Forensic Science International: Digital Investigation 31 (2019) 200895

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

Identifying suspicious addresses in Bitcoin thefts

Yan Wu [a], Anthony Luo [b], Dianxiang Xu [c, *]

[a] School of Computer Science, Jiangsu University, Zhenjiang, Jiangsu, 212013, China
[b] Fu Foundation School of Engineering and Applied Science, Columbia University, New York, NY, 10027, USA
[c] Department of Computer Science and Electrical Engineering, University of Missouri – Kansas City, Kansas City, MO, 64110, USA

ARTICLE INFO

Article history:
Received 24 May 2019
Received in revised form
7 November 2019
Accepted 10 November 2019
Available online xxx

Keywords:
Blockchain
Bitcoin
Forensic analysis
Pattern matching

ABSTRACT

Bitcoin as a popular digital currency has been a target of theft and other illegal activities. Key to the forensic investigation is to identify bitcoin addresses involved in the bitcoin transfers. This paper presents a framework, FABT, for forensic analysis of bitcoin transactions by identifying suspicious bitcoin addresses. It formalizes the clues of a given case as transaction patterns defined over a comprehensive set of features. FABT converts the bitcoin transaction data into a formal model, called Bitcoin Transaction Net (BTN). The traverse of all bitcoin transactions in the order of their occurrences is captured by the firing sequence of all transitions in the BTN. When analyzing transaction flows, FABT exploits the notion of "bitcoin fluid" to track where the bitcoins passed through given addresses (called dyeing addresses) have flown and determine the extent to which each of the other addresses is related to the dyeing addresses. The splitting, merging, and dyeing operators are used to capture the distribution of coins throughout transaction flows. FABT also applies visualization techniques for further analysis of the suspicious addresses. We have applied FABT to identify suspicious addresses in the Mt.Gox case. A subgroup of the suspicious addresses has been found to share many characteristics about the received/transferred amount, number of transactions, and time intervals.

1. Introduction

Bitcoin (Nakamoto, 2008) has become increasingly popular as an electronic form of currency. Users hold bitcoins via addresses that are not linked to personally identifiable information. Therefore, bitcoins had been commonly used for trades at major darknet markets such as Silk Road, AlphaBay, and Hansa.[1] There have been numerous high-profile cases of bitcoin theft in the past. An operator of the BTC-e bitcoin exchange laundered more than $4 billion worth of illegal funds for criminals, ranging from computer hackers to drug traffickers. In 2014, the Mt. Gox exchange announced that approximately 850,000 bitcoins, valued at more than $450 million at the time, were missing and likely stolen. In 2015, 19,000 bitcoins, worth about $5 million at the time, were stolen from the Bitstamp exchange and in 2016, nearly 120,000 bitcoins, worth about $72 million at that time, were stolen from the Bitfinex exchange. NiceHash, a marketplace for mining digital currencies, announced in 2017 that 4700 bitcoins, worth $75 million at that time, were stolen from its account.

A key to the forensic investigation of such cases is the identification of bitcoin addresses that are involved in the related transactions. Although bitcoin holders are pseudonym, all transactions on the bitcoin blockchain are public. If a criminal bitcoin address is known, we can track the bitcoins that have passed through the address. If these coins are then deposited in Bitcoin exchanges (places that convert bitcoins to government-issued currencies), law enforcement would be able to obtain the suspect's identity information because Bitcoin exchanges are required by "Know Your Customer" laws to collect personal information.

This paper presents a framework, FABT, for forensic analysis of bitcoin transactions by identifying suspicious bitcoin addresses involved in a case under investigation. It formalizes the clues of a given case as transaction patterns defined over a comprehensive set of features regarding transactions, addresses, and transaction flows. To facilitate pattern matching, FABT converts the bitcoin transaction data into a formal model, called Bitcoin Transaction Net (BTN), which is an extended form of safe Petri nets (Göbel, 2016). The formal model allows the transaction and address features to be formalized in terms of the structural information of the BTN and

* Corresponding author.
E-mail addresses: wuyan04418@ujs.edu.cn (Y. Wu), anthony.luo@columbia.edu (A. Luo), dxu@umkc.edu (D. Xu).

[1] Such darknet sites as Silk Road, AlphaBay, and Hansa are no longer available.

https://doi.org/10.1016/j.fsidi.2019.200895
1742-2876/

the transaction flow features to be analyzed by the dynamic semantics of transition firing of the BTN. The traverse of all bitcoin transactions in the order of their occurrence is captured by the firing sequence of all transitions in the BTN. When analyzing transaction flows, FABT uses the notion of "bitcoin fluid" to track where the bitcoins passed through given addresses (called dyeing addresses) have flown and determine the extent to which each of other addresses is related to the dyeing address. The splitting, merging, and dyeing operators are used to capture the distribution of coins throughout transaction flows. In addition, FABT applies visualization techniques for further analysis of the suspicious addresses identified by the pattern matching.

We have applied FABT to the investigation of the Mt.Gox case according to the transfer pattern reported by WizSec (2015). The clues in the transfer pattern are formalized as a set of rules with respect to the features of transactions, addresses, and transaction flows. Our analysis resulted in 187 suspected gathering addresses. The visualizations of these addresses have also revealed that a subgroup of 16 addresses share many characteristics about the received/transferred amount, number of transactions, and time interval. Although these addresses are believed to be highly suspicious, verification of these addresses is beyond the scope of this paper.

The rest of this paper is organized as follows. Section 2 introduces related work. Section 3 presents the proposed framework. Section 4 describes formal modeling of bitcoin transactions. Section 5 focuses on analysis of bitcoin transactions. Section 6 presents the Mt.Gox case study. Section 7 concludes this paper.

2. Related work

Reid and Harrigan (2011) conducted temporal flow analysis, egocentric analysis and visualization of Bitcoin transactions based on the construction of a transaction network and a user network. Entities in the transaction network were formed by the clustering of multiple addresses via transactions with multiple inputs. External information from web sources was incorporated into the user network. Their method can track coins from a specified address and cluster addresses, but cannot indicate the strength of relationship between addresses. Tracking coins and calculating the strength of relationship between addresses are two functions of our proposed bitcoin fluid method. D. Ron and A. Shamir (Ron and Shamir, 2013) used the same clustering method to create a "contracted transaction graph". The statistical analysis revealed certain patterns and behaviors of large transactions that were possibly indicative of attempts to mask linkage. Their study focus on finding typical bitcoin spending/moving behavior features of bitcoin users by analyzing blockchain data, whereas our method is to find suspected addresses according to a defined transaction pattern. Fleder et al. (2015) also applied the clustering method with external information to tag entities and performed graph analysis. Their improvement is using PageRank to identify node importance. They do not address the question of finding suspected addresses by known information. Meiklejohn et al. (2013) used an additional clustering algorithm that clustered "change addresses". These addresses are created to collect changes when Bitcoins are sent during a transaction. As the "change address" is one of the transaction outputs, the initial address and the "change address" can be clustered together. BitIodine (Spagnuolo et al., 2014) is a framework for forensics analysis of Bitcoins, based on existing clustering heuristics in (Reid and Harrigan, 2011; Meiklejohn et al., 2013; Androulaki et al., 2013) in conjunction with data scraped from the web to create transaction and user graphs. It has been used to imply ownership of an address to the Silk Road and to find connections between Dread Pirate Roberts and an address. These address clustering methods can help to identity suspicious addresses. If address *a* is a known address that used to transfer stolen bitcoins, then the addresses in the same cluster with address *a* are suspicious addresses because they may belong to one user or group. However, address cluster methods only use transaction inputs and outputs information. Androulaki et al. (2013) demonstrated the effectiveness of behavioral analysis in blockchain transactions. Our method proposed 19 transaction features to defined transaction patterns, which can utilize various information of users' transaction behaviors.

Pinna et al. (2017) proposed an approach to Bitcoin analysis by creating Petri nets of Bitcoin addresses and address clusters. It focuses on the clustering of addresses that belong to a certain group or user with the use of external information to tag clustered addresses. It does not aim to find suspected addresses. In comparison, our paper exploits Petri nets as a formal model of bitcoin transactions in order to track bitcoin flow through specific addresses and find addresses of interest. Monaco (2015) proposed several transaction features, including hour of day, coin flow and input/output balance, to de-anonymize users from their transaction behavior over time. Harlev et al. (2018) used supervised machine learning to predict bitcoin cluster categorization. Our paper uses a more comprehensive set of transaction and address features for analysis.

Visualization methods have also been used for Bitcoin analysis. Moser et al. (Möser et al., 2013) utilized Bitcoin taint analysis and visualization to gauge the effectiveness of various mixing services. McGinn et al. (2016) focused on the use of large-scale transaction visualization and demonstrated patterns of money laundering, DDOS attacks, and potential application to the detection of transaction patterns such as tumbling and payment services. Battista et al. (2015) developed BitConeView, a bitcoin transaction visualization tool, and demonstrated a use case scenario to track Bitcoin money laundering in the experiments performed by Moser et al. (Möser et al., 2013). Bistarelli et al. (Bistarelli and Santini, 2017) created BlockChainVis, a tool for Bitcoin flow visualization with different filters and views to allow a user to capture visually interesting characteristics. Kondor et al. (2014) and Maesa et al. (Di Francesco Maesa et al., 2018) performed analysis of the topology of the Bitcoin network overall. Christin (2013) analyzed overall trends of users with regards to connections with illegal activity such as the Silk Road. Feder et al. (2017) analyzed the impact of security shocks (focusing on Mt.Gox in particular) on Bitcoin trade. Ron and Shamir (2014) tracked the flow of Bitcoins of Dread Pirate Roberts who ran the Silk Road. In our paper, visualization method is used as a tool for refining the formulation of bitcoin transaction patterns.

3. Overview of FABT

The problem of forensic analysis in FABT is formulated as follows: given the Bitcoin blockchain data and a set of clues of the case under investigation, including (input) bitcoin addresses (e.g., at which bitcoins were stolen or money laundering was started), we want to identify a set of (output) bitcoin addresses that likely held or still hold the bitcoins originally from the given input addresses. Similar to bank account numbers, addresses can be used to try to identify bitcoin owners. However, de-anonymization to find the owners of the suspicious bitcoin addresses is beyond the scope of this paper.

Fig. 1 presents the investigation workflow in our approach. First, we transform the bitcoin transactions in the given blockchain into a formal model, called bitcoin transaction net (BTN). As an extended form of safe Petri nets with well-defined semantics, BTN facilitates rigorous analysis of bitcoin transactions. We express clues as transaction patterns and extract information about the features involved in the transaction patterns by analyzing the bitcoin