# Poster: De-mixing Bitcoin Mixing Services

Younggee Hong, Hyunsoo Kwon, Sangtae Lee, Junbeom Hur
*Department of Computer Science and Engineering, Korea University*
{gee308, hs_kwon, tkdxo0624, jbhur}@korea.ac.kr

***Abstract*—Bitcoin mixing services improve anonymity by breaking the connection between Bitcoin addresses. In the darkweb environment, many illegal trades, such as in drugs or child pornography, avoid their transactions being traced by exploiting mixing services. Therefore, de-mixing algorithms are needed to identify illegal financial flows and to reduce criminal activities. In this paper, we conduct an in-depth analysis of real-world mixing services, and propose a de-mixing algorithm. The proposed algorithm can effectively find relationships among the input addresses and corresponding output ones of mixing services by exploiting the static and dynamic parameters of mixing services.**

***Index Terms*—Bitcoin, Mixing service, Anonymity**

## I. Introduction

Since Bitcoin [1] addresses act as pseudonyms for their owners, identifying specific users by the addresses themselves is difficult. However, Bitcoin cannot completely guarantee user anonymity for the following reasons. First, since the blockchain is public, anyone can see the transaction flow transparently, which in turn can increase probability of the deanonymization attack by clustering related addresses into a single wallet. Second, most exchanges have a Know Your Customer (KYC) policy. That is, before purchasing Bitcoins, customers must go through the process of authentication, such as by account or mobile phone.

In order to overcome such limitations and improve anonymity in practice, the Bitcoin ecosystem has adopted mixing services. To achieve this, a third-party called a mixer mixes multiple Bitcoin transactions in such a way that the relationships between the transactions are hidden from the outsiders point of view. As a result, they enhance anonymity by disconnecting input and output addresses.

Unfortunately, several studies show that mixing services are being frequently abused for criminal activities such as the trading of illegal goods. For example, *silk road* traded various drugs, malicious code, hacking technologies, credit card information and stolen accounts. In addition, recent ransomware attackers have enforced victims to pay them in Bitcoin by a certain deadline to restore encrypted files. Such cases, also include the use of a mixing service to avoid tracking by investigative agencies.

TABLE I
Transaction increment of mixing service

| Period | Number of transactions |
|---|---|
| 2015-07-01 ~ 2016-06-30 | 186166 |
| 2016-07-01 ~ 2017-06-30 | 795066 |

We looked into the transaction volumes of mixing services from 2015-07-01 to 2017-06-30 to figure out how many people are using them. Especially, we measured the volume of $Helix$, which is one of the most widely used mixing services in practice. As shown in Table 1, the transaction volume from mid 2016 to mid 2017 increased 4.27 times from the previous year, revealing the rapid growth in mixing service usage. Even though several previous studies [2], [3] have been proposed analyzing mixing services, their results are specific to a few specific mixing services, which are now closed. Therefore, we conduct an in-depth analysis of real-world mixing services, and propose a generic de-mixing algorithm.

## II. Related Work

Moser et al. [2], analyzed three mixing services (*Bitcoin Fog*, *Blockchain.info*, *BitLaundry*) using the taint analysis function of *Blockchain.info*. However, some limitations apply when using this method to analyze mixing services these days. First, the taint analysis function of *Blockchain.info* is currently removed. Second, transaction volumes have significantly increased so such manual analyses of a few mixing transactions has become infeasible. Third, *BitLaundry* disappeared from the web and *Blockchain.info* has stopped its mixing service. Therefore, such an analysis method specific to certain mixing services cannot be used as a generic tool for analyzing mixing services.

Balthasar et al. [3], analyzed three mixing services (*DarkLaunder*, *Helix*, *Alphabay*) using Chainalysis, which is a commercial Bitcoin transaction analysis and clustering tool. However, this analysis has similar limitations to Moser et al.'s study [2]. The mixing algorithm can change at any time and mixing services may become inaccessible. *DarkLaunder*, for instance, cannot be accessed these days. In addition, *Alphabay* was terminated by the US Government. Furthemore, their de-

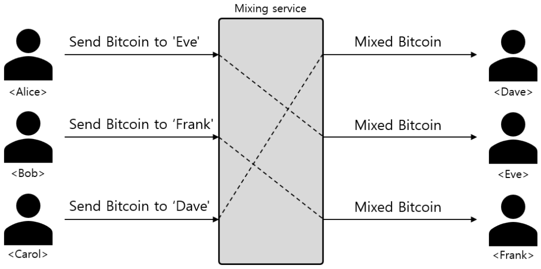

Fig. 1. Mixing service

TABLE II
MIXING SERVICE LIST

| Mixing service | Mixing service fee | Delay | Max_output_address |
|---|---|---|---|
| *CoinMixer* | 1 - 3% | ~120h | 5 |
| *BitcoinBlender* | 1 - 3% | ~99h | 10 |
| *CryptoMixer* | 0.5 - 3% | ~48h | 10 |
| *BitMix* | 0.4 - 4% | ~24h | 5 |
| *PrivCoin* | 0.8 - 3.8% | ~24h | 10 |
| *Bitcoin Fog* | 1 - 3% | ~48h | 20 |
| *BitCloak* | 1 - 3% | ~8h | 1 |
| *Bitcoin Mixer* | 1.5% | ~24h | 10 |
| *Helix* | 2.5% | ~24h | 5 |
| *Helix light* | 2.5% | ~6h | 5 |

mixing algorithm is not generic, and thus limited to specific mixing services. Hence, designing a generic mixing service analysis algorithm remains an open and challenging problem.

## III. Mixing Service Analysis

Bitcoin mixing services improve anonymity by breaking the connections between addresses. If there are multiple input-output transaction pairs, the mixer mixes them in such a way that associating input and output transactions from the outsider's point of view is impossible, as shown in Fig 1. Fortunately, we can reduce the anonymity level by using other information such as time and Bitcoin (BTC) transaction values. Therefore, we analyze the mixing parameters commonly used in practical mixing services.

- **Mixing service fee**. Most mixing services receive various fees rather than a fixed one. The amount of the mixing fee is set by the user or randomly determined by the mixing service. The randomness of the mixing fee is used to make it difficult to associate the input and output transactions.
- **Delay**. If the mixing service generates output transactions as soon as it mixes the input transactions, time-based attacks are easily possible. Therefore, mixing services avoid this by setting delays to some extent. The delay is set by the user or randomly determined by the mixer.
- **Max_output_address**. The mixing service can split an input into multiple outputs. Most mixing services can also set a different delay time for each output. Thus, splitting transactions with different delays makes the services much less vulnerable to de-mixing.

Analyzing mixing services would be complex if there parameters were used in a diverse combinatorial way. However, after investigating real-world mixing services, we found there is a gap between the theoretically achievable and practically implemented anonymity. As shown in Table II[1]. For *Bitcoin Mixer*, *Helix* and *Helix light*, the mixing service fee is fixed. If the fee is fixed, the output value can easily be calculated and used to find possible connections to given input addresses. In the next section, we propose a de-mixing algorithm by exploiting these observations for real-world mixing services.

## IV. De-mixing Algorithm

We have designed a de-mixing algorithm for mixing services where the mixing service fee is a fixed fee. The de-mixing algorithm procedure is as follows.

1) **Filtering step.** For each input, it extracts the output set satisfying the following conditions.
   a) The output time is between input time and input time + Delay provided by the mixing service.
   b) The Bitcoin output value is less than the input value.

   This step reduces unnecessary combination operations in the next step.
2) **Combination operation step.** It calculates all combinations in the output lists extracted from the filtering step that can be made up to Max_output_address (provided by the mixing service) or less.
3) **Matching step.** It compares each sum of result values calculated in the combination operation step and (Bitcoin input values) $*$ (1 - mixing service fee). If there is only a single match, which means a unique relationship is found, go to the next removing step.
4) **Removing step.** It removes the input and corresponding outputs that matched in the previous step, and repeats the algorithm from the first filtering step.
5) **Termination step.** If matching fails for all remaining inputs, the algorithm cannot determine the unique output transactions associated with a given input transaction. The algorithm terminates and prints the candidate output list corresponding to each input.

## V. Conclusion and Future Work

In this study, we investigated several real-world mixing services, and their mixing policies. As a result, we found some traceable features which can be practically exploited to analyze the mixing service. On the basis of these observations, we designed a generic de-mixing algorithm to find input-output relationships among the mixed transactions. As future work, we will verify the algorithm based on the real-word data.

## Acknowledgment

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIP) (No.2018-0-00477, Development of Malware Analysis Technique based on Deep Web and Tor). This work was also supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIP) (No. 2016R1A2A2A05005402).

## References

[1] Nakamoto, Satoshi."Bitcoin: A peer-to-peer electronic cash system." (2008).

[2] Moser, Malte, Rainer Bohme, and Dominic Breuker. "An inquiry into money laundering tools in the Bitcoin ecosystem." eCrime Researchers Summit (eCRS), 2013. IEEE, 2013.

[3] de Balthasar, Thibault, and Julio Hernandez-Castro. "An Analysis of Bitcoin Laundry Services." Nordic Conference on Secure IT Systems. Springer, Cham, 2017.

[1] As of January 3, 2018.