockchain [102].

It is crucial to strike a balance between the need for untraceability and the potential risks associated with internal traceability. Techniques should be designed and implemented in a way that minimizes the potential leakage of user data and preserves the confidentiality of participants' information. Further research can focus on improving the privacy guarantees of techniques that have internal traceability, exploring methods to mitigate the risks associated with information leakage, and enhancing the overall untraceability of mixing transactions.

Efforts should be made to ensure that the level of untraceability achieved by the techniques is robust and comprehensive, providing users with a high degree of privacy protection against both external blockchain analysts and potential internal adversaries. By addressing the challenges and limitations related to untraceability, the evaluated techniques can offer users greater confidence in the privacy and security of their transactions within the blockchain ecosystem.

Transaction value privacy. The ability to hide the actual payment value in mixing transactions enhances overall transaction privacy. Among the evaluated techniques, ValueShuffle proposes the use of confidential transactions (CT) to conceal transaction values, which requires a soft-fork in the Bitcoin protocol.

If CT are implemented in Bitcoin, all the mixing techniques can benefit from enhanced transaction value privacy, eliminating the need for fixed denomination in the proposed techniques. This would significantly improve the usability and liquidity of other mixing techniques, allowing users to mix their desired number of coins without restrictions. A comparison by [128] evaluates the implementation of CT in TumbleBit and CoinJoin, indicating that CT would reduce the mixing cost for transactions with large values, but increase it for transactions with small values. It should be noted that applying CT to Bitcoin transactions results in an additional factor of nine in transaction fees.

In the context of CoinJoinXT, the chaining of transactions can provide a certain level of value privacy. However, it is important to consider the potential impact of the subset-sum problem, which could potentially compromise this criterion. PayJoin, on the other hand, offers partial value privacy by concealing true payment amounts.

Further research and development are required to explore effective techniques for preserving transaction value privacy without imposing significant overhead. The implementation of confidential transactions or the development of alternative solutions can contribute to strengthening transaction value privacy, offering users greater control over their financial privacy while mitigating the risks associated with precise value attacks. It is crucial to strike a balance between privacy and transaction costs, ensuring that the benefits gained in preserving transaction value privacy outweigh the potential drawbacks, such as increased transaction fees.

4.5.2 Security

Theft-resistance.

The irreversible nature of blockchain transactions poses challenges when it comes to reclaiming stolen or lost coins, making theft-resistance a crucial aspect to consider in evaluating the techniques.

While many of the evaluated techniques strive to address this criterion, it is worth noting that mixing websites typically do not provide theft-resistance. MixCoin and BlindCoin demonstrate that although theft can be detected in these techniques, it cannot be effectively prevented. Incidents of exit scams involving mixing websites have raised concerns and eroded trust in such services, further highlighting the importance of theft-resistance in the context of mixing protocols [33, 129].

Techniques based on threshold signatures, while offering certain security advantages, may not provide robust theft-resistance. These techniques rely on the assumption that the majority of users in a peer-to-peer network are honest and trustworthy. However,

achieving such a majority consensus can be challenging, making it difficult to ensure strong theft-resistance in practice.

On the other hand, atomic swap and CoinJoin-based techniques have the potential to provide theft-resistance in the envisioned protocols. By leveraging the properties of atomic swaps, participants can securely exchange their assets without the risk of theft or loss. Similarly, CoinJoin-based techniques enable users to pool their transactions, obscuring the individual ownership of coins and reducing the likelihood of theft.

DoS resistance.

Ensuring resistance against Denial-of-Service (DoS) attacks is an important security criterion for any transaction protocol, including mixing techniques. DoS attacks aim to disrupt the normal operation of a system by overwhelming it with malicious or invalid requests, causing a denial of service to legitimate users.

In the evaluation of techniques, it is observed that most CoinJoin-based and threshold signature techniques lack inherent DoS resistance. These techniques rely on the assumption that participants will behave honestly during the protocol. If malicious users intentionally disrupt the protocol, it can result in service disruptions or delays for other participants. Thus, preventing DoS attacks in these techniques becomes a challenge.

To address this issue, some techniques such as CoinShuffle and CoinShuffle++ propose measures to mitigate DoS attacks. These measures include finding and excluding malicious users, rerunning the protocol to circumvent disruptions caused by malicious users, and locking a malicious user's Unspent Transaction Output (UTXO). While these measures can help mitigate the impact of DoS attacks, they may not provide perfect prevention against determined attackers.

Among the CoinJoin-based techniques, PayJoin stands out as a DoS-resistant technique. In PayJoin, if the sender refuses to sign the PayJoin transaction, the recipient has the ability to broadcast the original transaction. This mechanism ensures that the protocol can proceed even if one party attempts to disrupt it, making PayJoin more resilient to DoS attacks compared to other CoinJoin-based techniques.

On the other hand, centralized mixers and atomic swap techniques inherently exhibit DoS resistance. In these techniques, none of the participants have the ability to unilaterally abort the protocol or disrupt the transactions of others. This characteristic ensures that the mixing process can continue uninterrupted, even in the presence of malicious participants.

To enhance the DoS resistance of mixing techniques, future research should focus on developing robust mechanisms to detect and mitigate attacks, as well as exploring techniques that minimize the impact of malicious users on the overall protocol.

Sybil resistance.

To prevent Sybil attacks, many techniques employ the use of upfront fees. Participants are required to pay a fee before they can join the mixing process. This fee serves as a

deterrent to Sybil attackers, as they would need to invest significant resources to create and maintain a large number of fake identities, making the attack economically unfeasible.

However, it is important to note that not all techniques provide upfront fees as a means of Sybil resistance. CoinJoin, CoinShuffle, CoinShuffle++, and ValueShuffle, for instance, do not incorporate upfront fees into their protocols. As a result, these techniques are categorized as not-Sybil-resistant. This means that they may be more vulnerable to Sybil attacks compared to techniques that enforce upfront fees.

To enhance Sybil resistance in mixing techniques, future research could explore alternative mechanisms or incentives that discourage Sybil attackers. These mechanisms should be designed to impose significant costs or barriers on attackers attempting to create and control multiple identities within the system.

4.5.3 Efficiency

No interaction between input users.

In the context of this criterion, it is worth noting that all centralized mixers and the majority of atomic swap techniques do not necessitate any interaction between input users. These techniques rely on a central entity or an automated process to handle the mixing operations, eliminating the need for direct communication among the participants. This characteristic can be advantageous in terms of user experience, as it simplifies the process and reduces the burden on users.

On the other hand, most CoinJoin-based techniques typically require interaction between input users at various stages of the protocol execution. For example, participants may need to register their inputs, collaborate in the creation of the mixing transaction, and sign the transaction. These interactions ensure the proper coordination and execution of the CoinJoin process. However, it also introduces additional challenges, such as the need for synchronous communication, potential delays caused by participants' unavailability or lost connections, and the increased risk of protocol failure due to the absence of any participant.

Similarly, threshold signature techniques also require interaction between input users, particularly during the signing phase of the transaction. This interaction is essential to achieve the necessary threshold of signatures and ensure the security and validity of the mixed transaction.

Techniques that minimize or eliminate the need for interaction between input users offer advantages in terms of usability and convenience. They allow for smoother and faster execution of the mixing process, reducing the reliance on participants' active involvement.

No interaction with the recipient.

Among the evaluated techniques, Obscuro, PayJoin, and PaySwap rely on interaction with the recipient, meaning that the recipient needs to be online and actively participate in the protocol to complete the mixing process. This requirement can introduce challenges,

as it relies on the availability and responsiveness of the recipient. If the recipient is not online or unwilling to participate, it can delay or hinder the completion of the protocol.

In contrast, techniques such as CoinSwap, BSC, and TumbleBit initially require interaction with the recipient in their original protocols. However, an interesting approach to circumvent direct recipient interaction is for the sender to assume the recipient's role through different identities. In this scenario, the sender receives the mixed coins at their own newly generated address and then performs an additional transaction to send the mixed coins to the final destination address. By assuming the recipient's role, the sender can effectively avoid direct interaction with the actual recipient, providing a level of convenience.

The absence of interaction with the recipient can enhance the usability of the mixing protocols, as it reduces dependencies on the recipient's availability and active participation. However, it is essential to consider the trade-offs associated with this characteristic. For instance, assuming the recipient's role may introduce additional complexities in the protocol, requiring the sender to manage multiple identities and perform additional transactions.

Direct send to the recipient.

In some of the evaluated techniques, such as CoinJoin-based and threshold signature techniques, a common challenge arises where the participant needs to first send the coins to their own address before forwarding them to the final destination address. This problem mainly occurs when the protocol enters the blame phase, and the participant is required to provide a new output. ValueShuffle addresses this problem by utilizing stealth addresses. Stealth addresses allow for the creation of one-time-use payment addresses, ensuring that the coins can be directly sent to the recipient without the need for intermediate addresses.

To address this problem in other CoinJoin-based and threshold signature techniques, further research can explore the potential application of stealth addresses or similar cryptographic techniques. Investigating the feasibility and impact of incorporating stealth addresses into these protocols can provide valuable insights into enhancing their usability. Additionally, considering alternative approaches that enable direct send to the recipient without compromising the anonymity guarantee of the mixing techniques can contribute to the advancement of this criterion. Enabling direct send to the recipient in mixing techniques can streamline the process, reduce transaction complexities and decrease the fees.

Bitcoin-compatible.

Most of the evaluated techniques demonstrate compatibility with the current Bitcoin blockchain implementation. They leverage the existing transaction structure and cryptographic primitives to achieve their mixing functionality. This compatibility ensures that the techniques can be seamlessly integrated into the Bitcoin network without requiring major modifications or disruptions to the underlying system.

However, it should be noted that some techniques have specific requirements or dependencies that may necessitate changes on the Bitcoin blockchain implementation. For example, ValueShuffle relies on the implementation of Confidential Transactions (CT) through a soft-fork. Similarly, the BSC technique requires the implementation of blind signatures through a soft-fork. Obscuro, another evaluated technique, also requires specific changes in the Bitcoin Core implementation to ensure its compatibility. These changes are necessary to support the unique features and functionalities of the Obscuro protocol.

While these techniques may require modifications or enhancements to the Bitcoin blockchain, it is important to assess the feasibility and impact of these changes. This evaluation ensures that the proposed modifications align with the principles and objectives of the Bitcoin network, including security, decentralization, and community consensus.

Number of transactions and required block.

The number of transactions and the required blocks indicated in the last two columns of Table 4.1 provide valuable insights into the operational aspects of the evaluated mixing techniques. These metrics offer an understanding of the delays and transaction fees associated with each technique, which are essential considerations for the participants.

It is crucial to assess the cost that participants would incur when engaging in the mixing process. Apart from the mixing fee, additional transaction fees within the privacy techniques can act as a barrier to their widespread adoption. Even in CoinJoin-based techniques, participants are required to pay at least one additional transaction fee for mixing their coins before transferring them to the destination address. Since a single round of CoinJoin may not provide sufficient anonymity, users often need to perform multiple rounds of mixing to achieve their desired anonymity set. This increased number of rounds consequently leads to a higher number of transactions and blocks that need to be confirmed, resulting in additional costs and potential delays.

Atomic swap techniques, on the other hand, require a minimum of four transactions spread across at least two blocks. These multiple transactions and blocks contribute to the overall costs and introduce additional delays in the mixing process.

Considering the number of transactions and required blocks is vital for participants as it directly affects their user experience, financial expenses, and the time it takes to complete the mixing protocol. Higher transaction volumes and the need for multiple blocks for confirmation can increase the overall complexity and duration of the mixing process, potentially discouraging users from adopting these techniques.

Furthermore, it is worth noting that the transaction fees associated with each technique should be carefully evaluated. These fees are determined by various factors, including the size of the transactions, network congestion, and the prevailing fee market. Participants need to consider these fees in addition to the mixing fees when calculating the overall costs of utilizing the mixing techniques.

4.5.4 Implementation in Practice

The practical implementation of the described mixing techniques varies, with most of them either not being implemented or experiencing significant delays between the release of the protocol and its adoption. Table 4.2 provides an overview of the current implementations, revealing that centralized mixing websites dominate the landscape.

Dumplings [130] highlights the increase in CoinJoin transactions since 2018. It is important to note that the high number of CoinJoin transactions can be attributed to users conducting multiple mixing rounds to achieve a better anonymity set. Joinmarket [108], Wasabi [131], and Samourai [132] are examples of CoinJoin wallet implementations. Joinmarket adopts a taker-maker model, where the taker expresses their interest in performing a CoinJoin transaction, and makers join in and earn fees. In this approach, privacy primarily benefits the taker who initiates the CoinJoin transaction [133]. Wasabi utilizes Chaumian CoinJoin [134], where participants register their inputs and blindly sign the outputs to the coordinator, resulting in a CoinJoin transaction. Samourai introduces Whirlpool, which offers specific pools where users can join and mix their coins with other participants to create CoinJoin transactions. However, it should be noted that in Samourai, the wallet has knowledge of the xpub from which the users' Bitcoin addresses are derived, thereby lacking privacy against the wallet itself [130].

Previous implementations like SharedCoin (until 02.09.2016) [135] by Blockchain.info and Darkwallet (until 23.01.2015) [127], which utilized CoinJoin transactions and stealth addresses, have been discontinued. Joinmarket, Wasabi, and Samourai are commercially available options that we have installed and used. In Chapter 6, we delve into a usability and feature comparison of these wallets.

In 2020, BTCpay integrated PayJoin to enable merchants to accept PayJoin transactions in their stores. Currently, Wasabi, Samourai, Joinmarket, and Bluewallet [136] support PayJoin transactions. The creation of PayJoin transactions between users had already been implemented in the Joinmarket and Samourai wallets.

Shufflepuff [137] is an alpha version available on GitHub, with the latest updates dating back to 2016. The Nxt [138] Coin Shuffling feature has been activated since block 621,000 (09.03.2020) on the mainnet. Nevertheless, it should be noted that, at the time of writing, the CoinShuffle feature has been removed from the Nxt wallet feature list.

According to [102], Fairexchange transactions cannot be identified in the blockchain. However, there is currently no commercial implementation of atomic swap techniques. Recently, a new CoinSwap design and PaySwap wallet have been proposed by [107]. Alpha implementations of TumbleBit can be found on GitHub (NTumbleBit and Breeze), but they are not commercially available as of now.

One major challenge is the technical barrier associated with implementing these privacy techniques in a robust and efficient manner. Developing secure and reliable protocols that can withstand various attacks and provide the desired level of privacy requires extensive research, testing, and optimization. It takes time to ensure that the protocols can

operate effectively in the real-world environment, considering factors such as scalability, compatibility with existing blockchain infrastructure, and interoperability with different wallets and services.

Security concerns also play a crucial role in the delay or absence of practical implementations. Privacy techniques must be thoroughly scrutinized to identify any potential vulnerabilities or weaknesses that could be exploited by malicious actors. Additionally, since these techniques involve financial transactions and the safeguarding of user assets, stringent security measures must be in place to protect against theft, fraud, and other risks. Conducting comprehensive security audits and assessments is essential but can be time-consuming and resource-intensive.

Adoption hurdles pose another challenge for implementing these techniques in practice. Despite the benefits they offer in terms of privacy, users and businesses may be reluctant to adopt new protocols or technologies due to factors such as usability (See Chapter 6), familiarity, and the perceived trade-offs between privacy and convenience. Achieving widespread adoption requires not only technical advancements but also effective education, awareness, and user-friendly interfaces that simplify the process of using these privacy-enhancing tools.

Furthermore, the need for adequate infrastructure and ecosystem support is crucial for practical implementation. For these techniques to be widely adopted and seamlessly integrated into existing blockchain systems, there must be robust infrastructure, such as reliable mixing services, compatible wallets, and supportive regulatory frameworks. Collaboration among various stakeholders, including developers, researchers, wallet providers, exchanges, and regulatory bodies, is essential to create an ecosystem that fosters the implementation and usage of these privacy techniques.

Overcoming these challenges requires a combination of technical advancements, security assurance, user education, and collaborative efforts among industry players. As the field of blockchain privacy continues to evolve, it is expected that more practical implementations will emerge, addressing these challenges and providing users with enhanced privacy options in real-world scenarios.

Table 4.2: Adoption of Bitcoin privacy techniques in practice

Centralized mixers		**CoinJoin based**		**Atomic swap**
Mixing websites adapted from [129]	**CoinJoin**	**CoinShuffle**	**PayJoin**	**TumbleBit**
ChipMixer.com/tumbler.to/	Joinmarket[108]	Shufflepuff[137]	Samouraiwallet	NTumbleBit[139]
BitMix.Biz/MyCryptoMixer.com/	Wasabiwallet[131]	NXT[138]	BTCPay[140]	Breeze[141]
Bitcloak43blmhmn.com/MixerTumbler.com/	Samouraiwallet [132]		Wasabiwallet[131]	
Mixer.money/FoxMixer.com/	Darkwallet [127]		Joinmarket[108]	
MixTum.io/Blender.io	Sharedcoin [135]		Bluewallet[142]	

4.6 Conclusion

This chapter aimed to review and evaluate privacy techniques in the context of Bitcoin, providing insights into their privacy, security, and efficiency characteristics. By comparing selected techniques against defined criteria, we gained valuable insights into their strengths and limitations. However, it is crucial to acknowledge that strong privacy measures often come at the expense of efficiency and usability.

Among the atomic swap techniques, New CoinSwap and its predecessors demonstrated the ability to meet most of the evaluation criteria. However, these techniques require a higher number of transactions, resulting in increased time and fees. On the other hand, CoinJoin-based techniques have gained widespread adoption in practice. While they offer reduced transaction numbers and affordability, they face challenges such as transaction distinguishability and susceptibility to DoS attacks. The recently proposed PayJoin method, based on CoinJoin, shows promise in addressing distinguishability and improving anonymity.

A notable advantage of CoinJoin-based techniques is their ability to achieve privacy with a reduced number of transactions, making them cost-effective. However, multiple rounds of CoinJoin can introduce additional fees and delays. Furthermore, most CoinJoin techniques struggle to provide a large anonymity set and plausible deniability. ValueShuffle's proposal of confidential transactions, which conceal UTXO amounts, presents an effective solution to this challenge, providing indistinguishability for CoinJoin-based techniques.

The number of transactions required in privacy techniques plays a crucial role in concealing the sender-recipient connection. While an increased number of transactions can enhance anonymity, it also incurs transaction fees. Although mixing fees may be negligible, the presence of additional transaction fees could limit the widespread adoption of these techniques among users.

Based on our evaluation, it can be concluded that, apart from centralized mixers and threshold signature techniques, most of the evaluated techniques demonstrate theft resistance. This criterion offers assurance to participants that their coins are protected against theft or loss, which is a critical consideration in payment networks such as blockchain.

Additionally, we examined the practical adoption of these techniques to provide insights into their real-world implementations and any additional features incorporated. It is worth noting that while the primary intention behind ensuring strong privacy is to safeguard user information from malicious adversaries and criminals, it is essential to develop methods that can distinguish transactions used for illicit activities from regular mixing transactions, thus allowing for financial privacy without enabling illicit practices.

Moving forward, future research should focus on addressing the identified limitations and challenges associated with privacy techniques in Bitcoin. This includes exploring innovative methods to enhance privacy while balancing efficiency and usability. Furthermore, efforts should be made to establish regulatory frameworks and industry collaborations

that support the adoption of these techniques, ensuring a balance between privacy and responsible use within the cryptocurrency ecosystem.

In the next chapter, we use Bitcoin as a case study to highlight the inconsistencies between users' privacy expectations and preferences and the current state of privacy solutions. We aim to identify the gap between users' expectations and the practical implementation of privacy techniques and to raise questions regarding the effectiveness of proposed solutions when implemented in real-world scenarios.

CHAPTER 5

User-Perceived Privacy in Blockchain

5.1 Introduction

This chapter studies users' privacy perceptions of UTXO-based blockchains such as Bitcoin. 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.

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 users prefer using add-on privacy techniques on top of Bitcoin or built-in privacy features in privacy coins (e.g., Monero)?
- ii) Are users willing to use privacy-preserving techniques despite the potential higher fees and longer transaction time?
- iii) Do users 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 chapter is structured as follows: In Section 5.2, we describe our quantitative and qualitative study, while in Section 5.3 and Section 5.5, we present the results and discussion. Finally Section 5.6 concludes the chapter.

5.2 Methodology

To investigate user perception of privacy in blockchain, a comprehensive methodology was employed, including multiple rounds of pilot interviews, discussions, and expert consultations. The goal of the methodology was to collect both qualitative and quantitative data to gain insights into users' perceptions and preferences regarding privacy in UTXO-based blockchains like Bitcoin. The methodology encompassed the following steps:

Pilot Interviews and Discussions: Pilot interviews and discussions were conducted with participants who had knowledge and experience in blockchain technology. These sessions helped refine the questionnaire by collecting initial feedback and clarifying technical terms and questions. The insights gained from these pilot sessions ensured the clarity and comprehensibility of the questionnaire.

Blockchain Workshop and Think-Aloud Study: A questionnaire was administered during a Blockchain workshop attended by eleven participants with technical backgrounds. The participants' responses to the questionnaire provided valuable qualitative data on their perception of privacy in blockchain. Additionally, a think-aloud study was conducted with four blockchain experts, where they shared their thoughts and verbalized their decision-making process while interacting with the questionnaire. The think-aloud study provided deeper insights into users' reasoning and thought patterns.

We used the data obtained from the pilot interviews and think-aloud study to improve our questions in the main qualitative and quantitative study.

Expert Consultations: To enhance the quality and rigor of the research, consultations were sought from security and privacy usability experts, a legal expert, and an English proofreader. Their expertise and insights ensured the methodology's alignment with established research standards and improved the overall quality of the study.

Questionnaire Design: The questionnaire underwent iterative revisions based on the feedback received during the pilot interviews, discussions, and expert consultations. The design process of the questionnaire is illustrated in Figure 5.1. The questionnaire was refined to ensure clarity, eliminate ambiguities, and include appropriate technical terms.

Qualitative and Quantitative Evaluation: The research employed both qualitative and quantitative evaluation methods. A qualitative interview was conducted with 14 participants, consisting of both users and non-users of UTXO-based blockchains. Open-ended questions were used to gather in-depth insights into participants' perceptions of

privacy. For the quantitative part, multi-choice options were added to some questions, enabling participants to provide structured responses. The finalized questionnaire, including the qualitative and quantitative components, was published on Survey Monkey to collect data from a broader range of participants.

The overall logic and flow of the questionnaire were defined, taking into account the participants' familiarity with cryptocurrencies and their privacy awareness. Figure 5.2 visually depicts the questionnaire logic, illustrating how participants were directed based on their responses.

Participants' responses were analyzed based on their privacy awareness, perceptions of Bitcoin anonymity, knowledge of de-anonymization attacks, familiarity with add-on techniques and privacy coins, privacy preferences, willingness to pay extra fees or accept delays for enhanced privacy, understanding of privacy issues in public blockchains, and demographic information.

By employing this comprehensive methodology, the research aimed to capture a holistic understanding of users' perceptions, preferences, and awareness of privacy in UTXO-based blockchains. The combination of qualitative and quantitative data provided a rich dataset for analysis and enabled robust conclusions to be drawn regarding users' attitudes toward privacy in blockchain technology.

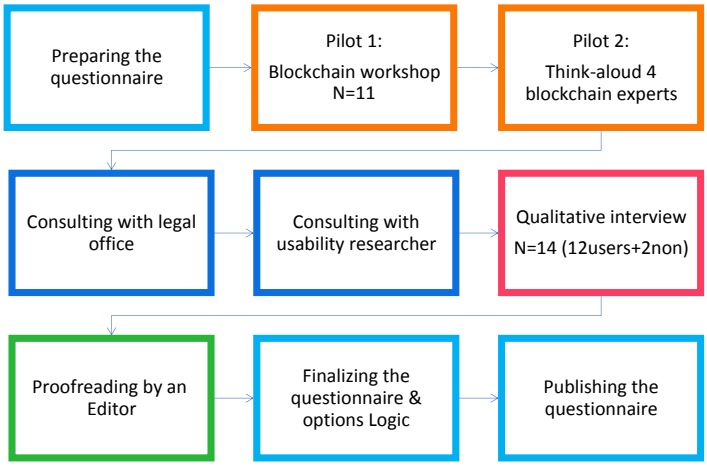


Figure 5.1: Designing the Questionnaire

5.2.1 Qualitative Research

To gain deeper insights into users' perceptions of privacy in blockchain, qualitative research was conducted through semi-structured interviews. This section provides an overview of the interview procedure, recruitment process, coding methodology, and sampling strategy employed in the qualitative research.

Interview Procedure: Prior to the interviews, participants were given a brief introduction to the research context and asked to sign a consent form. The interviews conducted

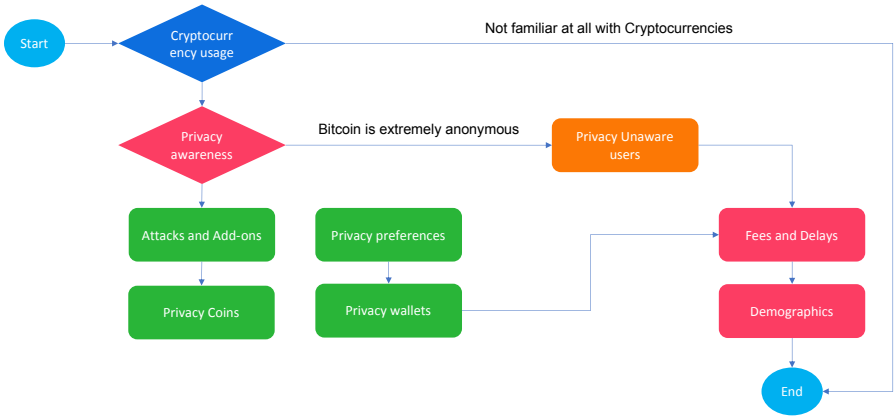


Figure 5.2: Questionnaire Logic

both in-person and via online meetings, had an average duration of 30 minutes. To ensure consistency, an interview guide with open-ended questions (see Appendix 7.3) was developed and used by the researchers. The questions underwent revisions and validation in two pilot rounds to enhance their effectiveness. All interviews were recorded, anonymized, and fully transcribed for analysis.

Recruitment: Participants were recruited through various channels, including social media, universities, and companies with a focus on blockchain technology. Eligibility criteria were defined to ensure a diverse participant pool. Users were required to possess basic knowledge of blockchain and cryptocurrencies, have experience using a cryptocurrency wallet, and have performed a transaction in the past. Non-users, on the other hand, were selected based on their lack of familiarity with cryptocurrencies and absence of prior experience using cryptocurrency wallets or conducting transactions. Additionally, all participants were required to be at least 18 years old. The specific focus on privacy aspects of blockchain and Bitcoin was not disclosed during the recruitment process to ensure participants' responses were based on their genuine knowledge and perceptions.

Sampling: The sampling strategy aimed to capture a diverse range of participants with varying levels of knowledge and usage of cryptocurrencies. Participants were selected based on their reported level of knowledge and experience, ranging from expert to novice users. Fourteen participants were interviewed, including twelve users (age range: 26-45) and two non-users (age range: 35-45). Among the twelve users, seven were employed in IT-related fields. It is important to note that all user participants had owned, bought, or mined cryptocurrencies and had previously conducted transactions.

The demographics of the participants are presented in Table 5.1, providing further details on their backgrounds and characteristics.

Table 5.1: 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%		

Coding

The data collected from the interviews were subjected to coding to identify and group statements related to similar concepts. In each coding round, two security and privacy researchers engaged in discussions to establish the relationships between categories and define higher-level categories where necessary. This iterative coding process allowed for the refinement and addition of options in the quantitative study based on the qualitative findings.

To code the data we followed the suggested coding in Grounded theory. Grounded theory [143] is an iterative and systematic approach used to analyze and code qualitative data. The coding process involves breaking down the data into meaningful units and assigning descriptive labels or codes to each segment. These codes capture the essence of the data and facilitate the identification of patterns, themes, and relationships. It serves as the connection between the initial collection or generation of data and the subsequent development of theories to explain that data [144].

Limitations

While the qualitative research provided valuable insights into users' perceptions of privacy in blockchain, it is important to acknowledge the limitations of the study. The following limitations should be considered when interpreting the findings:

- **Participant Characteristics:** The participants in the study were recruited through various channels, including social media, universities, and companies. Although efforts were made to achieve a diverse sample, there were certain limitations in participant characteristics. For example, there were no participants in the 18-24 and 55-64 age groups, which may limit the generalizability of the findings to these age ranges. Additionally, there were no participants with a high school or college level of education. Therefore, the perspectives and experiences of individuals with these backgrounds are not represented in the study. However, despite these limitations, the sample did encompass participants with diverse knowledge levels, education/work backgrounds, and genders, providing valuable insights within those ranges.

- **Self-Reporting Bias:** The study relied on self-reported information provided by the participants. As with any self-reporting method, there is a possibility of bias or inaccuracies in participants' responses. Participants may have provided socially desirable answers or may have misunderstood or misinterpreted certain questions. However, efforts were made to minimize this bias by ensuring a comfortable and non-judgmental environment during the interviews and by employing a mix of qualitative and quantitative research methods.

- **Generalizability:** It is important to note that the findings of this study may not be fully generalizable to the entire population. The study focused on a specific group of participants who had knowledge of and experience with cryptocurrencies. Therefore, the findings may not fully represent the perceptions and preferences of individuals who have limited access to technology. Further research with a larger and more diverse sample is necessary to enhance the generalizability of the findings.

5.2.2 Quantitative Research

In addition to the qualitative research conducted through interviews, we also conducted quantitative research to gather a larger and more geographically diverse set of participants. This phase of the study involved hosting a survey on the SurveyMonkey platform, allowing us to collect data from a wider range of participants.

Survey Design and Logic: The survey questionnaire was designed to capture quantitative data on users' perception of privacy in UTXO-based blockchains, focusing specifically on Bitcoin and privacy coins. The questionnaire utilized a logic-based structure, where follow-up questions were presented based on the respondents' previous answers. This

approach allowed us to tailor the survey experience to each participant and gather more specific and relevant data.

Sampling Strategy: Our target audience for the survey was Bitcoin users and individuals familiar with UTXO-based privacy coins. To ensure a diverse sample, the questionnaire was distributed through various international channels. We shared the survey on popular Bitcoin forums such as Bitcointalk.org and on social media platforms including Reddit, Telegram, Facebook, Twitter, and LinkedIn. We also reached out to blockchain and cryptography mailing lists, international research centers, researchers, university students, and businesses in our country. In total, we received responses from 101 participants. After applying our exclusion criteria, we obtained a final sample of n = 58 participants who met the necessary criteria for analysis.

Demographics and Cryptocurrency Familiarity: The participants' demographics and cryptocurrency familiarity were captured and analyzed to provide a comprehensive overview of the sample. Table 5.1 presents detailed information on the participants' characteristics, including age, gender, education, and occupation. The majority of participants reported owning, buying, or mining cryptocurrencies (91.38%), and a significant proportion had engaged in at least one cryptocurrency transaction (81.03%). Additionally, 62.96% of participants reported using Bitcoin wallet software.

Self-Reported Roles and Wallet Types: The survey included questions to gather insights into participants' self-reported roles in the cryptocurrency ecosystem and the types of wallets they used. Figure 5.3 illustrates the distribution of self-reported roles, with "investors" and "curious about the technology" being the most commonly selected options. Figure 5.4 provides an overview of the types of wallets used by the participants, with desktop wallets and mobile wallets being among the most frequently reported types.

Through the quantitative research phase, we were able to gather a larger and more diverse dataset, expanding the scope of our study and obtaining a broader range of perspectives. The quantitative findings complement the qualitative insights and contribute to a more comprehensive understanding of users' perceptions of privacy in UTXO-based blockchains.

5.2.3 Ethical Considerations

As researchers conducting this study, we are committed to upholding ethical principles and ensuring the protection of participants' rights and privacy. Our research center, located in Austria, adheres to the European General Data Protection Regulation (GDPR), which sets strict guidelines for the handling of personal data.

Informed Consent: In the qualitative research phase, all participants were provided with consent forms before the interviews. These forms clearly outlined the objectives of the study and the academic context in which the data would be used. The consent forms did not include any personally identifiable information (PII) of the participants, and we assigned unique IDs to each participant for data analysis purposes. By signing the consent forms, participants acknowledged their voluntary participation and gave their informed consent to be part of the study.

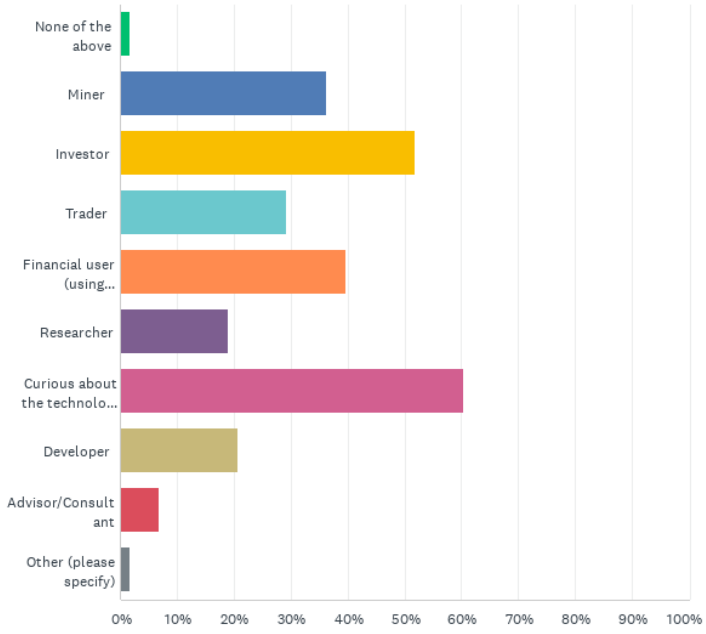


Figure 5.3: Current role in cryptrocurrency

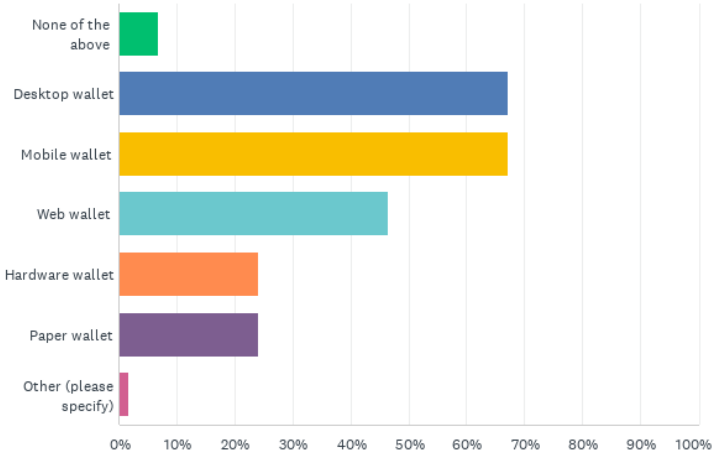


Figure 5.4: Wallet type used by participants

Protection of Privacy: To comply with the GDPR regulations and protect the privacy of participants, we ensured that the questions asked in both the qualitative and quantitative parts of the study did not request any information that could disclose PII. The questions were carefully designed to prevent any inference to the identities of the participants. The collected data was treated with strict confidentiality and anonymized during the analysis process.

Ethical Notice: In the quantitative research phase, at the beginning of the questionnaire, we provided participants with an ethical notice that outlined the research objectives and informed them about their rights as participants. This notice also covered the handling of personal data and informed participants about the raffle that was conducted as part of the study.

5.2.4 Validity and Reliability

To ensure the validity and reliability of our research findings, we employed various measures throughout the data collection and analysis process.

Participant Background: In both the qualitative and quantitative parts, we gathered demographic information, including whether participants studied or worked in IT-related fields. This information allowed us to assess the diversity of our sample and understand the background of the participants. In the qualitative part, 58.33% of participants had IT-related backgrounds, while in the quantitative part, 65.52% of respondents reported similar backgrounds.

Sample Size and Composition:

The required sample size for a single proportion test with a significance level (Alpha) of 0.05 and a power of 0.8 (recommended in [145]) is estimated to be 47 [146]. This means that, in order to detect a meaningful effect size with the specified level of significance and power, we would need a sample size of 47. In the quantitative part of the study, we collected responses from a total of 101 participants. After applying our exclusion criteria, a final sample of n = 58 participants was considered for analysis, resulting in a power of 0.8821 at a significance level of 0.05, which exceeds the recommended power in best practices. Participants who had no knowledge of cryptocurrencies were excluded from the study, ensuring that the sample consisted of individuals with relevant experience and understanding of the topic. The qualitative part of the study involved twelve participants, all of whom were cryptocurrency users.

Questionnaire Design and Control: The questionnaire was designed to be comprehensive and coherent, following established guidelines for survey design. It was distributed in English, and participants were given the option to provide unassisted answers by adding an "other" option. To maintain the integrity of the data, we implemented measures to prevent resubmission, allowing only one submission per device and IP address. Participants were also unable to change their responses to previous questions, ensuring consistency throughout the questionnaire.

Exclusion Criteria: To ensure data reliability, we followed the exclusion criteria proposed by [147]. This involved removing participants who demonstrated a lack of knowledge about cryptocurrencies, provided incomplete responses, selected incorrect options in quality control questions, chose invalid answers, or failed to re-phrase earlier questions correctly. By applying these criteria, we maintained the quality and integrity of the data for analysis.

By adhering to these ethical considerations and implementing measures to ensure validity and reliability, we strive to conduct rigorous and trustworthy research that contributes to the field of user-perceived privacy in the blockchain.

5.3 Results

In this section, we delve into the outcomes of our qualitative and quantitative study, encompassing privacy awareness, privacy preferences, and privacy wallets.

5.3.1 Privacy Awareness

The Importance of Privacy in Transactions

One of the key aspects we examined was the participants' perception of the importance of privacy in cryptocurrency 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 of 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, 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]*".

These results highlight the diverse perspectives on the importance of privacy in cryptocurrency transactions, ranging from a strong emphasis on privacy and anonymity to varying levels of importance and even disinterest. It also underscores the influence of factors such as blockchain transparency, government surveillance, and the context of transaction information access.

QNT.[1] Participants were asked to rate the importance of anonymity in such transactions on a scale ranging from "Not at all important" to "Extremely important." Participants were asked to rate the importance of anonymity in such transactions on a scale ranging from "Not at all important" to "Extremely important."

The results indicate that the majority of participants highly value the anonymity of cryptocurrency transactions. Specifically, 46.55% of participants rated the importance of privacy as "Extremely important," emphasizing the significance they attribute to the privacy aspect. Additionally, 24.14% of participants considered it "Very important." These findings underscore the prevailing sentiment among participants that privacy is a critical factor in their cryptocurrency transactions.

In contrast, a minority of participants expressed relatively lower importance placed on privacy. About 22.41% rated it as "Somewhat important," suggesting a moderate level of concern for privacy. A smaller percentage, 5.17%, considered privacy "Not so important." Finally, only 1.72% of participants rated privacy as "Not at all important," indicating a minority view that places minimal importance on privacy in cryptocurrency transactions.

These results highlight the varying degrees of importance that participants attach to privacy in their transactions. The majority of participants prioritize privacy and perceive it as an essential feature in cryptocurrency transactions, while a smaller proportion holds a less significant view on privacy concerns.

Bitcoin Anonymity

Participants were asked to rate Bitcoin's 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 to traditional banking systems.*" PU3 notified

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

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 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 as 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.*"

These results highlight concerns about transaction transparency, monitoring tools, privacy issues with wallets, and the tracing possibilities associated with Bitcoin transactions. It also reveals participants' varying levels of knowledge and awareness regarding the intricacies of Bitcoin's anonymity.

QNT. Participants were asked to rate Bitcoin's anonymity on a scale ranging from "Not

at all anonymous" to "Extremely anonymous."

The results reveal a diverse range of perceptions regarding the level of anonymity provided by Bitcoin. Among the participants, 15.52% rated Bitcoin as "Not at all anonymous," indicating a clear understanding that Bitcoin transactions do not provide any significant anonymity. Another 27.59% of participants considered Bitcoin as "Not so anonymous," suggesting a perception that Bitcoin offers limited anonymity.

In contrast, a significant proportion of participants recognized some level of anonymity in Bitcoin transactions. Specifically, 36.21% of participants rated Bitcoin as "Somewhat anonymous," reflecting a belief that Bitcoin provides a moderate degree of anonymity. Additionally, 18.97% of participants perceived Bitcoin as "Very anonymous," indicating a stronger belief in the anonymity provided by the cryptocurrency.

Interestingly, a small percentage of participants, 1.72%, rated Bitcoin as "Extremely anonymous," signaling a misconception or overestimation of Bitcoin's anonymity.

Of particular note is a user who selected Bitcoin as "Extremely anonymous" and was directed to the privacy-unaware user questions. This participant stated that their belief in Bitcoin's extreme anonymity is rooted in the absence of real identities in the transactions, including names or personally identifiable information (PII).

These findings highlight the varied perspectives on Bitcoin's anonymity among participants. While a significant number recognize the limited anonymity offered by Bitcoin, a considerable portion still perceive it as at least somewhat anonymous. The presence of participants who believe Bitcoin is extremely anonymous indicates a potential misconception that requires further investigation.

Privacy Risks

Participants were asked to identify and describe privacy risks associated with Bitcoin transactions. Their responses provided insights into their level of awareness and understanding of potential 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 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.*"

The result demonstrates varying levels of awareness and understanding among participants regarding privacy risks associated with Bitcoin transactions. Participants highlighted risks related to monitoring tools, exchanges, address reuse, web wallets, and tracing transactions. However, some participants exhibited limited knowledge or were unaware of these risks.

QNT. Among the participants, a majority (68.96%) demonstrated awareness of privacy risks in Bitcoin transactions.

Upon analyzing the participants' responses, it was observed that some participants misunderstood the concept of privacy risks and mentioned issues related to security or financial risks, such as "losing money" and "password hack," which are not directly related to privacy. However, the majority of participants provided responses that align with privacy concerns.

The most commonly reported privacy risks identified by participants were:

- **Centralized exchanges (KYC)**: Participants expressed concerns about privacy risks associated with centralized cryptocurrency exchanges that require Know Your Customer (KYC) procedures. These procedures often involve identity verification, which can compromise the anonymity of users.
- **Identity identification**: Participants mentioned the risk of identity identification through various means, such as linking wallet addresses to real-world identities or using additional information to reveal a user's identity.
- **Creating transaction graphs**: Participants recognized the potential privacy risks associated with the creation of transaction graphs, where the flow of funds can be traced and analyzed to reveal the relationships between different addresses and transactions.
- **Public and immutable database**: Participants acknowledged that the public and immutable nature of the blockchain poses privacy risks, as transaction details are permanently recorded and accessible to anyone.

These responses indicate a good level of awareness among participants regarding the privacy risks associated with Bitcoin transactions. However, it is worth noting that some participants may have focused more on the broader implications of privacy, such as identity protection, rather than specific technical risks within the blockchain protocol itself.

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), and decentralized exchanges. PU3 also proposed to not directly transfer from personal wallets to other addresses, using mixing, using TOR or VPN, and 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.

The analysis demonstrates the diverse range of strategies and measures proposed by participants to mitigate privacy risks associated with Bitcoin transactions. These measures include using different platforms and wallets, leveraging DeFi and decentralized exchanges, avoiding direct wallet-to-wallet transfers, utilizing mixing and privacy coins, employing TOR or VPN, being mindful of monitoring system improvements, and selecting exchanges and wallets with minimal identity requirements. However, some participants exhibited limited awareness of certain options, indicating the importance of education and awareness regarding privacy-enhancing measures in the cryptocurrency space.

Awareness of De-anonymization Techniques

We examined participants' awareness of de-anonymization techniques in the context of blockchain transactions. De-anonymization techniques refer to methods or strategies that can be used to reveal the identities or link transactions to specific individuals or entities. 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.

The result indicates a range of awareness levels among the participants regarding de-anonymization techniques. Some participants demonstrated a general understanding of monitoring tool functionalities, address reuse vulnerabilities, transaction patterns, or transaction graphs. However, many participants showed limited awareness or did not mention any specific de-anonymization techniques. This highlights the need for further education and awareness regarding the potential risks and techniques associated with de-anonymizing blockchain transactions.

QNT. Among the participants, the majority (73.68%) reported being aware of the de-anonymization technique known as address reuse. Address reuse occurs when the same Bitcoin address is used for multiple transactions, making it easier to link those transactions together and potentially identify the involved parties.

More than half of the participants (64.91%) indicated that they are aware of the practice of tagging addresses through the information available on the Internet. This technique involves associating additional information, such as online profiles or publicly available data, with specific addresses to potentially reveal the identity of the address owner.

Transaction graphs were recognized as a de-anonymization technique by 57.89% of the participants. Transaction graphs involve analyzing the flow of funds and tracing the relationships between different addresses and transactions to identify patterns and potentially link them to specific individuals.

Similarly, change address detection was acknowledged by 54.39% of the participants. Change address detection refers to the identification of change addresses used in transactions, which can be leveraged to link different transactions and potentially de-anonymize the parties involved.

It is worth noting that a small portion of the participants (10%) reported being unaware of any de-anonymization techniques. This highlights the need for further education and awareness-raising efforts to ensure users have a comprehensive understanding of the potential privacy risks associated with blockchain transactions.

Awareness of Correlation Attacks

We examined participants' awareness of correlation attacks in the context of blockchain transactions. Correlation attacks refer to techniques that exploit various correlations, such as network patterns, transaction timing, and transaction amounts, to potentially de-anonymize users or link transactions together. 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.

The results indicate the majority of participants were unaware of correlation attacks, indicating a need for increased education and awareness regarding the potential risks associated with correlation attacks in blockchain transactions.

QNT. Among the participants, a significant majority (60%) reported being aware of network, time, and amount correlation attacks. On the other hand, a small portion of the participants (15.79%) reported being unaware of any correlation attacks.

Awareness of Add-on Techniques

We explored participants' awareness of add-on techniques that can be utilized to enhance privacy in blockchain transactions. Add-on techniques refer to external tools, services, or protocols that users can employ alongside the blockchain to augment the privacy of their transactions. 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.

The result indicates that while a few participants showed some awareness of mixers and CoinJoin, the majority of participants were unaware of add-on techniques for enhancing privacy in blockchain transactions.

QNT. Among the participants, a majority (66.67%) reported being aware of mixing websites. Participants also displayed awareness of other add-on techniques. Specifically,

49.12% reported being aware of CoinJoin-based techniques. Additionally, 43.86% of participants indicated awareness of threshold signatures. Other add-on techniques mentioned by participants included off-chain solutions (42.11%), and Fairexchange / Coinswap (31.58%). However, a notable portion of participants (17.54%) reported being unaware of any of the mentioned add-on techniques. Figure 5.5 provides a visual representation of participants' awareness of add-on techniques.

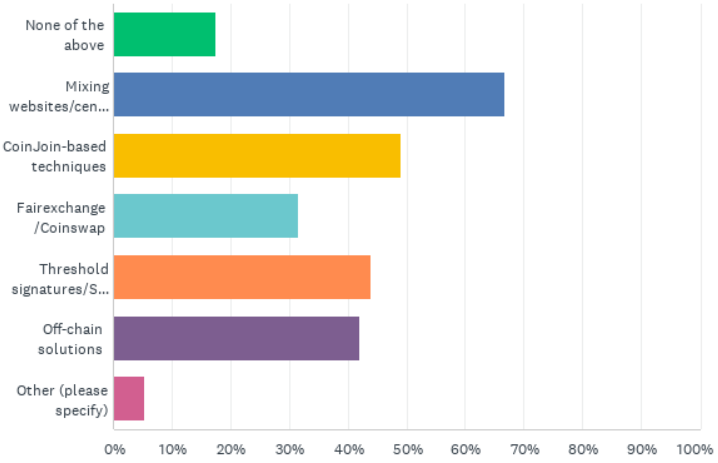


Figure 5.5: Awareness of Add-on Techniques

Awareness and Usage of Privacy Coins

Participants were asked to indicate their awareness of various 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 ones 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 Zcash or Monero, but they were unaware they are privacy coins. PU4, PU6, and PU12 were unaware of privacy coins.

The result suggests that while a few participants showed awareness of Monero and Zcash as privacy coins, the majority had limited knowledge or were completely unaware of privacy coins and their purpose.

QNT.The two most prominent privacy coins in terms of awareness were **Monero** and **Zcash**. A significant majority of participants (78.95%) reported being aware of Monero, while 70.18% indicated awareness of Zcash. These findings indicate a substantial level of recognition among participants regarding privacy coins and their purpose in providing enhanced privacy features in transactions.

Figure 5.6 provides a visual representation of participants' awareness of privacy coins.

Among the privacy coins that participants were aware of, Monero and Zcash emerged as the top coins that participants had owned, bought, or mined. This suggests that participants not only recognize the importance of privacy in their transactions but also actively engage with privacy coins as a means to achieve better anonymity and as an investment opportunity.

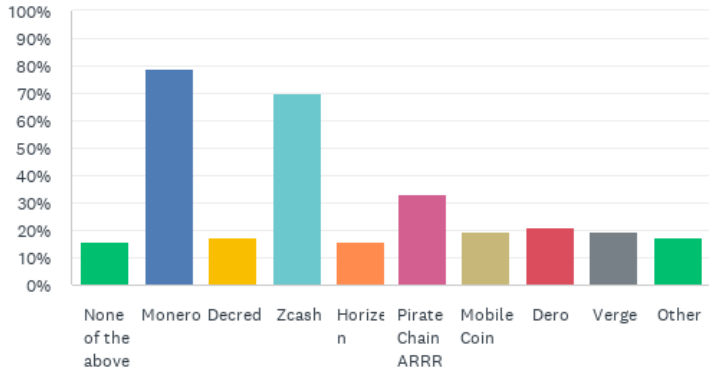


Figure 5.6: Privacy coins awareness

5.3.2 Privacy Preferences

Preference Between Bitcoin Add-on Techniques and Privacy Coins

Participants were asked to indicate their preference between using Bitcoin add-on techniques (such as CoinJoin-based solutions, threshold signatures, off-chain solutions, etc.) or privacy coins (such as Monero, Zcash, etc.) for enhancing the privacy of their transactions. This inquiry allows us to understand participants' inclinations towards either integrating privacy-focused features into the existing Bitcoin network or utilizing dedicated privacy coins as a means to achieve enhanced anonymity.

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 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-ons 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.

The result reveals a variety of preferences among participants. While many participants favored privacy coins for their built-in privacy provisions and trust in the developers' focus on privacy, others either preferred Bitcoin add-on techniques or expressed neutral stances. Alternative approaches, such as DeFi platforms or prioritizing security, were also mentioned.

QNT. The results revealed that a majority of the participants (63.16%) preferred using privacy coins over Bitcoin add-on techniques. This preference suggests that participants view privacy coins as a more effective and convenient solution for safeguarding their transactional privacy compared to utilizing additional techniques within the Bitcoin network.

- *Reasons for Preferring Privacy Coins:* Among participants who favored privacy coins, two primary reasons emerged as significant factors influencing their preference.

The first reason was **mandatory built-in privacy**, which was cited by 91.67% of participants. This indicates that participants value privacy coins' inherent privacy features, which are integrated into the design of these cryptocurrencies from the outset. The second reason was the desire for **stronger anonymity**, as reported by 83.33% of participants.

- *Reasons for Preferring Bitcoin Add-on Techniques:* Among the participants who expressed a preference for Bitcoin add-on techniques, several reasons were cited. The most commonly selected options included Bitcoin's reputation (85.71%), availability of Bitcoin tools (such as wallets and explorers) (71.43%), and Bitcoin market cap (71.43%). These findings suggest that participants who favor Bitcoin add-on techniques value the established reputation of Bitcoin, the convenience and familiarity of existing tools and infrastructure, and the overall market capitalization of Bitcoin.

Preferences Between Bitcoin Built-in and Add-on Privacy Techniques

Participants were asked to indicate their preference regarding the application of privacy techniques in Bitcoin. Specifically, they were asked to express their preference for either *mandatory built-in privacy techniques* integrated into the Bitcoin network or *add-on privacy techniques* that can be implemented externally to enhance transaction privacy.

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 knowledgeable 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 Hypertext Transfer Protocol Secure (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.

While some participants advocate for mandatory built-in techniques, others have concerns about potential consequences. These findings provide insights into participants'

considerations, including risks, impact, public benefit, and the need for monitoring, when expressing their preferences between Bitcoin built-in and add-on privacy techniques.

QNT. The results showed that approximately half of the participants (50%) preferred the adoption of *mandatory built-in privacy techniques* in Bitcoin. This finding suggests that a significant portion of participants believes that privacy should be an inherent feature of the Bitcoin network, with privacy measures incorporated directly into its design. These participants recognize the importance of privacy as an essential aspect of cryptocurrency transactions and advocate for privacy to be a fundamental component of the Bitcoin protocol itself.

A considerable proportion of participants (29.82%) responded that they did not know which option they preferred. This indicates a lack of clarity or uncertainty among these participants regarding the advantages and disadvantages of each approach. It highlights the need for further education and information dissemination to help users make informed decisions about privacy preferences in the context of Bitcoin.

A smaller percentage of participants (12.28%) expressed a preference for *add-on privacy techniques*. These participants believe that external solutions, separate from the core Bitcoin protocol, can be effective in enhancing transaction privacy. Their preference for add-on techniques may stem from factors such as compatibility with existing infrastructure, familiarity with specific privacy solutions, or concerns about potential disruptions that could arise from modifying the core Bitcoin network.

A small fraction of participants (8.77%) held *other opinions* that differed from the primary options presented. These participants expressed reservations about implementing built-in privacy techniques in Bitcoin, citing concerns such as the potential negative impact on the Bitcoin ecosystem and the possibility of a "complete crash" or bankruptcy for certain stakeholders. These opinions highlight the complex considerations and trade-offs involved in implementing privacy features in Bitcoin and underscore the need for careful analysis and evaluation of potential implications.

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 preventing 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.

The result reveals that interviewees prioritize features that conceal the source, amount, and destination in Bitcoin transactions to enhance privacy. They also expressed a desire to prevent address mapping, transaction tracing, and the creation of transaction graphs. Some participants highlighted the importance of protecting personal data associated with wallets.

QNT. The results revealed that participants had strong preferences for certain privacy features. The most commonly selected privacy feature was *hiding the source of the transaction*, with 70.18% of participants choosing this option. This indicates that participants highly value the ability to obfuscate the origin or sender of a transaction.

Similarly, *hiding the amount* of the transaction was also chosen by 70.18% of participants.

Another privacy feature that received significant attention was *hiding the destination* of the transaction, with 63.16% of participants selecting this option.

Accepting Extra Fees

Participants were asked whether they were willing to pay extra fees for better privacy in their Bitcoin transactions. 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 they pay for the technique they are confident about the provided level of privacy. 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.*"

The result demonstrates varying attitudes towards paying extra fees for privacy in Bitcoin transactions. While some participants recognized the importance of privacy and were willing to incur additional costs, others deemed the existing level of privacy sufficient or saw paying for privacy as unnecessary for their circumstances. These findings shed light on the complex considerations individuals have when balancing privacy concerns with the costs associated with Bitcoin transactions.

QNT. The results showed that almost half of the participants (53.45%) were willing to accept additional fees in exchange for improved privacy. On the other hand, a notable proportion of participants (32.76%) expressed their unwillingness to pay extra fees for privacy-enhancing measures. Their reasons varied and included concerns about the current high transaction fees in Bitcoin, the perception that the current level of privacy provided by Bitcoin meets their expectations, and the low volume of their investments in the cryptocurrency market. Some participants also mentioned that privacy should be a default feature in the system and should not require additional fees to access. They argued that charging extra fees for privacy would create a paywall that could potentially exclude certain users from enjoying privacy protection. Additionally, a few participants expressed their preference for alternative cryptocurrencies or systems that inherently provide better privacy without the need for additional fees.

Among those participants who were willing to pay extra fees, the average amount they were willing to pay for a transaction worth $1000 was $18.13. The maximum fee reported was $200, while the minimum was $0.1, and the median fee was $10. These figures indicate the range of values participants are willing to pay to secure their privacy when conducting higher-value transactions.

Accepting Extra Delays

Participants were asked about their willingness to accept additional delays in their Bitcoin transactions for the sake of improved privacy. All of the interviewees except PU6 accepted waiting longer for better privacy. We 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 Bitcoin price 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 it 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.*"

The result reveals most participants recognized the importance of privacy and were willing to wait longer.

QNT. The responses varied among participants, with different thresholds for acceptable delays. The distribution of responses showed that 22.41% of participants were willing to accept delays of less than a minute, 29.31% were willing to tolerate delays of less than an hour, 15.52% were willing to wait for less than a day, 5.17% were willing to wait for less than a week, and 5.17% were willing to wait for less than a month.

A significant majority of participants (77.58%) expressed their willingness to accept extra delays in their Bitcoin transactions. This suggests that a majority of participants prioritize privacy protection over transaction speed, and they are willing to trade off faster transaction times for enhanced privacy and anonymity.

Conversely, a smaller portion of participants (13.79%) stated that they were not willing to accept extra delays in their Bitcoin transactions. Their reasons for rejecting delays varied. Some participants cited the existing delays in Bitcoin confirmation as a factor that made them hesitant to accept further delays. They expressed concerns about the potential impact on transaction efficiency and usability. Others mentioned that they preferred not to use Bitcoin as a privacy option altogether, suggesting a preference for alternative cryptocurrencies or privacy-enhancing solutions that offer faster transaction times without compromising privacy.

5.3.3 Privacy Wallets

Awareness and Usage of Privacy Wallets

Participants were asked about their awareness and usage of privacy wallets in the Bitcoin ecosystem. 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.*"

The result reveals a general lack of awareness and usage of privacy wallets among the participants. While PU3 showed some knowledge of specific privacy wallets and expressed concerns about being flagged by monitoring tools, others had limited understanding or misconceptions about the purpose and functionality of privacy wallets.

QNT. The findings revealed that Wasabi and Samourai were the most well-known and widely used privacy wallets among the participants. These wallets have gained prominence due to their robust privacy features and user-friendly interfaces, which cater to the needs of privacy-conscious Bitcoin users.

Figure 5.7 provides a visual representation of the participants' awareness of different privacy wallets. It illustrates that a significant portion (43.86%) of the participants were unaware of the existence of privacy wallets. This highlights the need for further education and awareness campaigns to ensure that users are well-informed about the privacy-enhancing options available to them.

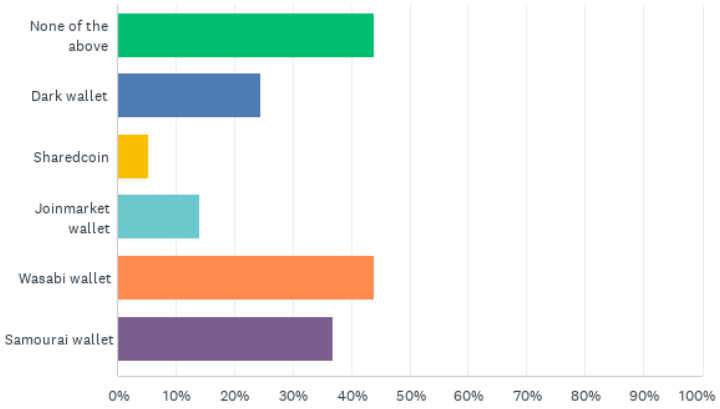


Figure 5.7: Privacy wallets awareness

Most wallets have not been widely used by the participants, indicating a relatively low adoption rate. Among the participants who reported using privacy wallets, Wasabi was the most popular with a usage rate of 28.13%, followed by Samourai with 12.50%. Additionally, 9.38% of participants reported using the JoinMarket wallet. The level of satisfaction with these privacy wallets is summarized in Table 5.2. Participants were asked to rate their satisfaction on a Likert scale ranging from "extremely satisfied" to "not at all satisfied".

Table 5.2 reveals that the majority of users expressed a high level of satisfaction with the privacy wallets they utilized. Six out of nine users of Wasabi reported being "very satisfied" with the wallet. Similarly, three out of four users of Samourai expressed a high level of satisfaction. One out of three users of JoinMarket reported being "very satisfied" with the wallet.

In addition to the users who were highly satisfied, there were participants who reported being "somewhat satisfied" with the privacy wallets. Two out of nine Wasabi users and two out of three JoinMarket users fell into this category.

However, it is worth noting that a small proportion of users reported lower levels of satisfaction with Wasabi and Samourai. One out of nine Wasabi users and one out of four Samourai users indicated being "not at all satisfied" with their respective wallets.

The result demonstrates a generally positive user experience with privacy wallets, particularly with Wasabi and Samourai, as a majority of users expressed high satisfaction levels. This suggests that these wallets have successfully met the expectations of users in terms of privacy features and functionality.

Table 5.2: 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

Trusting Third-party Wallets

The participants' level of trust in third-party wallets was assessed in this study, with a focus on the factors influencing their trust. Except for PU8, who did not trust the wallets, other interviewees argued about which wallets they could trust. PU12 had no answer to the question as they were not familiar with the subject of privacy in the blockchain.

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 reliable experts with a good experience and background in this context.*" PU5 and PU10 pointed to the wallet's reputation and the number of users; however, PU10 did not prefer to use third-party wallets. PU4 added recommendations from trusted websites. PU6 and PU7 also referred to users' reviews about the wallet. PU7 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.*"

The result reveals that participants' trust in third-party wallets is influenced by factors such as open-source code, approval by reliable individuals, reputation, user base, recommendations, user reviews, and the ability to research and verify a wallet's features.

QNT. Among the participants, 55.17% expressed trust in a privacy wallet if it is open-source and allows for code verification. This finding suggests that participants value

transparency and the ability to independently verify the security measures implemented in the wallet. By making the source code accessible, users can assess the quality of the code, identify any potential vulnerabilities, and gain confidence in the privacy wallet's functionality.

On the other hand, 22.41% of participants reported that they do not trust third-party services in general. This perspective highlights a level of skepticism and concerns regarding the reliability and security of third-party wallets. Users may be apprehensive about placing their trust in external entities, preferring to rely on their own means to ensure the privacy and security of their transactions.

Another aspect influencing trust is the information available in forums or provided by friends, which was selected by 8.62% of participants. This finding suggests that individuals place importance on personal recommendations and experiences shared by trusted sources. Seeking guidance and opinions from knowledgeable individuals or communities can play a significant role in building trust in third-party wallets.

Interestingly, a small percentage of participants (3.45%) did not provide a specific answer to the question about trust in third-party wallets. This response could indicate a lack of clarity or uncertainty regarding their level of trust or the factors influencing their trust.

One participant who selected "other" mentioned the importance of a wallet "surviving over a long period." This response implies that users may associate trust with the longevity and reliability of a wallet. The participant's statement suggests that wallets that have stood the test of time and demonstrated their reliability are more likely to be trusted.

5.4 Coding and Theory

As aforementioned in subsection 5.2, we encoded the data according to Grounded Theory [143], a methodical and iterative approach for analyzing and coding qualitative data. This process entails breaking down the data into meaningful components and assigning descriptive labels or codes to each part. These codes encapsulate the core of the data, aiding in the recognition of patterns, themes, and connections. In this section, we will provide the details of initial and advanced coding to build our theory.

5.4.1 Initial Coding

We followed [144, 53] and used open, axial, and selective coding to code the statements in the qualitative study. In evolved Grounded Theory, coding terminology encompasses open coding, axial coding, and selective coding, finally generating a coherent set of theoretical propositions [144]. We utilized affinity mapping as a means of organizing the interviews. This involved segmenting the interview transcripts into smaller sections and employing sticky notes to mark emerging categories that recurred or related to each other. After each iteration of individual coding, collaborative discussions by two IT security researchers were undertaken to delve into the interrelationships among the

recently identified categories. Through these discussions, a consensus was reached by the two researchers regarding a comprehensive set of higher-level categories, which were then subjected to axial coding. In the process of selective coding, we collectively determined a definitive set of core categories that revolved around the identified misconceptions or perceptions. These misconceptions and perceptions were subsequently organized into three overarching categories, namely privacy misconceptions, privacy risks, and privacy measures. Each of these top-level categories further encompassed multiple subcategories, offering a more detailed and comprehensive understanding of the data.

The final codebook can be found in Table 5.3. The top-level categories are represented by the orange color for privacy misconceptions, privacy risks, and privacy measures. The sub-categories for each final codebook are depicted in purple.

5.4.2 Advance coding

In the advanced coding stage, when ideas become categories, they become more abstract. This means they summarize stories from different sources in a simple way. Instead of showing themes, we present the results as a connected group of ideas [144]. The storyline is the main idea of the core category. This process creates a story that links the categories together and forms a group of theoretical ideas. Once the storyline is established, the Grounded Theory is finalized using theoretical codes that help explain the storyline more effectively, transforming it into a theory [144]. To develop our theory, we constructed the story around three key categories: privacy misconceptions, privacy risks, and privacy measures. We investigated the misconceptions or the impact of unawareness and incorrect assumptions among our participants.

5.4.3 Privacy misconceptions

Our study explored participants' perceptions of Bitcoin's anonymity. Interestingly, when asked to rate Bitcoin's anonymity, four out of twelve participants believed it to be high or very high. However, this assumption doesn't hold true in light of research findings indicating numerous de-anonymization attacks on the Bitcoin blockchain [10]. This indicates an overestimation of Bitcoin anonymity. Among those who perceived Bitcoin's anonymity as very high, one participant (PU6) pointed out that users don't know to whom the public key belongs, emphasizing the alphanumeric nature of the key and the hidden identities within the network. They expressed confidence that users performing Bitcoin transactions couldn't be identified, citing the story of the Silk Road developer as evidence. They believed that law enforcement agencies had to employ sophisticated methods to track down the developer, attributing the difficulty to the use of TOR and Bitcoin payments in the system's design. However, this perception reflects a misconception, as the user seemed unaware of the de-anonymization techniques employed in Bitcoin to link addresses to real identities.

Two participants held the misconception that Bitcoin provides complete anonymity because it uses addresses instead of real identities. This belief overlooks the fact that

Table 5.3: Final codebook

Privacy misconceptions	Tags	Privacy risk mitigation
Technical	flagged wallets	Non-KYC
Bitcoin high anonymity	criminal wallets	non KYC exchanges
addresses rather than identity	distinguishable techniques	non KYC wallets
encryption algorithms	Government regulations	Multi platform/wallet
privacy in bitcoin network	government trace	using different wallets
security priority	cryptocurrency law	using different platforms
Application	cryptocurrency ban	DeFi platforms
no industry usage	cryptocurrency taxing	defi/lending platform
no real-world usage	capital outflow	decentralized exchange
money laundering	de anonymization	Anonymity networks
tax evasion	address reuse	VPN
special activities	patterns	TOR
special people/organization	transaction graphs	one time IP
Privacy risks	no implmentation of privacy attacks	being full node
centralized	Correlation attacks	prepaid sim card
centralized exchange	network correlation: user/wallet ip	Fresh address generation
KYC	node behavior	fresh address
authentication	checking explorers	Privacy-preserving techniques
web / custodial wallet	amount correlation: high volume	Privacy coin
only wallets and exchanges	time correlation: specific time	Mixing
Communication tools	Auxiliary Information	Privacy techniques
email	exchange: users information	
sim card	exchange: trade information	
mobile device	companies accepting bitcoin	
Transaction parties	online shops	
coin source	gambling websites	
recipient	Private key management	
others' assets	custodial wallet control	
Tracking and analysis	leaked private key	
analysis tools	Illicit activities	
government\police tracking	exchange hack	
de anonymization algorithms	losing money by hack	
block explorers	information stealing	
	theft	

Bitcoin transactions are recorded on a public ledger, making them potentially traceable, and they are possible to be linked to the identities once it is used in the services requiring KYC. Additionally, one participant had a misunderstanding about privacy in Bitcoin transactions. They believed that Bitcoin's anonymity stemmed from encryption algorithms and the absence of identity records in the blockchain. They argued that since transactions can be made from wallets not associated with any identity, both the sender and recipient remain anonymous. However, this overlooks the fact that while Bitcoin addresses are pseudonymous, they can still be linked to real-world identities through various methods, undermining the anonymity of transactions.

Our research uncovered a common misconception among some participants who believed that Bitcoin offers anonymity within the network but not outside of it. However, this belief is inaccurate. While Bitcoin transactions may appear anonymous on the surface, they are still traceable and can be linked to real-world identities through various means. This misunderstanding could potentially lead to users neglecting to employ privacy-enhancing methods while using Bitcoin, assuming their transactions are inherently secure.

We also observed some users have security priority rather than privacy and consider privacy as not an important aspect. In our study, we encountered participants who explicitly stated that privacy holds little importance to them. For instance, PU8 remarked, "*privacy is not important at all to me as nothing happens if this information is disclosed. However, I prefer it not to be [disclosed].*" This sentiment aligns with findings from a previous study [53].

Additionally, we observed a level of uncertainty among certain participants regarding Bitcoin's anonymity. For instance, PU10 expressed uncertainty, stating, "I've just heard Bitcoin anonymity is less than other cryptocurrencies, I'm not sure." This uncertainty underscores the need for clearer communication and education about the realities of Bitcoin's privacy features, as well as the importance of implementing additional privacy measures to safeguard user information and transactions.

In our study, we encountered participants who held negative views about privacy in cryptocurrency transactions. One participant (P2) believed that privacy coins have no industry or real-world usage. Another participant (PU12) expressed the belief that privacy matters only to those involved in illicit activities like money laundering, stating, "I do not perform anything special or illegal; privacy does not matter to me." This mindset is concerning, especially considering the regulatory actions taken by governments to restrict privacy-preserving techniques in cryptocurrencies, as noted in a report by the U.S. Treasury ([148]. Such attitudes can hinder efforts to enhance user privacy and develop effective privacy-protection techniques.

5.4.4 Privacy risks

In our study, participants were asked to pinpoint and discuss the privacy risks associated with Bitcoin transactions. Several interviewees (PU2, PU4, PU5, PU7, and PU8) brought up concerns about anonymity when using exchanges or services that accept Bitcoin. However, it's important to note that privacy issues with exchanges mainly arise when users utilize centralized exchanges with Know Your Customer (KYC) requirements. Among the participants, only PU5 highlighted the privacy issues associated with centralized exchanges that implement KYC protocols. Despite acknowledging these concerns, they still believed that "*Bitcoin is still more anonymous than traditional banking.*" However, it's worth considering that while Bitcoin transactions may offer some degree of anonymity, traditional banking systems generally provide more privacy from the public's perspective, given the traceability of Bitcoin transactions.

One of the participants (PU8) also brought up privacy concerns related to wallets, mentioning that the information about your e-mail, your mobile phone, and your phone number are recognized. Their comments were specifically based on their experiences with mobile or web wallets. However, it is important to note that software wallets installed on desktop computers typically do not require email information or connection to mobile SIM cards. Additionally, this interviewee seemed unaware that full-node wallets, which operate independently of third-party services, do not encounter these privacy issues. The interviewee assumed that privacy risks are only associated with wallets and exchanges, stating that "*as long as you are not trading and the wallet you are using are not related to you, privacy is OK.* However, this assumption could jeopardize the interviewee's privacy when spending their coins on services that can trace their IP addresses [70] or when de-anonymization heuristics are applied to their transactions [2].

Some participants emphasized a significant privacy risk: the possibility that their transaction partners might recognize them. This situation opens the door to the potential exposure of sensitive financial or personal information. Indeed, transacting with someone who knows them personally poses a real privacy risk. In such cases, peers could potentially connect their transaction history to their identity, thereby compromising their financial privacy.

Only a few participants demonstrated awareness of the privacy risks posed by monitoring tools. PU1 explained, "*they [monitoring tools] find suspicious transactions, like those from gambling websites or potential money laundering activities. They trace suspicious UTXOs to identify the user or exchange involved.*" Similarly, PU2 highlighted how monitoring tools detect mixers or ransom transactions by tracking various wallets, potentially uncovering criminal groups. Moreover, one of the participants elaborated on the collaboration between monitoring tools and explorers, noting how transactions can be tagged with users' IP addresses and how address reuse can link transactions. Interestingly, two participants even mentioned specific monitoring tools such as Crystal and CipherTrace. PU3 went as far as suggesting alternatives such as Monero or Zcash for anonymous transactions, recognizing that Bitcoin's privacy is compromised by monitoring tools. However, these participants lacked insight into the specific algorithms and techniques used by monitoring tools to flag and track transactions.

Although some participants did not explicitly mention monitoring tools, they demonstrated an understanding of the algorithms utilized to track relationships between accounts and trace transactions. For instance, PU9 explained, *"it is possible to trace a specific transaction and recognize how it was funded, for instance, in which exchange."* However, despite this awareness, they could not specify well-known de-anonymization techniques in Bitcoin. This lack of awareness among users can be concerning because it may lead them to spend their Bitcoin without considering necessary measures to enhance their privacy. This emphasizes the importance of educating users about the potential privacy risks associated with Bitcoin transactions and the measures they can take to mitigate them.

One of the participants demonstrated an understanding of tracing methods through

their observation of news stories involving Bitcoin-related criminal investigations. This indicates that the participant recognized instances where law enforcement agencies successfully traced criminals who used Bitcoin. This suggests that news consumption played a role in shaping the participant's perception of Bitcoin's traceability and the effectiveness of law enforcement efforts in identifying Bitcoin users involved in illegal activities.

Two participants in our study recognized Bitcoin explorers as a potential privacy risk. This designation reflects an understanding that these tools can readily provide transaction information to ordinary users, potentially exposing sensitive data. Given that tracing transactions often requires technical expertise and resources, this privacy risk is important, particularly when users are aware of each other's involvement in a transaction. Explorers can easily furnish information to users, facilitating the tracking of transactions and compromising privacy. However, tracking of transactions by cryptocurrency explorers is not the only privacy risk. Cryptocurrency explorers service providers can also map users' IP addresses to transactions under examination. While this risk was only highlighted by one interviewee, others may be unaware of it, potentially compromising their privacy when utilizing blockchain explorers.

One participant (PU5) expressed concern about potential future laws regarding cryptocurrencies. They explained, "*at the moment my investment is too low, that's why privacy is not important for me...I'm afraid of future laws on taxing crypto transactions or if the government bans crypto transactions.* " This viewpoint suggests that the significance of privacy for users might vary depending on the amount of cryptocurrency they own. However, if governments introduce taxation or ban cryptocurrencies altogether, users may feel compelled to resort to privacy-preserving techniques to safeguard their assets. While this may seem like a proactive measure, it could potentially lead to the misuse of transactions outside the boundaries of the law. This indicates the complex interplay between privacy concerns, government regulations, and individual behavior in the realm of cryptocurrency transactions.

When asked about potential techniques that could compromise users' privacy, two participants accurately identified tracing and linking transactions, particularly when addresses are reused. However, it's concerning that only two out of twelve participants recognized this as the most significant privacy issue in Bitcoin. This lack of awareness is also evident in cases where users repeatedly use the same Bitcoin address for their transactions, as highlighted in previous research [74]. Transaction graphs mentioned by one participant further indicate a lack of awareness among other participants. This suggests that many users may not realize that their Unspent Transaction Outputs (UTXOs) can be linked to other transactions, allowing analyzers to track both previous and subsequent transactions.

Another participant wrongly assumed that privacy attacks have not yet been implemented. PU8 stated, "*Privacy attacks are only implemented in academic papers; I haven't seen any implementation in practice.*" However, this participant was unaware of current monitoring tools and companies actively working in this context as part of their business

operations. This highlights the need for greater awareness among users regarding the practical implementation of privacy attacks and the existence of monitoring tools in the cryptocurrency ecosystem.

In our investigation of awareness regarding correlation attacks, we uncovered some interesting findings. Surprisingly, most participants were unaware of these types of attacks, except for three individuals who stood out. PU3 demonstrated awareness by mentioning IP address mapping to addresses and identifying access patterns as network correlations. PU4 highlighted time and amount correlations, particularly through services where users pay with Bitcoin. Additionally, PU8 brought attention to issues with patterns derived from transactions involving the same amounts. This lack of awareness among the majority of participants is concerning because it leaves users vulnerable to having their transactions correlated, as demonstrated in previous studies [69, 74]. It underscores the importance of educating users about the potential risks associated with correlation attacks and the measures they can take to protect their privacy in blockchain transactions.

In the context of auxiliary information, One participant pointed out that exchanges can possess a wealth of transaction history and track user behavior, stating, "*my identity can be identified, [and] along with tracking systems they can identify my behaviors.*" This is a true privacy risk that highlights the potential for exchanges and tracking systems to obtain insights from user behavior and potentially identify individuals. However, user identity is typically revealed only when transactions are conducted through Know Your Customer (KYC) services.

Several participants in our study identified security risks as potential privacy concerns. For example, PU5 raised a red flag about the security practices of web wallets, noting that platforms such as Blockchain.com hold users' private keys. This poses a privacy risk, as a compromised web wallet could potentially spend users' funds without their consent, implicating them in transactions they did not initiate.

Additionally, two participants highlighted exchange hacks as another security issue that could compromise users' privacy. If hackers gain unauthorized access to exchanges, they could misuse users' funds for illegal transactions or obtain sensitive user information, particularly in the case of exchanges requiring KYC verification.

However, it is worth noting that some interviewees struggled to pinpoint specific privacy risks associated with Bitcoin. PU12, for instance, admitted, "I haven't heard it because the people around me haven't talked about it." This suggests a lack of awareness or discussion surrounding privacy risks within their social circles.

5.4.5 Privacy measures

When it came to privacy measures, some participants offered suggestions aimed at minimizing the exposure of their personal information and using Non-KYC exchanges and wallets. They proposed diversifying the platforms and wallets they use to avoid sharing all their information on a single platform. Additionally, they recommended

exploring alternatives such as Decentralized Finance (DeFi) and decentralized exchanges, which are perceived as privacy-enhancing options since they typically do not require KYC verification. However, it is important to acknowledge that DeFi platforms have faced several security issues, as reported in recent studies [149], which could pose challenges for users seeking privacy by using these platforms.

One participant mentioned their strategy of avoiding exchanges and opting for wallets that require less identity information. However, this approach may stem from a lack of awareness about decentralized exchanges and desktop or full-node wallets, which offer alternative avenues for cryptocurrency transactions with reduced privacy risks.

One participant offered a strategy to enhance privacy by avoiding direct transfers from personal wallets to other addresses. Instead, they recommended utilizing mixing services, TOR, VPNs, or privacy-focused cryptocurrencies such as Zcash or Monero. However, it is important to note that researchers have identified limitations in using TOR for privacy purposes. They found that transactions issued by the same cryptocurrency node can be linked by adversaries before they are broadcasted to the network [71]. This highlights the importance of understanding the effectiveness and potential drawbacks of various privacy-enhancing measures before relying on them.

Participants also correctly mentioned creating a fresh address for each transaction as a privacy measure, which is an important step that can prevent transactions from being linked to each other through the same address.

One participant admitted to not implementing any measures to mitigate privacy risks, attributing it to their relatively low investment in the market. Interestingly, most interviewees displayed a lack of awareness regarding additional techniques for enhancing privacy. Only a few participants had heard of mixers and were familiar with terms such as CoinJoin and CoinSwap, albeit without a deep understanding of how they function.

One participant expressed skepticism about the efficacy of CoinJoin, mentioning that analyzers can identify CoinJoin transactions and flag them. This skepticism is warranted, as CoinJoin transactions lack distinguishability by the same output amount, as highlighted in recent research [150]. This underlines the importance of understanding the limitations of privacy-enhancing techniques and the need for further education in this area.

Out of the twelve participants, seven were not familiar with privacy coins or their purpose. This lack of awareness indicates that privacy coins are not widely recognized among ordinary users for the unique features they offer. Among those who were aware of privacy coins, a few could name Monero and Zcash. However, their understanding of how these coins provide privacy was limited. For example, only one participant knew that Zcash uses Zero-knowledge proofs to verify transactions, but they were unfamiliar with the specifics of these transactions. This finding is important because when participants assume that a coin provides privacy without understanding the underlying techniques, they may not fully benefit from the privacy features offered by these coins. This issue was highlighted in previous research [74], where users exchanged Bitcoin for privacy coins but failed to adequately protect their privacy by shifting their coins back to the same

Bitcoin address. Additionally, previous studies [151, 152] have shown that transactions in Zcash can still be traced. Moreover, the majority of transactions in Zcash occur in an unshielded pool, where de-anonymization attacks similar to those used in Bitcoin can be applied. This indicates the importance of understanding the nuances of privacy features in different cryptocurrencies to effectively protect users' privacy.

5.5 Discussion

5.5.1 Privacy Awareness

The findings from both the quantitative and qualitative results highlight the increasing awareness of privacy among Bitcoin users. The majority of participants emphasized the importance of privacy in their transactions, indicating a growing recognition of the need for anonymity in the cryptocurrency space. These findings align with and extend previous studies on Bitcoin anonymity [51, 52], suggesting that privacy awareness has improved over time.

It is worth noting that some participants in the qualitative study held misconceptions about Bitcoin's anonymity. They believed that Bitcoin transactions were fully anonymous, with no real identities associated with them. When confronted with questions about privacy attacks and potential solutions, they acknowledged their lack of knowledge but expressed a willingness to explore and implement measures to enhance privacy. This finding indicates a gap in understanding the privacy risks and de-anonymization techniques associated with Bitcoin.

Interestingly, while address reuse and auxiliary information obtained from exchanges or services received significant attention among participants in the quantitative part, common input ownership, a prominent heuristic in de-anonymization techniques, remained largely unknown to the respondents. This suggests that there is a need for increased education and awareness regarding privacy attacks and the specific techniques employed to de-anonymize Bitcoin transactions.

Furthermore, the qualitative study revealed a lack of understanding among some participants about the distinction between custodial and non-custodial wallets. They either lacked awareness or disregarded the risks associated with using centralized exchanges to manage their funds. Despite being aware of past security breaches in well-known exchanges(e.g., Mt. Gox [153], Bitstamp [154], Binance [155]), some participants continued to use them due to the convenience they offered. The complexity of managing cryptographic keys independently discouraged them from adopting non-custodial wallets. While some participants acknowledged the privacy concerns associated with custodial wallets, such as the potential correlation of transactions and the requirement of Know Your Customer (KYC) procedures, others were either unaware or simply did not consider these privacy issues.

There were participants who held the perception that blockchain itself ensures privacy as transactions are conducted using addresses rather than real identities. Additionally,

some participants associated privacy-preserving tools or coins with criminal activities or tax evasion, leading them to refrain from adopting privacy-enhancing measures or tools. These findings highlight the presence of privacy misconceptions among users, similar to those identified in previous studies [53]. It is essential to address these misconceptions and educate users about the implications of transaction transparency on the blockchain.

Wallets play a crucial role in shaping user behavior and understanding regarding privacy. They have the opportunity to implement educational features or notifications to inform users about the public nature of transactions on the blockchain. For example, wallets can notify users about the public availability of their transactions and discourage address reuse by automatically generating new addresses or providing warnings when reusing addresses. By indexing addresses and providing feedback on address reuse, wallets can actively engage users in practicing better privacy hygiene.

The findings from both the qualitative and quantitative studies highlight a significant lack of awareness among Bitcoin users regarding privacy-enhancing techniques and privacy-by-design blockchains.

In the qualitative study, it was observed that most participants were unaware of the existence of add-on techniques for improving privacy in Bitcoin, as well as the availability of privacy-by-design blockchains. This indicates a gap in knowledge and understanding among users regarding the various methods and tools that can be employed to enhance privacy in the Bitcoin ecosystem.

The quantitative study further revealed that, even among the participants who responded to being aware of privacy-enhancing techniques, their understanding of these techniques was limited. Mixing websites emerged as the most popular technique, while other techniques were selected by less than half of the participants. These findings suggest that, even when considering potential biased answers, a significant portion of the participants remains unaware of the range of privacy-enhancing techniques available in Bitcoin. This aligns with the findings of a previous study [52], which showed that more than half of the participants were unaware of popular techniques like CoinJoin and ZeroCoin (now known as Zcash). It is important to note that our study considered additional add-on techniques and privacy coins beyond what was explored in the previous study.

However, it is worth noting that in the quantitative study, a majority of the participants (over two-thirds) were aware of privacy coins like Monero and Zcash. This suggests that these privacy-focused cryptocurrencies have gained more visibility and recognition among users. Nevertheless, the participants' understanding of these privacy coins and their underlying mechanisms was limited, indicating a need for further education and awareness.

The qualitative findings also revealed that many participants had little to no understanding of how to use privacy-enhancing techniques or the mechanisms behind them. They lacked knowledge about the type of data that these techniques can hide or protect. Some participants perceived these techniques as overly technical and believed that they were

more suitable for advanced users, rather than novice users who primarily engage in cryptocurrency trading and investment activities.

This lack of understanding is compounded by negative perceptions associated with using privacy tools, such as the assumption that they are primarily used for criminal activities or tax evasion. Additionally, there is a need to educate users about the potential misuse of blockchain for malicious actions. Integrating educational information and features directly into wallets, such as meaningful notifications and privacy features like generating fresh addresses, could help address these gaps in understanding. Furthermore, comprehensive documentation and social media campaigns can also contribute to raising awareness and fostering a better understanding of privacy-enhancing techniques in the Bitcoin community.

It is important to distinguish between public privacy and private privacy. Public privacy refers to information that is publicly available on the blockchain and visible to everyone. Private privacy, on the other hand, involves data that is not public but accessible to governments, exchanges, or wallets. Exploring collaborative de-anonymization research for achieving private privacy can be valuable [156].

5.5.2 Privacy Preferences

The study revealed interesting insights into the privacy preferences of Bitcoin users. While more than half of the participants expressed a preference for using privacy coins, a significant number of those who chose to use Bitcoin indicated their expectation of future built-in privacy improvements. However, it is important to note that achieving built-in privacy improvements in Bitcoin itself may not be realistic in the near future. Instead, such enhancements are more likely to be implemented through wallets or layer two solutions.

Interestingly, users expressed a willingness to accept longer transaction times in exchange for better privacy. This suggests that users prioritize privacy over transaction speed, recognizing the trade-off between convenience and protecting their personal information. However, when it comes to paying extra fees for privacy, opinions were divided, with half of the participants dismissing the idea. This finding highlights the importance of implementing privacy solutions in a way that minimizes additional fees, as users may be reluctant to incur high transaction costs, especially considering the current high Bitcoin transaction fees.

It is worth noting that many existing privacy solutions for Bitcoin, such as CoinJoin and CoinSwap, require multiple transaction fees due to the need for multiple rounds of the protocol to achieve sufficient privacy. This results in higher overall fees for users. Given the current transaction fee landscape, the cost of utilizing privacy solutions can be relatively expensive. Therefore, it is crucial to explore and develop privacy solutions that require fewer fees, as users may be unwilling to pay additional transaction fees, particularly for transactions with smaller amounts.

Participants who were aware of the distinguishability issues associated with CoinJoin transactions with the same output amount expressed reluctance to use this technique. Instead, they favored alternative privacy techniques that preserve indistinguishability, making it difficult for monitoring tools to flag the transactions. Techniques such as PayJoin, threshold signatures, and CoinSwap offer varying degrees of indistinguishability, but their adoption in practice is still limited.

It is worth mentioning that the potential of PayJoin transactions being flagged with unnecessary input heuristics has been investigated in a related study [157]. This highlights the need for further research and development to address potential vulnerabilities and improve the effectiveness of privacy-enhancing techniques.

5.5.3 Privacy Wallets

Although privacy wallets have been in development since around 2015, they continue to face challenges in attracting a larger user base. The complexity of these wallets and the requirement for users to possess a basic understanding of privacy concepts and techniques contribute to this struggle [13]. As a result, the adoption of privacy wallets remains limited.

One of the challenges faced by current Bitcoin CoinJoin wallets is the distinguishability issue associated with CoinJoin transactions that have the same output amount. This issue compromises the privacy-enhancing capabilities of these wallets, as the transactions can be identified on the blockchain. Conversely, the newly implemented indistinguishable techniques, such as PayJoin, may face potential bans imposed by governments. Such a scenario would pose a significant problem for both wallet developers and users who rely on these privacy techniques.

Another finding from our study is that users prefer wallets that support multiple cryptocurrencies. It is unrealistic to expect users to install separate wallets for each individual coin, and asking them to install additional wallets specifically for privacy purposes would further add to the burden of learning and managing multiple wallet functionalities.

To address these challenges, future efforts should focus on improving the usability and user experience of privacy wallets. Simplifying the setup and operation processes, as well as providing clear and intuitive user interfaces, can help lower the barriers to entry for non-technical users. Moreover, ongoing research and development should explore innovative privacy-enhancing techniques that offer better privacy guarantees and are less susceptible to distinguishability issues or potential bans.

5.6 Conclusion

In this chapter, we conducted a comprehensive study to explore user perceptions and preferences regarding privacy in Bitcoin. Our findings shed light on the disparity between users' preferences and the actual implementation of privacy techniques in practice. One

key finding of our study is that most users expressed a preference for privacy coins over add-on techniques in Bitcoin. This indicates a strong desire among users for cryptocurrencies that inherently prioritize privacy. Additionally, our results revealed that participants were more inclined to accept transaction delays as a trade-off for achieving anonymity, rather than paying extra fees.

Furthermore, our study highlighted users' preference for indistinguishable privacy techniques that evade detection by monitoring tools, as opposed to techniques that may be flagged due to distinguishable transaction patterns. This finding emphasizes the importance of developing and implementing privacy solutions that effectively preserve users' anonymity without raising suspicions.

However, it is worth noting that current privacy wallets offering CoinJoin transactions with equal-sized outputs suffer from distinguishability issues on the blockchain. This raises important questions regarding the efficacy of existing privacy wallet implementations and calls for further research and development to address these challenges.

Our study demonstrates that users who prioritize privacy are less likely to choose Bitcoin as their preferred cryptocurrency. Instead, they favor the integration of built-in privacy features directly into the Bitcoin protocol. These findings underscore the importance of exploring and implementing robust privacy measures within Bitcoin itself to meet users' expectations and enhance the overall privacy of the cryptocurrency.

In the next chapter, we evaluate the usability of Bitcoin privacy wallets that facilitate CoinJoin transactions, with a specific focus on three major Bitcoin wallets that offer this feature, namely JoinMarket, Wasabi, and Samourai. We conduct a cognitive walkthrough, drawing on the feedback of two experts in blockchain security and privacy research.

CHAPTER 6

Usability of Cryptocurrency Wallets Providing CoinJoin Transactions

6.1 Introduction

This chapter presents a comprehensive usability study of three prominent Bitcoin wallets that integrate the CoinJoin technique: JoinMarket [108], Wasabi [131], and Samourai [132]. The objective of this study is to evaluate the ease of use and user experience of these wallets by conducting a cognitive walkthrough based on usability and design criteria. The findings of this study will provide valuable insights to privacy wallet developers, enabling them to enhance user experience and improve the usability of their wallets.

CoinJoin-based techniques have emerged as popular privacy-preserving methods for coin mixing, as evidenced by previous blockchain analyses [158, 159, 160]. However, in order to achieve widespread adoption of privacy wallets, it is crucial to address usability aspects and ensure a seamless user experience. This becomes particularly important when considering the significance of user numbers in achieving the desired level of anonymity [161]. If a privacy wallet is not designed with usability in mind, it may become a barrier to user adoption.

Furthermore, an understandable, informative, intuitive, and user-friendly privacy wallet is essential for guiding users through their journey and preventing actions associated with risks that could lead to undesired and irreversible outcomes. Therefore, studying the ease of use of privacy wallets can provide insights into user acceptance of sophisticated technologies like coin mixing.

In this chapter, we aim to address the intersection of privacy-preserving techniques and user experience by conducting an extensive evaluation of the usability of JoinMarket,

Wasabi, and Samourai wallets. These wallets have been selected as they are currently the primary options supporting CoinJoin transactions, which are a prevalent privacy-enhancing feature in Bitcoin [11]. We have excluded other wallets that either no longer offer CoinJoin transactions or have been discontinued [11].

While our previous works [11] have provided comprehensive evaluations of mixing techniques, this chapter specifically focuses on the usability aspect of Bitcoin wallets that support CoinJoin transactions.

We define the following research questions for this study:

RQ 1: How do the selected wallets differ in terms of anonymity set and CoinJoin creation time, and how do these differences impact their overall effectiveness in enhancing transaction privacy?

RQ 2: What are the specific usability issues [8] identified during the cognitive walkthrough and user study in the context of coin mixing within the selected wallets, and how do these issues vary among the wallets?

RQ 3: What are the fundamental design criteria [9] outlined in the learnability walkthrough, and how well do the selected wallets adhere to these criteria in terms of their coin-mixing functionality?

RQ 4: What specific improvements or design changes can be recommended for each wallet based on the results of the cognitive walkthrough and user study?

To evaluate the usability of these wallets, we employ a cognitive walkthrough methodology based on the expertise of two researchers with a background in blockchain security and privacy research. This approach allows us to gain insights into the user experience by simulating typical user interactions with the wallets. Additionally, we discuss prominent usability issues and identify important features that privacy wallets should provide to enhance user satisfaction and security.

Furthermore, we conducted a small-scale user study involving two participants who are experts in security and privacy in computer science and five participants in a blockchain workshop. This study allows us to assess task success and completion time, which are key indicators of usability. By involving domain experts, we can gain valuable insights into the usability challenges and potential improvements from a technical perspective.

Additionally, we conducted a usability test on the most user-friendly wallet identified through the cognitive walkthrough and small-scale user study. This usability test involved five participants in a blockchain workshop, providing a broader perspective on the usability of the selected privacy wallet.

By conducting this usability study, we aim to contribute to the development of more user-friendly privacy wallets and provide guidance to users in selecting the most suitable wallet for their specific needs. The insights gained from this study can inform wallet developers on improving the user experience of their products, ultimately facilitating wider adoption of privacy-enhancing techniques in the cryptocurrency ecosystem.

The remainder of the chapter is structured as follows: Section 6.2 discusses the methodology and the evaluation criteria, while Section 6.3 introduces the main concepts and reviews the wallets. Section 6.5 evaluates the usability of the wallets according to predefined criteria in 6.4. While Section 6.6 outlines the walkthrough discussion, Section 6.7 presents the results from the small-scale study. Section 6.8 provides issues reported by authors and experts. Section 6.9 provides the usability test result with the participants in a workshop, and Section 6.10 concludes the work and summarizes the challenges.

6.2 Methodology

To evaluate the usability of CoinJoin wallets, we employed a cognitive walkthrough methodology inspired by the approaches outlined in [55, 56]. The cognitive walkthrough technique focuses on assessing the effectiveness of application tasks and features, particularly by examining how well first-time users can perform these tasks without formal training. The Cognitive Walkthrough is a method that evaluates user interfaces by delving into the mental processes users undergo. The process involves an analyst selecting a specific task, figuring out the right sequences of actions for that task, and evaluating whether a hypothetical user could effectively choose suitable actions at each step. Cognitive Walkthrough aims to provide early evaluations of designs, assisting designers in understanding how features come together to support users' tasks. The method encourages thorough consideration of task performance and interface support. Cognitive Walkthrough provides feedback for designers to assess the reasonableness of their expectations regarding user interactions [162]. In contrast to user testing, Cognitive Walkthrough is cost-effective as it does not require user involvement [163].

The overall process of our methodology is illustrated in Figure 6.1. We initiated the evaluation by defining the problem statement and formulating research questions that aimed to investigate the practicality, intuitiveness, and ease of use of privacy wallets. Subsequently, we carefully selected a set of wallet candidates for the evaluation, ensuring that they supported the CoinJoin technique.

Next, we proceeded to define the specific tasks that would be performed by both experts and users during the evaluation. The experts, who were security and privacy researchers, assessed the learnability of each wallet by observing how novice users would navigate through the tasks and identifying any potential errors or issues they might encounter [55]. On the other hand, the user study involved a small sample size of two computer science experts specializing in information technology security and privacy, who possessed a strong familiarity with cryptocurrency wallets, and also five participants for evaluating the usability of the most user-friendly wallet obtained from walkthrough and expert usability test.

Throughout the evaluation, we meticulously captured and documented the results obtained from the cognitive walkthrough and user study. These results were then subjected to careful analysis to identify patterns, trends, and recurring issues that emerged during

the usability assessment. Based on the analysis, we proposed potential improvements and recommendations to address the identified usability challenges.

By following this comprehensive methodology, we aimed to provide a robust evaluation of the usability of CoinJoin wallets. The combination of cognitive walkthroughs and user studies allowed us to gain valuable insights from both expert and user perspectives, facilitating a holistic understanding of the strengths and weaknesses of the evaluated wallets. These insights served as the basis for proposing practical recommendations to enhance the user experience and usability of privacy wallets in the context of CoinJoin transactions.

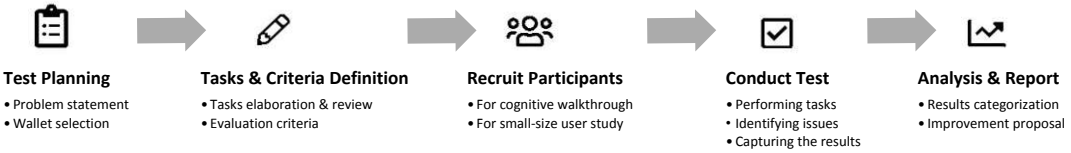


Figure 6.1: Methodology Process

6.3 Wallet Design

6.3.1 Wallet Selection and Basic Design

In this study, we have selected three prominent wallets that support CoinJoin transactions, namely JoinMarket, Wasabi, and Samourai. Below, we provide a summary of each wallet's design and highlight its key properties.

JoinMarket wallet.

JoinMarket [108] is a desktop wallet that employs a taker-maker model to facilitate the generation of CoinJoin transactions. In this model, a user acts as a taker and initiates a request to create a CoinJoin transaction by broadcasting their willingness to join on the Internet Relay Chat (IRC) messaging channel. The taker specifies the desired amount, fee, and the number of counterparties (input peers) they wish to include in the transaction.

Makers who are listening on the IRC respond to the taker's request by confirming their participation and providing information about their fees. Once the taker receives the participation confirmations from the makers, they proceed to create the transaction with the desired CoinJoin amount and send it to the makers for signing.

One of the challenges faced by JoinMarket is the issue of liquidity. Finding a sufficient number of peers to participate in CoinJoin transactions can be a difficult task due to the limited availability of counterparties. Insufficient liquidity impacts the overall effectiveness and feasibility of creating CoinJoin transactions using JoinMarket. Additionally, the IRC messaging channel has limitations and cannot efficiently handle a significant number of participating makers [164].

An interesting feature of JoinMarket is that the taker has the ability to include the desired recipient address among the outputs of the CoinJoin transaction. This design choice allows the taker to directly send the mixed coins to the intended recipient address. This is different from other wallets where users typically send the mixed coins to their own addresses and then create a separate transaction to send the coins to the desired destination address.

Wasabi wallet.

Wasabi [131] is a desktop wallet that utilizes a coordinator to facilitate CoinJoin transactions based on the Chaumian CoinJoin technique [134]. The process of creating a CoinJoin transaction in Wasabi involves three main phases: input registration, output registration, and signing.

In the input registration phase, users register their inputs by providing the UTXOs, proof of UTXO ownership, change address to receive the remainder, and their blinded output to the coordinator. This registration process helps prevent the correlation of inputs to outputs. The coordinator then verifies the inputs, ensuring that they contain sufficient funds and have not been spent before, and signs the blinded output before sending it back to the user.

In the output registration phase, users unblind their outputs and send them to the coordinator. The coordinator checks if her signature is present on the output and proceeds to create a CoinJoin transaction with all the registered UTXOs as inputs and the registered outputs and change addresses as the transaction's outputs.

In the signing phase, the coordinator sends the transaction for signing by the corresponding users, collects all the signed transactions, combines the signatures, and broadcasts the final transaction to the network [134].

Wasabi provides an interface with a dedicated CoinJoin tab where users can select the coins they wish to mix and register them into the Wasabi pool. At the time of our research, there is only one pool available with a predetermined amount (e.g., 0.104 BTC on the mainnet). The CoinJoin transaction is created either when a certain number of inputs are registered (100 peers) or when a specific time interval is reached (e.g., one hour). Once the CoinJoin transaction is broadcasted, the mixed coins, along with their associated anonymity set, are listed in the "CoinJoin" and "Send" tabs, allowing users to spend them.

Samourai wallet.

Samourai [132] is a mobile wallet specifically designed for Android devices. It incorporates a coordinator-based approach using the Chaumian CoinJoin technique, known as "Whirlpool," to facilitate CoinJoin transactions. Currently, Samourai offers four different pools with varying denominations (0.001 BTC, 0.01 BTC, 0.05 BTC, and 0.5 BTC) for users to create CoinJoin transactions. These transactions are executed with a flat fee rate, providing a convenient and transparent cost structure.

In the Samourai wallet, users register their coins into one of the available pools and wait for the necessary number of peers to participate in order to create a CoinJoin transaction. Upon registration, the coins are initially split into the chosen pool's specified amount in transaction 0 (TX0). These unspent transaction outputs (UTXOs), referred to as pre-mix UTXOs, are distinct from mixed UTXOs as they have not undergone the mixing process yet. The pre-mix UTXOs are listed in the pre-mix wallet within the Samourai application.

Once registered, the pre-mix UTXOs are associated with a coordinator, which orchestrates the creation of the CoinJoin transaction for the selected pool. As a result, the mixed UTXOs, which have gone through the CoinJoin process, appear in the post-mix wallet of the Samourai wallet application.

The Samourai wallet consists of multiple wallet compartments, including the main wallet, pre-mix wallet, and post-mix wallet. The main wallet serves as the primary interface for managing and storing users' bitcoins. The pre-mix wallet displays the registered pre-mix UTXOs, providing visibility into the coins awaiting mixing. Finally, the post-mix wallet showcases the mixed UTXOs resulting from the CoinJoin process. Users have the flexibility to select and send the mixed coins from the post-mix wallet to their desired addresses, enabling secure and private transactions.

6.3.2 Wallet Basic Properties

In this section, we discuss the fundamental properties of each wallet, including platform support, CoinJoin transaction fees, and anonymity set. Table 6.1 provides a summary of these properties for both mainnet and testnet environments.

Table 6.1: Features of the selected wallets

Wallet	Platform Support	Network	Anonymity set **	CJ† creation time	CJ amount	CJ fee
JoinMarket [108]	Linux, MacOS, Windows, RaspiBlitz, RaspiBolt, Qubes+Whonix	testnet/ mainnet	Set by user (Current default: 9)	X±±	Set by user	Set by user (Random fees ∼0.001%)
Wasabi [131]	MacOS 10.13+, Windows 10, Debian / Ubuntu, and Other Linux systems	testnet	3 peers	24 hours	0.0001 BTC	Coordination fee 0.003%⋆
		mainnet	100 peers	1 hour	∼0.104 BTC	Coordination fee 0.003%⋆
Samourai [132]	Android	testnet/ mainnet	5 peers	X±±	0.001 BTC 0.01 BTC 0.05 BTC 0.5 BTC	TX0 fee+Pool fee 0.00005BTC TX0 fee+Pool fee 0.0005BTC TX0 fee+Pool fee 0.0025BTC TX0 fee+Pool fee 0.025BTC

** Per CoinJoin transaction. † CoinJoin. ±± Depends on the liquidity.⋆ Per anonymity set.

Platform support: Wasabi and JoinMarket are desktop wallets that offer compatibility with various operating systems, ensuring broad accessibility for users. On the other hand, Samourai exclusively functions as a mobile wallet, specifically designed for the Android platform.

Anonymity set per CoinJoin transaction: The concept of an anonymity set refers to the number of peers participating in a CoinJoin transaction, thereby obscuring the link between inputs and outputs. Wasabi has the potential to provide large anonymity sets due to the liquidity within its network. As of the time of writing, Wasabi can achieve an anonymity set of up to 100 participants. In contrast, Samourai currently creates CoinJoin pools with a fixed number of five peers. JoinMarket's anonymity set is determined by

user-defined preferences but is constrained by the available liquidity on the network and the handling capacity of the IRC messaging channel.

CoinJoin creation time: This property denotes the minimum duration required to initiate a single round of CoinJoin. The creation process of a CoinJoin transaction in JoinMarket and Samourai relies on the availability of other peers within the network. Consequently, the time taken to create a CoinJoin transaction may vary depending on the number of participants available. Conversely, Wasabi imposes a requirement of reaching a certain number of registered peers (100) or a predetermined waiting time (typically one hour) before a CoinJoin is created on the Bitcoin mainnet.

CoinJoin amount: The CoinJoin amount refers to the number of coins that a user can register for a CoinJoin transaction. JoinMarket does not impose any restrictions on the amount, allowing users the flexibility to choose the desired transaction size. Furthermore, JoinMarket users are not confined to a specific number of input peers, as this parameter can be set by the user. On the other hand, Samourai offers specific pools with predefined amounts, limiting user options to select from these preconfigured denominations. Wasabi, similarly, provides a single pool with a predetermined amount, restricting users to that specific value.

CoinJoin fee: The CoinJoin fee represents the cost associated with executing a CoinJoin transaction. JoinMarket employs a random fee distribution to the makers, which is typically around 0.001% of the transaction amount on the testnet. In Wasabi, the fee is calculated based on a percentage (0.003%) of the transaction per anonymity set. Samourai, on the other hand, adopts a flat fee rate for its pools, irrespective of the user's UTXO amount. However, users need to pay the transaction fee for transaction 0 in advance to participate in the pool.

By considering these basic properties, users can assess the platform compatibility, anonymity guarantees, and operational timeframes offered by each wallet. Considering the CoinJoin amount and CoinJoin fee provides valuable insights into the cost-effectiveness and financial implications of utilizing CoinJoin wallets. Users can evaluate the suitability of each wallet based on their specific requirements and budget. These factors play a vital role in the usability and attractiveness of CoinJoin wallets, especially for privacy-conscious users seeking optimal privacy protection while minimizing transaction costs.

6.4 Evaluation Criteria

To assess the usability and design effectiveness of the evaluated wallets, a set of tasks and evaluation criteria are established. The tasks aim to capture the essential functionalities of the wallets, while the evaluation criteria provide a framework for assessing usability and design aspects. The following sections outline the defined tasks and evaluation criteria.

6.4.1 Tasks Definition.

The participants in the evaluation are required to perform the following tasks:

- **T.1 Installing the application**: Participants are tasked with installing the wallet application on their respective devices.
- **T.2 Generating a wallet**: Participants need to generate a new wallet within the application.
- **T.3 Funding the wallet**: Participants are instructed to add funds to their wallets, simulating the process of funding the wallet with cryptocurrencies.
- **T.4 Performing a CoinJoin transaction**: Participants are expected to initiate and complete a CoinJoin transaction within the wallet application.
- **T.5 Transferring CoinJoin coins to the destination address**: Participants need to transfer the mixed coins resulting from the CoinJoin transaction to a specified destination address.

6.4.2 Evaluation Criteria

. The evaluation criteria are derived from established usability and design principles, which provide a comprehensive framework for assessing the wallets. The following criteria are considered:

1) Usability criteria (adapted from Nielsen's Usability Heuristics [8]):

- *Learnability*: This criterion evaluates the ease with which users can perform tasks correctly on their first attempt, without prior experience or guidance.
- *Errors*: The errors made by users during task completion and the system's ability to support error recovery are assessed.
- *Efficiency*: The time taken by users to complete tasks is measured, focusing on the speed and efficiency of task execution. This criterion is evaluated exclusively during the user study.

2) Fundamental design criteria (adapted from Ljunggren and colleagues [9]):

- *Visibility*: The visibility criterion assesses whether users can clearly perceive and identify elements (e.g., buttons, tabs) that are essential for interaction. Visible elements aid users in discovering and utilizing the available features.

- *Feedback*: This criterion examines whether users receive appropriate feedback when they perform actions (e.g., clicking buttons or tabs). Clear and informative feedback is crucial to prevent user confusion. In case of any problems, explicit notifications should be provided.
- *Constraints*: The constraints criterion evaluates the extent to which the interaction possibilities are limited and clearly communicated to users. Well-defined constraints help users understand what actions they can take and prevent confusion.
- *Mapping*: Mapping refers to the clarity of the relationship between functions (e.g., buttons) and associated actions. This criterion examines whether users can easily understand the connections between various elements in the interface. Additionally, the terminology used in the interface should be clear and understandable.
- *Consistency*: Consistency assesses whether users can perform similar actions using similar elements within the interface. Consistent design patterns and interaction elements improve learnability and memorability, enabling users to transfer their knowledge from one part of the system to another.

6.5 Cognitive walkthrough

The cognitive walkthrough was conducted using the Bitcoin testnet to evaluate the usability of the JoinMarket, Samourai, and Wasabi wallets. This approach allows us to gain insights into the user experience by simulating typical user interactions with the wallets. This walkthrough highlights potential usability issues.

6.5.1 JoinMarket Wallet

We tested JoinMarket version 0.8.2 on Ubuntu 20.04.2 LTS and Windows 10, focusing on the usability of JoinMarket's graphical user interface (GUI), known as JoinMarket QT.

T.1 Installing the application.

Learnability: Installing the JoinMarket wallet requires following the instructions provided on the JoinMarket GitHub page. However, the process involves installing several dependencies, such as Python 3 and Bitcoin Core, which can be time-consuming. Selecting the appropriate assets for download based on the user's operating system may also be confusing for novice users, as it fails to meet the constraints criterion. On Linux, the installation process involves running the "install.sh" script interactively, following the commands provided on the quick start page, and running the wallet scripts. During the installation, users are informed about the availability of the Qt GUI, which can be selected.

The GitHub page redirects users to the "usage guide" page if they are new to JoinMarket or to the "JoinMarket-QT walkthrough" page if they are familiar with the wallet. The usage guide mentions that running the wallet script will result in an error unless the

Bitcoin Core configuration is completed, which can be a barrier for users who can not conduct the configuration. The Bitcoin Core configuration instructions are provided separately in the documentation, and consolidating all Bitcoin Core configuration guides into one section would improve visibility and reduce confusion. Additionally, the separate instructions for configuration should be clearly referenced when necessary.

Using JoinMarket QT on Windows 10 resulted in an error related to the secp256k1 library. As a workaround, we had to use QT.exe instead. When users download the .exe file via Chrome, they may receive a warning message suggesting discarding the file. If the user proceeds to open the file, Windows prevents the app from running, which is an unpleasant experience for users. The installation guide should inform Windows users about this issue and provide instructions on how to verify the file. Furthermore, when QT is run for the first time, it exits with a Bitcoin Core connection failure error, and users must configure Bitcoin Core after the initial attempt, similar to the Linux configuration process.

Errors: The release page on GitHub does not categorize files based on different operating systems, potentially leading to confusion for users when selecting the appropriate files for their OS.

T.2 Generating a wallet.

Learnability: When launching JoinMarket QT for the first time, the user is presented with a menu that allows them to choose between loading an existing wallet or generating a new one, achieving visibility. Clicking the "generate" button initiates a prompt that asks the user to enter a two-factor mnemonic recovery passphrase, which may be technical and unfamiliar to some users. To ensure accuracy, the passphrase needs to be entered twice, meeting the constraints criterion. The user has the option to leave the wallet name as the default or customize it according to their preference. After the wallet is generated, the recovery words and seed phrase are displayed, and the user is instructed to write them down for future reference, providing clear feedback. A confirmation message confirms the successful generation of the wallet, providing further feedback.

Upon wallet generation, a message appears recommending the restart of Bitcoin Core for wallet recovery or generation. If the user clicks "OK," they are presented with the option to quit JoinMarket with "yes" or "no" options. Choosing "no" will load the wallet, while selecting "yes" will close JoinMarket. However, if the user loads the wallet without restarting Bitcoin Core as recommended, they may become confused if they recall the previous message, indicating a mapping issue.

Errors: The wallet lacks clear instructions regarding the importance of the order of the recovery words and does not prompt the user to verify the recovery words for accuracy. These improvements in the user interface and instructions can enhance the overall user experience and minimize the risk of wallet loss due to inaccurate recovery phrase entry.

T.3 Funding the wallet.

Learnability: In JoinMarket QT, there is no dedicated "Receive" button commonly found in other wallets to create an address for receiving Bitcoin. Instead, addresses are generated within "mixdepths" that are not initially visible to the user, failing the visibility criterion. To access the addresses, the user must click on the mixdepths to expand them and view the corresponding addresses. Once an address is selected, the user can copy it and use it to receive funds. After receiving funds, the new balance is updated in JoinMarket. However, the wallet does not provide any notification to inform the user of the funds received, thus failing the feedback criterion. It is important to note that the current presentation of addresses based on mixdepths may not be intuitive for novice users.

Errors: The use of indexed addresses, indicated by the color red for deposits, as a means to mitigate address reuse is not a clear indication for the user to avoid reusing addresses. This can lead to privacy concerns as address reuse can link transactions to a single entity. Furthermore, there is a possibility of accidentally copying a funded address and reusing it, which compromises privacy. To ensure better privacy, the wallet should implement a more user-friendly approach to address generation and management while actively discouraging address reuse. Clear instructions and warnings can be provided to educate users about the importance of using new addresses for each transaction and avoiding the reuse of previously funded addresses.

T.4 Performing a CoinJoin transaction

Learnability: During our testing, due to limited liquidity on the testnet, we conducted a single CoinJoin transaction with one counterparty using JoinMarket. To initiate the CoinJoin process in JoinMarket QT, the user needs to open the "Coinjoins" tab, which achieves visibility. In this tab, the user must provide the recipient address, the number of counterparties, mixdepth, and amount for the transaction. However, the concept of mixdepth may be confusing for novice users, and the current presentation in JoinMarket QT does not clarify that coins from different mixdepths cannot be spent in a single transaction. Therefore, it is important to provide a clear guide or explanation to users about the concept of mixdepths and their limitations.

Once the CoinJoin transaction is broadcasted to the IRC channel, the details of the ongoing process are displayed in a box at the bottom of JoinMarket QT. However, some of the technical messages in the box may not be easily understood by novice users, resulting in a lack of clear feedback.

If a user wants to spend the entire balance of a mixdepth, they need to enter zero as the amount, which is not clearly indicated in JoinMarket QT, failing the visibility criterion. To enhance the user experience, the wallet could incorporate a "maximum" button that automatically fills in the maximum amount for the selected mixdepth. After the CoinJoin transaction is created and broadcasted, the user can view the details in the "TX History" tab. It is worth noting that JoinMarket also offers additional features like MultiJoin and the ability to act as a maker to earn money by creating CoinJoin transactions, which were beyond the scope of our study.

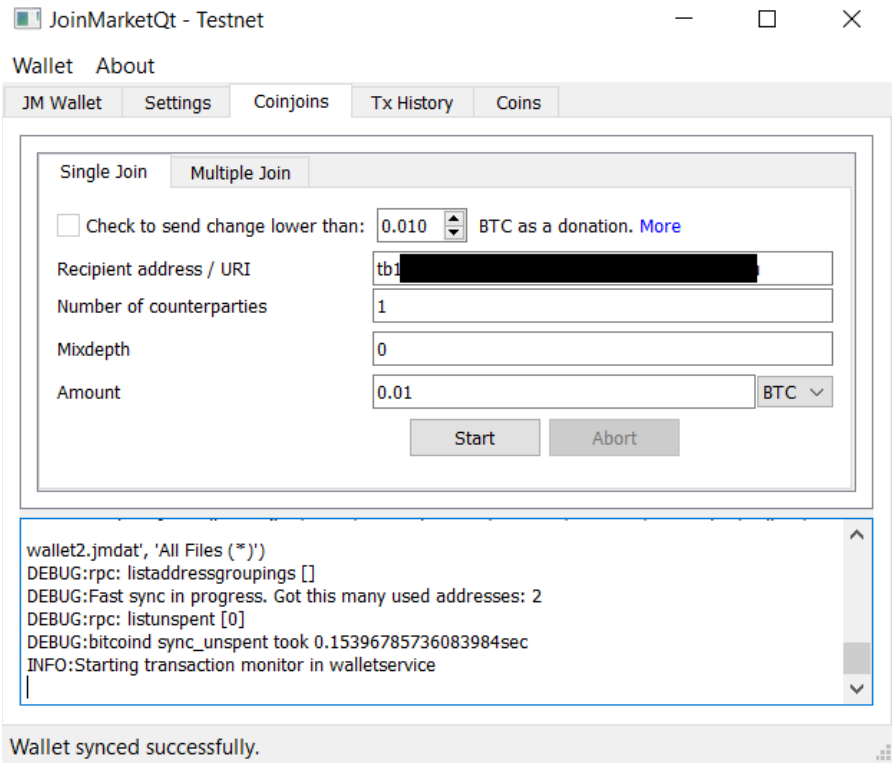


Figure 6.2: JoinMarket CoinJoin

Errors: If the user chooses to spend coins with less than five confirmations, the transaction is aborted. However, the error message displayed is not clear and provides a lengthy list of three possible reasons for the transaction abort, failing the feedback criterion. Providing a clear and concise error message that specifically indicates the cause of the transaction abort would greatly assist users in troubleshooting such issues. Additionally, it is recommended to check for unconfirmed coins before broadcasting the transaction to the IRC channel to prevent confusion caused by the "Transaction is aborted" error.

In our testing, we encountered an error stating "error pushing = -26 min relay fee not met" during our first attempt to create a CoinJoin transaction. This error message was not clear, failing the feedback criterion. Upon researching the issue, we found that increasing the transaction fee in the configuration can resolve the error. JoinMarket currently does not provide clear guidance or suggestions to address such errors, which may lead users to fail in creating a CoinJoin transaction if they encounter this error. It would be more convenient for users if the transaction was automatically confirmed and created without requiring manual confirmation after a maker is found.

Furthermore, in JoinMarket QT running on Windows, the transaction history does not include incoming transactions, only listing the CoinJoin transactions created by the wallet. This omission can make it difficult for users to find details of incoming transactions, failing

the mapping criterion. Improving the transaction history functionality to include all relevant transactions, including incoming transactions, would enhance the user experience and make it easier to track the flow of funds within the wallet.

T.5 Transferring CoinJoin coins. As a result of the direct send possibility, T.5 could be done during T.4.

6.5.2 Wasabi Wallet

We tested Wasabi Wallet version 1.1.12.5 on Ubuntu 18.04.5 LTS and Windows 10.

T.1 Installing the application

Learnability: The installation process for Wasabi Wallet is straightforward and user-friendly. The download button on the website is clearly visible, achieving the visibility criterion. Users can easily select the appropriate package based on their operating system, meeting the constraints criterion. A step-by-step installation guide is provided, which assists users in installing the wallet. On Windows, the package is signed and verified, ensuring the integrity and authenticity of the software. For other operating systems, the installation guide suggests verifying the package using Pretty Good Privacy (PGP). The installation steps are well-documented, guiding users through the process and minimizing the likelihood of critical errors.

Errors: The installation process for Wasabi Wallet is designed to prevent critical errors by providing clear instructions and guidance to users. By following the recommended installation steps, users can install Wasabi Wallet without encountering significant errors or issues.

T.2 Generating a wallet.

Learnability: The process of generating a wallet in Wasabi Wallet is designed to be user-friendly and intuitive. When Wasabi is run for the first time, the user is prompted to generate a wallet, meeting the constraints criterion. The wallet generation page requires the user to fill in a name and a password, achieving visibility. A warning message informs the user that the password is crucial for wallet recovery and cannot be forgotten. The option to show the characters entered in the password field helps the user verify their input. Leaving the password field empty is also acceptable.

On the next page, the twelve recovery words are displayed. The user is required to confirm that they have written down both the recovery words and password to proceed with wallet generation. However, to prevent any misinterpretation, we suggest adding the word "BOTH" before "your Recovery Words AND your Password" in the instructions. Once the user clicks on the generate button, the wallet name is displayed on the page, achieving the mapping criterion. To load the wallet, the user needs to enter their credentials, including the password. The password box is located at the bottom of the page, and if the user accidentally double-clicks on the wallet, a "Wrong password" message appears at the bottom right, providing immediate feedback. To further enhance clarity, the message can be replaced with "Enter the password" to guide the user appropriately.

Additionally, Wasabi Wallet provides easy access to the log and the folder containing all the wallet files, achieving the feedback criterion. The user interface is designed to be simple and not overloaded with functionalities, meeting the constraints criterion. The feature names within the wallet interface are self-explanatory, ensuring a clear understanding of the available options, achieving the mapping criterion. Furthermore, notifications are color-coded with green indicating success and red signaling potential problems, providing visual feedback to the user.

Errors: To improve the wallet generation process, we suggest making a few enhancements. Firstly, we recommend asking the user to enter the recovery words on the next page to ensure they have correctly written down the backup of their recovery words. This additional step provides an extra layer of assurance for the user.

Furthermore, it is important to inform the user that the order of the recovery words is crucial for wallet recovery. Currently, Wasabi Wallet displays twelve recovery words in three columns, with each column containing four words. The order of the words is based on the columns, which may differ from other wallets where the order is based on the rows. To avoid confusion and potential wallet recovery issues, it is important to clearly state that the order of the recovery words should follow the provided sequence, highlighting the column-based arrangement. This will help prevent accidental errors by users who may mistakenly follow a row-based order.

T.3 Funding the wallet.

Learnability: Upon loading the wallet for the first time, the user is directed to the "Receive" tab, meeting the constraints criterion. In this tab, the user can generate an address by labeling it and clicking the "Generate receive address" button, achieving visibility. However, the purpose of labeling the address is not clearly explained, leading to a mapping failure. To avoid confusion, a clear message should be displayed, indicating that the labeling is for the user's own reference.

The generated address is displayed with its label, and double-clicking on the address copies it and displays a feedback message of "Copied," achieving the feedback criterion. However, clicking on the address or its label does not show additional information, resulting in a visibility failure. To improve accessibility, a new button labeled "More info" can be added, which, when clicked, displays the QR code, public key, and key path of the address. Additionally, displaying the QR code alongside the address can enhance visibility.

After an address is funded, it disappears from the receive tab to prevent address reuse, and a feedback message is displayed at the bottom of the page, achieving the feedback criterion. The received coins can be viewed in the history tab, including transaction time, amount, transaction ID, and specified label. Double-clicking on a row opens a new tab with additional confirmation status and block height information. However, the address that received the funding is not displayed in the transaction details, which can cause confusion. To provide a complete overview, the funded address should be included in the transaction details.

To check incoming transactions, the user can navigate to the history tab, where incoming transactions are shown in green and outgoing transactions in red, achieving the mapping criterion. However, if the user funds multiple addresses, they have to manually copy the transaction ID and use a blockchain explorer to view their address as the input or output of the transaction, which can be confusing. To simplify this process, the user should be automatically redirected to a blockchain explorer when clicking on the transaction ID. Additionally, currently, only the characters located before the cursor are selected when double-clicking on the transaction ID to copy it, leading to inconsistency. Allowing users to copy the entire ID by double-clicking would provide a more consistent experience.

Errors: The public key and key path displayed in the drop-down menu of the created address may be too technical for novice users. When an address is funded, it is important to provide clear feedback to the user, informing them that they can check the transaction status in the history tab. Currently, this feedback is missing, leading to a feedback failure. Adding an informative message on the page after funding would guide the user in the next steps.

Another error occurs on the transaction details page, where it does not update properly, and clicking on a transaction in the history tab takes the user back to the previously opened transaction details with outdated confirmation information, resulting in a consistency failure. To address this issue, the transaction details page should be automatically updated to reflect the most current information, and clicking on a transaction in the history tab should always display the latest details.

T.4 Performing a CoinJoin transaction.

Learnability: CoinJoin transactions can be created through the "CoinJoin" tab, achieving both visibility and mapping criteria (see Fig. 6.3). In this tab, the user is presented with a list of coins along with their labels and associated privacy levels, displayed in different colors (red, yellow, or green). By hovering the cursor over the privacy color, the anonymity set of the coin is shown, providing feedback to the user.

To initiate a CoinJoin, the user selects the desired coins and enqueues them, referred to as input registration in a CoinJoin transaction. The user can specify the target anonymity set by clicking the "Target", achieving visibility. Although three default anonymity sets are shown, the user is not informed that these values can be changed in the settings. Adding a message, such as a tooltip when the user hovers over the Target, informing them about the ability to customize the anonymity set in the settings, would enhance learnability.

To enqueue the coins, the user enters the wallet's password and clicks the "Enqueue Selected Coins" button, achieving mapping. After enqueuing, a status column is added, displaying "queued" in front of the selected coins, providing feedback to the user. As the coin (transaction input) gets registered, the status changes to "registered." At the bottom right of the page, the user can observe the number of registered peers and the remaining time for input registration, achieving visibility. However, it is important to clarify that a CoinJoin is only created if either the minimum number of peers or the

minimum time requirement is met, as this mapping is currently missing. Adding a clear message to inform the user about these conditions would provide valuable guidance.

During the CoinJoin process, the user should keep the wallet open until the completion of the CoinJoin rounds. The status of the coin changes to "Connection confirmed," "Output registered," and "Signed" once the required peers are registered, providing feedback to the user. The mixed coins resulting from the CoinJoin are listed in both the "CoinJoin" and "Send" tabs. The privacy level (anonymity set) and cluster labels are displayed alongside the coins in these tabs, achieving visibility. However, the concept of cluster labels and how they relate to tracing coins in the blockchain may be too technical for novice users.

It is worth noting that the CoinJoin amount in Wasabi Wallet is at the time of our research set to 0.104 BTC on the mainnet and 0.0001 on the testnet. For users with a large number of coins or those selecting larger anonymity sets, the creation of CoinJoin transactions may result in longer wait times as the wallet performs the process repeatedly. This automatic repetition can lead to significant delays. Users need to be aware that they not only have to wait for at least one confirmation for each transaction, clearly indicated by a label in front of the coins, but also for the minimum number of peers required to create the next CoinJoin. In cases where a peer leaves the wallet or the user experiences interruptions in the internet or Tor connection, or shuts down their computer during the CoinJoin creation, the affected coin is subject to a ban for a specific time [165], further adding to the delay. To clarify the ban to users, specific reasons for the ban should be provided in the ban message. Additionally, including the time zone when specifying the ban duration would improve clarity.

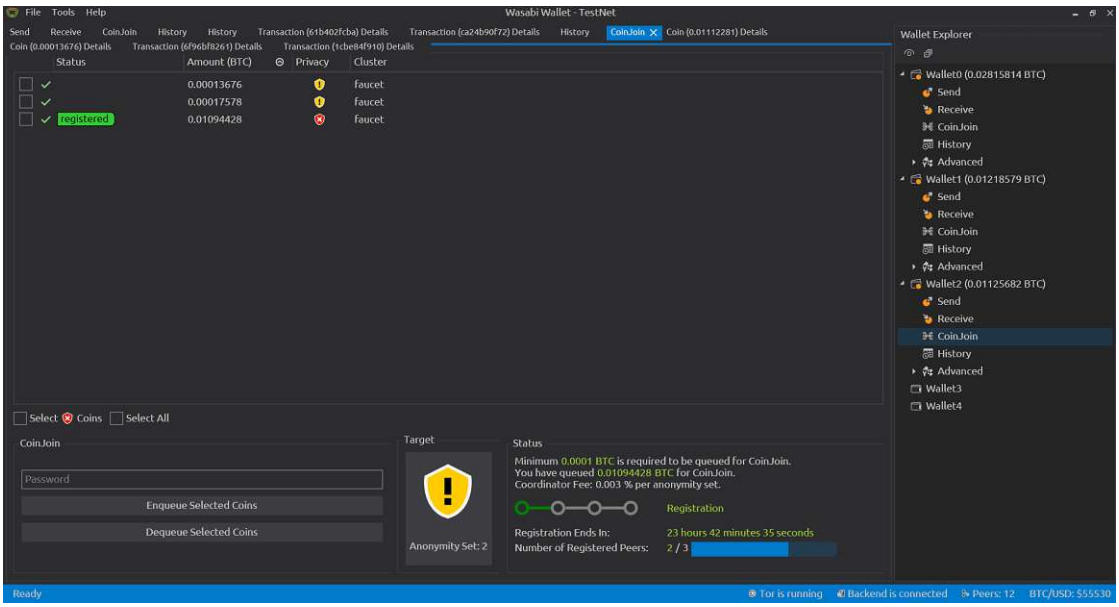


Figure 6.3: Wasabi CoinJoin

Errors: There is an issue in Wasabi Wallet where users can inadvertently close the wallet during multiple rounds of CoinJoin, resulting in a loss of CoinJoin participation in subsequent rounds. This issue fails to provide appropriate feedback to the user and lacks a warning mechanism to prevent such unintended actions.

To address this issue, it is recommended to implement a warning system that alerts users when they attempt to close the wallet during multiple rounds of CoinJoin. Currently, the wallet only provides a warning if the user closes the wallet after input registration and before signing the CoinJoin. In this scenario, the wallet asks the user to be patient and wait for the completion of the created CoinJoin transaction, restricting the user from leaving or closing the wallet until the process is finished. While this achieves feedback, it does not cover the situation where users close the wallet during multiple rounds of CoinJoin.

To improve the feedback and prevent users from inadvertently closing the wallet during multiple rounds of CoinJoin, a warning message should be displayed whenever users attempt to close the wallet while CoinJoin is in progress. This warning should clearly explain the consequences of closing the wallet, emphasizing that it will result in the loss of CoinJoin participation in subsequent rounds. By implementing this warning mechanism, users will be alerted to the potential impact of their actions and can make informed decisions about whether to proceed with closing the wallet or wait for the CoinJoin process to complete.

T.5 Transferring CoinJoin coins.

Learnability: In the "Send" tab of Wasabi Wallet, all coins, including both CoinJoin coins and non-CoinJoin coins, are conveniently listed (achieves visibility). To initiate a transaction, the user can easily follow the process of selecting the coin she wishes to spend, entering the destination address, amount, label, and wallet password, and then clicking the "Send Transaction" button. This user interface is straightforward, ensuring ease of use and fulfilling the constraints and mapping principles.

The inclusion of the "Max" button is particularly beneficial as it calculates and displays the maximum amount that can be spent while accounting for the transaction fee. This feature eliminates the need for manual calculation if the user intends to spend the entire balance of the selected coins. Furthermore, it is essential to emphasize to the user the importance of filling out the label field associated with the destination address. Placing an informative message near the label field when the cursor is hovered over it can help guide the user in providing relevant information. Finally, once the transaction has been broadcasted, the user is promptly informed, providing effective feedback.

Errors: An issue arises when a user selects both CoinJoin coins and non-CoinJoin coins for spending in the same transaction. While the wallet displays a warning message indicating that "Merging unmixed coins with mixed coins undoes the mixes," it allows the user to proceed with merging the coins regardless of the warning. This behavior fails to enforce the intended feedback and control mechanism.

Moreover, if a user selects all of their CoinJoin coins as inputs for a single transaction, they can unintentionally merge all of these coins together without receiving any warning. Unfortunately, this can compromise privacy due to the "common input ownership" heuristic. To mitigate this risk, it is recommended to implement a more robust feedback mechanism. Specifically, before allowing the user to merge all their CoinJoin coins into a single transaction, a warning and confirmation message should be displayed, ensuring that the user is aware of the potential privacy implications. By incorporating this additional layer of feedback, users can make informed decisions and avoid unintentional loss of privacy.

6.5.3 Samourai Wallet

We tested Samourai .apk package version 0.99.96f on Android 5.1.1, Android 10, and Bluestack.

T.1 Installing the application.

Learnability: The installation process of the wallet application primarily occurs on the Android platform, and users can choose from three installation methods: Android .apk package, Google Play, and F-Droid. These installation packages are readily accessible on the downloads tab of the Samourai website, ensuring visibility and ease of access for users.

Currently, the installation via .apk package offers users the option to select either the mainnet or testnet during installation. On the other hand, installing the wallet from Google Play only provides the mainnet version, without the ability to switch to the testnet. The installation process itself is straightforward, with users simply needing to press the install button on Google Play or download the .apk package and install it manually.

Errors: During the installation via the .apk file for the first time, users are required to choose between the "testnet" or "mainnet" options. This decision can be confusing for novice users who may not fully understand the distinction between the two networks. As a result, there is a risk of users inadvertently sending a testnet address to a malicious seller, potentially leading to significant issues. To mitigate this confusion, it is recommended to set the default network to mainnet and provide the option to switch to testnet through advanced settings within the application's menu. Furthermore, the wallet should include a warning message when the user is operating on the testnet to ensure awareness of the network being used.

The installation process itself remains simple, allowing users to install the wallet effortlessly by pressing the install button on Google Play or downloading the .apk package from the Samourai website (achieves visibility).

T.2 Generating a wallet.

Learnability: The process of generating a wallet begins by tapping on the "Create Wallet" button, which becomes visible when the wallet is opened for the first time,

ensuring its visibility and adherence to constraints. The user is then prompted to enter a passphrase, which should be done twice to minimize the risk of errors. To enhance the user experience and reduce the chances of mistakes, it is recommended to include a "show character" icon that allows the user to view the passphrase as they enter it.

Moving to the next page, the user is required to create a PIN code and confirm it by re-entering the PIN. This step adds an additional layer of security to the wallet. On the final page of the wallet generation process, a set of twelve recovery words is displayed to the user. It is crucial to emphasize the importance of writing down these recovery words and storing them securely. To ensure accuracy in recording the recovery words, it is recommended to include a prompt for the user to enter the twelve recovery words once again. Additionally, it is essential to inform the user that the order of the recovery words is critical for wallet recovery. To address this, a message indicating the significance of the recovery word order should be added to the first page of the wallet generation process. This early notification ensures that users are aware of this requirement from the outset, preventing potential issues in the future. Once the wallet is successfully generated, the main page of the wallet is displayed, providing the necessary mapping for the user.

Errors: To mitigate the risk of user errors and ensure the accuracy of the recovery words, it is suggested to incorporate a step where the user is prompted to enter the twelve recovery words. This additional verification process provides assurance that the user has recorded the correct recovery words. Moreover, it is essential to explicitly inform the user that the order of the recovery words is of utmost importance. This clarification is crucial as the current version may lead to critical problems for novice or careless users who could potentially lose their funds permanently if they cannot recover their wallets due to a misplacement or misordering of the recovery words. By emphasizing the significance of both the recovery words and their order, users can better understand and adhere to the necessary precautions for wallet recovery, reducing the risk of irreversible loss.

T.3 Funding the wallet

Learnability: To fund the wallet, the user needs to locate and tap the plus button at the bottom right of the interface, which reveals various wallet functions, including the "Receive" option. However, the visibility of the "Receive" button on the main page is inadequate, creating difficulties for users to locate it easily (fails visibility). To address this issue, it is recommended to display all the functions associated with the plus button on the user's initial interaction with the app. This enhancement ensures that users can promptly access the desired functions without any confusion. Upon tapping the "Receive" button, a page is presented, displaying the wallet's address as both text and a QR code, allowing for seamless transactions (achieves mapping).

By pressing the advanced button, users gain access to additional options, enabling them to specify the requested amount, change the address type, and access information about the key path. This approach effectively prevents novice users from becoming overwhelmed by unnecessary details. To enable address copying, a message alerting the user about the potential visibility of the copied address to other applications is displayed. However,

the message fails to provide a clear solution to this alert. To address this, it could be suggested that users utilize QR code scanning as an alternative method, offering them a secure way to share their address information.

Once the wallet's address is successfully funded, the balance is updated, and the incoming transaction amount is displayed on the main page of the wallet (achieves feedback). Incoming transactions are indicated in green, while outgoing transactions are shown in white. Clicking on the transaction amount provides users with access to transaction details such as the date, time, status (number of confirmations), miner fee rate, miner fee paid, and transaction ID. Furthermore, clicking on the icon located in the top right corner redirects the user to the Blockstream.com website, where they can verify the transaction's status using the block explorer. However, the presentation of the block explorer is unclear unless the user taps on the icon, resulting in a failure to achieve proper mapping. To improve this, it is suggested to include a clear tag such as "Checking transaction status" alongside other items in the transaction details, providing users with a more explicit indication of the purpose of the icon.

The wallet's main page can be refreshed by pulling down the page to obtain the latest transaction status. However, this functionality is not explicitly communicated to the user, leading to a lack of visibility. Adding a visible refresh icon would effectively address this issue, making the feature more discoverable.

Errors: On the transaction detail page, at the bottom, there is a "Boost transaction fee" button that allows the user to increase the fee to expedite confirmation. However, if the user remains on this page and clicks the button after the transaction has already received confirmation, an error message stating "No value for address" is displayed, which is not clear to the user (fails feedback). To improve this, it is recommended to provide a more user-friendly error message that clearly communicates the situation, such as "Transaction already confirmed" or "No action needed, transaction already confirmed." Additionally, if the user refreshes the page, the button disappears, and the confirmation status is shown, which should be communicated to the user.

The status in the transaction details indicates the number of confirmations out of three. However, when the transaction reaches a 3/3 confirmation status, it remains labeled as "unconfirmed," which can be confusing for users, as a total of four confirmations is required to consider a transaction confirmed (fails mapping). To address this, it is recommended to update the status label to reflect the accurate number of confirmations.

T.4 Performing a CoinJoin transaction.

Learnability: To initiate a CoinJoin transaction, the user is required to tap the plus button on the main page and select "Whirlpool." However, the term "Whirlpool" differs from the commonly used terminology "CoinJoin" for the protocol, which creates confusion regarding its purpose (fails mapping). To enhance learnability, it is recommended to clarify that selecting "Whirlpool" enables users to create CoinJoin transactions.

Upon selecting "Whirlpool," a new page opens, and the user should click on the Whirlpool

icon located at the bottom right. On the subsequent page, two options are presented: “Mix coins” and “Spend mixed coins” (fails consistency). To establish a consistent user experience, it is suggested to incorporate these options within the wallet’s main page using appropriate icons, such as a plus button that encompasses these functions.

The term “UTXO” may be too technical for novice users, and it would be beneficial to replace it with more user-friendly terms such as “coins” or “bitcoin.” Additionally, the presence of multiple terminologies for the same concept, including “Mix,” “CoinJoin,” and “Whirlpool,” can lead to confusion. Standardizing the terminology would enhance user understanding of the wallet functions.

By selecting “Mix coins,” the user is directed to a new page (Fig. 6.4) where they can choose the coins they want to include in the CoinJoin process (achieves constraints). The next page displays three options for cycle priority: “low,” “normal,” and “high.” However, the term “cycle” lacks clear explanation, leaving users uncertain about its meaning (fails mapping). To address this, it is recommended to provide a brief description or tooltip clarifying the purpose of the cycle options.

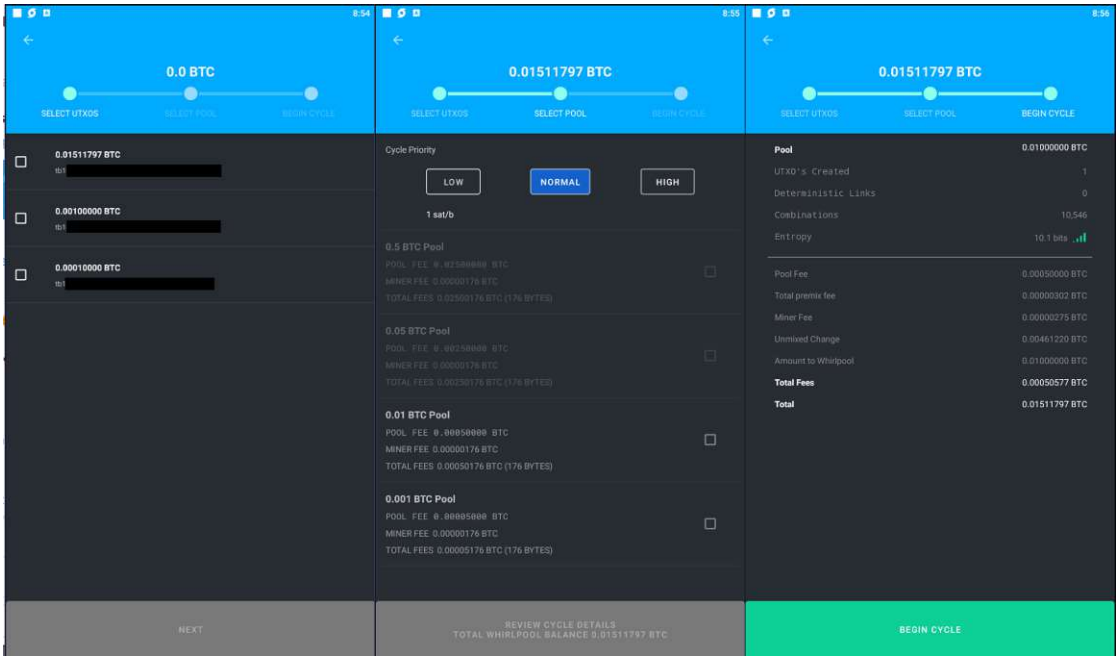


Figure 6.4: Samourai CoinJoin

The user should then select one of the listed pools (achieves visibility) (Fig. 6.4). The available pools are determined based on the user’s previously selected amount, preventing entry into larger pools (achieves constraints). The pool fee, miner fee, and total fee are displayed. Upon pressing “Review Cycle,” the details of the CoinJoin transaction are presented (achieves mapping). However, certain items may still be unclear to novice users, such as “UTXOs created,” which refers to the number of newly created UTXOs or coins

(e.g., if a user selects 0.8 bitcoin and enters a 0.1 pool, they receive eight new UTXOs, each containing 0.1 bitcoin). Similarly, terms like "Deterministic links," "Combinations," and "Entropy" are technical and require further explanation to facilitate user comprehension.

Subsequently, the fees, change, and amount to be Whirlpooled are shown, and the user is required to press the "begin cycle" button to join the pool (achieves visibility). The user is also prompted to select "Doxxic change," allowing them to mark the change as non-spendable to mitigate the risk of being tagged. A message informs the user that even if they make the change non-spendable, it will still appear in the list of unspent transactions. However, the message fails to provide information about the location of this unspent transaction list (fails feedback). Currently, it is accessible through the top-right menu on the wallet's main page. Clarifying the location of the unspent transaction list would address this issue. By selecting "yes" and refreshing the Whirlpool page, all the coins are listed as "Unmixed". The amount and "Mix 1/5-Queued" tag are indicated in front of each coin.

When a new transaction is created on the wallet's main page, the selected amount to be mixed, along with the fees, is deducted from the wallet as an outgoing transaction. This deduction represents the user's contribution to the CoinJoin process. Simultaneously, the first UTXO associated with the transaction in the Whirlpool page should change its status to "Mix 1/5-Joined a mix" once it is successfully added to the pool. However, during testing on the testnet, we encountered a bug where the status failed to update even after six days, without any indication of the underlying problem (fails feedback). In an attempt to resolve this issue, we created additional wallets on different devices to join the same pool, but the status remained stuck at "Mix 1/5-Joined a mix" across all wallets. This bug was also reported by others in [166].

Once the coins enter the Whirlpool, the corresponding amount is transferred from the user's main wallet balance to the Whirlpool balance. This transfer signifies that the funds are now part of the CoinJoin process. Similarly, when the mixing process is completed, the amount is transferred from the Whirlpool balance to the post-mix wallet balance, reflecting the user's ownership of the mixed coins.

However, the current approach of checking different balances across various wallets can be confusing for users who prefer to view their total balance (fails visibility). To address this, it is recommended to prominently display all balances associated with their respective wallets on the main page. This could include the main wallet balance, Whirlpool balance, post-mix wallet balance, and any other relevant balances, providing users with a comprehensive overview of their funds.

Furthermore, the existing method of switching between wallets lacks clarity, causing difficulties in accessing the desired wallets (fails visibility). To improve user experience, it is advisable to implement a more straightforward and intuitive mechanism for navigating between wallets. This could involve incorporating a dedicated wallet selection feature or a clear and easily accessible menu that allows users to switch between different wallets seamlessly.

Errors: During our testnet walkthrough, we observed that selecting different cycle priorities did not result in any change in the amount displayed under this option. Regardless of the chosen priority, the displayed amount remained constant, which indicates a failure in mapping the selected priority to the corresponding fee (fails mapping). This inconsistency in the user interface could lead to confusion and misinterpretation of the actual fee associated with each priority level.

Furthermore, we discovered a significant issue during our testing where one of the UTXOs failed to appear in the unmixed list even after six days. Despite this missing UTXO, the Whirlpool balance and pre-mix balance accurately reflected the sum of the coins, including the amount associated with the hidden UTXO. This behavior indicates a bug in the system that needs to be addressed promptly to ensure the accuracy and integrity of the user's funds.

An additional critical problem we encountered while using Samourai was the inability to abort the CoinJoin process and access our coins. Once the mixing process has started, there is no provision or option available to interrupt or cancel the CoinJoin transaction and regain control over the coins (fails feedback). This limitation can be frustrating for users who may urgently need to utilize their funds or change their course of action. Introducing a feature that allows users to abort the CoinJoin process and reclaim their coins would enhance the flexibility and user control within the wallet.

T.5 Transferring CoinJoin coins.

Learnability: Unfortunately, we were unable to complete this task as we were unable to receive CoinJoin coins. However, we can provide an overview of the process involved in spending the mixed coins. To initiate a transfer of CoinJoin coins, the user is required to access the post-mix wallet. This can be achieved by either selecting the Samourai icon on the main page or the Whirlpool icon on the Whirlpool page. However, it should be noted that neither of these options is clearly visible, indicating a visibility issue (fails visibility). Once in the post-mix wallet, the user can proceed to fill out the destination address and the desired amount before clicking the "Review the transaction" button, which allows them to review the transaction details and ensure accuracy (achieves mapping).

It is important to note that the process of sending coins from the post-mix wallet is similar to spending coins from the main wallet, ensuring consistency in the wallet's functionality (achieves consistency). Once the user has reviewed the transaction and is ready to proceed, they can tap the send button to create, sign, and broadcast the transaction. This information is displayed on the page, providing the user with feedback on the progress of the transaction (achieves feedback). Additionally, the wallet offers privacy add-ons such as "Ricochet: additional hops between wallet and destination" and "Cahoot: create on-demand CoinJoin." Each add-on is accompanied by a description of its functionality. However, inconsistencies arise when the wallet uses different terminologies for the same concept. For example, "Whirlpool" and "mix UTXOs" are used to describe CoinJoin, but it is unclear whether they all refer to the CoinJoin protocol (fails mapping). This inconsistency can lead to confusion and hinder the user's understanding of the

underlying processes involved.

Errors: During our evaluation, we encountered an error in the send page of the wallet. On this page, the user has the option to select all the available coins as the transaction amount. However, at this stage, transaction fees are not deducted from the selected amount. It is only on the subsequent page that the fees are deducted based on the user-selected fee rate, and the actual amount that will be sent to the destination is displayed as a message. If the user fails to read this message carefully, they may mistakenly believe that the sent amount corresponds to the initial amount entered on the first page. To address this issue, we recommend deducting the minimum fee from the maximum amount displayed on the first step. This modification would provide clearer information to the user regarding the deducted fees and the actual amount that will be sent.

6.6 Walkthrough Discussion

In this section, we will discuss the usability aspects of CoinJoin Wallets based on our walkthrough experience.

Wasabi is considered user-friendly due to its ease of installation and well-structured documentation. The documentation provided by Wasabi includes explanations at different levels, catering to both beginners and advanced users. It effectively describes all the necessary steps, workflows, and best practices involved in using the wallet. Compared to other wallets, Wasabi's interface is intuitive and user-friendly. A notable feature of Wasabi is its ability to create CoinJoin transactions with a relatively large number of input peers, up to 100. This enhances privacy by increasing the anonymity set.

However, a limitation of Wasabi is its tendency to create numerous small coins when conducting CoinJoin transactions. This is primarily due to the pool amount being set to a fixed value that cannot be adjusted by users. Consequently, when a user intends to send a large amount to a destination address, they face two options: either merging all the small coins together or spending the coins individually. Merging the small coins can lead to privacy concerns due to the "common input ownership" heuristic, while spending the coins individually requires creating a significant number of separate transactions. This limitation can impact both usability and privacy aspects of the wallet. It is worth noting that this limitation is not unique to Wasabi but is also observed in Samourai Wallet. In contrast, JoinMarket allows users to CoinJoin the entire amount, which provides greater flexibility and convenience.

JoinMarket's configuration can be challenging for non-technical users, requiring them to consult the documentation and search the internet for assistance when encountering errors. The error messages may not always provide clear guidance on how to resolve the issues. This aspect of JoinMarket's usability indicates that it may require a higher level of technical knowledge and familiarity with the platform.

Despite these challenges, JoinMarket offers distinctive features that set it apart from Wasabi and Samourai. One notable advantage is the ability for users to modify settings

related to fees and the number of counterparties involved in the CoinJoin process. This flexibility allows users to customize their transactions according to their preferences and requirements, providing them with greater control over the CoinJoin process.

JoinMarket also provides two essential features that are not found in the other wallets. Firstly, users can specify the desired amount for CoinJoin without being limited to a specific pool size.

Secondly, JoinMarket allows users to directly send the mixed coins to the destination address instead of sending them back to the user's address and then creating another transaction to send the CoinJoin coins to the destination. This streamlined process eliminates the need for an additional transaction, resulting in one less transaction fee compared to the other wallets.

Samourai provides a straightforward installation process and offers a satisfactory experience as a regular wallet. However, there are certain limitations and usability issues that need to be addressed.

One notable limitation of Samourai is its availability exclusively for Android devices. This platform restriction may limit its accessibility for users who prefer or primarily use other operating systems, such as iOS or desktop platforms. Expanding the availability of Samourai to different platforms could enhance its usability and reach a wider user base.

In terms of wallet interface, Samourai faces visibility challenges. The functions and features of the wallet are not prominently displayed or easily discoverable, which may lead to confusion and difficulty in understanding the wallet's capabilities. Additionally, the terminology used in the wallet interface differs from the commonly used terms in the community. This discrepancy in terminology can create a barrier for users who are already familiar with standard terminologies, hindering their ease of use and comprehension.

Creating a CoinJoin transaction with Samourai can be somewhat difficult. Users may encounter difficulties in understanding the status of their CoinJoin process and may not receive clear information about why a CoinJoin is stuck or delayed. Lack of feedback or informative messages regarding the CoinJoin status can be frustrating for users and may cause uncertainty and confusion. Providing transparent and informative feedback about the CoinJoin process can greatly enhance the user experience and improve the usability of Samourai.

Another aspect that affects the usability of Samourai is the inability to abort a CoinJoin process and spend the coins in separate transactions. Users may encounter situations where they need to access their coins immediately or use them for different purposes.

The findings of our research highlight a significant challenge for novice users in effectively utilizing the mixing services provided by CoinJoin wallets. Despite the utilities offered by these wallets, it can be cumbersome for inexperienced users to navigate the complexities of using their mixing services correctly. It requires users to not only have a basic understanding of the CoinJoin protocol but also be cautious about undoing the mix inadvertently by spending the CoinJoin UTXOs as inputs of a single transaction.

During our investigation, we encountered instances where users demonstrated a misconception about spending the CoinJoin UTXOs as inputs for a single transaction, potentially compromising the privacy and anonymity benefits provided by CoinJoin. This misconception was also evident in the chat support of one of the wallets [1], indicating that it is a common point of confusion among users.

6.7 Small-Scale Usability Test of Three CoinJoin Wallets

To assess the usability of three CoinJoin wallets, namely Wasabi, JoinMarket, and Samourai, we conducted a small-scale user study with a sample size of two participants. The selected users were individuals with a background in information technology security and privacy, and they possessed prior knowledge and experience with cryptocurrency wallets. The aim of this study was to evaluate the success rate and completion time of specific tasks assigned to the participants. The results of the study are summarized in Table 6.2.

Both users (U1 and U2) successfully completed all tasks using the Wasabi wallet. However, it should be noted that both users required a second attempt in Task 4 (T.4) to complete the CoinJoin process successfully. The primary reason for their initial failure was attributed to the ambiguous interface and insufficient information provided regarding the requirement for participating users to create a CoinJoin.

User 1 (U1) encountered some confusion while using the CoinJoin interface in the Wasabi wallet, they faced difficulties related to the liquidity of the testnet, which hindered their ability to create a CoinJoin with other participants. Despite these challenges, U1 managed to complete the tasks after the second attempt in T.4.

User 2 (U2) displayed impatience during the CoinJoin process, as they were not willing to wait for a sufficient number of peers. The combination of waiting for confirmation status and the information regarding the end of registration for CoinJoin participants led to confusion for U2, ultimately resulting in their initial failure in T.4.

In the case of JoinMarket, U1 encountered various errors, such as “error pushing (trx fees)” and difficulties in reducing the number of counterparties. These issues contributed to their failure in completing the assigned task during their first attempt. On the other hand, U2 was unable to complete the tasks in JoinMarket due to a security measure on their Windows 10 system, which flagged the .exe file as malicious.

In the Samourai testnet, both users encountered a similar problem. They reported being stuck at the “Mix 1/5-Joined a mix” status for several days without any further progress, leading to their inability to complete T.4.

The small-scale usability test revealed several usability issues and challenges in the evaluated CoinJoin wallets. Wasabi exhibited usability concerns related to its interface

[1] https://t.me/WasabiWallet/65300

design and lack of clear instructions for joining participants in the CoinJoin process. JoinMarket demonstrated issues such as error messages and installation difficulty. Samourai suffered from a significant problem where users were unable to proceed beyond the "Mix 1/5-Joined a mix" status. These findings highlight areas that require improvement to enhance the user experience and usability of these CoinJoin wallets and support the findings in our walkthrough.

Table 6.2: Users' Task Success and Time on Task in Minutes (m)

	Wasabi		**JoinMarket**		**Samourai**	
	U1	U2	U1	U2	U1	U2
OS	Ubuntu 18.04.5 LTS	Windows 10	Ubuntu 18.04.5 LTS	Windows 10	Android 10	Android 8
T.1 Installing the application.	✓ 4m	✓ 6m	✓ 13m	X	✓ 2m	✓ 5m
T.2 Generating a Wallet.	✓ 1m	✓ 2m	✓ 3m	X	✓ 2m	✓ 5m
T.3 Funding the wallet.	✓ 8m	✓ 4m	✓ 3m	X	✓ 2m	✓ 3m
T.4 Performing a CoinJoin transaction.	✓ several hours	✓ 90m	✓ 30m	X	X	X
T.5 Transferring CoinJoin coins to destination.	✓ 1m<	✓ 5m	*	*	X	X

✓: Success on the first attempt ✓: Success in the second attempt X: No success
*T.5 in JoinMarket can be conducted in T.4.

6.8 Wallet Issues and Possible Improvements

We provided issues reported by authors and the experts from small-scale study and suggested possible improvements in Table 6.3 to Table 6.15.

Table 6.3: JoinMarket wallet task 1 issues and possible improvements

Issue	**Reporter**	**Possible Improvement**
T.1 Installing the application.		
Novice users may find it confusing to select the correct assets to download based on their operating system.	Authors	Provide clear and easily identifiable download buttons for each operating system.
The instructions for wallet configuration that refer to different parts are confusing.	Authors	Consolidating all Bitcoin core configuration instructions into a single guide and referencing it whenever necessary.
Windows is blocking the app from running.	Authors U2	Include clear instructions in the installation guide for Windows users. Provide information on how to verify the authenticity of the installation file.

Table 6.4: JoinMarket wallet task 2 issues and possible improvements

Issue	**Reporter**	**Possible Improvement**
T.2 Generating a Wallet.		
The backup process is not questioned, leaving users unsure whether they actually wrote down the backup phrase.	Authors	Ask for the password and backup phrase in the correct order.
Lack of information regarding the importance of the order of recovery words in a wallet recovery process.	Authors	Ask for the password and backup phrase in the correct order.

Table 6.5: JoinMarket wallet task 3 issues and possible improvements

Issue	Reporter	Possible Improvement
T.3 Funding the wallet.		
Difficulty in finding the button to generate a new receive address in the wallet. It was not clear that the receive addresses are automatically generated, which caused confusion and took some time to figure out.	Authors U1	Update the user interface to make it clearer that receive addresses are automatically generated.
There is no notification displayed when funds are received in the wallet. The funds are updated but there is no message shown to inform the user.	Authors U1	Provide a notification.
The term "mixdepth" in the address tab may be confusing for novice users.	Authors	Provide a brief description or explanation of what it means in a language that is easy to understand. Add a tooltip or a help icon next to the term.

Table 6.6: JoinMarket wallet task 4 issues and possible improvements

Issue	Reporter	Possible Improvement
T.4 Performing a CoinJoin transaction.		
The current QT presentation does not provide information about the inability to spend coins from different mixdepths in a single transaction.	Authors	Provide a brief notification.
The technical messages in the QT box cannot be easily understood by novice users, which can cause confusion and difficulty in troubleshooting issues.	Authors	Provide contextual help or tooltip messages that explain technical terms and concepts in a user-friendly way. Error messages can be written in plain language and presented with clear instructions on how to resolve the issue. The wallet can also provide links to relevant documentation or support resources for users who need additional assistance.
When a user selects to spend the entire amount of a mixdepth, QT does not clearly indicate that the user should enter zero as the amount.	Authors	A clear instruction should be added to the QT interface to guide the user on how to spend the entire amount of a mixdepth.
If the user tries to spend coins that have less than five confirmations, the transaction is automatically aborted. This can be confusing for users who may not understand the reason for the transaction failure.	Authors	The wallet can display a message informing the user that the transaction cannot be completed due to the low number of confirmations. Coins with fewer than five confirmations can be grayed out or marked as unavailable for spending until they reach the required number of confirmations.
If the user is not available once a maker is found, she may eventually miss the CoinJoin creation.	Authors	The wallet can automatically create the CoinJoin.
The user encountered several errors, including errors related to transaction fees and having to reduce the number of counterparties.	Authors U1	Make a guide on how to handle the errors.
The transaction history in the running QT on Windows does not contain the incoming transactions, which can cause confusion and difficulty in tracking transactions.	Authors	Include all incoming transactions in the transaction history.

Table 6.7: Wasabi wallet task 1 issues and possible improvements

Issue	Reporter	Possible Improvement
T.1 Installing the application.		
Uncertainty about whether users would understand why the first tab in the wallet is labeled "files," since it seems to primarily pertain to the wallet itself.	U2	Use a meaningful name for the tab.

Table 6.8: Wasabi wallet task 2 issues and possible improvements

Issue	Reporter	Possible Improvement
T.2 Generating a Wallet.		
The backup process is not questioned, leaving users unsure whether they actually wrote down the backup phrase. Additionally, the password is only questioned once during setup, without any confirmation step, which could lead to errors if the user misspelled their password.	Authors U2	Ask for the password and backup phrase in the correct order.
Lack of information regarding the importance of the order of recovery words in a wallet recovery process. Users may not be aware that the sequence of words must be entered in the correct order for the recovery process to succeed, which can lead to frustration and confusion if they try to recover their wallet and fail due to incorrect word order.	Authors	Ask for the password and backup phrase in the correct order.
Lack of clarity regarding address labeling in a wallet. Users may not be sure if the labels they assign to addresses are related to the party that sends the coins to that address, which can cause confusion when trying to track transactions or organize their wallets. This ambiguity can lead to labeling errors or incorrect assumptions about the nature of certain transactions.	Authors	Provide a clear explanation of labeling the addresses.
When a user clicks on an address or its label in a wallet, the QR code and other relevant information are not displayed. This lack of functionality can be frustrating for users who may need to quickly access the address or associated information and may lead to errors or delays in transactions if they have to manually enter the address or search for the information elsewhere.	Authors	Add a new button labeled "More Info." When the user clicks on this button, it will expand to show the relevant information, including the QR code, associated transactions, and any other details related to the address.

Table 6.9: Wasabi wallet task 3 issues and possible improvements

Issue	Reporter	Possible Improvement
T.3 Funding the wallet.		
The wallet app does not inform the user about the current network being used, whether it is the mainnet or testnet.	U1	Inform the user clearly about the current network being used and provide options to switch to the appropriate network when necessary.
The wallet app does not make it clear to users whether a generated address is on the mainnet or testnet. This lack of information can be confusing for users, especially those who are new to cryptocurrency and may not understand the difference between the two networks. As a result, users may inadvertently send transactions on the wrong network, leading to failed transactions or lost funds.	U1	Provide clear and prominent information within the app indicating whether a generated address is on the mainnet or testnet. This information could be displayed alongside the address itself or in a separate section of the app
It is not clear to users why there is a feature to generate multiple receive addresses with different labels in the wallet app. While this functionality is described in the documentation, it may not be immediately apparent to users, and they may not understand the purpose or benefits of having multiple labeled addresses.	U2	Provide clear and concise information within the app itself, explaining why users may want to generate multiple receive addresses with different labels and how they can use this feature to manage the privacy of their cryptocurrency more effectively. This information could be presented in a user-friendly way, such as a pop-up or tooltip, to ensure that users are aware of this functionality and can take advantage of it as needed.
It seems unclear what the key path and the public key are for.	Authors U2	Provide clear and concise information to users within the wallet app about the key path and public key, as well as the purpose of each.
Some users may not understand the purpose of the QR code within the wallet app or may not understand how to use it effectively.	U2	Explain how to use the QR code to send and receive cryptocurrency.
If a user funds several addresses within the wallet app, it can be difficult to track the flow of cryptocurrency between these addresses. The user must copy the transaction ID and then use a blockchain explorer to view this information.	Authors	Add a feature that allows users to easily track transactions between their various addresses, or provide a more user-friendly interface for accessing and viewing transaction information.
When a user clicks on a transaction ID within the wallet app to copy it, the selected part only contains the characters that are located before the cursor, and the entire ID is not selected by simple double-clicks.	Authors	The app could be updated to allow for simple double-clicks to select the entire transaction ID.
Once a wallet address is funded, it disappears from the user's address list within the wallet app. This can be problematic for users who want to keep track of their transaction history and monitor the flow of cryptocurrency within their wallets.	Authors	The app could include a pop-up message or notification that appears after a transaction has been submitted, informing the user that they can check the status of the transaction in the transaction history.
While the transaction history tab is open, each time the user clicks on a transaction within the history, they are redirected to the previously opened transaction details page, which may contain outdated information. This can be confusing for users who want to track the status of their transactions in real-time and may lead to incorrect assumptions about the state of their transactions.	Authors	Implement an automatic refresh feature that updates the transaction details page.

Table 6.10: Wasabi wallet task 4 issues and possible improvements

Issue	Reporter	Possible Improvement
T.4 Performing a CoinJoin transaction.		
The CoinJoin interface can be confusing for users, despite receiving notifications about the various states of the CoinJoin process.	U1 U2	Provide users with more detailed instructions and explanations about the registration process, as well as the different states of the CoinJoin process. The app could also include a progress bar or a color-coded status indicator.
The user is not sure what the expected behavior is when selecting "enqueue". Additionally, the status of these options is not clear, and the user is unsure how or if they can influence the status.	U2	Provide more information and clarity around these options and their status.
It is not clear whether the password required for Coinjoin is the same as the one chosen for the wallet.	U2	The instructions should specify the password required for Coin join is the same as the password chosen for the wallet. The wallet could also provide password hints.
The privacy is not clear on what it depends, and the user is not sure what the "Cluster" is referring to.	Authors U2	Provide more information and clarity around these items.
The user is not informed that she is able to change anonymity set.	Authors	Add a clear and prominent button or link labeled "Change Anonymity Set" within the CoinJoin interface.
The user is not notified that the CoinJoin transaction is only created once one of the conditions (minimum peers or minimum time) is met.	Authors	Provide clear and concise information to the user about the CoinJoin creation process.
The current coin ban message lacks specific details or explanations, leaving the user confused about the reason for their "banned" status.	Authors	Provide specific details about why the coin has been banned.
The coin ban message does not specify the time zone of the displayed time.	Authors	Add the time zone.
Closing the wallet during the CoinJoin results in the loss of CoinJoin participation in the next rounds, and no warning is displayed to the user.	Authors	Add a pop-up message asking the user if she really wants to close the wallet while CoinJoin is in progress, and informing her that closing the wallet will result in the loss of CoinJoin participation in the next rounds.

6.9 Usability Test of Wasabi Wallet 1.0

In this subsection, we analyze the user study of the Wasabi wallet involving five participants who participated in a blockchain workshop. The participants in the wallet test had either purchased or already owned cryptocurrency, and had installed a wallet, and demonstrated their proficiency by successfully transferring cryptocurrencies to another address. We chose the Wasabi wallet based on its reputation as the most user-friendly wallet in our small-scale user study and walkthroughs. The participants were given five tasks, including installing the application, generating a wallet, funding the wallet (using a provided faucet link to receive free coins on testnet), performing a CoinJoin transaction, and transferring CoinJoin coins to a destination address. The task sheet that each participant should fill out is included in Appendix 7.3. We also asked them to provide transaction IDs to check that they completed the tasks and ensure the reliability of the reported data.

Table 6.11: Wasabi wallet task 5 issues and possible improvements

Issue	Reporter	Possible Improvement
T.5 Transferring CoinJoin coins to destination.		
The process of sending coins to another address is not user-friendly because the user has to manually type in the recipient address, and using a QR code would be a simpler and less error-prone solution.	U2	Add QR code scanning.
The user is unsure why she needs to enter the password every time she performs a coin registration or spending action.	U2	One solution could be to allow the user to save their password for a certain period of time after entering it once. Another solution could be to provide more information about the security benefits of requiring the password for each action to help the user understand its importance.
The user had trouble finding and setting the options to label observers and choose the transaction fee in the wallet, despite reading about them in the documentation. She also notes that the terminology used in the documentation differs from what she saw in the actual wallet.	U2	Improve the documentation to better reflect the terminology used in the wallet, and provide more detailed instructions on how to find and use the labeling and fee options.
When a user selects both CoinJoin coins and non-CoinJoin coins for spending, a warning message appears that says "Merging unmixed coins with mixed coins undoes the mixes". However, the user can still choose to ignore the warning and merge the coins.	Authors	The wallet could provide the user with an option to separate the CoinJoin and non-CoinJoin coins and spend them separately to avoid undoing the mixes.
When a user selects all of her CoinJoin coins as inputs for a transaction, she can merge them all in one transaction without receiving any warning.	Authors	Add a warning message, informing the user that this action would undo the privacy provided by the CoinJoin process. The warning message could provide alternative solutions or recommendations to maintain privacy, such as selecting only a subset of the CoinJoin coins or waiting for more CoinJoin rounds before spending them.

Table 6.12: Samourai wallet task 1 issues and possible improvements

Issue	Reporter	Possible Improvement
T.1 Installing the application.		
Selecting between "testnet" and "mainnet" via APK may result in some problems for novice users who do not understand the difference between the two networks.	Authors	Add a warning message that explains the implications of selecting the wrong network, such as potentially losing funds or transacting with fake coins. Automatically select the default network to mainnet and provide changing the network to testnet via advanced options.

Table 6.13: Samourai wallet task 2 issues and possible improvements

Issue	Reporter	Possible Improvement
T.2 Generating a Wallet.		
The "testnet" network is not visible in the app.	U2	Clearly indicate the current network (testnet or mainnet) on the interface so that users can easily identify which network they are currently using.
The backup process is not questioned, leaving users unsure whether they actually wrote down the backup phrase.	Authors U2	Ask for the password and backup phrase in the correct order.
Lack of information regarding the importance of the order of recovery words in a wallet recovery process.	Authors	Ask for the password and backup phrase in the correct order.
Users find it unclear what Whirlpool and PayNyms do.	U2	Utilize simple language and visual aids to make it easy for novice users to understand.

Table 6.14: Samourai wallet task 3 issues and possible improvements

Issue	Reporter	Possible Improvement
T.3 Funding the wallet.		
The user is having difficulty finding the "Receive" function to fund the wallet. It is not clearly visible on the main page, and the user had to hit the plus button at the bottom right to access it.	Authors	Add a clear and prominent button or tab on the main page of the wallet specifically labeled "Receive" or "Add funds".
The user cannot determine the amount of the transaction fee, as it is automatically set by the system. This can result in the loss of a significant amount of money, and the user has no control over it.	U2	Provide an option for the user to determine the amount of the transaction fee.
Some lay users may find it difficult to understand the difference between BTC and sats, and the difference between the miner fee rate and the actual miner fee paid, which can cause confusion.	U2	The wallet can provide options for users to switch between BTC and sats when making transactions, and clearly display the miner fee rate and estimated fee, as well as the actual fee paid after the transaction has been processed.
The presentation of the block explorer is not clear to the user unless they click on the icon.	Authors	Provide a brief explanation or tooltip about the block explorer when the user hovers over the icon.
The user is unaware of the feature to refresh the wallet main page by pulling down the page to check the latest status of the transaction.	Authors	Add a refresh button or an automatic refresh feature to make it more convenient for the user to check the transaction status without having to manually refresh the page.
The user encounters an error message ("No value for address") when attempting to boost the transaction fee on a transaction detail page that has already received confirmation. This error message is not clear and may cause confusion for the user.	Authors	The error message should be replaced with a more descriptive message, such as "This transaction has already been confirmed and cannot be boosted."
The status in the transaction details shows the confirmations out of 3, but even if 3/3 confirmations are reached, the status is still shown as unconfirmed.	Authors	The status should accurately reflect the number of confirmations received by the transaction.

Table 6.15: Samourai wallet task 4 issues and possible improvements

Issue	Reporter	Possible Improvement
T.4 Performing a CoinJoin transaction.		
The terminology used in the wallet is confusing, with "Whirlpool", or "Mix" being used to describe a feature that is actually a variation of the "CoinJoin" protocol.	Authors	The wallet should use consistent and clear terminology adopted by the community to avoid confusing users.
The term "UTXO" is technical and may be confusing for novice users.	Authors	Replace the term "UTXO" with a more user-friendly term like "coin" or "bitcoin".

Task 1: Installing the application The participants did not face any difficulties while installing the application. They were able to complete this task with ease, and it did not take much time. In Figure 6.5, the operating systems of the participants are reported. Figure 6.6 and Figure 6.7 illustrate the success and satisfaction of Task 1. Time on task was reported 2.6 minutes on average.

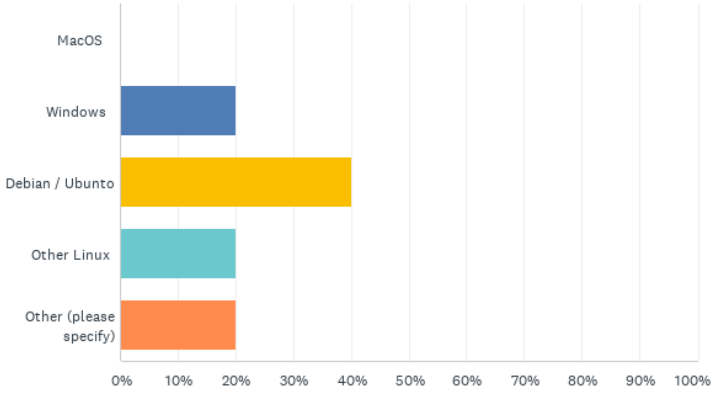


Figure 6.5: Participants' operating systems

Task 2: Generating a wallet The participants found generating the wallet to be easy. All participants could pass the task on the first attempt. However, some of them reported issues during conducting the task. One of the participants mentioned that the generation process took some time and did not show any progress. It was unclear whether the process was stuck or not, but ultimately the process succeeded. Another participant reported that the wallet took some time to load, and initially, they thought it was an error. However, they discovered that they just needed to wait for it to load. Another participant found the application quite confusing. They noted that the wallet address did not show up directly and only appeared after synchronization was complete. They also had to manually restart the application for synchronization to work.

These comments indicate that the usability of the wallet application could be improved by providing more feedback during the generation process, adding a progress bar or

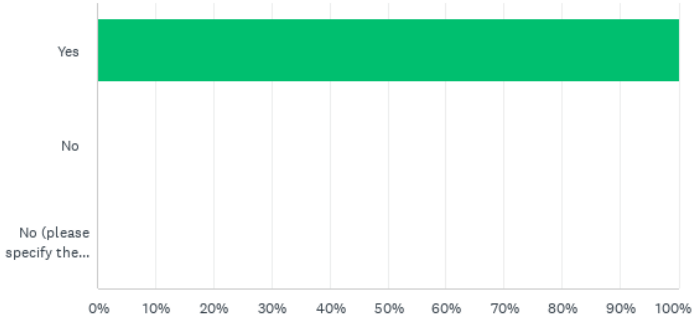


Figure 6.6: Wasabi wallet task 1 success

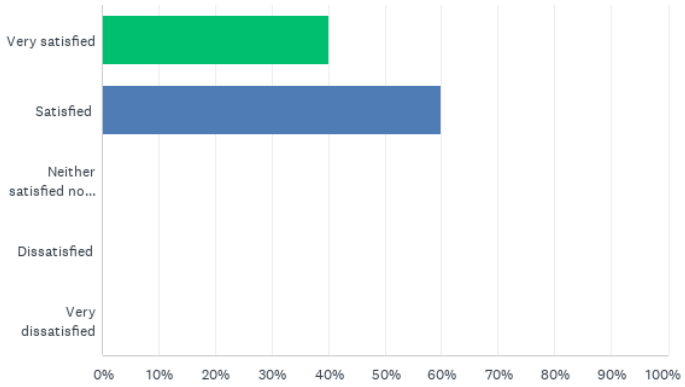


Figure 6.7: Wasabi wallet task 1 satisfaction

indication of loading time, and making the wallet address more visible and accessible. Additionally, the synchronization process should be made more intuitive and less prone to errors.

Figure 6.8 and Figure 6.9 illustrate the success and satisfaction of Task 2. Time on task was reported 1.8 minutes on average.

Task 3: Funding the wallet One participant had some difficulties funding the wallet on the first attempt. They could complete the task on the second attempt. They reported that provided faucet link did not work for them and they had to fund the wallet with a different faucet. Therefore, this failure was not related to the Wasabi wallet. The following are comments from participants regarding the issues while conducting Task 3. A participant reported that the wallet took some time to initialize and they were unsure

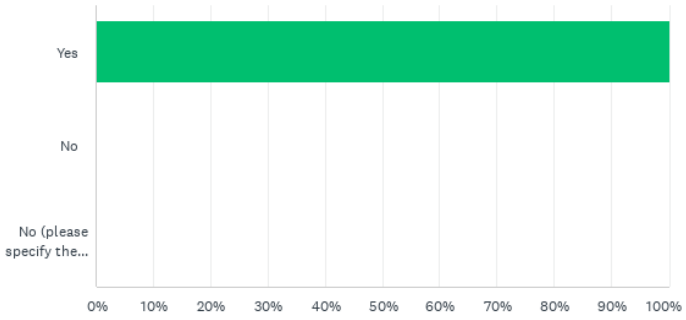


Figure 6.8: Wasabi wallet task 2 success

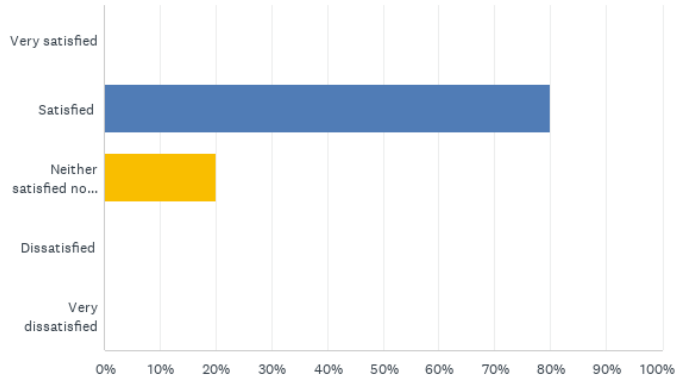


Figure 6.9: Wasabi wallet task 2 satisfaction

if it was stuck or not. The other one mentioned that they needed to restart the wallet.

These comments suggest that the usability of the wallet application could be improved by providing clearer feedback during the initialization process. Additionally, the issue of needing to restart the wallet should be addressed to prevent frustration and potential loss of data.

Figure 6.10 and Figure 6.11illustrate the success and satisfaction of Task 3. Time on task was reported 3.8 minutes on average.

Task 4: Performing a CoinJoin Transaction Before starting the usability test, we provided participants with an explanation of privacy concerns and how CoinJoin works. All participants were able to successfully complete this task. However, one reported difficulty with the UI/UX of the application. We also reminded participants to wait for the completion of the CoinJoin round and avoid confusion.

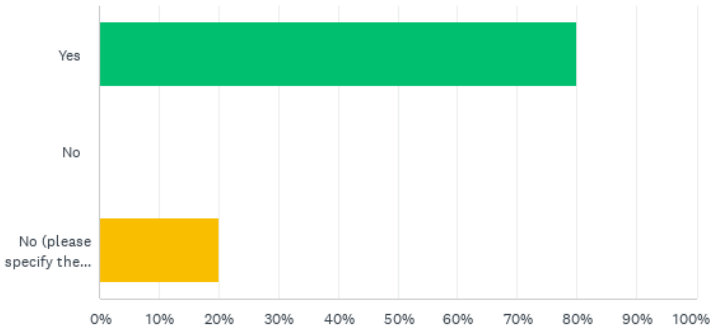


Figure 6.10: Wasabi wallet task 3 success

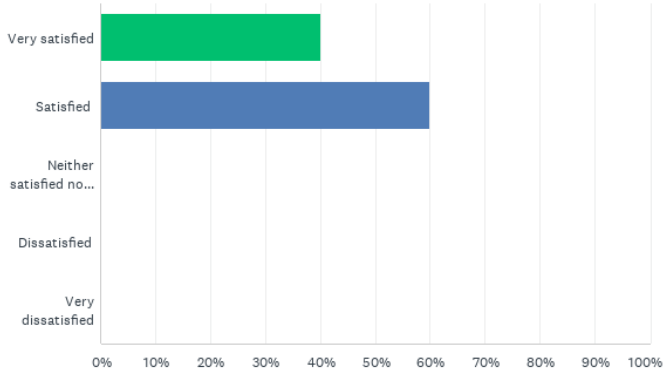


Figure 6.11: Wasabi wallet task 3 satisfaction

Figure 6.12 and Figure 6.13illustrate the success and satisfaction of Task 3. The average time spent on the task was 7.6 minutes.

Task 5: Transferring CoinJoin Coins to the Destination Address The participants found transferring CoinJoin coins to the destination address easy, without any issues. However, some participants encountered problems that developers should consider. One participant reported that the application did not save the addresses used under the "receive" tab, despite having enough space. As a result, they lost the first address they sent the transaction to and had to repeat the process. Although this feature is meant to prevent address reuse, the participant thought that the wallet had a problem by not listing the previous addresses. Another participant faced a similar issue as they could not see their old receive address history, causing them to lose track of their first transaction. The reported issue should be addressed by developers as it was not clear to the participant where to find the history of the address since they expected to see the address under the

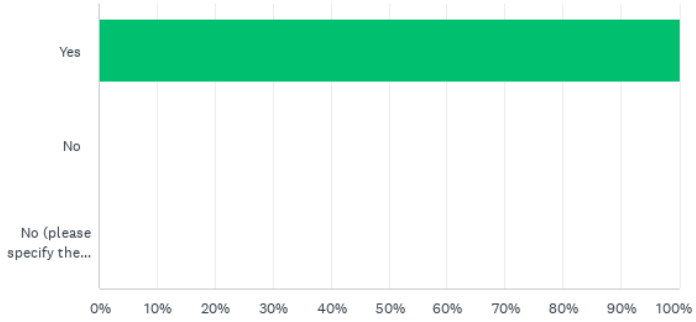


Figure 6.12: Wasabi wallet task 4 success

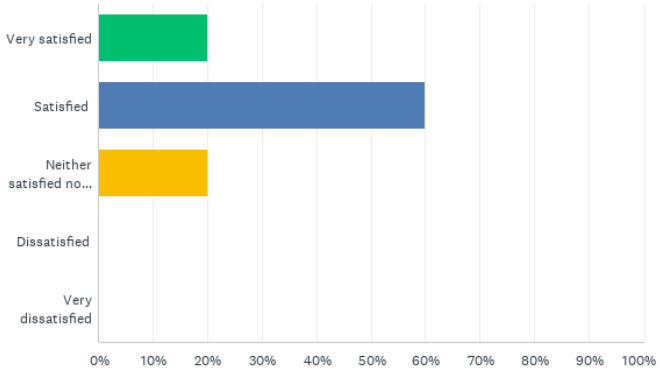


Figure 6.13: Wasabi wallet task 4 satisfaction

receive tab.

These comments suggest that the usability of the "receive" tab could be improved by adding a history feature that saves previously used addresses. This would prevent users from losing track of their transactions and manage their funds more efficiently. However, users should be informed through colors or warnings that they should not use previously used addresses to prevent address reuse and endanger their privacy.

Figure 6.14 and Figure 6.15 illustrate the success and satisfaction of Task 3. Time on task was reported 7.8 minutes on average.

The usability study of the Wasabi wallet showed that the participants found the application to be user-friendly. However, some tasks were found to be more challenging than others. The participants were able to complete all tasks with the help of the brief presentation

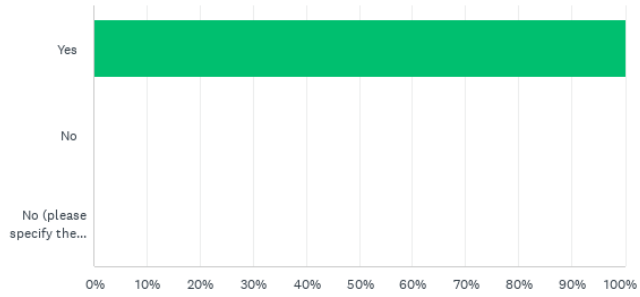


Figure 6.14: Wasabi wallet task 5 success

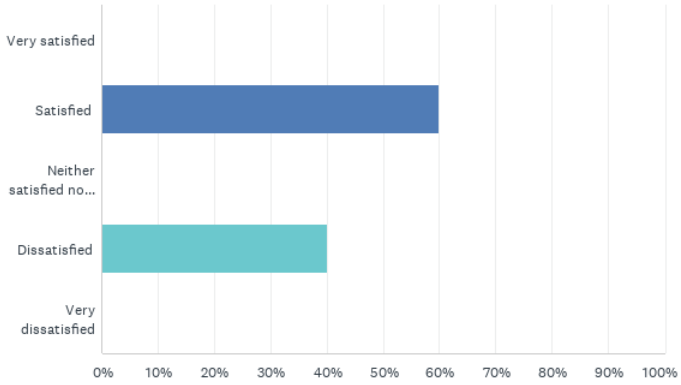


Figure 6.15: Wasabi wallet task 5 satisfaction

and instructions provided. The study also highlighted some areas where the application could be improved, such as simplifying funding the wallet and providing more information on creating CoinJoin transactions.

6.10 Conclusion

Bitcoin transactions are inherently transparent, allowing for potential privacy risks and the possibility of de-anonymization through heuristic analysis. In response to these concerns, various cryptocurrency wallets have been developed, incorporating privacy-preserving techniques such as mixing protocols. However, the practical usability of these privacy features for novice users requires a comprehensive understanding of the underlying concepts and intuitive design.

In this chapter, we conducted a cognitive walkthrough to evaluate the usability of

three prominent wallets that support CoinJoin transactions. Our findings emphasize the need for further improvements to enhance the usability of these wallets for novice users. The user study conducted in parallel with the cognitive walkthrough corroborated our results, revealing the challenges associated with performing CoinJoin transactions, particularly for users lacking a fundamental understanding of the CoinJoin technique. Additionally, issues such as error messages and the merging of previously mixed coins with other UTXOs owned by the same user can compromise the intended mixing benefits, potentially exposing user identities through the "common input ownership" heuristic. An intuitive and informative interface can facilitate novice users in successfully performing CoinJoin transactions and comprehending the associated risks.

One key problem is that using privacy tools requires users to understand the techniques behind them. For example, when using privacy tools, users need to know that merely employing privacy features does not guarantee complete privacy, which can be considered one of the largest gaps between users' perceived privacy and the actual level of privacy.

In our experiment, we asked users to join a Coinjoin pool, perform Coinjoin transactions, and then transfer the resulting coins to a destination address. Surprisingly, some users merged all the coins in one transaction and transferred them to the destination address, thereby reducing their privacy, as the common input ownership heuristic can be applied to their transactions. This misconception was also evident in the chat support of one of the wallets [2], indicating that it is a common point of confusion among users. This misconception aligns with the finding in [74], where users shifted their Bitcoin holdings to a privacy coin such as Zcash in pursuit of enhanced privacy. However, these users failed to achieve heightened anonymity by adopting Zcash. This is evidenced by their utilization of the same address in 54.24% of cases, or by immediately re-transferring the exact same coin received in 28.75% of cases.

To enhance the usability of the privacy achieved by wallets, both users' awareness of the basics of privacy techniques and the responsibility of wallet developers in educating users are essential. However, informing users poses challenges. Even if the wallet warns about privacy issues — for instance, when merging mixed coins in one transaction — users may ignore the messages and proceed with actions that could potentially reduce their privacy. Balancing usability and privacy is tricky for wallet developers, as users desire flexibility in managing their coins. The wallet cannot prevent users from spending the coins if they choose to redo the mixing.

Switching to security concerns, key management poses a significant challenge. Many users lose their coins due to carelessness, such as forgetting mnemonic words or mishandling backups. Wallets should emphasize the importance of mnemonic word order and prevent easy snapshotting to enhance security. While users should possess a basic understanding of key management, developers play an important role in informing users about security features. Without proper guidance, users may inadvertently compromise their security, as evidenced in various studies [51] and real-world examples [167].

[2] https://t.me/WasabiWallet/65300

Overall, we believe transaction basics (addresses, transaction fees, transaction confirmations, etc), differences between blockchains (UTXO-based model, account-based model), using multiple addresses and avoiding using the same address, and coin mixing basics could help users in providing privacy for their transactions. Moreover, understanding the difference between wallet types (software wallets, hardware wallets, web wallets, and paper wallets), and key management basics such as safeguarding mnemonic words and private keys, backing up the keys, using passphrases for wallets, and handling wallet recovery can be considered as the minimum set of knowledge for security in using blockchain wallets.

In our study, the Bitcoin testnet was utilized due to the high fees associated with the mainnet, which may have influenced the observed time on tasks. Furthermore, the inability to execute CoinJoin transactions on the Samourai testnet limited our evaluation. Future research can expand upon our study by including a more diverse user group, encompassing both technical and non-technical users.

To encourage wider adoption of CoinJoin wallets and facilitate their effective use, future work should focus on addressing the identified usability challenges. Improvements in interface design, clearer instructions and feedback, simplified CoinJoin processes, and educational resources can empower novice users to leverage the privacy benefits offered by CoinJoin transactions. By enhancing the usability of these wallets, we can contribute to the broader goal of strengthening user privacy and the adoption of these tools.

In the next chapter, we provide a summary of the significant findings and contributions of the research study. We focus on presenting the key results, conclusions, and recommendations that have emerged from our investigations. We also propose possible future research directions.

CHAPTER 7

Conclusion

7.1 Highlights of Research Contributions

This section provides an overview of the key contributions made in this research, encompassing the analysis of privacy attacks, evaluation of privacy-preserving techniques, investigation of user perceptions and preferences, and the assessment of the usability of wallets supporting CoinJoin transactions.

Firstly, at the 2021 Business Process Management (BPM), Blockchain forum, we presented the classification of privacy attacks into four main categories: heuristics, side-channel attacks, flow analysis, and auxiliary information. By comprehensively understanding these categories, we then conducted an evaluation of privacy attacks on the did:btcr Blockchain application. This initial stage provided insights into the vulnerabilities and privacy risks inherent in the Bitcoin ecosystem.

Secondly, at the 2022 Availability, Reliability, and Security (ARES) conference, we categorized various privacy-preserving techniques into centralized mixers, atomic swaps, CoinJoin-based techniques, and threshold signatures. To compare these techniques, we considered multiple criteria, including privacy, security, efficiency, and real-world adoption. Our findings revealed that CoinSwap and its predecessors offer strong privacy guarantees but require more time and fees. On the other hand, CoinJoin-based techniques are commonly adopted but suffer from transaction distinguishability and denial-of-service (DoS) attacks. Additionally, we highlighted the benefits of PayJoin for enhancing anonymity and ValueShuffle for providing indistinguishability in CoinJoin. We also discussed the challenges associated with identifying illicit transactions and the need for innovative methods to differentiate them from regular mixing transactions.

Thirdly, our investigation of user perception and preferences regarding Bitcoin privacy and various add-on privacy techniques, presented at the FC 2022 Workshop on Coordination of Decentralized Finance (CoDecFin), shed light on user perspectives. The results indicated

that most users favor privacy coins over add-on techniques in Bitcoin and are willing to tolerate delays in order to achieve anonymity without incurring extra fees. Participants also expressed a preference for indistinguishable privacy techniques to avoid being flagged by monitoring tools. The study revealed important questions surrounding the use of current privacy wallets offering CoinJoin transactions with distinguishable outputs, as users who prioritize privacy are unlikely to use Bitcoin and instead prefer built-in privacy features. These findings provide valuable insights into user preferences and expectations regarding Bitcoin privacy.

Finally, to evaluate the usability of wallets supporting CoinJoin transactions, we conducted a cognitive walkthrough presented at the 2022 Symposium on Usable Security and Privacy (USEC). The results highlighted the need for improvements to enhance the user-friendliness of these wallets, particularly for novice users. One identified issue was the merging of previously mixed coins with other user UTXOs, which can compromise the benefits of mixing and potentially reveal user identities. To address this concern, we recommend the design of intuitive and informative interfaces that help users understand the risks associated with specific actions. Such interfaces can empower users to perform CoinJoin transactions more effectively and securely.

In conclusion, this research makes significant contributions to the understanding of privacy attacks and privacy-preserving techniques in Bitcoin, user preferences and expectations related to Bitcoin privacy, and the usability of wallets supporting CoinJoin transactions. The findings from this research can inform the development of more robust, user-friendly privacy-preserving techniques and wallets, ultimately enhancing privacy in the realm of cryptocurrency transactions.

7.2 Future Research

The use of privacy-preserving techniques in blockchain technology has gained increasing importance as concerns about user privacy and data protection continue to grow. While significant advancements have been made in this area, there is still much work to be done to fully realize the potential of these techniques. This section outlines three areas for future research in privacy-preserving blockchain technologies: usability, law enforcement, and practicality.

Usability. Usability is a critical factor in the adoption of privacy-preserving techniques. Research has shown that usable systems can attract more users and provide greater anonymity [161]. Future research in this area should focus on evaluating the usability of privacy-preserving techniques in the blockchain, particularly in terms of the differences in payment behavior between privacy-aware and privacy-unaware users. The cognitive walkthrough study highlighted the challenges associated with using wallets that support CoinJoin transactions, especially for novice users. Therefore, future research can address these issues and extend the study to include a more diverse range of technical and non-technical users. Improving the usability of privacy-preserving techniques in the

blockchain can encourage more users to adopt them, thereby enhancing overall privacy and security.

Future research can investigate how users' misconceptions about the building blocks lead to dangerous errors, monetary losses, and irreversible privacy compromises.

In this thesis, we focused on privacy wallets as a layer-two solution on top of Bitcoin. However, a comparative study can shed light on the usability of privacy solutions when offered as a layer-one solution (such as Monero). Future research can investigate which form of privacy solution (layer-one or layer-two) is more understandable and preferable for users.

Furthermore, exploring how privacy-preserving techniques can be integrated with digital identity solutions is becoming increasingly important in the context of decentralized identity systems. Future research can delve into methods to ensure that users have control over their personal data while maintaining the usability and convenience of identity wallets.

Law enforcement.

Privacy-preserving techniques in blockchain-based systems have raised concerns for law enforcement agencies. While these techniques can protect user privacy, they can also be exploited for illicit activities. Therefore, there is a need for research into the legal and regulatory aspects of these techniques, including finding ways to comply with relevant requirements while ensuring user privacy.

Moreover, research should be conducted to identify methods for categorizing the destination addresses of transactions utilizing privacy-preserving techniques (such as Coinjoin) to understand the usage of these techniques on the Bitcoin blockchain. This research can shed light on the potential for illicit activities and help law enforcement agencies collaborate with the involved parties in privacy-preserving transactions to identify criminals.

In de-anonymization techniques, while existing research has uncovered diverse heuristics and techniques for analyzing blockchain, particularly in identifying patterns of illicit activities, a need exists to refine and innovate robust heuristics explicitly designed to detect transactions utilizing privacy-enhancing techniques.

It is noteworthy that, in research on de-anonymization of UTXO-based blockchains such as Bitcoin, CoinJoin transactions are found and excluded from the analysis to prevent misleading results. However, many research papers do not take into account other privacy-preserving techniques such as PayJoin, which is indistinguishable in the blockchain and can lead to misleading results when de-anonymization heuristics such as common input ownership are applied. This gap highlights the necessity for a more holistic approach covering the complete range of privacy-preserving techniques, thereby gaining a better understanding of their inherent challenges and opportunities. In some cases, where it is mathematically not feasible to distinguish the connection between inputs and outputs, identifying fingerprints such as identical wallet features in both inputs

and outputs can aid in de-anonymizing these privacy transactions. This necessitates a comprehensive investigation to uncover both patterns and fingerprints.

The potential consequences of erroneous findings by surveillance entities include unwarranted investigations, breaches of privacy, and reputational harm. Such misjudgments also pose a threat to the broader adoption of cryptocurrencies by law-abiding individuals who fear being wrongly linked to criminal activities. By advancing the precision of these heuristics, researchers can actively contribute to the development of tools for law enforcement and regulatory bodies to detect suspicious cryptocurrency transactions. This is essential for a robust defense against money laundering and other illicit activities facilitated through cryptocurrencies.

It is worth mentioning that Tornado Cash an Ethereum mixing service, faced a significant setback when it was banned by the United States government in 2022 due to its alleged role in facilitating money laundering and illicit activities [148]. This event highlighted the challenges faced by developers of privacy-enhancing tools when their applications are misused for illicit activities, even if they were not designed for such purposes. Striking a balance between privacy for most users and preventing the misuse of technology for criminal activities remains an unresolved problem in the field.

Additionally, future research should evaluate the effectiveness of existing Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) measures in detecting money laundering specifically involving privacy techniques and privacy coins. The research can seek to specify gaps and areas for improvement by analyzing the strengths and limitations of the current regulatory framework.

Practicality. Finally, practicality is another critical factor to consider when implementing privacy-preserving techniques in the blockchain. It is essential to evaluate the efficiency of these techniques since their usage may introduce additional overhead that could negatively impact performance. Therefore, future research should prioritize investigating the trade-offs between privacy and efficiency and devising methods that strike a balance. For instance, further research could be conducted on non-equal amount CoinJoin transactions, which have the potential to improve the indistinguishability of these types of transactions. Additionally, the research could explore techniques such as Knapsack, proposed in [168] to enhance the practicality of privacy-preserving techniques in the blockchain.

Moreover, assessing the adequacy of existing mixing techniques in the Bitcoin blockchain is crucial. This involves evaluating the effectiveness of mixing services, such as CoinJoin, in providing the desired level of transaction privacy. Research could involve both empirical analysis and theoretical considerations to understand the potential vulnerabilities and limitations of current techniques.

In addition, expanding the scope of research to include cross-chain mixing or exploring privacy techniques on other blockchains, such as Ethereum, can provide valuable insights into the interoperability and compatibility of privacy-preserving methods. Investigating

how mixing techniques can be applied across different blockchains might lead to the development of standardized approaches that can be adopted in multi-chain ecosystems.

In conclusion, there is still significant work to be done to fully realize the potential of privacy-preserving techniques in blockchain-based systems. Future research in usability, law enforcement, and practicality can significantly improve the adoption and effectiveness of these techniques, leading to enhanced user privacy and security in the blockchain.

7.3 Published papers

[1] Simin Ghesmati (main contribution), Walid Fdhila (proofreading), and Edgar Weippl (supervision). "Studying Bitcoin privacy attacks and their Impact on Bitcoin-based Identity Methods." Business Process Management: Blockchain and Robotic Process Automation Forum: BPM 2021 Blockchain and RPA Forum, Rome, Italy, September 6–10, 2021, Proceedings 19. Springer International Publishing, 2021. [10]

[2] Simin Ghesmati (main contribution), Walid Fdhila (proofreading), and Edgar Weippl (supervision). "SoK: How private is Bitcoin? Classification and Evaluation of Bitcoin Privacy Techniques." Proceedings of the 17th International Conference on Availability, Reliability and Security. 2022. [11]

[3] Simin Ghesmati (equal contribution), Andreas Kern (equal contribution), Aljosha Judmayer (proofreading), Nicholas Stifter (proofreading), and Edgar Weippl (supervision). "Unnecessary input heuristics and PayJoin transactions." HCI International 2021-Posters: 23rd HCI International Conference, HCII 2021, Virtual Event, July 24–29, 2021, Proceedings, Part II 23. Springer International Publishing, 2021. [157]

[4] S. Ghesmati (main contribution), W. Fdhila (proofreading), and E. Weippl (supervision), "User-perceived privacy in blockchain," in International Conference on Financial Cryptography and Data Security Workshops, pp. 164–194, Springer, 2022[12]

[5] Simin Ghesmati (main contribution), Walid Fdhila (proofreading), and Edgar Weippl (supervision). "Usability of cryptocurrency wallets providing CoinJoin transactions.", Usable Security and Privacy (USEC) Symposium, 2022. [13]

[6] Simin Ghesmati (main contribution), Walid Fdhila (proofreading), and Edgar Weippl (supervision). "User-Centric Public Blockchain Privacy Threats.", pre-print, 2022. [169]

List of Figures

List of Tables

Acronyms

API Application Programming Interface. 32, 176

CLTV Check Lock Time Verify. 56, 176

CSV Check Sequence Verify. 56, 176

CT Confidential Transactions. 63, 75, 176

DID Decentralized Identifiers. 20, 22, 38, 40, 176

DoS Denial-of-Service. 73, 176

ECDSA Elliptic Curve Digital Signature Algorithm. 8, 9, 57, 66, 67, 73, 176

GDPR General Data Protection Regulation. 91, 92, 176, 193

GUI graphical user interface. 133, 176

HTLC Hash-Time-Locked Contracts. 15, 104, 176

HTTPS Hypertext Transfer Protocol Secure. 105, 176

IDP Identity Provider. 176

IOI Item of Interest. 33, 176

IPFS InterPlanetary File System. 41, 44, 176

IRC Internet Relay Chat. 128, 131, 176

KYC Know Your Customer. 45, 50, 96, 98, 115, 176

PGP Pretty Good Privacy. 137, 176

PII Personally Identifiable Information. 39, 43, 91, 92, 97, 176

PRNG Pseudo-Random Number Generator. 67, 176

RSA Rivest–Shamir–Adleman. 59, 176

SMC Secure Multi-party Computation. 66, 176

SPV Simplified Payment Verification. 16, 176

TEE Trusted Execution Environment. 52, 176

TOR The Onion Router. 39, 176

UTXO Unspent Transaction Output. 2, 10, 41, 44, 64, 65, 129, 146, 176

VCs Verifiable Credentials. 40, 43, 176

VPN Virtual Private Network. 35, 36, 39, 176

Bibliography

[1] F. Reid and M. Harrigan, "An analysis of anonymity in the bitcoin system," in *Security and privacy in social networks*, pp. 197–223, Springer, 2013.

[2] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "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.

[3] M. Harrigan and C. Fretter, "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.

[4] M. Jourdan, S. Blandin, L. Wynter, and P. Deshpande, "Characterizing entities in the bitcoin blockchain," in *2018 IEEE International Conference on Data Mining Workshops (ICDMW)*, pp. 55–62, IEEE, 2018.

[5] P. Tasca and C. J. Tessone, "Taxonomy of blockchain technologies. principles of identification and classification," *arXiv preprint arXiv:1708.04872*, 2017.

[6] A. Liberati, D. G. Altman, J. Tetzlaff, C. Mulrow, P. C. Gøtzsche, J. P. Ioannidis, M. Clarke, P. J. Devereaux, J. Kleijnen, and D. Moher, "The prisma statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration," *Annals of internal medicine*, vol. 151, no. 4, pp. W–65, 2009.

[7] M. Tomitsch, C. Wrigley, M. Borthwick, N. Ahmadpour, J. Frawley, A. B. Kocaballi, C. Núnez-Pacheco, and K. Straker, *Design. think. make. break. repeat. A handbook of methods.* BIS publishers, 2018.

[8] N. N. Group, "Usability 101: Introduction to usability," *URL: https: //www.nngroup.com/articles/ usability-101-introduction-to-usability/*, 2012.

[9] N. Ljunggren, "Improving the usability of secure information storing within blockchain applications," 2019.

[10] S. Ghesmati, W. Fdhila, and E. Weippl, "Studying bitcoin privacy attacks and their impact on bitcoin-based identity methods," in *Business Process Management: Blockchain and Robotic Process Automation Forum: BPM 2021 Blockchain and RPA Forum, Rome, Italy, September 6–10, 2021, Proceedings 19*, pp. 85–101, Springer, 2021.

[11] S. Ghesmati, W. Fdhila, and E. Weippl, "Sok: How private is bitcoin? classification and evaluation of bitcoin privacy techniques," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, pp. 1–14, 2022.

[12] S. Ghesmati, W. Fdhila, and E. Weippl, "User-perceived privacy in blockchain," in *International Conference on Financial Cryptography and Data Security*, pp. 164–194, Springer, 2022.

[13] S. Ghesmati, W. Fdhila, and E. Weippl, "Usability of cryptocurrency wallets providing coinjoin transactions," *Cryptology ePrint Archive*, 2022.

[14] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[15] A. M. Antonopoulos, *Mastering Bitcoin: Programming the open blockchain*. " O'Reilly Media, Inc.", 2017.

[16] K. Qin, J. Ernstberger, L. Zhou, P. Jovanovic, and A. Gervais, "Mitigating decentralized finance liquidations with reversible call options," *arXiv preprint arXiv:2303.15162*, 2023.

[17] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in *2015 IEEE symposium on security and privacy*, pp. 104–121, IEEE, 2015.

[18] S. Nakamoto, "A peer-to-peer electronic cash system," *URL: https:// bitcoin. org/ bitcoin. pdf*, 2008.

[19] A. Triwinarko, "Elliptic curve digital signature algorithm (ecdsa)," *Program Studi Teknik Informatika ITB, Bandung*, 2006.

[20] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[21] I. F. Blake, G. Seroussi, and N. P. Smart, *Advances in elliptic curve cryptography*, vol. 317. Cambridge University Press, 2005.

[22] Wiki, "Secp256k1," *https:// en.bitcoin.it/ wiki/ Secp256k1*, Last accessed 20 July 2020.

[23] G. M. Lilly, "Device for and method of one-way cryptographic hashing," Dec. 7 2004. US Patent 6,829,355.

[24] H. Dobbertin, A. Bosselaers, and B. Preneel, "Ripemd-160: A strengthened version of ripemd," in *International Workshop on Fast Software Encryption*, pp. 71–82, Springer, 1996.

[25] Wiki, "Base58check encoding," *https:// en.bitcoin.it/ wiki/ Base58Check$_e$ncoding*, *Lastaccessed*20*July*2020.

[26] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, "Mixcoin: Anonymity for bitcoin with accountable mixes," in *International Conference on Financial Cryptography and Data Security*, pp. 486–504, Springer, 2014.

[27] J. H. Ziegeldorf, F. Grossmann, M. Henze, N. Inden, and K. Wehrle, "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.

[28] Wiki, "Technical background of version 1 bitcoin addresses," *https:// en.bitcoin.it/ wiki/ Technical$_b$ackground$_o$f$_v$ersion$_1$Bitcoin$_a$ddresses*, *Lastaccessed*28*July*2020.

[29] M. M. Chakravarty, J. Chapman, K. MacKenzie, O. Melkonian, M. Peyton Jones, and P. Wadler, "The extended utxo model," in *Financial Cryptography and Data Security: FC 2020 International Workshops, AsiaUSEC, CoDeFi, VOTING, and WTSC, Kota Kinabalu, Malaysia, February 14, 2020, Revised Selected Papers 24*, pp. 525–539, Springer, 2020.

[30] Wikipedia, "Double-spending," *https:// en.wikipedia.org/ wiki/ Double-spending*, Last accessed 21 July 2020.

[31] Wikipedia, "Unspent transaction output," *https:// en.wikipedia.org/ wiki/ Unspent transaction output*, Last accessed 21 July 2020.

[32] D. York, *Seven deadliest unified communications attacks*. Syngress, 2010.

[33] E. Heilman, L. Alshenibr, F. Baldimtsi, A. Scafuro, and S. Goldberg, "Tumblebit: An untrusted bitcoin-compatible anonymous payment hub," in *Network and Distributed System Security Symposium*, 2017.

[34] Wiki, "Script," *https:// en.bitcoin.it/ wiki/ Script*, Last accessed 21 July 2020.

[35] Wikipedia, "Forth (programming language)," *URL: https:// en.wikipedia.org/ wiki/ Forth (programming language)*, Last accessed 21 July 2020.

[36] bitcoin.org, "Pay-to-public-key-hash," *https:// developer.bitcoin.org/ devguide/ transactions.html#p2pkh-script-validation*, Last accessed 21 July 2020.

[37] bitcoin.org, "Pay-to-script-hash," *https:// developer.bitcoin.org/ devguide/ transactions.html#p2sh-scripts*, Last accessed 21 July 2020.

[38] Wiki, "Multisignature," *https:// en.bitcoin.it/ wiki/ Multisignature*, Last accessed 16 July 2020.

[39] bitcoin.org, "Multisig," *https:// developer.bitcoin.org/ devguide/ transactions.html#multisig*, Last accessed 21 July 2020.

[40] P. Franco, *Understanding Bitcoin: Cryptography, engineering and economics*. John Wiley & Sons, 2014.

[41] Wiki, "Timelock," *https:// en.bitcoin.it/ wiki/ Timelock*, Last accessed 16 July 2020.

[42] Wiki, "Hashlock," *https:// en.bitcoin.it/ wiki/ Hashlock*, Last accessed 21 July 2020.

[43] Wiki, "Htlc," *https:// en.bitcoin.it/ wiki/ Hash Time Locked Contracts*, Last accessed 22 July 2020.

[44] S. Bowe and D. Hopwood, "Hashed time-locked contract transactions," *Bitcoin Improvement Proposal, https:// github. com/ bitcoin/ bips/ blob/ master/ bip-0199. mediawiki*, 2018.

[45] P. Chatzigiannis, F. Baldimtsi, and K. Chalkias, "Sok: Blockchain light clients," in *Financial Cryptography and Data Security: 26th International Conference, FC 2022, Grenada, May 2–6, 2022, Revised Selected Papers*, pp. 615–641, Springer, 2022.

[46] M. Corallo, "Bip 152: Compact block relay (2016)," *URl: https://github. com/bitcoin/bips/blob/master/bip-0152. mediawiki*, 2020.

[47] S. Baek, H. Nam, Y. Oh, M. Tran, and M. S. Kang, "Short paper: On the claims of weak block synchronization in bitcoin," in *Financial Cryptography and Data Security: 26th International Conference, FC 2022, Grenada, May 2–6, 2022, Revised Selected Papers*, pp. 663–671, Springer, 2022.

[48] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management," 2010.

[49] D. Ermilov, M. Panov, and Y. Yanovich, "Automatic bitcoin address clustering," in *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*, pp. 461–466, IEEE, 2017.

[50] M. Möser and A. Narayanan, "Resurrecting address clustering in bitcoin," in *Financial Cryptography and Data Security: 26th International Conference, FC 2022, Grenada, May 2–6, 2022, Revised Selected Papers*, pp. 386–403, Springer, 2022.

[51] K. Krombholz, A. Judmayer, M. Gusenbauer, and E. Weippl, "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.

[52] B. Fabian, T. Ermakova, and U. Sander, "Anonymity in bitcoin?–the users' perspective," 2016.

[53] A. Mai, K. Pfeffer, M. Gusenbauer, E. Weippl, and K. Krombholz, "User mental models of cryptocurrency systems—-a grounded theory approach," 2020.

[54] A. Voskobojnikov, B. Obada-Obieh, Y. Huang, and K. Beznosov, "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.

[55] A. Whitten and J. D. Tygar, "Why johnny can't encrypt: A usability evaluation of pgp 5.0.," in *USENIX Security Symposium*, vol. 348, pp. 169–184, 1999.

[56] S. Eskandari, J. Clark, D. Barrera, and E. Stobert, "A first look at the usability of bitcoin key management," *arXiv preprint arXiv:1802.04351*, 2018.

[57] D. Norman, "Psychopathology of everyday things," 2013.

[58] H. Halpin, "Holistic privacy and usability of a cryptocurrency wallet," *arXiv preprint arXiv:2105.02793*, 2021.

[59] A. Voskobojnikov, O. Wiese, M. Mehrabi Koushki, V. Roth, and K. Beznosov, "The u in crypto stands for usable: An empirical study of user experience with mobile cryptocurrency wallets," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pp. 1–14, 2021.

[60] A. Cooper, H. Tschofenig, B. Aboba, J. Peterson, J. Morris, M. Hansen, and R. Smith, "Privacy considerations for internet protocols," *Internet Architecture Board*, 2013.

[61] R. Henry, A. Herzberg, and A. Kate, "Blockchain access privacy: Challenges and directions," *IEEE Security & Privacy*, vol. 16, no. 4, pp. 38–45, 2018.

[62] M. Spagnuolo, F. Maggi, and S. Zanero, "Bitiodine: Extracting intelligence from the bitcoin network," in *International conference on financial cryptography and data security*, pp. 457–468, Springer, 2014.

[63] H. Kalodner, M. Möser, K. Lee, S. Goldfeder, M. Plattner, A. Chator, and A. Narayanan, "Blocksci: Design and applications of a blockchain analysis platform," in *29th {USENIX} Security Symposium)*, pp. 2721–2738, 2020.

[64] M. Conti, A. Gangwal, and S. Ruj, "On the economic significance of ransomware campaigns: A bitcoin transactions perspective," *Computers & Security*, vol. 79, pp. 162–189, 2018.

[65] D. Y. Huang, M. M. Aliapoulios, V. G. Li, L. Invernizzi, E. Bursztein, K. McRoberts, J. Levin, K. Levchenko, A. C. Snoeren, and D. McCoy, "Tracking ransomware end-to-end," in *2018 IEEE Symposium on Security and Privacy (SP)*, pp. 618–631, IEEE, 2018.

[66] S. Lee, C. Yoon, H. Kang, Y. Kim, Y. Kim, D. Han, S. Son, and S. Shin, "Cybercriminal minds: An investigative study of cryptocurrency abuses in the dark web.," in *NDSS*, 2019.

[67] Y. Boshmaf, C. Elvitigala, H. Al Jawaheri, P. Wijesekera, and M. Al Sabah, "Investigating mmm ponzi scheme on bitcoin," in *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, pp. 519–530, 2020.

[68] P. Koshy, D. Koshy, and P. McDaniel, "An analysis of anonymity in bitcoin using p2p network traffic," in *International Conference on Financial Cryptography and Data Security*, pp. 469–485, Springer, 2014.

[69] A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in bitcoin p2p network," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pp. 15–29, 2014.

[70] T. Neudecker and H. Hartenstein, "Could network information facilitate address clustering in bitcoin?," in *International conference on financial cryptography and data security*, pp. 155–169, Springer, 2017.

[71] A. Biryukov and S. Tikhomirov, "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.

[72] S. M. English and E. Nezhadian, "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.

[73] F. Sabry, W. Labda, A. Erbad, H. Al Jawaheri, and Q. Malluhi, "Anonymity and privacy in bitcoin escrow trades," in *Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society*, pp. 211–220, 2019.

[74] H. Yousaf, G. Kappos, and S. Meiklejohn, "Tracing transactions across cryptocurrency ledgers," in *28th {USENIX} Security Symposium ({USENIX} Security 19)*, pp. 837–850, 2019.

[75] Linddun, "Linddun go threat categories," *https:// www.linddun.org/ linddun-go-categories*, Last accessed 30 May 2022.

[76] G. Maxwell, "Coinjoin: Bitcoin privacy for the real world, 2013," *URl: https:// bitcointalk. org/ index. php*, 2013.

[77] H. Kalodner, "Privacy," *https:// citp.github.io/ BlockSci/ reference/ heuristics/ change.html*, Last accessed 23 July 2020.

[78] A. Gibson, "Payjoin," *https://joinmarket.me/blog/blog/payjoin/*, Last accessed 23 Aug 2020.

[79] Wiki, "Privacy," *https:// en.bitcoin.it/ wiki/ Privacy*, Last accessed 23 July 2020.

[80] Wiki, "Address reuse," *https://en.bitcoin.it/wiki/Address_reuse*, 2021.

[81] D. Reed, M. Sporny, D. Longley, C. Allen, R. Grant, M. Sabadello, and J. Holt, "Decentralized identifiers (dids) v1. 0," *Draft Community Group Report*, 2021.

[82] M. Sporny, D. Reed, D. Longley, M. Sabadello, and C. Allen, "Decentralized Identifiers (DIDs) v1.0," W3C Recommendation 20210609, World Wide Web Consortium (W3C), June 2021.

[83] M. Sporny, G. Noble, D. Longley, D. Burnett, and B. Zundel, "Verifiable credentials data model," 2019.

[84] C. Allen, K. Hamilton Duffy, R. Grant, and D. Pape, "Btcr did method," *https://w3c-ccg.github.io/didm-btcr/*, 2019.

[85] Wiki, "Op_return," *https://en.bitcoin.it/wiki/OP_RETURN*, 2020.

[86] A. Gibson, "Payjoin," *https:// joinmarket.me /blog /blog /payjoin/*, 2018 (Last accessed 23 August 2020).

[87] L. Lesavre, P. Varin, P. Mell, M. Davidson, and J. Shook, "A taxonomic approach to understanding emerging blockchain identity management systems," *arXiv preprint arXiv:1908.00929*, 2019.

[88] C. C. G. (W3C), "A primer for decentralized identifiers," *https://w3c-ccg.github.io/did-primer/*, 2020.

[89] J. Andrieu, S. Appelcline, J. Lohkamp, D. Reed, M. Sabadello, O. Terbu, and A. Guy, "Did method rubric v1.0," *https://w3c.github.io/did-rubric/privacy*, 2021.

[90] P. Dunphy and F. A. Petitcolas, "A first look at identity management schemes on the blockchain," *IEEE Security & Privacy*, vol. 16, no. 4, pp. 20–29, 2018.

[91] H. Halpin and M. Piekarska, "Introduction to security and privacy on the blockchain," in *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pp. 1–3, IEEE, 2017.

[92] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose, "Sok: Security evaluation of home-based iot deployments," in *2019 IEEE Symposium on Security and Privacy (SP)*, pp. 1362–1380, IEEE, 2019.

[93] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–90, 1981.

[94] L. Valenta and B. Rowan, "Blindcoin: Blinded, accountable mixes for bitcoin," in *International Conference on Financial Cryptography and Data Security*, pp. 112–126, Springer, 2015.

[95] D. Chaum, "Blind signatures for untraceable payments," in *Advances in cryptology*, pp. 199–203, Springer, 1983.

[96] Z. Bao, W. Shi, S. Kumari, Z.-y. Kong, and C.-M. Chen, "Lockmix: a secure and privacy-preserving mix service for bitcoin anonymity," *International Journal of Information Security*, pp. 1–11, 2019.

[97] M. Tran, L. Luu, M. S. Kang, I. Bentov, and P. Saxena, "Obscuro: A bitcoin mixer using trusted execution environments," in *Proceedings of the 34th Annual Computer Security Applications Conference*, pp. 692–701, 2018.

[98] M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted execution environment: what it is, and what it is not," in *2015 IEEE Trustcom/BigDataSE/Ispa*, vol. 1, pp. 57–64, IEEE, 2015.

[99] S. Barber, X. Boyen, E. Shi, and E. Uzun, "Bitter to better—how to make bitcoin a better currency," in *International conference on financial cryptography and data security*, pp. 399–414, Springer, 2012.

[100] G. Bissias, A. P. Ozisik, B. N. Levine, and M. Liberatore, "Sybil-resistant mixing for bitcoin," in *Proceedings of the 13th Workshop on Privacy in the Electronic Society*, pp. 149–158, 2014.

[101] G. Maxwell, "Coinswap: transaction graph disjoint trustless trading (2013)," *URL: https:// bitcointalk. org/ index. php*, 2013.

[102] M. Möser and R. Böhme, "Anonymous alone? measuring bitcoin's second-generation anonymization techniques," in *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pp. 32–41, IEEE, 2017.

[103] A. Gibson, "New coinswap," *https:// joinmarket.me /blog /blog /coinswaps/*, 2017 (Last accessed 23 August 2020).

[104] P. Todd, "Bip 65: Op checklocktimeverify," *Github (accessed 18 October 2015) https://github. com/bitcoin/ bips/blob/master/bip-0065. mediawiki*, 2014.

[105] M. F. BtcDrak and E. Lombrozo, "Bip 112: Checksequenceverify," *URl: https://github. com/bitcoin/bips/ blob/master/ bip-0112. mediawiki*, 2015.

[106] E. Lombrozo, J. Lau, and P. Wuille, "Bip 141: Segre-gated witness (consensus layer), 2015," *Avail-able: https://github. com/bitcoin/bips/blob/master/bip-0141. mediawiki*, 2017.

[107] C. Belcher, "Design for a coinswap implementation for massively improving bitcoin privacy and fungibility," *https:// gist.github. com/ chris-belcher/ 9144bd57a91c194e332fb5ca371d0964*, Last accessed 16 July 2020.

[108] C. Belcher, "Joinmarket," *https://github.com/JoinMarket-Org/ joinmarket-clientserver*, (2018) Last accessed 24 March 2021.

[109] E. Heilman, F. Baldimtsi, and S. Goldberg, "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.

[110] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[111] T. Ruffing, P. Moreno-Sanchez, and A. Kate, "Coinshuffle: Practical decentralized coin mixing for bitcoin," in *European Symposium on Research in Computer Security*, pp. 345–364, Springer, 2014.

[112] H. Corrigan-Gibbs and B. Ford, "Dissent: accountable anonymous group messaging," in *Proceedings of the 17th ACM conference on Computer and communications security*, pp. 340–350, 2010.

[113] T. Ruffing, P. Moreno-Sanchez, and A. Kate, "P2p mixing and unlinkable bitcoin transactions.," in *NDSS*, pp. 1–15, 2017.

[114] T. Ruffing and P. Moreno-Sanchez, "Valueshuffle: Mixing confidential transactions for comprehensive transaction privacy in bitcoin," in *International Conference on Financial Cryptography and Data Security*, pp. 133–154, Springer, 2017.

[115] A. Gibson, "Coinjoinxt - a more flexible, extended approach to coinjoin," *https://joinmarket.me /blog/blog /coinjoinxt/*, 2018 (Last accessed 31 August 2020).

[116] C.-P. Schnorr, "Efficient identification and signatures for smart cards," in *Conference on the Theory and Application of Cryptology*, pp. 239–252, Springer, 1989.

[117] G. Malavolta, P. Moreno-Sanchez, C. Schneidewind, A. Kate, and M. Maffei, "Anonymous multi-hop locks for blockchain scalability and interoperability.," in *NDSS*, 2019.

[118] A. Gibson, "Snicker - simple non-interactive coinjoin with keys for encryption reused," *https://joinmarket.me /blog /blog/snicker/*, 2017 (Last accessed 31 August 2020).

[119] Blockstream, "Improving privacy using pay-to-endpoint (p2ep)," *https://blockstream.com/2018/ 08/08/en-improving-privacy-using-pay-to-endpoint/*, Last accessed 20 September 2020.

[120] R. Havar, "Bustapay bip: a practical sender/receiver coinjoin protocol," *https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-August/016340.html*, Last accessed 20 September 2020.

[121] N. Dorier, "Bip78: A simple payjoin proposal," *https://github.com/bitcoin/bips/blob/master/bip-0078.mediawiki*, Last accessed 20 Sep 2020.

[122] M. H. Ibrahim, I. Ali, I. Ibrahim, and A. El-Sawi, "A robust threshold elliptic curve digital signature providing a new verifiable secret sharing scheme," in *2003 46th Midwest Symposium on Circuits and Systems*, vol. 1, pp. 276–280, IEEE, 2003.

[123] M. H. Ibrahim, "Securecoin: A robust secure and efficient protocol for anonymous bitcoin ecosystem.," *IJ Network Security*, vol. 19, no. 2, pp. 295–312, 2017.

[124] Q. Wang, X. Li, and Y. Yu, "Anonymity for bitcoin from secure escrow address," *IEEE Access*, vol. 6, pp. 12336–12341, 2017.

[125] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, "Secure distributed key generation for discrete-log based cryptosystems," in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 295–310, Springer, 1999.

[126] N. Van Saberhagen, "Cryptonote v 2.0," 2013.

[127] caedesvvv, "Darkwallet," *https:// github.com/ darkwallet/ darkwallet/ releases/ tag/ 0.8.0*, 2015.

[128] nopara73, "Tumblebit vs coinjoin," *https://nopara73.medium.com/tumblebit-vs-coinjoin-15e5a7d58e3*, Last accessed 3 Feb 2021.

[129] LeGaulois, "2020 list bitcoin mixers bitcoin tumblers websites," *https:// bitcointalk.org/ index.php?topic=2827109.0*, Last accessed 11 August 2020.

[130] . nopara, "Dumplings," *https://github.com/nopara73/Dumplings*, Last accessed 3 Feb 2021.

[131] Wasabi, "Wasabiwallet," *https://wasabiwallet.io/*, Last accessed 05 August 2020.

[132] Samourai, "Samouraiwallet," *URL: https:// samouraiwallet.com/ whirlpool*, Last accessed 05 August 2020.

[133] A. Gibson, "From mac to wabisabi," *https://joinmarket.me/blog/blog/from-mac-to-wabisabi/*, Last accessed 3 Feb 2021.

[134] A. Ficsor, "Zerolink: The bitcoin fungibility framework," *URL: https: //github.com/ nopara73/ZeroLink*, 2017.

[135] R. Ver, "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.

[136] BlueWallet, "Bluewallet," *URL: https: //github.com /BlueWallet /BlueWallet*, Last accessed 04 September 2020.

[137] D. Weigl, "Mycelium shufflepuff," *https:// github.com/ DanielWeigl/ Shufflepuff*, 2016 (Last accessed 11 August 2020).

[138] Jelurida, "Nxt," *https://nxtdocs.jelurida.com/ Coin Shuffling*, Last accessed 11 August 2020.

[139] NTumbleBit, "Ntumblebit," *https://github.com/nTumbleBit/nTumbleBit*, Last accessed 10 Nov 2021.

[140] BTCPay, "Btcpay server payjoin guide," *https:// docs.btcpayserver.org/ Payjoin/*, Last accessed 23 August 2020.

[141] Breeze, "Breeze," *https://github.com/stratisproject/Breeze*, Last accessed 10 Nov 2021.

[142] Bluewallet, "Bluewallet," *https://bluewallet.io/features/*, Last accessed 10 Nov 2021.

[143] B. G. Glaser and A. L. Strauss, "The discovery of grounded theory: Strategies for qualitative research," *Sociology Press*, 1967.

[144] Y. Chun Tie, M. Birks, and K. Francis, "Grounded theory research: A design framework for novice researchers," *SAGE open medicine*, vol. 7, p. 2050312118822927, 2019.

[145] C. C. Serdar, M. Cihan, D. Yücel, and M. A. Serdar, "Sample size, power and effect size revisited: simplified and practical approaches in pre-clinical, clinical and laboratory studies," *Biochemia medica*, vol. 31, no. 1, pp. 27–53, 2021.

[146] R. Ristl, "Sample size calculator," 2024.

[147] K. Pfeffer, A. Mai, A. Dabrowski, M. Gusenbauer, P. Schindler, E. Weippl, M. Franz, and K. Krombholz, "On the usability of authenticity checks for hardware security tokens," in *30th {USENIX} Security Symposium ({USENIX} Security 21)*, 2021.

[148] D. O. T. T. U.S., "U.s. treasury sanctions notorious virtual currency mixer tornado cash," *https://home.treasury.gov/news/press-releases/jy0916*, Last accessed 24 March 2023.

[149] L. Zhou, X. Xiong, J. Ernstberger, S. Chaliasos, Z. Wang, Y. Wang, K. Qin, R. Wattenhofer, D. Song, and A. Gervais, "Sok: Decentralized finance (defi) attacks," in *2023 IEEE Symposium on Security and Privacy (SP)*, pp. 2444–2461, IEEE, 2023.

[150] R. Stütz, J. Stockinger, P. Moreno-Sanchez, B. Haslhofer, and M. Maffei, "Adoption and actual privacy of decentralized coinjoin implementations in bitcoin," in *Proceedings of the 4th ACM Conference on Advances in Financial Technologies*, pp. 254–267, 2022.

[151] J. Quesnelle, "On the linkability of zcash transactions," *arXiv preprint arXiv:1712.01210*, 2017.

[152] G. Kappos, H. Yousaf, M. Maller, and S. Meiklejohn, "An empirical analysis of anonymity in zcash," in *27th {USENIX} Security Symposium ({USENIX} Security 18)*, pp. 463–477, 2018.

[153] Wiki, "Mt. gox," *https:// en.wikipedia.org/wiki/Mt.*$_{G}$*ox*, *Lastaccessed*17*January*2022.

[154] 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.

[155] 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.

[156] P. Keller, M. Florian, and R. Böhme, "Collaborative deanonymization," *arXiv preprint arXiv:2005.03535*, 2020.

[157] S. Ghesmati, A. Kern, A. Judmayer, N. Stifter, and E. Weippl, "Unnecessary input heuristics and payjoin transactions," in *International Conference on Human-Computer Interaction*, pp. 416–424, Springer, 2021.

[158] Nopara73, "Dumplings," *URL: https://github.com/nopara73/Dumplings*, Last access 12 May 2021.

[159] M. Möser and R. Böhme, "Join me on a market for anonymity," in *Workshop on Privacy in the Electronic Society*, 2016.

[160] J. Stockinger, B. Haslhofer, P. Moreno-Sanchez, and M. Maffei, "Pinpointing and measuring wasabi and samourai coinjoins in the bitcoin ecosystem," *arXiv preprint arXiv:2109.10229*, 2021.

[161] R. Dingledine, N. Mathewson, and P. Syverson, "Challenges in deploying low-latency anonymity," *NRL CHACS Report*, pp. 5540–625, 2005.

[162] C. Lewis and C. Wharton, "Chapter 30 - cognitive walkthroughs," in *Handbook of Human-Computer Interaction (Second Edition)* (M. G. Helander, T. K. Landauer, and P. V. Prabhu, eds.), pp. 717–732, Amsterdam: North-Holland, second edition ed., 1997.

[163] N. N. Group, "Evaluate interface learnability with cognitive walkthroughs," *URL: https://www.nngroup.com/articles/cognitive-walkthroughs/*, 2022.

[164] A. Gibson, "Joinmarket update for oct 2020," *URL: https: //joinmarket.me /blog /blog/oct-2020-update/*, 2020.

[165] zkSNACKs, "Use of wasabi," *URL: https://docs.wasabiwallet.io/ FAQ/FAQ-UseWasabi.html #how-can-i-mix-large-amounts*, 2018.

[166] Timmy2905, "Samourai wallet] whirlpool stuck on "joined a mix"," *URL: https://www.reddit.com/r/Bitcoin/ comments/in2kzt/samourai_wallet_whirlpool_stuck_on_joined_a_mix/*, 2020.

[167] Coolwallet, "The 5 biggest bitcoin private key horror stories," *URL: https://www.coolwallet.io/blog/bitcoin-lost-private-key-horror-stories/*, 2021.

[168] F. K. Maurer, T. Neudecker, and M. Florian, "Anonymous coinjoin transactions with arbitrary values," in *2017 IEEE Trustcom/BigDataSE/ICESS*, pp. 522–529, IEEE, 2017.

[169] S. Ghesmati, W. Fdhila, and E. Weippl, "User-centric public blockchain privacy threats," 2022.

Appendices

User perceived privacy questionnaire

* 1. Please check the box.

☐ I read all the information about the objective, 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.) [1]

☐ List of bitcoin.org wallets

☐ Other (please specify)

* 10. Why did you use MyMaps as your Bitcoin wallet? It was shown to whom that

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

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.) In de-anonymization techniques, the attacker finds the relationship between addresses and tries to relate the addresses to the real identities.
This question contained an invalid answer (Relating the input and output).

☐ Address reuse (reusing the address in different transactions)

☐ 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 on 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

thefees and delays questions?

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

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

☐ 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 to 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 to 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.
Make sure that it is a valid address and that you are able to redeem coins from it.

* 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

Wasabi Wallet usability study task sheet

Perform the following tasks and fill out the form: You need to provide the time spent on each task.

Tasks:

T.1 Install Wasabi application. https://wasabiwallet.io/ Note: We have to configure the wallet for TestNet (Menu/Tools/Setting/Network=TestNet). Close the application and reopen the app. Do not consider the time for TestNet setting in the task sheet.

T.2 Generate a wallet.

T.3 Fund the wallet, which includes creating a receive address and checking the balance. Note: Bitcoin Faucet can be used to fund the wallet. https://coinfaucet.eu/en/btc-testnet/

T.4 Perform a CoinJoin transaction with the lowest anonymity set (2 or 3).

T.5 Transfer CoinJoin coins to the destination address (your optional address).

Before starting the tasks, read the following questions.

2. Please provide your OS type.

☐ MacOS

☐ Windows

☐ Debian / Ubunto

☐ Other Linux

☐ Other (please specify)

T.1: Installing the application

3. Provide the time on task T.1 in terms of minutes.
4. Did you succeed in performing task T.1 on the first attempt?

☐ Yes

☐ No (please specify the number of failures)

5. Any errors you have received/ any suggestions to improve the wallet in performing T.1.
6. Overall, how satisfied were you with performing task T.1?

☐ Very satisfied

☐ Satisfied

☐ Neither satisfied nor dissatisfied

☐ Dissatisfied

☐ Very dissatisfied

T.2: Generating the wallet

7. Provide the time on task T.2 in terms of minutes.
8. Did you succeed in performing task T.2 on the first attempt?

☐ Yes

☐ No (please specify the number of failures)

9. Any errors you have received/ any suggestions to improve the wallet in performing T.2.
10. Overall, how satisfied were you with performing task T.2?

☐ Very satisfied

☐ Satisfied

☐ Neither satisfied nor dissatisfied

☐ Dissatisfied

☐ Very dissatisfied

T.3: Funding the wallet

11. Provide us with the funding transaction ID.
12. Provide the time on task T.3 in terms of minutes.
13. Did you succeed in performing task T.3 on the first attempt?

Yes

No (please specify the number of failures)

14. Any errors you have received/ any suggestions to improve the wallet in performing T.3.
15. Overall, how satisfied were you with performing task T.3?

☐ Very satisfied

☐ Satisfied

☐ Neither satisfied nor dissatisfied

☐ Dissatisfied

☐ Very dissatisfied

T.4: Performing a CoinJoin transaction

16. Provide us with the CoinJoin transaction ID. (one would be enough)
17. Provide the time on Task T.4 in terms of minutes.
18. Did you succeed in performing task T.4 on the first attempt?

☐ Yes

☐ No (please specify the number of failures)

19. Any errors you have received/ any suggestions to improve the wallet in performing T.4.
20. Overall, how satisfied were you with performing task T.4?

☐ Very satisfied

☐ Satisfied

☐ Neither satisfied nor dissatisfied

☐ Dissatisfied

☐ Very dissatisfied

T.5: Transferring CoinJoin coins to the destination address

21. Provide us the transaction ID of sending to the destination address. (one would be

enough)
22. Provide the time on Task T.5 in terms of minutes.
23. Did you succeed in performing task T.5 on the first attempt?

☐ Yes

☐ No (please specify the number of failures)
24. Any errors you have received/ any suggestions to improve the wallet in performing T.5.
25. Overall, how satisfied were you with performing task T.5?

☐ Very satisfied

☐ Satisfied

☐ Neither satisfied nor dissatisfied

☐ Dissatisfied

☐ Very dissatisfied