2019

Characteristics of Bitcoin Transactions on Cryptomarkets

Xucan Chen

Mohammad Al Hasan

Paval Skums

Xintao Wu

Mohammad Javad Feizollahi

See next page for additional authors

Authors

Xucan Chen, Mohammad Al Hasan, Paval Skums, Xintao Wu, Mohammad Javad Feizollahi, Marie Ouellet, Eric L. Sevigny, David Maimon, and Yubao Wu

Characteristics of Bitcoin Transactions on Cryptomarkets

Xucan Chen[1,6], Mohammad Al Hasan[2,6], Xintao Wu[3,6], Pavel Skums[1,6], Mohammad Javad Feizollahi[4,6], Marie Ouellet[5,6], Eric L. Sevigny[5,6], David Maimon[5,6], and Yubao Wu[1,6]

[1] Department of Computer Science, Georgia State University, Atlanta, GA, USA
[2] Department of Computer and Information Science, Indiana University - Purdue University Indianapolis, Indianapolis, IN, USA
[3] Department of Computer Science and Computer Engineering, University of Arkansas, Fayetteville, AR, USA
[4] Institute for Insight, Georgia State University, Atlanta, GA, USA
[5] Department of Criminal Justice and Criminology, Georgia State University, Atlanta, GA, USA
[6] email: xchen41@student.gsu.edu, alhasan@iupui.edu, xintaowu@uark.edu, pskums@gsu.edu, mfeizollahi@gsu.edu, mouellet@gsu.edu, esevigny@gsu.edu, dmaimon@gsu.edu, ywu28@gsu.edu

Abstract. Cryptomarkets (or darknet markets) are commercial hidden-service websites that operate on The Onion Router (Tor) anonymity network. Cryptomarkets accept primarily bitcoin as payment since bitcoin is pseudonymous. Understanding bitcoin transaction patterns in cryptomarkets is important for analyzing vulnerabilities of privacy protection models in cryptocurrecies. It is also important for law enforcement to track illicit online crime activities in cryptomarkets. In this paper, we discover interesting characteristics of bitcoin transaction patterns in cryptomarkets. The results demonstrate that the privacy protection mechanism in cryptomarkets and bitcoin is vulnerable. Adversaries can easily gain valuable information for analyzing trading activities in cryptomarkets.

Keywords: Cryptomarket · Cryptocurrency · Bitcoin · Peeling Chain

1 Introduction

The darknet is a portion of the Internet that purposefully protects the identities and privacy of both web servers and clients. The Onion Router (Tor) is the most popular instance of a darknet and also the most popular anonymous network. Tor provides hidden services (also known as onion services) for users to hide their locations and identities while offering web publishing services. A cryptomarket (or darknet market) is a commercial website operating on the darknet. Specifically, in Tor, a crytomarket is a hidden service website with a ".onion" link address. Most products being sold in cryptomarkets are illicit. Some example popular products in cryptomarkets are drugs, malware, and stolen credit cards. After the demise of the first cryptomarket called Silk Road on 2013, new cryptomarkets have proliferated. As of March 2019, we have observed at least 35 active cryptomarkets. Table 1 shows the largest six cryptomarkets at present according to the total number of ads listed in each market.

Table 1: Cryptomarkets and their accepted cryptocurrencies as of March 2019

Cryptomarkets	#Ads	Bitcoin	Monero	Litecoin	Ethereum	Bitcoin Cash
Dream	166,216	✓				✓
Berlusconi	38,462	✓				
Wall Street	16,847	✓	✓			
Empire	9,538	✓	✓	✓		
Point Tochka	6,468	✓			✓	✓
Silk Road 3.1	5,738	✓	✓	✓	✓	

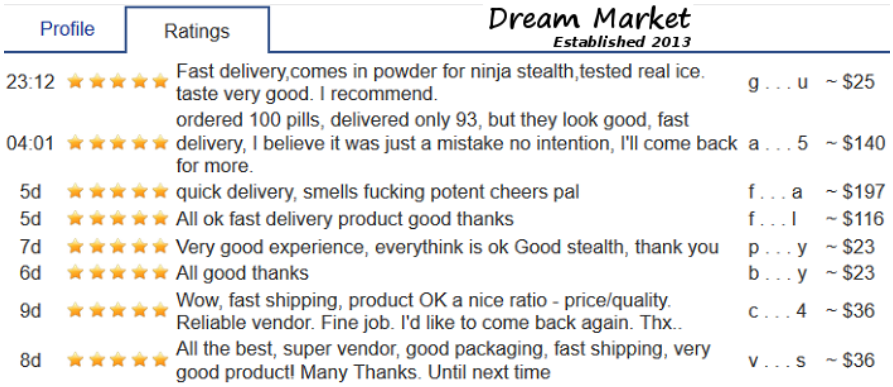
From Table 1, we can see that bitcoin is accepted in all cryptomarkets. In addition to bitcoin, four other types of cryptocurrencies are also accepted by different markets. They are monero, litecoin, ethereum, and bitcoin cash. Note that bitcoin cash is a variant of but different than bitcoin and is an independent currency. Bitcoin cash is generally considered to be faster in the transaction confirmation process but less secure than bitcoin. In our study, we focus on bitcoin since it is the most popular cryptocurrency and widely accepted by all markets. The observed bitcoin transaction patterns in this paper provide insights for analyzing other types of cryptocurrencies.

Bitcoin is the first decentralized cryptocurrency (also known as digital currency or electronic cash). Bitcoin operates on the peer-to-peer network without the need for intermediaries and there are no central banks or administrators. Transactions are verified by network nodes via cryptography and recorded in a public distributed ledger called a blockchain. Bitcoin has millions of unique users. Bitcoin is pseudonymous because funds are not tied to real-world entities but rather bitcoin addresses. Owners of bitcoin addresses are not explicitly identified, but all transactions on the blockchain are public.

Since all bitcoin transactions are public, it is hard to fully protect the privacy of bitcoin users. The news have revealed that adversaries could spy on a careless company by first paying it in bitcoins and then tracking how that money flows [4, 6, 3]. For better protecting the privacy, bitcoin users have extensively used mixing services to obscure the bitcoin trails [4].

In cryptomarkets, adversaries could place orders and then track money flows. Cryptomarkets display the buyers' feedback in order to demonstrate the vendors' reputation. Figure 1 shows the screenshot of the feedback page in the Dream Market. From Figure 1, we can see the post time, rating star, text comment, masked buyer ID, and approximate amount of money. Each rating actually represents a bitcoin transaction. Even we can only observe approximate time and money in ratings, the accumulation of a lot of of such approximate transaction records could potentially allow adversaries to reveal relevant bitcoin addresses. Figure 2 shows the screenshot of the feedback page in the Wall Street Market. From Figure 2, we can observe similar ratings. All markets in Table 1 display feedback publicly. This potentially allows adversaries to re-identify the bitcoin addresses of buyers, vendors, and escrow accounts in cryptomarkets, thus increases the vulnerability of the privacy protection in bitcoin.

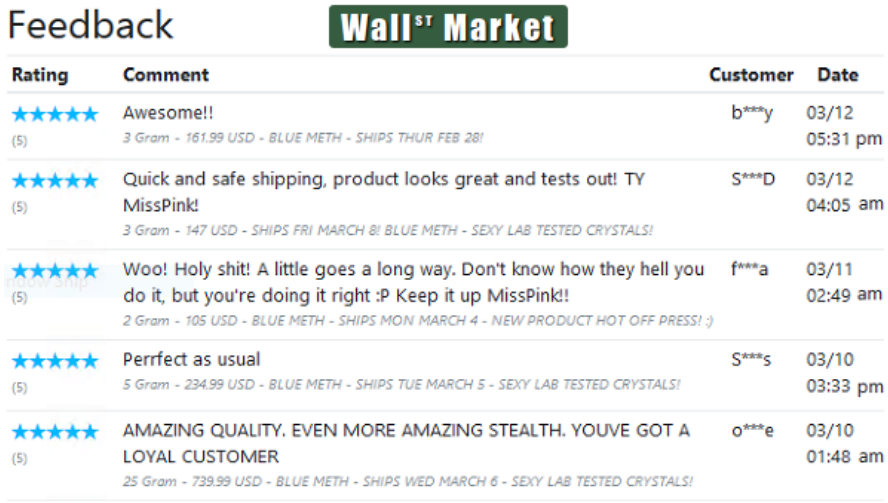
In this paper, we systematically study the vulnerabilities of bitcoin privacy that exist in cryptomarkets. We identify and categorize patterns of bitcoin transactions in cryptomarkets. The observations are then used for discussing the possibility of re-identifying bitcoin addresses related to crytomarkets. The conclusions obtained from this paper can help design better bitcoin payment systems and strengthen the privacy protection. On



Profile | Ratings | Dream Market Established 2013

23:12	Fast delivery,comes in powder for ninja stealth,tested real ice. taste very good. I recommend.	g . . . u	~ $25
04:01	ordered 100 pills, delivered only 93, but they look good, fast delivery, I believe it was just a mistake no intention, I'll come back for more.	a . . . 5	~ $140
5d	quick delivery, smells fucking potent cheers pal	f . . . a	~ $197
5d	All ok fast delivery product good thanks	f . . . l	~ $116
7d	Very good experience, everythink is ok Good stealth, thank you	p . . . y	~ $23
6d	All good thanks	b . . . y	~ $23
9d	Wow, fast shipping, product OK a nice ratio - price/quality. Reliable vendor. Fine job. I'd like to come back again. Thx..	c . . . 4	~ $36
8d	All the best, super vendor, good packaging, fast shipping, very good product! Many Thanks. Until next time	v . . . s	~ $36

Fig. 1: The feedback in the Dream Market



Feedback — Wall ST Market

Rating	Comment	Customer	Date
★★★★★ (5)	Awesome!! *3 Gram - 161.99 USD - BLUE METH - SHIPS THUR FEB 28!*	b***y	03/12 05:31 pm
★★★★★ (5)	Quick and safe shipping, product looks great and tests out! TY MissPink! *3 Gram - 147 USD - SHIPS FRI MARCH 8! BLUE METH - SEXY LAB TESTED CRYSTALS!*	S***D	03/12 04:05 am
★★★★★ (5)	Woo! Holy shit! A little goes a long way. Don't know how they hell you do it, but you're doing it right :P Keep it up MissPink!! *2 Gram - 105 USD - BLUE METH - SHIPS MON MARCH 4 - NEW PRODUCT HOT OFF PRESS! ;)*	f***a	03/11 02:49 am
★★★★★ (5)	Perrfect as usual *5 Gram - 234.99 USD - BLUE METH - SHIPS TUE MARCH 5 - SEXY LAB TESTED CRYSTALS!*	S***s	03/10 03:33 pm
★★★★★ (5)	AMAZING QUALITY. EVEN MORE AMAZING STEALTH. YOUVE GOT A LOYAL CUSTOMER *25 Gram - 739.99 USD - BLUE METH - SHIPS WED MARCH 6 - SEXY LAB TESTED CRYSTALS!*	o***e	03/10 01:48 am

Fig. 2: The feedback in the Wall Street Market

the other hand, the conclusions can also be used by law enforcement to understand the activities in cryptomarkets.

2 Escrow Services in Cryptomarkets

In this section, we review the escrow services in cryptomarkets. All cryptomarkets provide escrow services to avoid scams and protect both buyers and vendors.
Figure 3 shows the typical process of one transaction [12]. The buyer places an order and pays with bitcoins after browsing the products within the Tor web browser. The market holds the bitcoins until the buyer confirms the order. The vendor accepts and fulfills the order. The buyer confirms the order and gives feedback reviews. The market releases the bitcoins to the vendor and charges a commission fee. If the buyer is not satisfied with the product or service, the buyer disputes the order. In this case, the market

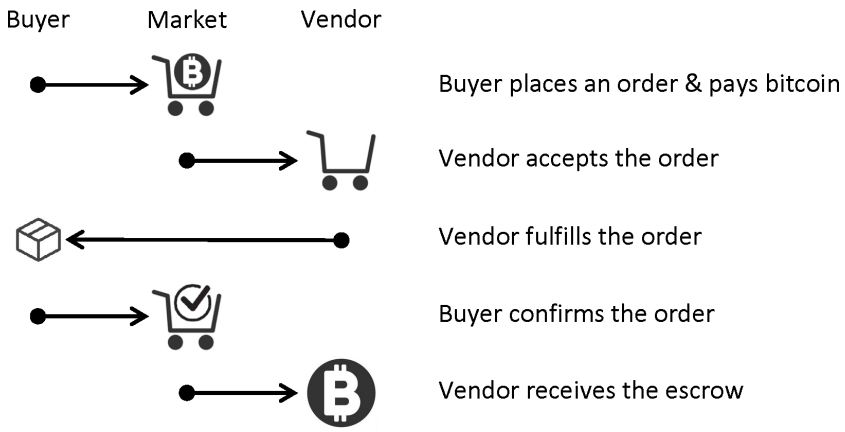


Fig. 3: A flowchart depicting a transaction in cryptomarkets

decides where the escrow bitcoins go. The escrow bitcoins go either back to the buyer or to the vendor depending on the dispute result.

3 Parsing and Understanding Bitcoin Transactions

To trace the bitcoin flow, we parse the blocks in the public bitcoin blockchain and obtain the bitcoin transactions. We install the bitcoin core program [2] and run a bitcoin full node [7]. The bitcoin full node automatically synchronizes with other nodes in the bitcoin network, and downloads all blocks in the blockchain. The blocks contain the public ledger data and are the inputs of our parsing algorithm. A new block is generated around every 10 minutes.

Algorithm 1 shows our parsing algorithm. We use the existing Python bitcoin parser to parse the blocks (raw Bitcoin data) and construct the bitcoin transaction tree [5, 1]. In Algorithm 1, we parse the blocks one by one (lines 1-12) and save one timestamp for all transactions in one block (line 2). For each transaction in one block, we parse the transaction hash (line 5), the receiver list (lines 6-8), and the sender list (lines 9-11). Each transaction contains four parts: timestamp, hash, sender_list, and receiver_list, and is written into a json file (line 12). One receiver contains the bitcoin address and the bitcoin values. Each sender in one transaction does not contain bitcoin address neither bitcoin value. Instead, each sender contains transaction hash and index pointing to an earlier transaction. We can use that transaction hash to retrieve the earlier transaction and use the transaction index to find the referred receiver from the receiver list. By linking the sender in current transaction with the receiver in the earlier transaction, we can generate a bitcoin transaction flow tree.

Algorithm 2 shows the construction of bitcoin transaction flow tree. Algorithm 2 processes the json files in the chronological order. This guarantees that old transactions will be processed earlier than new transactions. Since a receiver has bitcoin address, we can directly add a node (transaction_hash, bitcoin_address) to the flow tree. Since a sender does not have bitcoin address, we need to look it up in an earlier transaction. Since earlier transactions have been processed, the sender must exist in the node set V

Algorithm 1 Parsing Bitcoin Transactions

Input: Blocks in the bitcoin blockchain
Output: Bitcoin transactions (a set of .json files whose names are formatted timestamps)

```
1:  for each block do
2:      transaction_time ⇐ block.timestamp;
3:      create a new file: formatted_transaction_timestamp.json;
4:      for each transaction in the block.transactions do
5:          transaction_hash ⇐ transaction.this_transaction_hash;
6:          receiver_list = [] ;
7:          for each receiver in the transaction.receivers do
8:              receiver_list.add(receiver.index, receiver.bitcoin_address, receiver.bitcoin_value)
9:          sender_list = [] ;
10:         for each sender in the transaction.senders do
11:             sender_list.add(sender.index, sender.previous_transaction_hash,
                  sender.previous_transaction_index)
12:         [transaction_time, transaction_hash, sender_list, receiver_list] ⇒
              formatted_transaction_timestamp.json
```

Algorithm 2 Constructing Bitcoin Transaction Flow Tree

Input: Bitcoin transactions (a set of .json files whose names are formatted timestamps)
Output: Bitcoin transaction flow tree $G(V, E)$

```
1:  read the list of json files;
2:  for each json file (process them in the chronological order) do
3:      read all transactions in the json file;
4:      for each transaction tx do
5:          for each receiver in tx.receiver_list do
6:              add node r = [tx.transaction_hash, receiver.index, receiver.bitcoin_address,
                  receiver.bitcoin_value] to the node set V;
7:              for each sender in tx.sender_list do
8:                  find node s ∈ V with s.transaction_hash = sender.previous_transaction_hash
                      and s.index = sender.index;
9:                  add an edge (s, r) to the edge set E;
```

as a receiver. Therefore, we search over all the nodes in V and compare the transaction_hash and index values (lines 8). Then we add an edge from this earlier receiver to the current receiver in flow tree. If there are multiple senders and receivers in a mixing transaction, these senders and receivers will form a complete bipartite graph, i.e., there is an edge from any sender to any receiver. We do not know who sends money to whom in a mixing transaction.

Algorithm 3 shows a local search algorithm that retrieves a subtree containing all nodes that are k-hop away from the query node. The query node is determined by the transaction hash and bitcoin address. In our experiment, we use Algorithm 3 to extract a

Algorithm 3 Local search algorithm for extracting a subtree

Input: Bitcoin transaction flow tree $G(V, E)$, query $q = (q\_hash, q\_btc\_address)$, k hops
Output: Subtree $G[T]$

```
ignore the edge direction, G.Adj[u] represents the neighbors;
for each node v ∈ V do v.d = ∞ ;
S ⇐ {q}; T ⇐ {}; q.d = 0;
while True do
    extract node u with minimum u.d value among all nodes in the set S − T;
    if u.d > k then break;
    T ⇐ T ∪ u; S ⇐ S ∪ G.Adj[u];
    for each node x in G.Adj[u] do x.d = min{x.d, u.d + 1} ;
```

subtree given an query node containing our bitcoin address. The subtree is nimble for us to analyze interesting patterns.

Shadow Address: Bitcoin creates a new address for the sender in each transaction to obtain better anonymity [15]. The newly generated address is called "shadow address" or "change address" of the original address of the sender [8]. Figure 4 shows one bitcoin transaction. The sender's original address has ฿.09. After ฿.05 is sent to the receiver, the sender still has ฿.04 in the change address.

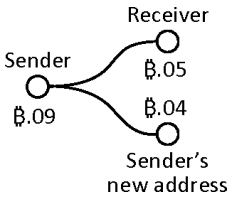


Fig. 4: shadow address

Multiple inputs and single output: Considering the multiple addresses one user can own, bitcoin supports a user to send bitcoins from multiple addresses in one transaction. Figure 5 shows one bitcoin transaction containing multiple inputs and one output. The sender sends money from four bitcoin addresses to the receiver's address. We assume that it is unlikely that two senders send money to the same address at the same time since the bitcoin addresses keep changing. If we observe a transaction with multiple inputs and single output, we can assume all input addresses belong to the same sender.

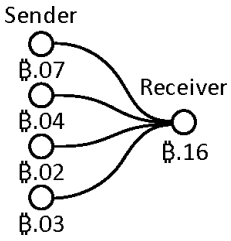


Fig. 5: multi-inputs

These two properties help track bitcoin flows or cluster addresses into wallets [14, 8, 10].

Mixing services: are widely used as a privacy overlay on top of bitcoin [11]. Mixing services are also known as tumblers. The mixer will mix several transactions into one, intending to confuse the trail linking back to the source. In a mixing transaction, the multiple inputs are from different senders and the multiple outputs go to different receivers. Mixing services reduce the traceability of bitcoin flows which makes the analysis of bitcoin graph more difficult. Figure 6 shows a mixing transaction with four senders and three

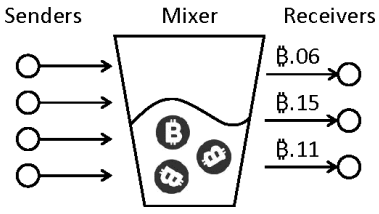


Fig. 6: A mixing transaction

receivers. In this example, we do not know who send money to whom because there are multiple possible flows.

4 Actions and Observed Resulting Transactions

In this section, we describe our experiments in cryptomarkets. All cryptomarkets offer escrow services to avoid scams. With the escrow service, the bitcoin is saved in escrow accounts after a buyer places an order and is sent to the vendor until the buyer confirms the order. Since we know the start point (buyer address) of the transaction, we can trace bitcoin flows to uncover escrow and vendors' addresses.

Table 2: Observed bitcoin flow from operation in different cryptomarkets

Cryptomarkets	Deposit	Withdraw	Order	Confirm
Point Tochka	✓	✓	✓	✓
Dream	✓	✓	No observation	No observation
Empire	✓	✓	No observation	No observation
Silk Road 3.1	✓	✓	No observation	No observation
Wall Street	No such function	No such function	✓	✓
Berlusconi	No such function	No such function	✓	No observation

In each market, four operations are performed: deposit, withdraw, order, and confirmation. The resulting transactions may or may not be observed in the bitcoin transaction flow. Table 2 shows whether we can observe the bitcoin transactions for the four operations in cryptomarkets. From Table 2, we can see that the Dream, Empire, and SilkRoad 3.1 Market operate in a similar way. These markets require buyers to deposit bitcoins first. When buyers withdraw bitcoins from the market, the market will send bitcoins to buyers' wallets from an address different than the deposit address. When we order or confirm a purchase, we cannot observe any transactions in bitcoin flow. The Point Tochka Market also requires deposit. When we order and confirm a purchase in the Point Tochka Market, we can observe the transactions from buyer to escrow and then to vendor in the bitcoin flow. The Wall Street and Berlusconi Markets do not require deposit. In the Wall street Market, when we order and confirm a purchase, we can also observe the corresponding transactions in the bitcoin flow. In the Berlusconi Market, we can observe the transactions in bitcoin flow when we order. The bitcoins sent to escrow are transferred to other escrow addresses through mixing service before we confirm the purchase. Therefore, we cannot observe the transaction when we conform the purchase.

Table 3: Deposit and Withdrawal in the Point Tochka Market

Action	Observed bitcoin transaction		Balance
	Sender	Receiver	
Deposit ฿.0024	A1: ฿.0030	⟶ B1: ฿.0024, A2: ฿.0006	฿.0024
Withdraw ฿.0008	B1: ฿.0024	⟶ A2: ฿.0008, B1: ฿.0016	฿.0016
Deposit ฿.0010	A2: ฿.0006, A2: ฿.0008	⟶ B1: ฿.0026, A3: ฿.0004	฿.0026
Withdraw ฿.0006	B1: ฿.0026	⟶ A3: ฿.0006, B1: ฿.0020	฿.0020

In the next, we will study the bitcoin transaction patterns when we interact with the markets. We first study the deposit and withdrawal actions and then the order and confirmation actions. In each market, four operations are performed: deposit Ƀ.0024, withdraw Ƀ.0008, deposit Ƀ.0010, and withdraw Ƀ.0006. We monitor the bitcoin transaction flow to see whether we can observe any related transactions or not. To simplify the illustration, we omit the fees charged during the deposit and withdrawal actions.

Deposit and Withdrawal in the Point Tochka Market: Table 3 shows the actions we perform and the resulting bitcoin transactions in the Point Tochka Market. In Table 3, each row represents an action we perform and the resulting Bitcoin transaction. We use letter "A" followed by an integer to represent our bitcoin addresses and letter "B" followed by an integer to represent the deposit bitcoin addresses provided by the market. For example, in the first row, we deposit Ƀ.0024 and the resulting transaction is "A1: Ƀ.0030 $\rightarrow$ B1: Ƀ.0024, A2: Ƀ.0006". In the sender part "A1: Ƀ.0030", A1 represents our bitcoin address and Ƀ.0030 represents the money in that address. In the receiver part "B1: Ƀ.0024, A2: Ƀ.0006", B1 represents the deposit bitcoin address provided by the Point Tochka Market, Ƀ.0024 represents the money that B1 receives, A2 represents our new bitcoin address, and Ƀ.0006 represents the change in the new address A2. The last column in Table 3 shows the balance in the market wallet.

In the second row of Table 3, we withdraw Ƀ.0008 and the resulting transaction is "B1: Ƀ.0024 $\rightarrow$ A2: Ƀ.0008, B1: Ƀ.0016". B1 still represents the deposit bitcoin address and A2 still represents our bitcoin address for receiving the money. We further deposit Ƀ.0010 and withdraw Ƀ.0006, and the resulting transactions are shown in Table 3.

From Table 3, we can see that the deposit bitcoin address in the market does not change. Among all cryptomarkets in Table 1, the Point Tochka Market has the most transparent bitcoin transaction flows, which can be further confirmed when we study the order and confirmation actions.

Table 4: Deposit and Withdrawal in the Dream Market

Action	Observed bitcoin transaction		Balance
	Sender	Receiver	
Deposit Ƀ.0024	A1: Ƀ.0030	⟶ B1: Ƀ.0024, A2: Ƀ.0006	Ƀ.0024
Withdraw Ƀ.0008	B2: Ƀ.0008	⟶ A2: Ƀ.0008	Ƀ.0016
Deposit Ƀ.0010	A2: Ƀ.0006, A2: Ƀ.0008	⟶ B3: Ƀ.0010, A3: Ƀ.0004	Ƀ.0026
Withdraw Ƀ.0006	B4: Ƀ.0006	⟶ A4: Ƀ.0006	Ƀ.0020

Deposit and Withdrawal in the Dream Market: We perform the same sequence of actions in the Dream Market and Table 4 shows the resulting transactions. From Table 4, we can see that the bitcoin address B2 that sends us money during the first withdrawal is different than the bitcoin address B1 that receives our money during the first deposit. After the second withdrawal, we find that there is still Ƀ.0024 in B1. This means that the Dream Market uses different bitcoin addresses to receive deposit and send withdrawal. From the subsequent deposit and withdrawal actions, the deposit is sent to B3 and the withdrawal is received from B4. This further confirms the observation. This mechanism makes it harder to track the bitcoin flow, thus better protects the privacy of the market and prevents the re-identification attack.

The Empire and Silk Road 3.1 Markets have similar transaction patterns as Dream Market for the deposit and withdrawal actions. We omit the tables for them. The Wall Street and Berlusconi Markets provide neither deposit nor withdrawal functions. They allow buyers directly pay from their own bitcoin addresses.

In the next, we study patterns in the resulting bitcoin transactions for the order and confirmation actions.

Table 5: Order and Confirmation in the Point Tochka Market

Action	Observed bitcoin transaction		Balance
	Sender	Receiver	
Order ฿.0014	B1: ฿.0040	C1: ฿.0014, B1: ฿.0026	฿.0026
Confirm	C1: ฿.0014	D1: ฿.0014	฿.0026
Order ฿.0015	B1: ฿.0026	C2: ฿.0015, B1: ฿.0011	฿.0011
Confirm	C2: ฿.0015	D2: ฿.0015	฿.0011

Order and Confirmation in the Point Tochka Market: We purchase two orders and Table 5 shows the resulting bitcoin transactions. After we place the first order, the money is sent from the deposit bitcoin address B1 to an escrow account C1. The balance is sent back to B1. After the vendor fulfills the order, we confirm it. The money in the escrow C1 is then immediately transferred to a new bitcoin address D1, which is suspected of being the vendor's bitcoin address. In the second order, we pay ฿0.0015 to a different vendor. Similar to the transactions in the first order, the money moves to an escrow account C2 after the order and then moves from C2 to the destination bitcoin address after confirmation. The escrow address C2 is different than the old escrow address C1. From this experiment, we can see that the bitcoin transaction flows are transparent. For each new order, the market will generate a new escrow bitcoin address. We also observe that our deposit bitcoin address will not change. By tracking the money flowing out of the escrow accounts, we can potentially find the suspicious bitcoin addresses of vendors.

Table 6: Order and Confirmation in the Dream Market

Action	Observed bitcoin transaction		Balance
	Sender	Receiver	
Order ฿.0014	B1: ฿.0040 does not change		฿.0026
Confirm	B1: ฿.0040 still no change. No transactions observed		฿.0026
Order ฿.0015	B1: ฿.0040 does not change		฿.0011
Confirm	B1: ฿.0040 still no change. No transactions observed		฿.0011

Order and Confirmation in the Dream Market: We also purchase two products in the Dream Market and Table 6 shows the resulting transactions. After we place the first order of ฿0.0014, we find that no transaction associated with the deposit bitcoin address B1 happen. After the vendor fulfills the order and we confirm it, still nothing happens. This means Dream Market uses a different escrow bitcoin address to pay the vendor and the money in the original deposit address B1 does not move. Since we know neither the

escrow address used to pay the vendor nor the vendor bitcoin address, there is no easy way for us to observe the relevant transactions. We suspect that the Dream Market has its own private ledger to record the balances of the deposit and escrow accounts for each user. After each order, the bitcoin in the deposit account will be transferred to the escrow account. After each confirmation, the bitcoin in the escrow account will be transferred out to vendor's accounts. The ledger of Dream Market might be a private and centralized ledger. This strategy makes the transactions within the Dream Market stealthy and cannot be seen from the public. This strategy well protects the privacy of the market and vendors.

Table 7: Order and Confirmation in the Wall Street Market

Action	Observed bitcoin transaction	
	Sender	Receiver
Order ฿.0014	A1: ฿.0040 ⟶	C1: ฿.0014, A2: ฿.0026
Confirm	C1: ฿.0014 is transferred to another address through mixing	
Order ฿.0015	A2: ฿.0026 ⟶	C2: ฿.0015, A3: ฿.0011
Confirm	C2: ฿.0015 is transferred to another address through mixing	

Order and Confirmation in the Wall Street Market: The Wall Street Market does not have deposit function. It allows us to pay directly with our bitcoin address. When we purchase, we are required to send a specific amount of bitcoin to a newly generated escrow address and to provide a bitcoin address for receiving the refund if the order fails. Following this procedure, we purchase two products. Table 7 shows the resulting transactions. After we place the first order, we can see the escrow address C1. After we confirm the order, we can observe that the money in the escrow C1 is transferred to a new bitcoin address through a mixing service. Since there are multiple receivers, we do not know which one is the receiver corresponding to the escrow C1.

Table 8: Order and Confirmation in the Berlusconi Market

Action	Observed bitcoin transaction	
	Sender	Receiver
Order ฿.0014	A1: ฿.0040 ⟶	C1: ฿.0014, A2: ฿.0026
Confirm	C1: ฿.0014 is transferred to another address through mixing	
Order ฿.0015	A2: ฿.0026 ⟶	C2: ฿.0015, A3: ฿.0011
Confirm	C2: ฿.0015 is transferred to another address through mixing	

Order and Confirmation in the Berlusconi Market: The Berlusconi Market does not have deposit function neither. We directly pay with our bitcoin address and Table 8 shows the resulting transactions. After we place the first order, we can see the escrow address C1. But before we confirm the order, the money in the escrow C1 is already transferred to a new bitcoin address through the mixing service. This makes it hard for us to track the bitcoin flows. Similar pattern is observed for the second order. The Berlusconi Market applies mixing services on escrow addresses to further protect the privacy of the market and vendors.

Since the Wall Street and Point Tochka Markets provide more transparent bitcoin transaction patterns, the feedback reviews may help re-identify the bitcoin addresses of vendors. A feedback review is usually posted right after the buyer confirms the order. Each review represents an approximate bitcoin transaction including approximate date and money. We will see more details in the next sections.

5 Bitcoin Transaction Patterns in the Dream Market

In this section, we track back the bitcoin flows of the withdrawal operation in Dream Market with Algorithm 3. We find a bitcoin address containing more than 800 bitcoins which is worth over 3 million dollars at present, and it collects those bitcoins from multiple addresses in one transaction. Figure 7 shows part of the flow tree we observed. The red node represents our bitcoin address for receiving money in the withdrawal. We observe a bitcoin transaction pattern called "peeling chain" [14].

Peeling Chain: The head of a peeling chain is a bitcoin address with a lot of bitcoins. A small amount of bitcoin is peeled off from this address in a transaction and a "Shadow address" is generated to collect the remaining and still large amount of bitcoin. By repeating this process, the large amount of bitcoin can be peeled down. Peeling chain is popular for organizations dealing with a lot of clients. The bitcoin addresses in a peeling chain are not necessary the addresses of Dream escrow accounts. They might be exchange addresses [9].

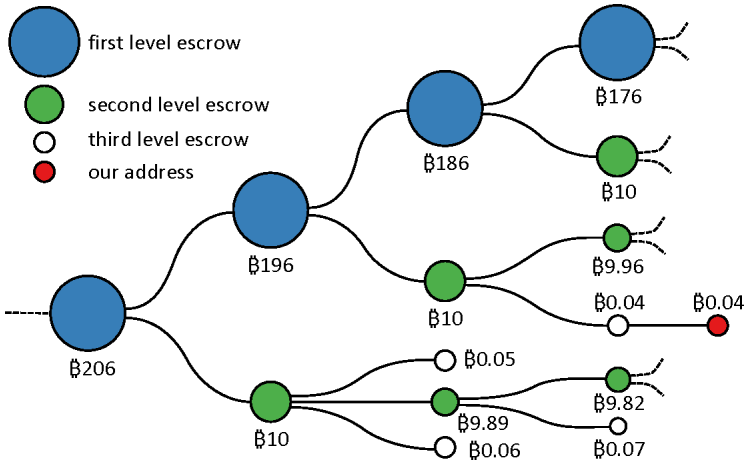


Fig. 7: Bitcoin "peeling chain" patterns in the Dream Market

The head of this peeling chain is a bitcoin address which receives more than 800 bitcoins. In each transaction, 10 bitcoins are transferred to a new address and the remaining amount is transferred to the shadow address. We call these blue addresses in the main chain the first level escrow addresses. Each of the addresses containing 10 Bitcoins becomes a head of a new smaller peeling chain. In this new chain, one transaction peels

off even smaller amount of bitcoin to pay different users. We call the green addresses in the smaller peeling chains the second level escrow addresses. The bitcoins peeled off from the second order addresses are send to third level escrow address, which are white nodes in Figure 7. The white nodes directly send bitcoins to users (red nodes) of dream market. The amount of bitcoin received by the third order escrow address is exactly the number of bitcoins required by users. No shadow addresses are generated.

In addition to this pattern, we also notice that the mixing pattern from the third order escrow addresses to users' addresses. The Dream market allows users to use mixing services. Users need to pay a certain percentage of fees to use mixing services when they withdraw bitcoins.

Clustering bitcoin addresses: The peeling chain patterns can potentially help cluster bitcoin addresses of users in the Dream Market. Since we can track the peeling chain easily, we may be able to identify other transactions happening in the Dream Market by comparing the white-red transactions with the feedback reviews.

6 Bitcoin Transaction Patterns in the Wall Street Market

In this section, we explore the possibility of linking Wall Street feedback reviews with bitcoin transactions. We order a product "Spotify Premium Lifetime Warranty" and pay $1.25 on about 4:40 pm, March 5, 2019, then we confirm the order and write a review by 01:36 am, March 8, 2019. Figure 8 shows some feedback reviews. In Figure 8, the fourth review is written by us and "u***y" is our account ID. Since we know our bitcoin address "15v3...", we track the money flow.

Table 9 shows the transaction relevant to the order action. The output address "33sY..." is the escrow account, and the other output address "14ZK..." is the shadow address containing our remaining money. Table 10 shows the transaction relevant to the confirmation action. It is a mixing transaction containing 24 inputs and 22 outputs. The escrow address "33sY..." is in the sender list. Table 10 shows top three output addresses whose receiving bitcoins are most close to the money we send. By comparing the bitcoins of the three outputs with our money $1.25, we can see that output address "3Jpp..." is most likely to be the vendor's address. We can also see that the transaction happens at 2019-03-08 02:06, which is 30 minutes later than our review time 01:36 am.

We further explore the transactions related to "3Jpp...". Table 11 shows the list of transactions relevant to the reviews in Figure 8. For example, the first transaction happens at 2019-03-08 23:07 and the amount of money is $1.12, which matches with the feedback review "H***e - 03/08 10:49 pm - 1.25 USD". The time of the transaction is 18-minute later than the time of review. Comparing the reviews in Figure 8 with the transactions in Table 10 and 11, we can see we successfully find the transactions of four reviews. For the first and sixth reviews in Figure 8, we do not find them manually. This is because the vendor may have multiple bitcoin address for receiving money and "3Jpp..." might be just one of them.

We purchase the product again and find the same bitcoin address "3Jpp..." receiving the money. This further confirms that "3Jpp..." belongs to the vendor.

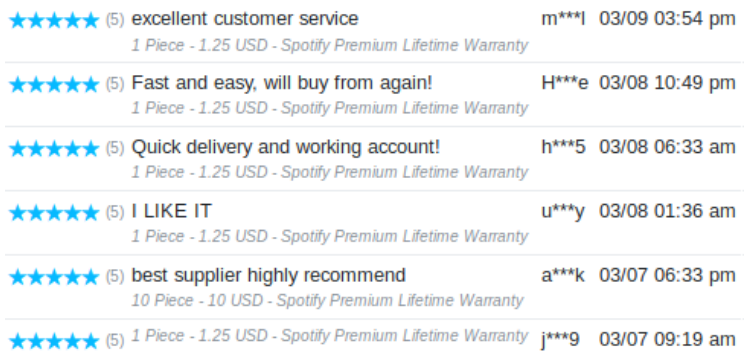


Fig. 8: Feedback Ratings in the Wall Street Market

Table 9: The bitcoin transaction relevant to the order action

Hash (txid)	25f33135c87b37205b49a9ade6faa1d6837a4fcb42340270753562b7e1802bee		
Time (UTC)	2019-03-05 16:49	Input count: 1 ; Output count: 2	
Input 0	15v3cQR4H9iz3nb1tXwNd33ETo7ZEX2wir	฿.03554909	$132.31
Output 0	33sYgQnBkBkm3mDbWJY6KMoT7no1eNd4j5	฿.00032256	$1.20
Output 1	14ZKcens6g6J58kBVGNk3Hs2a94NE3bnUT	฿.03517496	$130.92

Table 10: The bitcoin transaction relevant to the confirmation action

Feedback	u***y - 03/08 01:36 am - 1.25 USD		
Hash (txid)	27c4946ad1e5e648e987d66a882d98f08ebcb3bae8d11aea70b9dac7219aa036		
Time (UTC)	2019-03-08 02:06	Input count: 24 ; Output count: 22	
Input 16	33sYgQnBkBkm3mDbWJY6KMoT7no1eNd4j5	฿.00032256	$1.20
Output 8	39o2XAjmFTkSGFrkUPsJRNrDUvUCYiXyP5	฿.00061720	$2.39
Output 10	336djQeGFA4etdRv3xRESoKVV3zHr8YvMv	฿.00020500	$0.79
Output 18	3JppEPMTeUXWY96g5D19k6hhK1QLATdwJV	฿.00029320	$1.14

Table 11: The bitcoin transactions relevant to the feedback reviews in Fig. 8

Feedback	H***e - 03/08 10:49 pm - 1.25 USD		
Hash (txid)	5542aaf1c045f951ba7623510237217d97009eb403778cec6ae101d4462583e1		
Time (UTC)	2019-03-08 23:07	Input count: 47 ; Output count: 42	
Output 40	3JppEPMTeUXWY96g5D19k6hhK1QLATdwJV	฿.00028800	$1.12
Feedback	h***5 - 03/08 06:33 am - 1.25 USD		
Hash (txid)	bb6a4c9d5c747d941eeb6fc5031973351382cb0550be35bfbefda0c07380b63d		
Time (UTC)	2019-03-08 08:26	Input count: 15 ; Output count: 20	
Output 19	3JppEPMTeUXWY96g5D19k6hhK1QLATdwJV	฿.00029290	$1.13
Feedback	a***k - 03/07 06:33 pm - 10 USD		
Hash (txid)	c022177c6bb26a2c3ad82b699bb9d3d950131a8b13dd54665e7f6e4f8d8263a3		
Time (UTC)	2019-03-07 19:21	Input count: 35 ; Output count: 38	
Output 26	3JppEPMTeUXWY96g5D19k6hhK1QLATdwJV	฿.00251950	$9.75

7 Related Work

Ron et al. is the first to build a bitcoin graph and analyze the quantitative attributes in bitcoin transaction history [16]. Clustering bitcoin addresses into wallets is one basic task in the bitcoin transaction analysis. Researchers have widely used two simple heuristics [8, 18, 10]. The first heuristic is to put shadow/change address together with its input address into one wallet. The second heuristics is to put all input addresses into one wallet if there is a single output address. Androulaki et al. test the effectiveness of the bitcoin address clustering methods with stimulation [8]. Spagnuolo et al. link the clustered wallets to the Silk Road escrow addresses exposed by FBI and analyze the bitcoin flow [18]. Fleder et al. not only link the clustered wallets with Silk Road escrow but also link wallets with public wallets [10]. PageRank is then applied on the transaction graph to find interesting and important wallets [10]. The effectiveness of address clustering is also studied [13]. Mixing technology is also introduced to improve the anonymity [17, 19].

8 Conclusion

We find interesting Bitcoin transaction patterns associated with cryptomarkets. The results demonstrate that the privacy protection mechanism in Bitcoin is still vulnerable in terms of simple analysis. An adversary can easily gain valuable information for analyzing the activities happening in the markets.

References

1. bitcoin-blockchain-parser. https://github.com/alecalve/python-bitcoin-blockchain-parser/blob/master/README.md, accessed: 2019-03-10
2. Bitcoin core. https://bitcoin.org/en/bitcoin-core/, accessed: 2019-03-10
3. Five surprising facts about bitcoin. https://www.washingtonpost.com/news/the-switch/wp/2013/08/21/five-surprising-facts-about-bitcoin, accessed: 2019-03-10
4. How bitcoin lets you spy on careless companies. https://web.archive.org/web/20140209202222/http://www.wired.co.uk/news/archive/2013-06/06/bitcoin-retail, accessed: 2019-03-10
5. How to parse the bitcoin blockchain. http://codesuppository.blogspot.com/2014/01/how-to-parse-bitcoin-blockchain.html, accessed: 2019-03-10
6. Mapping the bitcoin economy could reveal users' identities. https://www.technologyreview.com/s/518816, accessed: 2019-03-10
7. Running a full node. https://bitcoin.org/en/full-node#what-is-a-full-node, accessed: 2019-03-10
8. Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T., Capkun, S.: Evaluating user privacy in bitcoin. In: International Conference on Financial Cryptography and Data Security. pp. 34–51. Springer (2013)
9. de Balthasar, T., Hernandez-Castro, J.: An analysis of bitcoin laundry services. In: Nordic Conference on Secure IT Systems. pp. 297–312. Springer (2017)

10. Fleder, M., Kester, M.S., Pillai, S.: Bitcoin transaction graph analysis. arXiv preprint arXiv:1502.01657 (2015)
11. Genkin, D., Papadopoulos, D., Papamanthou, C.: Privacy in decentralized cryptocurrencies. Communications of the ACM **61**(6), 78–88 (2018)
12. Gilbert, M., Dasgupta, N.: Silicon to syringe: Cryptomarkets and disruptive innovation in opioid supply chains. International Journal of Drug Policy **46**, 160–167 (2017)
13. Harrigan, M., Fretter, C.: 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). pp. 368–373. IEEE (2016)
14. Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M., Savage, S.: A fistful of bitcoins: characterizing payments among men with no names. In: Proceedings of the 2013 conference on Internet measurement conference. pp. 127–140. ACM (2013)
15. Nakamoto, S., et al.: Bitcoin: A peer-to-peer electronic cash system (2008)
16. Ron, D., Shamir, A.: Quantitative analysis of the full bitcoin transaction graph. In: International Conference on Financial Cryptography and Data Security. pp. 6–24. Springer (2013)
17. Ruffing, T., Moreno-Sanchez, P., Kate, A.: Coinshuffle: Practical decentralized coin mixing for bitcoin. In: European Symposium on Research in Computer Security. pp. 345–364. Springer (2014)
18. Spagnuolo, M., Maggi, F., Zanero, S.: Bitiodine: Extracting intelligence from the bitcoin network. In: International Conference on Financial Cryptography and Data Security. pp. 457–468. Springer (2014)
19. Ziegeldorf, J.H., Grossmann, F., Henze, M., Inden, N., Wehrle, K.: Coinparty: Secure multi-party mixing of bitcoins. In: Proceedings of the 5th ACM Conference on Data and Application Security and Privacy. pp. 75–86. ACM (2015)