Tracking Mixed Bitcoins

Tin Tironsakkul[0000−0000−0000−0000], Manuel Maarek[0000−0001−6233−6341], Andrea Eross[0000−0003−0899−7960], and Mike Just[0000−0002−9669−5067]

Heriot-Watt University, Edinburgh, Scotland, UK

Abstract. Mixer services purportedly remove all connections between the input (deposited) Bitcoins and the output (withdrawn) mixed Bitcoins, seemingly rendering taint analysis tracking ineffectual. In this paper, we introduce and explore a novel tracking strategy, called *Address Taint Analysis*, that adapts from existing transaction-based taint analysis techniques for tracking Bitcoins that have passed through a mixer service. We also investigate the potential of combining address taint analysis with address clustering and backward tainting. We further introduce a set of filtering criteria that reduce the number of false-positive results based on the characteristics of withdrawn transactions and evaluate our solution with verifiable mixing transactions of nine mixer services from previous reverse-engineering studies. Our finding shows that it is possible to track the mixed Bitcoins from the deposited Bitcoins using address taint analysis and the number of potential transaction outputs can be significantly reduced with the filtering criteria.

1 Introduction

A Bitcoin *mixer service* (also commonly known as *tumblers* or *laundering services*) is a cryptocurrency service that allows users to "anonymise" their Bitcoins by eliminating any possible connection between their original deposited Bitcoins and the *mixed* Bitcoins that they withdraw later from the service [6, 16]. This mixing process can make the tracking of Bitcoin movements between addresses challenging, such as when using techniques like *taint analysis* [11]. Mixer services are also frequently used as one of the core components in transaction obscuring for illicit activities, such as theft, ransomware, and dark market trade [15, 17].

In a normal Bitcoin transaction, address A would send Bitcoins directly to address B. However, this interaction establishes a connection between the two addresses in the blockchain, allowing anyone to observe the movement of Bitcoins [13]. Mixer services attempt to prevent this traceability by serving as an intermediary between the two addresses where Address A deposits Bitcoins to a mixer service address (receiver address) for mixing. Next, the mixer service uses another address(es) (delivery address) to deliver completely unrelated Bitcoins to address B in withdrawn transactions.

As a result, the interaction between address A and B is obscured in the blockchain, as there is no direct connection or transaction between the two endpoint addresses. Furthermore, simple transaction tracking methods are incapable

of tracking the actual exchange of Bitcoins between the two addresses. One method used to track the mixed Bitcoins is to calculate every possible combination on every transaction within the mixing time for the potential withdrawn transaction outputs [19], which requires computational resources.

Few studies have investigated reverse-engineered mixer services to discover their internal operations [3,11,18]. We are aware of only one study that proposed a tracking method for mixed Bitcoins, which adapted from the aforementioned approach, and evaluated their method on a single mixer service [19]. In particular, we are not aware of any proposed tracking method to overcome the transaction obscuring feature of mixer services.

Hence, in this paper we introduce a novel tracking method called *address taint analysis* that focuses on tainting at the address level, whereas previous taint analysis approaches have focused on tainting at the transaction level. We investigate this method, both on its own and in combination with other tracking methods such as *address clustering* and *backward tainting*. We also introduce a set of filtering criteria in an attempt to reduce the number of false-positive results, and we evaluate our solutions with verifiable mixing transactions of nine mixer services from previous reverse-engineering studies.

The remainder of the paper is structured as follows. We describe the related work in Section 2. We define our new methods and filtering criteria in Section 3. Using the sample cases presented in Section 4, we evaluate the results of these methods and discuss the results in Section 5. In Section 6, we conclude and discuss improvements we envision.

2 Related Work

2.1 Taint Analysis

Taint analysis is a transaction tracking method that determines the relationship or connection of addresses based on exchanges of specific Bitcoins in transactions [11]. It is often adapted to track the movement of specific Bitcoins (e.g., stolen Bitcoins) by classifying the tracked Bitcoins as tainted or clean and calculating the distribution of tainted Bitcoins used in subsequent transactions.

One taint analysis method, the *Poison method*, considers all of the resulting transaction outputs as fully tainted [12]. There are other tainting strategies that utilise different approaches of tracking and distributing Bitcoins, such as the *Haircut method* [12] and *FIFO method* (First In, First Out) [1]. Taint analysis can also be performed backwards, where instead of tainting forward to the next transaction, the algorithm taints backwards following previous transactions, possibly all the way back to the coinbase transaction where the Bitcoins originate from [1].

Aside from transaction tracking, taint analysis is utilised to measure the effectiveness of transaction obscuring methods where results with tainted connections indicate that the obscuring method is ineffective and can still be tracked [9,14]. We hereafter refer to the original transaction-based taint analysis as *transaction*

taint analysis to distinguish it from the address-based taint analysis we define in this paper (see Section 3.1).

2.2 Address Clustering

Address clustering is a method that operates by grouping addresses into a cluster based on specific transaction behaviours. Address clustering methods are utilised in de-anonymisation which attempts to classify Bitcoin addresses likely to belong to the same user for tackling illegal activities [10].

One address clustering method, called *input-sharing clustering* or *multi-input heuristic*, is based on the assumption that all the addresses that share inputs in the same transaction belong to the same entity because every input address must sign a digital signature with its private key for the transaction to be valid. As such, if there are two or more input addresses in the same transaction, these addresses are being controlled by the same user [5].

Although this address clustering method has the advantage of relying only on information available inside the Bitcoin blockchain, it is frequently considered to be less effective for de-anonymisation purposes due to the existence of *CoinJoin*[1]. Input-sharing clustering classifies every address that shares input in the same transaction via CoinJoin as belonging to the same user. As a result, input-sharing clustering will create inaccurate address clusters that belong to different users and cannot be practically utilised for de-anonymisation purposes.

Another clustering approach, 'change address clustering', operates by clustering the input addresses with the output addresses that are likely to be the change addresses – this is an address that is owned by the transaction's sender and which receives the remaining change Bitcoins in the transaction[2] [10].

3 Methodology

In this section we describe the address taint analysis method and the other tracking methods, address clustering and backward tainting methods, that we evaluate in combination with address taint analysis. Subsequently, we discuss the filtering criteria we develop and the rationales behind them.

To evaluate the effectiveness of our four tracking methods and filtering criteria, we compare the number of tainted transaction outputs of each method to the baseline of all outputs occurring in the same time frame. Our definition of the baseline is based on work from a previous study [19].

Baseline *All outputs of every transaction recorded in the blockchain within the tainting time frame of a given sample case.*

[1] *CoinJoin* is a method which allows multiple users to combine their Bitcoin transactions in a single transaction to improve their transaction privacy [8].

[2] For example, if address A uses a 10 Bitcoins input to send 5 Bitcoins to address B, the owner of address A will need a change address (either address A or another address) to receive 5 Bitcoins back.

3.1 Address Taint Analysis

The majority of mixer services usually utilise either a central address or multiple central addresses in order to combine and mix deposited Bitcoins from their users [3, 11, 18]. We assume that the receiver and delivery addresses within the mixer services are both likely to interact with the central addresses at some point in time.

Our taint analysis method, *Address Taint Analysis*, is shown in Figure 1. It operates at the address connection level, where any address that has received any Bitcoin from tainted addresses at any point in time will be considered a tainted address. Existing taint analysis methods operate at the transaction level, where the tainted Bitcoins of a received address do not affect other Bitcoins belonging to that address, unless they are used together in the same transactions.

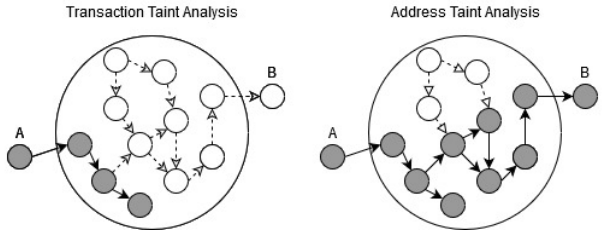

Fig. 1: (Transaction) taint analysis and address taint analysis
The figure depicts the difference between the transaction taint analysis and address taint analysis methods on an example mixing case that shows the deposited transaction from address A and the withdrawn transaction to address B. A small white circle represents a clean address and a grey circle represents a tainted address. A black arrow indicates a transaction that involves tainted Bitcoins, while a dashed line with a white arrow indicates a transaction that does not involve tainted Bitcoins.

The assumption for address taint analysis is that any transaction and address that can be connected to the receiver addresses at any point in time, whether directly or indirectly, may be related to the mixer service in some ways. Therefore the objective of address taint analysis is not only to track the mixed Bitcoins, but to also map the network of address clusters and their transactions that may involve the mixer service operation, similar to the concept of network analysis [7]. Hence, address taint analysis tracking should be able to discover a relationship between the deposited and withdrawn transactions that the transaction taint analysis is unable to accomplish, as shown in Figure 1.

We describe three methods below for using address taint analysis (one further method, is described in Section 3.2). The first method uses only address taint analysis. For the second and third methods, we investigate the potential of incorporating address clustering methods into the address taint analysis in order to improve the address cluster tracking results. As de-anonymisation is not

our primary objective, we utilise the address clustering method to assist the address taint analysis algorithm for capturing relationships between addresses that are outside the scope of address taint analysis, which regard only the Bitcoin movement (address A sends Bitcoins to address B).

Method 1 *Address taint analysis only.*

The operation of address taint analysis used in this paper is conceptually similar to Poison transaction tainting [12] as the entire address is considered tainted, regardless of the number of tainted Bitcoins involved but goes further by affecting every Bitcoin possessed by the address throughout time. Since our main priority is to discover the connection between the deposited and withdrawn Bitcoins, other transaction tainting methods, which generally emphasise the distribution of tainting proportions, would not provide further information for this purpose.

As mixer services typically perform the mixing operation continuously, it is possible for the service to deliver Bitcoins that are already mixed prior to the time of the deposited transactions. As such, address taint analysis will also need to taint from the time period before the deposited transactions occurred. To put it simply, address taint analysis will taint all Bitcoins that the tainted addresses send both before and after the deposited transactions time.

Method 2 *Address taint analysis with input-sharing clustering.*

We use the input-sharing clustering method coupled with address taint analysis to taint any address that shares inputs with the tainted addresses. We use the same hypothesis as the original input-sharing clustering for our adaptation – any address that shares input in the same transaction with any tainted address is also likely to be one of the mixer service addresses and will be classified as a tainted address.

Method 3 *Address taint analysis with input-sharing and output-sharing clustering.*

As an augmentation to Method 2, here we also incorporate the output-sharing clustering method with the assumption that in the case of the mixing operation, the central addresses would often distribute the mixed Bitcoins to other mixer addresses first, before delivering them to the users. Consequently, we expect that output-sharing clustering should improve the chance of tracking such scenarios, even if the delivery addresses of the mixer service never send mixed Bitcoins to one another, or share input in the transaction.

3.2 Backward Address Taint Analysis

The address taint analysis method operates with the assumption that the deposited and withdrawn mixer addresses may have an indirect connection with each other because of the presence of the central addresses. It will be unable to

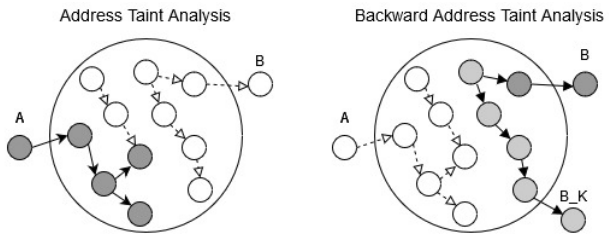

Fig. 2: Address taint analysis and backward address taint analysis
The figure depicts mixer service with two separate groups tainted with address taint analysis and backward address taint analysis. Notice the lack of any interaction between the address A and B groups. B_K represents the withdrawn output(s) from a known case used for backward address tainting in Method 4. In the backward address taint analysis, the lighter grey colour represent tainting result of backward address taint analysis and the darker grey colour circle represent tainting result of address taint analysis performed after backward address taint analysis (Method 4).

discover any connection between the deposited inputs and withdrawn transaction outputs if there is no such connection, as shown in Figure 2.

In such situation, address tainting from the deposited address cannot reach the withdrawal address. However, the knowledge of pre-existing withdrawal addresses could be used to identify the targeted withdrawal address. The search would consist of tainting backward from this known withdrawal address and then forward towards potential withdrawal addresses.

Therefore, we introduce another method for this scenario by applying backward tainting to address taint analysis to create another tracking method called *Backward Address Taint Analysis*. This method operates by tainting any address that sends Bitcoins to a tainted address. Rather than attempting to discover the connection between the mixed Bitcoins, the purpose of this method is to investigate whether it's possible to discover the address clusters used for withdrawn transactions. The idea would be that these addresses could subsequently be used to find the targeted withdrawn transaction outputs. Thus, this method operates in two steps, as described in the example below.

Method 4 *Perform Method 3 on the results of backward address taint analysis on the known pre-existing withdrawn transactions from the same mixer service.*

Using the example from Figure 2, Method 4 starts by performing the backward taint analysis variation of the address taint analysis from the withdrawn transactions of another case from the same mixer service (B_K) for three days to trace the mixed Bitcoins back to the central address clusters. Next, we use the results of backward address taint analysis to perform address taint analysis at the time of the deposited transactions of the targeted sample case (A).

3.3 Filtering Criteria

To further reduce the number of false-positive results, we define five filtering criteria based on the information of the withdrawn transactions obtained from reverse-engineering experiments of previous studies [3, 11, 18].

The criteria can be applied for mixed Bitcoins in general with appropriate calibration. The calibration of the criteria parameters can also be specified to be stricter to reduce the false-positive results even further but this can increase the risk of missing the target. The parameters used in this experiment are obtained from observing the sample cases provided by the studies mentioned above. We set the parameters conservatively to reduce the risk of losing the targeted withdrawn transactions for this experiment. In establishing the filtering criteria for our investigation we had the advantage of knowing the target withdrawn outputs that we were searching for. For future studies we plan to investigate the criteria on data with unknown target values.

Criterion 1 (Value of Withdrawn Bitcoins) *The transaction output value of the targeted withdrawn transaction outputs cannot be higher than the deposited input value minus the mixing fee.*

As mixer services typically subtract a specific mixer service fee[3] from the initial deposited Bitcoins, the amount of the withdrawn Bitcoins would be lower than the original deposited amount. Depending on the mixer service, the mixing fee can vary in a specific range, such as between 1-2% of the deposited Bitcoins. For this experiment, we use a minimum mixing fee for this criterion.

This criterion does have at least one limitation, as it may be possible for the mixer services to combine the withdrawal of multiple deposited Bitcoins, which can make the withdrawn transaction outputs larger than the deposited input.

Criterion 2 (Withdrawn transaction's shape) *The number of transaction inputs and outputs of the targeted withdrawn transactions must be in the same pattern as the other withdrawn transactions by the same mixer service.*

The reverse-engineering examples from the literature [3, 11, 18] show that the mixer services usually perform withdrawn transactions in a specific pattern. For example, one of the most common shapes of withdrawn transaction is in the form of a one-to-two addresses transaction where a single transaction output is sent to two addresses, one belonging to the user and the other to the mixer service.

A limitation of this criterion is that it is also possible for the mixer service to randomise the shape pattern or have an exception scenario (e.g., the withdrawn Bitcoins are large valued so that the service needs to combine other inputs in a withdrawn transaction) that can make the targeted withdrawn transaction different from the common pattern.

[3] Note that mixer service fee is different from Bitcoin transaction fee, which is mentioned in Criterion 5.

Criterion 3 (Withdrawn transaction chain's shape) *If the mixing algorithm has a continuous withdrawn transaction chain pattern (e.g., peeling chain shown in Figure 3), either the transaction prior or after the targeted withdrawn transactions must have the same number of transaction inputs and outputs as the common pattern.*

Following from Criterion 2, the reverse-engineering results of the mixing sample cases indicate that multiple mixer services usually perform the withdrawn transactions in a continuous peeling chain (as shown in Figure 3), where a single transaction input with a large amount of Bitcoins is continuously peeled into two transaction outputs with one typically much smaller than the other [3].

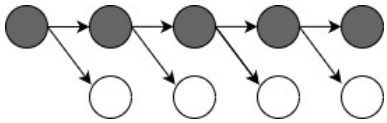

Fig. 3: Example of a peeling chain
The figure depicts the peeling chain of a transaction chain that is commonly used by mixer services. A black circle represents a delivery address that belongs to the mixer service and a white circle represents a user address that receives a withdrawn transaction output.

As such, either the previous or next transaction of the targeted withdrawn transactions must also follow the peeling chain pattern, accounting for the possibility that the targeted withdrawn transactions can be at the start or end of the withdrawn transaction chain.

Similar to a limitation for Criterion 2, the mixer service can randomise the transaction chain shape or simply does not have one, which can increase the risk of missing the targeted outputs or make this criterion inapplicable.

Criterion 4 (Reused addresses) *The input address in the targeted withdrawn transactions is not used as transaction input more than once in its lifetime.*

Our analysis of the verifiable mixing transactions from previous studies shows that the majority of the mixer services never reuse their delivery addresses before and after the withdrawn transaction. Therefore, we can utilise this information as a criterion to exclude any transaction with input addresses that have been reused at any point in time.

A limitation of this criterion is that although generally mixer services do avoid reusing the same address more than once, which is one of the most common Bitcoin privacy practices [2], it is possible for a mixer service to disregard this practice.

Criterion 5 (Withdrawn transaction fee) *The transaction fee value of the targeted withdrawn transactions must be the same as in other withdrawn transactions in the same time period.*

From our own analysis of the verifiable mixing transactions from the previous studies, we detected a specific pattern in the transaction fee values of the withdrawn transactions. In particular, the transaction fee value were commonly the same specific amount, such as 0.0005 BTC or 0.0001 BTC, even with a different transaction fee per byte ratio[4] and at a different time and day. This suggests that mixer services generally do not automatically adjust the transaction fee setting in real-time but by a specific amount of time. As such, if the transaction fee always remains constant for the other withdrawn transactions in a similar time by the same mixer service, we can use the transaction fee as a criterion to exclude unrelated transactions.

Similar to the other criteria, it is possible for a mixer service to not have the practice of using a constant transaction fee for a period of time, which would make this criterion inapplicable.

4 Sample Cases

We use 15 mixing transactions samples from previous studies [3, 11, 18] which have shown that transaction taint analysis could not taint the withdrawn Bitcoins from the deposited Bitcoins. We show these samples in Table 1. These studies perform reverse engineering on prominent mixer services: Blockchain.info's Shared Send function, Bitcoin Fog, Bitlaundry, BitLaunder, DarkLaunder, Alphabay and Helix Light. As one study [18] chose to not publicly name their tested mixer services, we will also exclude any identifiable information of the services and transactions, and refer the mixer services from that study as *Unnamed*.

For the address taint analysis experiment we use the transaction hash of deposited transactions to perform the address taint analysis and the transaction hash of withdrawn transactions are used to verify whether the address taint analysis can successfully reconnect the withdrawn Bitcoins back to the original deposited Bitcoins. If all of the targeted withdrawn transactions appear in the tainting results, we consider the experiment successful for that sample case.

In some of the mixing sample cases a *change address* that belongs to the user and is reused to interact with the withdrawn Bitcoins later on is used. This type of scenario can severely decrease the effectiveness of mixer services and make the mixed Bitcoins easily traceable. As user error is an extraneous variable that is not related to the mixer services and can affect the results of our experiment, we exclude any such change addresses from the deposited transactions.

5 Results and Discussion

5.1 Address Taint Analysis

We set the time limit for the address taint analysis operation to begin tainting from five days before the deposited transactions until the maximum amount of

[4] Transaction fee per byte ratio is a metric to calculate the recommended transaction fee often used by miners to determine which transactions should be prioritised to maximise their mining profit.

Case Service	*Baseline*	*Method 1*	*Method 2*	*Method 3*	*Method 4*
1 Blockchain.info	485,155	—	—	451,840	n/a
2 Bitcoin Fog	713,899	—	—	—	682,901
3 Bitcoin Fog	1,525,276	—	—	—	1,495,431
4 BitLaundry	1,013,374	841,563	845,846	976,745	989,264
5 BitLaundry	1,016,043	843,277	847,662	984,089	463,584
6 Unnamed 1	1,337,727	1,111,329	1,121,851	1,233,912	n/a
7 Unnamed 2	1,264,966	1,065,511	1,074,187	1,172,663	n/a
8 Bitlaunder	1,867,536	1,505,252	1,525,339	1,739,058	1,668,100
9 Bitlaunder	2,156,487	1,712,671	1,731,779	2,006,007	1,919,906
10 Darklaunder	1,712,521	1,407,023	1,421,073	1,606,730	1,637,210
11 Darklaunder	1,845,130	1,495,535	1,527,367	1,730,747	1,745,119
12 Alphabay	1,949,670	1,576,817	1,612,756	1,823,635	1,874,048
13 Alphabay	2,175,263	1,770,505	1,800,171	2,055,219	2,055,248
14 Helix Light	1,858,540	1,406,001	1,434,067	1,732,733	1,750,071
15 Helix Light	1,777,542	1,326,101	1,358,043	1,669,601	1,669,599

Table 1: Number of transaction outputs with each address tainting method
A horizontal line in a cell indicates that the method's experiment for the sample case was unsuccessful. The letter "n/a" indicates the absence of experiment for that method. (Method 4 requires another case of the same mixer service to performed). The colour in each cell represents the percentage of the method's transaction output number compared to the Baseline method. The lighter the colour, the lower the percentage.

mixing time allowed by the mixer service (e.g., BitLaundry allows up to maximum 10 days mixing time). If the mixer service did not have a mixing time setting, we set the time limit to three days.

As shown in Table 1, the results of our experiment demonstrate that even mixed Bitcoins are not always perfectly immune to tracking. The majority of the sample cases show successful results for all three methods except for Blockchain.info and Bitcoin Fog cases where the target withdrawn outputs could not be found. The address taint analysis methods manage to accomplish the experiment's main objective, which is to reconnect the original deposited Bitcoins to the mixed Bitcoins, albeit with the extensive spreading of the tainted results. It should be noted that the number of transaction outputs in Table 1 (and later in Table 3) only count from when the deposited transactions occurred until the end of mixing time limit.

For the majority of sample cases, Method 1 yields the lowest number of transaction outputs compared to the other three methods and the Baseline method, followed by Method 2 and lastly Method 3. The number of transaction outputs for Method 1 is considerably lower than the Baseline method at roughly 20% for the successful cases. For example, Method 1 has 21% (443,816) fewer transactions than the Baseline for Case 9, and 17% (171,811) fewer transactions in Case 4.

The results of Method 2 are generally similar to those of Method 1. For example, Method 2 has only 1% (8,676) more transactions than Method 1 in

Case 7, and 2% (35,939) more in Case 12. Meanwhile, Method 3 produces a greater number of transaction outputs compared to the first two methods and is much closer to the Baseline method. For example, Method 3 has 12% (199,707) more transactions output than Method 1 in Case 10, and 6% (105,791) fewer than the Baseline method. As such, our results suggest that the incorporation of address clustering and backward tainting methods is not always necessary for the tracking of mixer services though a few cases, Bitcoin.info's Shared Send and Bitcoin Fog, are notable exceptions from our data set.

5.2 Backward Address Tainting

As shown in Table 1, the address taint analysis experiment on the Bitcoin Fog cases (2 and 3) produces unsuccessful results. This is because the mixer service keeps the deposited Bitcoins idle for an extremely long time, which is outside the time period verification for our experiments.

While the initial deposited transaction for Case 2 occurred on 29/04/2013, the deposited Bitcoins were not used at all until 07/11/2013, even though the withdrawn transactions occurred on 30/04/2013. This is similarly the situation for Case 3. This type of scenario indicates that the central address clusters used for deposited and withdrawn transactions are separate and cannot be connected because of the time limit constraint in this experiment.

Method 4 shows successful results for all sample cases as shown in Table 1. Although, aside from the Bitcoin Fog cases, both of the Method 4 tainting results (and the results after applying filtering criteria – see Section 5.3) do not provide improved results compared to the other three methods. In particular, the number of transaction outputs resulting from Method 4 is higher than Method 3 in most cases. For example, Method 4 has 2% (30,480) more transaction outputs than Method 3 for Case 10 which is only 4% (75,311) lower than the Baseline method results. However, there are some exceptions where Method 4 performs better than Method 3 such as in Cases 5 and 9 where the number of transaction outputs are 53% and 5% lower than Method 3, respectively.

Nevertheless, the results of the backward address tainting of Method 4 shows that it is possible to defeat the mixer service operation with separate central address clusters. If the attackers can initiate mixing transactions the same time as the targeted mixing transactions so as to perform backward address tainting, he/she can discover the central address clusters that are being used for withdrawal of the targeted mixed Bitcoins.

5.3 Filtering Criteria

After performing address taint analysis on each sample case, we applied the filtering criteria listed in Section 3.3 on each method's results for every case, as shown in Table 2. While the majority of the sample mixer services employ a one-to-two peeling chain method (continuous one-to-two transaction), there are some exceptions.

Service	*Criterion 1*	*Criterion 2*	*Criterion 3*	*Criterion 4*	*Criterion 5*
Blockchain.info	0.5%	one-to-one	one-to-two	Y	10,000 Sat
Bitcoin Fog	1%	one-to-two	one-to-two	Y	50,000 Sat
BitLaundry	2.49%	one-to-two	one-to-two	Y	50,000 Sat
Unnamed 1	1.5%	one-to-two	one-to-two	Y	10,000 Sat
Unnamed 2	1%	one-to-two	one-to-two	Y	10,000 Sat
Bitlaunder	2%	N	N	Y	N
Darklaunder	2%	N	N	Y	N
Alphabay	10,000 Sat	one-to-two	N	N	N
Helix Light	2%	one-to-many	N	Y	50,000 Sat

Table 2: Calibration of the filtering criteria applied to all mixer services The letter "Y" indicates that the criteria can be applied to the mixer services and the letter "N" indicates otherwise. The Bitcoin value is presented in Sat or Satoshis, which is the smallest unit of the Bitcoin (1 Bitcoin is equal to 100,000,000 Satoshis).

- The Blockchain.info's shared send function operates slightly differently than the other mixer services. Instead of peeling the withdrawn Bitcoins and sending them to the users directly, the service always peels off the withdrawn Bitcoins and transfers them to one of its addresses first, before sending them to the users in a one-to-one address transaction type. As such, Criteria 2 and 3 can still be applied for this mixer service case.
- The BitLaunder, DarkLaunder and Helix Light cases use a different version of a peeling technique. Instead of continuous one-to-two address transactions, the mixer services' algorithm peels a single large value transaction input to multiple transaction outputs (one-to-many). Additionally, the mixing algorithm of the BitLaunder and DarkLaunder cases do not always perform the withdrawal transactions in one specific pattern, hence we cannot apply Criteria 2 and 3 for these two mixer services' samples. Moreover, we also cannot apply transaction fee Criterion 5 as the mentioned mixer services regularly adjust the transaction fee based on the transaction size.

The address tainting results show significant improvement in terms of the number of transaction outputs for all of the methods including the Baseline method after applying the filtering criteria, as can be seen in the extensive reduction in the transaction outputs number shown in Table 3. Assuming that our assumptions are correct, and the filtering criteria are correctly adjusted, this would mean that we've reduced a number of false positive transaction outputs.

For the sample cases that can apply more filtering criteria, which are Cases 1 to 7, 14 and 15, the number of false-positive transaction outputs is reduced by from 90% to as high as 99%. Although the transaction output number after applying filtering criteria for the first three methods is closer to the Baseline method at around 10% lower. For example, the number of transaction outputs for Method 1 in Case 5 is reduced by 97% (821,957), but when comparing to the Baseline method's results, the difference in transaction output number is becoming less after applying the filtering criteria from 17% to only 6% lower.

Case Service	*Baseline*	*Criteria*	*Method 1*	*Method 2*	*Method 3*	*Method 4*
1 Blockchain.info	485,155	87	—	—	84	—
2 Bitcoin Fog	713,899	9,804	—	—	—	9,428
3 Bitcoin Fog	1,525,276	12,945	—	—	—	12,320
4 BitLaundry	1,013,374	24,885	23,617	23,661	24,696	24,710
5 BitLaundry	1,016,043	22,712	21,320	21,361	22,376	10,236
6 Unnamed 1	1,337,727	51,099	37,593	37,951	44,440	—
7 Unnamed 2	1,264,966	48,626	38,102	38,587	43,705	—
8 Bitlaunder	1,867,536	385,811	335,268	335,966	373,020	347,389
9 Bitlaunder	2,156,487	428,042	371,251	372,103	411,334	380,805
10 Darklaunder	1,712,521	333,400	280,894	288,290	320,199	319,447
11 Darklaunder	1,845,130	367,516	299,026	315,474	353,674	354,285
12 Alphabay	1,949,670	181,512	154,426	157,425	174,487	174,419
13 Alphabay	2,175,263	227,718	178,960	180,799	215,534	215,539
14 Helix Light	1,858,540	6,329	5,764	5,778	6,166	6,172
15 Helix Light	1,777,542	6,160	5,731	5,792	6,009	6,009

Table 3: Resulting number of transaction outputs with each address tainting method and after applying filtering criteria

The Criteria column refer to the number of transaction outputs of the Baseline method after applying the filtering criteria. Each method column is the result of the method after applying filtering criteria. The colour in each cell represents the percentage of the method's transaction output number after applying the filtering criteria comparing to the Criteria column. The darker colour means that percentage is closer to 100% of the baseline results after applying the criteria.

While the sample cases that have less applicable filtering criteria, which are Cases 8 to 13, generally have lower reduction number of transaction outputs at around 80%. When compared to the result of the Baseline method after applying filtering criteria, the number of transaction outputs show a larger reduction than the other cases at around 20% lower. For example, the number of transaction outputs for Method 1 in Case 11 is reduced by 80% (1,196,509) after applying the filtering criteria, but is 18% (27,086) lower than the Baseline method.

However, there are cases where the results yield different result patterns. For example, with Case 7 and 8, the number of transaction outputs is much lower in the three methods compared to the baseline, unlike the other cases with less applicable filtering criteria. Further, Method 1 in Case 6 has a transaction outputs (after applying filtering criteria) that are 27% less, and Case 7 has 22% less than the baseline. Interestingly, Helix light cases (Case 14 and 15) show the largest reductions in the number of transaction outputs. We hypothesise this is because the constant 50,000 Sat transaction fee used in the one-to-many transaction type by the Helix service makes the withdrawn transactions extremely unusual compared to the other transactions.

The differences in the results may be because the exploitable transaction patterns of mixer services are exceedingly unique patterns that make their transactions possess characteristics that are considerably different from other transac-

tions. Thus, this makes them less difficult to distinguish. We hypothesise that the fewer filtering criteria that can be applied to reduce the number of false-positive results, the more of an advantage the address taint analysis can provide over the Baseline method. Nevertheless, the significant reduction in transaction outputs suggests that the filtering criteria can be adopted for other tracking methods of mixer services in general.

5.4 Limitations

Despite the successful results and potential of the address taint analysis and filtering criteria, there are limitations of our approach that we discuss below.

The number of tainted transaction outputs with and without the filtering criteria are still relatively large when compared to the number of targeted withdrawn transaction outputs, as can be seen in Table 1. The address taint analysis in this paper taints the whole address, similar to the Poison method for transaction tainting, and does not utilise any other additional information besides the information of the deposited transactions. Future research might attempt to further reduce the number of potential outputs.

Similar to other transaction tracking methods, address taint analysis can also be counteracted by the mixer services or the development of new privacy enhancement techniques that defeat the tainting algorithm. This is similar to how the CoinJoin method is introduced to oppose the input-sharing clustering method or mixer services to prevent transaction taint analysis tracking. Hence, the address taint analysis method will always require continuous development and improvement to remain applicable to new transaction obscuring techniques.

The backward tainting approach is also not without challenges. The approach operates with the requirement that the attacker needs to know which mixer service is used for the targeted mixed Bitcoins. As shown in the Bitcoin Fog cases the receiver addresses are not reused addresses and have a very long idle time after receiving the deposited Bitcoins. It would be difficult to perform backward tainting within a similar time frame unless the attacker can identify the mixer service with other means in time, or simply perform backward tainting attacks on every mixer service that uses this type of mixing algorithm.

Additionally, the risk increases if the mixer service uses a better randomised mixing algorithm to obscure any exploitable pattern. As the filtering criteria are currently designed based on the common transaction pattern found in the withdrawn transactions, the current criteria would be less effective as shown in the results of Table 3. This ultimately has a high probability to create inaccurate results if the criteria are applied incorrectly. Thus, to avoid the risk of false incrimination of innocent users, the tracking method should always be utilised with caution and should only be implemented after a thorough exploration of the mixing algorithm involved.

6 Future Work and Conclusion

As transaction obscuring methods improve, so should tracking methods to remain effective and relevant. We identify two possible improvements for both address taint analysis and filtering criteria, as follows;

- *Utilising external information to improve tracking results.* The external information of address ownership can be collected from online websites, forums or services to exclude verifiable and reputable addresses that are unlikely to be a part of the mixer services likes cryptocurrency exchange service from the tainting results [4]. This in turn can significantly reduce both the tainting operation time and the number of false-positive results. However, relying on external information comes with the risk of false or fabricated information depending on the source. Therefore, caution must be exercised to collect information from reliable sources.
- *Incorporating more complex address clustering methods.* There is another address clustering method that clusters based on transaction chain behaviour, instead of a single transaction [5]. For example, when one address distributes its Bitcoins to multiple other addresses, then those addresses transfer all of the distributed Bitcoins to a single address. We can assume that most of the addresses involved are likely to belong to the same user. Such a clustering technique could also be combined to address taint analysis similarly to the one we implemented in this paper.

The address taint analysis method we propose in this paper demonstrates a good potential for reconnecting the original deposited Bitcoins to the mixed Bitcoins – this has not been possible with taint analysis methods. We also illustrate that address taint analysis can be incorporated with other tracking methods such as address clustering and backward tainting for mixer services that utilise an irregular mixing algorithm. Although the number of false-positive results is still not substantially different than the Baseline method when implementing the methods on their own, by exploiting the transaction pattern of the withdrawn transactions to create filtering criteria, the number of false-positive results can be reduced further.

With further improvement, our approach could possibly be used to assist cryptocurrency regulation implementation and cryptocurrency crime forensics in clearing the mystery of past illegal activities, such as exchange service thefts. Nevertheless, more mixing samples from other mixer services are still required for evaluating and improving the tracking method further, considering that mixer services can evolve as new transaction obscuring techniques are introduced.

Acknowledgment

We would like to express our gratitude to Malte Möser, Rainer Böhme, Dominic Breuker, de Balthasar Thibault, Hernandez-Castro Julio C., Rolf van Wegberg, Jan-Jaap Oerlemans and Oskar van Deventer for providing with the transaction information of Bitcoin mixing samples used in their research work.

References

1. Anderson, R., Shumailov, I., Ahmed, M.: Making Bitcoin Legal. In: Cambridge International Workshop on Security Protocols (2018)
2. Anil, G., Yan, L., Hang, L.: Do bitcoin users really care about anonymity? an analysis of the bitcoin transaction graph. In: IEEE Big Data (2018)
3. de Balthasar, T., Hernandez-Castro, J.: An analysis of bitcoin laundry services. In: Nordic Conference on Secure IT Systems (NordSec) (2017)
4. Fleder, M., Kester, M.S., Pillai, S.: Bitcoin transaction graph analysis. CoRR abs/1502.01657 (2015)
5. Harrigan, M., Fretter, C.: The Unreasonable Effectiveness of Address Clustering. In: IEEE Advanced and Trusted Computing (ATC) (2016)
6. Herrera-Joancomartí, J.: Research and challenges on bitcoin anonymity. In: Data Privacy Management (DPM) (2015)
7. Lischke, M., Fabian, B.: Analyzing the bitcoin network: The first four years. Future Internet **8** (2016)
8. Maurer, F.K., Neudecker, T., Florian, M.: Anonymous coinjoin transactions with arbitrary values. In: IEEE Trustcom/BigDataSE/ICESS (2017)
9. Meiklejohn, S., Orlandi, C.: Privacy-enhancing overlays in bitcoin. In: Financial Cryptography and Data Security (2015)
10. 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: ACM Internet Measurement Conference (IMC) (2013)
11. Möser, M., Böhme, R., Breuker, D.: An inquiry into money laundering tools in the Bitcoin ecosystem. In: APWG eCrime Researchers Summit (2013)
12. Möser, M., Böhme, R., Breuker, D.: Towards Risk Scoring of Bitcoin Transactions. In: Financial Cryptography and Data Security (2014)
13. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System White Paper. https://bitcoin.org/bitcoin.pdf (2009), [Accessed: 2020-01-11]
14. Ruffing, T., Moreno-Sanchez, P.: ValueShuffle: Mixing confidential transactions for comprehensive transaction privacy in bitcoin. In: Financial Cryptography and Data Security (2017)
15. Samsudeen, Z., Perera, D., Fernando, M.: Behavioral Analysis of Bitcoin Users on Illegal Transactions. Advances in Science, Technology and Engineering Systems Journal **4**(2) (2019)
16. Simon, B., Xavier, B., Elaine, S., Ersin, U.: Bitter to better — how to make bitcoin a better currency. In: Financial Cryptography and Data Security (2012)
17. Turner, A., Irwin, A.S.M.: Bitcoin transactions: a digital discovery of illicit activity on the blockchain. Journal of Financial Crime **25**(1) (2017)
18. van Wegberg, R., Oerlemans, J.J., van Deventer, O.: Bitcoin money laundering: mixed results? an explorative study on money laundering of cybercrime proceeds using bitcoin. Journal of Financial Crime **25** (2018)
19. Younggee, H., Hyunsoo, K., Jihwan, L., Junbeom, H.: A practical de-mixing algorithm for bitcoin mixing services. In: ACM Blockchains, Cryptocurrencies, and Contracts (BCC) (2018)