Conference Paper

Anonymization Technologies of Cryptocurrency Transactions as Money Laundering Instrument

Goriacheva A., Jakubenko N., Pogodina O., Silnov D.

National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Kashirskoe shosse 31, Moscow, 115409, Russia

Abstract

This article is devoted to the exploration of services of anonymizing transactions, based on the Mixer, CoinJoin and CoinSuffle technologies, as well as to the description of the core principles of operation of these technologies and technical details. It analyzes the advantages and disadvantages of different realizations of this service. It formulates the problem of cryptocurrency laundering through anonymization services and offers solutions to this problem.

Keywords: cryptocurrency, blockchain, bitcoin, mixing service, mining, money laundering.

Corresponding Author:
Goriacheva A.
goriacheva.antonina@gmail.com

Received: 11 December 2017
Accepted: 20 January 2018
Published: 13 February 2018

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the FinTech and RegTech: Possibilities, Threats and Risks of Financial Technologies Conference Committee.

1. Introduction

After the global economic crisis of 2008, Satoshi Nakamoto (perhaps this pseudonym hides a group of people) has developed a cryptocurrency (bitcoin) protocol and released software to work with it.

Cryptocurrency was invented as an act of disobedience, as an instrument of fighting against the injustice and corruption of the traditional financial system. Due to the fact that after the crisis people lost confidence in financial institutions, more and more often cryptocurrency was used as a substitute for traditional money.

All operations with cryptocurrencies are based on a blockchain technology. Blockchain is a public database with information about all transactions with cryptocurrency. The main principle of the operation of blockchain is transparency of performed transactions with no ability to change them [1]. Blockchain allows you to disclose corruption schemes associated with illegal financial flows. This is possible due to the basic principle of its work: all transactions and every person who commits them are

recorded in a single database, access to which is available to each party of the process [2]. This gives the possibility to track criminals and disclose them on time.

2. Formulation of the problem

In order to hide the origin of money, criminals use anonymization services and technologies such as the Tor network (darknet), Dark Wallet (darknet), Bitcoin Laundry (Mixer), CoinJoin, CoinShuffle [3].

The general principle of any instrument of anonymizing cryptocurrency transactions is as follows: at one of the stages of money transfer there is a collective transaction, which excludes the opportunity to fix one-to-one correspondence between coins and their senders.

Thus, using anonymization technologies, criminals can launder money without fear of their identity disclosure, which creates a serious problem for the competent authorities. In order to find a solution, it is necessary to find out operating principles of such services and to identify their vulnerabilities.

3. Analysis of anonymization technologies

3.1. Mixing service

In accordance with the FATF terminology, Mixer (laundry service) is a type of an anonymizer that obscures the chain of transactions on the blockchain by linking all transactions in the same bitcoin address and sending them together in a way that makes them look as if they were sent from another address. A Mixer sends transactions through a complex, semi-random series of dummy transactions that makes it extremely difficult to link specific virtual coins (addresses) with a particular transaction. Mixer services operate by receiving instructions from a user to send funds to a particular bitcoin address. The mixing service then "commingles" this transaction with other user transactions, so that it becomes unclear to whom the user intended the funds to be directed [3]. Examples of mixing services are Bitmix; SharedCoin; Bitcoin Laundery; Bitlaunder; Easycoin [1].

3.2. Bitmix

The most popular mixing service is Bitmix. This service charges an occasional commission from 0.8 to 3%, which the user can set by himself/herself during the exchange process. All incoming bitcoins are assigned for a unique label, and the user will never receive their own bitcoins back [4, 5]. Bitmix allows performing a mixing operation by using the public Internet, but mixing without anonymous data transfer significantly increases the risk of disclosure of the user.

3.3. Mixer.Money

The key feature of this Mixer is the combination of the classical principle of mixing service work and engagement of world exchanges. So, after a classic Mixer, the coins are sent to one of the largest exchanges (Kraken, Poloniex, BTCChina), where they are replaced by coins of other traders [6]. As a result, on two addresses, at different times and in different proportions, the user receives clean coins from one of the foreign exchanges. Thus, it is extremely difficult to track the movement of the cryptocurrency by Taint analysis [7] and comparison of volumes over the period.

The service provides three modes of operation: a classical Mixer (commission is less than 1% + 0.001 btc, cleaning time: 10 minutes to 1 hour; the allowable amount is from 0.015 btc to 50 btc for one cleaning); Mixer + exchange (commission less than 3% + 0.0015 btc, cleaning time: 1 to 3 hours, allowable amount: from 0.015 btc to 50 btc per cleaning), complete anonymity (commission less than 5% + 0.0015 btc, cleaning time: 2 to 5 hours).

3.4. CoinJoin

In addition to the Mixer technology, there is the CoinJoin technology that was invented by security expert Gregory Maxwell. Blockchain.info opened the Sharedcoin service, which was based on this technology. Users, who are going to use CoinJoin, synchronize their actions, create a common transaction with a lot of inputs and outputs, and sign the result. The external observer cannot fix the correspondence between the participants of any transaction and inputs/outputs of their funds. The funds merge into one heap from various sources, and are then sent to other addresses [8]. The scheme of the process is shown in Fig.1

3.5. CoinShuffle

By modifying the technology CoinJoin, researchers from the University of Saarland in Germany proposed a new mixing principle called CoinShuffle, which eliminated the main disadvantage of CoinJoin - deanonymization of users of group transactions to each other. Users agree to conduct a transaction using cryptographic methods of information protection. The process is divided into three stages:

1. All users announce their addresses, from which they want to make their translations. The output addresses and the sum of the transaction are not announced. Users generate a pair of one-time keys (public and secrete). Participants know each other's public keys, but not secret keys. In addition, every member has their ordinal number in chain.

2. The second stage is based on a cryptographic secret sharing protocol.

   Symbols: R-Rick, M-Morty, J-Jessica, SK_R, SK, SK_J- R, M and J are secret keys respectively, PK_R, PK, PK_J - P, M and J are public keys respectively. The scheme is shown in Fig.1

   R: Encrypts the output address and the sum of the transaction using PK_J, and then encrypts this result using PK. Sends the result to Morty.

   M: Decrypts this message by using SK and receives the part of Rick's message, which it cannot decrypt, because it is encrypted with a key J. Encrypts its (Morty's) part of the transaction using PK_J, and then mixes both parts (Rick's and Morty's). Sends J both transactions, its and Rick's, encrypted with the key of Jessica.

   J: Decrypts, adds its own part, once again mixes up these three elements and finally forms a transaction, which offers for signature to each party.

3. If the final transaction satisfies all users, then everyone signs it with their secret key and one member puts the final transaction in Blockchain for confirmation [8, 9].

CoinShuffle has the following disadvantage: the participant cannot be sure that the others are not in collusion or are not the same person, so its output address in this case can be calculated [8].

The considered tools cannot provide an ideal anonymization. So, while the mixing operation is not successfully completed by the Mixer, the money does not belong to the owner. Anonymization of funds is carried out by a Mixer on remote servers, which

are controlled by specific individuals. So, there are risks that the attacker bears because of the possibility of disclosing their identity by the owner of the server.

In addition, the source code is not available to the users of Mixer, CoinJoin and CoinShuffle. The server part is under the control of only the owners. Users cannot control the operation of the algorithms of the server platform. So, arbitrary code, aimed at deanonimization of user-made operations, can be executed.

4. Solutions to the problem

4.1. The solution to the problem, based on the use of the vulnerabilities of the Mixer technology

No anonymization service can guarantee the absence of logs. The only way to make sure of their absence is to get full access to the servers and databases of the Mixer, which is impossible for an ordinary user, but it is possible for competent authorities.

In this way, the owner of the service cannot guarantee that, at the request of the law enforcement agencies, he/she will not provide the logs (i.e. the identity of the attacker will be disclosed).

4.2. Solution to the problem based on the blocking transparency

Deanonymization of the user is possible by mapping all transactions that meet certain parameters and are stored in the blockchain [2]. So knowing the number of coins sent by the attacker, we can find out the data we need and reduce the amount of suspects. The scheme of the process is shown in Fig. 3

4.3. Solving the problem by analyzing the actions of criminals who perform mixing operations on the public Internet.

With the help of the information collected by advertising trackers about the user and his/her purchases, it is possible to identify both the person and the entire cluster of his/her addresses and transactions on the blockchain [10].

Each website stores cookies for each user or shares information about customers with advertising companies, which can contain information about the purchases,

prices, e-mail addresses and delivery. An attacker or government agency can aggregate the data from several advertising agencies, which will allow to create user profiles and linking suspicious addresses to real personalities.

5. Conclusion

Nowadays anonymizing services allow you to launder the cryptocurrency. This means that virtual currencies in the hands of criminals, persons involved in the financing of terrorism and other criminal elements trying to avoid sanctions, become a new powerful tool for moving and storing money in such a way that they cannot be reached by law enforcement and other competent authorities. However, even the most reliable anonymization services for transactions have certain drawbacks, so it is possible to figure out the identity of violators and bring them to justice.

6. Application

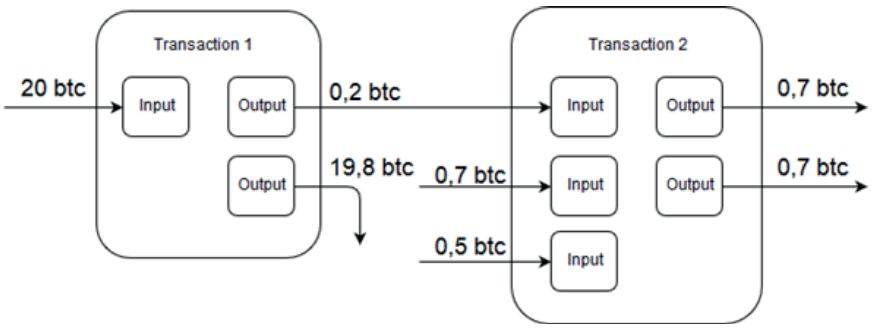

Figure 1: SharedCoin.

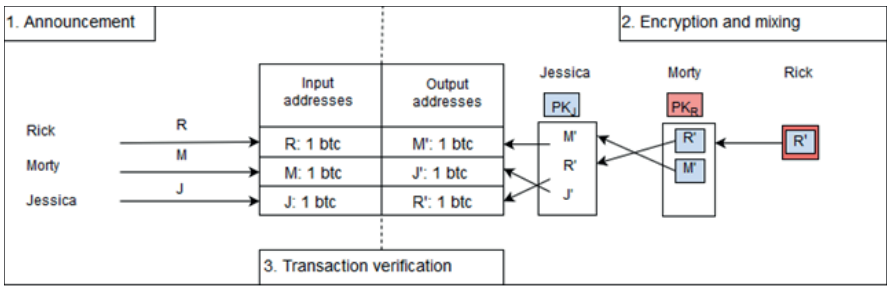

Figure 2: The second stage of CoinShuffle technology.

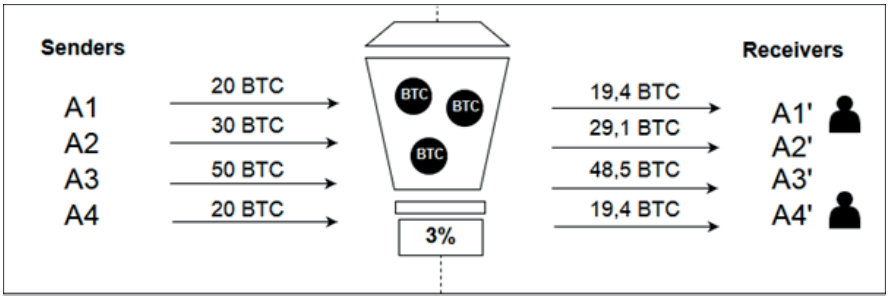

Figure 3: Solving the problem of money laundering through transaction mapping.

Acknowledgements

This work was supported by Competitiveness Growth Program of the Federal Autonomous Educational Institution of Higher Education National Research Nuclear University MEPhI (Moscow Engineering Physics Institute).

References

[1] Diana Sat, Grigory Krylov, Kirill Bezverbnyi, Alexander Kasatkin, Ivan Kornev. Investigation of money laundering methods through cryptocurrency. January 2016. Available at: http://www.jatit.org/volumes/Vol83No2/11Vol83No2.pdf

[2] Blockchain.info: blockchain. Available at: https://blockchain.info/

[3] FATF Report: Virtual currencies, key definitions and potential AML/CFT risks. June 2014

[4] Bits.media: Information web site about cryptocurrency Bitcoin. Available at: https://bits.media/news/o-mikserakh-starykh-i-novykh/

[5] BitMix: Bitcoin Mixing Service. Available at: https://bitmix.biz

[6] Mixer.Money: Bitcoin Mixing Service. Available at: https://mixer.money

[7] Laurence Tennant. Improving the Anonymity of the IOTA Cryptocurrency. October 2017. Available at: http://iotafeed.com/wp-content/uploads/2017/08/anonymity-iota.pdf

[8] Concide.ru: Information web site about cryptocurrency Bitcoin. Available at: https://www.coinside.ru/2014/10/13/coinjoin-i-coinshuffle-borba-s-psevdonimnostyu/

[9] CrypSys: CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin Tim Ruffing, Pedro Moreno-Sanchez, and Aniket Kate. Available at: http://crypsys.mmci.uni-saarland.de/projects/CoinShuffle/

[10] S. Goldfeder, H. Kalodner, D. Reisman, and A. Narayanan. When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies. Available at: https://arxiv.org/pdf/1708.04748.pdf