Probing the mystery of cryptocurrency theft: An investigation into methods for cryptocurrency tainting analysis

Tin Tironsakkul, Manuel Maarek, Andrea Eross, and Mike Just

Heriot-Watt University, Edinburgh, United Kingdom

Abstract

Since the first theft of the Mt.Gox exchange service in 2011, Bitcoin has seen major thefts in each subsequent year. For most thefts, the perpetrators remain uncaught and unknown. Although every transaction is recorded and transparent in the blockchain, thieves can hide behind pseudonymity and use transaction obscuring techniques to disguise their transaction trail. This paper investigates methods for transaction tracking with tainting analysis techniques. We discuss strategies proposed in the literature and improve on these by presenting new methods applied to a specific theft case. We also propose a metrics-based evaluation framework to compare these strategies with the goal of improving tracking accuracy.

Keywords: Address Profiling, Cryptocurrency, Tainting Analysis, Transaction Tracking

1. Introduction

While Bitcoin is no longer the cryptocurrency with the most effective privacy system today, it remains the most prominent and valuable cryptocurrency in use today with pseudonymous privacy to protect its users' identities. This makes Bitcoin attractive to individuals who are looking for a less traceable currency – compared to traditional currency – to be used for illegal activities, whether it be for dark market transactions, ransomware, scam, gambling, money laundering, prostitution, or even theft of the cryptocurrency itself.

Such illegal activities can diminish Bitcoin's value and its potential to become the official alternative to traditional money. This is even more important for the thefts of cryptocurrency performed on multiple cryptocurrency exchange services. For example, security issues of the cryptocurrency service platforms that result in hacking and theft incidents – such as the hacking of the Coinrail exchange platform on 9th June 2018 with the loss of 30 percent of their total

cryptocurrency holding – caused Bitcoin and other cryptocurrencies prices to drop by almost 10 percent in one hour (Eric et al., 2018).

Since the thefts at cryptocurrency services can affect both the service and its direct users, they can also often cause a negative impact to the economy of cryptocurrencies, which in-turn can affect other users, and even the real-world economy to a degree. It is in the interests of cryptocurrency market participants, and organisations – such as the government, regulatory agencies – as well as researchers to be able to decipher and track transaction network of a cryptocurrency, whether it be for research, crime forensic, law enforcement, or personal interest purposes.

However, because of the privacy protection system in Bitcoin, the tracking of Bitcoin transactions still remains a difficult challenge. In particular, the lack of precise identity information, and the existence of transaction obscuring methods such as laundering services, ease of address creation, and anonymous connections with TOR network[1], allow the perpetrators of cryptocurrency theft to evade the grasp of law enforcement.

As such, this paper will focus on the analysis and tracking of Bitcoin transactions that involve the theft of Bitcoin using *transaction tainting analysis*. The purpose of this paper is to compare tainting strategies, address profiling and other techniques that have the potential to provide the most accurate tracking result. Ultimately, the aim is to reveal the way forward, whereby misappropriated cryptocurrencies find their way into the real financial markets via money laundering activities.

2. Bitcoin transaction tainting

Bitcoin uses an open, distributed transaction ledger called blockchain which allows transaction flow to be easily traced and visualised. However, the tracking of Bitcoin is still difficult to accomplish, especially in the case of finding the exact ownership of tainted Bitcoins. This is due to the fact that, aside from the pseudonymous system, the possession of Bitcoins in each address

[1] TOR is a software that allows user to anonymously connect to its network with data encryption as a gateway to other networks or the Internet.

is in the form of unspent outputs[2], which are newly created from the sum of inputs[3] of previous transactions. As a result, when some (possibly stolen) inputs are combined with other inputs to become new outputs, it is difficult to identify or classify the resulting output for tainting without a clear and precise methodology. The main idea of tainting is that the stolen coins are considered tainted (or "dirty"), and any address that uses or transfers them is also considered to be a tainted address. As such, the tainted coins should not be accepted by other users or businesses; this is similar to how the blacklisting of addresses works.

2.1 Background method

The past literature identifies three strategies or methods for tracking transactions and classifying tainting using transaction information from the blockchain: Poison, and Haircut methods by Möser, et al. (2014), and FIFO (First In, First Out) method by Anderson, et al. (2018). We now discuss each in some more detail.

2.1.1 Poison method

The Poison method is the simplest tainting strategy; the rule is that any transaction output that originated from either a whole, or a part of, tainted[4] input will be considered as a tainted output regardless of the proportion of tainted Bitcoins involved (Möser et al., 2014). This means that the clean Bitcoins involved in the transaction will also become tainted, hence as the tainting progresses, the amount of tainted Bitcoin will increase exponentially over time. Möser et al. (2014) argue that as the method works only on transaction level and not address level, there is no risk of a criminal attempting to sabotage publicly known addresses by purposely sending them a proportion of tainted Bitcoins (so that it becomes mixed with other clean coins). This implies that so long as innocent recipients do not use the tainted outputs along with clean outputs in the same transaction, their clean Bitcoins are safe from being tainted. While this method is considered extreme in terms of the number of Bitcoins impacted, and it has less practical use for blacklisting, the tainting result can still be used to provide a baseline sample or full tainted transaction network for further study and analysis.

[2] The result of each transaction is stored in the form of output, which can be used in the next transaction.

[3] Input is a reference of the output from previous transaction that is being used in the transaction.

[4] In this paper, tainted coin are the coins that are originally stolen from specific address while clean coins are unrelated coins.

2.1.2 Haircut method

The Haircut method works in a similar way as the Poison method, but the Haircut method implements an additional rule: the tainted output value is based on the proportional value of the tainted input (Möser et al., 2014). The tainting compares the proportion of clean and tainted currency in the outputs that are used as the inputs of the transaction, and each output will contain the proportion of tainted and clean Bitcoins appropriately. For example, suppose that a transaction with two inputs, 1 clean Bitcoin and 1 tainted Bitcoin, is sent to two other addresses as two outputs, each at 1 Bitcoin. Each resulting output will then contain a half portion (0.5 BTC) of the tainted Bitcoins and another half (0.5 BTC) of the clean one. This means that the resulting number of tainted addresses and transactions from both the Poison and Haircut policies would be similar, as both consider all the outputs with tainted inputs in the transaction to be tainted. The only difference from the Poison method is that the tainted Bitcoins do not affect the amount of the clean Bitcoins in the Haircut method.

As both Poison and Haircut methods consider every output in the transaction to always receive a part of tainted input, the tainting often results in a large number of tainted transactions and addresses as the mixing between clean and tainted coins increases. The end result of Poison and Haircut tainting usually concludes in a massive portion of active Bitcoins in existence classified as tainted coins.

2.1.3 FIFO method

The FIFO Method (First In, First Out) uses a similar concept from asset inventory management to sort the order of tainting transaction that cannot be specifically identified. The concept can be summarised as follows: the first item that goes in is also the one that goes out first. In the Bitcoin case, the item would be the coins or transaction outputs that are transferred from some addresses to others (Anderson et al., 2018). Similar to the Poison and Haircut methods, FIFO also operates at the transaction level by first looking at the order of inputs of the transaction, after which the method considers transaction outputs.

Anderson et al. (2018) argue that the FIFO method provides more precise tainting results compared to Poison and Haircut methods which would allow the government or organisation to implement more clear regulation or blacklists. As an aside, it is worth noting that the FIFO

method is used in the common law (in English law) for money distribution or withdrawal from an account originated from a historical case in 1816 called Clayton's case.

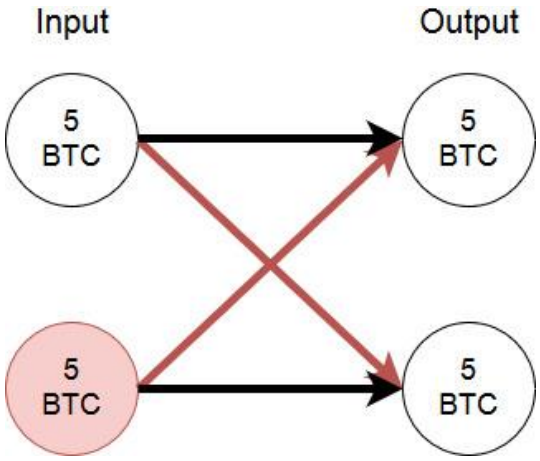

Figure 1: Example of Bitcoin transaction with the comparison of FIFO method and actual transaction context

The diagram in Figure 1 demonstrates an example of a transaction with two inputs and outputs. The red circle represents tainted input/coins. The black arrows represent the transaction flow according to FIFO method, while the red arrows represent actual flow.

Furthermore, the tainting result of this method does not necessarily reflect the transaction's contexts or intended purposes of the senders as demonstrated in Figure 1, where the FIFO method would distribute the tainted coins into the second output based on the transaction order, while the actual intended destination of the tainted coin is at the first output. Hence, the actual context of the transaction can be a contradiction to the tainting result of FIFO. As a result, while this method might solve the issues for legal purposes, it still does not truly solve the problem of tracking accuracy, which is the main goal of the present research paper.

2.2 Proposed new tainting methods

Using the same principle as the FIFO asset inventory management, there are other strategies we propose to implement in the tainting process. We describe these two proposals, LIFO and TIHO, below.

2.2.1 LIFO method

LIFO (Last In, First Out) is an alternative method to FIFO concept of asset inventory management with the ordering reversed from FIFO. Instead of the assumption that the first item that goes in is the first to go out, LIFO assumes the last item that goes in is the first to go out.

As we discussed earlier that using FIFO method alone by itself cannot achieve the aims of providing accurate tainting result as there is a possibility that the result of FIFO tainting does not match the actual context of the transaction. Therefore, we will implement LIFO tainting method to evaluate whether such possibility is true or not.

2.2.2 TIHO method

Using the same principle as in the FIFO and LIFO methods, we design a new tainting method based on the transaction order, but also incorporate the context of the tainting as a factor of the tainting process which is the tainting classification itself. The fundamental assumption in this method is that in the transactions that involve the mixing of clean and tainted coins, the resulting transaction output that has highest value or in other word the address that receive the highest amount of Bitcoin is the main purpose or target of the transaction, and that tainted inputs are the most important inputs of the transaction. In summary, this method prioritises the distribution of the tainted input to the outputs with higher values first, then the remaining clean inputs will be distributed to the other outputs afterwards. We call this tainting method, *Taint In, Highest Out* (TIHO).

This method is not without limitation as the method can still be manipulated by an attacker to purposely make the intended output small in the transaction. Although, there are valid reasons for small outputs such as using large value Unspent Transaction Outputs[5] to purchase products from a merchant. Similar to using traditional large value banknote to buy a cheap product, this would mean that the outputs that go to the merchant address, which is the actual purpose of the transaction would be smaller than the change outputs which is the remaining that goes back to the address belonging to owner of the transaction. For such reasons, this method can be somewhat accurate mostly during the early phases of transferring tainted coins when the tainted coins are still likely to be in the thief's possession.

[5] Unspent Transaction Output (UTXO) is an output that still haven't been used in any transaction.

3. Methodology

3.1 Attacker Model

The attacker model implemented in this paper uses the concept of transaction tainting. The tainting starts from at least one known and confirmed account involved in theft transaction and linking together related multiple transactions and addresses using mainly the information from the blockchain. It is worth noting that the tainting itself does not directly deanonymise the addresses involved, however the resulting transaction pattern found from the tainting can be used to help accomplish such an objective. In this paper, the tainted address classification is slightly different than proposed in previous literature in that while an address would be considered as tainted only after it uses the tainted coins; we will classify an address as tainted from just receiving the tainted coin for tracking purpose.

3.2 Address Profiling

Although deanonymisation, which aims to reveal the real identity of Bitcoin addresses, is not the goal of this paper, we believe that tainting should be context-aware and be adapted to the kind of addresses being tainted. Tainting indiscriminately would miss our goal to understand theft strategies. Address profiling is one of the methods that can assist the tainting by providing the context for the tainting so that it can track the transactions more precisely. As a result, we classify the address profile in Bitcoin into three categories using the information available in the blockchain and the result of tainting methods as follows.

3.2.1 Service address

In this paper, we consider a service address to be an address that has very high transaction traffic compared to other addresses. As high transaction traffic often implies that the address is a point of central exchange for many users, similar to how businesses operate in the real world. Services in cryptocurrency exist in many forms with different purposes such as the followings.

1. *Cryptocurrency exchange services*, where users can exchange cryptocurrency for real money or other cryptocurrencies, e.g., Kraken, Bitflinex or Mt.Gox.
2. *E-commerce businesses* that accept payment with cryptocurrency, e.g., Microsoft, Newegg, Humblebundle and Expedia, among others. This also includes marketplaces or websites that facilitate transactions for the user such as Silk Road Darknet market or gambling sites.

3. Websites or organisational donation sites that accept Bitcoins as donation, e.g., Wikipedia, Reddit, 4Chan and Wikileaks, among others.
4. *Laundering/mixing services*, which are a type of service that helps randomising the transaction flow for the users to make it more difficult to track, such as Helix Mixer, Coinmixer and Bitblender. The service would take a certain amount of Bitcoin from the mixed transaction as their fee, which is usually based on the complexity and number of mixing requested. Each mixing service usually employs different types of mixing methods but generally the complexity of the mixing is more sophisticated with a higher number of mixing transactions, randomness and mixing time (Möser et al., 2013).

In this paper, we classify service addresses by looking at the transaction traffic of the tainted address and comparing to other addresses within a similar time period. If the tainted address has considerable higher transaction number than the average address at the time, then it will be classified as a service address. The boundary that we choose in this paper for an address to be identified as a service address is at 19 total transactions within the limited time period. The classification process and the selection of the boundary for the service addresses will be described in more detailed in the section 4.

Additionally, we consider service addresses to be the end goal or exit point of the tainted transaction. This assumes that all Bitcoin transactions, including those with stolen coins, have the purpose to reach its uses to achieve the real-world monetary value, and thus for the analysis in this paper we consider service addresses to be exit point or usage purpose of the coins.

3.2.2 Tainted Address

A tainted (or dirty) address is any address that the tainting methods consider to be tainted from interacting with the tainted Bitcoins regardless of the amount. As each tainting method employs different ways of tracking and classifying, each tainted address may or may not be classified as tainted in each method. Likewise, the tainted addresses may or may not belong to the accomplices of the theft incident as Bitcoin addresses can be easily created without any cost. In this paper, we use the same classification of tainted address as previous literature but with an exception for the service addresses. In other words, for our results, such as the number of tainted addresses, we don't count beyond the first encounter of a service address in our implementation of each of the tainting methods (Poison, Haircut, FIFO, LIFO, and TIHO).

As we incorporate the address profiling into every tainting method in this paper, the tainting methods used in this paper is a slightly different version than the one present in previous literature. So, the tainting result of the methods used in this paper would also be different. As such we will indicate the inclusion of the address profiling in the methods with asterisk sign (*) behind the method name in our implementation.

Due to the reason that we are using only data from the blockchain for our tainting analysis in this paper, it is still possible for the tainting method to classify addresses that belong to services as a tainted address (in case we don't recognize an address as belonging to a service) especially for services that use multiple short-lived addresses instead of reusing few longer-lived addresses.

3.2.3 Normal/Clean Address

A normal or clean address is any address that does not yet have any interaction with tainted Bitcoins. In the same way as tainted addresses, normal or clean addresses can also belong to the theft accomplices depending on how the tainting method operates. Some tainting methods may mistakenly consider an address as clean, e.g., even when it is the recipient address of stolen coins.

3.3 Evaluation matrix

In order to evaluate the performance of each tainting strategy, we have created an evaluation matrix using information that is available in the blockchain data. We discuss these evaluation metrics in the subsections below.

3.3.1 Transaction fee

A Transaction fee is a number of Bitcoins specified by the transaction sender as an incentive for a miner to prioritise the transaction over other transactions in the process of block mining. The transaction fee is taken from the sum difference of inputs and outputs of the transaction (Satoshi, 2018). Normally, the transaction fee is calculated from the data size of the transaction, which comes mainly from the number of inputs and outputs in the transaction, and the number of transactions that are waiting to be confirmed at the same time.

A Miner is a person or a group of individuals that manages to be the first to complete the block mining challenge provided by the Bitcoin protocol. The challenge involves miners finding the hash of the block they are going to create that is lower than the provided target, which is

calculated from the total mining computation power from every miner who participated in the mining of the previous blocks. Miners will receive rewards of a specific number of Bitcoins and transaction fees of all the transactions included in the block that they mined as the first transaction in the block called 'Coinbase transaction' (Pedro, 2015). While mining could be accomplished by a single person during the early years of Bitcoin, as more individuals join to compete for mining due to increasing value and reputation of Bitcoin, the cost-effectiveness of being a single miner decreases. As a result, miners instead typically join "mining pools" to complete the block mining together and then distribute the reward based on each contribution to the mining.

In this paper, we hypothesize that the amount of the transaction fee in tainted transactions will be higher than normal transactions in order for the thief to obscure his/her transaction trail by rapidly moving the stolen coins; therefore, he/she needs to provide sufficient incentive through the transaction fee to accomplish this. As a result, the tainting strategy with better tracking accuracy should have overall higher average transaction fee for the tainted transactions according to our hypothesis.

3.3.2 Reaching a Service address; the end point of a transaction trail

Using the address profiling method mentioned in section 3.2.1 to classify service addresses, we can observe the point in transaction flow when the tainted coins are received by a service address. We hypothesize that as the thief would want to spend the stolen coins as soon as possible in order to minimise the transaction trail - as the longer the stolen coins are still in his/her possession - the higher the chance for it to be detected. The tainting strategy that shows the earliest route to any service address is more likely to be more accurate in our hypothesis.

3.3.3 Privacy and transaction obscuring measure

While privacy protection is one of the most important aspects of Bitcoin, many users are believed to not be as privacy-conscious as can be observed from the high frequency of reusing addresses (Harrigan and Fretter, 2016). However, due to the nature of the transactions involving theft, we argue that a thief would likely try to employ transactions obscuring and privacy techniques as much as possible in order to prevent tracking. Avoiding the reuse of the same address multiple times is one such technique, as the Blockchain system (including exchanges) allows users to easily create multiple new addresses in a matter of minutes. We assume that the

thief would try to avoid using any address more than once in order to reduce the traceability of the transactions. So, we can use this basis as one of the hypotheses to test the accuracy of each tainting strategy.

The 'reused address' metric does not include service addresses, nor any transactions outside of the limit tainting period. Rather, we will classify addresses that have transactions – including ones from the outside of the limit time period prior to receiving tainted coins – as 'fresh address'. Moreover, since the system allows the user to send their Bitcoins to any address without requiring confirmation from the receiver address, we will classify reused addresses using only the number of sending transactions.

4. Results

In this paper, we use a historical theft as a sample for testing the transaction tainting analysis. The case we are going to use is the Bter hack from 2015, which resulted in theft of 7,170 Bitcoins with the total value of 1.7 million USD at the time (Higgins, 2015). Bter is a cryptocurrency exchange service located in China. Its service was shut down in 2017 due to the Chinese government's ban on the use of cryptocurrency in that year.

The theft occurred on 2015-02-14 at 04:32:26 where the hacker stole 7,170 Bitcoins from the Bter cold wallet exchange[6]. The exchange then temporarily suspended its service and announced the theft in the following day, and further announced a bounty for providing information about the thief (Haggins, 2015). The theft involved only one initial transaction in which coins were moved from Bter's cold wallet address to two other addresses which are `1FETsHZyjppcs8KJUvh82vNCNqsJYD5pWy` and `1KPNHv8mfMPNivHptAiwwytUVZmzovVF8f`. The transaction includes a transaction fee of 0.0055 BTC and it was mined into block 343379 by the F2Pool mining pool.

[6] Cold Wallet is a type of wallet that is stored without connection to any network or internet as a safeguard against theft.

Table 1: The Number of transaction and addresses in each specified time limit

Time limit	**Transaction**	**Address**
6 hours	33,806	100,597
12 hours	60,797	130,515
1 day	161,244	490583
2 days	265,876	671,138
4 days	474,583	1,006,212

For this paper, to test each tainting method, to limit the amount of computational resources required and time taken for our evaluation, we limited the tainting of the transactions to within 4 days after the first distribution transaction of the stolen coins from block 343401. Table 1 shows the exact total number of all transactions and the addresses that appear in the blocks within the time period limit. To test and evaluate the tainting methods, we divide the time limit period into 5 periods which are 6 hours, 12 hours, 1 days, 2 days and 4 days to show gradual change of the results within the space of limited time.

To put this theft into perspective, the total number of Bitcoins in every transaction, excluding the initial theft transaction is 3,692,467.31451518 Bitcoins. At the exchange value of 230 per 1 Bitcoin at the time of the theft, this equals to around 85 million USD. The Bter exchange theft of 7,170 Bitcoins has a value of 1.7 million USD which is around 2 percent of total transaction value within 4 days.

4.1 Service Address Classification

In order to find the most efficient classification of the service addresses, we use the total number of transactions of all active addresses in the same time period as the sample data; next we compare the number of transactions of every address that appears in the blockchain within a six-month period of the theft (three months before and after the theft transaction). There are 17,466,256 transactions and 22,266,571 active addresses in total within the six months period. The results of transaction number percentiles and the service address classification results of each percentile can be seen in Table 2.

Table 2: Percentile of the transactions number of all active addresses within three months before and after the theft transaction

Percentile	**Number of Transactions**	**Number of service addresses**
99.99th	2159	2,231
99.95th	770	11,143
99.90th	485	22,278
99.80th	276	44,615
99.70th	186	66,960
99.55th	118	100,858
99.35th	76	146,458
99.10th	53	201,005
99th	46	225,984
98th	19	452,400

In this experiment, we choose the classification for service addresses to be at the very top percentile of all addresses in the time limit at 99^{th} percentile. As shown in in Figure 2, the majority of the addresses have a low number of transactions at only around two transactions, but the total number of transaction increases exponentially for the addresses at the top percentile. This finding appears to be in line with the finding of Dorit and Adi (2012), which means that sufficient number of users of Bitcoins are concerned enough about their privacy and avoid reusing the same address multiple times. At the 99^{th} percentile, the transaction number required for an address to be classified as a service address is at 19 transaction. At this percentile, 8,058 out of 1,006,212 addresses would be classified as service addresses.

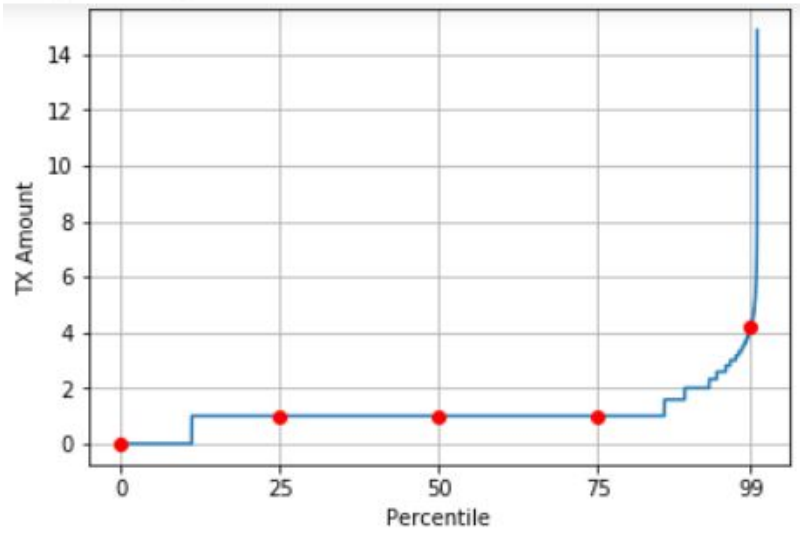

Figure 2: Percentile distribution graph of addresses' transaction number within the four days limit

While choosing the lower percentile would mean a higher chance to include services that employ transaction obscuring techniques, such as laundering service addresses, it would also increase the chance of false classification for the normal addresses. Though it should be noted that there are still many individuals who reuse their address, as pointed out in Harrigan and Fretter (2016). Thus, there is still a possibility that the top percentile addresses are actually not service addresses.

Table 3: The results of each tainting method on the sample data with the four days limit

Variables	6 Hours	12 Hours	1 Days	2 Days	4 Days
Poison* and Haircut* [7]					
No. affected transactions	171	1,084	11,256	28,696	69,840
No. affected addresses	1,271	8,471	55,099	118,002	255,831
No. service addresses	7	80	939	1,999	3,502
No. reused addresses	120	599	4,420	9,235	17,019
No. fresh addresses	829	7,007	43,735	97,184	214,675
Avg. transaction fee value	28,450 sat [8]	30,392 sat	25,799 sat	21,157 sat	19,609 sat
Avg. transaction fee sat per byte ratio	20.27	22.21	26.31	25.85	27.11
FIFO*					
No. affected transactions	24	35	60	64	91
No. affected addresses	62	72	105	109	149
No. service addresses	0	2	2	2	2
No. reused addresses	18	21	27	27	30
No. fresh addresses	20	27	44	46	67
Avg. transaction fee value	30,000 sat	30,571 sat	48,500 sat	47,187 sat	38,901 sat
Avg. transaction fee sat per byte ratio	17.71	21.17	25.1	24.59	24.06
LIFO*					
No. affected transactions	22	29	56	62	78
No. affected addresses	59	66	109	115	140
No. service addresses	0	1	2	2	2
No. reused addresses	17	18	26	26	29
No. fresh addresses	18	21	42	46	60
Avg. transaction fee value	31,818 sat	34,827 sat	68,938 sat	65,000 sat	57,820 sat
Avg. transaction fee sat per byte ratio	18.72	20.96	34.23	32.53	29.93
TIHO*					
No. affected transactions	20	25	44	48	68
No. affected addresses	55	60	83	87	115
No. service addresses	0	1	2	2	2
No. reused addresses	16	17	22	22	25
No. fresh addresses	17	21	32	34	50
Avg. transaction fee value	33,500 sat	38,000 sat	62,045 sat	59,166 sat	46911 sat
Avg. transaction fee sat per byte ratio	18.05	22.12	27.02	26.35	25.62

[7] Due to the fact that we incorporate the address profiling into every tainting method in this paper, the tainting methods used in this paper is a slightly different version than the one present in previous literature. As such, we indicate the inclusion of the address profiling in the methods with asterisk sign (*) behind the method name.
[8] Sat/Satoshis is a smallest unit in Bitcoin value. 1 Bitcoin is equal to 100,000,000 Satoshis.

4.2 Poison* and Haircut*

As the Poison* and Haircut* methods consider all the involved outputs to be tainted, the number of tainted transactions for both methods are the same including the addresses. Hence, we will combine the Poison and Haircut* methods together in the results and discussion section.

The Poison and Haircut* tainting methods result in the highest number of tainted addresses and transactions compared to other tainting methods as shown in Table 3. The results of the Poison* and Haircut* tainting display an intriguing pattern that we didn't expect. While we expect that due to the nature of Poison* and Haircut* method, the number of tainted transactions and addresses would be much higher than the other methods. The number of tainted transaction and addresses that increase in such short amount of time is in a much higher rate than we expected at first.

The number of tainted transactions and addresses increase exponentially within the first day of the tainting period. Furthermore, the tainted coins manage to reach 7 addresses that we classify as service addresses within the first six hours after the first distribution transaction of the stolen coins. Within the first day of the tainting, the tainted coins managed to spread to 55,099 addresses with 11,256 transactions in total and as high as 939 service addresses receive a portion of the tainted coins. At the end of the time limit tainting, there are 69,840 tainted transactions that involve 255,831 addresses and 3,502 service addresses in total.

The number of reused addresses in the Poison* and Haircut* tainting results are considerably high at around 10 percent of the total addresses, though the ratio of reused addresses to total tainted addresses decreases over time. Interestingly, the number of fresh addresses (the addresses that receive tainted transactions as its first transaction) is very high throughout the entire time period. The average value of transaction fee in tainted transactions decreases over time, yet the fee proportion to the size of the transaction actually increases over time.

The first tainted transaction that involves a service address occurs on block 343,435 which is mined at 12:30:29 on 2015-02-14. The transaction occurs roughly 5 hours after the stolen coins' distribution transaction on block 343,401 at 07:34:04 on 2015-02-14.

4.3 FIFO*

As shown in Table 3, The FIFO* tainting method results in a much lower number of tainted transactions and addresses compared to the Poison* and Haircut* methods; moreover, the number of tainted transactions and addresses increase much more steadily compared to the Poison* and Haircut* methods. On the first day of tainting using the FIFO* method, there are 60 tainted transactions with 105 addresses involved and only 2 service addresses appear to receive the tainted coins. On the fourth day, there are 91 tainted transactions and 149 tainted addresses in total. The number of service addresses does not increase further after the first day of tainting.

The number of reused addresses in the Poison* and Haircut* tainting is higher during the first day of tainting, unlike for the Poison* and Haircut* methods, which is at about 20 to 30 percent of the total address. However, similar to the Poison* and Haircut* methods, the ratio of reused addresses to total tainted addresses decreases on the following days. However, the number of fresh addresses is considerably less than for the Poison* and Haircut* methods throughout each tainting time period. The average value of transaction fee is much higher than for the Haircut* method and increases over time; yet, the fee-size proportion of transaction fee pattern is similar, though lower, in comparison to the Poison* and Haircut* methods.

For the FIFO* tainting, the first tainted transaction that involves service addresses occurs on block 343,469 which is mined at 17:01:30. The transactions occur around 9 hours after the first stolen coins' distribution transaction.

4.4 LIFO*

As shown in Table 3, the LIFO* tainting method's results show a similar pattern compared to the FIFO* method results overall; the number of tainted transactions and addresses is slightly lower compared to the FIFO* method results. On the first day of the LIFO* tainting, there are 56 tainted transactions with 109 addresses involved including 2 service addresses. Further, the number of service addresses does not increase further afterwards. On the fourth day, there are 78 tainted transactions and 140 tainted addresses in total.

The number of reused addresses in the LIFO* tainting is almost the same as for the FIFO* tainting method throughout the entire period, including the ratio to the total number of addresses. However, the number of fresh addresses is slightly lower than the FIFO* method. Unexpectedly,

the average value of transaction fee is much higher than both the Poison*, Haircut* and FIFO* methods including the proportion to the transaction size. The average transaction fee is as high as 68,938 Satoshis compared to 48,500 Satoshis for the FIFO* method and 25,799 Satoshis in the Poison* and Haircut* tainting methods. Although, the average value and ratio of the transaction fee gradually decreases on the following days, similar to the Poison*, Haircut*, and FIFO* methods.

The first tainted transaction that involves service address in the LIFO* method is the same one as in the FIFO* method, which occurs on block 343,469.

4.5 TIHO*

As shown in Table 3, the TIHO* tainting method's results show a similar pattern to the FIFO* and LIFO* methods overall, albeit with a smaller number of tainted transactions and addresses. On the first day of the TIHO* tainting, only 44 transactions and 83 addresses are considered to be tainted. The number of service addresses is similar to the FIFO* and LIFO* methods. In the end, there are 68 tainted transaction and 115 addresses in total.

The number of reused and fresh addresses in the TIHO* tainting is slightly lower than for the FIFO* and LIFO* methods but shows a similar increasing pattern as for the other two methods. However, the TIHO* method has a higher number of reused and total addresses ratio than the other two methods. The average value of transaction fee is considerably higher than in the other tainting methods at the early tainting period, but becomes lower than the LIFO* method afterwards, while still much higher than FIFO*, Poison* and Haircut* methods. Despite the higher average transaction fee value, the transaction fee per byte ratio is closer to the FIFO* method than the LIFO* method.

The first tainted transaction that involves a service address in the TIHO* method is the same as the FIFO* and LIFO* methods, which occurs on block 343,469.

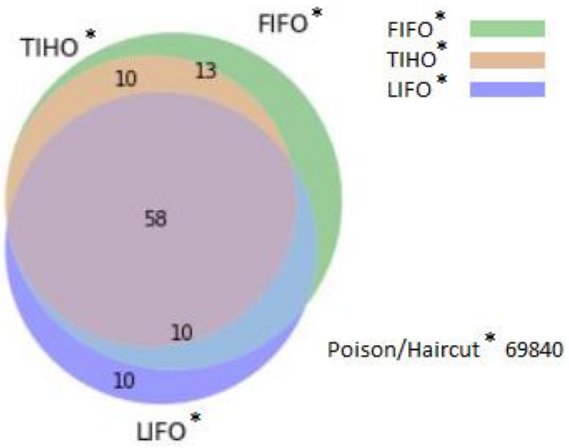

Figure 3: The number of overlapping tainted transactions between three tainting methods within the 4 days tainting limit.

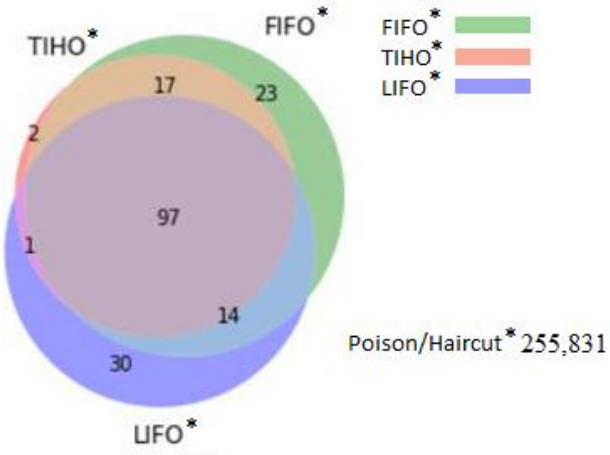

Figure 4: The number of overlapping addresses that receive tainted coins between three tainting methods within the 4 days tainting limit.

As shown in Figures 3 and 4, a significant number of tainted transactions and addresses are considered to be tainted by all the three tainting methods. The FIFO* and LIFO* methods have similar portions of tainted transaction and address that are not shared by the other methods. The TIHO* tainting yields almost the same tainting result as the FIFO* method in this sample case, with a minor difference in the tainted address result.

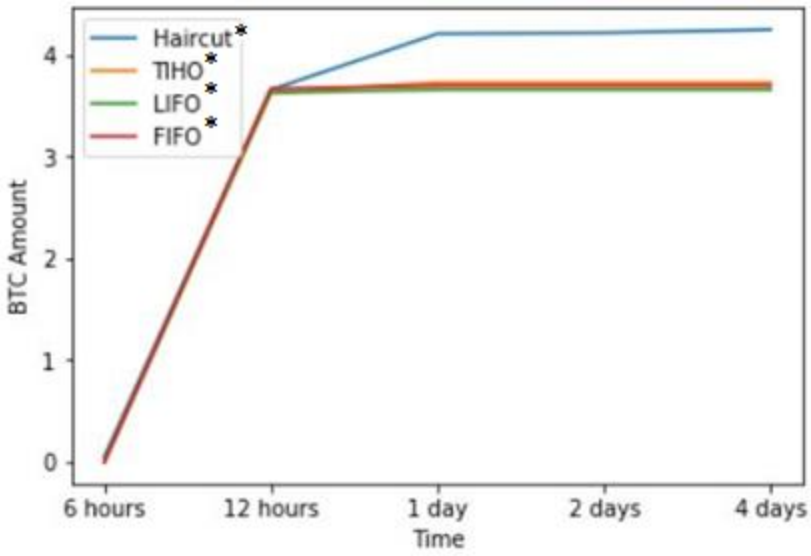

Figure 5: The number of tainted coins received by service addresses at each limit time period for all the tainting methods.

Despite a very high number of service addresses in the Poison* and Haircut* methods, the value of tainted coins that reach service addresses is still rather low as can be seen in Figure 5. This means that most of the transactions that involve service addresses consist of a very low number of Bitcoins overall. The amount of tainted coins that manage to reach the service addresses is very low, at roughly 0.4% of the total tainted coins for all four tainting methods.

The experiment has limitation of the lack of control group for evaluation of the tainting methods. So, we cannot yet compare the tainting result to normal/clean transactions for further evaluation in this paper, this limitation will be addressed further in Section 5.1.

5. Discussion and Evaluation

The result of Poison* and Haircut* tainting methods yield very intriguing and unexpected results. As can be seen in Table 2, the number of transactions that the Poison* and Haircut* methods considered to contain tainted coins is very high on the first day (almost 10 percent of total transactions). We assume that the thief distributes the tainted coins in extremely rapid fashion with high possibility involving money laundering services multiple times right within the first day of the theft. As our implementation of the tainting methods stops tainting at the addresses that have a very high number of transaction traffic within the time period (i.e., likely a

service address), the tainting process is not yet able to effectively detect money laundering service addresses considering the low number of transactions.

However, even with the lack of money laundering transaction analysis and profiling, the number of addresses that the tainting considers to be a service entity is considerably high at 939. There are three possible explanations for the high number of service address that the tainted coins manage to reach within the first day. First, the thief employed the services of the laundering services to mix the tainted coins, then the laundering services mix the tainted coins with other clean coins from other users and distribute portion of them to the other users that also employ the services. This would create a possibility that the addresses that spend the tainted coins on the service addresses that we detected is actually owned by unrelated users. Second, the thief himself spent the stolen coins right away on the first day of the theft. Third, some of the service addresses are actually not service addresses, meaning the users reuse their addresses multiple times.

While we cannot yet confirm which possibility is correct due to the lack of consecutive money laundering analysis, we cannot prove or disprove either of the first and second theory. The third theory can be partially true as while many users do indeed reuse their address, it is still quite unlikely that many non-service addresses would have enough transactions to reach the top percentile of all the addresses. In any case, the only way we can truly disprove those possibilities is by performing further analyses of the involved addresses while considering additional information.

Another consideration that should also be taken into account is that illegal activities are one of the most important aspects of the Bitcoin economy, considering that as high as 33 percent of all Bitcoin transaction involve illegal activities (Foley, 2018). Thus, the classification of service addresses as an exit point of tainted transactions that use only transaction traffic may not be sufficient enough, considering that thieves would more likely prefer spending the stolen coins on the exit points, with the least chance of being caught, as opposed to official services like cryptocurrency exchange services at which governments can enforce laws. As the services or businesses that engage in illegal activities are likely to employ transaction obscuring techniques to protect their own privacy, the address profiling should not solely rely on the number of transactions alone in order to capture more accurate result.

The result of the FIFO*, LIFO* and TIHO* methods display very similar patterns and value, especially during the first six hours. This entails that the majority of the transactions during the first day consists of simple structures of input and output with low amounts of coin mixing, hence the minor difference in value. Yet, the results at the end of the first day and afterwards show significant difference in value between the three tainting methods, despite considerable amount of overlap of transactions and addresses, as shown in Figures 3 and 4.

Overall, the FIFO* tainting result has the higher number of tainted transactions and addresses including the number of reused and fresh addresses of all the three tainting methods. However, in term of proportion between total tainted, reused and fresh addresses, the FIFO* tainting method performs better than both LIFO* and TIHO* methods, considering our hypothesis that the thief would less likely to reuse addresses in order to reduce transactions traceability.

For transaction fee, even though each tainting method presents varied results for both the average fee value and size ratio, they seem to all share the same pattern in changing their value throughout the entire tainting period. Also, while all of the tainting methods have similar results in this aspect during the early tainting, the results seem to greatly diverge passing the first half of the first day tainting. The FIFO* method results in a much lower average transaction fee in its tainted transactions for both value and size ratio compared to the LIFO* and TIHO* methods. The LIFO* method, the tainted transactions have much higher transaction fee than the other two. Based on our hypothesis, the LIFO* tainting results provide the most accurate tracking result in this aspect, followed by the TIHO* and FIFO* methods.

Table 4: The transaction fee of clean transactions according to Poison* and Haircut* methods within 4 days limit period.

Variables	**6 Hours**	**12 Hours**	**1 Days**	**2 Days**	**4 Days**
Avg. transaction fee value	15,746 sat	14,994 sat	15,029 sat	14,661 sat	14,361 sat
Avg. transaction fee sat per byte ratio	35.29	35.50	37.02	37.24	37.79

In order to evaluate the transaction fee results, we also extract the transaction fee of all other clean transactions according to Poison* and Haircut* methods within the same time period as the tainted transaction, which can be used to represent the average transaction fee at the time as shown in Table 4. The transaction fee value and size ratio of the clean transactions are constant throughout the four days period at around 15000 Satoshis and 37 Satoshis per byte. Compared to the tainting results, the average transactions fee for the clean transactions is much lower for every limit time period. However, the transaction fee size ratio is much higher than the tainted transactions from all four tainting methods. We can interpret this difference as follows: due to the higher-than-average value of the stolen coins, the tainted transactions would have much higher transaction fee value than the average transactions in the same period. Although, interestingly, the fee size ratio of tainted transactions in this sample case is much lower than the average transactions ratio. Therefore, it is likely that the thief prioritises saving the stolen coins rather than the speed of transaction confirmation into the block in this sample theft case.

Based on our transaction fee hypothesis, the assumption that the thief would include a higher transaction fee to speed up the transaction confirmation time does not perfectly match the common pattern shown in the result and comparison to the average clean transaction fee in this sample case. The inclusion of those variables still provides an interesting insight due to the distinct difference in transaction fees between the tainted transaction and clean transaction.

While the address profiling of service addresses that we incorporated into the tainting shows interesting results in the Poison* and Haircut* method as there are as high as 3,502 service addresses receiving the tainted coins, our hypothesis for service reaching – that the thief would like to try to spend the stolen coins as soon as possible – is in contradiction to the results shown in Figure 5. Although, the number of service addresses is very high in the Poison* and Haircut*

methods, the total value of the tainted coins that reach a service is very low compared to the total tainted coins involved for every tainting method. This ineffectiveness may be the result of the short evaluation period, as there is also a possibility that the thief would try to “lay low”, until the public awareness decreases before spending the stolen coins.

Nevertheless, the results still prove that there is already certain amount of tainted coins that manage reach addresses that are likely to belong to service entities as soon as the first four days of the tainted coin distribution. This means that the integration of address profiling into the tainting method can improve further the tainting exercise, while providing a more accurate and detailed profiling for both classification and address profiling. This can be achieved by incorporating additional techniques such as address clustering in the likes of input sharing clustering, transaction behaviour clustering, and so on.

5.1 Limitations

There are some limitations in our experiment that we plan to address in our future work. First, the four-day limit used in this tainting experiment may not be able to uncover the full nature of the theft case. In our future work, we will investigate longer durations for every tainting method. Second, the number of sample case, as the theft case that we used in this paper may not share the same characteristics as the other cases. Hence, there is possibility that the variable hypotheses we implement in this paper can work better or worse in other cases. We will include additional theft cases for further evaluation of the tainting methods in our future work.

Third, as described in the result section, there is no control group for the evaluation of the tainting methods. In our future work, we plan to investigate possible control groups, for example by selecting samples from clean transaction within the same time period that possess similar characteristics as the theft transaction, such as the transaction value, the transaction structure and so on, for the evaluation between the tainted transactions and clean transactions.

Fourth is the lack of analysis for transactions involving laundering service. Laundering services are arguably one of the most crucial challenges in transaction tracking as they can obscure the transaction trail even further than normal transaction obscuring methods. It is still possible to discern the flow of transaction mixing by the laundering service based on the common pattern in the mixing methods that each service employs, and even create groups of addresses that likely belong to the same entity with address clustering. This means that cryptocurrency transaction

mixing does not make the transactions completely immune to tracking and tainting (de Balthasar and Hernandez-Castro, 2017).

6. Conclusion and Future Work

While the privacy that Bitcoin can bring to users is revolutionary in today's modern society, the privacy features to commit crimes or even cause harm to others which also bring a negative image to Bitcoin as can often be seen in today's news. In an attempt to combat crime and illegal activities in Bitcoin, tracing the coins to the end of the blockchain alone would only show who are the unlucky winners to be the last holders of dirty coins chosen by the tainting process. In order to truly track the crime in Bitcoin, it is crucial to understand the context of each transaction involved.

The context of the transaction can be obtained by combining both blockchain information and external information that are available in public such as forum website (Michael et al., 2015). The variables we used to analyse the context of transaction in this paper are the transaction information that can be found directly in the blockchain. Such information cannot be falsified due to the nature of the blockchain and bitcoin protocol itself. However, in the case of retrieving the information from external sources, there is a risk of the information being either incorrect or purposely falsified, so extra caution must be exercised when handling external information.

The result of our experiment shows that some of our hypotheses are in conflict of the actual result which means that the comparison between each tainting method still requires further analysis and validation before we can truly measure and evaluate their accuracy. Still, the hypothesis variables that we applied show potential to be used further as evaluation variables in the taint analysis.

The address profiling process can be developed further by incorporating additional techniques such as address clustering and network analysis techniques to assist in the address profiling process, incorporating other information of the transaction as evaluation variables and analysis, Address profiling can also incorporate network analysis to analyse the transaction network to find out the structure patterns of transaction and address, the result can then be used to discern the transaction flow and relationship of the addresses involved in the tainted transaction (Bianconi and Agrawal, 2017).

This paper laid the foundation for our future work on transaction tainting analysis to not only discover the most accurate tainting strategy but to also improve upon the current tainting analysis methods. The results of transaction tainting can then be used for assisting cybersecurity in combating against cryptocurrency cybercrime. This will have important implications not only to cybersecurity but to financial regulatory developments.

References

Anderson, R., Shumailov, I. and Ahmed, M. (2018). Making Bitcoin Legal, In: Matyáš, V. et al. (eds) *Security Protocols XXVI*. Cham: Springer International Publishing. DOI: 10.1007/978-3-030-03251-7_29, pages. 243–253

de Balthasar, T., and Hernandez-Castro, J. (2017). An Analysis of Bitcoin Laundry Services. In H. Lipmaa, A. Mitrokotsa, & R. Matulevičius (Eds.), *Secure IT Systems*. Springer International Publishing. pages 297–312

Bianconi, G. and Agrawal, M. (2017) Predicting Bitcoin Transactions with Network Analysis. University of Stanford. http://snap.stanford.edu/class/cs224w-2017/projects/cs224w-65-final.pdf. Accessed: 2018-10-23.

Dorit, R. and Adi, S. (2012). Quantitative Analysis of the Full Bitcoin Transaction Graph. 10.1007/978-3-642-39884-1_2.

Eric, L., Jiyeun, L., and Jordan, R. (2018). Cryptocurrencies lose 42 billion usd after south korean bourse hack. https://www.bloomberg.com/news/articles/2018-06-10/bitcoin-tumbles-most-in-two-weeks-amid-south-korea-exchange-hack. Accessed: 2018-12-11.

Foley, S., Karlsen,J.R., and Putniņš, T.J. (2018). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? SSRN:3102645.

Higgins, S. (2015) BTER Claims $1.75 Million in Bitcoin Stolen in Cold Wallet Hack. https://www.coindesk.com/bter-bitcoin-stolen-cold-wallet-hack. Accessed: 2019-01-13.

Harrigan, M., and Fretter, C. (2016). The Unreasonable Effectiveness of Address Clustering. In *2016 Intl IEEE Conferences on Ubiquitous Intelligence Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet*

of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld. DOI: 10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld.2016.0071, pages 368–373.

Michael, F., Michael, S.K., and Sudeep, P. (2015). Bitcoin Transaction Graph Analysis. arXiv:1502.01657 [cs].

Möser, M., Böhme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the Bitcoin ecosystem. In *2013 APWG eCrime Researchers Summit*. DOI: 10.1109/eCRS.2013.6805780, pages 1–14.

Möser M., Böhme R., Breuker D. (2014). Towards Risk Scoring of Bitcoin Transactions. In: Böhme R., Brenner M., Moore T., Smith M. (eds*) Financial Cryptography and Data Security*. FC 2014. Lecture Notes in Computer Science, vol 8438. Springer, Berlin, Heidelberg, pages 16 – 32.

Pedro, F. (2015). Understanding Bitcoin: Cryptography, Engineering and Economics. John Wiley and Sons Ltd., 1st edition.

Satoshi, N. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf Accessed: 2018-09-03.