2020 11th International Conference on Information and Communication Systems (ICICS) 978-1-7281-6227-0/20/$31.00 ©2020 IEEE 10.1109/ICICS49469.2020.239510

Deanonymization of Litecoin Through Transaction-Linkage Attacks

Zongyang Zhang*, Jiayuan Yin*, Yizhong Liu†, and Jianwei Liu*
*School of Cyber Science and Technology, Beihang University, Beijing, China
Email: {zongyangzhang,yinjiayuan,liujianwei}@buaa.edu.cn
†School of Electronic and Information Engineering, Beihang University, Beijing, China
Email: liuyizhong@buaa.edu.cn

***Abstract*—With the development of blockchain technology, the use of cryptocurrencies in online payments has become increasingly prevalent. Litecoin, proposed in 2011, is currently the fifth-largest cryptocurrency in market value. Due to certain characteristics, such as the use of pseudonyms as transaction addresses, user privacy could be protected to some extent. However, there are some problems about its privacy guarantees.**

In this paper, we aim to reveal the severity of deanonymization attacks on online Litecoin payments. Firstly, we simulate purchases on merchant websites accepting Litecoin and monitor trackers embedding on information and payment pages. Secondly, we conduct transaction-linkage attacks on simulated digital and physical transaction flows, respectively. Our results show that a tracker is more likely to find the target transaction on Litecoin blockchain by collecting the digital transaction flows and implementing transaction-linkage attacks. The number of digital transaction flows with anonymous set size 1 and 2 account for 95% and 5% of all digital transaction flows, respectively. The success rate of the transaction-linkage attack is 0.975. To get the optimal uncertainty parameters of transaction-linkage attacks, we introduce a refined deanonymization attack by making real purchases. Finally, we present two new privacy protection measures against transaction-linkage attacks.

***Index Terms*—Litecoin, privacy, web payment, deanonymization, transaction-linkage.**

I. Introduction

Proposed in 2008, Bitcoin [1] is the first decentralized cryptocurrency and provides users with a certain degree of privacy and anonymity. As more and more users choose to make online payment via cryptocurrencies, the problem of privacy leakage during payments gradually emerges. Trackers may embed on a merchant's website via third-party scripts [2], collect user's purchase information and link the purchase to a single transaction via transaction-linkage attacks. Furthermore, trackers may get the user's other transactions via address clustering attacks. In this way, trackers may build a connection between the user's identity information and all of the user's addresses, which is against the will of cryptocurrency users in pursuit of privacy and anonymity.

To investigate the privacy risks of web payments via cryptocurrencies, Goldfeder et al. [3] present a simulation of trackers to deanonymize cryptocurrency users. They focus on transaction-linkage attacks and try to establish a linkage between a user's purchase and a transaction on the blockchain. They implement transaction-linkage attacks on 10000 simulated transaction flows and get the distribution of anonymous sets. The size of an anonymous set indicates that for a given transaction flow, how many transactions might be confused with it. They also propose a cluster intersection attack to bypass mixing [4]. Mixing means that multiple users send the same amount in a single multi-input and multi-output transaction, which is called a mixing transaction, breaking the association between input and output addresses. Even if a user adopts multiple rounds of mixing, his Bitcoin wallet (we define a user's wallet as all of his addresses) still might be exposed, as long as a tracker gets sufficient mixing transactions.

There are still some insufficiencies about the work of [3]. They lack detailed investigation on other cryptocurrencies and fail to obtain the optimal uncertainty parameter for transaction-linkage attacks. In addition, a detailed analysis of privacy protection measures is not given. We improve the work of [3], and select Litecoin as the deanonymization target to analyze its privacy leakage.

A. Motivations to Analyze Litecoin

As the earliest cryptocurrency with the largest market value, Bitcoin has low capacity, poor scalability and other limitations. Various altcoins are proposed subsequently. There exist obvious differences among characteristics of those altcoins' blockchains, such as transaction processing speed and density of transactions. There have been many studies analyzing Bitcoin privacy issues, but for other cryptocurrencies, there are few relevant analyses. In addition, using the same parameters as Goldfeder et al. [3] attacking Bitcoin to attack other cryptocurrencies may not be optimal or not applicable. Therefore, to expose the severity of deanonymization attacks on online payments of a particular altcoin, we need to do further research.

Proposed in 2011, Litecoin [5] is currently the fifth-largest cryptocurrency measured in market value.[1] An increasing number of online merchants start to accept Litecoin. However, Litecoin still has certain problems in terms of privacy protection. It is necessary to conduct a separate analysis on this important altcoin. As far as we know, our work represents the first research of the severity of deanonymization attacks on online Litecoin payments.

[1]https://coinmarketcap.com/(access on April 29, 2019)

We discuss the differences between Litecoin and Bitcoin as follows. Inspired by Bitcoin, Litecoin [5] is a peer-to-peer cryptocurrency similar to Bitcoin. However, Litecoin has three distinct differences. Firstly, in Litecoin, the time interval between blocks is 2.5 minutes, which provides a faster transaction confirming rate. Secondly, Litecoin issues 84 million coins in total, four times as many as Bitcoin. Thirdly, Litecoin's proof-of-work mechanism uses the scrypt algorithm proposed by Percival [6], facilitating ordinary computer miners.

B. Our Contributions

In this paper, we make the following contributions.

- We simulate purchases on 31 websites of merchants accepting Litecoin and monitor privacy leaks of users. Not surprisingly, most of the merchants leak users' important information to more than one trackers.
- In order to link a user's identity information to transactions, transaction-linkage attacks are simulated. The simulated transaction flows are divided into two groups: digital flows and physical flows. The simulation results show that trackers are more likely to deanonymize physical transactions than digital ones.
- A new deanonymization attack based on existing transaction-linkage attacks is proposed. We repeatedly complete small-amount purchases and adjust the three uncertainty parameters. By mounting multiple transaction-linkage attacks, we finally obtain the optimal value of the uncertainty parameters and improve the success rate of transaction-linkage attacks.
- We propose two new privacy protection measures. Specifically, a user may delay his payment for a certain time after the payment page loads, reducing the success rate of transaction-linkage attacks. A user may also divide his addresses into a number of unrelated clusters, so as to reduce the success rate of clustering attacks. We carry out a simulation experiment to verify the effectiveness of the first new protection measure.

C. Organization

In Section II and Section III, we give related works and monitor privacy leakage, respectively. In Section IV, transaction-linkage attacks against Litecoin are simulated. Then a new deanonymization attack is proposed and simulated In Section V. In Section VI, we summarize existing privacy protection measures and propose two new privacy protection measures. Finally, in Section VII, a conclusion is given.

II. Related Works

To deanonymize cryptocurrency users, a tracker needs to complete two operations, namely, OP_1 and OP_2. OP_1 aims at linking a cryptocurrency address, i.e., the hash of a public key, to a particular user's real identity, using techniques such as network analysis and transaction-linkage. In OP_2, the address obtained in OP_1 is used to obtain all the addresses belonging to the same user, using techniques such as addresses clustering and cluster intersection.

a) Work related to OP_1: Goldfeder et al. [3] propose transaction-linkage attacks and try to establish a linkage between a user's purchase and a transaction on the blockchain. Specifically, during a user purchasing from a merchant, a tracker embeds on an information page and gets the loading time, the legal tender price pair (t_i, d_i), and the LTC-dollar exchange rate at time t_i ER_{t_i}. Then, the tracker computes $b_i = d_i/ER_{t_i}$. If the tracker finds a transaction on blockchain with transacting time t_0 and output Litecoin amount b_0, where $t_0 = t_i$ and $b_0 = b_i$, this transaction is exactly the target transaction. In fact, there exists some discrepancy between t_i and t_0. Also, there may be some deviation between the legal tender price (excluding shipping fee) d_i and the actual legal tender price (including shipping fee) d_0. The exchange rate ER_{t_i} may differ from the one that is used by the payment processor. Due to these differences, Goldfeder et al. propose three uncertainty parameters: payment time U_T, price U_P and exchange rate U_E. For a given time, a legal tender price pair and different levels of U_T, U_P and U_E, they intend to find how many transactions are on the blockchain.

Goldfeder et al. define the anonymity set as all the transactions which satisfy uncertainties of a time and a legal tender price pair. They assume that the number of anonymous sets with size i is A_i, and define true positive rate $P = \Sigma_i(A_i/i)/N$, where N denotes the number of transaction flows. We regard P as the success rate of the transaction-linkage attack. The larger P is, the more successful the transaction-linkage attack is. Note that if the size of the anonymity set is 1, the transaction flow corresponds to a single transaction, which means the transaction could be uniquely identified. On the contrary, a large anonymous set means that the target transaction is mixed with many other transactions, i.e., it is hard to distinguish the target transaction from others. Thus, a tracker expects more anonymous sets of size 1.

However, Goldfeder et al. do not make real purchases. Instead, they collect 100 prices commonly used on merchant websites, randomly select 100 timestamps, and form $10,000$ simulated trading flows. These simulated flows had no corresponding transactions on the blockchain. They define the size of the anonymity set of these simulated flows as one plus the number of transactions that satisfy the uncertainty parameters of $U_T = 15$ minutes, $U_P = \$5$ and $U_E = 5$ minutes. Note that the three uncertainty parameters are set empirically. They calculate P and evaluate the success rate of their simulated transaction-linkage attacks.

In addition to transaction-linkage attacks, several network analysis methods are proposed to link an address to a user's identity. Koshy, Koshy and Mcdaniel [7] build CoinSeer, a Bitcoin client, collect data and design heuristics to map Bitcoin addresses to IP addresses. Biryukov, Khovratovich and Pustogarov [8] succeed in establishing connections between transactions and Bitcoin clients by discovering the entry nodes of Bitcoin clients, monitoring servers and maping transactions to entry nodes. Biryukov and Pustogarov [9] deanonymize the users who connect to Bitcoin network via Tor.

b) Work related to OP_2: Ron and Shamir [10] propose a heuristic that all the inputs of a Bitcoin transaction belong to a single user with a high probability. Meiklejohn, Pomarole and Jordan [11] improve this heuristic and propose the complete address clustering algorithm, which provides trackers with potential opportunities to obtain all the Bitcoin addresses belonged to a single user from a single Bitcoin address of him.

To resist address clustering, Maxwell [12] present CoinJoin, in which multiple senders combine their transactions into a single joint transaction, breaking the one-to-one correspondence between sending and receiving addresses [13]. Moser and Bohme [14] introduce JoinMarket, a platform for Bitcoin users to make CoinJoin transactions. The more mixing rounds a user conducts, the greater anonymity he enjoys. A tracker will get multiple wallets by solely using the clustering algorithm towards a mixing transaction, failing to identify the user. Encountered with this situation, Goldfeder et al. [3] propose cluster intersection attack. If a tracker gets multiple mixing transactions of a single user, the tracker is able to carry out cluster intersection attack to identify the user's wallet.

III. Monitoring of Information Leakage

In this section, we monitor the information leakage of online payment using Litecoin. Theoretical analysis and practical results are given respectively.

A. Important Information During a Purchasing Process

In order to monitor the leaked information of online payment, we first look at important information that a user may reveal when making online payments. A standard online purchasing process is as follows.

1) A user selects the products that he wants to buy on the shopping website and adds them to the shopping cart.
2) After clicking the "checkout" button, the user is presented with a legal tender price excluding shipping fee d_i on the information page.
3) Then the user fills in his real identity information and delivery address and submits.
4) After the submission, the merchant gives a legal tender price including shipping fee d_0. Meanwhile, the payment processor gives the payment address and Litecoin price b_0 in accordance with the exchange rate at that time.
5) Then, the user sends b_0 Litecoin to the payment processor, who gives the receipt to the user. The products will be delivered to the real address filled in by the user and the entire transaction will be completed.

We show important information that may be leaked during a purchasing process and the ways of leakage in Table I. Embedment on an information page enables a tracker to reveal a user's real identity, while embedment on a payment page allows a tracker to acquire payment address and Litecoin price. With payment address, a tracker is able to easily locate the corresponding transaction on blockchain. However, payment processors often take measures to protect payment pages. Consequently, in most cases, a tracker only uses a payment time and a legal tender price excluding shipping fee to link the purchase information to a transaction. Then, the tracker further builds a connection between the user's identity information and the transaction.

TABLE I: Information that may be leaked during purchases and the ways of leakage

Information type	Leaked important information	The ways of leakage
Purchase information	Payment address	Payment page
	Litecoin price	Payment page
	Payment time	Information page
	Legal tender price excluding shipping fee	Cart page or information page
Identity information	User's real identity	Information page

B. Monitoring Process and Results

We monitor the leakage of important information during purchases on merchant websites. We find Litecoin Foundation [1], a website listing nearly a hundred of merchant sites accepting Litecoin, filter out the merchants temporarily closed or refuse to ship physical products to China and select 31 merchants. Then, we register on them and simulate purchases, during which we use Fiddler 4 [2], a common-used web debugging tool, to monitor the trackers embedding on information and payment pages. Concretely, we remove all preexisting sessions in Fiddler 4, enter information or payment pages, collect all HTTP(S) requests and responses and pick out all potential trackers.

As shown in Table II, all but one merchants' information pages are embedded by trackers. Among them, 87% are embedded by more than one trackers. On average, one merchant's information page is embedded by 3.87 trackers. In contrast, none but three merchants' payment pages are embedded by trackers. We guess that, in most cases, trackers may only monitor the loading time of an information page and a legal tender price. It is almost impossible for trackers to get a payment address and a Litecoin price.

Goldfeder et al. [3] adopt a relatively larger sample space to conduct a similar experiment on merchants accepting Bitcoin. We use a relatively smaller sample space, as Litecoin, after all, is a derivation of Bitcoin and there are fewer merchants accepting Litecoin. According to our results, the leakage of users' important information on merchant sites is also quite severe.

IV. Transaction-Linkage Attacks Against Litecoin

After monitoring information leakage in Section III, we then simulate transaction-linkage attacks to link a user's identity information to his transactions. The specific attack procedures are given in Section IV-A. In Section IV-B, we mount transaction-linkage attacks towards our own simulated transaction flows.

[1]https://litecoin-foundation.org/businesses/

[2]https://www.telerik.com/download/fiddler/fiddler4

TABLE II: Trackers' embedding statistics on merchant sites

Type of merchandise	Website	Information page	Payment page
Featured	https://bitify.com	2	0
	https://cryptocurrencyposters.com	5	0
Art/Collectibles	https://bitographs.com	3	0
	https://cryptoart.com	5	0
	https://unratio.com	3	2
	https://wallpapers4Litecoin.com	0	0
Books	https://jbestbooks.com	1	0
	http://9bravos.com.br	11	1
	https://psychedelicpress.co.uk	7	0
Clothes	https://hodlmonkey.com	3	0
	https://topshelftoker.com	5	0
	https://allthingsdecentral.com	5	0
	https://cryptoverge.com	5	0
Food/Drinks	https://crypto-coffee.com	1	0
	http://drapis.com	2	0
	http://bronxdeli.com	3	0
	https://eichenhain.com	4	0
	https://svryfood.com	4	0
	https://mitragaia.com	6	0
Gift cards	https://cryptodechange.com	2	0
	https://egifter.com	6	0
	https://bitcoingiftcards.com.au	2	0
Gold/Silver	https://coaex.com	2	0
	https://jmbullion.com	7	0
Electronics	https://shop.secpoint.com	4	0
	https://rexsilentium.com	2	0
Jewelry	https://floraandfaun.com	7	0
	https://lefkarasilver.com	2	0
	https://ravenandriley.com	3	1
	https://fudmartng.com	1	0
	https://arrowandboard.com	7	0

A. Specific Attack Procedures

Before discussing the details of transaction-linkage attacks, we describe the specific attack procedures in Fig. 1.

1) Firstly, a tracker monitors a user's purchase process. If the tracker successfully embeds on the payment page, he gets a payment address and a Litecoin price.
2) Secondly, the tracker could find the target transaction easily on blockchain, where the user sends Litecoin to the payment processor. If the tracker only embeds on the information page, he gets a loading time of information page, a legal tender price and the user's real identity information. In this case, he mounts transaction-linkage attacks to link purchase information to a target transaction on the blockchain.
3) Thirdly, the tracker judges whether the target transaction is a mixing transaction. If not, the tracker directly uses a clustering algorithm to obtain the user's Litecoin wallet. Otherwise, the tracker tries to get more mixing transactions belonging to the same user and mounts a cluster intersection attack.

The attack procedures establish a connection between a user's real identity and his Litecoin wallet. As in most cases, a tracker could only embed on a user's information page, and transaction-linkage attacks play an important role in the attack procedures.

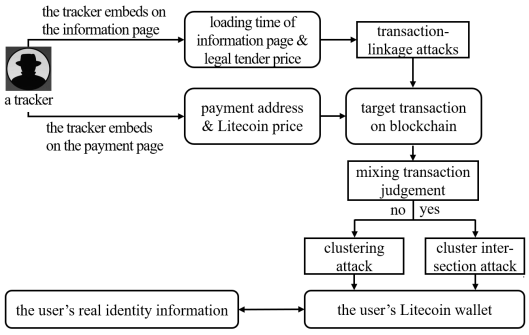


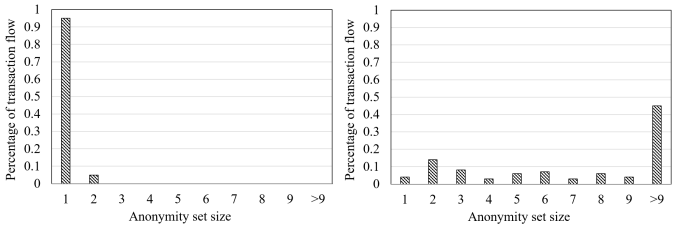
Fig. 1: Specific attack procedures

B. Simulating Transaction-Linkage Attacks on Litecoin Blockchain

To simulate transaction-linkage attacks on Litecoin blockchain, we make the following preparations:

1) Download and install Litecoin Core [15];
2) Download Litecoin blockchain and synchronize the Litecoin client with Litecoin network;
3) Install and configure python-bitcoinrpc [16] to implement python calls to the Litecoin client;
4) Download the LTC-dollar exchange rate historical data [1] (LTC means Litcoin);
5) Convert time of historical exchange rate into Unix time.

Methods and Results. Note that no shipping fee is required for digital products and most physical products charge shipping fees. A tracker is able to distinguish whether a user pays for digital products or physical products. Therefore, we discuss simulated digital transaction flows separately from simulated physical transaction flows. We select 10 prices of digital products on merchant websites and randomly produce 10 Unix timestamps from 7:00 am on April 1, 2018, to 7:00 am on April 4, 2018, making up 100 digital transaction flows. We set the uncertainty parameters as follows: $U_T = 15$ minutes, $U_P = \$0$ and $U_E = 5$ minutes. Similarly, we select 10 prices of physical products, making up 100 physical transaction flows and change U_P to \$5. We carry out simulated transaction-linkage attacks on the two groups of transaction flows respectively. The distributions of anonymity sets size are shown in Fig. 2.



(a) Simulated digital transaction flows ($U_P = \$0$). (b) Simulated physical transaction flows ($U_P = \$5$).

Fig. 2: Distribution of anonymity set size of simulated transaction flows ($U_T = 15$ minutes and $U_E = 5$ minutes).

[1] https://www.coindesk.com

According to Fig. 2(a), the number of digital transaction flows with anonymous set size 1 accounts for 95%, and the number with anonymous set size 2 accounts for 5%. The true positive rate is 0.975. Therefore, a tracker is very likely to find the target transaction on Litecoin blockchain. According to Fig. 2(b), the number of physical transaction flows with anonymous set size 1 only accounts for 4%, the number with anonymous set size 2 accounts for 14%, and the number with anonymous set size greater than 9 reaches up to 45%. The true positive rate is less than 0.229. Therefore, due to the interference of shipping fee, it is much more difficult for a tracker to attack a physical transaction flow.

V. A New Deanonymization Attack Against Litecoin

The uncertainty parameters discussed in Section IV are determined empirically, without taking into account of comparision and optimization of three uncertainty parameters. We propose a new deanonymization attack, where 50 real small-amount transactions are completed in Section V-A. We obtain the optimal values of three uncertainty parameters for a specific transaction flow in Section V-B. In Section V-C, we give some explanations.

A. Generation of Real Transaction Flows

We purchase Poetry Vol 1 (1.30 AUD e-book) on online merchant of J Best Books for 50 times from April 29, 2018 to May 7, 2018. We record the loading time of information page and the legal tender price for each purchase. The specific steps of a complete purchase are as follows:

1) Select the products and confirm to pay by Litecoin.
2) Visit the information page of and record its loading time.
3) Record the legal tender price of the product (i.e, 1.30 AUD), enter an email address and confirm. It takes about 20 seconds from loading the information page to completing the identity information.
4) Visit the payment page and record the payment address as well as the Litecoin price.
5) Send Litecoin to the payment address and record each sending address. It takes about 30 seconds from loading the payment page to completing the payment.

Eventually, we acquire 50 groups of triples, each of which includes the loading time of the information page, the price in USD and the sending address.

B. Transaction-linkage Attacks on Real Transaction Flows

a) Adjustment of payment time uncertainty parameter: Considering all the 50 transactions, we relax the price uncertainty parameter U_P to \$10 and the exchange rate uncertainty parameter U_E to 20 minutes. In order to find out the minimum value of U_T, we change the payment time uncertainty parameter U_T and repeat transaction-linkage attacks. The results are shown in Fig. 3. When U_T is set to 10 minutes, all 50 Litecoin transactions are included. While if U_T is set to larger than 10 minutes, irrelevant transactions might appear, increasing the probability of confusion and reducing the success rate of transaction-linkage attacks. Therefore, we set U_T to 10 minutes.

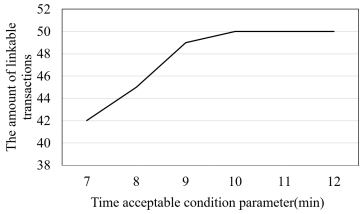
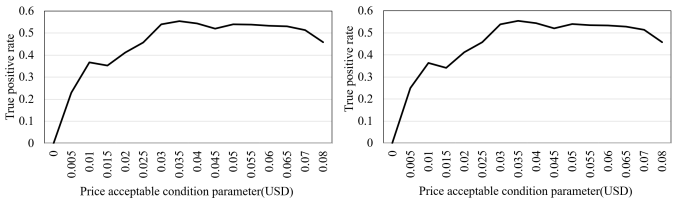


Fig. 3: Effect of payment time uncertainty parameter on transactions amount (Price uncertainty parameter $U_P = \$10$ and exchange rate uncertainty parameter $U_E = 20$ minutes).

b) Adjustment of price and exchange rate uncertainty parameters: We download the historical data of the LTC-dollar exchange rate on Coindesk [1] and those of the AUD-dollar exchange rate on X-RATES website [2]. Dividing the former by the latter, we obtain the LTC-AUD exchange rate (updating every 5 minutes). Since all of the 50 transactions have been recorded by blockchain 10 minutes after the loading of information page, we neglect U_E that is greater than 10 minutes. U_T and U_E are set to 10 minutes and 5 minutes, respectively. We repetitively adjust U_P and mount transaction-linkage attacks. The results are shown in Fig. 4(a). Then we change U_E to 10 minutes and repeat the above attacks. The results are shown in Fig. 4(b).

According to Fig. 4(a), when $U_T = 10$ minutes and $U_E = 5$ minutes, the maximum true positive rate is 0.554 and U_P is \$0.035. As shown in Fig. 4(b), under $U_T = 10$ minutes and $U_E = 10$ minutes, the maximum true positive rate is also 0.554 and U_P is also \$0.035. To sum up, the maximum true positive rate is 0.554, at which point U_P is \$0.035.

For items with other prices, trackers can also adopt a similar heuristic, first setting U_P and U_E large enough to find the minimum value of U_T, and then adjusting U_E and U_P to achieve the maximum true positive rate.



(a) Exchange rate uncertainty parameter $U_E = 5$ minutes.

(b) Exchange rate uncertainty parameter $U_E = 10$ minutes.

Fig. 4: Effect of price uncertainty parameter on true positive rate. Payment time uncertainty parameter $U_T = 10$ minutes.

C. Explanation

Note that our uncertainty parameters in Section V-B are only optimal for purchasing a 1.3 AUD digital product for 50

[1] https://www.coindesk.com/price/Litecoin

[2] https://www.x-rates.com/calculator/?from=AUD&to=USD&amount=1

times from April 29, 2018 to May 7, 2018. If the purchasing period, the product price or the sample size change, the optimal uncertainty parameters may vary. We will explain it in detail as follows.

a) Experimental period: The transaction processing speed of Litecoin blockchain is not constant as time goes by. Also, the density of transactions and the distribution of transaction amount may vary from time to time. Hence, if a tracker aims at attacking transactions within a certain period of time, he should select a sample set within this specific period of time.

b) Product price: Transactions of different Litecoin amount have different distribution characteristics. Thus, our optimal uncertainty parameters are by no means a reference for digital products with higher price. A high attack rate for a product with a specific price relies on the tracker's careful selection of samples. The tracker should select sample products with price close to that price.

c) Sample size: Due to limited funds, we only conduct 50 small-amount transactions. To increase the accuracy of optimal uncertainty parameters evaluation, a tracker should select as many samples as possible.

VI. Suggestions for Users to Protect Privacy

In this section, we discuss privacy protection measures. We review existing privacy protection measures in Section VI-A. We propose two new privacy protection suggestions in Section VI-B from the aspect of users.

A. Existing Privacy Protection Measures

As shown in Table III, privacy protection measures are classified into three categories: the network layer, the transaction layer and the application layer. The transaction layer realizes the core function of a blockchain, that is, reliable and credible data transmission between two cryptocurrency addresses. At the network layer, users may connect Bitcoin network via Tor [17] or deploy HyperLedger [18]. At the transaction layer, users may adopt centralized or discentralized mixing to break the relationship between sending addresses and receiving addresses. Some new cryptography schemes, such as Monero [19] and Zcash [20] may help protect user privacy as well. At the application layer, cold storage [21] could be used to store users' keys offline, protecting them against cyber attackers.

B. Our Suggestions for Users to Protect Privacy

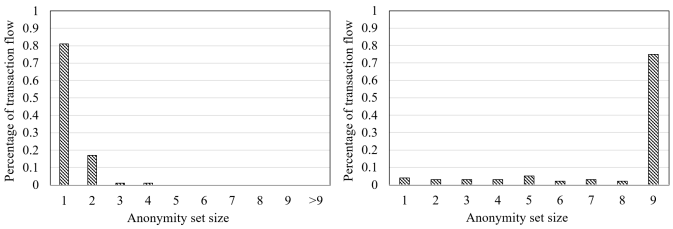
In order to increase the difficulty of an attacker to deanonymize a user, we propose the following suggestions.

a) Suggestion one: Delaying payment for a certain time: At present, most of cryptocurrency users are unaware of their privacy leakage. After selecting products and entering the information page, a user usually inputs his identity information and confirms the transaction without a long delay. When the user enters the payment page, the payment processor requires the user to pay within a limited time period. Most users choose to pay immediately, rather than deliberately delay the payment for some certain time. If so, a tracker is very likely to mount transaction-linkage attacks successfully by setting a relatively small payment time uncertainty parameter. We change the payment time uncertainty parameter from 15 minutes to 30 minutes and mount the same transaction-linkage attacks as in Section IV-B.

[1]Bitlaundry, Bitcoin wiki (2010), https://en.bitcoin.it/wiki/BitLaundry

TABLE III: Existing privacy protection measures

Layer	Measure	Key technique
Network	Blockchain on Tor [17]	Data obfuscation
	HyperLedger [18]	Alliance chain
Transaction	Bitlaunder [1]	Centralized mixing
	Bitcoin Fog [22]	
	Mixcoin [4]	
	CoinJoin [12]	Discentralized mixing
	CoinShuffle [23]	
	CoinParty [24]	
	Monero [19]	New cryptography scheme
	Zcash [20]	
Application	Cold storage [21]	Offline key storage



(a) Simulated digital transaction flows ($U_P = \$0$). (b) Simulated physical transaction flows ($U_P = \$5$).

Fig. 5: Distribution of anonymity set size of simulated transaction flows ($U_T = 30$ minutes and $U_E = 5$ minutes).

As shown in Fig. 5, the number of digital flows with anonymity set size 1 is decreased from 95% to 81%. Meanwhile, there is almost no physical transaction flows with anonymous set size 1, and the number of physical flows with anonymity set size greater than 9 accounts for 75%. Thus, along with the increase of payment time uncertainty parameter, a tracker is more likely to get a larger anonymous set.

To protect privacy, users ought to slow down the confirmation of identity information and payment speed. In fact, users don't have to wait too long. Even if the user waits for a shorter time period, such as 20 minutes or 15 minutes, it will help to mitigate the transaction-linkage attacks. Given that most users know nothing about their privacy leakage, payment processors should provide users some hints and encourage users to moderately slow down their payment speed.

In the real world, most users may feel reluctant to delay payments, since it may waste his precious time or he does not care about his privacy. However, the reputation of an online merchant and its payment processor will be negatively impacted if the privacy of their users is seriously leaked. To maintain a green website and gain a good reputation, an online merchant and its payment processor have motivation to prevent

users from being tracked. A website could implement incentives mechanisms, such as accumulate points and bonuses, to encourage users delaying payments.

b) Suggestion two: Dividing addresses into a number of unrelated clusters and managing the keys on your own: Currently, the most popular Litecoin client is Litecoin Core [15], which stores its keys on local storage [25]. While a user installs Litecoin Core, the software automatically generates 100 public and private key pairs, forming a keypool. When the user sends Litecoin to other addresses, Litecoin Core automatically selects a key pair from the keypool as a change address to receive the remaining Litecoin.

The advantage of Litecoin Core mainly lies in its simple interface and easy operation. It automatically generates keys and signs transactions. However, such a key management mechanism is vulnerable to an address clustering attack. A tracker could easily cluster change and sending addresses.

To resist address clustering attacks, we suggest professional users to manage keys by themselves. For instance, a user may utilize Bitaddress [1] to generate public and private key pairs. When needed, a user may manually input the private key or scans the QR code to transfer the private key into the client (such as blockchain.info). In addition, a user may intend to use password-derived keys, such as Brainwallet [2] to generate key pairs that could be exclusively managed by himself.

Some further measures should be taken to resist the clustering attack. A user could divide all his addresses into two sub-wallets, i.e., SW_1 and SW_2. Addresses in SW_1 should never be used in the same transaction with addresses in SW_2. In such way, a tracker only obtains two sub-wallets of the user. The user could keep his wallet confidential by dividing all his addresses into multiple unrelated sub-wallets.

VII. Conclusion

We analyze the privacy leakage during Litecoin online payments in detail, highlighting the severity and harm of privacy leakage. We show that digital products buyers are more vulnerable to transaction-linkage attacks than physical products buyers. In addition, we improve the transaction-linkage attack and get the optimal uncertainty parameters. Besides, two privacy protection suggestions are given to provide more privacy for users.

Acknowledgment

This work was supported in part by the National Natural Science Foundation of China (61972017, 61972018, 61932014), in part by the Beijing Natural Science Foundation (4182033), in part by the National Cryptography Development Fund (MMJJ20180215), and in part by the Beihang University Innovation & Practice Fund for Graduate (YCSJ-02-2019-011).

[1] https://github.com/pointbiz/bitaddress.org

[2] Brainwallet (2015), https://brainwallet.io

References

[1] N. Satoshi. (2008) Bitcoin: A peer-to-peer electronic cash system. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] S. Englehardt, D. Reisman, C. Eubank, P. Zimmerman, J. Mayer, A. Narayanan, and E. W. Felten, "Cookies that give you away: The surveillance implications of web tracking," in *24th International Conference on World Wide Web*. ACM, 2015, pp. 289–299.

[3] S. Goldfeder, H. Kalodner, D. Reisman, and A. Narayanan. (2017) When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies. [Online]. Available: https://arxiv.org/abs/1708.04748

[4] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, "Mixcoin: Anonymity for bitcoin with accountable mixes," in *18th International Conference on Financial Cryptography and Data Security*, 2014, pp. 486–504.

[5] C. Lee. (2011) [ann] litecoin - a lite version of bitcoin. launched! [Online]. Available: https://bitcointalk.org/index.php?topic=47417

[6] C. Percival and S. Josefsson. (2016) The scrypt password-based key derivation function. [Online]. Available: https://www.rfc-editor.org/rfc/rfc7914.txt

[7] P. Koshy, D. Koshy, and P. McDaniel, "An analysis of anonymity in bitcoin using p2p network traffic," in *18th International Conference on Financial Cryptography and Data Security*. Springer, 2014, pp. 469–485.

[8] A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in bitcoin p2p network," in *21st ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2014, pp. 15–29.

[9] A. Biryukov and I. Pustogarov, "Bitcoin over tor isn't a good idea," in *36th IEEE Symposium on Security and Privacy*. IEEE, 2015, pp. 122–134.

[10] D. Ron and A. Shamir, "Quantitative analysis of the full bitcoin transaction graph," in *17th International Conference on Financial Cryptography and Data Security*. Springer, 2013, pp. 6–24.

[11] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A fistful of bitcoins: characterizing payments among men with no names," in *2013 conference on Internet measurement conference*. ACM, 2013, pp. 127–140.

[12] G. Maxwell. (2013) Coinjoin: Bitcoin privacy for the real world. [Online]. Available: http://bitcointalk.org/index.php?topic=279249.0

[13] K. Atlas. (2014) Weak privacy guarantees for sharedcoin mixing service. [Online]. Available: http://www.coinjoinsudoku.com/advisory/

[14] M. Moser and R. Bohme, "Join me on a market for anonymity," in *15th Annual Workshop on the Economics of Information Security*. ICSI, 2016.

[15] P. Wuille and G. Maxwell. (2017) Base32 address format for native v0-16 witness outputs. [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0173.mediawiki

[16] J. Garzik. (2013) Python interface to bitcoin's json-rpc api. [Online]. Available: https://github.com/jgarzik/python-bitcoinrpc

[17] R. Dingledine, N. Mathewson, and P. Syverson. (2004) Tor: The second-generation onion router. [Online]. Available: http://www.dtic.mil/dtic/tr/fulltext/u2/a465464.pdf

[18] (2015) Hyperledger architecture working group paper. [Online]. Available: https://www.hyperledger.org/

[19] N. V. Saberhagen. (2013) Cryptonote v 2.0. [Online]. Available: https://cryptonote.org/whitepaper.pdf

[20] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed e-cash from bitcoin," in *34th IEEE Symposium on Security and Privacy*. IEEE, 2013, pp. 397–411.

[21] A. M. Antonopoulos, *Mastering Bitcoin: unlocking digital cryptocurrencies*. "O'Reilly Media, Inc.", 2014.

[22] A. Omedetou. (2011) Bitcoin fog: Secure bitcoin anonymization. [Online]. Available: https://bitcointalk.org/index.php?topic=50037

[23] T. Ruffing, P. Moreno-Sanchez, and A. Kate, "Coinshuffle: Practical decentralized coin mixing for bitcoin," in *19th European Symposium on Research in Computer Security*, 2014, p. 345–364.

[24] J. H. Ziegeldorf, F. Grossmann, M. Henze, N. Inden, and K. Wehrle, "Coinparty: Secure multi-party mixing of bitcoins," in *proceedings of the 5th ACM Conference on Data and Application Security and Privacy*. ACM, 2015, pp. 75–86.

[25] S. Eskandari, J. Clark, D. Barrera, and E. Stobert. (2018) A first look at the usability of bitcoin key management. [Online]. Available: https://arxiv.org/abs/1802.04351