Characteristics of Bitcoin Transactions on Cryptomarkets

Xucan Chen[1,6], Mohammad Al Hasan[2,6], Xintao Wu[3,6], Pavel Skums[1,6], Mohammadjavad 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 bitcoins 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 · Peel 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

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	✓	✓	✓	✓	

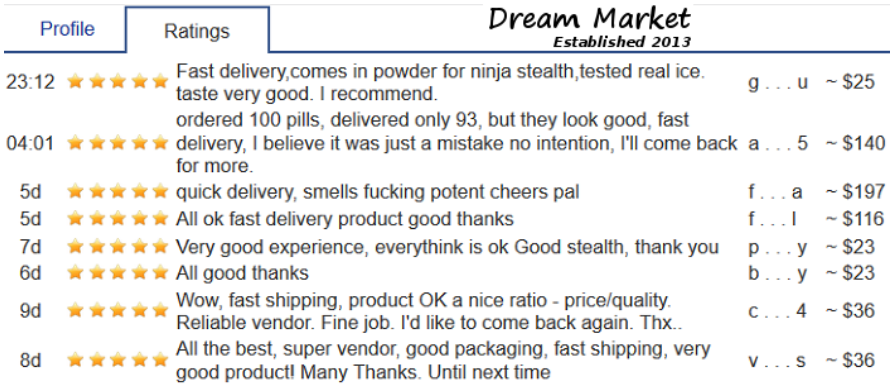
From Table 1, we can see that bitcoin is accepted in all cryptomarkets. In addition to bitcoin, four other types of cryptocurrencies are also accepted by different markets. They are monero, litecoin, ethereum, and bitcoin cash. Note that bitcoin cash is a variant of but different than bitcoin and is 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].

I am here

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

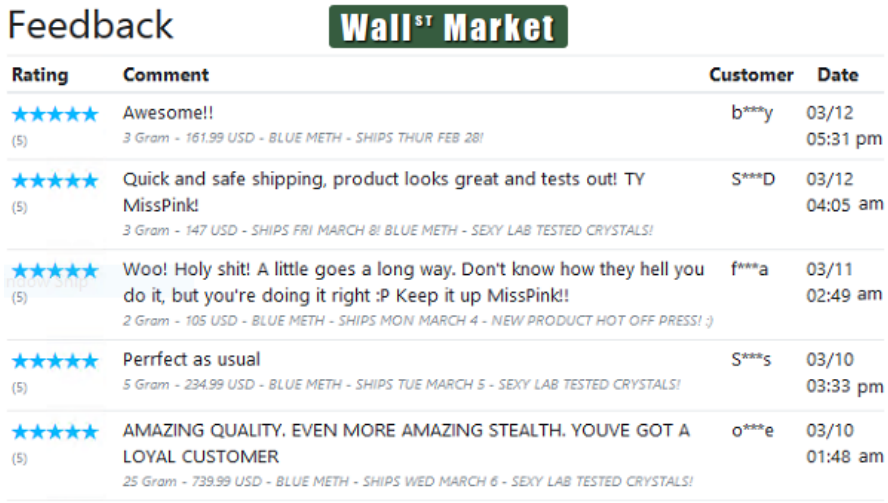
In this paper, we systematically study the vulnerabilities of bitcoin privacy that exist in cryptomarkets. We identify and categorize patterns of bitcoin transactions in cryptomarkets. The observations are then used for discussing the possibility of re-identifying bitcoin addresses related to crytomarkets. 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 reviews 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 reviews 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-based Bitcoin Transactions in Cryptomarkets

In this section, we review the escrow-based transactions 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 [10]. 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

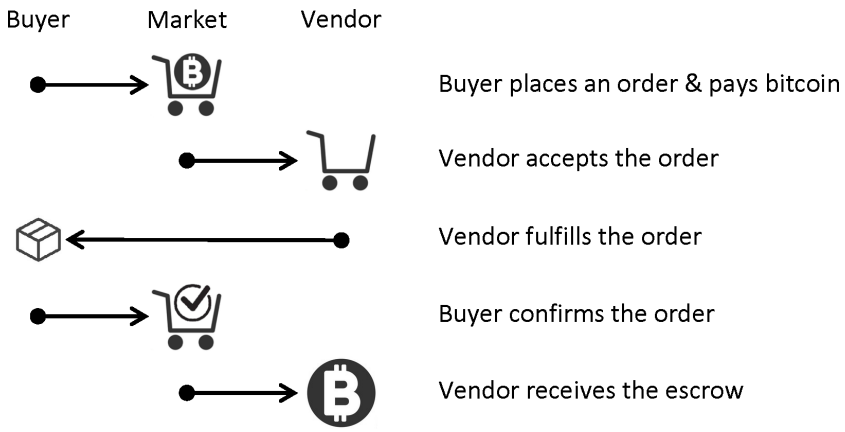


Fig. 3: A flowchart depicting an escrow-based transaction in cryptomarkets

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 Data Collection and Description

To trace the bitcoin flow, we parsed the public bitcoin transactions. We first install the bitcoin core program [2] and run a full node [7]. The 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. 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 graph [5, 1]. In Algorithm 1, we split each block from the blockchain and save the timestamp which is shared by all transaction data in this block. Bitcoin adopts a mechanism to control the generation speed of block based on the number of miners in Bitcoin. It will adjust the calculation workload for miners to realize a pattern that a new block will be generated around every 10 minutes.

For each transaction in transaction list, we gather information like transaction hash, sender list, and receiver list. Combined with timestamp of block, we save each transaction with four parts. One receiver contains information like the receiver address and the number of Sathochi it received. Sathochi is one hundred millionth of a bitcoin and is the smallest unit of bitcoin. In bitcoin, an address has to receive bitcoin first before it sends bitcoin. Therefore, each sender in transaction data does not contain bitcoin address or bitcoin value. Instead, it contains transaction hash and transaction index, which refer to an earlier transaction. We can use the transaction hash to find this earlier transaction and use the index number to find the referred receiver from the receiver list. By combining the sender in current transaction with receiver in referred transaction to one address, we can generate a bitcoin flow.

Algorithm 2 shows how we can build flow graph with transaction data we parsed. Transaction data we parsed were ranked with time already. We start with the earliest transaction. Receivers of transaction contain address information. Consequently, we add re-

Algorithm 1 Parsing Bitcoin Transactions

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

```
for each block do
    this_transaction_time ⇐ block.timestamp;
    for each transaction in the block.transactions do
        this_transaction_hash = transaction.this_transaction_hash;
        sender_list = [] ;
        for each sender in the transaction.senders do
            sender_list.add(sender.index, sender.previous_transaction_hash,
              sender.previous_transaction_index)
        receiver_list = [] ;
        for each receiver in the transaction.receivers do
            receiver_list.add(receiver.index, receiver.bitcoin_address,
              receiver.bitcoin_value)
        [this_transaction_time, this_transaction_hash, sender_list, receiver_list] ⇒
          formatted_this_transaction_time.json
```

Algorithm 2 Constructing Bitcoin Transaction Graph

Input: Bitcoin Ledger L
Output: Bitcoin Transaction Graph $G(V, E)$

```
Rank the transactions in the ledger L with timestamp;
for each transaction tx in the ledger L do
    for each receiver in tx.receiver_list do
        add a node i = [tx.this_transaction_hash, receiver.bitcoin_address] to the node set
          V;
        for each sender in tx.sender_list do
            find transaction tx′ in the ledger L with tx′.this_transaction_hash =
              sender.previous_transaction_hash;
            find sender.bitcoin_address in tx′.receiver_list ;
            find or create a node j = [sender.previous_transaction_hash,
              sender.bitcoin_address] ;
            add an edge (i, j) to the edge set E ;
```

ceivers to the graph as nodes directly. For each sender, we look for an earlier receiver with reference information and this referred receiver should already be inside the graph. Then we connect this earlier receiver to the current receiver in graph.

If we want to trace bitcoin flow with a specific transaction, we can build a local flow graph with Algorithm 3. In Algorithm 3, we find nodes in flow graph generated by Algorithm 2 that are close to query node within k hops.

Algorithm 3 Extract local graph for the query node

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

```
Ignore the edge direction, G.Adj[u] represents the neighbors;
S ⇐ {q};
T ⇐ {};
for each node v in V do
    v.d = ∞;
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};
```

3.1 Properties of Bitcoin transactions

When Bitcoin was first proposed in 2008 [13], the creator of bitcoin system recommended the user of bitcoin can create a new address for each transaction to obtain better anonymity.

Shadow Address: If a owner wants to spend bitcoins in one address, he has to spend all bitcoins during one transaction. In the current implementation of Bitcoin, a change address, which is called "Shadow address" would be generated to collect the remaining bitcoins of this transaction [8]. This mechanism forces the user to change their address to strengthen privacy.

Multi-Inputs: Considering the multiple addresses one user can own, bitcoin supports a user to send bitcoins from multiple addresses in one transaction.

These two properties of bitcoin transaction have been utilized by researchers as strategies to cluster bitcoin addresses[12, 8, 9]. And we can still trace the bitcoin flow in transaction data although bitcoin adopts these two mechanisms.

3.2 Mixing of Bitcoin Transactions

Apparently the multiple addresses strategy provided by Bitcoin is not enough to protect users' identity. As a consequence, different mixing services have emerged which can randomly mix different transactions into one transaction. In mixed transactions, the multiple inputs are from different senders and multiple outputs go to different receivers. Mixing services reduce the traceability of bitcoin flows, and make the analysis of bitcoin graph more challenging.

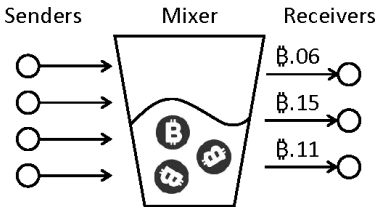


Fig. 4: A bitcoin transaction containing mixing service

4 Actions and Observed Resulting Transactions

In this section, we describe our re-identification attack by purchasing products in cryptomarkets. All cryptomarkets offer escrow services to avoid scams. With escrow system, the bitcoin used to buy products will be saved in escrow accounts after a buyer places an order and would be available to the vendor until the buyer finalizes the order. Since we know the start point (buyer address) of the transaction, we can trace the bitcoin flow to uncover the escrow mechanism in cryptomarkets. With this attack, we are able to find some escrow addresses controlled by the cryptomarkets at the same time.

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 are observed in the bitcoin transaction graph if there are any. Table 2 shows whether we can observe the bitcoin transactions for the four operations in cryptomarkets. We notice that Dream Market, Empire Market, and SilkRoad 3.1 operate in a similar way. These markets ask buyers to deposit bitcoins to some deposit addresses and these bitcoins will be collected to their escrow addresses pool in near future. Users of these markets could not manipulate bitcoins in deposit addresses. Once bitcoins are withdrawn, the market will send the bitcoin to the external wallet from the market escrow address pool. Although adopting the deposit system as well, the Point Tochka Market is operated in a totally different way with the three markets above. The deposit address of Point Tochka will transfer the bitcoin following our operations, which makes the bitcoin flow from buyer address to escrow address and then to vendor address clear and transparent. Wall Street Market and Berlusconi Market don't utilize the deposit system. In Wall street Market, the bitcoin flow is synchronized with users' operation like Point Tochka. In the Berlusconi Market, bitcoins sent to escrow accounts are transferred to the escrow addresses pool before we finalize the transaction. Based on different mechanisms in different markets, we can adopt corresponding strategies to analyze the data to achieve deanonymization of these addresses used for illicit activities. In Wall Street and Point Tochka, we can get the information of reviews of each vendors. A review will be posted after a buyer confirms a order. Therefore each review in these two markets represents a bitcoin transaction from an escrow address to an vendor address. It's unrealistic to purchase products from all these vendors in market to obtain bitcoin address of each vendor. We can take advantage of the review information of each vendor to find a bitcoin address whose receive history is matched with the reviews list. For Dream Market, Emprie Market, and SilkRoad 3.1 Market, We can trace

the deposit bitcoin future flow or trace back from the withdrawal flow to analyze the transaction pattern in their escrow addresses pool.

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 how the bitcoin addresses change during the process of an transaction. We first study the deposit and withdrawal actions and then the order and confirmation actions. In each market, four operations are performed: deposit ₿.0024, withdraw ₿.0008, deposit ₿.0010, and withdraw ₿.0006. The resulting transactions are observed in the bitcoin transaction graph if there are any. 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 ₿.0024 and the resulting transaction is "A1: ₿.0030 $\rightarrow$ B1: ₿.0024, A2: ₿.0006". In the sender part "A1: ₿.0030", A1 represents our bitcoin address and ₿.0030 represents the money in that address. In the receiver part "B1: ₿.0024, A2: ₿.0006", B1 represents the deposit bitcoin address provided by the Point Tochka Market, ₿.0024 represents the money that B1 receives, A2 represents our new bitcoin address, and ₿.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 ₿.0008 and the resulting transaction is "B1: ₿.0024 $\rightarrow$ A2: ₿.0008, B1: ₿.0016". B1 still represents the deposit bitcoin address and A2 still represents our bitcoin address for receiving the money. We further deposit ₿.0010 and withdraw ₿.0006, and the resulting transactions are shown 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 ₿.0024	A1: ₿.0030	⟶ B1: ₿.0024, A2: ₿.0006	₿.0024
Withdraw ₿.0008	B2: ₿.0008	⟶ A2: ₿.0008	₿.0016
Deposit ₿.0010	A2: ₿.0006, A2: ₿.0008	⟶ B3: ₿.0010, A3: ₿.0004	₿.0026
Withdraw ₿.0006	B4: ₿.0006	⟶ A4: ₿.0006	₿.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 ฿.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 money, thus better protects the privacy of the market and prevents the re-identification attack.
The Empire and Silk Road 3.1 Markets have similar resulting transaction patterns as Dream Market for the deposit and withdrawal actions. Thus 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.
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 transactions 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

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

neither the escrow address used to pay the vendor neither 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 ledger to record the balances of the deposit account and escrow account 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 is 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 also 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.

5 Bitcoin Transaction Pattern Behind Dream Market

In this section we traced back the bitcoin flow of withdrawal operation in Dream Market with the algorithm 3, we found an address with more than 800 bitcoins which is worth over 3 million dollars currently, and it collect those bitcoins from multiple addresses at one transaction.

Figure 5 is part of the flow graph we observed based on the withdrawal transaction. We notice there exists a bitcoin activity called “peeling chain” which based on “Shadow Address” mechanism we mentioned in Section 3 [12].

Peeling Chain: In a peeling chain, an address with large amount of bitcoins is head of this chain. A smaller part of bitcoin is peeled off from this address through a transaction and an one-time ”Shadow address” is generated to collect the remaining large amount of bitcoin. By repeating this process, the large amount of bitcoin can be pare down. This pattern is very popular for organizations dealing with a large amount of clients.

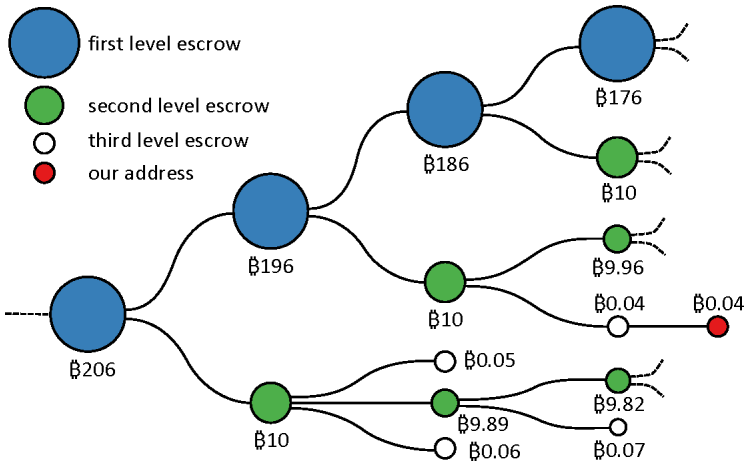


Fig. 5: Bitcoin flow patterns in the Dream Market

The head of this peeling chain we found is a bitcoin address which received more than 800 bitcoins. After the start of peeling process, 10 bitcoins are transferred to one address and the remaining amount is transferred to the shadow address every time. We defined

these addresses in the main chain as the first level escrow addresses in dream market. For all the addresses received 10 Bitcoin from main chain, each of them then works as a head of a new peeling chain. In this new chain, one transaction peels off even smaller amount of bitcoin-mostly less than 1 bitcoin. And the amount of bitcoin took off from these branch chain was different. For addresses in these branch chain, we defined them as second level escrow addresses. The bitcoin peeled off from the second order address are send to third level escrow address, represented by white nodes in Figure 5 which is also the address that directly send bitcoins to users of dream market. The amount of bitcoin received by the third order escrow address is exactly the number of bitcoins required by users of Dream Market. These bitcoins were sent to users without shadow address. At the same time, we also noticed existence of mixing from the third order escrow address to users address, which is provided by Dream market. Users can pay a certain percentage of fees to use mixer when they withdraw bitcoins.

Clustering of Addresses: The shadow address property makes it reasonable to cluster shadow address and the sender address to one entity. In a peeling chain structure, all the addresses in a chain can be clustered together.

If we treat clustered addresses as one entity here, bitcoin flow in the Dream Market is very clear. Users(mainly buyers) deposit bitcoins to deposit address. Bitcoins in deposit addresses will be collected and gathered to one hub entity, then the bitcoin will be transferred through only three hops to the users address(mainly vendors). Mix technology may exist in the last transaction during this process. Through this graph, we can find a lot of bitcoin addresses that directly interact with Dream Markets and most of them belong to vendors in the Dream Market.

6 Related Work

Since the blockchain data is accessible to all users, multiple papers were published regarding bitcoin analysis. Ron et al. is the first to build a bitcoin graph and analyze the quantitative attributes in bitcoin transaction history [14]. Address Clustering is one of the main challenge in anonymity analysis. Researchers clustering addresses for one user by applying two simple heuristics [8, 16, 9]. One is clustering multiple inputs of a transaction and the other is clustering Shadow address with sender address which is also utilized in our analysis in Section 5. Androulaki et al. clustered bitcoin addresses and test its effectiveness with stimulated data [8]. Spagnuolo et al. cluster addresses with same strategies to get a new graph whose nodes represent entities, then they linked the SilkRoad hub address exposed by FBI to an entity in graph and analysis the bitcoin flow related with SilkRoad entity [16]. Fleder et al. did a similar work [9]. Besides linking the SilkRoad to entity in clustered graph, they also linked some others entities to Bitcoin forum users. Some users in Bitcoin forum exposed their bitcoin address in internet. In that paper, they apply PageRank algorithm on the transaction graph to find the closeness level between SilkRoad with these forum users. Because of the effectiveness of address clustering [11], Mixing technology [15, 17] was introduced to Bitcoin community to improve the anonymity.

7 Conclusion and Future Works

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.
Our next step would be to design innovative graph mining and machine learning algorithms to automatically detect novel and interesting subtree or subgraph patterns with or without the query transactions obtained by purchasing activities. We will also study how to optimize the purchasing frequency so that we can maximize the likelihood of the detected patterns. We also want to study whether we can match each approximate transaction in review ratings to the bitcoin transaction graph. The study of these concrete problems will eventually lead us to consider the theoretical analysis of the privacy-threat model in Bitcoin or other types of cryptocurrecy. We will also design simulations and generate synthetic transaction graphs to verify the theoretical analysis.

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. Fleder, M., Kester, M.S., Pillai, S.: Bitcoin transaction graph analysis. arXiv preprint arXiv:1502.01657 (2015)
10. Gilbert, M., Dasgupta, N.: Silicon to syringe: Cryptomarkets and disruptive innovation in opioid supply chains. International Journal of Drug Policy **46**, 160–167 (2017)
11. 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)

12. 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)
13. Nakamoto, S., et al.: Bitcoin: A peer-to-peer electronic cash system (2008)
14. 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)
15. 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)
16. 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)
17. 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)