Everything You Ever Wanted to Know About Bitcoin Mixers (But Were Afraid to Ask)

Jaswant Pakki, Yan Shoshitaishvili, Ruoyu Wang, Tiffany Bao, and Adam Doupé

Arizona State University
{jpakki1, yans, fishw, tbao, doupe}@asu.edu

Abstract. The lack of fungibility in Bitcoin has forced its userbase to seek out tools that can heighten their anonymity. Third-party Bitcoin mixers use obfuscation techniques to protect participants from blockchain transaction analysis. In recent years, various centralized and decentralized Bitcoin mixing methods were proposed in academic literature (e.g., CoinJoin, CoinShuffle). Although these methods strive to create a threat-free environment for users to preserve their anonymity, public Bitcoin mixers continue to be associated with theft and poor implementation.
This paper explores the public Bitcoin mixer ecosystem to identify if today's mixing services have adopted academia's proposed solutions. We perform real-world interactions with publicly available mixers to analyze both implementation and resistance to common threats in the mixing landscape. We present data from 21 publicly available mixing services on the deep web and clearnet.
Our results highlight a clear gap between public and proposed Bitcoin mixers in both implementation and security. We find that the majority of key security features proposed by academia are not deployed in any public Bitcoin mixers that are trusted most by Bitcoin users. Today's mixing services focus on presenting users with a *false sense of control* to gain their trust rather than employing secure mixing techniques.

1 Introduction

In May of 2019, European Union authorities seized Bestmixer, a mixing service that advertised to eradicate any criminal history associated with a user's Bitcoin. After an investigation, authorities asserted that the majority of the $200 million that traveled through the service had "a criminal origin or destination" [6].

Bitcoin mixing services are not illegal by nature: Their guarantee to obfuscate a trail of funds appeals to benign users who seek anonymity, and various centralized mixing services are available to the public today. The techniques implemented by these services have a direct impact on user privacy and security. For example, Bestmixer claimed to eradicate all "order history completely and automatically in 24 hours" [5]. This claim was proven false when authorities seized IP-addresses, transactions logs, wallet addresses, and chat messages that were stored on multiple Bestmixer servers.

The dual use of mixing services, by both privacy-wary users and cybercriminals, provides two motivations for their study. Aiding the former, security researchers in academia have proposed plethora designs and implementations for secure mixing [11, 12, 15, 16, 22–25]. Hunting the latter, researchers developed techniques that are capable of tracking Bitcoins through deployed mixers [10, 19, 21]. However, a gap remains: Despite active research in Bitcoin mixing and *un-mixing*, it is unclear on what techniques current, actually deployed dual-use Bitcoin mixers base their operation and, thus, it is unclear what security properties their users can expect. The effect of this is clear: Although protocols for ideal mixing exist, the majority of publicly available services are still associated with distrust and scam accusations [7].

In this paper, we provide the first *active* and systematic measurement of the current public Bitcoin mixing ecosystem to identify if academically proposed solutions are adopted. The key challenge of this measurement is to scalably analyze public mixers and correlate our observations with academically proposed solutions. Another challenge is the majority of public mixers are black-box services, which do not have their code available to the public. To tackle these challenges, we perform real-world mixer interactions with five public mixers to identify *actual behaviors* that are indicative of their implementation and their resistance to common threats. We leverage our direct interactions, the public nature of Bitcoin's blockchain, and mixer-specific features to identify these behaviors.

Our results highlight a gap of implementation and security between academically proposed mixing solutions and actual public mixers. For example, our security analysis identifies a lack of coin theft prevention in *all five public mixers studied*, even though solutions exist, such as Obscuro [23]. Our results also include mixer-specific characteristics that would benefit from longitudinal research.

Overall, this paper makes the following contributions:

- We provide an overview of the current Bitcoin mixing service landscape, both regarding published academic literature and through information that is collected from actual public mixers.
- We conduct active experiments with five popular public mixing services to collect data and transaction IDs of real-world mixer interactions.
- We perform an implementation and security analysis on our mixing dataset. Among other insights, we determined that none of the studied public mixers implement cutting-edge security properties as proposed by academia.

2 Background

Bitcoin mixing services provide their users with improved anonymity by leveraging inherent characteristics of both Bitcoin and blockchain technology. Before diving into the details of mixers, here we present background knowledge on Bitcoin itself and discuss prior research work that is related to Bitcoin mixers.

Bitcoin and Blockchain. Bitcoin (BTC) is a decentralized digital currency that relies on a peer-to-peer (P2P) distributed network to store and check the

validity of transaction data [20]. This data is stored on a public ledger where users are identified by pseudonymous addresses (we will discuss the security implications of these addresses further in Section 2). The blockchain is the underlying architecture of the public ledger. Each block holds the hash of its predecessor and a Merkle tree of transactions. Any change in transaction information would lead to a different Merkle root hash and hash of the block itself.

Another integral part of Bitcoin's implementation is its use of the Elliptic Curve Digital Signature Algorithm (ECDSA). The pseudonymous addresses users create are each derived from corresponding public/private key pairs stored in user's wallets. To prevent forgery of transactions, Bitcoin users sign created transactions with their private key. When transaction information is sent out to nodes in the P2P network, they use the sender's public key to validate that the transaction was signed by the corresponding private key.

Anonymity in Bitcoin. Bitcoin uses pseudonymous addressing to identify its users. While these users are capable of creating as many addresses as they would like, they are not required to do so. In turn, researchers have used clustering, transaction analysis, taint analysis, and behavior analysis to track patterns and build relationships between public keys [9, 13, 14, 17, 18]. The official Bitcoin website highlights potential threats to user anonymity and clearly states that the currency is not anonymous [1].

Bitcoin Transactions. Bitcoin makes use of a transaction-based public ledger. Inputs and outputs of transactions are referred to as Unspent Transaction Outputs (UTXOs). Transactions consume UTXOs as inputs and create new ones as outputs. UTXOs can only be used in full or not at all. It is quite unlikely that a UTXO will match the exact requested spent amount. Thus, the majority of Bitcoin transactions have two outputs. While the recipient receives one output, the left over (change output) amount is sent back to the sender at a new address.

Transaction metadata includes public keys, input and output UTXOs, size of the transaction, and hash of the transaction as a unique identifier. Transaction inputs also include signatures using the sender's private key; this allows anyone to use the sender's public key to verify the validity of the signed transaction.

Related Work. In 2013, Moser *et al.* [19] explored Bitcoin Fog, BitLaundry, and the Send Shared functionality of Blockchain.info to attempt tracing their outputs back to their input accounts in a series of experiments. They identified that two of the services, Bitcoin Fog and Blockchain.info, successfully obfuscated their funds. They were successfully able to trace their BitLaundry outputs back to their original inputs using Blockchain.info's transaction graph functionality which has since been deprecated. In 2015, Novetta [21] conducted experiments with BitMixer, BitLaunder, Shared Coin, and Bitcoin Blender to identify provable links in mixing schemes, identify fingerprints of individual mixers, and identify if mixing can be detected on the blockchain. The study found fingerprinting patterns in the services based on recurring addresses, fees, and branching patterns. Balthasar and Hernandez-Castro [10] interacted with DarkLaunder, Bitlaunder, CoinMixer, Helix, and Alphabay and identified security and pri-

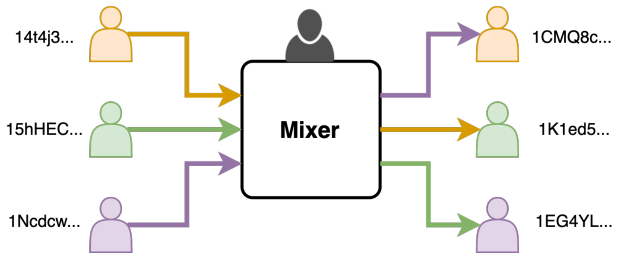

Fig. 1: High-Level diagram of a Bitcoin mixer with three participants and a centralized mixer run by an operator. The participants send their Bitcoin to the mixer. From its pool of collected Bitcoin, the mixer returns funds to participants' specified output addresses such that they are not returned their initial deposit.

vacy limitations in the services. Their work highlights the need for secure and privacy-aware protocols to improve the Bitcoin mixing ecosystem.

3 Bitcoin Mixers

Bitcoin mixers are services that offer the ability to obfuscate users' funds. Figure 1 depicts the general functionality of a mixer with three users. Each user sends their Bitcoins into the service and is returned another user's input to a different address. This output is associated with a completely different transaction history. The mixer operator runs the service and is aware of all connections (permutations) between inputs and outputs. Although this high-level view may seem easily traceable, mixers use obfuscation techniques that make it difficult to trace transactions and identify mixing service use on the blockchain.

Obfuscation Techniques. Since their inception, mixing services have adapted to threats stemming from transactional analysis. Traceable characteristics of transactions include the mixer's input address, the user's address, the amount sent to and from the service, and the timestamps of input and output transactions. The mixer input address is presented to the user to send their funds to the service. If the same input address was used for all users, it would be simple to identify mixing participants and the Bitcoin the mixer has in its pool. To avoid this, mixers generate new input addresses for each user. Additionally, the user's address could be traceable if kept consistent throughout the mixing interaction. Therefore, mixers allow their participants to specify multiple output addresses.

Patterns in amounts and timestamps of transactions could also indicate mixer use. Because network fees are public information, mixers add private, randomized mixing fees to each transaction. Additionally, mixing delays are used to make blockchain analysis more difficult. There are more than 300,000 Bitcoin transactions every 24 hours [8]. Thus, it is in mixing participants' best interest that delays are maximized. While the majority of services randomize fees and delays, some allow users to customize these features.

Threats. Trust is incredibly important for the success of a Bitcoin mixer. As third-party services, they must convince users that funds will be properly mixed and returned. Thus, mixers often offer features for users to check the status of their mix or proudly promote positive reviews from forum posts. Still, Bitcoin mixers are continuously accused of scams and poor implementation [7].

While mixers may pose threats to their participants' funds and anonymity, users and external attackers also contribute to the threat landscape. Some of the threats posed by users and external attackers, such as tracing transactions, are mitigated with obfuscation features. Others, such as coin theft, can be mitigated by the proposed mixer implementations that will be discussed in Section 4. The majority of current mixing implementations involve a centralized third party that is run by an all-powerful operator. The threats that are posed by this mixer operator are much more difficult to detect. In this paper, we focus our security analysis on the following threats presented by Tran *et al.* [23]:

Permutation Leak: An adversary is able to access mixing logs or a database pertaining to the permutation between input and output addresses.

Coin Theft: An adversary steals the input coins by providing users with an alternative address or by compromising the mixer's address. The mixer operator can also steal users' funds.

Dropping of Participants: A malicious mixer operator can deny participation to selected benign users to reduce the anonymity set.

Small Mixing Set Size: The mixing set size during each round is directly indicative of the quality of the mix. A large mixing set ensures anonymity and protection against blockchain analysis.

Join-then-abort: An adversarial participant disrupts the mix by aborting the mixing protocol before its execution.

4 Academic Mixing Techniques

In response to the threats facing Bitcoin mixers, the Bitcoin community and academic literature have proposed alternative methods to improve trust and eliminate threats. In this section, we discuss the general architecture of four decentralized and four centralized proposed mixing protocols.

4.1 Decentralized Mixing Protocols

The intrinsic anonymity in the Bitcoin ecosystem makes trusting a third party that runs a mixing service highly risky. Therefore, decentralized mixing protocols strive to avoid the use of a third party. Most of the following protocols assume a decentralized method for users to find other participants, which is called *bootstrapping*. Generally, decentralized protocols suffer from limited scalability and long wait times to find mixing peers.

CoinJoin. CoinJoin is a method for multiple transactions from multiple senders to be combined into one transaction [15]. Without any modification to the current Bitcoin protocol, this technique makes it difficult for outside entities to

identify the corresponding recipient for each input. Users may collaborate to identify a uniform output amount and combine their transactions into one. In turn, senders face lower transaction fees and lessen the transactions on the Bitcoin network. Additionally, participants of CoinJoin transactions do not face risk of theft: each participant must sign the transaction before it is considered valid.
CoinShuffle. Ruffing *et al.* presented CoinShuffle in 2014 [22]. The mixing protocol requires no third party, is compatible with the existing Bitcoin network, and uses CoinJoin to execute transactions. The protocol assumes that users have a secure, decentralized method to express their interest in participation. Output address shuffling and a final CoinJoin transaction eliminate the risk of permutation leak and coin theft attacks.
CoinParty. Ziegeldorf *et al.* proposed CoinParty, a mixing protocol with multiple one-to-one transactions to and from escrow addresses [25]. While compatible with the existing Bitcoin network, CoinParty uses secure multi-party computation for users to collaborate. Temporary threshold ECDSA escrow addresses eliminate the risk of coin theft if 2/3 of the participants are benign users. Similar to CoinShuffle, output addresses are shuffled to avoid permutation leaks.
Xim. Bissias *et al.* explored the threats presented by Sybil-based denial-of-service attacks to Bitcoin mixing services. They present Xim, a two-party mixing implementation [11]. Unlike the previously described methods, Xim provides a decentralized method for finding mixing participants. Joining a mix interaction requires both participants to spend funds. The requirement to pay to advertise and respond to desired mixing partners make Sybil attacks difficult.

4.2 Centralized Mixing Protocols

Centralized mixing protocols aim to secure a scheme where an untrusted third party exists, and participants send their funds through these centralized services.
Obscuro. Tran *et al.* presented a centralized Bitcoin mixer using Trusted Execution Environments (TEEs) [23]. Obscuro addresses the threats posed by mixing operators to lessen the control they have on the functionality and day-to-day activity of the service. To do so, the mixer codebase is isolated from the rest of the system. Users are given the ability to verify the isolated functionalities using remote attestation and are guaranteed a large mixing set size. Obscuro's implementation requires no changes to the existing Bitcoin network and is generic such that it can be implemented with any TEE technique.
Mixcoin. Bonneau *et al.* propose Mixcoin, a Bitcoin mixing protocol that provides accountability to expose malicious centralized mixers [12]. To do so, signed warranties are implemented between the participants and the service. If any wrongdoing occurs on the mixer's part, users have proof of an agreement between both parties to post on public forums. Warranties can be verified by publicly available information such as transactions or public keys. Thus, Mixcoin provides an incentive for mixers to operate in a trustworthy manner. The protocol assumes there are various mixers M_i, and each mixer has a warranty signing key K_{M_i} which is consistently used to sign warranties with each participant.

Thus, the mixer's reputation relies heavily on the use of their key. Although accountability is achieved, the mixer can steal funds from its users and potentially leak permutations between inputs and outputs.

Blindcoin. Valenta and Rowan address Mixcoin's susceptibility to permutation leak attacks with Blindcoin [24]. Without any changes to the existing Bitcoin protocol, a blind signature scheme and an append-only public log are added onto the Mixcoin protocol. The user includes a blinded token consisting of their output address and a nonce in their initial offer to the mixing service. The use of this token eliminates the threat of a permutation leak attack by the mixer operator. In addition, the mixing service is required to post this blinded token to an append only public log. As a result, Blindcoin ensures accountability while keeping the mapping of input to output addresses secret. However, Blindcoin does not prevent coin theft since the mixer can still steal funds from its users.

TumbleBit. Heilman *et al.* present TumbleBit, a unidirectional and unlinkable payment hub protocol [16]. TumbleBit is completely compatible with the current Bitcoin protocol and relies on an untrusted centralized intermediary $\mathcal{M}$ to transfer funds between users. TumbleBit's transactions are sent off-blockchain and are not affected by the latency issues in Bitcoin. These payments are essentially off-blockchain puzzles generated through interactions with $\mathcal{M}$.

5 Public Mixing Services

Today's most popular Bitcoin mixing services are centralized to avoid scalability and participant bootstrapping issues inherent in decentralized methods. To begin our analysis of the current mixing service landscape, we first gathered a list of centralized mixers. The majority of these mixers were posted as service announcements on Bitcointalk, a key forum for Bitcoin-related discussions. Appendix A outlines the characteristics we collected for each mixing service. Our findings are displayed in Table 1 with some of these characteristics omitted for simplicity. A ✓ signifies that the service offers the feature while a ✗ indicates lack of the feature. Any field marked with a dash was not found or not applicable to the service. Note that the information presented is solely based on the data that is available on each mixer's website and does not involve any actual transactions.

Popularity Analysis. Our next step was to identify a metric to rank mixing services based on popularity for in-depth analysis. As seen in Table 1, every mixing service has a Tor mirror that is highly recommended. These sites have a `.onion` extension and cannot be indexed by standard search engines. As a result, identifying the amount of traffic for each service is quite difficult.

To address this obstacle, we first categorized mixers into two categories: Trusted and Untrusted. We based this categorization on service support and user activity on the Bitcointalk forum. Trusted mixers displayed consistent communication with an active user base on the forum and had zero scam accusations at the time of the study. Untrusted mixers displayed a lack of communication with their users and had one or more scam accusations. Any mixer without

	Mixer	Year	Account	Mixing Fees	Distribution Control	Delay	Multiple Output Addr	Multiple Input Addr	Tor	Clearnet	Bitcointalk	Open Source	Min. Blocks	Forum Posts	Scam Accusation(s)
Trusted	Samourai Whirlpool	2015	✗	✓	✓	✗	✓	✗	✓	✓	✗	✓	-	-	-
	CryptoMixer	2016	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	1	356	✗
	Mixer.money	2016	✗	✓	✗	✓	✓	✗	✓	✓	✓	✗	-	151	✗
	BitCloak	2016	✗	✓	✗	✓	✓	✗	✓	✓	✓	✗	1	174	✗
	ChipMixer	2017	✗	✗	✓	✓	✓	✗	✓	✓	✓	✗	1	1887	✗
	BitMix.biz	2017	✗	✓	✗	✓	✓	✗	✓	✓	✓	✗	1	147	✗
	FoxMixer	2017	✗	✓	✓	✓	✓	✗	✓	✓	✓	✗	6	39	✗
	Wasabi Wallet	2018	✗	✓	✗	✗	✓	✗	✓	✓	✗	✓	-	-	-
	MixTum	2018	✗	✓	✗	✓	✓	✗	✓	✓	✓	✗	1	99	✗
	Bitcoin Mixer	2019	✗	✓	✓	✓	✓	✗	✓	✓	✓	✗	1	108	✗
	Sudoku Wallet	2019	✗	✓	✗	✓	✓	✗	✓	✓	✓	✗	3	68	✗
Untrusted	Bitcoin Fog	2011	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	6	647	✓
	PenguinMixer	2017	✗	✓	✗	✓	✓	✗	✓	✗	✗	✓	2	-	-
	Blender.io	2017	✗	✓	✗	✓	✓	✗	✓	✓	✓	✗	3	103	✓
	BMC Mixer	2017	✗	✓	✗	✓	✓	✓	✓	✗	✓	✗	2	2	✗
	SmartMix	2019	✗	✓	✓	✓	✓	✗	✓	✓	✓	✗	3	170	✓
	Mixer Tumbler	2019	✗	✓	✗	✓	✗	✗	✓	✓	✓	✗	3	17	✗
	AtoB Mixer	2019	✗	✓	✗	-	✓	✗	✓	✓	✓	✗	-	102	✓
	Anonymix	2020	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	1	-	-
	BlockMixer	2020	✗	✓	-	-	✗	✗	✓	✓	✓	✗	3	1	✗
	DarkWeb Mixer	-	✗	✓	✗	-	✓	✗	✓	✗	✗	✗	-	-	-

Table 1: The inclusion of various Bitcoin mixer features on current Bitcoin mixing services. This data is based solely on publicly available information on the mixer's website or Bitcointalk forum posts and does not involve any transactions. Furthermore, the mixers are categorized as Trusted or Untrusted based on their standing and activity on the Bitcointalk forum.

a service announcement on Bitcointalk or an inactive open-source community was also marked as Untrusted due to a lack of information from its user base. The only exceptions to this categorization were Samourai Wallet's Whirlpool and Wasabi Wallet. Although these services do not have Bitcointalk service announcements, they were categorized as Trusted due to their active community and open-source implementation.

After analysis of forum posts, 11 mixers were Trusted and 10 were Untrusted. We chose five web-based Trusted services for in-depth analysis: ChipMixer, MixTum, Bitcoin Mixer, CryptoMixer, and Sudoku Wallet. These services were chosen based on their popularity and unique features. We did not select any Untrusted mixing services for this in-depth analysis due to ethical concerns.

ChipMixer was established in 2017. With over 95 pages of Bitcointalk forum posts and no scam allegations, the service is the most popular mixer. ChipMixer is a unique implementation with the introduction of *chips*. It generates addresses and funds them with increments of 0.001 BTC up to 8.192 BTC. These addresses are provided to ChipMixer's participants along with their corresponding private keys as outputs. Rather than executing on-blockchain transactions, users are expected to import the given private keys to their wallets off-blockchain. Thus, there is no link between funds deposited to ChipMixer and the chips given to participants. Users may split, merge, even *bet or donate* the given chips before withdrawal using the corresponding private keys. These features can be used multiple times, in any order, and on individual chips.

While ChipMixer does not require an account, users are given a session token and an input address that lasts for seven days. The service also gives users the option to destroy their sessions prematurely within this seven-day period, and service logs are kept for the same length. Mixing fees are purely donation-based and users may choose to donate any amount of their given chips. On withdrawal, users are given a cryptographically signed receipt proving that the funds are coming from ChipMixer. Additionally, users are given the option to receive a voucher code and use the non-withdrawn chips in other ChipMixer interactions.

MixTum was established in 2018. The service claims to have a separate pool of Bitcoin from cryptocurrency stock exchanges such as Binance, OKEex, and DigiFinex. MixTum guarantees that participant funds are not mixed within a pool of other user's Bitcoin and instead outputs are from exchanges.

MixTum is a traditional Bitcoin mixer that sends on-block-chain transactions to return participant funds. Mixing fees are up to 5% (randomized) plus 0.00015 BTC for the output network fee. Users can specify up to two output addresses which receive multiple payments when funds are returned. The number of payments and distribution of funds between these addresses is randomized by the service. In addition, randomized delays of up to six hours are implemented on output transactions. MixTum provides users with a PGP signed letter of guarantee with information regarding the mixing interaction.

MixTum offers a free trial with the minimum required amount of 0.001 BTC, one output address, and no mixing fees. Although MixTum claims logs are not kept, they do keep data regarding participant interactions until the completion of the output transaction or until the session expires in seven days.

Bitcoin Mixer was established in 2019. The service provides its users with a Mix ID to check the status of their mix. The minimum input amount accepted is 0.0002 BTC. When multiple output addresses are specified (up to seven), users can control the distribution and delays for each. Delays for each output address range from less than one hour (rapid) to 12 hours. The service keeps logs for up to seven days but gives users the option to manually delete their session details. The mixing fees for Bitcoin Mixer are 0.25% plus 0.000001 BTC per output.

CryptoMixer was established in 2016. The service's initial announcement on Bitcointalk stated that it has over 2,000 BTC in reserve. CryptoMixer leveraged the trust of reputable Bitcointalk users to verify the services pool of funds [2–4].

CryptoMixer allows a minimum input of 0.001 BTC. The maximum input changes based off of the amount of Bitcoin in its reserve. Accounts are not required, and instead users are given a CryptoMixer code to identify their sessions. This code can be used in future sessions to receive discounts and ensure previous inputs are not returned. CryptoMixer's site claims it has a 100% zero-logs policy but also states that transaction details are routinely deleted. Based on the fees, delays, distribution, and number of output addresses set, participants are given a security level for their mix. The Standard, Silver, and Gold security levels offer higher thresholds for obfuscation. For example, the Standard level offers up to 24-hour delays while Gold offers up to 96 hours.

Unlike the other services, CryptoMixer allows users to generate an unlimited number of input addresses to send their funds. Each input address also comes with a verifiable, digitally signed letter of guarantee, proving that it was generated by the service. Each given address is valid for 24 hours.

Sudoku Wallet was established in 2019. The service is a single-use wallet which outputs private keys rather than on-blockchain transactions. These outputs are of two to four addresses funded from previously executed CoinJoin transactions. The distribution between these addresses is not configurable by the user. There is no minimum or maximum input enforced. Sudoku Wallet does not require accounts but provides users with a wallet key to access their session before it is automatically deleted in seven days. The service claims to have a strict "no logs" policy. To send funds to Sudoku Wallet, one input address is provided along with its corresponding private key. The mixing fee is randomized from 0.5% to 1% plus the CoinJoin fee which is described as the number of output addresses involved in the CoinJoin times the transaction fee.

6 Evaluation

In this section, we describe the methodology of our in-depth experiments on five chosen mixers to understand more about the implementation of these mixer services. In addition, we outline our results of the experiments conducted with each mixer. Detailed results are included in Appendix B with transaction IDs.

6.1 Methodology

The experiments are real-world interactions with five public mixing services: ChipMixer, MixTum, Bitcoin Mixer, CryptoMixer, and Sudoku Wallet. Our goal is to identify if these mixers have adopted implementation and security solutions provided by the academic literature discussed in Section 4. Overall, we use data from Table 1 and our experiments to compare implementation and security of the five services with the proposed mixing protocols from Section 4.

We conducted three trials of experiments: each consisted of one transaction with each of five mixing services. We ensured that all five interactions during a trial were finished before moving onto the next. To estimate the necessary amount of funds to execute all 15 mixer interactions, we set a constant network

Data Field	Description
Obfuscation Parameters	Obfuscation features set (number of output addresses, delays, distribution, etc.)
Input Amount	Amount sent to mixer (before network fees)
Input Network Fee	Network fee on transaction to mixer (BTC)
Input Address	Address given to user by mixer to send initial funds
Time In	Date and time of input transaction
Input Transaction ID	Transaction ID of input transaction
Output Amount	Amount sent back to user's deposit address(es)
Output Network Fee	Amount of network fees on transaction(s) to deposit address(es)
Time Out	Date and time output transactions are sent from mixer
Output Transaction ID	Transaction ID of output transaction
Mixer Fee	Service fee collected
Additional Information	Information unique to service: Letter of Guarantee, Special Mixing Code, Receipt, etc.

Table 2: Data collected during our experiments with each studied mixer along with their description.

fee of 0.50 USD (0.000053 BTC) and calculated the worst-case mixing fees for each service. The total fees were estimated to be 57.25 USD (0.00635 BTC). To account for changing network fees, unexpected mixer fees, or coin theft, we determined 100 USD (0.011 BTC) would be sufficient to execute all three trials.

During the first trial, input amounts were set to the minimum required by each service. Inputs were gradually raised in the second and third trials. We increased the obfuscation parameters from trial to trial when customizable. This included longer delays, a higher number of output addresses, and higher fees. The public nature of the blockchain allowed for comparison between interactions with a single service to identify unexpected behavior. We specify the exact parameters, input, and output values for each trial in the results for each service and Appendix B. To calculate the mixing fees for on-blockchain transactions the total BTC sent to and from the mixing service (excluding network fees) were subtracted.

All five mixers offer a Tor mirror, so we used the Tor Browser. To store, receive, and send Bitcoin, we used the desktop wallet Electrum. We maintained two separate wallets for legacy and SegWit functionality. All transactions were labeled according to their corresponding mixer and trial number. In addition to collecting screenshots of every mixing interaction, the data described in Table 2 was recorded. This includes transaction information such as the input and output transaction IDs, the obfuscation parameters, and unique information for each service including letters of guarantee. Next, we will discuss the general steps taken and any special data collected for each service.

Setup. Before beginning the first trial, we purchased 100 USD worth of Bitcoin from the exchange Coinbase. At the time, this equated to 0.01788742 BTC. Then, we created two separate Electrum wallets: Legacy and SegWit.

ChipMixer. There are five general steps in interactions with ChipMixer. During Step 1, users are given their session token and told to save it permanently to

access their session for the next seven days. Step 2 is the Deposit step: send at least 0.001 BTC in one transaction to a given input address, wait for one network confirmation on this transaction, and then refresh the page. During this step, users are also able to enter voucher codes from previous interactions to use funds that have not been withdrawn. At Step 3, users have a full view of their current chips grouped by value and have the ability to split, merge, commonize, bet, and donate. On this page, they are also given the option to withdraw or receive a voucher for chips. These two options directly lead to Step 4, the withdrawal. Users are given the private key to their withdrawn chips and steps on how to import this key to Electrum, Bitcoin Core, or to a JSON file. As another option, they can sweep the chips to a desired output address. Before the final step, a signed receipt is offered for download. In Step 5, sessions can be destroyed.

We created a new session for each trial with ChipMixer. The session token was recorded to test its validity after the seven-day period or after sessions were manually deleted. The given input address and the input transaction ID was noted to identify patterns in the movement of funds. Chipmixer's method of returning funds does not involve output addresses, so we used the SegWit wallet for all three trials. We considered the obfuscation parameters for ChipMixer to be the set of features used (split, merge, and donate) as well as the method of withdrawal. Commonize and betting were not used in all three trials. We attempted both sweep and private key transfer withdrawals to identify effects on traceability. Before destroying each session, we attempted to access each session's signed receipt to verify the signature.

Results. The results from each ChipMixer trial are displayed in Appendix B Table 6. In our trials with ChipMixer, we did not encounter any unexpected mixing fees. In Trial 1, we swept the private keys to our Electrum wallet with an on-blockchain transaction (requiring network fees). In Trial 2, we transferred the private keys to our Electrum wallet off-blockchain (no network fees). In all three trials, we could not access the signed receipt offered by ChipMixer due to an internal server error.

MixTum. In MixTum for Step 1, users enter up to two output addresses. In Step 2, users are given an input address along with its corresponding QR code. In addition, a signed letter of guarantee is provided for download.

Trials for MixTum were attempted with both legacy and SegWit addresses. The only customizable obfuscation parameter was the number of output addresses. On Step 2, all letters of guarantee were downloaded and signatures were verified using GnuPG. Transactions from MixTum were analyzed for their distribution and randomized delay. Mixing fees were also checked to see if they were accurately calculated. Input and Output transaction IDs were used to gain insight about the movement of funds.

Results. Table 7 in Appendix B displays the obfuscation parameters, total input, total output, output network fees, and mixing fees pertaining to each trial with MixTum. For all three trials, signed letters of guarantee were successfully downloaded and verified. MixTum's calculator output displayed a smaller value

than received on all three trials. In Trials 2 and 3, mixing fees were up to 5% plus 0.00015 BTC as advertised. However, Trial 1 charged a mixing fee of 0 BTC.

Bitcoin Mixer. In Step 1, users specify up to seven output addresses each with distribution (%) and delay (rapid to 12 hours). In Step 2, the service provides a Mix ID and an input address. After delays, the output transactions are executed. In Step 3, users review their mix information and can delete their mix.

In Step 1, we attempted specifying both legacy and SegWit addresses to Bitcoin Mixer. The main obfuscation parameters for this service were the number of output addresses, percentage distribution, and delay. We heightened the intensity of these parameters from trial to trial and verified the accuracy of distributions and delays. Mix IDs for each session were noted to check their validity after deletion of the mix. After receiving outputs, we calculated the mixing fees to identify unexpected behavior. In all three trials, we deleted our mix information.

Results. Table 8 in Appendix B outlines the obfuscation parameters, input, output, and mixer fees associated with each Bitcoin Mixer trial. The distributions, mixing fees, and outputs were accurately calculated. Outputs were generally received 20 to 30 minutes early, indicating randomization of delays. The deletion of Mix IDs was successful in all three trials.

CryptoMixer. In Step 1, users specify up to 10 output addresses and set the delay and distribution for each. Users can then specify their preferred service fee. The combination of these three obfuscation parameters determines the security level of the mix. On the same page, CryptoMixer's calculator displays the expected amount that each output address will receive. Before continuing to Step 2, the CryptoMixer code can be entered. In Step 2, a letter of guarantee is presented along with an input address. As input transactions are made the service displays the received amounts and their confirmations. If the amount is not sufficient, the service specifies the expected output as a negative value. Finally, users are also provided with a CryptoMixer code to use with future transactions.

Trials with CryptoMixer were conducted with both legacy and SegWit addresses. The customizable obfuscation parameters for this service include the number of input and output addresses, delay, distribution, and service fee. While Trial 1 was customized to fall under the Standard security level, Trial 2 and 3 were both set to the Silver security level. We recorded the output values displayed from the service's calculator to check for accuracy. The CryptoMixer code from Trial 1 was used in Trial 2 to test its effectiveness against receiving previous inputs. Finally, the letter of guarantee was downloaded for each input address in all three trials and both the signature and contents were verified.

Results. Appendix B Table 9 displays the obfuscation parameters, input, output, and mixer fees associated with each CryptoMixer trial. The service's calculator displayed accurate outputs based on the set mixing fee for each trial. We did not receive any output from CryptoMixer on Trials 2 and 3. We were successfully able to download and verify the letters of guarantee provided by the service. Additionally, we received five-digit CryptoMixer codes in each trial but could not evaluate the effectiveness of their use.

Sudoku Wallet. In Step 1, users are presented with a wallet key. In Step 2, an input address is presented along with its corresponding private key. After three confirmations on the input transaction(s), the user can proceed. In Step 3, two to four addresses with balances adding up to the user's input amount minus mixing fees are presented along with their private keys. The user then has the option to sweep these funds or import the private keys to their wallet. In Step 4, users are urged to delete their wallet and generate a new one to mix more funds.

We created a new wallet for each transaction and recorded the wallet key to check its validity after deletion. In Step 2, we noted the input address and its private key. The obfuscation parameter for Sudoku Wallet is limited to the method of withdrawing the funds. In Step 3, we recorded the given output addresses and calculated the mixing fee to identify unexpected behavior. We studied the history of these output addresses to ensure they used CoinJoin transactions.
Results. Appendix B Table 10 displays the obfuscation parameters, input, output, output network fees, and mixer fees associated with each Sudoku Wallet trial. Mixing fees for each trial were inconsistent and unverifiable with any previously executed CoinJoin transactions. Trial 1 had a mixer fee of 0 BTC while Trial 3 had a fee of 0.0027 BTC (90% of the input).

7 Analysis

In this section, we provide an implementation and security analysis of the five public mixing services.

7.1 Implementation Analysis

We use the data gathered in Section 5 regarding current public mixers and our experiments (discussed in Section 6) to identify the adoption of academically proposed solutions in ChipMixer, MixTum, Bitcoin Mixer, CryptoMixer, and Sudoku Wallet.

Table 3 outlines which mixing services include key characteristics of proposed solutions in their implementation. The characteristics selected include CoinJoin, shuffling of output addresses in one transaction, multisignature escrows, TEXT field use to share data, signed warranties, blinding, and off-blockchain transactions. Each of these characteristics are used in at least one of the academically proposed solutions.
ChipMixer. Through tracing our input transactions and outputs received by ChipMixer, we identified that funds sent to the service are routinely involved in the creation of chips ranging from 0.001 BTC to 8.192 BTC. For example, our Trial 1 input of 0.001 BTC was involved in the creation of five chips of 8.192 BTC. The creation involves a CoinJoin transaction with UTXOs sent to ChipMixer by users as its input set. The output is a set of chips of a uniform size. Unlike CoinShuffle, this CoinJoin is solely created with funds available in ChipMixer's wallet. Thus, the need for multiple signatures and shuffling of output addresses is eliminated.

	CoinJoin [15, 22]	Output Address Shuffling [22, 25]	Multisig Escrow [16, 25]	TEXT Field Use [11, 23]	Remote Attestation [23]	Signed Warranty [12, 24]	Blinding [16, 24]	Off-Blockchain Txns [11, 16]
ChipMixer	✓	✗	✗	✗	✗	✗	✗	✓
MixTum	✗	✗	✗	✗	✗	✓	✗	✗
Bitcoin Mixer	✗	✗	✗	✗	✗	✗	✗	✗
CryptoMixer	✗	✗	✗	✗	✗	✓	✗	✗
Sudoku Wallet	✗	✗	✗	✗	✗	✗	✗	✓

Table 3: The inclusion of academically proposed techniques in the five studied public mixers. The five mixers exhibit a lack of adoption of proposed techniques. Output address shuffling, multisignature escrows, the use of TEXT fields in transactions, remote attestation, and blinding are not implemented by any of the services studied.

ChipMixer incorporates off-blockchain transactions by giving users the option to split, merge, bet, commonize, and donate their given chips. These options have an impact on the amount and distribution of the mix without executing multiple on-blockchain transactions. The withdrawal of funds via importing private keys is also done off-blockchain. Thus, a complete ChipMixer mixing interaction can be done with only one on-blockchain input transaction. This is comparable to TumbleBit and its incorporation of off-blockchain puzzles to send Bitcoin between two users.

ChipMixer claims to provide a signed receipt on withdrawal of chips. Although the service was unable to provide this receipt in all three trials, we do not believe it is comparable to the signed warranties produced in Mixcoin and Blindcoin. While ChipMixer's signed receipt aims to prove the origin of output funds, Mixcoin and Blindcoin's signed warranty outlines the terms of the mix before any input or output.

Overall, our analysis did not provide any evidence that ChipMixer implements signed warranties, blinding, remote attestation, output address shuffling, or multisignature escrow addresses.

MixTum. MixTum offers a PGP signed letter of guarantee before any inputs to the service. The letters for all three trials included the generated input address, the output address(es), the maximum mixing time, the deadline for users to send their input by, and the maximum service fee. This guarantee can be compared to the signed warranty provided in Mixcoin which includes the value to be mixed, the deadline for the input to be sent, the deadline for the service to return

funds, the output address, the mixing fee rate, a nonce, and the number of confirmations required on the input. Mixcoin's protocol requires that users create the terms of the mix and provide them to the service. In the case of MixTum, the service creates the majority of the terms including the fee and deadline to return funds. Overall, the PGP signed letter of guarantee from MixTum provides enough information to identify a breach in protocol and holds the service accountable.

We did not identify any evidence that MixTum incorporates CoinJoin, output address shuffling, multisignature escrow addresses, TEXT field use, remote attestation, blinding, or off-blockchain transactions.

Bitcoin Mixer. Through our analysis and experiments with Bitcoin Mixer, we identified that the service does not implement any of the proposed mixing solutions found in CoinShuffle, CoinParty, Xim, Obscuro, Mixcoin, Blindcoin, or TumbleBit. The service does not implement CoinJoin transactions or shuffle output addresses of multiple users in one transaction. In addition, Bitcoin Mixer does not implement multisignature escrow addresses, TEXT fields in transactions, remote attestation, a signed warranty, blinding, or off-blockchain transactions.

CryptoMixer. CryptoMixer provides a signed letter of guarantee along with each input address. Unlike MixTum, CryptoMixer's letter of guarantee is signed using its Bitcoin private key. This letter provides confirmation of the origin of the input address, distribution of funds to each output address, delay for each output address, deadline for inputs, minimum and maximum input allowed, and mixing fee. This guarantee can be compared to the signed warranty provided in Mixcoin. In this case, the user specifies output addresses, delays, distributions, and the fees. Thus, CryptoMixer's letter of guarantee ensures accountability and can be used against the service in case of a breach of protocol.

Overall, the signed warranty was the only academically proposed solution adopted by CryptoMixer. We did not identify any evidence of CoinJoin, output address shuffling, multisignature escrow addresses, TEXT field use, remote attestation, blinding, or off-blockchain transactions.

Sudoku Wallet. Sudoku Wallet claims to provide funds from pre-mixed CoinJoin transactions. Blockchain analysis in all three trials revealed that inputs were not involved in uniform output CoinJoin transactions after being sent to the service. Additionally, outputs had not been involved in uniform output CoinJoin interactions in recent history. Thus, we do not believe the service uses CoinJoin transactions. However, Sudoku Wallet does make use of off-blockchain transactions on withdrawal. Like ChipMixer, the use of private keys as outputs ensures that outputs are not detectable on the blockchain.

Overall, we did not identify any evidence of CoinJoin transactions, output address shuffling, multisignature escrow addresses, TEXT field use, remote attestation, signed warranties, or blinding.

7.2 Security Analysis

We build our security analysis upon Obscuro's security analysis performed on CoinJoin, CoinShuffle, CoinParty, Xim, Mixcoin, Blindcoin, and TumbleBit [23].

	Coin Theft Prevention	Relationship Anonymity	Participation Guarantee	Large Mixing Set Guarantee	Join-then-abort Resistance	Minimum On-Chain Txns
ChipMixer	✗	✗	✗	✗	✓	1
MixTum	✗	✗	✗	✗	✓	2
Bitcoin Mixer	✗	✗	✗	✗	✓	2
CryptoMixer	✗	✗	✗	✓	✓	2
Sudoku Wallet	✗	✗	✗	✗	✓	1

Table 4: A security comparison of the five public mixing services against the threats presented in Section 3. All five services lack prevention against coin theft, relationship anonymity attacks, and do not guarantee participation. A similar table conducting a security comparison of academically proposed mixers is provided in OBSCURO [23].

We expand on their academically proposed Bitcoin mixer comparison by performing similar analysis on the five mixing services included in this study. Table 4 displays the results of this analysis. We compare the mixers based on their resistance to the threats outlined in Section 3.

Coin Theft. The five mixers in the study do not have protections in place against coin theft. ChipMixer, Bitcoin Mixer, and Sudoku Wallet provide no proof of origin for the provided input address, making it possible for adversaries or malicious mixer operators to steal funds. MixTum and CryptoMixer provide signed letters of guarantee, making it difficult for an attacker to inject their own address. However, the letter of guarantee is ineffective against malicious mixer operators. Although it sets accountability, users can still have their funds stolen. Mixcoin and Blindcoin suffer from the same protections against a malicious operator. Thus, six out of eight mixing services in OBSCURO's analysis implement protections against coin theft. For example, CoinJoin, CoinShuffle, and TumbleBit use multisig addresses to ensure all parties are involved in the movement of funds.

ChipMixer and Sudoku Wallet provide private keys as outputs. Importing these keys to a wallet may be appealing because of its off-blockchain nature, however it leaves users susceptible to coin theft. The mixing service could still access the private key and sweep the funds to a separate address without user permission.

Relationship Anonymity. Relationship anonymity is not guaranteed in any of five mixing services. Malicious mixing operators can directly learn the permutation between inputs and outputs. Additionally, all five services store or log

session data for at least a limited amount of time, providing a tempting target for adversaries. In comparison, five out of eight proposed mixing services from Obscuro's analysis provide a method to ensure relationship anonymity. For example, CoinParty and CoinShuffle use output address shuffling while Blindcoin and TumbleBit use blinding.

Participation Guarantee. All five public mixers lack resistance against dropping participants. This is common in protocols that involve a mixer operator who can control the mixer's worldview. In comparison, five out of eight protocols studied in Obscuro's analysis guarantee participation for all users. The only centralized protocol included in these five is Obscuro. In its implementation, selective dropping of participants results in a DoS attack because of the protocols dependence on public bulletin boards.

Large Mixing Set Guarantee. Of all five services, CryptoMixer was the only to guarantee a large mixing set size. For public mixing services, we view the mixing set to be the pool of UTXOs that the mixing service controls. To guarantee a large mixing set, CryptoMixer provided reputable Bitcointalk users with access to a list of their owned addresses along with signatures for each. The users confirmed that the service had nearly 2,000 BTC in their pool. In comparison, two out of eight proposed services provide a guarantee of a large mixing set. For example, Obscuro refunds user inputs when a minimum number of participants is not reached. Mixcoin, Blindcoin, and TumbleBit do not include an agreement of a minimum mixing set size in their centralized protocols. In decentralized protocols such as CoinJoin, CoinShuffle, and CoinParty, users are guaranteed a small set due to the communication overhead and long wait times with larger anonymity sets.

Join-then-abort Resistance. All five public mixing services provide resistance against join-then-abort attacks. Users are unable to abort the mixing protocol after funds have been sent to the given input address. In comparison, five out of eight proposed protocols also provide resistance against this attack. In CoinJoin implementations, like CoinShuffle, users are able to disrupt the mix by disapproving of the final transaction.

Minimum On-Chain Transactions. The number of on-block-chain transactions for the five mixers in this study is similar to the proposed protocols in Obscuro's analysis. Aside from Xim, which requires three ads on-blockchain before the four transactions in Barber's Fair Exchange, and TumbleBit, which uses two escrow channels, the proposed protocols require one to two transactions.

7.3 Additional Interesting Behavior

Our experiments on ChipMixer, MixTum, CryptoMixer, and Sudoku Wallet revealed additional, interesting behavior associated with each service. We believe these behaviors represent an opportunity for a long-term study to learn more about the underlying service implementation.

ChipMixer. ChipMixer generates new chips by creating CoinJoin transactions with uniform output chip values ranging from 0.001 BTC to 8.192 BTC. The set of inputs for these chip generation transactions is comprised of UTXOs adding

up to the exact amount necessary to create the specified number of chips. In turn, chip generation does not include change transactions in its output. We identified this pattern in all four of our input transactions with ChipMixer. Additionally, we were able to trace these created chips to identify outputs to other users. It is possible that a large number of inputs could be sent to ChipMixer to gain a better understanding of their pool of chips. Appendix C provides some example chip generation transactions.

Although ChipMixer claims logs and session information is deleted in seven days, we found that our session tokens for all three trials were still valid after 16 days. This could indicate that deletion of logs and session tokens is manually done by the mixer operator.

ChipMixer incorporates various features that focus on providing users with an illusion of control over their funds. However, off-blockchain transactions such as split and merge essentially have no impact on the chips available in ChipMixer's pool. In addition, voucher codes carry no value outside of the service.

MixTum. MixTum is built upon Jambler.io, a mixing platform that provides the source code to start a mixer. The letter of guarantee and the input address are generated from Jambler.io, and the platform pays MixTum a commission on completion of each mixing interaction. Jambler.io claims to obtain funds from cryptocurrency exchanges and use a scoring algorithm to only mix with "pure" funds.

MixTum's typical mixing fees are up to 5% + 0.00015 BTC. However, in Trial 1 we sent the minimum 0.001 BTC, we received an output of 0.001 BTC. The transaction fee on this output was 0.00024227 BTC. Thus, the service did not charge a mixing fee and lost money. This was tested twice with the same result.

CryptoMixer. CryptoMixer returned an output in Trial 1 even though the service stated that the input amount was less than required. In Trial 2, we identified that the service does not accept transactions less than the minimum 0.001 BTC. However, CryptoMixer's calculator still recognizes inputs less than the minimum and calculates accordingly. We believe CryptoMixer treats all inputs to a session as donations if an input less than the minimum is detected before an output transaction is scheduled. The first three inputs for Trial 2 were 0.001 BTC, 0.001 BTC, and 0.0005 BTC. All three received their first confirmation at the same time. We believe CryptoMixer recognized that one of these inputs was less than 0.001 BTC and treated all inputs as donations as a result. In Trial 3, we learned that input addresses do not accept more than one transaction. Our second transactions were not recognized and CryptoMixer did not send an output. Overall, CryptoMixer has poor implementation and lacks proper documentation.

Sudoku Wallet. On the presentation of the input address, Sudoku Wallet also provides a corresponding private key. We believe this is done to give users the illusion that they still have access to their funds. However, in all three of our trials, Sudoku Wallet moved the funds associated with the input address before we obtained our output. For example, in Trial 1, we swept our outputs at 12:51

AM, however the input address funds had been moved to a separate address at 12:33 AM. This shows how simple coin theft is when mixers output private keys.

Sudoku Wallet's mixing fees are described as 0.5% to 1% (randomized) plus the CoinJoin fee. However, mixing fees were inconsistent in all three trials. We were not able to identify any CoinJoin transactions to calculate the fees in each output's blockchain history. Thus, more transactions will need to be executed to understand the mixing fees.

During Trial 3, the provided wallet key was entered onto the Sudoku Wallet website. We received an error stating that the Bitcoin Client function `loadwallet()` verification failed. This error reveals that Sudoku Wallet creates a new wallet for each user to keep track of balances. This is the only implementation of separate wallet creation. Although Sudoku Wallet states that logs are not maintained, this is similar to logging transaction data for each participant.

8 Discussion and Limitations

Our analysis shows a clear disconnect between the five publicly available mixers studied and academically proposed solutions. Key characteristics of these solutions have not been widely adopted by today's most trusted Bitcoin mixing services. We found that none of the five public mixing services we tested use the proposed features of output address shuffling, multisignature escrow addresses, TEXT fields in transactions, remote attestation, or blinding. The only three characteristics adopted include CoinJoin, signed warranties, and off-blockchain transactions.

All five mixers performed poorly in security analysis. The lack of prevention against coin theft, permutation leaks, and dropping of participants in public services shows that these services are not built to prioritize security and anonymity concerns addressed in academic literature. Rather, most services appear to be focused on providing their users with the illusion of control over their mix. On a positive note, centralized mixers displayed complete resistance against join-and-abort attacks, unlike proposed decentralized solutions. CryptoMixer also leverages Bitcointalk to guarantee a minimum mixing set size.

To gain credibility and trust from their users, today's mixers must employ a combination of key characteristics provided by proposed academic solutions. Public mixing services should advertise the use of proven solutions from academic literature, use trusted third-party remote attestation services, provide signed letters of guarantee, and adopt open-source practices. Mixers should also aim to leverage the solidified trust users have with reputable members of Bitcointalk and actively engage with their participants. Output addresses can be encrypted with the mixer's public key and included in the TEXT field of input transactions to lessen the threat of selective dropping of participants. Although it would result in higher network fees, mixers should identify a minimum mixing set size and ensure outputs include multiple users rather than one-to-one transactions. The use of private keys as outputs must be eliminated from services to ensure safety against coin theft.

Ultimately, our trials were quite lightweight. A higher number of trials with larger transactions could lead to a more in-depth understanding of the reasoning behind certain mixer behavior. Our understanding of mixer features relies heavily on information collected from each service's website as well as posts from Bitcointalk. A long-term analysis of both trusted and untrusted services could paint a better picture of the ever-changing features being implemented into the public mixing atmosphere. Additionally, this study could be expanded to include open-source wallets that provide their own mixing implementations such as Wasabi Wallet and Samourai Wallet.

9 Conclusion

The Bitcoin mixing ecosystem attracts a wide range of users, many of whom simply wish to remain anonymous. The association of scams and poor implementation by these services has led to the proposal of secure protocols in academic literature. These proposed solutions provide methods to ensure accountability for mixing services and secure communication between participants without the leakage of input and output permutations. Through real world mixer interactions, we identified that there exists a disconnect in both implementation and resistance to common mixing threats between today's public mixing services and academically proposed solutions. We strongly believe that the disparities identified in this work represent an overall lack of regard for secure implementation. Although mixing services are often associated with criminal activity, the adoption of secure mixing methods could better their reputation and provide a foundation for future Bitcoin mixer research.

Acknowledgements. We would like to express our gratitude to the anonymous reviewers for their valuable feedback. This work was supported in part by the National Science Foundation (NSF) in grants 2000792, 1651661, and 1703644.

References

1. Protect your privacy. http://bitcoin.org/en/protect-your-privacy (2013), https://bitcoin.org/en/protect-your-privacy
2. Cryptomixer.io fast, secure and reliable bitcoin mixer (since 2016) (2016), https://bitcointalk.org/index.php?topic=1484009.msg15350012#msg15350012
3. Cryptomixer.io fast, secure and reliable bitcoin mixer (since 2016) (2016), https://bitcointalk.org/index.php?topic=1484009.msg15256505#msg15256505
4. Cryptomixer.io fast, secure and reliable bitcoin mixer (since 2016) (2016), https://bitcointalk.org/index.php?topic=1484009.msg15428183#msg15428183
5. Bestmixer.io the future of bitcoin mixing! technology is here (2018), https://bitcointalk.org/index.php?topic=3140140.0
6. Multi-million euro cryptocurrency laundering service bestmixer.io taken down (May 2019), https://www.europol.europa.eu/newsroom/news
7. 2020 list bitcoin mixers bitcoin tumblers websites (2020), https://bitcointalk.org/index.php?topic=2827109.msg29058223#msg29058223

8. Bitcoin charts & graphs - blockchain (2020), https://www.blockchain.com/en/charts
9. Alsalami, N., Zhang, B.: Sok: A systematic study of anonymity in cryptocurrencies. In: 2019 IEEE Conference on Dependable and Secure Computing (DSC). pp. 1–9 (Nov 2019). https://doi.org/10.1109/DSC47296.2019.8937681
10. de Balthasar, T., Hernandez-Castro, J.: An analysis of bitcoin laundry services. In: NordSec (2017)
11. Bissias, G., Ozisik, A.P., Levine, B.N., Liberatore, M.: Sybil-resistant mixing for Bitcoin. In: Proceedings of the ACM Conference on Computer and Communications Security. pp. 149–158. WPES '14, ACM (2014). https://doi.org/10.1145/2665943.2665955
12. Bonneau, J., Narayanan, A., Miller, A., Clark, J., Kroll, J.A., Felten, E.W.: Mixcoin: Anonymity for bitcoin with accountable mixes. In: Christin, N., Safavi-Naini, R. (eds.) Financial Cryptography and Data Security. pp. 486–504. Springer Berlin Heidelberg, Berlin, Heidelberg (2014)
13. Delgado-Segura, S., Bakshi, S., Pérez-Solà, C., Litton, J., Pachulski, A., Miller, A., Bhattacharjee, B.: Txprobe: Discovering bitcoin's network topology using orphan transactions. In: Financial Cryptography (2018)
14. DuPont, J., Squicciarini, A.C.: Toward de-anonymizing bitcoin by mapping users location. In: Proceedings of the 5th ACM Conference on Data and Application Security and Privacy. pp. 139–141. CODASPY '15, Association for Computing Machinery, New York, NY, USA (2015). https://doi.org/10.1145/2699026.2699128
15. Gregory Maxwell: CoinJoin: Bitcoin privacy for the real world (2013), https://bitcointalk.org/index.php?topic=279249
16. Heilman, E., AlShenibr, L., Baldimtsi, F., Scafuro, A., Goldberg, S.: TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub. In: NDSS. Internet Society (May 2017). https://doi.org/10.14722/ndss.2017.23086
17. Koshy, P., Koshy, D., McDaniel, P.: An analysis of anonymity in bitcoin using p2p network traffic. In: Financial Cryptography and Data Security, pp. 469–485. Springer Berlin Heidelberg (2014). https://doi.org/10.1007/978-3-662-45472-5_30
18. Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M., Savage, S.: A fistful of bitcoins: Characterizing payments among men with no names. In: Proceedings of the 2013 Conference on Internet Measurement Conference. pp. 127–140. IMC '13, Association for Computing Machinery, New York, NY, USA (2013). https://doi.org/10.1145/2504730.2504747
19. Möser, M., Böhme, R., Breuker, D.: An inquiry into money laundering tools in the bitcoin ecosystem. In: 2013 APWG eCrime Researchers Summit. pp. 1–14 (2013)
20. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2009), http://www.bitcoin.org/bitcoin.pdf
21. Novetta, L.: Survey of bitcoin mixing services: Tracing anonymous bitcoins. Tech. rep., McLean, VA (September 2015), https://www.novetta.com/wp-content/uploads/2015/10/NovettaBiometrics_BitcoinCryptocurrency_WP-W_9182015.pdf
22. Ruffing, T., Moreno-Sanchez, P., Kate, A.: CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin. Tech. rep. (2014)
23. Tran, M., Luu, L., Suk Kang, M., Bentov, I., Saxena, P.: Obscuro: A Bitcoin Mixer using Trusted Execution Environments. In: ACSAC '18 (Annual Computer Security Applications Conference). ACSAC '18, vol. 18, pp. 692–701. ACM, New York, NY, USA (2018). https://doi.org/10.1145/3274694.3274750

24. Valenta, L., Rowan, B.: Blindcoin: Blinded, accountable mixes for bitcoin. In: Brenner, M., Christin, N., Johnson, B., Rohloff, K. (eds.) Financial Cryptography and Data Security. pp. 112–126. Springer Berlin Heidelberg, Berlin, Heidelberg (2015)
25. Ziegeldorf, J.H., Grossmann, F., Henze, M., Inden, N., Wehrle, K.: CoinParty: Secure multi-party mixing of bitcoins. In: CODASPY 2015 - Proceedings of the 5th ACM Conference on Data and Application Security and Privacy. pp. 75–86. ACM (mar 2015). https://doi.org/10.1145/2699026.2699100

A Public Mixer Characteristics

Characteristic	Description
Min	Minimum mixing amount allowed
Max	Maximum mixing amount allowed
Account	Is registration required to participate?
Fees	Mixing fees
Time	Time to finish mixing
Delay	Amount of delay on mixing output
Logs	Amount of time service keeps logs
Input Addresses	Number of input addresses given to user
Output Addresses	Number of output addresses user may specify
Distribution Control	Does the user have control of the distribution of funds across their specified output addresses?
Minimum Blocks	Number of network confirmations needed before mixing begins
Additional Features	Additional unique features (letter of guarantee, receipt, check mix function, etc.)
Tor	Hidden service URL
Clearnet	Clearnet URL
Established	Year established
Bitcointalk	Bitcointalk service announcement URL
Forum Posts	Number of forum posts as of May 1st, 2020
Scam Accusation(s)	Does the mixer have any unresolved scam accusations?

Table 5: Mixer characteristics collected for our initial analysis of the public Bitcoin mixer landscape.

B Trial Results

B.1 ChipMixer

Trial	Obfuscation Parameters	Input (BTC)	Output (BTC)	Output Network Fees (BTC)	Mixer Fees (BTC)	Txn IDs
1	sweep	0.001	0.000921	0.000079	0	[1]
2	split, donate, merge, withdraw	0.003	0.002	0	0.001	[2]
3	voucher, sweep	0.004	0.00381195	0.00018805	0	[3]

Table 6: Results for ChipMixer trials.

[1] I_1: `467e3de55595849259650ef0dfdcad22b945bf98cc99cb0cc5d2f4ad6c4a9c9b`
O_1: `5e2673cb8e845aa41ba7c04b1aa6b1da415bffa87d01806f4e762133964694e1`

[2] I_1: `a0e9c07185369c217f740ee06a8b3499dd15d365647c78f34e6d3195132eb99b`
I_2: `3a8f4b06c8d30dcb333376b7168df3c1a93812086f5c31cf7c104715d2dc0d3b`
O_1: `6647ea4eaf7b6968101e2618a21608d4111f836aec7cf1589972f678a5a06ad4`

[3] I_1: `7675b43440cd2ac9c95134085262c1df8a8284ac4daeb9223402084363f53405`
I_2: `2fac417838683750b879e743811cea0c263efc0bf8c24a72b5f80cb393b78578`
O_1: `47a373922147c11b3a7b3d0675a62bf94c6d1e1d8252e915ca8bef83e37a0cd2`
O_2: `0755d63c3e989810bb8b0f65e852845d8c9538446278f438f0ca3a5f99310e00`

Trial 1 In Trial 1, 0.001 BTC was sent in one transaction, I_1, from the SegWit wallet. Within 30 seconds of the first confirmation on this input, we received one chip of 0.001 BTC. In Step 3, we were given the option to donate, withdraw, or receive a voucher. Options to split or merge were unavailable. We chose to withdraw our chips and proceeded to Step 4. We attempted to download the signed receipt but received an internal server error. Next, we chose to sweep the chip to the SegWit wallet with a network fee of 0.000079 BTC. The interaction resulted in 0 BTC mixing fees and our final output, O_1, was 0.000921 BTC.

Trial 2 In Trial 2, 0.003 BTC was sent to ChipMixer in two separate transactions from the SegWit wallet, I_1 and I_2. These transactions were 0.002 BTC and 0.001 BTC. The service provided one chip of 0.002 BTC (chip 1) and one of 0.001 BTC (chip 2). We split chip 1 into two chips of 0.001 BTC. Then, we donated one of these chips to ChipMixer and did not identify any movement of funds from the input address. Next, we merged the two remaining 0.001 BTC chips into one 0.002 BTC chip. On Step 4, we attempted to access the signed receipt but received an internal server error. We chose to withdraw our final chip by importing the private key into a new wallet. Importing resulted in 0 BTC network fees and 0 BTC mixer fees. The output to our wallet, O_1, was 0.002 BTC.

Trial 3 In Trial 3, two separate sessions were created. In the first session, transaction I_1 of 0.001 BTC was sent to ChipMixer and withdrawn for a voucher. The service provided a 53 character alphanumeric code. In the second session, transaction I_2 of 0.003 BTC was sent to the given input address. The voucher code from the first session was also redeemed. In total, the service provided two 0.001 BTC and one 0.002 BTC chips. On withdrawal, the chips were swept into the SegWit wallet. This resulted in two on-blockchain transactions with outputs of 0.00190361 BTC and 0.00190834 BTC, O_1 and O_2. The network fees associated with these transactions were 0.00009639 BTC and 0.00009166 BTC respectively. The total mixer fee was 0 BTC.

B.2 MixTum

Trial	Obfuscation Parameters	Input (BTC)	Output (BTC)	Output Network Fees (BTC)	Mixer Fees (BTC)	Txn IDs
1	1 Output	0.001	0.001	0.00024227	0	[4]
2	2 Outputs	0.002	0.001762	0.0004707	0.000238	[5]
3	2 Outputs	0.003	0.00276	0.00049838	0.00024	[6]

Table 7: Results for MixTum trials.

Trial 1 In Trial 1, one legacy output address was specified. A SegWit output address was attempted but was not accepted by the service. One input transaction, I_1, of 0.001 BTC was sent to a compatibility format input address provided by MixTum. Within five minutes, an output transaction, O_1 of 0.001 BTC was received. The network fee on the output was 0.00024227 BTC and mixing fees were 0 BTC.

Trial 2 In Trial 2, two legacy output addresses were specified. One input transaction, I_1, of 0.002 BTC was sent to a compatibility format input address provided by MixTum. The first output, O_1, of 0.001 BTC was received in one hour and 14 minutes. The network fee on this transaction was 0.00024227 BTC. A second output, O_2, of 0.000762 BTC was received in four hours and 55 minutes with a network fee of 0.00022843. The overall mixing fee for this interaction was equal to 4.4% of the input plus 0.00015 BTC.

Trial 3 In Trial 3, two legacy output addresses were specified. Two input transactions, I_1 and I_2, were sent to a compatibility format input address provided by MixTum. I_1 was 0.002 BTC and I_2 was 0.001 BTC. The first output address received two output transactions, O_1 and O_2, of 0.0004 BTC and 0.001 BTC 47 minutes after the input. The second output address received an output, O_3, of 0.00136 BTC in 52 minutes. The network fees for these output transactions were 0.00017997 BTC, 0.00017305 BTC, and 0.00014536 BTC respectively. The overall mixing fee for this trial was 3% of the input amount plus 0.00015 BTC.

B.3 Bitcoin Mixer

[4] I_1: 0cf2b5ae532f7efb78133b0cf63b8a11af658dba5cab810a6125cb8c81433896
O_1: 41102ce0aab86f143bd836cecae1495c1c4dbb3cf4b2b4ee19e2f7e9c8dd264b

[5] I_1: 3acc63ef655aed1a47323aeace7d3107ce8e26dc046a3a05998b284aa9221d91
O_1: 24b0e68ee157eef4567ce853198f1af5196fc0ffbfa875e20a84044bf6b82de0
O_2: 9f60da6b97b39c6de65f7b7e59def229fe990a70c66ab1263a71f7d262aac9ca

[6] I_1: 32328f8ea37163f06894e3ddd8620e4bfb93c1b968b70a1c7973d5fa4e81ffb3
I_2: 3863aab6e6f84f4da584975b9719511954ebc10a0ceca918b26f250d3553b211
O_1: da0f4c46f528f4df7d7383eee5064e69759403410f63049f4fe59341f1ee9991
O_2: 8ac7f54fb2fa52811d07ff3fa5f7031f8499e0d63ba37691e8979612e3107181
O_3: d9cf6777e294f2936f9219cbd10a4926f93986fa9d79829e72e6f422eae1e59f

[7] I_1: 1e986fcb917e3b6702f7c0855ef97bb63852f3a7b4b732c979c24a650d83d60a
O_1: 1752cc1c59e086a41e5eff494a3e949220585174df969524ba0315ff43baacc1

[8] I_1: f3ea2711301deda2a6e1721a6cb535c8d989a9536089c72b1df693ec72d3a979
O_1: a445e5f62e7a7aaccbb5f0094dead98ff340f00fa461bb02bcebb5c39209ce39
O_2: b29103754707b9553948efe16e0f0f2ed24afd9344851ae6aba53d48d6295188
O_3: a38b52879b069709aa7baa3928b71f3c2ebb8dcfbce23b481fc0f5b00f00afe1

[9] I_1: 101a29a16be3357b5b9733e9cb5576d735ba4526f0937071a1bc43158e4cf4ab
O_1: 1423cc8eadc7be5b71c25286244ca9815479691a816c545eb46ce9d40ae6d3c8
O_2: fa5bb1ade1c6e99ffa964ad5b76f005c4e6c4b740b1697fd664e43f0f8522e2a

Trial	Obfuscation Parameters	Input (BTC)	Output (BTC)	Mixer Fees (BTC)	Txn IDs
1	1 Output rapid delay	0.0002	0.0001985	0.0000015	[7]
2	3 Outputs distribution (%): 35, 35, 30 delay (hr): 1, 2, 2	0.0004	0.000396	0.000004	[8]
3	5 Outputs distribution (%): 13.3, 5.36, 21.98, 30.72, 28.64 delay (hr): 1, 2, 5, 10, 12	0.0006	0.0005935	0.0000065	[9]

Table 8: Results for Bitcoin Mixer trials.

Trial 1 In Trial 1, one output SegWit address was specified with rapid delay. The service provided a compatibility format input address and a mix ID. One transaction, I_1, of 0.0002 BTC was sent to this address. Within 30 seconds of the first network confirmation, an output transaction, O_1, of 0.0001985 BTC was received. Overall, the interaction had a mixing fee of 0.0000015 BTC.

Trial 2 In Trial 2, three legacy output addresses were specified. Delay and distribution among these addresses was set to be 1 hour with 35%, 2 hours with 35%, and 2 hours with 30% respectively. The service provided one compatibility format input address. One transaction, I_1, of 0.0004 BTC was sent to this address. The first output address received output O_1 of 0.0001386 BTC in 43 minutes. The second received output O_2 of 0.0001386 BTC in 1 hour and 44 minutes. The third received output O_3 of 0.0001188 BTC in 1 hour and 44 minutes. The overall mixing fee for this trial was 0.000004 BTC.

Trial 3 In Trial 3, five SegWit output addresses were specified. Delay and distribution was set to be 1 hour with 13.3%, 2 hours with 5.36%, 5 hours with 21.98%, 10 hours with 30.72%, and 12 hours with 28.64% respectively. The service provided one compatibility format input address. One transaction, I_1, of 0.0006 BTC was sent to this address. Output O_1 of 0.00007894 BTC was received by the first output address in 31 minutes. Output O_2 of 0.00003181 BTC was received by the second output address in 1 hour and 26 minutes. Output O_3 of 0.00013045 BTC was received by the third output address in 4 hours and 26 minutes. Output O_4 of 0.00018232 BTC was received by the fourth output address in 9 hours and 26 minutes. Finally, output O_5 of 0.00016998 BTC was received by the fifth output address in 11 hours and 26 minutes. The overall mixing fee for this trial was 0.0000065 BTC.

Trial	Obfuscation Parameters	Input (BTC)	Output (BTC)	Mixer Fees (BTC)	Txn IDs
1	1 Output 2 Input 0.5060% fee 1hr 15min delay	0.001	0.00049494	0.00050506	[10]
2	CryptoMixer Code 3 Outputs 4 Inputs distribution (%): 20.05, 19.96, 59.99 delays: 3hr 7m, 9hr 1min, 15hr 2min	0.002	0	0	[11]
3	3 Outputs 2 Inputs distribution (%): 20.43, 19.85, 59.72 delays: 3hr 3min, 9hr 8min, 15hr 4min	0.002	0	0	[12]

Table 9: Results for CryptoMixer trials.

B.4 CryptoMixer

Trial 1 In Trial 1, one SegWit output address was specified. Additionally, the mixing service fee and delay were set to 0.5060% and 1 hour and 15 minutes respectively. This qualified for a Standard security level. The service provided a five character alphanumeric CryptoMixer code and one legacy format input address with its corresponding letter of guarantee. One transaction, I_1, of 0.001 BTC was sent to this address. The service's calculator stated that the output would be 0.00049494 BTC. However, after one confirmation the service displayed an error stating that the "amount is less than required." The error did not disappear and the number of confirmations on our original input did not update after the first detected confirmation. Assuming the service expected an additional payment of 0.00049494 BTC, we generated a second input address and executed another input transaction, I_2. However, this was ignored by the service. After 1 hour and 21 minutes of the first input, we received output O_1 of 0.00049494 BTC with a network fee 0.00007749 BTC. The overall mixing fee for this interaction was 0.00050506 BTC.

Trial 2 In Trial 2, the CryptoMixer code from Trial 1 was used and three legacy output addresses were specified. Delay and distribution for these output addresses was 3 hours and 7 minutes with 20.05%, 9 hours and 1 minute with

O_3: `a1d08152d1e5e9d75996591e69b663f0eefb96fa31f06fd6ca907084d2e04f26`
O_4: `61ef79f1ff7ae348a453f4e1d073ce5cf7a732d6c0e50d9fe04d0005eec142f4`
O_5: `32ad310b25f2f4f11288e8115fce4126526643f49afc5c5e80f081bab3d853b1`

[10] I_1: `a02d447aae65ce5d671b2cf1ba183cf08399655f17ed26269c0124e0cf4f5e3d`
I_2: `73e8f1f233c9ca966f7ab34a4074a558269b37cfb65c4f1a3482f66b8d6e3c6f`
O_1: `f60a746dd452f1c687f0ff92849ede81ecbe7787440f2906c47385f0d9279fcd`

[11] I_1: `1268643164dddfee0fce627295fb6c26d62dadb418630c3601e812feb612d0fe`
I_2: `02667f20e8355136aec0295409c5d689bf8a7a9ec1302e8a2941154ec565062e`
I_3: `1c2bfe577e9bb80cbbd2d56108145d640112128b4518348676b468032f947b62`
I_4: `9b5e7617ee123c10e697c838d9d061118c3749bf0b89c12107c6daf0df2f798d`

[12] I_1: `fb930e8d5c9ffe10edc40f880671da7bc8370eee101bc46a20e9fafc0ceb4ddb`
I_2: `5d010989689bae4d4ec4bd4e9c3984a4632548fa15aeac9ea90d94f15fc2928d`

19.96%, and 15 hours and 2 minutes with 59.99% respectively. The mixing fee was set to 1.0176%. These parameters qualified the interaction for a Silver security level. The service provided the same CryptoMixer code from Trial 1 and we manually generated four legacy format input addresses. The letter of guarantee for each of these addresses was successfully downloaded. Input transactions I_1, I_2, I_3, and I_4 were executed with 0.001 BTC, 0.001 BTC, 0.0005 BTC, and 0.001 BTC respectively. The service's calculator stated that 0.00039386 BTC, 0.00039209 BTC, and 0.001178 BTC would be deposited to out output addresses. However, no outputs were received.

Trial 3 In Trial 3, no CryptoMixer code was used and three legacy output addresses were specified. Delay and distribution for these output addresses was 3 hours and 3 minutes with 20.43%, 9 hours and 8 minutes with 19.85%, and 15 hours and 4 minutes with 59.72% respectively. The mixing service fee was set to 1.0820%. These parameters qualified this trial for Silver security level. We received a new five character CryptoMixer code and manually generated two legacy format input addresses. The letter of guarantee for each of these addresses was successfully downloaded. Input transactions I_1 and I_2 were executed with 0.001 BTC each. However, we received the same error from Trial 1 stating "amount is less than required." For both inputs the service stated 0.00051082 BTC was pending. Thus, two transactions of 0.0005 BTC and 0.00001082 BTC were sent to each input address. However, the service did not identify these transactions and no outputs were received.

B.5 Sudoku Wallet

Trial	Obfuscation Parameters	Input (BTC)	Output (BTC)	Output Network Fees (BTC)	Mixer Fees (BTC)	Txn IDs
1	sweep	0.001	0.00087261	0.00012739	0	[13]
2	sweep	0.002	0.00171162	0.00024839	0.00003999	[14]
3	sweep	0.003	0.0000769	0.00022310	0.0027	[15]

Table 10: Results for Sudoku Wallet trials.

Trial 1 Sudoku Wallet provided a 25 character alphanumeric wallet key. The service then presented an input address with its corresponding private key. We sent one transaction, I_1, of 0.001 BTC to this input address. After the service

[13] I_1: `175996ac5b80fcc2df3cc44894ecbdd4e26a35ae20f076ff242d112900bc4898`
O_1: `d37438550d5418c26b3b9a0cadc20007d80d12177b096ef286c53ef10cad11c9`

[14] I_1: `778e990edf67d546bd8eeae9111078e381c7cc7d0eff93e58da8b13bb0d275d2`
O_1: `a63076611384abf4cd1e3df92b327c324af910e14914c6038b60e037814935c9`

[15] I_1: `3c18b011a01f243d2cace66c07cf6016385ffa20f55e0cbdfccf34fa96f18088`
O_1: `310ec6f888c9db47c1d24410f5a38b3b40461b378a355f0363faaed8f5166443`

detected three confirmations on this input, we were able to view two output addresses funded with 0.00059025 BTC and 0.00040975 BTC along with their private keys. These funds were then swept to our SegWit wallet through an on-blockchain transaction, O_1. The network fee for this transaction was 0.00012739 BTC and 0.00087261 BTC was the final output. The overall mixing fee for this interaction was 0 BTC.

Trial 2 Sudoku Wallet provided a new 25 character alphanumeric wallet key. The service presented an input address with its corresponding private key. We sent one transaction, I_1, of 0.002 BTC to this address. After three confirmations, we were presented three output addresses with 0.00066667 BTC, 0.00064667 BTC, and 0.00064667 BTC. These funds were then swept to our legacy wallet through an on-blockchain transaction, O_1. The network fee for this transaction was 0.00024839 BTC and 0.00171162 BTC was the final output. The overall mixing fee for this interaction was 0.00003999 BTC.

Trial 3 We received a new 25 character alphanumeric wallet key. We sent one transaction, I_1, of 0.003 BTC to the given input address. After three confirmations, we were presented three output addresses of 0.0001 BTC each with corresponding private keys. These funds were swept to our SegWit wallet through an on-blockchain transaction. O_1. The network fee for this transaction was 0.00022310 BTC and 0.0000769 BTC was the final output. The overall mixing fee for this interaction was 0.0027 BTC.

C Chip Generation Transactions

Chip Size (BTC)	Transaction ID
8.192	a3098c6d8961c6674ad4590a3b50c2ca213d833b49a2c774ce5248cabed135a2
0.256	5b7bfd2f60d6058344cdb59fe64d3c1402378c3489210de2a6d18a34e1c0bd5b
4.096	66c3429e06f5e8732717bbeba30d7df28f81a785c4018ad0a269959bbd37bce6

Table 11: Example Chip Generation Transactions.