Cryptocurrencies: Transparency vs. Privacy

By: Nir Kshetri

Kshetri, Nir (2018)." Cryptocurrencies: Transparency vs. Privacy", *IEEE Computer*, 51(11), 99-111.

Made available courtesy of IEEE: https://doi.org/10.1109/MC.2018.2876182

Abstract:

Cryptocurrencies can have significant privacy costs. A motivated adversary has available a range of actions to identify the actual user associated with a cryptocurrency account. By taking appropriate measures, cryptocurrency users can minimize privacy violations and reduce the risk of privacy breaches.

Keywords: privacy | security of data | computer security | bitcoin | blockchain

Article:

Transparency is a major factor that is driving the use of blockchain-based applications such as cryptocurrencies. A major question becomes whether transparency provides reasonable privacy protection. For instance, many firms in the financial sector do not like the fact that blockchain's transparent nature gives other users access to the details of conducted transactions.

Let's begin with cryptocurrencies. It is important to note that cryptocurrencies possess built-in mechanisms that provide reasonable levels of privacy to users. To make the costs of transparency less severe to privacy, Bitcoin and other cryptocurrencies employ pseudonymity. Users can conduct transactions with one another without disclosing any information related to their identity.

Concealing the Internet Protocol (IP) addresses of users is another mechanism that provides protection to cryptocurrency user privacy. For example, in the Bitcoin network, correspondence cannot be established between transactions and IP addresses. Bitcoin users are connected to a peer-to-peer (P2P) network. Data continue to flow among the devices connected to the P2P network until everyone has the information related to a transaction. No one, except for the originator, knows who initiated the transaction.[1]

CONSEQUENCES OF PRIVACY VIOLATIONS IN THE CRYPTO-WORLD

Individuals and organizations are likely to suffer more severe consequences from cases of privacy violation if they engage in illegal behaviors using cryptocurrencies (compared with other transaction models). For example, if someone is caught in a crime, the cryptocurrency account can be linked to any crime committed by that person in the past. Privacy breaches are likely to lead to more severe criminal consequences, referred as an *amplified technical impact*.[2]

Privacy is important for citizens and businesses. If an individual uses Bitcoin to pay for certain goods or services, the party with whom the transaction is being made can know exactly how much money the individual has. This may increase the threat to personal safety. A supplier that has received a payment from a business would know how much money the business has. Knowing fund availability and customer price sensitivity could affect future negotiations. Finally, if online businesses have information about a consumer's spending patterns, they could predict the highest price that the consumer could pay. The business could then use price tampering to increase profits.[3]

UNWANTED PERSONAL INFORMATION LINKS

There are various sources of unwanted personal information leaks in transactions involving cryptocurrencies. For instance, while Bitcoin transactions are difficult to track, they are not completely anonymous. All transactions are recorded in a permanent public ledger. After the Bitcoins are moved from that address, financial movements can be traced. Users can be traced through IP addresses and money flows. A team of researchers studied 130 major merchants that allow Bitcoin transactions. They found that at least 53 of the merchants leaked payment information to at least 40 third parties. While most of the information leaked was intentional and used for advertising and analytics, some merchant websites also leaked precise blockchain transaction information to trackers.[4]

Blockchain ledgers are searchable and, hence, can be used to track transactions.[5] If a leak involves the amount and time of the purchase, a motivated adversary can convert the purchase amount into Bitcoins using the exchange rate at that time. Then, a blockchain can be searched for a transaction of that amount and at that time. This gives away the user's Bitcoin address. Any other purchases made using that address are now easier to trace.[4]

Sometimes, an act of carelessness on the part of the user may decrease privacy. This happened to Ross Ulbricht, who created the online black market Silk Road, best known as a platform for selling illegal drugs. When Ulbricht looked for help to expand the Silk Road business, he used the same pseudonym that he had adopted previously to post announcements on illegal drug discussion forums. This made him an FBI suspect. The FBI tracked his IP address to an Internet café in San Francisco and caught Ulbricht as he was logging in to Silk Road as an administrator.[1]

Another privacy problem occurs when users of cryptocurrencies such as Bitcoin reuse addresses. By doing so, they publicly disclose information about past financial transactions, and this can compromise their privacy. The transparency and immutability features of cryptocurrencies like Bitcoin make it possible to track every transaction involving a given address. Even if a person has engaged in careful processes to hide his or her identity, once a link has been established between a person’s identity and a Bitcoin address, all past transactions made by the owner of the Bitcoin address will be associated to the owner’s identity.

CRYPTOCURRENCIES HAVE DIFFERENT LEVELS OF PRIVACY

Well-known cryptocurrencies such as Bitcoin have not been able to meet all privacy needs of users. As mentioned, financial firms are concerned that blockchain’s ledger allows other users to access the details of transactions already conducted. In response to these demands, some cryptocurrencies provide users with higher levels of privacy protection.

Blockchain is still in early-stage development, and various alternative models and forms of cryptocurrencies are evolving along with it. For instance, to make blockchain more appealing to financial institutions, the cryptocurrency Zcash, which was launched in October 2016, has promised transactional privacy.[6] It employs cryptography to enhance user privacy.

Zcash transactions can be made transparent, like those of Bitcoin, or shielded through a zero-knowledge proof. Zcash transactions have two types of addresses: transparent and shielded. In transparent addresses, as is the case for Bitcoin, the monetary amount of the transaction as well as information about the receiver and the sender appears in the blockchain. On the other hand, if a shielded address is used, the address is “obscured” on the public ledger. Also, if both the sender and the receiver use shielded addresses, the transaction amount is encrypted.

Users of shielded addresses constitute a small proportion of Zcash adopters. In early 2017, shielded addresses accounted for about 0.8% of Zcash transactions.[7] That proportion is predicted to increase to 4% by mid-2018.[8]

A relatively low adoption rate of shielded addresses might be due to the additional time and computational resources required. Shielded addresses require a more computationally intensive process. To use Zcash’s privacy features, users may need 4 GB or more of RAM (tinyurl.com/y9dtj3dh).With 4 GB of RAM, operations were reported to take as long as 2 min to complete.[9] Therefore, most exchanges and wallets support only transparent Zcash transactions.[8]

Likewise, Monero focuses on privacy and untraceability by hiding the transaction’s sender, receiver, and monetary amount. To achieve this, Monero mixes Monero “coins” with other forms of payments. This makes it nearly impossible to link a transaction to any particular identity or previous transaction from the same source if only Monero’s blockchain is searched.[10]

Despite higher levels of user privacy from Monero and Zcash, these cryptocurrencies have not yet achieved higher popularity. For instance, as of mid-July 2018, market capitalization of Monero and Zcash was about 2 billion and 816 million, respectively, compared with Bitcoin’s 115 billion and Ethereum′s 48 billion (coinmarketcap.com/).

REGULATORY AND LAW ENFORCEMENT RESPONSES

Regulatory and law enforcement agencies are now focusing on illegal activities associated with cryptocurrencies. Law enforcement agencies are concerned with the anonymity features of cryptocurrencies. At a congressional hearing, former assistant US attorney Kathryn Haun noted that, when regulators issue subpoenas requesting documents relating individual identities to illicit activities at cryptocurrency exchanges, subpoenas may return information such as “Mickey Mouse” living at “123 Main Street” (tinyurl.com/y8g2x23c).

Academic researchers and blockchain intelligence companies are using advances in computer science, economics, and forensics to help law enforcement. Law enforcement agencies now have access to advanced techniques to track illegal activities that employ cryptocurrencies. Elliptic, a blockchain intelligence company, uses artificial intelligence to scan and analyze the Bitcoin network to identify suspicious transactions. It can trace transactions to individuals and groups. Elliptic’s services are used by online exchanges and law enforcement to detect money laundering (bit.ly/1T3SBwc).

The higher levels of privacy offered by cryptocurrencies such as Monero and Zcash concern regulators who are focused on money laundering. A cybercrime expert at the European Union’s law enforcement agency, Europol, noted that criminals have begun shifting away from Bitcoin to cryptocurrencies with higher levels of privacy (tinyurl.com/yat9hucw). In recent years, regulators have increased their focus on cryptocurrencies with higher degrees of nontraceability. In June 2018, in testimony before the House of Representatives Committee on Financial Services Subcommittee on Terrorism and Illicit Finance, an official of the US Secret Service recommended better regulation of less traceable cryptocurrencies to prevent illegal activities from benefiting from nontraceable coins (tinyurl.com/ycot283t).

Cryptocurrencies’ transparency and immutability features come with a privacy cost. Adversaries can use a range of actions to identify the actual user associated with a specific cryptocurrency account.

It is important for cryptocurrency users to be aware that their privacy can be compromised. Users need to take precautions to minimize privacy violations and mitigate the risk of privacy breaches. Users should refrain from reusing identities in both their noncryptocurrency and cryptocurrency worlds. Likewise, by reusing cryptocurrency addresses, users are more likely to publicly disclose personal information. Higher levels of privacy require generating a new address for each transaction.

ACKNOWLEDGMENTS

I thank Jeff Voas for numerous edits and suggestions on previous versions of this article.

REFERENCES

1. J. Bohannon., "Why criminals can’t hide behind Bitcoin", *Science*, Mar. 2016, [online] Available: http://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin.

2. *Generating value from big data analytics*, 2014, [online] Available: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Generating-Value-From-Big-Data-Analytics.aspx.

3. "What is Monero? Everything you need to know", *Draglet*, 2018, [online] Available: https://www.draglet.com/what-is-monero/.

4. "Bitcoin transactions aren't as anonymous as everyone hoped", *Technology Review*, Aug. 2017, [online] Available: https://www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped/.

5. E. Aldaz-Carroll, E. Aldaz-Carroll, "Can cryptocurrencies and blockchain help fight corruption?", *Brookings*, Feb. 2018, [online] Available: https://www.brookings.edu/blog/future-development/2018/02/01/can-cryptocurrencies-and-blockchain-help-fight-corruption/.

6. L. Clozel, "How Zcash tries to balance privacy transparency in Blockchain", *American Banker*, 2016, [online] Available: http://www.americanbanker.com/news/law-regulation/how-zcash-tries-to-balance-privacy-transparency-in-blockchain-1092198-1.html.

7. A. Hertig., "Hardly anyone seems to be using Zcash's anonymity features", *Coin Desk*, Jan. 2017, [online] Available: https://www.coindesk.com/hardly-anyone-is-using-zcashs-anonymity-features-but-we-couldnt-tell-if-they-were/.

8. B. Penny, "What is ZEC? Introduction to Zcash: Blockchains can cause zzzzz but pure currency cryptos can really push boundaries", *Crypto Briefing*, May 2018, [online] Available: https://cryptobriefing.com/what-is-zec-introduction-to-zcash/.

9. P. Peterson, "User expectations at Sprout Pt. 2: Software usability and hardware requirements", *Zcash*, Oct. 2016, [online] Available: https://blog.z.cash/software-usability-and-hardware-requirements/.

10. A. Greenberg, "The dark web's favorite currency is less untraceable than it seems", *Wired*, Mar. 2018, [online] Available: https://www.wired.com/story/monero-privacy/.