Rise of Anonymous Cryptocurrencies: Brief Introduction

Jong-Hyouk Lee
Sangmyung University

***Abstract*—Bitcoin cannot provide enough anonymity for its users and, thus, people started to worry about a possible traceability in their cryptocurrency transactions. More and more people get into the crypto-ecosphere while privacy concerns are paramount. In this paper, five well-known cryptocurrencies that claim they provide anonymity are analyzed to see how, if at all, they achieve anonymity. We then examine the considered cryptocurrencies: Dash, Monero, Verge, PIVX, and Zcash.**

Bitcoin[1] **as a** cryptocurrency uses cryptography to secure its transactions and to verify the transfer of digital assets over the Internet without a centralized banking system.[1] Since its first release in 2009, it is the cryptocurrency the most popular among all the available ones (Figure 1 shows history of cryptocurrencies). According to the CoinMarketCap,[2] there are 1,517 cryptocurrencies available and 8,632 online markets to buy, sell, or exchange cryptocurrencies for other digital or traditional currency as of February 2018. The cryptocurrency market capitalization already surpassed $472 billion, with Bitcoin accounting for around $185 billion of the total. The volume has been increasing with a continuously growing expectation. The cryptocurrency market is something that we cannot ignore. The cryptocurrencies have evolved to the point where they pose a serious threat not only to financial sectors, e.g., banks and insurance companies, but also to other industrial sectors operating based on centralized control systems.[3]

Bitcoin was known as an anonymous cryptocurrency by many people in its early years. On the contrary, a coin history tracing is a well-known issue that consists into the possibility of analyzing the used coin's trace to connect identities to addresses. It is possible due to the flow of coins being highly public as the Bitcoin blockchain is public, i.e., anyone can see the flow of the coins from an address A to an address B. As the

Digital Object Identifier 10.1109/MCE.2019.2923927
Date of current version 30 August 2019.

Published by the IEEE Consumer Electronics Society

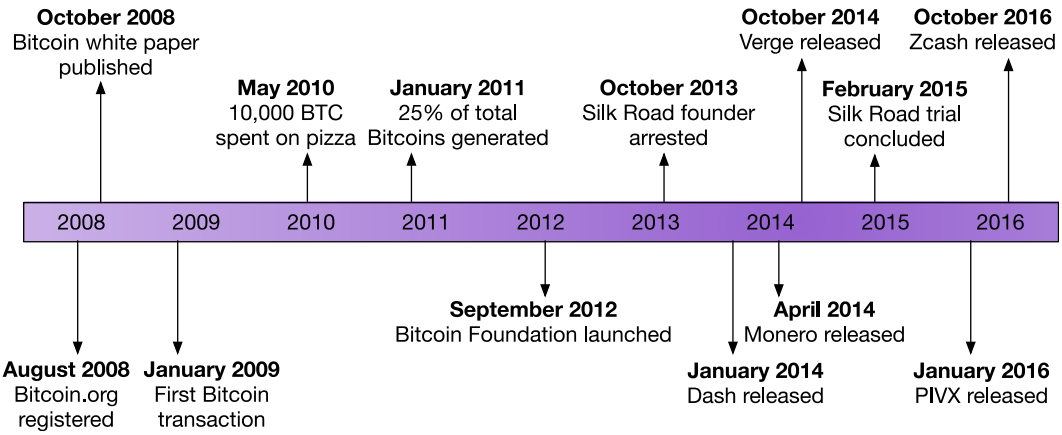

Figure 1. Short history related to Bitcoin and other cryptocurrencies.

addresses are just random strings generated basing on public keys of the address owners, the knowledge of *A* and *B* itself does not provide enough information to identify the address owners. However, if any of *A* and *B* in a transaction's past or future can be tied to an actual identity, it becomes possible to guess who may own the address. The identity information can be obtained in various ways, e.g., network analysis, surveillance, or just googling the address. There is thus a high demand for anonymous cryptocurrencies.

IS BITCOIN ANONYMOUS?

In short, Bitcoin is not really anonymous. Bitcoin was considered as an anonymous digital currency in the early stage. Many governments had worried about a possible untraceability of Bitcoin and potential unlawful uses such as tax evasion and money laundering. People also believed that Bitcoin would provide a certain level of anonymity that may avoid being tracked by public authorities. However, as shown in the Silk Road trial, a former federal agent unveiled how he traced 3,760 bitcoin transactions over 12 months. Bitcoin has the following particular characteristics that make its transactions traceable with appropriate extra analysis:[14] 1) Public blockchain; 2) public key-based address; and 3) peer-to-peer (P2P) networking over the Internet.

As all transactions are public and addresses are visible, one can associate a Bitcoin address, i.e., public key, with user information such as user identification, email address, and, bank account details. For instance, online shops that accept the cryptocurrency may require user information and record information like the IP addresses used for accessing the online shops. We, thus, can imagine that it would be possible to trace or reveal the real identify of a user associated with a particular transaction when such user information is available. It will be the same when considering cryptocurrency exchanges that are websites where you can buy, sell, or exchange cryptocurrencies. These websites, in general, require users to provide the real identification information with bank accounts. The Bitcoin network operates over the Internet, which means traffic analysis approaches used for the Internet can be well applied to investigate the leakage of identity information. It has been demonstrated that using real-time transaction traffic collected over five months was adequate to identify ownership relationships between Bitcoin addresses and IP addresses.[4]

ANONYMOUS CRYPTOCURRENCIES

Everyone has the right to privacy and untraceability in their financial transactions that is also applied for cryptocurrency transactions. Some cryptocurrencies focus on convenient payment or fast transactions, while some others are more focused on providing anonymity for users. An anonymous cryptocurrency is a cryptocurrency designed to have high levels of cryptographic qualities for providing anonymity for its users. In general, the anonymous cryptocurrency is required to provide the followings.

- *Privacy*: It is ensured that the origins, destinations, and amounts of all transactions are not observable by possible adversaries.

- *Untraceability*: It is ensured that coins that are being sent or received are not traceable nor linkable with a transaction history.
- *Fungibility*: It is ensured that all coins are pairwise indistinguishable and, thus, they are mutually interchangeable.

Among the cryptocurrencies claiming that they provide anonymity, in this paper, the following five are considered that provide technical documents and available source code: Dash,[5] Monero,[6] Verge,[7] PIVX,[8] and Zcash.[9]

Dash is a portmanteau of Digital Cash. It was originally released as Xcoin (also known as Darkcoin). Its cryptocurrency's basic feature is based on Bitcoin but features for providing anonymity have been added on top. Dash operates a two-tier network. The first tier of the Dash network is operated like the Bitcoin network. The second tier, constituted by master nodes, is the core of Dash. The master nodes are distributed nodes over the Dash network used to perform a coin mixing service that is the core feature for providing anonymity. To perform anonymous transactions, Dash relies on PrivateSend, which is a coin mixing service developed based on CoinJoin.[10] In addition to PrivateSend, Dash provides a fast transaction called InstantSend that solves the double-spending problem with less confirmation times than Bitcoin.

Monero was developed based on Bytecoin, which uses CryptoNote.[11] It has three features for providing anonymity in transactions: 1) ring signature, 2) stealth address, and 3) ring confidential transaction. A ring signature is used for protecting a sender's privacy, while a stealth address is generated for each transaction to protect a receiver's privacy. This makes impossible to link transactions between the sender and the receiver. A ring confidential transaction is used to hide the actual amount of the transaction between the sender and the receiver. It also offers the feature of letting someone else view the details of a transaction by sharing a view key.

Verge, previously known as DogeCoinDark, relies on an integration of Tor and I2P to obfuscate the IP address and geolocation of senders and receivers rather than employing extra cryptography techniques for providing anonymity. Verge was developed based on Bitcoin and no cryptography techniques applied to its transactions like for Bitcoin. The transactions in the blockchain are thus transparent. For instance, an observer can see the transactions stored at the blockchain. For improving receiver's privacy, a plan to develop a stealth address feature is being explored.

PIVX, formerly known as Darknet, stands for private instant verified transaction. PIVX is a fork cryptocurrency of Dash, meaning that it inherits the technical features of Dash, including the master nodes, coin mixing transactions, and fast transactions. However, unlike Dash, PIVX adopted a proof of stake (PoS) mechanism as its consensus algorithm that uses the master nodes to verify transactions instead of miners used in the proof of work (PoW) of Dash. Mining, required in all cryptocurrencies using the PoW as a reward system, is not exist in PIVX.

Zcash is a cryptocurrency developed for providing anonymity by using zk-SNARKs, which are a type of zero-knowledge proof. Its fundamental feature comes from Bitcoin, but features to obscure the sender, receiver, and amounts of transactions are added. The obscured transactions are called shielded transactions. The anonymity support in Zcash is optional and to perform shielded transactions both sender and receiver are required to use shielded addresses, instead of transparent ones. It is observed that about 6.3 percent of Zcash coins are controlled by shielded addresses on average. Zcash provides a feature called a selective disclosure that allows a user to prove its payment for auditing reasons.

COMPARISONS OF CRYPTOCURRENCIES

Comparisons among the five cryptocurrencies considered in this paper are given in Table 1, with Bitcoin is as the baseline. Most of the cryptocurrencies have been developed based on Bitcoin, except Monero and PIVX. Note that PIVX is based on Dash, but Dash was built upon Bitcoin's core code.

Most of the cryptocurrencies use the PoW as a consensus algorithm. The PoW-based cryptocurrencies maintain a reward system in their blockchains. The system is typically hardware

Table 1. Comparisons of cryptocurrencies.

	Bitcoin	Dash	Monero	Verge	PIVX	Zcash
Origin	-	Bitcoin	Bytecoin	Bitcoin	Dash	Bitcoin
Release	January 2009	January 2014	April 2014	October 2014	February 2016	October 2016
Consensus algorithm	PoW	PoW	PoW	PoW	PoS	PoW
Hardware mineable	Yes	Yes	Yes	Yes	No	Yes
Block time	600 s	150 s	120 s	30 s	60 s	150 s
Rich list	Yes	Yes	No	Yes	Yes	No
Master node	No	Yes	No	No	Yes	No
Sender address hidden	No	Yes	Yes	No	Yes	Yes
Receiver address hidden	No	Yes	Yes	No	Yes	Yes
Sent amount hidden	No	No	Yes	No	No	Yes
IP addresses hidden	No	No	No	Yes	No	No
Privacy	No	No	Yes	No	No	Yes
Untraceability	No	No	Yes	No	No	Yes
Fungibility	No	No	Yes	No	No	Yes

mineable and gives a reward to miners that use their computing power to validate a block. PIVX uses the PoS that is not hardware mineable. It has a different reward system for its operation in the public blockchain. PIVX users can have a chance to earn a reward by keeping PIVX coins in their online wallet, an operation that is called staking. Another way to earn a reward is to operate a master node that requires 10,000 PIVX coins into a locked account. Dash also provides a reward for its master nodes.

One of the limitations that Bitcoin has is a long block time: the average time to generate a block is 10 minutes. A transaction in Bitcoin takes around an hour, on average, if six confirmations are needed. The popularity of Bitcoin has caused network congestion and the average time just for one confirmation thus increased from 30 minutes to more than 8 hours in extreme cases. Compared to Bitcoin's block time, all the cryptocurrencies proposed for anonymity offer reduced block times. That means the developers of the cryptocurrencies care about the transaction speed. Verge just takes 30 seconds to generate its one block.

Only Monero and Zcash do not provide a rich list, which is a coin address list showing the largest coin holders. The other cryptocurrencies provide the rich lists. The rich lists are made based on the transaction information stored at the blockchains. The existence of a rich list of a cryptocurrency means that the cryptocurrency provides the transparent blockchain, which may be considered as a weak point for an anonymous cryptocurrency.

Dash and PIVX utilize the master nodes to implement the anonymity support features. However, it is an arguable issue. It is possible to operate some master nodes for logging transactions for breaking anonymity of a specific target. Also, master nodes are good targets for distributed denial-of-service attacks to bring them down for fun or profit.

Bitcoin does not provide any features for hiding the sender's and receiver's addresses, the

amount of coins sent, and IP addresses of the peers. It, thus, does not provide any privacy, untraceability, and fungibility for its users. Monero and Zcash, which provide the features for hiding the addresses of sender and receiver and the amount of coins sent, are considered as the cryptocurrencies providing privacy, untraceability, and fungibility for its users.

Dash provides the features for hiding the sender's and receiver's addresses. However, this cryptocurrency is questionable regarding the privacy, untraceability, and fungibility supports, due to the partnership for the antimoney laundering (AML) and know your customer (KYC) compliance with Coin-firm, which is a company selling a solution for cryptocurrency AML/KYC compliance. Verge uses Tor and I2P so that it provides the IP addresses hiding, but as presented by Biryukov and Pustogarov,[12] there are a couple of attack vectors through which an attacker can link user's transactions and in certain cases the attacker can recognize the user's IP address.[13] PIVX provides the features for hiding the address of sender and receiver. However, PIVX has its rich list visible to anyone examining the transaction, so its privacy and fungibility supports are questionable. Moreover, the master nodes of PIVX can be used for tracing transactions, and therefore, its untraceability support is also questionable.

It is obvious that anonymity is not free and often comes with a high price attached to the cryptocurrency. In other words, cryptocurrencies focused on providing anonymity for users usually require additional things to do that make them less desirable, e.g., this may be a reason why about 6.3 percent of Zcash coins are in the shielded pool as of January 2018.

CONCLUSION

The recent interest in cryptocurrencies extends beyond information technology to politics, society, and economy.[3,14,15] Since Bitcoin was released in 2009, more than 1,500 cryptocurrencies have been developed, but only some of them are focused on providing anonymity for users. The developers had noticed the increasing demand for financial privacy and there are already several cryptocurrencies claiming they provide enough anonymity for its users. The five cryptocurrencies—Dash, Monero, Verge, PIVX, and Zcash—have been examined. According to the comparison results, only Monero and Zcash are considered to be the cryptocurrencies providing privacy, untraceability, and fungibility for its users. The others are not (or questionable) providing all the three requirements.

ACKNOWLEDGMENTS

This work was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF), funded by the Ministry of Science, ICT, and Future Planning under Grant NRF-2017R1A1A1A05001405.

REFERENCES

1. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Oct. 2008. [Online]. Available at: https://bitcoin.org/bitcoin.pdf
2. [Online]. Available at: https://coinmarketcap.com, Accessed on: Feb. 22, 2018.
3. J.-H. Lee and M. Pilkington, "How the blockchain revolution will reshape the consumer electronics industry," *IEEE Consum. Electron. Mag.*, vol. 6, no. 3, pp. 19–23, Jul. 2017.
4. P. Koshy, D. Koshy, and P. McDaniel, "An analysis of anonymity in Bitcoin using P2P network traffic," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, Mar. 2014, pp. 469–485.
5. E. Duffield and D. Diaz, "Dash: A privacy-centric crypto-currency." [Online]. Available at: https://github.com/dashpay/dash/wiki/Whitepaper, Accessed on: Feb. 22, 2018.
6. [Online]. Available at: https://getmonero.org/resources/research-lab, Accessed on: Feb. 22, 2018.
7. [Online]. Available at: https://vergecurrency.com/assets/Verge-Anonymity-Centric-CryptoCurrency.pdf, Accessed on: Feb. 22, 2018.
8. [Online]. Available at: https://pivx.org/what-is-pivx/white-papers, Accessed on: Feb. 22, 2018.
9. D. Hopwood, S. Bowe, T. Hornby, and N. Wilcox, "Zcash protocol specification (version 2018.0-beta-9)," Feb. 22, 2018.
10. [Online]. Available at: https://en.bitcoin.it/wiki/CoinJoin, Accessed on: Feb. 22, 2018.
11. N. Saberhagen, "CryptoNote v2.0," Oct. 2013.
12. A. Biryukov and I. Pustogarov, "Bitcoin over Tor isn't a good idea," in *Proc. IEEE Symp. Secur. Privacy*, May 2015, pp. 122–134.

13. [Online]. Available at: http://xvg.keff.org/, Accessed on: Feb. 22, 2018.
14. D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you wanted to know about the blockchain," *IEEE Consum. Electron. Mag.*, vol. 7, no. 4, pp. 6–14, Jul. 2018.
15. D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework," *IEEE Consum. Electron. Mag.*, vol. 7, no. 2, pp. 18–21, Mar. 2018.

Jong-Hyouk Lee is a Professor with the Sangmyung University, Cheonan, South Korea. Contact him at: jonghyouk@smu.ac.kr.