A Survey on Enhancing Anonymity of Bitcoin

Nikita Moolchandani[1], Goutam R[2]
[1, 2] Dept of ,Computer Science
[1, 2] Atria Institute of Technology, Bangalore, India.

Abstract- *Bitcoin is a decentralized digital currency, widely used for its perceived anonymity property, and has surged in popularity in recent years. Bitcoin publishes the complete transaction history in a public ledger, under pseudonyms of users. This is an alternative way to prevent double-spending attack instead of central authority. Therefore, if pseudonyms of users are attached to their identities in real world, the anonymity of Bitcoin will be a serious vulnerability. It is necessary to enhance anonymity of Bitcoin by a coin mixing service or other modifications in Bitcoin protocol [1]. Therefore in this paper, we are going to present the various techniques that have been proposed to enhance anonymity of Bitcoin. Also we are going to have a look at the various techniques that have been introduced to de-anonymize the users of Bitcoin.*

Keywords- Crypto-currency, Bitcoin, anonymity, deanonymity

I. INTRODUCTION

Bitcoin has been known about as a distributed cryptographic digital currency which has drawn much attention in the literature since introduced by Satoshi Nakamoto in 2008[2]. Bitcoin has become an outstanding digital currency owning a market capitalization of about 60 billion dollars nowadays. It is expected to reach more than 5 million users by 2019. The current Bitcoin exchange rate is above 4000 dollars from around 600 dollars in mid-2016.

In traditional electronic payment systems, there is a trusted centralized agent to keep the consensus of transactions. It may acts as a bank, a Chartered Accountant (CA), a notary, or any other trusted service. The use of such an authenticator increases the cost of transactions since a nominal fee is deducted as a payment by these third parties. For the purpose of removing high transaction fees and issue right of currency by a central trusted authority, Bitcoin works as a decentralized crypto-currency thanks to its peer to peer network structure. There is no possibility to change the amount of bitcoins or cause inflation by producing large amount of currency in this ecosystem. The issue and circulation of bitcoins are achieved through transactions in its peer to peer network. The generation of bitcoins depends on solving an arithmetical puzzle regarded as mining. Cryptographic primitives guarantee the security of every transaction in Bitcoin. Coins can only be spent by the owner with their private keys, and they can only be used in a single transaction with no chance of duplication. There is no supervision or management agents like banks in traditional currency systems in Bitcoin network [1].

Bitcoin is a decentralized currency that utilizes cryptography to validate itself. Bitcoin represents each user by his address from his public key. Someone possesses his bitcoins by knowing his private keys. Any time a user Alice wants to send her bitcoin c to another user Bob, she generates a signed transaction message, which states that Alice (denoted by her public key) transmitted c to Bob (denoted by his public key). After a transaction is created, it is propagated to the network and collected by verifiers, called miners. The job of miners is to verify all transactions in Bitcoin network. They collect a number of transactions that are broadcasted in the network over a period of time and put them together in a block. Specifically, each miner aggregates a group of transaction messages into a block and then completes a computational proof-of-work. The miner who is first to complete proof-of work appends their new block to the public ledger known as blockchain and reaps a reward of newly-minted bitcoins and transaction fees. This income serves as a reward for their efforts in block verification by spending computing resources. Initially this reward is set to 25 bitcoins. The amount is cut in half every 4 years. This procedure of cutting rewards in half will continue until the total bitcoins reaches 21 million. At that point, miners will only get transaction fees as reward for their verification efforts. The transaction message structure is shown as Figure 1[1].

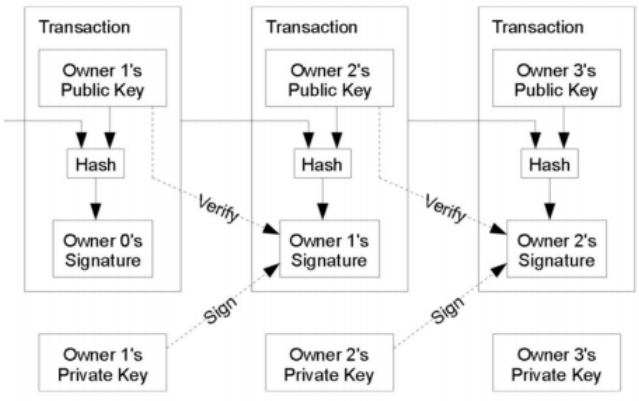

Figure 1. Simple structure of Bitcoin transactions [1]

Bitcoin is often considered as anonymous in the public eye, despite explicit statements to the contrary in the original Bitcoin paper[1]. The blockchain preserves history of every bitcoin from its generation. Anonymity of users in Bitcoin lies in pseudonyms because everyone could see all transaction records in blockchain. Many researchers have delved into deanonymizing users in the blockchain through various analysis method, such as literatures [3][4][5][6][7]. Once a user's address information is leaked, all his transaction records can be linked to reveal his true identity in real world. Many relevant researches about analysis of Bitcoin blockchain have been published in recent years.

Some papers develop techniques to deanonymize users[5][6][8], some papers cluster transactions[9][10], and others evaluate the protection offered by anonymizing services[11]. Such leakage represents a massive privacy violation, and would be deemed unacceptable in traditional banking systems.

II. DEANONYMIZING TECHNIQUES PROPOSED

A. Evaluating User Privacy in Bitcoin[3]

This is a technique wherein the privacy provisions in Bitcoin is investigated when it is used as a primary currency to support the daily transactions of individuals in a university setting. More specifically, the privacy that is provided by Bitcoin is evaluated (i) by analyzing the genuine Bitcoin system and (ii) through a simulator that faithfully mimics the use of Bitcoin within a university. In this setting, the results show that the profiles of almost 40% of the users can be, to a large extent, recovered even when users adopt privacy measures recommended by Bitcoin.[3]

B. *Bitcoin Transaction Graph Analysis[4] and Structure and Anonymity of the Bitcoin Transaction Graph[5]*

This is the second technique to deanomymize the users by analyzing the transaction graphs of Bitcoin. The approach is two-fold: (i) annotating the public transaction graph by linking bitcoin public keys to real people - either definitively or statistically. (ii) and run the annotated graph through the graph-analysis framework to find and summarize activity of both known and unknown users.

C. *An Analysis of Anonymity in the Bitcoin System [6]*

In this paper , the authors consider the topological structure of two networks derived from Bitcoin's public transaction history. They show that the two networks have a non-trivial topological structure, provide complementary views of the Bitcoin system and have implications for anonymity. They combine these structures with external information and techniques such as context discovery and flow analysis to investigate an alleged theft of Bitcoins, which, at the time of the theft, had a market value of approximately half a million U.S. dollars.

D. Quantitative Analysis of the Full Bitcoin Transaction Graph[7]

The authors of this paper downloaded the full history of this scheme, and analyzed many statistical properties of its associated transaction graph. They answer for the first time a variety of interesting questions about the typical behavior of users, how they acquire and how they spend their bitcoins, the balance of bitcoins they keep in their accounts, and how they move bitcoins between their various accounts in order to better protect their privacy. In addition, They isolated all the large transactions in the system, and discovered that almost all of them are closely related to a single large transaction that took place in November 2010, even though the associated users apparently tried to hide this fact with many strange looking long chains and fork-merge structures in the transaction graph.

III. ENHANCING ANONYMITY TECHNIQUES PROPOSED FOR BITCOIN

There are various different techniques proposed by various different authors in order to enhance the anonymity with bitcoins. Some of which we are going to have a look at:

A. *Mixcoin: Anonymity for bitcoin with accountable mixes [12]*

Coin mixing services help users confuse their transactions in order to prevent transaction records from being tracked. Malicious entities are not able to link confused addresses to their real owners after coin mixing. However, the mixing server could collect all the information before and after mixing these transactions. If the mixing server has interest to recover transaction paths, it can track all the mixing transaction records arbitrarily.[1]

Mixcoin is a mixing service with accountability[12]. Bitcoin customers negotiate a set of parameters with the server, including the addresses where the coins should be sent to. Mixcoin is compatible with Bitcoin and does not require any modifications in Bitcoin. As a central mixing service, it is easier to protect against DoS attacks by a single user compared to p2p mixing protocols. However, the mixer will know about the connection from all inputs to outputs. Therefore, it is able to keep information about input addresses

to output addresses locally and has ability to track the transaction history of a specific customer. There is a risk for the mixer to leak the privacy of customers and disrupt the anonymity of its customers in the future.[1]

B. *Blindcoin: Blinded, accountable mixes for bitcoin [13]*

Blindcoin improves on Mixcoin by using blind signatures to ensure that the mixer can't map the input addresses to output addresses[13]. Nevertheless, the amount that will be mixed is still fixed and the anonymity depends on its simultaneous customers. Also, its users must be able to anonymously publish the output addresses to a public log which might result into a bootstrapping problem.[1]

C. *Coinjoin: Bitcoin privacy for the real world [14]*

CoinJoin provides a distributed mixing service, which needs every user's signature on an union transaction[14]. It guarantees the anonymity of users and security of their possession at the same time. No one could transfer any coins without the user's authority by his signature. Its disadvantage is that there is no countermeasures to DoS attack in case of someone refuses to sign on the union transaction after he initializes a mixing service. Therefore, Coinjoin can't defend malicious internal entities. [1]

D. *Coinshuffle: Practical decentralized coin mixing for bitcoin [15]*

CoinShuffle provides anonymous mixing service through a peer to peer network[15]. Malicious entities will be excluded from mixing service through a penalty mechanism, and the union transaction will be confirmed eventually. An optional blame phase is introduced to defend against DoS attacks without any financial commitments required from users participating a mixing service.[1]

E. *Coinswap [16]*

CoinSwap is another proposal of Gregory Maxwell to perform a transaction with a trusted third party[16]. There is a lack of explicit collection method for coin mixing fees. It may not incentivize mix servers to offer coin mixing service.[1]

F. Zerocoin:

Anonymous distributed e-cash from Bitcoin[17] and Zerocash: Decentralized anonymous payments from Bitcoin[18]

Some other cryptocurrencies can be exchanged with Bitcoin providing another method to mix transactions in Bitcoin blockchain. A customer can exchange his bitcoins for other digital currencies and exchange them back for bitcoins after a certain period. Zerocoin[17] and Zerocash[18] are designed for this purpose. These cryptocurrencies provide strong anonymity of users, but they are not compatible with existing Bitcoin protocol.[1]

G. How to leak a secret [19]

In 2001, Rivest proposed a novel signature algorithm to reveal secret anonymously, called ring signature[19]. Ring signature works as a special group signature without a trusted center and the process of group building. The signer is completely anonymous for the verifier. Ring signature provides an ingenious way to reveal secrets anonymously. The unconditional anonymity of ring signature is very useful in some special environments where information can not be revealed with its signature. [1]

The general model of ring signature scheme is elaborated as follows:

Key generation(Gen): a polynomial time algorithm with an input parameter k, two outputs as public key pk and private key sk. Suppose that it generates a public key pki and a private key ski as a key pair for each signer Ci. The public and private keys of different users may come from different public key systems, such as RSA, DLP and ECSDA. [1]

Ring sign(Sign): a polynomial time algorithm. A signature s on a message m is generated after entering the message m, public keys of ring members pk1, pk2,⋯ , pkn and the private key ski of its owner. Some parameters in s are circular according to certain rules. [1]

Signature verify(Verify): A deterministic algorithm, after entering a signature s, a message m and the public keys of members in ring signature scheme, it will output true in case that the ring signature s is verified. Otherwise, it will output false. The ring signature sketch is shown in Figure 2.[1]

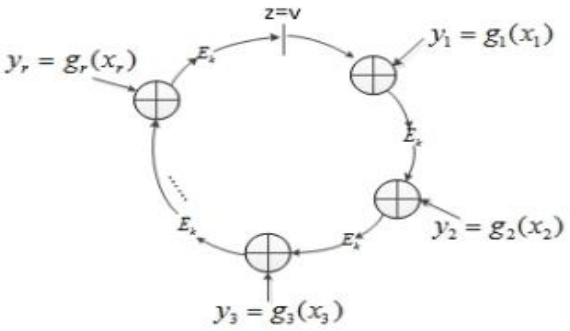

Figure 2. Ring signatures[1]

G.a) How ring signatures can be used to increase anonymity.

The mixing service will be detailed in the following subsection.

(1) In the requesting phase, a customer desiring to mix his bitcoins sends an initial request message to the mixing server. The request message comprises the public key of the customer pkc and the transactions he wants to mix. After receiving the request from a customer, the mixing server sends back a certain amount of public keys {pk1, pk2, ⋯ , pkn} collected from customers applying for mixing service, including pkc. The amount of public keys n should be adjusted in consideration of the server performance. [1]

(2) In the generation phase, the customer receives public keys of other customers and generates Bitcoin addresses {addr1, addr2, ⋯ , addrm} for getting back his own bitcoins after mixing. To obtain address addrm, a public key is hashed with SHA-256 algorithm first and RIPEMD-160 algorithm subsequently. After concatenating a check sum and a version number with the hash value, it is encoded through a special base58 to generate a valid address addrm.[1]

Then he signs all generated addresses through ring signature and sends them back to the mixing server one by one. Upon receiving response from the customer, the mixing server generates a mix transaction containing all the input transactions and output addresses, and sends it to corresponding customers respectively.[1]

(3) In the final confirmation phase, the customer will check if the mixing transaction contains all his input transactions and output addresses. If all the information included in the mixing transaction is corrected, the customer will sign the mixing transaction and broadcast it in the Bitcoin network as normal transactions. The protocol flow is shown in Figure 3. [1]

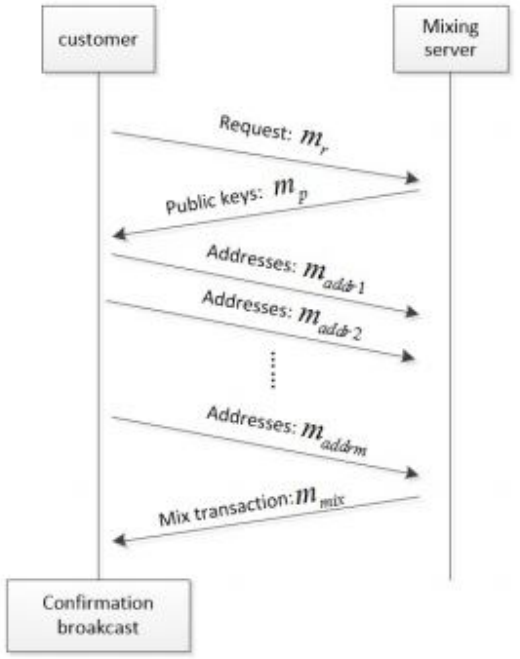

Figure 3. Protocol flow of mixing service[1]

An initial request message mr consists of customer's public key pkc and transactions going to be mixed. The response message from mixing server contains all the public keys of customers, who want to mix their own transactions. Each address message maddrn includes only one Bitcoin address and amount of bitcoin transfers to this address. A flag byte representing whether all addresses have been transferred is appended to address message maddrn. At last, the customer checks whether the mixing transaction mmix containing all the amount of bitcoins corresponding with his addresses is correct.[1]

IV. CONCLUSION

Bitcoin is a new successful approach to realize cryptocurrency but does not guarantee anonymity. Many researches have delved into how to deanonymize the Bitcoin through its blockchain. To enhance anonymity in Bitcoin, there have been several approaches to provide coin mixing services.

Therefore in this paper, we presented the various techniques that have been proposed to enhance anonymity of Bitcoin. Also we had a look at the various techniques that have been introduced to de-anonymize the users of Bitcoin.

Therefore, we had a successful review of the current scenario regarding how the anonymity of the users of Bitcoin is maintained.

REFERENCES

[1] Yi Liu, Ruilin Li, Xingtong Liu, Jian Wang, Chaojing Tang and Hongyan Kang, "Enhancing Anonymity of Bitcoin Based on Ring Signature Algorithm," 13th International Conference on Computational Intelligence and Security, 2017.

[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[3] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun, "Evaluating user privacy in bitcoin," in Financial Cryptography and Data Security: 17th International Conference, 2013.

[4] M. Fleder, M. S. Kester, and S. Pillai, "Bitcoin transaction graph analysis," Computer Science, 2015.

[5] M. Ober, S. Katzenbeisser, and K. Hamacher, "Structure and anonymity of the bitcoin transaction graph," Future Internet, 2013. 320

[6] F. Reid and M. Harrigan, "An analysis of anonymity in the bitcoin system," in Security and Privacy in Social Networks, 2011, pp. 197–223.

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

[8] 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 Proceedings of the 2013 conference on Internet measurement conference, Barcelona, Spain, 2013.

[9] M. Harrigan and C. Fretter, "The unreasonable effectiveness of address clustering," pp. 368–373, 2016.

[10] M. Spagnuolo, F. Maggi, and S. Zanero, "Bitiodine: Extracting intelligence from the bitcoin network," in Financial Cryptography and Data Security: 18th International Conference, Christ Church, Barbados, March 3-7, 2014.

[11] M. Moser and R. Bohme, "Anonymous alone? measuring bitcoin's second-generation anonymization techniques," in 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS PW), 2017, pp. 32–41.

[12] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, "Mixcoin: Anonymity for bitcoin with accountable mixes," in Financial Cryptography and Data Security: 18th International Conference, Christ Church, Barbados, 2014.

[13] L. Valenta and B. Rowan, "Blindcoin: Blinded, accountable mixes for bitcoin," in Financial Cryptography and Data Security: FC 2015 International Workshops, 2015.

[14] G. Maxwell, "Coinjoin: Bitcoin privacy for the real world," 2013.

[15] T. Ruffing, P. Moreno-Sanchez, and A. Kate, "Coinshuffle: Practical decentralized coin mixing for bitcoin," in Computer Security - ESORICS 2014: 19th European Symposium on Research in Computer Security, Wroclaw, Poland, 2014.

[16] "Coinswap," 2013. [Online]. Available: https://bitcointalk.org/index.php?topic=321228.

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

[18] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," ser. 2014 IEEE Symposium on Security and Privacy, 2014, pp. 459–474.

[19] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," ser. Advances in Cryptology ł ASIACRYPT 2001: 7th International Conference on the Theory and Application of Cryptology and Information Security Gold Coast, Australia, December 9-13, 2001.