Anonymity in Cryptocurrencies



Hulya Boydas Hazar

Abstract Cryptocurrencies are defined as anonymous digital currencies. It is widely assumed that the real-world identities of the persons who engage in cryptocurrency transactions are secret and will remain secret. Digital signatures serve as identities of the parties involved in cryptocurrency transactions. They are essentially composed of a pair of keys, the secret key and the public key, which are used for signing transactions. These keys are issued as many times as needed thus creating different identities for the same person. Since transactions are recorded with these pseudo names, it is thought that the real identities may not be linked to the transactions. Unlinkability has to be achieved for complete anonymity. However, recent studies show that real-life identities can be linked to addresses of these cryptocurrencies and transactions which use them. Therefore, it is safe to say that most cryptocurrencies are pseudonymous rather than anonymous. In this chapter, the problem with anonymity and its implications in accounting will be discussed. In addition to this, protocols and services, which make it harder or even impossible to link addresses and transactions to their senders and recipients, will be reviewed.

Keywords Cryptocurrency · Blockchain · Bitcoin · Altcoins · Anonymity · Pseudonymity

1 Introduction

Cambridge Dictionary defines anonymity as "the situation in which someone's name is not given or known" (2019). Therefore, the concept of anonymity in cryptocurrencies is related to disguising the real identities of those who are involved in cryptocurrency transactions.

H. B. Hazar (✉)
Department of Business Administration, Istanbul Aydın University, Istanbul, Turkey
e-mail: hulyahazar@aydin.edu.tr

© The Editor(s) (if applicable) and The Author(s), under exclusive licence to Springer Nature Switzerland AG 2020

M. H. Bilgin et al. (eds.), *Eurasian Economic Perspectives*, Eurasian Studies in Business and Economics 14/1, https://doi.org/10.1007/978-3-030-53536-0_12

When Bitcoin, the first successful cryptocurrency, was introduced, it was said that the identities of those involved in Bitcoin transactions are kept secret. The way to keep the anonymity in Bitcoin transactions is to use a public key instead of a real identity. Nakamoto (2008) states that privacy can be achieved by keeping public keys anonymous. The public can follow the transactions, i.e., anyone can see that a certain amount is transferred to a recipient from another person. However, the public does not have information that links the transaction to any real-life person. Cryptocurrencies like Bitcoin are believed to be anonymous in the eyes of public because there is no need to use one's real name. "Bitcoin addresses are hashes of public keys" (Narayanan et al. 2016, p. 165). The hash of one's public key is his identity. No one needs to use his real identity so that the related transaction is accepted into the blockchain network.

However, Nakamoto (2008) warns us about the possibility of linkability of the public keys to real identities. When there is a transaction with multiple inputs, it is easy to see that they are all made by the same person. If a key which is used in any of these transactions is linked to a real-world identity, it is unavoidable to link all the related transactions to the same person. Key properties for unlinkability are as follows (Narayanan et al. 2016):

1. It should be hard to link different addresses of the same user.
2. It should be hard to link different transactions made by the same user.
3. It should be hard to link the sender of a payment to its recipient.

In terms of computer science, cryptocurrencies are considered pseudonymous, but not anonymous. An assumed identity that is not the real name of the person is called pseudonymity, and anonymity is achieved if unlinkability is maintained together with pseudonymity.

From these statements, it is understood that cryptocurrency transactions are pseudonymous. Moreover, there is a possibility of linking such transactions to real identities. Most countries are concerned that cryptocurrencies may be used in illegal activities and money laundering. Therefore, they are trying to regulate such currency markets. This chapter argues that there is no need for overregulation since it is possible for governments to find who is using these currencies.

2 Linking Cryptocurrency Transactions to Real Identities

Most cryptocurrencies are developed using the blockchain technology. The blockchain network is a public ledger where any user can see the history of transactions (Berg et al. 2018). Since identities and cryptocurrencies are addresses in the network, anyone can obtain hashes of these addresses (Dimitri 2017). When cryptocurrencies change hands, they move from one address to another. Even if every cryptocurrency has a different address, a person looking into the network will see that the ownership of some cryptocurrencies is changing (Icaew IT Faculty 2017). After that it is easy to map the addresses of sending and receiving parties.

There is no general protocol or a system to link the public keys, i.e., pseudonyms to the transactions. Careful mapping of transactions to addresses is required. On the other hand, linking the public keys to real identities is more difficult. However, privacy risk is more imminent for those who use paid services that store personal data (Catalini and Gans 2017).

Linking transactions to a public key are easier if a lot of transactions are made using the same public key. It is not easy to reveal the identities of those who hold on to their cryptocurrencies and do not use those addresses again. Unlinkability is tougher if the transaction is related to purchasing goods. The payment is in cryptocurrency. However, the goods have to be sent to a real name and address. This means the vendor has to keep a record which links the payment to a real identity.

3 Studies on Deanonymization of Cryptocurrencies

3.1 Methods Used in Studies

Studies related to deanonymization of cryptocurrencies use mainly two methods:

1. Analysis of the transaction chain: The studies which use this method obtain transactions from the public blockchain, classify addresses, and relate these addresses to real-world identities. Coin mixing is found to be a powerful way against this method.
2. Analysis of the protocols and network: The studies, which use this method, find the initial IP address of a new transaction via Sybil attacks. Sybil attack is a way to link a new transaction to an IP address to find the relationship between the cryptocurrency and the related IP address. Using services like The Onion Router (TOR) is found effective against Sybil attacks.

3.2 Literature Review

Meiklejohn et al. (2013) published their work on traceability of Bitcoin flows. The study states heuristics that can be used to link addresses that are controlled by the same user in the Bitcoin network. These heuristics do not automatically reveal the names of the owners of the addresses, but group them with respect to their controlling bodies. For instance, wallet services control addresses that they generate, but these services are not the owners of the money in these addresses. Initially, addresses are tagged to find out their controlling bodies. For instance, the addresses of widely used exchanges and wallets are determined by actually involving in Bitcoin transactions with them. Then, Bitcoin transactions in and out of these addresses are traced. These transactions are represented graphically.

When wallets and other services use the change address function, it is very difficult to trace Bitcoin transactions. However, such services are highly centralized and most of the time they would know the real identities of those who do business with them. These services do not register these identities to the blockchain network, but keep for their internal use. Such services would know the real identities of owners of the money, which use their addresses. Therefore, under certain conditions these services may reveal the true identities of the owners of the money in question.

Fleder et al. (2015) parsed publicly available information in the Internet like public forums, donation sites, and public social networks for real names of public keys. They collected the public key addresses of the Bitcoin network and the related usernames. The reason that users of the Bitcoin network reveal their public key addresses in public forums is stated in the study (Fleder et al. 2015). The study reveals that it is a common practice to attach a bitcoin address as a signature to emails or forum posts. For instance, in forum posts, users leave their addresses in the signature block when they make contributions. Their aim was to associate as many public key addresses as possible with the real usernames. They concentrated on the real name and public key pairs that they could find rather than the whole Bitcoin network. They followed the transactions of these addresses developing a user graph showing Bitcoin transactions with the real-world names. The study states that they successfully uncovered the FBI intervention and the seizure of Silk Road funds, transactions between users and gambling sites like SatoshiDice and transfers to Wikileaks donations. Nick (2015) analyzed the performance of several clustering algorithms in the Bitcoin network and stated that the approach called clustering in the Bitcoin network refers to the process of finding addresses that belong to the same wallet. In this study, he was able to capture 37,585 Bitcoin wallets and the addresses they own. He demonstrated that modern wallet software cannot protect its users fully. He found that even with the most basic clustering technique the probability of guessing the address of a user is 68.59%.

ShenTu and Yu (2015) summarize the findings of many studies of the weakness of Bitcoin anonymity as follows:

1. Most service providers in the Bitcoin network require that the users register their real names. This enables such services to find the real-world names and addresses of those involved in transactions.
2. A Bitcoin address which is revealed in the internet can be related to its real-world owner.
3. Transactions that follow one after another are fully transparent and traceable.
4. Gathering Bitcoins that have different addresses and sending them together to a recipient may expose other addresses of the sender.
5. If the change address function is used when transferring Bitcoins, attackers may follow the related transactions to the sender.

4 Techniques and Services to Secure Anonymity

Mixing technique requires the need for an intermediary, which is called a mixing service. Users of the mixing service transfer their cryptocurrency to this intermediary. The mixing service joins all coins in a pool. When a user asks back his coin, it comes from a different address. Coin mixing is a simple and effective anonymization method. It helps to break the link between the input and output of a cryptocurrency transaction and even hide the amount of the transaction. However, there are weaknesses with centralized coin mixing services (ShenTu and Yu 2015):

1. Mixers must know a user's input and output addresses, and hence cannot provide true anonymity for users.
2. Users must trust mixers and send coins to mixers in advance, so users face with the risk of currency loss.

Some online wallets may act as mixing services. However, there are dedicated services for coin mixing like Tor. Dedicated mixing services claim that they do not keep records nor ask the identity of users.

Each cryptocurrency may have a different address. Wallet software stores these addresses for future use. Moreover, some wallet software randomly changes the addresses of returned coins to increase unlinkability.

Online wallets are services where users store their coins online. Users are allowed to withdraw these coins when they need. Coins that are withdrawn are not the same ones that are deposited. Since they would have different addresses, it is difficult to draw a transaction graph and link the coins to their owners. The anonymity set gets bigger as more people use the service and keep their money for longer periods of time.

Online wallets are reputable businesses that are often regulated. They usually require users' identities and keep records of transactions internally. Therefore, they are able to link the deposits to withdrawals and both these transactions to real identities. Users need to trust online wallets that they will not reveal user identities.

Tor is considered to be an anonymous communication network (Narayanan et al. 2016, p.169). It is defined as "free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security" (Torproject 2018). Tor is developed to protect against Internet surveillance known as traffic analysis. Traffic analysis is used for tracking the behavior of a user when the source and the destination of information transmission are known. Tor users do not have a direct communication with the party at destination. These users transmit information to other users in the network. After several transmissions to unrelated users, the information is sent to the party at destination. The path of transmission is never the same for multiple communications between the same parties. In 2015, FBI closed 400 illegal websites on the TOR network (ShenTu and Yu 2015). This statement makes one wonder whether Tor is as anonymous as it claims to be.

Zerocoin and Zerocash
Zerocoin is initially proposed by researchers from Johns Hopkins University. Miers et al. (2013, p. 397) defined Zerocoin as "a distributed e-cash system that uses cryptographic techniques". Zerocash is the improved version of Zerocoin. Zerocoin is actually a coin mixing protocol. It has Mint and Spent operations. Mint operation is used for transforming Bitcoins to Zerocoins. Spent operation exchanges Zerocoins to Bitcoins. Zerocoin hides the addresses of the sender and the receiver by employing a protocol level mixing. Anonymity is achieved with cryptography. A mixing service is not needed. Zerocoin and Zerocash are not compatible with the existing Bitcoin network. They require protocol change. Protocol changes may cause a hard fork to the Bitcoin network. Therefore, studies concentrate on developing Zerocoin and Zerocash for altcoins.

5 Importance of Anonymity

Privacy is a requirement for a financial system since it deals with sensitive monetary information. The names of the related parties and the value of the transaction should not be public information (Nick 2015). If a cryptocurrency address is linked to a real identity, any user of the related network would know who owns the money. Moreover, user's past transactions with that money are exposed. His/Her other cryptocurrencies are compromised if he/she is using the same pseudonym for his/her other cryptocurrencies as well. As it is seen, privacy is totally lost when the anonymity is lost.

Governments and public are concerned that cryptocurrencies may be used for money laundering and illegal activities. These currencies are not controlled by any central authority, and the markets where they are traded are not regulated. This adds to the worries of financial regulators and cybercrime fighters (Möser et al. 2013). There are cases that justifies this concern. For instance, there was an e-commerce web site called Silk Road where anything may be bought and sold with Bitcoins. It was found that drugs and firearms were traded as well. The positive side of anonymity is that it provides privacy. Privacy is required to protect people against those who may harm them. The downside of anonymity is that it may facilitate financial crimes.

6 Implications of Anonymity in Accounting

Transactions in cryptocurrency do not require personal identification. The data related to the cryptocurrency transaction does not cover any confidential information (name, surname, registered address, etc.) However, each transaction is registered to a public ledger, making the transaction transparent to the public, yet concealing the identities of the involved parties. As businesses begin to accept cryptocurrencies,

taxation poses a problem. “The major concern related to the taxation of virtual currencies is the difficulty to trace them because they are mined, used, and traded online completely anonymously” (nomoretax 2018).

In some countries, like the United States and Canada, virtual currency is treated as property. Therefore, any income in cryptocurrency should be taxed. Capital gains from trading such currencies need to be taxed as well. When cryptocurrencies are used to purchase goods and services, gains must be reported and taxed. However, it is unlikely that a tax authority will know about the income unless the vendor voluntarily reports it. Therefore, cryptocurrencies have the potential to become tax havens. Tax havens allow traders to conceal earnings from revenue services (Marian 2013).

Another problem with the anonymity of cryptocurrencies is that they can be used for money laundering and other crimes. Some countries take measures to identify the owners of cryptocurrencies to address the issue of anonymity (nomoretax 2018). For instance, China and South Korea passed laws related to cryptocurrency trading. In these countries, it is mandatory to register the real names of those who trade with exchanges.

The regulatory requirements in accounting are high regulatory requirements with respect to validity and integrity (Deloitte 2018). Regulation demands centralization where identities are fully disclosed. However, cryptocurrencies run on decentralized networks where privacy is the utmost concern. Therefore, accounting and anonymity seem to oppose each other.

7 Conclusion

Privacy, therefore anonymity, is important in financial systems. Cryptocurrencies use blockchain technology which is a public ledger. This means that all transactions can be viewed by users of the network. To maintain anonymity, the parties involved in transactions use public keys instead of their real names. Anonymity is needed when transactions are open to public. However, it raises concerns in the eyes of public and governments. The use of cryptocurrencies for illegal activities and the regulations of taxation for investing and trading such currencies pose problems. The current status of cryptocurrencies with its pseudonymous feature poses some problems for traditional accounting.

Different studies show that a relational graph of transactions between the public keys, i.e., pseu-identities, can be designed. Although more difficult, it is possible to reveal the real-world identities of these pseudonyms. It seems that the need of maintaining the privacy in financial systems cannot be completely achieved with the cryptocurrency network. In addition to this, illegal activities with cryptocurrencies can be traced to the source with special information technology.

References

Berg, C., Davidson, S. & Potts, J. (2018). *The Blockchain Economy: A beginner's guide to institutional cryptoeconomics* [online]. Accessed May 3, 2018, from https://medium.com/@cryptoeconomics/the-blockchain-economy-a-beginners-guide-to-institutional-cryptoeconomics-64bf2f2beec4

Cambridge Dictionary. (2019). *Encyclopaedia Britannica Online*. [online] London: Cambridge Dictionary (UK). Accessed September 9, 2019, from https://dictionary.cambridge.org/dictionary/english/anonymity?q=Anonymity

Catalini, C. & Gans, J.S. (2017). Some simple economics of the blockchain. *Rotman School of Management*, Working Paper No. 2874598 and *MIT Sloan*, Research Paper No. 5191–16.

De Hoon & Partners. (2018). *Can the Taxman Identify Owners of Cryptocurrencies*. [online] Accessed September 12, 2018, from http://www.nomoretax.eu/can-taxman-identify-owners-cryptocurrencies/

Deloitte. (2018). *Blockchain technology*. [online] Accessed May 15, 2018, from https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Blockchain_A%20game-changer%20in%20accounting.pdf

Dimitri, N. (2017). The blockchain technology: Some theory and applications. *Maastricht School of Management*, Working Paper No. 2017/03, [online] Accessed May 17, 2018, from https://www.msm.nl/resources/uploads/2017/10/Working-Paper-No.-2017-3.pdf

Fleder, M., Kester, M. S. & Pillai, S., (2015). *Bitcoin transaction graph analysis. Cornell university*. [archive online] Accessed May 15, 2018, from https://arxiv.org/abs/1502.01657

Icaew IT Faculty. (2017). *Blockchain and the future of accountancy*, [online] Accessed May 17, 2018, from https://www.icaew.com/-/media/corporate/files/technical/information-technology/technology/blockchain-and-the-future-of-accountancy.ashx

Marian, O. (2013). Are cryptocurrencies super tax havens. Michigan law review. *First Impressions, 112*, 38–48.

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M. & Savage, S., (2013). *A fistful of Bitcoins: Characterizing payments among men with no names*. In: IMC '13 Proceedings of the 2013 Conference On Internet Measurement Conference, Barcelona, Spain, October 23–25, 2013, p. 127–140.

Miers, I., Garman, C., Green, M. and Rubin, A.D. (2013). *Zerocoin: Anonymous distributed E-cash form Bitcoin*. In: IEEE, IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 19–22 May 2013. [online] Accessed Auguest 28, 2019, from https://ieeexplore.ieee.org/document/6547123

Möser, M., Böhme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the Bitcoin ecosystem. In *2013 APWG eCrime researchers summit*. San Francisco, California, USA, 17-18 September 2013.

Nakamoto, S. (2008). *Bitcoin: A Peer – to – Peer Electronic Cash System*. [online] Accessed Auguest 8, 2018, from https://bitcoin.org/bitcoin.pdf

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency technologies*. USA: Princeton University Press.

Nick, J. D. (2015). *Data-Driven De-Anonymization in Bitcoin*. [online] Accessed September 6, 2018, from https://www.research-collection.ethz.ch/handle/20.500.11850/155286

ShenTu, Q. C. & Yu J. P. (2015). *Research on Anonymization and De-anonymization in the Bitcoin System*. [online] Accessed September 6, 2019, from https://arxiv.org/ftp/arxiv/papers/1510/1510.07782.pdf

TOR. (2018). *What is TOR*. [online] Accessed August 29, 2018, from https://www.torproject.org/