Bitcoin Users Deanonimization Methods

S.M. Avdoshin <savdoshin@hse.ru>
A.V. Lazarenko <avlazarenko @edu.hse.ru>
School of Software Engineering,
National Research University Higher School of Economics,
20, Myasnitskaya st., Moscow, 101000 Russia

Abstract. Bitcoin is the most popular cryptocurrency on the planet. It relies on strong cryptography and peer-to-peer network. Bitcoin is gaining more and more popularity in criminal society. That is why Bitcoin is often used as money laundering tool or payment method for illegal products and services. In this paper we explore various methods for Bitcoin users deanonimization, which is an important task in anti-money laundering process and cybercrime investigation.

Keywords: bitcoin; cryptocurrency; deanonymization

DOI: 10.15514/ISPRAS-2017-30(1)-6

For citation: Avdoshin S.M., Lazarenko A.V. Bitcoon Users Deanonimization Methods. Trudy ISP RAN/Proc. ISP RAS, том 30, вып. 1, 2018 г., стр. 89-102. DOI: 10.15514/ISPRAS-2018-30(1)-6

1. Introduction

Cryptocurrencies and blockchain technology are gaining more and more popularity nowadays. Besides hype around technology, there are a lot of useful and practical properties around namely, they are

- Decentralization – peer-to-peer networks without central authority are used for maintaining blockchain systems
- Transparency – every transaction and public address are accessible for everyone in the network.
- Irreversibility – any transaction is irreversible so it is very hard to rewrite the history of transactions.

Cryptocurrencies and blockchain technology are a perfect tool for mitigating the need of a middleman for transaction processing. Blockchain systems are leveraging the necessity of central authority. Transactions transparency helps to prevent theft and fraud, thus, it becomes crucially important for government and voting systems.

Bitcoin currently is the most widespread cryptocurrency on the planet. Bitcoin is a decentralized electronic payment system, which was introduced by a man or a group of people using an alias of Satoshi Nakamoto [1]. Bitcoin is based on peer-to-peer network and probabilistic distributed consensus protocol. Electronic coin is defined as a chain of digital signatures. If Alice wants to send bitcoins to Bob, then she should digitally sign a hash of the previous transaction and the public key of the next owner and add this information to the end of the coin.

The source and destination addresses in bitcoin are defined as hashes of public keys. Hashes are providing users with a certain degree of anonymity. All the transactions in bitcoin are public, so the bitcoin is pseudo-anonymous system.

Transactions in Bitcoin are processed to verify their integrity, authenticity and correctness by a group of so-called Miners (bitcoin nodes used for transaction verification and creation of new blocks). Transactions are grouped into the block and then processed by the Miners. Miner advertises a block to the rest of the network by appending it to the end of the blockchain. If the block is successfully verified by other Miners, the block is added to the end of the blockchain, and miner that proposed the block is earning a reward (fixed price for new block mining and corresponding transaction fees).

There are five [2] major components in bitcoin system:

- Users that create new wallets, transfer payments and save bitcoins on exchanges; typically they use one of the publicly available bitcoin clients;
- Miners that mine bitcoin blocks and process transactions; miners invest money into hardware that mine bitcoins and install specific software for that purpose;
- Testers, developers and entrepreneurs are improving bitcoin system and proposing new features; they are forming a specific technical community around bitcoin ecosystem;
- Bitcoin exchanges are the places where fiat money can be exchanged for bitcoins; typical examples are Poloniex [3], Bitstamp [4], Localbitcoins [5];
- Wallets store users' coins and provide features for making payments via internet connection.

Any user can create a fresh new Bitcoin wallet with a single click of the mouse without revealing any personal information like email, phone number or name. That is why Bitcoin is a perfect payment method for illegal activities. While being pseudo anonymous, Bitcoin helps to preserve the anonymity of the criminal in an easy way.

There were a lot of cases, where Bitcoin was used as a payment method, money laundering tool or a specific target for hackers:

- Silk Road was the most widespread darkmarket collapsed by the FBI; the Silk Road showed the society that Bitcoin could be used for criminal transactions as well as legitimate transactions [6];
- WannaCry is a ransomware cryptoworm, which targeted computers running Microsoft operating system demanding ransom payments in Bitcoins [7];

- BTC-e cryptocurrency exchange managed by Russian citizens; the exchange was shut down by USA for money laundering [8];
- Numerous ICO hacking cases; for example, hackers stole 7 million dollars from CoinDash ICO [9].

In order to fight with Bitcoin related crimes, different governments are enhancing law enforcement and make special training on cryptocurrency.

The following paper is an overview of existing methods. We propose novel classification for deanonimization methods.

2. Threat Model

The main goal of the attacker is to tie real names or IP addresses to transactions and bitcoin addresses. Instead of real name an attacker could tie email, phone number, username or any other digital identifier to the transaction.

An attacker is able to access all public information on the Internet: private and public forums, websites and social networks. Thus, an attacker could reveal real name of the particular person by parsing all the available information. Another approach is to “overhear” imprecise transaction information from users [10]. For example, an attacker may overhear “Alice, its Bob. I will send you 45$ bitcoins tomorrow morning”.

Besides public information, an attacker can inject malicious bitcoin nodes into the network in order to eavesdrop IP addresses and try to link certain transactions to the client IP addresses. If the attacker will use both attack vectors together, he will be able to increase the deanonimization accuracy. Almost every deanonimization method consists of two phases: data collection phase and data analysis phase. Data collection could be online: using malicious bitcoin nodes to eavesdrop on traffic and address propagation mechanism. Data collection could be offline: for analyzing historical data parsed from blockchain an attacker doesn’t have the need to use any additional components besides bitcoin client.

3. Deanomization

The deanonimization process is the process of linking public bitcoin address to the digital identifier of the user or his IP address. The process itself is divided onto two layers: P2P network layer and transactions layer.

It is very important to define the owner of the bitcoin public address.

We will define the owner of the bitcoin address as holder of the corresponding private key. So, if the exchange or online website is used for transferring bitcoins, and user doesn’t have access to the private key, the exchange or website is the owner of the bitcoin address.

The ownership of bitcoin wallet is a complicated task. For example, if the exchange is holding the private key of a particular person then she is not able to control her bitcoins directly. Instead, the user is using external service which is managing the corresponding private key.

Deanonimization methods (see Fig. 1) could be divided into two categories they are passive and active ones.

Passive methods don’t interact directly with bitcoin peer-to-peer network. Passive methods only use data which is parsed from the blockchain or any other public information source. Passive methods often rely on comprehensive graph analysis techniques and various heuristics related to bitcoin protocol.

Active methods are using malicious bitcoin nodes and social engineering techniques. Malicious nodes are the nodes with modified software under control of the attacker. Such nodes are used for traffic interception or direct communication with other peers in the network. Social engineering attacks are suitable for deanonimization of partially unknown users in the transaction chain.

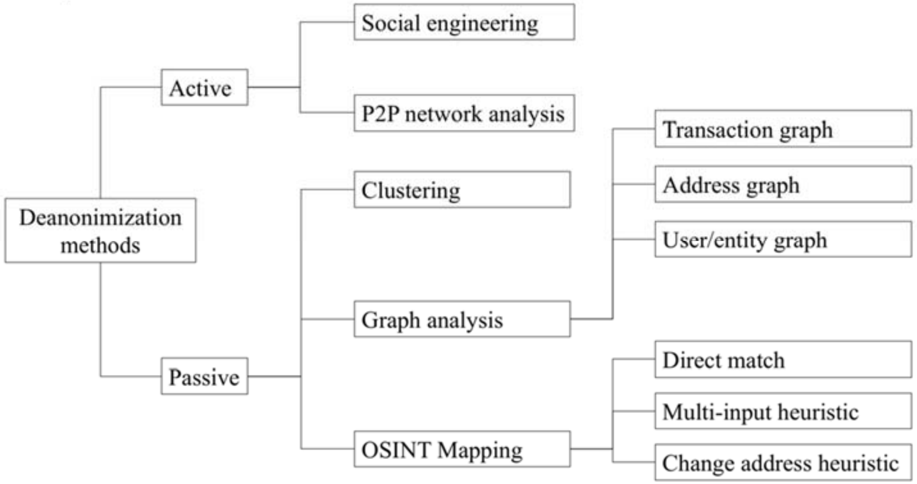

Fig. 1. Deanonimization methods classification

3.1 Open source intelligence on Bitcoin wallets

Without external information collected from various sources there is no way of finding the owner of the bitcoin wallet.

Information gathering stage can be classified into two different categories, namely, they are passive gathering and active gathering.

With active gathering an attacker is trying to find public address of the target by direct communication with it. Direct communication is an attempt to establish contact with target and find out the address during conversation or a request for payment [11]. This method is the most reliable, because a seller will not lie about his public address after the deal.

Another active approach uses malicious bitcoin nodes for traffic eavesdropping. This scenario will help to an attacker to collect IP addresses.

In passive gathering an attacker is trying to collect data from various data sources being in public access. There are various categories of data sources where an attacker can find digital names of bitcoin public address users: websites, forums, social networks, mining pools, wallets, bank exchanges, non-bank exchanges, vendors, gambling, laundry services. There are various information aggregators related to bitcoin wallets accessible online [12, 13].

The main goal of the information gathering stage is to collect as much tags for bitcoin wallets as possible because almost every deanonimization technique will be much more efficient in the wild with solid background on wallets participated in transactions.

3.2 Passive methods

3.2.1 Direct match

This is the easiest deanonimization method. An attacker is trying to find the owner of the bitcoin address by searching it in public sources. In case of success an attacker will find the corresponding digital identity.

3.2.2 Multi-input heuristic

Authors of the paper [14] proposed multi-input transaction heuristics. Multi-input transaction occurs when user wishes to perform a payment, and the payment amount exceeds the value of each of the available BTCs in user's wallet. Existing Bitcoin clients choose a set of BTCs from user's wallet and perform the payment through multi-input transactions. The straightforward conclusion is that if these BTCs are owned by different addresses, then the input addresses belong to the same user.

3.2.3 Change address heuristic

Change ("Shadow") addresses: bitcoin network generates a new address, so-called "shadow" address [1], at which each sender can collect back the "change". Using this heuristic, we can easily find the initial users wallet. Change addresses is the mechanism used to give money back to the input user in a transaction as bitcoins can be divided only by being spent.

All heuristic based methods heavily rely on direct match technique. Without properly collected data all the heuristics are useless for searching the real name of the person

3.2.4 Clustering

Authors of paper [11] proposed clustering techniques based on two previous heuristics. Using the first heuristic researchers were able to partition the network into 5,579,176 clusters of users (they started with 12 056 684 public keys). Authors used transaction graph and address graphs.

Authors of paper [11] enhanced second heuristics proposed by [14]. If an attacker can identify change addresses, she can therefore potentially cluster not only the input addresses for a transaction (according to Heuristic 1), but also the change address and the user himself. In addition, in custom usage of the Bitcoin protocol it is possible to specify the change address for a given transaction. Thus far, one common usage of

this setting that authors of [11] have observed has been to provide a change address that in fact is the same as the input address.

Overall the authors proposed a new clustering heuristic based on change address, allowing us to cluster addresses belonging to the same user. Using proposed technique researchers were able to identify major institutions (like exchanges and gambling websites) and interaction between them using only a small number of identified transactions.

3.2.5 Fingerprinting

In work [15] authors show that third-party web tracker can deanonimize users of cryptocurrencies. For example, when someone is paying on the shopping website, there is enough information to deanonimize a person in future. Since the online tracking is a very comprehensive and efficient tool in modern internet, the leakage of bitcoin payment data is a serious threat for today's users.

There are two options in fingerprinting process:

- Single transaction linkage. The purpose of the attack is to link a web user to a transaction on the cryptocurrency blockchain. If the tracker has access to the receiving address, it trivially enables linkage. Another case is when tracker knows approximate price and time of transaction. Attacker just search the logs of transactions.
- Cluster intersection. Complementary attack where the adversary aims to identify the cluster of addresses in the victims' Bitcoin wallets. The aim of the attack is to link two purchases of the same users to the blockchain. The further processing just uses known graph intersection attack methods.

3.2.6 Deanonimization with graph analysis

Bitcoin wallet owner's privacy is a very fragile thing. Once broken it is very hard to get it back. Public address is anonymous only when nobody knows the owner of the address. That is why it is highly recommended to use new bitcoin address for every new payment.

In combination with described passive methods graph analysis can help an attacker to reveal the real identity of the bitcoin wallet. For example, if we know intermediaries in the chain, we can use that information to manually find the real name using social networks or social engineering techniques.

Another example of graph analysis is community detection algorithms and centrality metrics. We can detect the community of friends or neighbors, find people in the middle of the chain who are implicated in illegal activity.

Authors of paper [16] used Page Rank on Directed Address graph. The main purpose of it was to determine the most interesting nodes. The technique is able to determine large Bitcoin gambling websites and marketplaces.

We are assured that sophisticated deanonimization techniques designed for social networks will also work on bitcoin transactions graph. That could increase the percentage of deanonimized users significantly.

Graphs that are described later are the main tool for passive bitcoin addresses deanonimization process.

3.2.7 Transaction graph

The whole blockchain can be viewed as acyclic transaction graph (see fig. 2) G = {T, E}, where T is a set of transactions stored in the blockchain, E – set of unidirectional edges between these transactions. G represents the flow of coins between transactions in the blockchain over time.

The set of input and output coins in a transaction can be viewed as weights on the edges of G. In particular, each incoming edge in a transaction carries a timestamp and the number of coins that forms an input for these transactions.

Transaction graph is the main graph in deanonimization attacks. Address graph and user/entity graph are constructed using transaction graph.

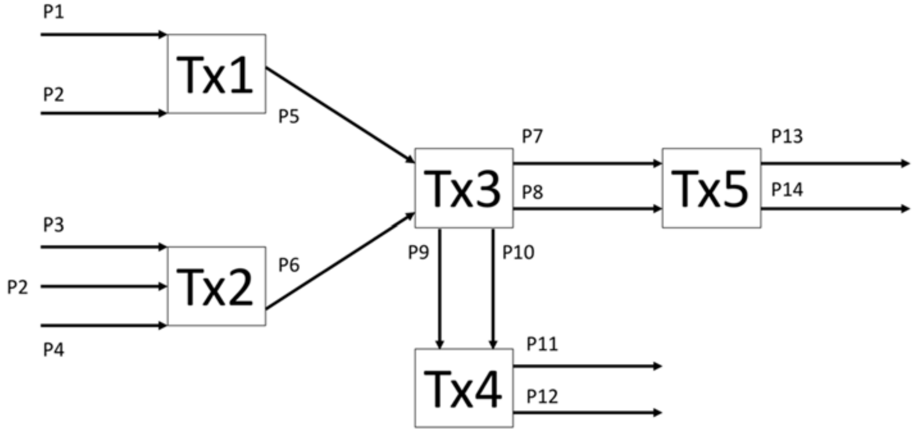

Fig. 2. Bitcoin transaction graph

3.2.8 Address graph

While traversing the transaction graph we can easily infer the relationship between various input and output addresses (public keys and these relations can be used for generation of address graph (see fig. 3), G = {P, E}, where P is a set of Bitcoin addresses and E are the edges connecting these addresses.

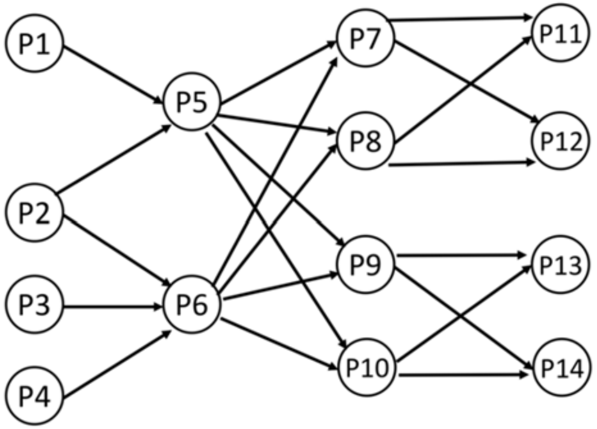

Fig. 3. Bitcoin addresses graph

3.2.9 User/entity graph

By using the address graph along with a number of heuristics, which are derived from Bitcoin protocol, the next step is to create an entity graph (see fig. 4) by grouping addresses that seem to belong to the same user.

3.3 Active methods

3.3.1 Social engineering

This method is quite exotic in case of bitcoin users deanonimization. However, it works perfectly in case of investigations. For example, if you only know the one-time pseudonym and associated bitcoin address, you can perform social engineering attacks.

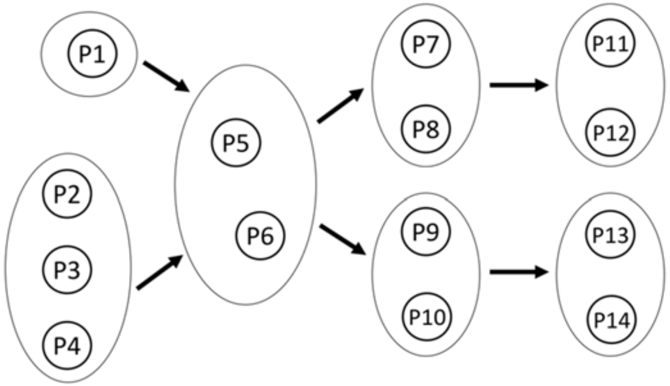

Fig. 4. Bitcoin user/entity graph

3.3.2 P2P network analysis

The Bitcoin P2P network contains two classes of nodes: servers and clients. Clients are nodes that do not accept in- coming TCP connections (e.g., nodes behind NAT), whereas servers do accept incoming connections. Clients and servers have different networking protocols and anonymity concerns. For instance, clients do not relay transactions. The focus of the deanonimization techniques is on servers.

All the attacks on P2P network are based on transaction broadcasting mechanism. An attacker should capture the IP address that initiated the transaction broadcast. If an attacker has resources, which are similar to the ISP, the IP-based deanonimization vector could be a powerful tool though.

Various researchers used gossip-based flooding protocols [17] to show that it is possible to deanonimize users using the linkage of users IP address with his pseudonym in the Bitcoin network.

In 2015 Bitcoin community responded to proposed attack by changing the network's flooding mechanism to a different protocol known as diffusion.

The attacks used "supernode" that is connected to active Bitcoin nodes and listens to the transaction traffic relayed by hones nodes. Using this technique, the linkage accuracy was up to 30% [17].

New version of protocol uses independent exponential delays. However, researchers in [17, 18] argue that it is unclear if such change actually protects against proposed attacks [17]. In diffusion spreading, each source or relay node transmits the message to each of its uninfected neighbors with an independent, exponential delay of rate λ.

The attacks in [17] use a supernode that is connected to most of the servers in the Bitcoin network. The supernode can make multiple connections to each honest server, with each connection coming from a different (IP address, port). Hence, the honest server does not realize that the supernode's connections are all from the same entity. The supernode can compromise arbitrarily many of a server's unused connections, up to the hard limit of 125 total connections.

The supernode in [17] also observes the timestamps at which messages are relayed from each honest server. Since the adversary maintains multiple active connections to each server, it receives the message multiple times from each server.

Supernodes are used for transaction and IP address matching via guessing the correct entry node set of a particular user. The supernode is trying to intercept clients IP propagation and correlate it with announced transaction. This attack comes for IP address spreading mechanism in Bitcoin. Such an attack achieves 86% IP matching probability on testnet (34% in average on the main net in 2013).

The paper [18] shows that new protocol is not effective against peer-to-peer traffic monitoring attacks.

4. Commetrcial Implementation

There exist various commercial and scientific tools closely related to this topic.

- BitIodine [19] – an open and modular blockchain analysis framework that allows to perform complex queries on transaction, group addresses together by controlling entity, and build clusters on top of blockchain data.
- BitConeView [20] is a graphical tool for the analysis of flows in the blockchain.
- Startups: Chainalysis, Blockchain Intelligence Group, Elliptic, Blockseer.

5. Future work

In future, we are going to try state-of-the-art social network deanonimization techniques on bitcoin transactions graph and adopt existing algorithms to fight with mixers. We will use graph based deanonimization techniques on other popular cryptocurrencies as well in order to prove that this technique is feasible with any cryptocurrency that is not especially designed for anonymous payment purposes.

Another open question is the possibility of achieving good accuracy on main net using P2P network level deanonimization techniques with significant amount of resources.

6. Conclusion

We have presented Bitcoin deanonimization techniques and provided classification of them.

Bitcoin privacy is an emergent field of research, which is gaining more and more attention from researchers all over the world. Being a popular payment tool along criminals, the society needs tools and suitable laws to fight with illegal usage of bitcoin.

References

[1]. S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System [Electronic resource]. Bitcoin [Official website]. URL: https://bitcoin.org/bitcoin.pdf (accessed: 22.10.2017).

[2]. M. Conti, E.S. Kumar, C. Lal, S. Ruj. A Survey on Security and Privacy Issues of Bitcoin [Electronic resource]. Cornell University Library [Official website]. URL: https://arxiv.org/abs/1706.00916 (accessed: 22.10.2017)

[3]. Poloniex – Bitcoin/Digital Asset Exchange [Electronic resource]. Poloniex [Official website]. URL: https://poloniex.com (accessed: 22.10.2017)

[4]. Bitstamp – buy and sell bitcoin [Electronic resource]. Bitstamp [Official website]. URL: https://www.bitstamp.net (accessed: 22.10.2017)

[5]. Localbitcoins [Electronic resource]. Localbitcoins [Official website]. URL: https://localbitcoins.com/ru/ (accessed: 22.10.2017)

[6]. M.Santori. Silk Road Goes Dark: Bitcoin Survives Its Biggest Market's Demise [Electronic resource]. Coindesk [Official website]. URL: https://www.coindesk.com/bitcoin-milestones-silk-road-goes-dark-bitcoin-survives-its-biggest-markets-demise/ (accessed: 22.10.2017)

[7]. WannaCry ransomware attack [Electronic resource]. Wikipedia [Official website]. URL: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack (accessed: 22.10.2017)

[8]. J.J.Roberts. Bitcoin Site Fined $110 Million for Money Laundering, Owner Arrested for Hacking [Electronic resource]. Fortune [Official website]. URL: http://fortune.com/2017/07/27/btc-e-digital-currency/ (accessed: 22.10.2017)

[9]. W.Zhao. $7 Million Lost in CoinDash ICO Hack [Electronic resource]. Coindesk [Official website]. URL: https://www.coindesk.com/7-million-ico-hack-results-coindash-refund-offer/ (accessed: 22.10.2017)

[10]. M.Fleder, M.S.Kester, S.Pillai. Bitcoin Transaction Graph Analysis [Electronic resource]. Cornell University Library [Official website]. URL: https://arxiv.org/pdf/1502.01657.pdf (accessed: 22.10.2017)

[11]. S.Meiklejohn, M.Pomarole, G.Jordan. A Fistful of Bitcoins: Characterizing Payments Among Men with no Names [Electronic resource]. UC San Diego [Official website]. URL: https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf (accessed: 22.10.2017).

[12]. Bitcoin Address Tags [Electronic resource]. Blockchaininfo [Official website]. URL: https://blockchain.info/ru/tags (accessed: 22.10.2017)

[13]. Bitcoin Address Checker [Electronic resource]. BitcoinWhosWho [Official website]. URL: http://bitcoinwhoswho.com (accessed: 22.10.2017)

[14]. E. Androukli, G.O. Karame Evaluating User Privacy in Bitcoin [Electronic resource]. Cryptology ePrint Archive [Official website]. URL: https://eprint.iacr.org/2012/596.pdf (accessed: 22.10.2017)

[15]. S.Goldfeder. When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies [Electronic resource]. Cornell University Library [Official website]. URL: https://arxiv.org/pdf/1708.04748.pdf (accessed: 22.10.2017)

[16]. M.Fleder, M.S. Kester, S. Pillai. Bitcoin Transaction Graph Analysis [Electronic reosurce]. Cornell University Library [Official website]. URL: https://arxiv.org/abs/1502.01657 (accessed: 22.10.2017)

[17]. A. Biryukov, D. Khovratovich. Deanonymisation of clients in Bitcoin P2P network [Electronic resource]. ACM DL [Official website]. URL: https://dl.acm.org/citation.cfm?id=2660379 (accessed: 22.10.2017)

[18]. G. Fanti, P.Viswanath. Anonymity Properties of the Bitcoin P2P Network [Electronic resource]. Cornell University Library [Official website]. URL: https://arxiv.org/abs/1703.08761 (accessed: 22.10.2017)

[19]. M. Spagnuolo, F. Maggi. BitIodine: Extracting Intelligence from the Bitcoin Network [Electronic resource]. FC & DS 2014 [Official website]. URL: http://fc14.ifca.ai/papers/fc14_submission_11.pdf (accessed: 22. 10. 2017)

[20]. BitConeView – first graphical tool for the analysis of flows in blockchain [Electronic resource]. BitConeView [Official website]. URL: http://www.bitconeview.info (accessed: 22.10.2017)

Методы деанонимизации пользователей биткоин

С.М. Авдошин <savdoshin@hse.ru>
А.В. Лазаренко <avlazarenko @edu.hse.ru>
Департамент программной инженерии,
Национальный исследовательский университет “Высшая школа экономики”,
101000, Россия, г. Москва, ул. Мясницкая, д. 20

Аннотация. Bitcoin является самой популярной криптовалютой на планете. В основе Bitcoin лежат криптография и пиринговая сеть. Будучи псевдоанонимной криптовалютой, Bitcoin очень часто используется преступным сообществом для отмывания денег или оплаты нелегальных товаров и услуг. В данной работе мы представляем ращличные методы для деанонимизации пользователей Bitcoin, что является чрезвычайно важной задачей при расследовании киберпреступлений и противодействию отмыванию денег.

Ключевые слова: биткоин; криптовалюты; деанонимизация.

DOI: 10.15514/ISPRAS-2018-30(1)-6

Для цитирования: Авдошин С.М., Лазаренко А.В. Методы деанонимизации пользовательелей биткоин. Труды ИСП РАН, том 30, вып. 1, 2018 г., стр. 89-102. DOI: 10.15514/ISPRAS-2018-30(1)-6

Список литературы

[1]. S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System [Electronic resource]. Bitcoin [Official website]. URL: https://bitcoin.org/bitcoin.pdf (дата обращения: 22.10.2017).

[2]. M. Conti, E.S. Kumar, C. Lal, S. Ruj. A Survey on Security and Privacy Issues of Bitcoin [Electronic resource]. Cornell University Library [Official website]. URL: https://arxiv.org/abs/1706.00916 (дата обращения: 22.10.2017)

[3]. Poloniex – Bitcoin/Digital Asset Exchange [Electronic resource]. Poloniex [Official website]. URL: https://poloniex.com (дата обращения: 22.10.2017)

[4]. Bitstamp – buy and sell bitcoin [Electronic resource]. Bitstamp [Official website]. URL: https://www.bitstamp.net (дата обращения: 22.10.2017)

[5]. Localbitcoins [Electronic resource]. Localbitcoins [Official website]. URL: https://localbitcoins.com/ru/ (дата обращения: 22.10.2017)

[6]. M.Santori. Silk Road Goes Dark: Bitcoin Survives Its Biggest Market’s Demise [Electronic resource]. Coindesk [Official website]. URL: https://www.coindesk.com/bitcoin-milestones-silk-road-goes-dark-bitcoin-survives-its-biggest-markets-demise/ (дата обращения: 22.10.2017)

[7]. WannaCry ransomware attack [Electronic resource]. Wikipedia [Official website]. URL: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack (дата обращения: 22.10.2017)

[8]. J.J.Roberts. Bitcoin Site Fined $110 Million for Money Laundering, Owner Arrested for Hacking [Electronic resource]. Fortune [Official website]. URL: http://fortune.com/2017/07/27/btc-e-digital-currency/ (дата обращения: 22.10.2017)

[9]. W.Zhao. $7 Million Lost in CoinDash ICO Hack [Electronic resource]. Coindesk [Official website]. URL: https://www.coindesk.com/7-million-ico-hack-results-coindash-refund-offer/ (дата обращения: 22.10.2017)

[10]. M.Fleder, M.S.Kester, S.Pillai. Bitcoin Transaction Graph Analysis [Electronic resource]. Cornell University Library [Official website]. URL: https://arxiv.org/pdf/1502.01657.pdf (дата обращения: 22.10.2017)

[11]. S.Meiklejohn, M.Pomarole, G.Jordan. A Fistful of Bitcoins: Characterizing Payments Among Men with no Names [Electronic resource]. UC San Diego [Official website]. URL: https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf (дата обращения: 22.10.2017).

[12]. Bitcoin Address Tags [Electronic resource]. Blockchaininfo [Official website]. URL: https://blockchain.info/ru/tags (дата обращения: 22.10.2017)

[13]. Bitcoin Address Checker [Electronic resource]. BitcoinWhosWho [Official website]. URL: http://bitcoinwhoswho.com (дата обращения: 22.10.2017)

[14]. E. Androukli, G.O. Karame Evaluating User Privacy in Bitcoin [Electronic resource]. Cryptology ePrint Archive [Official website]. URL: https://eprint.iacr.org/2012/596.pdf (дата обращения: 22.10.2017)

[15]. S.Goldfeder. When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies [Electronic resource]. Cornell University Library [Official website]. URL: https://arxiv.org/pdf/1708.04748.pdf (дата обращения: 22.10.2017)

[16]. M.Fleder, M.S. Kester, S. Pillai. Bitcoin Transaction Graph Analysis [Electronic reosurce]. Cornell University Library [Official website]. URL: https://arxiv.org/abs/1502.01657 (дата обращения: 22.10.2017)

[17]. A. Biryukov, D. Khovratovich. Deanonymisation of clients in Bitcoin P2P network [Electronic resource]. ACM DL [Official website]. URL: https://dl.acm.org/citation.cfm?id=2660379 (дата обращения: 22.10.2017)

[18]. G. Fanti, P.Viswanath. Anonymity Properties of the Bitcoin P2P Network [Electronic resource]. Cornell University Library [Official website]. URL: https://arxiv.org/abs/1703.08761 (дата обращения: 22.10.2017)

[19]. M. Spagnuolo, F. Maggi. BitIodine: Extracting Intelligence from the Bitcoin Network [Electronic resource]. FC & DS 2014 [Official website]. URL: http://fc14.ifca.ai/papers/fc14_submission_11.pdf (дата обращения: 22. 10. 2017)

[20]. BitConeView – first graphical tool for the analysis of flows in blockchain [Electronic resource]. BitConeView [Official website]. URL: http://www.bitconeview.info (дата обращения: 22.10.2017)