2021 International Conference on Computer, Communication, Chemical, Materials and Electronic Engineering (IC4ME2) | 978-1-6654-0637-6/21/$31.00 ©2021 IEEE | DOI: 10.1109/IC4ME253898.2021.9768636

A Framework for Tracing the Real Identity of a Bitcoin Scammer

Md. Nur Islam, Md. Golam Shakhawat Hossen, Samson P. Baidya,
Md. Ahsan Ullah Emon, and Md. Sakir Hossain
Department of Computer Science
American International University-Bangladesh (AIUB)
Dhaka, Bangladesh
Email: sakir.hossain@aiub.edu

***Abstract*—Bitcoin stores its transaction details in an open distributed public ledger. In cryptocurrencies, the real identity of a user is hidden, and the only information about a user publicly available is his public address, which is not linkable to his real identity, and the transactions are sent to the public address. Among all the cryptocurrencies, bitcoin is renowned for providing the highest anonymity. This feature is exploited by the scammers and illegal users to perform their illegal transactions anonymously. To rein in such illegal activities, it is essential to expose the real identity of bitcoin users. In this paper, we propose a technique to trace the real identity of a bitcoin user. In this technique, the blockchain maintains a public ledger where every transaction of that chain is recorded and anyone within the blockchain can monitor that. The proposed platform will have a tracker for tracking a bitcoin user. A victim submits a complain to the platform giving the pubic address of the scammer. The platform continues to track the scammer. The proposed technique exposes the user identity exploiting the bitcoin and real-world currency conversion scenarios. While the existing transaction tracing techniques require the IP address and/or absence of the mixing services, the proposed technique is free of such kinds of requirements.**

***Index Terms*—cryptocurrency, scamming, bitcoin, cybercrime, transactions, real identity**

I. Introduction

Everything is becoming digital day by day in this modern world, and currencies are also being digitized through cryptocurrencies. Cryptocurrencies are digital assets that do not have any physical existence. A decentralized control system is used to ensure their security, facilities, and transaction [1]. One of the most popular cryptocurrencies is bitcoin [2]. Bitcoin and other cryptocurrencies are getting increasing attention nowadays because of their unique characteristics. There is no centralized control over cryptocurrencies, and all transactions are carried out in a high degree of anonymity. Due to the high-level of anonymity, bitcoin has turned into a medium of illegal transactions in cyberspace. The shutting down of the drug market, named Silk Road, is the most well-known example in this regard [3]. Moreover, the cryptocurrencies are used for terror financing, thefts, scams, and ransomware [4]–[6]. To rein-in such transactions, it is necessary to know the real identity of the cryptocurrency users. Unfortunately, such information is not publicly available, and it is difficult to trace the real identity of the users. For this reason, it is imperative to find a way of tracing the real identity of the cryptocurrency users while maintaining as much anonymity as possible.

It is observed in [7] that the majority of the minted bitcoins remain inactive and hidden in addresses that never participate in any outgoing transactions. These accounts are not used in shopping or any kind of payment activities. For this reason, tracking those accounts is not feasible if the accounts are not used for any kind of transaction. An experiment is carried out in [8] in order to strengthen the privacy preserving algorithms of the bitcoin transactions. By replicating the behaviors and transactions of the bitcoin blockchain, it is shown that it is possible to uncover almost 40% of the users' profiles even after adopting bitcoin's recommended privacy measures [8]. However, this percentage rate will decrease in case of scammers and illicit users as they apply more sophisticated privacy measures in addition to the bitcoin recommended privacy measures. By observing real-time transaction relay traffic over a period of time, the authors in [9] show that it is possible to find the IP address of the bitcoin user's device using a heuristic algorithm, which enables us to reveal the true identity of a bitcoin user. However, the technique of using an IP address in exposing the real identity may not always be possible as there are many ways to spoof IP addresses. Thus, the mapping of the real identity of the scammers through their IP data is not practically feasible. In [1], the browsers' cookie is exploited in revealing the real identity of a user. If a user performs a transaction in an e-commerce site using a cryptocurrency, a third-party tracker can link the transaction information to the user's cookie and then further to link it to the user's real identity. Furthermore, if the third-party tracker is able to link two such online purchases from the same user onto the blockchain, then it is possible to identify the entire cluster of addresses and transactions, even if the user uses blockchain anonymity techniques to hide their identity. However, there are some approaches like mixing services which make bitcoin user's identity more anonymous, thereby making the identity more difficult to be tracked down [1].

From the above discussion, it is evident that the real identity of a bitcoin user can be figured out from the IP address. However, it is not a straightforward process. The above techniques can only reveal the real identity if the following two conditions

978-1-6654-0637-6/21/$31.00 ©2021 IEEE

Fig. 1. Real-time tracking of an address through OXT platform.

are not met: (a) users do to use any browser like "tor" which helps them to hide their IP address, and (b) no mixing services are used.

In this paper, we address the tracing of the user who is behind a cryptocurrency transaction. In the proposed technique, we consider almost all kinds of scenarios such as whether the scammers use a browser like "tor" or use mixing services. We mainly focus on scams, ransomware, stolen bitcoin, and similar cases where the victim is forced to pay through bitcoin or bitcoin got stolen somehow. The proposed technique can reveal the real identity of a scammer even if he uses tor browser and mixing service.

II. Bitcoin and its security issue

In this section, we will shortly discuss the bitcoin and the security issues involved in it.

A. Bitcoin

Bitcoin is a digital form of money. People can use bitcoin through online wallets. Wallet is an online platform which gives a user interface to send, receive and keep track of his bitcoin. In order to use bitcoin, one must have a wallet. Examples of the wallet include Coinbase, Trezor, SoFi, and so on. By registering in a wallet, a user gets a public address which acts as similar to a bank account number. This public address is used for every transaction, and each user gets a private key which is more like the pin/password of a traditional banking system.

In bitcoin, when a user sends bitcoin to another user, it has three major steps which are signing, broadcasting, and confirmation. When a user taps the send button in the bitcoin wallet, the bitcoin wallet generates a transaction message which includes sender public address, recipient public address, and the amount being sent. After generating this message, the wallet generates a digital signature by mathematically mixing it with the sender's private key. Every time a user tries to send some bitcoins, the wallet generates a unique signature with the private key of the sender. This makes the system much more secure. After creating a unique signature, a wallet then broadcasts the transaction file. In blockchain networks, every node connected to the network gets a copy of that transaction and verifies whether the transaction is legit. A node verifies a transaction by checking if the user actually has that bitcoin and if his digital signature is correct. When the node verifies the transaction as legitimate, then the transaction takes place in a virtual pool called mem pool. This is the second step of the bitcoin transaction. The final step is the confirmation. There are people who use their computer to add the transaction of the mem pool to the blockchain as a block, and those computer/nodes are called miners. When a transaction is added to a block it gets a confirmation, and the more blocks get added on top of that block the more confirmation it gets.

B. Security of Cryptocurrency Transactions

Bitcoin transactions are generally safe. However, if a hacker can have access to the private key of a user, then the hacker can transfer money from the user's account to his/her own account, and there is no way of knowing the hacker's identity. In 2013, an online wallet inputs.io was hacked twice and about 4100 bitcoins, worth about $1.2 million at that time, were stolen [10]. There are many scams that are done through bitcoin. Since the blockchain provides an extensive anonymity, it helps the scammers to get away easily. Hackers can perform double spending a bitcoin by using the confirmation method of the bitcoin transaction process, where the double-spending is a potential flaw in a digital cash scheme in which the same digital token can be spent more than once. Unlike physical cash, a digital token consists of a digital file that can be duplicated or falsified. The scammers mostly exploit the lack of knowledge of users about the blockchain to double spend it, and sometimes scammers pre-mined their transactions, and reverse the original transaction like that never happened.

III. Proposed Tracing Technique

In this section, the principle of the proposed technique will be presented. Thereafter, the proposed technique will be discussed with an example.

A. Principle of the proposed tracing technique

The proposed technique of revealing the real identity of a bitcoin user is stated below:

1) There will be a global platform where any victim around the world can submit a request for tracing the person behind a ransom demand giving the virtual identity such as the public address of the attacker who he had to send the ransom to. If cryptocurrency gets stolen, the public address of the account from where the money was stolen can be submitted along with the complaint to the global platform.
2) Blockchain network is a peer-to-peer network. In the blockchain every connected node has all the data of the blockchain. Blockchain stores all its transaction details to every node of its network which makes the blockchain data hard to modify but easy to monitor. As every node has all the transaction details of the network it is possible to track all the transactions in a blockchain network. There are some platforms such as Blockhain.Com, Chain Analysis, OXT, which continuously track every running transaction of every cryptocurrencies. The real-time

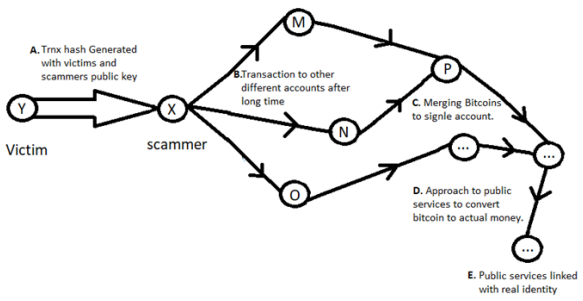

Fig. 2. Process of linking scammers address to real identity.

tracking is shown in Fig. 1, where the black circles represent a bitcoin public address or a wallet, and an edge represents a transaction between two accounts/wallets. The edge thickness indicates the amount of bitcoin sent in one transaction. The thicker the edge, the more bitcoin is sent in that particular transaction. Instead of tracking all running transactions, the proposed platform tracks those of the requested addresses only. Only tracking those wallet's transactions is much more feasible than tracking all the transactions in the blockchain. Moreover, tracking continuously those wallets can lead us to a group of scammers.

3) Since the cryptocurrencies do not have any physical existence, the scammer has to exchange the cryptocurrencies with the conventional currency to use the cryptocurrencies in real life. To this end, they need to use any public or common services or account. For example, if there is a web platform which provides services of exchanging traditional currency with the cryptocurrencies, it has to have a third-party tracker. The money exchange shop or bank can know the real identity of the sender. However it is not possible for the shops to know whether the bitcoin is illegal. They know the real identity of the bitcoin sender. On the other hand, our platform knows whether the transaction is linked with scamming or ransom. Combining these two factors, we can backtrack the transaction, and it can lead us to the real scammers. As our platform continuously tracks these scammers' transactions, as soon as a scammer uses any public services, our platform contacts those services to get the real identity of the scammer. If we keep tracking them similar to the tracking site mentioned in step 2, it will be possible to unearth the real identity of the scammer.

B. Illustrative Example

Let's assume that X is a scammer who has scammed Y (see Fig. 2). After scamming Y, he demands money to his bitcoin account as ransom from Y. Once Y pays the ransom, X does not do any transaction from that account. After a long time, the scammer gives the ransom money to other illegal users such as M, N, O. Then, M and N perform a transfer of that currency to someone else, say P. In this way, such

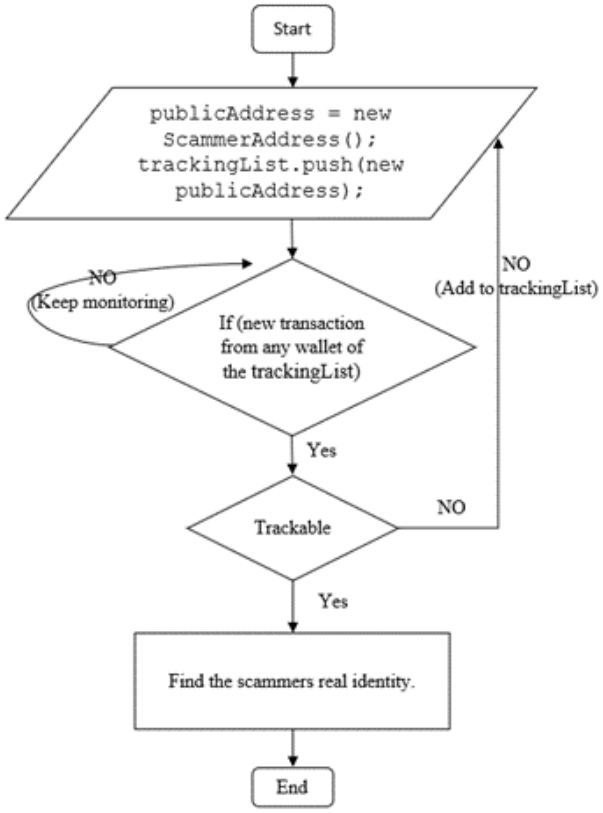

Fig. 3. Flow chart of the proposed technique.

transaction will continue. However, eventually, someone will exchange the cryptocurrency with the traditional currency in a money exchange shop or a bank. The proposed platform will keep tracking the nodes/wallets that are added in the tracking list. It will keep tracking those accounts until those accounts can be linked with any real-world service provider or any public service provider which has a third-party tracker to track those accounts. Then, with the help of the real-world server provider/account, a scammer's real identity can be tracked.

The step-by-step procedure of the proposed technique is illustrated in Fig. 3. First, the platform collects scammers' public addresses from the victims when the victims lodge any complaint. The platform will have a list where all scammers' wallet public addresses will be stored, and the proposed platform will read every new transaction that is happening in the blockchain network as a node of the network. When any transaction occurs from the scammers addresses, the system will add the new address as a new address of the scammer, and start tracking that account also. Our system stores this address and continuously tracks those wallets until a trackable position is achieved. Here a wallet is trackable if the system gets the IP address of the users or scammers use any public services with a third-party tracker. The platform will have a list of all the public services that track the users identity before giving them services. There might exist a scenario where the scammers take help from another third party whose address is

TABLE I
PERFORMANCE COMPARISON

Work	Trackable without IP address	Trackable in the presence of the mixing services	Trackable without third party app
[1]	×	✓	×
[9]	×	×	✓
Proposed	✓	✓	✓

not trackable. Suppose that a scammer "A" sends bitcoin to a person "B" from an account which buys and sells bitcoin, and that account does not use any real time services. In addition, the scammer uses proper IP spoofing tools . Now the scammers have the money in his/her hand. In this case, the platform is unable to track "A" down. However, it stores the address of the person "B", and will keep monitoring that address. Suppose that person "B" makes a transaction with "C" which eventually makes the bitcoin to real word currency conversion or uses the bitcoin for betting, or any take any services. Then the backtracking process can lead us to person "B". Finally, from "B" to the scammer as the scammer will not send bitcoin to an unknown person and even if he/she doesn't know the person the platform will keep tracking until it finds a proper link to the scammers.

C. System Benefits

The benefits of the proposed platform can be analyzed from two different perspectives: (i) benefits with respect to other techniques, and (ii) impact of the platform on society. We will evaluate the performance of the proposed technique with respect to three important features: the requirement of the IP address of the scammer, effectiveness in the presence of mixing services, and whether any third party app is required. As benchmarks, we consider the tracing system proposed in [1] and [9]. A summary of the comparison is shown in Table I. While the techniques proposed in [1] and [9] require the IP address of the scammer to trace him, the information about the IP address is not mandatory in our technique. In the proposed platform, the technique will keep tracking all transactions from the scammers, and the continuous tracking can lead to a point where the system will find a bitcoin wallet that is linked to both real life identity and to the scammers. Following that link, scammers identity will be traceable. Unlike [1], the proposed technique can effectively trace a scammer even if the mixing service is used for anonymization. In the mixing service, multiple addresses are mixed while sending cryptocurrencies to other addresses which makes it difficult to be confirmed which address is sending bitcoin to which address. However, the proposed technique tracks all of those addresses. Finally, it does not require any third party app in tracing the real identity of the person involved in a transaction. As the proposed technique will keep tracking a list of potential scammers and scammers will not directly do any transaction with the platform, the platform do not require any third party tracker. However, after finding that a bitcoin user in the tracking list used a public service with third party tracker in it, we can take help from that public service to uncover that users real identity.

The proposed system keeps track of scammers accounts. Different kinds of reports can be generated from the tracking, such as the regions where the most victims live, how most of the people are being scammed and so on. This type of reports can help the law enforcement authority of that region to track down the scammers, and the most used scammed process can be made public through the publications to create awareness among common people who are likely to be the next victims. Tracking those accounts for a long time, it is possible to find the organizational links of the scammers as they usually work in a group. The platform will continuously evolve through the data it receives, and over time it will be able to link almost every connection in the blockchain as it is not possible to clear any data from the public ledger.

IV. CONCLUSIONS

In this paper, we proposed a framework for tracing the real identity of cyber scammers who use cryptocurrencies for receiving ransom or doing any illicit transaction. The system takes complaints from a victim who gives the IP data or account information of the scammer. Then, it starts tracking the address or an account until it can map the IP data or account with some real identity. The success rate in unearthing the real identity of a scammer will be very high as the scammers or illegal activists must have to convert their bitcoin to traditional currency to be benefited from the cryptocurrency. This framework is for tracing the identity of the person who is behind an illegal transaction using cryptocurrency. More issues should be considered in implementing the system. We are leaving the implementation issue as a future work.

REFERENCES

[1] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, "Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction," *Journal of Economic Literature*, vol. 55, no. 2, pp. 647-649, 2017.

[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. https://bitcoin.org/en/bitcoin-paper. (Accessed: February 23, 2021)

[3] N. Christin, "Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace," In *Proc. International Conference on World Wide Web*, 2013, pp. 213–224.

[4] M. C. V. Hout and T. Bingham, "Silk Road, the virtual drug marketplace: A single case study of user experiences," *International Journal of Drug Policy*, vol. 24, no. 5, pp. 385–391, 2013.

[5] J. Martin, "Drugs on the Dark net: How Cryptomarkets are Transforming the Global Trade in Illicit Drugs," *The British Journal of Criminology*, vol. 55, no. 4, pp. 835-836, 2015.

[6] J. Martin, "Lost on the Silk Road: Online drug distribution and the cryptomarket," *Criminology and Criminal Justice*, vol. 14, no. 3, pp. 351–367, 2014.

[7] H. H. S. Yin, K. Langenheldt, M. Harlev, R. R. Mukkamala, and R. Vatrapu, "Regulating Cryptocurrencies: A Supervised Machine Learning Approach to De-Anonymizing the Bitcoin Blockchain," *Journal of Management Information Systems*, vol. 36, no. 1, pp. 37-73, 2019.

[8] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun, "Evaluating user privacy in Bitcoin," in *Proc. International Conference on Financial Cryptography and Data Security*, 2013, pp. 34-51.

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

[10] P. DeVries, "An Analysis of Cryptocurrency, Bitcoin, and the Future", *International Journal of Business Management and Commerce*, vol. 1, pp. 1-9, 2016.