Deanonymizing Bitcoin blockchain Transaction networks

Yi Luo

May 25, 2018

The anonymity of the blockchain has been controversial. Anonymity is a double-edged sword, which is very important from the perspective of protecting privacy, but it also provides an umbrella for some illegal acts. From the perspective of ordinary people, on the one hand, they need to protect their privacy and prevent individuals from using sensitive data to be used by others to conduct various kinds of fraud and harassment. On the other hand, they do not want the blockchain to be malicious. Behavior provides an anonymous platform and hurts himself. In the complex psychological struggle of mankind, the confrontation between anonymous and anonymized technology is still continuing.

1 Is Bitcoin completely anonymous?

Bitcoin cannot technically achieve complete anonymity. This has led to the attention of some researchers who have used data analysis methods to achieve de-anonymization of blockchains. The goal is to find multiple codenames owned by the same object. Some research results claim that the accuracy of the association can reach 80How to kill Bitcoin Anonymity: 1. Because Bitcoin is a peer-to-peer network (easily attacked by hackers), if a hacker can use a node or computer to connect to the Bitcoin network, the hacker can extract enough information to decrypt the origin of the transaction. 2. If a bitcoin wallet has been registered with real personal information, it would be extremely easy for hackers and cybercriminals to find a bitcoin breach. 3. Blockchain transparency allows analysis of transactions and can be associated with the originator of a transaction. for example: One of the most common ideas is to conduct financial flow analysis on open transaction book information. Each bill in the blockchain book records the transfer of a certain fund. The simplest transaction involves only two codes: one provider and one receiver. However, if there is a transaction that requires the provider to pay 10 coins, and the provider's code name is less than 10 coins each, what can be done? Simply, this user can just transfer money from multiple codes at the same time. This situation is common in real trading. So, if there is a transaction with multiple code as a provider, can it be determined that these codes belong to one user? The answer is: very likely, because in reality, it is rare to find a transaction and there are multiple different users as payment. Party's situation. This constitutes the first heuristic rule commonly used for code association: if a transaction has multiple payment codes, these codes belong to one user. In addition, the change is also a common transaction, for example, the user pays 50 to other people, the actual payment is only 40, to retrieve change 10 . Obviously, the change recipient code for change should also be controlled by the provider, which constitutes the second heuristic rule for code association: In a transaction, the change receive code and payment code of a change belong to the same user. The core of the second rule is how to confirm the receipt code of a change code. In Bitcoin and other blockchain technologies, change accounts are usually new and unused accounts, which can help us detect change recipient codes. Using these rules, we can associate some codes with the same user. According to the book information recorded in the blockchain, we can also draw the corresponding diagram of the transaction graph and code, and more intuitively reflect the flow of funds between the code. For example, the following figure draws a transaction flow chart including 19 codes and 7 transactions. According to the defined rules, we can find that codes 1 and 2 belong to the same user, and codes 8, 9, and 14 also belong to the same. user. Through the analysis of transaction data, it can be considered that the entire transaction process actually has only 6 users.

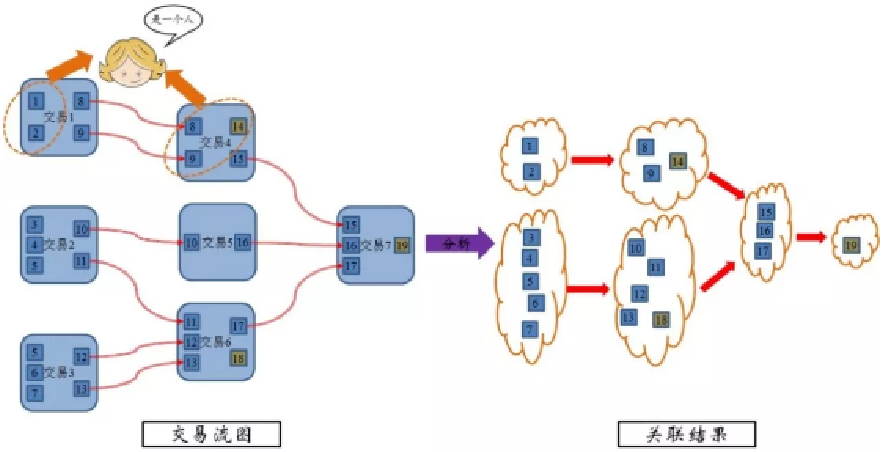

Figure 1: Transaction flow chart

2 What are the bad points?

When Bitcoin's de-anonymization may lead to Bitcoin's loss of interchangeability, thus decentralizing the demise of cryptocurrencies, this damages the value of all cryptocurrency units, not just the value of illegal activities. On the other hand, once de-anonymized, the user's entire financial history from the beginning will be exposed, which is worse than traditional banks.

3 What are the benefits?

When Bitcoin goes anonymized, it can be better regulated. On the one hand, illegal trading of criminals can be effectively countered. On the one hand, the supervision of Bitcoin can be made more effective and the theft of Bitcoin can be effectively tracked. In February 2014, MT.Gox, a Bitcoin exchange in Tokyo, announced the suspension of trading and subsequent bankruptcy. The reason is that it has been hacked, resulting in the theft of nearly 750,000 Bitcoins. In accordance with the price of Bitcoin at that time, the total loss was about US350$million(calculatedaccordingtoBitcoinpricesonFebruary7, 2018, totaling$ billion). At the end of January this year, Coincheck, another Japanese cryptocurrency exchange, was also hacked and about 534 million U.S. dollars were stolen. This shows that even if the decentralized Bitcoin is not safe enough, there is still the possibility of theft, and because of its anonymity, making tracking Bitcoin becomes a very difficult thing.

4 The need for Bitcoin to be de-anonymized

1. The anonymity of Bitcoin facilitates illegal activities such as the purchase of drugs and guns by criminals, and also greatly increases illegal money laundering. 2. The anonymity of Bitcoin does not protect the privacy of legitimate users. When Bitcoin users make small purchases, they may be able to hide their own information (eg, purchase anti-depressant drugs, and do not want others to know), so as to achieve the purpose of protecting privacy. However, when dealing with large amounts of money, it is difficult to protect your privacy, even if Bitcoin has anonymity. Since Bitcoin's transaction bills are transparent, large-scale transactions are prominent in countless Bitcoin transactions. There are already technologies for tracking Bitcoin.

5 Countries' Attitudes to Bitcoin Anonymity

China has completely banned ICO. Japans financial services agencies must be approved before listing cryptocurrencies and may not whitelist highly anonymous tokens. The Indian government has denied the possibility of the digital currency being the legal currency, Vietnam has banned Bitcoin and other digital currencies trading, and China claims that the digital currency disrupts the financial order and South Korea also holds the same attitude. South Korea intends to ban virtual accounts for digital currency transactions while allowing new transactions through certified bank accounts. The Securities and Exchange Commission (SEC) has already imposed sanctions on ICOs that have been found to be related to fraud. In addition, the US Commodity Futures Trading Commission (CFTC) has defined digital currencies as commodities, and the IRS requires virtual currency profits to be taxed.

6 Bitcoin de-anonymization technology development

The US Department of Homeland Security (DHS) Science Council and Sandia National Laboratories wanted to create a tool to anonymize. Block analysis and network traffic tracking make it possible to identify a large number of Bitcoin transaction sources. Reid and Harrigan's Anonymity Analysis of the Bitcoin System explores whether personal identities can be integrated with external data sources to determine the location of individual users. The results of the study indicate that it is possible to identify and prosecute unlawful actors through the analysis of Bitcoin exchange transactions. However, technical proficiency and well-funded criminal actors can bypass the identification control process and participate in Bitcoin transactions without revealing their true identities. Afterwards, researchers at the University of Zurich detailed Bitcoin's technology for anonymization. Another idea is to establish the relationship between each code number and its network card address by analyzing the routes in the network. The principle is that the same user's network card address is usually the same. Therefore, as long as it can be found that two different codes come from the same physical network card address, then these two codes are likely to belong to the same user. To implement such a mechanism, a super node needs to be created on the network to monitor the data of active nodes in the blockchain network at any time. Some research results claim that using network monitoring to achieve anonymization can achieve an accuracy of 30As the saying goes, One foot is tall and one foot is high, and while some scholars study how to go anonymous, there are also some scholars and institutions that study how to enhance the anonymity of the blockchain. Currently, there are three main research methods:) P2P mixing mechanism; (2) distributed confusing network; (3) zero-knowledge proof. The P2P mixing mechanism refers to a number of users signing an agreement to mix multiple transactions into one standard transaction. So, the level of anonymity depends on the number of mixed transactions. In this way, we cannot determine that multiple payment codes for the same transaction belong to the same user. In a mixed transaction, if multiple suppliers and receivers are randomly sorted, we cannot know which code a particular fund is flowing into. By breaking the continuity of the transaction, it can make it more difficult to establish associations between code numbers. The starting point of the distributed obfuscation network is also to blur the relationship between the input and output of capital flows. Its main strategy is to exchange funds with multiple traders through a third-party agency. The analysis of fund flow is invalid. Relatively speaking, zero-knowledge proofing technology has the highest degree of anonymity, but its efficiency and performance are still strict. Many users will reach the following agreement with a third-party institution: I will first deliver to the organization 10 After a period of time, the institution will return 10 coins to me. Simply put, this is money laundering. In this way, it is very difficult for outsiders to capture the correlation information between transactions. However, this approach also faces the risk of non-return of funds by third parties. Zero-knowledge proof can also be used to prevent financial flow analysis. Under this technology, fund providers do not need to verify the validity of funds by providing their own identity information, but only need to prove that the funds belong to the public of a valid fund. List. Further, the use of zero-knowledge proofs also allows users to pay directly in a completely private manner. The corresponding transaction hides the providers, recipients, and transaction volumes of the funds, and passes zero without providing such information. Knowledge certification technology allows others to verify the validity of the transaction. From the current technology point of view, the P2P mixing mechanism and distributed obfuscation network are mainly used to prevent existing fund flow analysis strategies. The goal is to cut down the relationship of funds between different users in the blockchain, resulting in a lack of weight. In short, these The latest blockchain anonymity technology still has a lot of immature areas that need to be further played.