Analyzing the peeling chain patterns on the Bitcoin blockchain

By:
Yanan Gong, Kam Pui Chow, Siu Ming Yiu, Hing Fung Ting

From the proceedings of
The Digital Forensic Research Conference
DFRWS APAC 2023
Oct 17-20, 2023

Forensic Science International: Digital Investigation 46 (2023) 301614

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

DFRWS 2023 APAC - Proceedings of the Third Annual DFRWS APAC

Analyzing the peeling chain patterns on the Bitcoin blockchain

Yanan Gong *, Kam Pui Chow, Siu Ming Yiu, Hing Fung Ting

The University of Hong Kong, Hong Kong, China

ARTICLE INFO

Keywords:
Bitcoin
Peeling chain
Self-change address
Behavior pattern

ABSTRACT

Bitcoin is a widely used decentralized cryptocurrency. The proportion of Bitcoin transactions used for illegal activities is increasing. Mixing services are commonly applied to enhance anonymity and make transaction records more challenging to follow and analyze. The current research on peeling chains is generally based on heuristic algorithms to identify change addresses. However, due to the characteristics and limitations of the Bitcoin blockchain, there is no such ground truth to ensure the accuracy of each derived change address. This research analyzes the peeling chain patterns based on self-change addresses. The use of self-change addresses implies that the input address and the address used for receiving the change are controlled by the same entity. Also, each chain's transaction details and generated chain parameters are further verified for more precise results. Combining the two methods ensures the accuracy of the extracted peeling chains to some extent. And the corresponding behavior pattern of the extracted chains is studied.

1. Introduction

Bitcoin was created in 2008 (Antonopoulos, 2014). Now it is a widely used decentralized cryptocurrency. Distributed ledger makes all transactions on the blockchain public and transparent. The money flow from a target Bitcoin address can be easily traced using Bitcoin Explorer. Bitcoin is pseudo-anonymous. Users create transactions through addresses consisting of letters and numbers without associating with real-world identities. Except for daily trading, Bitcoin is also popular for illegal actions. One famous case, WannaCry (Chen and Bridges, 2017), yielded worldwide disaster. According to the crypto crime report from Chainalysis (Chainalysis Team, 2023), last year, 2022, the share of cryptocurrency transactions correlated to illegal activities reached an all-time high of $20.6 billion.

When law enforcement agencies investigate crypto crimes, a critical forensic approach is to trace and analyze the money flow. And researches on Bitcoin de-anonymization have constantly been developing. Examples include address clustering (Meiklejohn et al., 2013; Zhang et al., 2020; Harrigan and Fretter, 2016), where different Bitcoin addresses are clustered together to uncover associations between these addresses, analysis studies for the behavioral patterns of Bitcoin transactions (Xiang et al., 2022; Phetsouvanh et al., 2021; Chen et al., 2019), and the classification of participants and entities in the Bitcoin blockchain network (Makarov and Schoar, 2021; Jourdan et al., 2018; Zola et al., 2019). However, criminals would exploit various approaches to launder the illegally acquired currency to evade being tracked by law enforcement. Mixing services are ordinarily employed to enhance anonymity and make transaction records more challenging to follow and analyze. The peeling chain is one technique used by mixers or laundry services (de Balthasar and Hernandez-Castro, 2017). It starts from a Bitcoin address and repeatedly peels off small amounts (Meiklejohn et al., 2013). In the Bitifnex hack, peeling chains were used to split some of the stolen funds (Statement of Facts).

Based on different assumptions, definitions, and conditions, the current studies have proposed various approaches for revealing peeling chains. Generally, when peeling, the larger amount will be transferred to a change address. The present research on peeling chains is usually based on heuristic algorithms to identify change addresses. However, due to the nature of the Bitcoin blockchain, it is impossible to associate each Bitcoin address with its actual owner. For example, the new change address identified in one peeling chain may be wrong; it may be a payment address. There is no such ground truth for the real-world Bitcoin blockchain. Therefore, it is challenging to evaluate the true quality of peeling chains obtained from heuristics. There is no guarantee of absolute accuracy. The behaviors derived rely on pre-defined hypotheses and features. There may be biases and errors that require further examination. Also, heuristics are based on particular conditions, and there are constraints on the execution. Once the user behaviors or blockchain technologies like wallet protocol change, some heuristics could be ineffective.

* Corresponding author.
E-mail address: u3556305@connect.hku.hk (Y. Gong).

https://doi.org/10.1016/j.fsidi.2023.301614

Available online 13 October 2023

Our research analyzes the peeling chain pattern based on self-change addresses. In the transaction, the usage of self-change addresses indicates that the input address and the address used for receiving the change are controlled by the same entity. Firstly, a preliminary definition is proposed, which does not involve redundant assumptions and constraints. Chains are collected from the Bitcoin blockchain network based on this definition. In addition, each chain's transaction details and generated chain parameters are examined to determine potential peeling chains. Finally, uncover corresponding behavior patterns by analyzing these chains. Our study can ensure certain reliability of recognized peeling chains and further guarantee the accuracy of the obtained behavioral patterns. The results may provide reference information and ideas for crypto investigators. The rest of this paper is organized as follows. Section 2 describes related work. Section 3 introduces how to extract peeling chains and get chain-related parameters. Section 4 further determines and verifies chain data and studies the behavior patterns of these potential peeling chains. The last section is the conclusion and outlines future research work.

2. Related work

There is no requirement in the Bitcoin network to use real names. It safeguards user privacy to a certain extent. But all transaction details are transparent. Bitcoin provides pseudo-anonymity (Conti et al., 2018). The publicly available blockchain data can be utilized to trace the flow of Bitcoin. By combining external information, Bitcoin addresses can even be linked to some actual owners behind them. Two widely used address clustering heuristics were first proposed by Meiklejohn et al. (2013) to cluster potentially related Bitcoin addresses. An approach that correlates Bitcoin addresses with IP data is presented by Koshy et al. (2014). At the same time, various mixing algorithms and designs have been introduced to improve security and privacy, such as Coinjoin (Greg Maxwell, 2013) and CoinShuffle (Ruffing et al., 2014). With the development of blockchain technologies and increased user security awareness, mixing services are generally adopted to strengthen anonymity. For whatever purpose, bitcoin mixers, also known as tumblers, are often used for Bitcoin transactions to avoid blockchain transaction analysis. Centralized mixers such as Blender.io (Blender.io) collect users' funds to mix. Decentralized mixers, conversely, do not need to rely on third-party services, such as Wasabi Wallet (Wasabi Wallet). Mixing services can lower the possibility of tracking and make money flow analysis more challenging and complex (Chen et al., 2019). And mixing services are frequently used for criminal activities like money laundering (Pakki et al., 2021).

When investigating cryptocurrency-related illegal activities, law enforcement authorities will trace and study the flow of cryptocurrency money. The research community has proposed different methods for Bitcoin mixing detection, for example, aiming for anti-money laundering prevention. Some studies explore Bitcoin mixers in the real world. A comprehensive overview of Bitcoin laundering tools is shown by Möser et al. (2013). Through reverse engineering, this work studies the operation modes and limitations of those mixing services and provides guidance for anti-money laundering. Pakki et al. (2021) interact with real mixing services, and real-world data is collected and analyzed. And an overview of the public Bitcoin mixer ecosystem is provided. de Balthasar and Hernandez-Castro (de Balthasar and Hernandez-Castro, 2017) conduct an investigation of some real-world tumblers and mixers to identify their characteristics. The study demonstrates some limitations and regularities of examined mixing services.

A part of the research develops various techniques to detect mixing related transactions, addresses, etc. Prado-Romero et al. (2018) apply a social network model to represent the Bitcoin network and explore mixing related accounts through outliers within the community. A transaction network analysis structure based on features is presented by Wu et al. (2021a). Network motifs are employed, and PU learning is utilized to represent the mixing detection problem. The framework determines the statistical characteristics of mixing services at the network, account, and transaction levels. In (Nan and Tao, 2018), Bitcoin transaction graphs are shown to have community properties. A more efficient deep learning way recognizes features from real-world mixing services. However, it has three drawbacks. And the mixing service transactions cannot be accurately characterized due to the lack of labels. Interacting with mixing services, from transaction and chain level (Shojaeenasab et al., 2022), differentiates typical features and discovers patterns. Based on these data, an integrated algorithm is proposed to detect mixing transactions, etc. However, accuracy and recall cannot be obtained because of the absence of authentic labels of addresses. Sun et al. (2022) generalize mixing detection as a transaction classification issue and apply transaction trees to trace mixing transactions. An LSTM Transaction Tree Classifier (LSTM-TC) algorithm is introduced, and it is tested with a pre-build mixing dataset, which achieves a good recall. However, it is still being determined whether all features from huge transactions can be covered, and the shortage of labeled data for experiments is a problem. Hu et al. (2019) demonstrate a node2vec-based classifier for finding laundering activities. Transaction graphs are adopted to separate laundering transactions from normal transactions to categorize and analyze graph features. The work is restricted due to inadequate trustworthy label data for illicit transactions. In (Wu et al., 2021b), current mixing service mechanisms are classified as obfuscating and swapping. And a heuristic-based algorithm and transaction analysis approach are presented for mixing-related detection, which is examined with real Bitcoin mixing services. But there may still be some uncertainties in the measurements due to the absence of absolute ground truth.

The peeling chain technique is everywhere. It is implemented in exchanges or gambling (Ahmed et al., 2019). It is also extensively applied for mixing services (Wu et al., 2021b). When mixing, the redirection of funds can be achieved through different peeling chains (de Balthasar and Hernandez-Castro, 2017). To avoid tracking where the illicit fund is going, peeling chains are an easy and suitable way to distribute money for money launderers. The peeling chain starts with a single Bitcoin address, and a small amount of Bitcoin keeps getting peeled off (Meiklejohn et al., 2013). For example, an address containing 30 BTC peels off 3 BTC the first time and 2 BTC the second time, and the peeling process is repeated until the funds are split into many small amounts. These small amounts can flow to different addresses or services to obfuscate money tracking. Wu et al. (2021b) divide peeling chains as a swapping mechanism of mixing services. The peeling chain is represented by starting, middle, and ending points. The end node is determined by whether the change output from this node is used for a multi-input transaction. de Balthasar and Hernandez-Castro (de Balthasar and Hernandez-Castro, 2017) think transactions on the peeling chain may include two to five outputs, and one general feature exhibited by peeling chains is that the chain node is only related to one receiving transaction and one sending transaction. Based on the address, transaction, and cluster features, Kappos et al. (2022) propose a new heuristic to identify peel chains. The heuristic starts from the cluster generated by the co-spend heuristic, then each transaction within the cluster will be examined by an algorithm to obtain the corresponding peeling chain. Even though the dataset is provided and manually verified by Chainalysis, it is still hard to determine the quality of the results. There needs to be relevant data to prove the correctness of these chains.

3. Chains on the Bitcoin blockchain

The blockchain data until UTC 2023-01-16 01:35:09 (block height: 0–772162) was parsed. The whole data has 796,564,036 transactions in total. We used BlockSci (Kalodner et al., 2020) to extract the relationships among all transactions. BlockSci is a blockchain analysis tool that assigns each transaction an internal index. The provided 'spending_tx_index' links a specific transaction output to the next transaction.

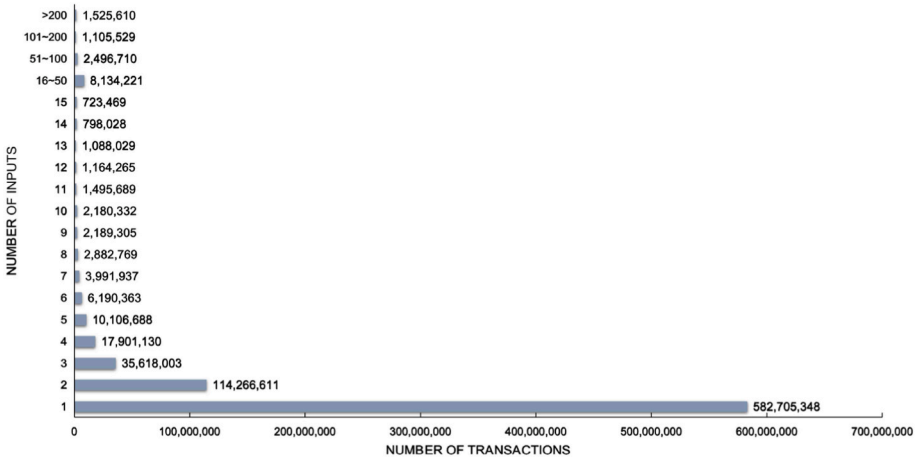

Fig. 1. Distribution of different numbers of inputs (Bitcoin blockchain).

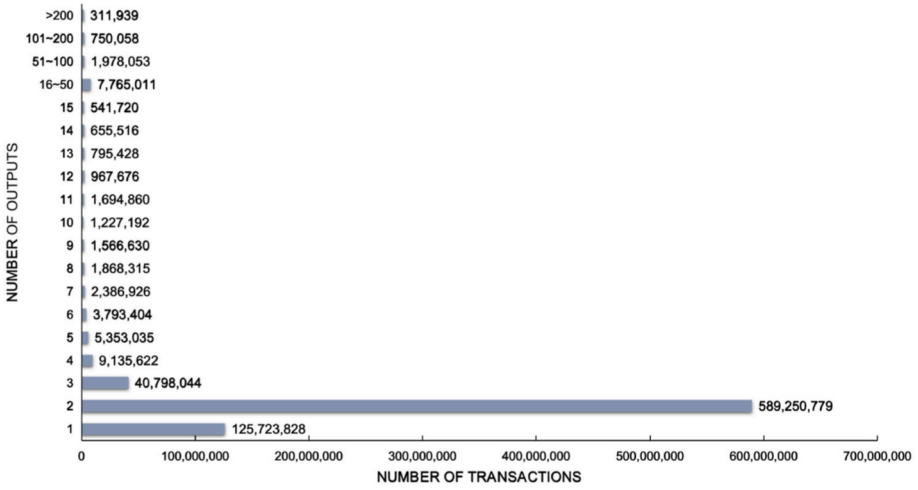

Fig. 2. Distribution of different numbers of outputs (Bitcoin blockchain).

3.1. Preliminary definition

The peeling chain starts from a Bitcoin address and peels off Bitcoin repeatedly (Meiklejohn et al., 2013). A Bitcoin transaction can have a random number of inputs and outputs. The input and output ratios of the parsed blockchain data were calculated. The distributions of different numbers of inputs/outputs are shown in Figs. 1 and 2. From the distribution results, it can be seen that the vast majority of transactions have input/output numbers between 1 and 6. For input, one input has the highest proportion of transactions, accounting for 73.1524%. For outputs, the largest percentage of transactions with two outputs is 73.9741%. The total number of transactions with one input and two outputs is 448,723,821, which accounts for 56.3324%. It is more than half of the total number of transactions.

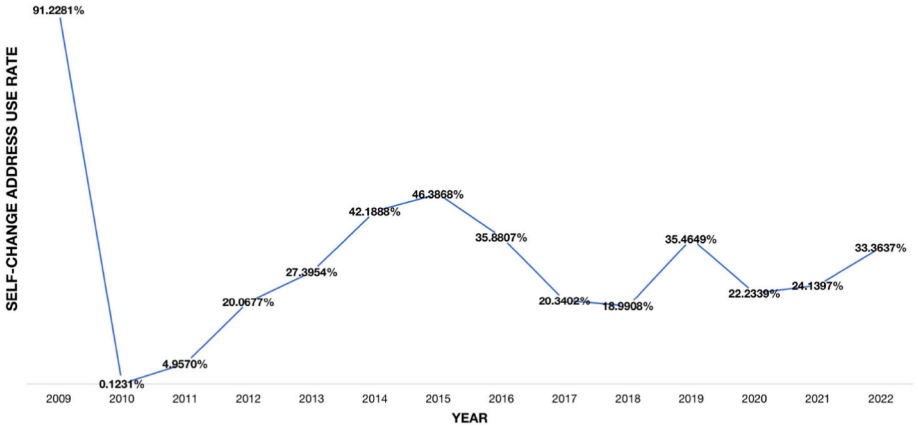

Fig. 3. Self-change address use rate.

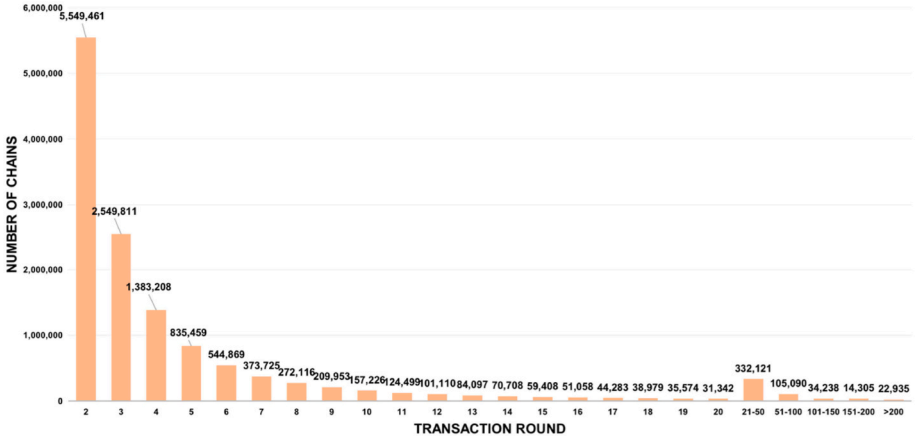

Fig. 4. Distribution of transaction rounds (Raw Dataset).

In current studies, most of them utilize the one-time change (OTC) heuristic (Meiklejohn et al., 2013) or its variants to identify the change address in a transaction. The OTC heuristic depends on address reuse (i.e., the appearance of an address) to determine the change address. With the development of blockchain technologies and increased user security awareness, the wallet usually generates a new address to receive Bitcoin for a transaction. Current heuristic algorithms are based on pre-defined hypotheses and characteristics. And because of the nature of the Bitcoin blockchain, it is impossible to reveal the real-world owner for every address. Hence, the change addresses produced by heuristics may contain errors. For example, a transaction with two outputs may have two receivers and has no change. But if one output meets pre-defined conditions, it is recognized as a change address, which will cause a false positive. In a transaction, a self-change address represents the address used to receive the change, the same as the input address (Meiklejohn et al., 2013). Bitcoin transactions require a pair of keys. The creation of a transaction needs the signature of the private key. For transactions with one input and two outputs, if one output is the self-change address, then the self-change output is undoubtedly the address used to receive the change. And the input address and change address are identical, which further illustrates that the input amount and the change amount are controlled by the same entity. The self-change address use rate for each year is calculated in Fig. 3. The percentage value means the proportion of transactions using self-change addresses among transactions with one input and two outputs. Last year, 2022, for transactions with one input and two outputs, the percentage of transactions that include the self-change address was 33.3637%. It is still common to use self-change addresses in Bitcoin transactions.

According to the above discussion, our preliminary definition for extracting peeling chains is as follows:

- Each transaction on the peeling chain only has one input and two outputs. One output is used to peel off part of Bitcoin, and the other is to receive the change. Under this condition, coinbase transactions cannot be the start transaction of a peeling chain. A coinbase transaction is used to obtain the block reward, and its input does not hold a valid address with the UTXO (Unspent Transaction Output) reference. It displays the coinbase field information. In some Bitcoin Explorers, like WalletExplorer (WalletExplorer.com), the input of the coinbase transaction is set to zero. In this research, the input number of the coinbase transaction is zero.
- In the two outputs, one is the self-change address. And the self-change address is a valid Bitcoin address. The condition is not satisfied if the address field is null. Note that the situation with two self-change addresses does not meet this condition.

3.2. Chain extraction

Based on the above definition, chains that satisfy these two conditions are extracted from the Bitcoin blockchain. This kind of chain includes at least two successive transactions. And this is the formation criteria for the smallest length of chains. Collect as much data as possible from the blockchain to avoid the loss of any potential peeling chains. The collected data requires further processing as the complexity of the Bitcoin blockchain. Remove non-necessary data records and errors to make the dataset more accurate. Perform pre-processing for the gathered data. Bitcoin blockchain allows the existence of Null data/OP_RETURN/Data carrier transactions (Null Data, OP_RETURN). Users can store data on the blockchain through the OP_RETURN opcode script (Null Data). The immutability of the Bitcoin blockchain ensures that the stored data is irreversible. Such transactions exist in the blockchain, and one of their outputs is OP_RETURN type, also known as null-data output type. This kind of output does not have a valid Bitcoin address and is not for trading. Outputs with OP_RETURN opcode cannot be spent (Bistarelli et al., 2019). Therefore, the transactions with OP_RETURN outputs are not peeling chains.

Check the obtained chain data and delete transactions containing the OP_RETURN type. Generally, the OP_RETURN output does not carry any Bitcoin amount. First, check the output amount for every transaction on each chain. The transaction is discarded if one output amount is zero. Bitcoin blockchain is different from the Ethereum blockchain. Sometimes the output of a transaction on the Ethereum blockchain is shown as 0, and the transaction may be a token transfer. BRC-20 (BRC-20 Tokens), the token based on the Bitcoin blockchain, was introduced in March of this year (Katie Rees, 2023). Our blockchain data collection is until January this year, and token transactions will not be considered. Among the chains having at least one OP_RETURN output, it is found that OP_RETURN outputs may contain Bitcoin, i.e., 0.00000001 BTC. In this case, all output addresses are further examined to see whether they are the null data type without valid Bitcoin addresses. The record is removed if the address type is null data and the address field is null. While processing, the entire chain containing OP_RETURN output is not removed directly. To avoid data loss, the chain will be rearranged according to the index (position) of this transaction. The new chain could be formed if at least two successive regular transactions exist.

Non-standard transactions exist in the Bitcoin blockchain. This type of transaction is rare, and the occurrence sometimes is the cause of errors (Bistarelli et al., 2019). Non-standard transactions are not considered. After pre-processing, the original chain dataset includes 13,025,575 chains, and the total number of transactions is 83,215,800.

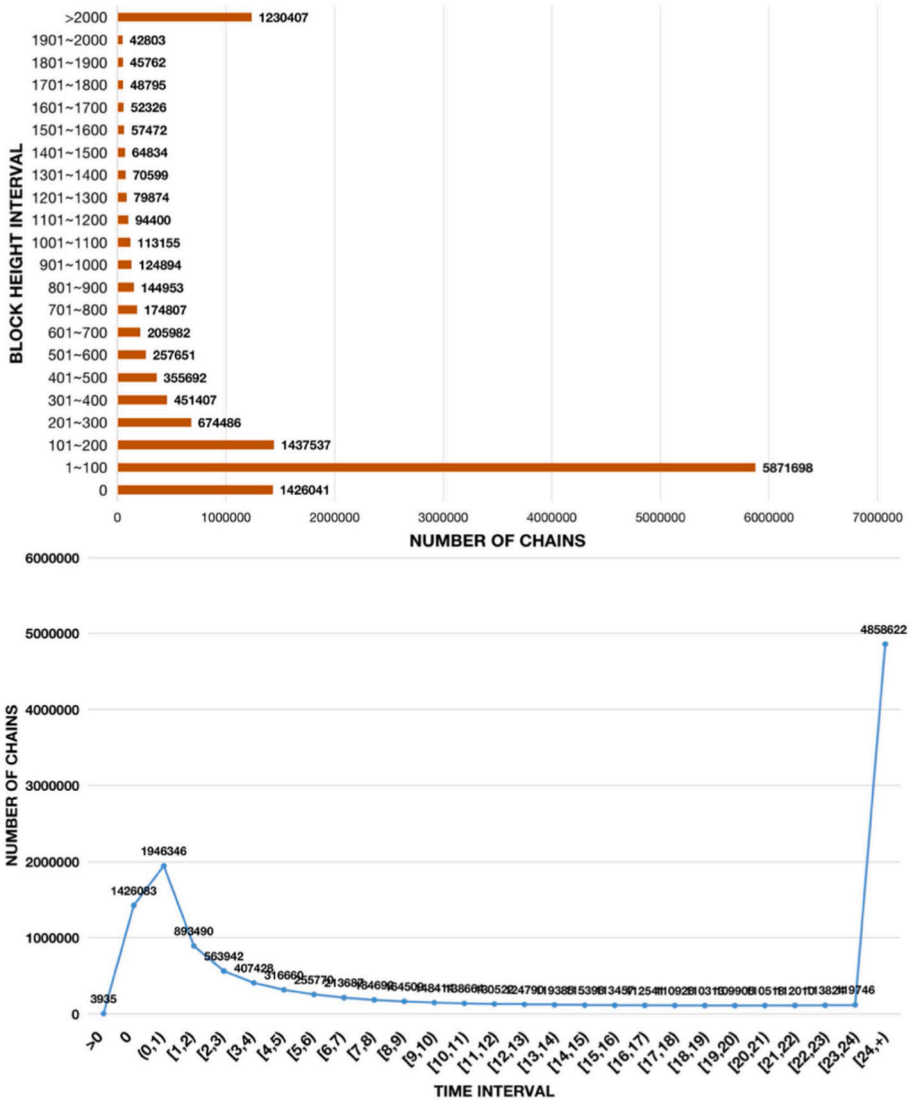

Fig. 5. Distribution of time/block intervals (Raw Dataset).

3.3. Chain parameter

Some chain-related parameters need to be calculated for subsequent observation and analysis. For each chain in the dataset, transaction round, time interval, block height interval, peeling amount, and peeling percentage are computed.

Transaction round. It indicates how many times Bitcoin amounts have been peeled off from a starting address when finishing a series of peeling. It is the total number of the peeling process. **Time interval.** It represents the interval between the transaction time of the first transaction and the time of the last transaction. There are two expressions for this parameter. The original interval shows the difference between two Unix timestamps. The other form is transformed into the human date and represented by hours. **Block interval.** It is the interval between the block height numbers of the last transaction and the first transaction on the chain. **Peeling amount.** It is the Bitcoin amount of each non-self-change output. That is the amount peeled off each time. **Peeling Percentage.** It is the percentage of the peeled Bitcoin amount to the input amount of this transaction. Fig. 4 shows the distribution of transaction rounds in the raw dataset. It can be seen that the proportion of chains with two transaction rounds is the highest, at 42.6043%. It is approaching half of the total number of chains. And Fig. 5 shows the time/block intervals for the raw dataset. The time interval is in hours. As can be seen, most chains have large time/block interval values. Some chains took longer than a day to create. The creation time of most chains is long, and large block height intervals exist. There are even some block intervals exceeding 32,400 blocks.

4. Pattern analysis

According to existing studies, peeling chains can have thousands of peeling series. The formation criteria for the smallest length of chains is to have at least two successive transactions. To prevent the loss of potential peeling data, chains with small transaction rounds will not be removed directly. Although there are many studies for mixing detection, the Bitcoin blockchain has no such ground truth data. There is no mixer revealing all mixing-related transaction details inside the service. Thus, any length of chain collected should be subjected to further examination.

4.1. Peeling chain determination

In the Bitcoin blockchain, the peeling chain is a commonly used technique. Not only can it be used for mixers but also exchanges. Our objective is to identify peeling chains generated by mixers and derive their behavior patterns. In general, mixers make use of auto-program

scripts to process a large number of transactions. Manually generated transactions are extremely unlikely, meaningless, and time-consuming. In order to determine the specific peeling chains generated by mixers, the internal details of the transactions and chain statistics are examined.

4.1.1. Transaction details

First, pay attention to the details inside the Bitcoin transaction script. The transaction version (Transactions), which specifies the version number of the transaction, can be either one or two. And each transaction has the 'lock_time' field (Transactions), which indicates the time or block height number that the transaction can be valid. The input for non-coinbase transactions includes the sequence number field (Sequence Number (Transactions)), which announces whether the transaction can be updated before the locktime. It is usually the default value, 0xFFFFFFFF (Transactions). The default one does not affect the transaction. A sequence number smaller than the default value, i.e., 0xFFFFFFFE, suggests that the transaction enables lock time. With the introduction of transaction replacement, sequence numbers below 0xFFFFFFFE can be used for Opt-in Replace-by-Fee (RBF) from 2016 (Opt-in RBF FAQ). Opt-in RBF indicates whether the transaction can be replaced. That is to increase the transaction fee to facilitate transaction confirmation. In the obtained chain dataset, the input number of transactions is always one, so there is only one sequence number for each transaction on a chain.

Second, focus on the address script details in Bitcoin transactions. There are different kinds of Bitcoin addresses, such as the pay-to-public-key-hash type. BlockSci (Kalodner et al., 2020) is utilized to classify address types, and it can categorize addresses in the Bitcoin blockchain into ten general types. Our preliminary definition requires all transaction addresses in the chain to be valid Bitcoin addresses. However, BlockSci is no longer developed since November 2020 (BlockSci Developers, 2020). For example, the outputs of the 'WitnessUnknownAddress' type have valid Bitcoin addresses, and BlockSci cannot parse address strings. For transaction records that BlockSci cannot generate the address strings, further parsing and checking are performed. As of block height 481824, which is August 2017, the Segregated Witness (SegWit) consensus rule can be executed (Segregated Witness Wallet Development Guide). SegWit has altered the format of Bitcoin transactions, and its introduction is to deal with the concerns related to transaction malleability (Bitcoin Developer Guide). It improves the speed of Bitcoin transactions, and SegWit transactions can achieve fewer transaction fees. If the wallet employed by mixers supports and enables SegWit, then all transactions created by that wallet should be SegWit transactions. Set a SegWit flag for each transaction.

Based on the above analysis, parse the transaction version number, 'lock_time' field, sequence number, all address types, and SegWit flag for each transaction in the chain dataset. The transaction version, address type, and locktime may be set identically in such chain if the mixer runs auto-programs to generate peeling chains. On the same chain, the sequence numbers should indicate the same meaning. The enabled functions indicated by each sequence number will be identical. To identify a chain from auto-programs, sequence numbers of all transactions are classified into three categories, which may all be the default value, 0xFFFFFFFE, or smaller than 0xFFFFFFFE. Also, chains with different sequence numbers are not deleted directly. New chains are formed by intercepting transactions that satisfy all conditions and meet the chain formation criteria. The transaction format on the same chain should be the same. That is, the SegWit flags on a peeling chain are all true or false. For more precise results, the chain dataset is further processed to select chains consisting of transactions with identical transaction version, address type, locktime, sequence number category, and SegWit flag. After selection, there are 5,598,367 chains that meet the criteria, and the size of the number of chains in the original dataset is reduced by nearly 60%.

4.1.2. Chain statistics

In the processed data, the chains with two or three transaction rounds account for 68.9900% of the total. This kind of chain with a small transaction round can be created by a normal user. For example, it could be two consecutive transactions for payments. And mixers may also make such chains. Chains with small transaction rounds should be further verified. When analyzing the whole blockchain data, it is found that the UTXOs (Unspent Transaction Outputs) of many chains with small transaction rounds will be aggregated in one transaction. That is, UTXOs from the same Bitcoin address are gathered in a consolidation transaction with only one output. And all the input and output addresses in the transaction are identical.

The verification for small chains is based on chain parameters. First, check whether the next transaction for the last transaction on the chain is a consolidation transaction (i.e., transactions having multiple inputs and only one output). According to the distribution of different inputs on the Bitcoin blockchain, the vast majority of transactions have input numbers between one and five, accounting for 95.4848%. Normal users rarely create transactions with more than five inputs. Therefore, if the inputs of the subsequent consolidation transaction are larger than five and all addresses within this transaction are the same, the chain having a small transaction round may be a peeling chain. Next, currently, the Bitcoin blockchain takes approximately 10 min to generate a new block. To attract customers, mixers advertise that the minimum mixing time will be several block times and the maximum time will be one day. The completion time for mixing is an essential consideration for customers when choosing mixers. Mixers usually ensure that customers can withdraw their funds as early as possible. According to the interval statistics, it is found that most short chains have block intervals within ten blocks and time intervals within an hour. Thus, if mixers generate the short chain via auto-programs and the user has not set a particular mixing time (i.e., lock_time $= 0$), the time interval between transactions is considered to be within 1 h, and the block interval should be no larger than ten. There are two reasons why the time or block interval of the short chain is not necessarily set to zero. Firstly, there are negative intervals in the real-world blockchain, and different blocks may have the same timestamp. Secondly, due to the complexity of the Bitcoin blockchain, the situation exists that transactions cannot be confirmed timely because of the large traffic of transactions, network delay, and other reasons.

According to the transaction round distribution of the processed dataset, the round between four to ten also accounts for a significant proportion, which is 26.2869%. For chains with a transaction round between four and ten, relying on the peeling amount may not be a suitable way. If the peeling amount is always the same for each transaction on the chain, it may be a peeling chain generated by the auto-program. It may also be that users have purchased identical products from merchants multiple times. The time period of the chain needs to be checked, and whether the locktime is set to a particular value. Considering traffic congestion and other issues, if locktime is zero, then keep sufficient time to be two block times for each transaction round, i.e., for chains with transaction round value n, the limitation for the maximum block interval is 2*n. This maximum block interval limit also applies to small chains containing two or three transactions. Based on the above analysis, extract the chain data that meets these conditions.

After verifying the transaction's internal details and chain parameters in the previous step, the obtained chain data is most likely peeling chains. It cannot be absolutely certain that the current chain data are all peeling chains from mixers. Even though we used self-change addresses, transaction details, and chain parameters for more exact peeling chains, the inability to know the actual owner of each address is currently a limitation of Bitcoin blockchain research. It is unsolvable now. And because of privacy and other issues, no mixer makes all used address data publicly available. Our method ensures the accuracy of the extracted peeling chains to some extent. The final dataset includes 624,573 chains, with a total transaction volume of 9,813,092.

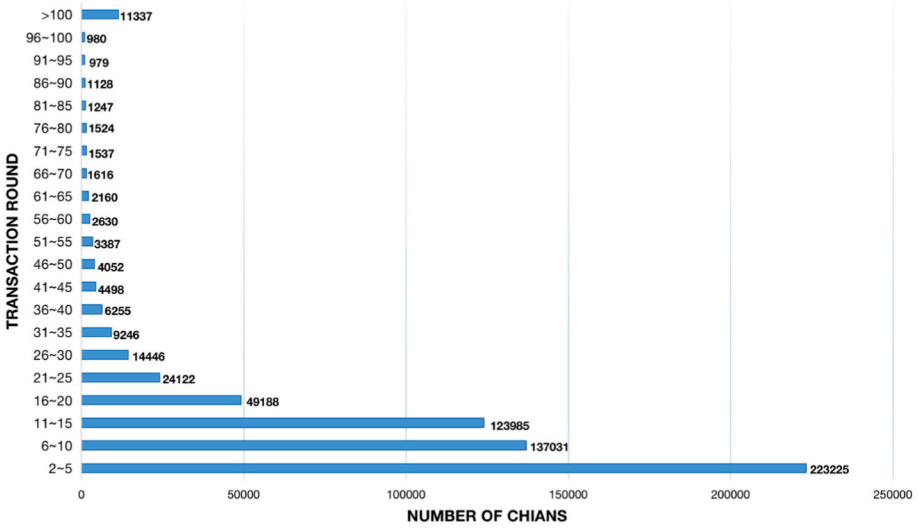

Fig. 6. Distribution of transaction rounds.

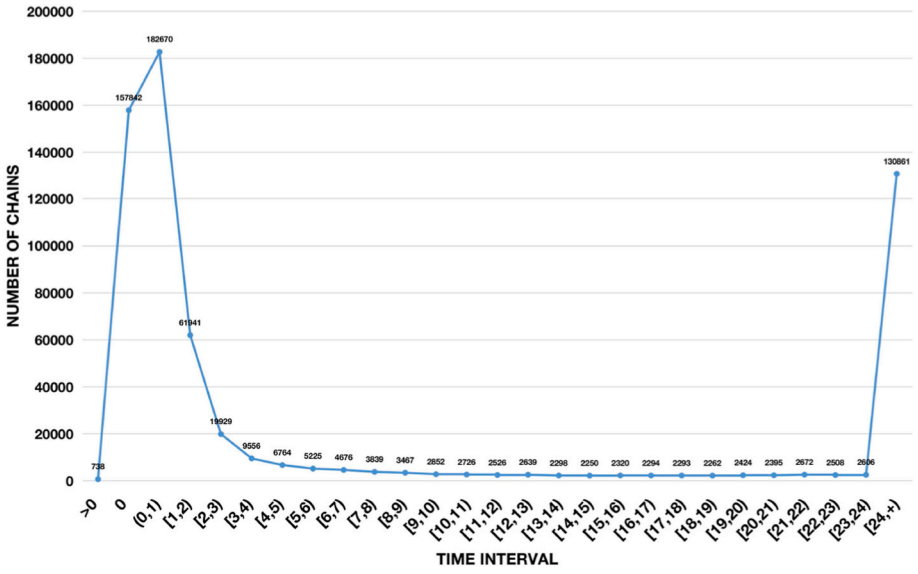

Fig. 7. Distribution of time interval.

4.2. Behavior discussion

Some figures show the details of the final obtained chains. From Fig. 6, the distribution of transaction rounds shows that the numbers of transactions for most chains are within five. As the number of transaction rounds increases, the number of chains decreases. A tiny portion of chains have a length larger than 120. In Fig. 7, about 79.0479% of the chains are created within a day. Chains with a time/block interval of 0 account for about a quarter of the total. And more than half of the chains were created within an hour. 63.5871% of chains have block intervals of no more than ten block heights in Fig. 8. There are chains with a block height interval larger than 200, as some chains have a long transaction round. Fig. 9 shows the most peeling amounts are no more than one Bitcoin. On some chains, the peeling amount is the same each time. And some chains' peeling address is also identical each time in the peeling process. Generally, this type of chain has a small block/time interval. In Fig. 10, the peeling percentage in 58.0550% of the transactions does not exceed 0.05%. And 71.1888% of the transactions peeled off the Bitcoin amount which is less than 1% of the input amount. Only 4.7771% of the transactions had a peeling percentage greater than 50%. And the peeling value for most transactions is less than half of the input amount. For transactions with a large peeling percentage, the explanation is provided in the subsequent part. From the distributions of these chain parameters, it can be seen that the distributions of time intervals and block intervals in this chain dataset indicate that most chains were created within a short period of time.

While calculating the time intervals, it is found that some chains have negative time intervals. There are 738 such chains in the dataset. The reason why negative time intervals exist is that there is a situation that the timestamp of the current block is earlier than the time of the previous block. For example, the UTC Time for block 362940 is 2015-06-28 17:18:34 while the UTC Time of block 362941 is 2015-06-28 17:16:02. The block time of block 362940 is later than that of block 362941. The proportion of negative time intervals on the whole blockchain is pretty small, but this situation exists (Marcel Waldvogel, 2022). Note that a block interval of zero does not necessarily mean that all transactions on the chain are in the same block. And a chain with zero time interval does not automatically imply the block height interval is also zero. That is, if the time interval of a chain is zero, the block height interval may not be zero. There are blocks with identical timestamps in

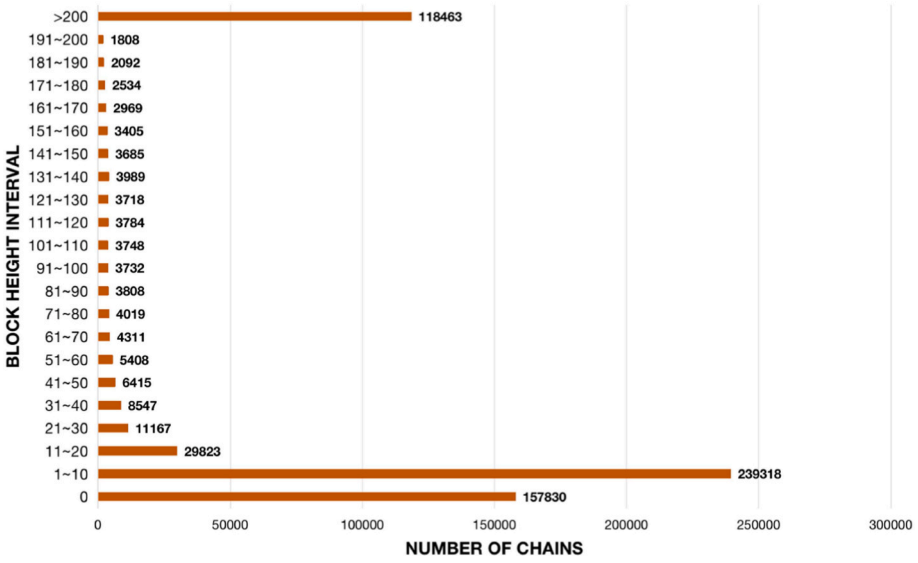

Fig. 8. Distribution of block interval.

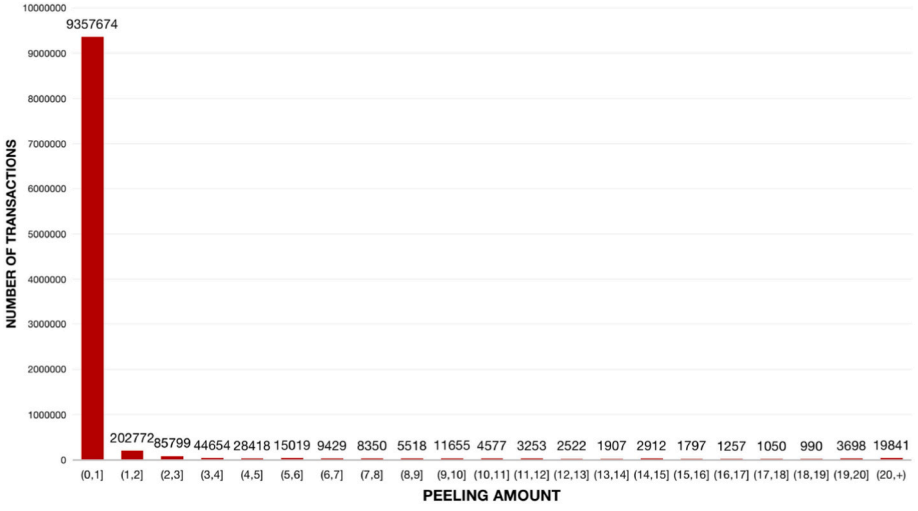

Fig. 9. Distribution of peeling amount.

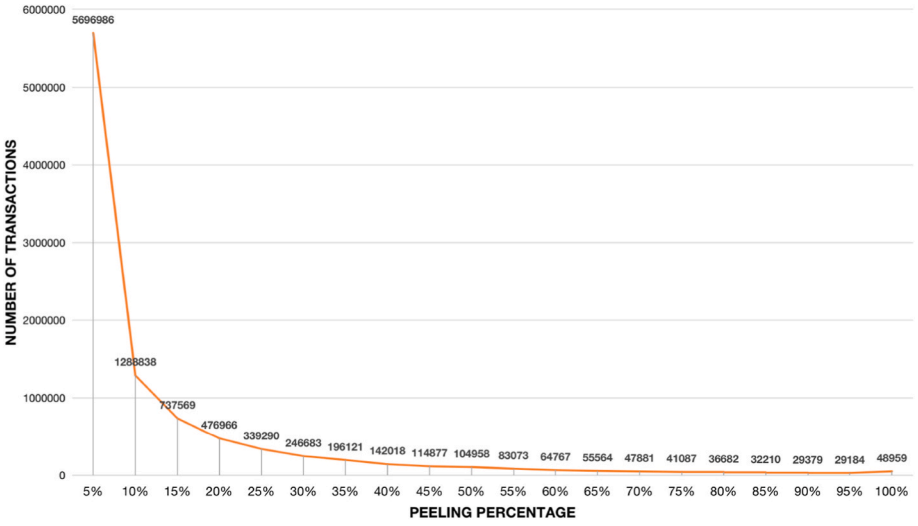

Fig. 10. Distribution of peeling percentage.

the blockchain. For example, block 655042 and block 655043 have the same timestamp.

These chain parameter data should be studied in combination when determining and analyzing peeling chains. Relying on a single chain parameter cannot accurately identify peeling chains and their behaviors. If the value of the transaction round is large, and the time/block interval is relatively small, there is a high probability that the chain is a peeling chain generated via auto-program script. Similarly, for chains having large time/block intervals, transaction rounds should be considered for the determination. For example, a chain with over 4,000 transactions, although the time interval is greater than one day, could be a peeling chain if it continuously peels off Bitcoin. The peeling percentage should not be required to be a smaller value every time, e.g., less than half of the input value. It is because when parsing the chain, it is found that the peeling amount of one transaction on the chain may exceed 50%, but the peeling amounts before and after that transaction satisfy the condition of peeling a smaller value. For example, in a chain, the transaction round is 22, and the peeling percentage of the twelfth transaction is 59.0999%, greater than 50%. However, each peeling percentage is smaller than 50% for other transactions on the chain (most of them are less than 10%). In this case, assessing whether the corresponding time and block intervals are reasonable values is essential. Suppose the block interval of the chain is 0, and the timestamps of all transactions are the same; the chain is likely to be a peeling chain.

In addition, the peeling amount and the peeling percentage should be evaluated together. Directly limiting the peeling amount/percentage to be within a particular value for each transaction on the chain is not a good way. In the experiments, it is found that the starting address of some chains has a large Bitcoin amount, and the peeling percentage is very low for the first peeling processes. As the peeling process continues, the input value of transactions in the later parts of the chain becomes smaller, increasing the peeling percentage. For example, the Bitcoin amount in the starting address in a particular chain is over 50 BTC, and 1.15 BTC is peeled off with a peeling percentage of less than 3% for the first time. And the transaction round of this chain is long. After a series of peeling, the input amount is less than 0.067 in one transaction, and the peeling amount is 0.05 BTC. The peeling percentage is greater than 75% this time. However, the chain is still undergoing the peeling process. The peeling amount becomes small each time, and the peeling percentage slightly increases. In this case, further checking the corresponding transaction round is necessary. The increase in the peeling percentage could be reasonable for chains with very long transaction rounds. Note that the above analysis of chain parameters is based on the pre-verified results that the transaction details on the chain are identical.

Our objective is to identify peeling chains generated by mixers and derive their behavior patterns. In general, mixers make use of auto-program scripts to process a large number of transactions. It can be learned from the extracted chain dataset that the trend of chain parameters is relatively obvious. The period of this type of chain is very short, usually no more than one day or even 1 h. And the Bitcoin peeling value is not large. However, the peeling amount may not always be a smaller value (below 50%). It should be linked with the corresponding peeling percentage. The sequence number of the vast majority of transactions is the default value, and the lock time is zero. Bitcoin is peeled off to a peeling address each time in the peeling process. Chains with totally identical peeling addresses account for 16.4970%. Overall, the resulting statistics are consistent with the expected characterization of a peeling chain. That is, the peeling chain can continuously peel off small amounts to other addresses within a short period to distribute and transfer funds.

5. Conclusion

The present research on peeling chains is usually based on heuristic algorithms to identify change addresses. Due to the features and limitations of the Bitcoin blockchain, there is no such ground truth data to mark the actual owner for each Bitcoin address. The accuracy of derived change addresses cannot be guaranteed. The subsequent behavior analysis of peeling chains may have bias. Our research studies the peeling chain patterns based on self-change addresses. The use of self-change addresses suggests that the input and the address used for receiving the change are controlled by the same entity. Also, the transaction details and chain parameters are further examined. Combining the two steps ensures the accuracy of the extracted peeling chains to some extent. However, relying on self-change addresses limits the number of extracted chains from the real-world Bitcoin blockchain. The peeling chains with one-time change addresses cannot be discovered. The incapacity to accurately identify every one-time change address is also a limitation of current Bitcoin de-anonymization and mixing detection work.

Future work will focus on whether peeling chains can be simulated with a Bitcoin simulation model. As the data generated by the simulator can associate the real owner with every address in the simulated network, it is possible to study peeling chains with one-time change addresses and verify the effectiveness of current techniques.

References

Ahmed, M., Shumailov, I., Anderson, R., 2019. Tendrils of crime: visualizing the diffusion of stolen bitcoins. In: Graphical Models for Security: 5th International Workshop, GraMSec 2018. Springer, Oxford, UK, pp. 1–12. July 8, 2018, Revised Selected Papers 5.

Antonopoulos, A.M., 2014. Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media, Inc.".

de Balthasar, T., Hernandez-Castro, J., 2017. An analysis of bitcoin laundry services. In: Secure IT Systems: 22nd Nordic Conference, NordSec 2017, Tartu, Estonia, November 8–10, 2017, Proceedings 22. Springer, pp. 297–312.

Bistarelli, S., Mercanti, I., Santini, F., 2019. An analysis of non-standard transactions. Front. Blockchain 2, 7.

Opt-in RBF FAQ. Available at: https://bitcoincore.org/en/faq/optin_rbf/. (Accessed 6 January 2023).

Blender.io. Available at: https://blendor.io/. (Accessed 3 March 2023).

Segregated Witness Wallet Development Guide. Available at: https://bitcoincore.org/en/segwit_wallet_dev/. (Accessed 6 January 2023).

Bitcoin Developer Guide. Available at: https://btcinformation.org/en/developer-guide#transaction-malleability. (Accessed 6 January 2023).

BlockSci Developers, 2020. Blocksci version 0.7 documentation. Available at: https://citp.github.io/BlockSci/index.html. (Accessed 21 March 2023).

BRC-20 Tokens. Available at: https://www.brc-20.io/. (Accessed 1 May 2023).

Chainalysis Team, 2023. The 2023 crypto crime report:everything you need to know about cryptocurrency-based crime. Available at: https://go.chainalysis.com/2023-crypto-crime-report.html. (Accessed 22 April 2023).

Chen, Q., Bridges, R.A., 2017. Automated behavioral analysis of malware: a case study of wannacry ransomware. In: 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA). IEEE, pp. 454–460.

Chen, X., Hasan, M.A., Wu, X., Skums, P., Feizollahi, M.J., Ouellet, M., Sevigny, E.L., Maimon, D., Wu, Y., 2019. Characteristics of bitcoin transactions on cryptomarkets. In: Security, Privacy, and Anonymity in Computation, Communication, and Storage: 12th International Conference, SpaCCS 2019. Proceedings 12, Springer, Atlanta, GA, USA, pp. 261–276. July 14–17, 2019.

Conti, M., Kumar, E.S., Lal, C., Ruj, S., 2018. A survey on security and privacy issues of bitcoin. IEEE commun. Surv. Tutorials. 20, 3416–3452.

Greg Maxwell, 2013. Coinjoin: bitcoin privacy for the real world. Available at: https://bitcointalk.org/index.php?topic=279249.0. (Accessed 6 March 2023).

Harrigan, M., 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). IEEE, pp. 368–373.

Hu, Y., Seneviratne, S., Thilakarathna, K., Fukuda, K., Seneviratne, A., 2019. Characterizing and Detecting Money Laundering Activities on the Bitcoin Network arXiv preprint arXiv:1912.12060.

Jourdan, M., Blandin, S., Wynter, L., Deshpande, P., 2018. Characterizing entities in the bitcoin blockchain. In: 2018 IEEE International Conference on Data Mining Workshops (ICDMW). IEEE, pp. 55–62.

Kalodner, H., Möser, M., Lee, K., Goldfeder, S., Plattner, M., Chator, A., Narayanan, A., 2020. {BlockSci}: design and applications of a blockchain analysis platform. In: 29th USENIX Security Symposium (USENIX Security 20), pp. 2721–2738.

Kappos, G., Yousaf, H., Stütz, R., Rollet, S., Haslhofer, B., Meiklejohn, S., 2022. How to peel a million: validating and expanding bitcoin clusters. In: 31st USENIX Security Symposium. USENIX Security 22, pp. 2207–2223.

Katie Rees, 2023. What are bitcoin's new brc-20 tokens and what do they do? Available at: https://www.makeuseof.com/what-are-bitcoin-brc-20-tokens/. (Accessed 1 May 2023).

Koshy, P., Koshy, D., McDaniel, P., 2014. An analysis of anonymity in bitcoin using p2p network traffic. In: Financial Cryptography and Data Security: 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers 18. Springer, pp. 469–485.

Makarov, I., Schoar, A., 2021. Blockchain Analysis of the Bitcoin Market. Technical Report. National Bureau of Economic Research.

Marcel, Waldvogel, 2022. Bitcoin block timing statistics. Available at: https://netfuture.ch/2022/03/bitcoin-block-timing-statistics/. (Accessed 1 April 2023).

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M., Savage, S., 2013. A fistful of bitcoins: characterizing payments among men with no names. In: Proceedings of the 2013 Conference on Internet Measurement Conference, pp. 127–140.

Möser, M., Böhme, R., Breuker, D., 2013. An inquiry into money laundering tools in the bitcoin ecosystem. In: 2013 APWG eCrime Researchers Summit. Ieee, pp. 1–14.

Nan, L., Tao, D., 2018. Bitcoin mixing detection using deep autoencoder. In: 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC). IEEE, pp. 280–287.

Null Data. Available at: https://developer.bitcoin.org/devguide/transactions.html#null-data. (Accessed 12 January 2023).

Null Data (OP_RETURN) Transaction. Available at: https://btcinformation.org/en/glossary/null-data-transaction. (Accessed 12 January 2023).

Pakki, J., Shoshitaishvili, Y., Wang, R., Bao, T., Doupé, A., 2021. Everything you ever wanted to know about bitcoin mixers (but were afraid to ask). In: Financial Cryptography and Data Security: 25th International Conference, FC 2021, Virtual Event, March 1–5, 2021, Revised Selected Papers, Part I 25. Springer, pp. 117–146.

Phetsouvanh, S., Datta, A., Oggier, F., 2021. Analysis of multi-input multi-output transactions in the bitcoin network. Concurrency Comput. Pract. Ex. 33, e5629.

Prado-Romero, M.A., Doerr, C., Gago-Alonso, A., 2018. Discovering bitcoin mixing using anomaly detection. In: Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications: 22nd Iberoamerican Congress, CIARP 2017. Springer, pp. 534–541. Valparaíso, Chile, November 7–10, 2017, Proceedings 22.

Ruffing, T., Moreno-Sanchez, P., Kate, A., 2014. Coinshuffle: practical decentralized coin mixing for bitcoin. In: Computer Security-ESORICS 2014: 19th European Symposium on Research in Computer Security, Wroclaw, Poland, September 7-11, 2014. Proceedings, Part II 19. Springer, pp. 345–364.

Sequence Number (Transactions). Available at: https://btcinformation.org/en/glossary/sequence-number. (Accessed 13 January 2023).

Shojaeenasab, A., Motamed, A.P., Bahrak, B., 2022. Mixing Detection on Bitcoin Transactions Using Statistical Patterns arXiv preprint arXiv:2204.02019.

Statement of Facts. Available at: https://www.justice.gov/opa/press-release/file/1470186. (Accessed 18 April 2023).

Sun, X., Yang, T., Hu, B., 2022. Lstm-tc: bitcoin coin mixing detection method with a high recall. Appl. Intell. 52, 780–793.

Transactions. Available at: https://developer.bitcoin.org/reference/transactions.html. (Accessed 13 January 2023).

WalletExplorer.com. Available at: https://www.walletexplorer.com/. (Accessed 10 May 2023).

Wasabi Wallet. Available at: https://wasabiwallet.io/. (Accessed 10 March 2023).

Wu, J., Liu, J., Chen, W., Huang, H., Zheng, Z., Zhang, Y., 2021a. Detecting mixing services via mining bitcoin transaction network with hybrid motifs. IEEE Transact. Syst. Man Cybernet.: Systems 52, 2237–2249.

Wu, L., Hu, Y., Zhou, Y., Wang, H., Luo, X., Wang, Z., Zhang, F., Ren, K., 2021b. Towards understanding and demystifying bitcoin mixing services. In: Proceedings of the Web Conference 2021, pp. 33–44.

Xiang, Y., Lei, Y., Bao, D., Ren, W., Li, T., Yang, Q., Liu, W., Zhu, T., Choo, K.K.R., 2022. Babd: A Bitcoin Address Behavior Dataset for Pattern Analysis arXiv preprint arXiv:2204.05746.

Zhang, Y., Wang, J., Luo, J., 2020. Heuristic-based address clustering in bitcoin. IEEE Access 8, 210582–210591.

Zola, F., Bruse, J.L., Eguimendia, M., Galar, M., Orduna Urrutia, R., 2019. Bitcoin and cybersecurity: temporal dissection of blockchain data to unveil changes in entity behavioral patterns. Appl. Sci. 9, 5003.