BitVis: An Interactive Visualization System for Bitcoin Accounts Analysis

Yujing Sun, Hao Xiong
Department of Computer Science
The University of Hong Kong
Hong Kong, China
yjsun@cs.hku.hk, hxiong@hku.hk

Siu Ming Yiu
Department of Computer Science
The University of Hong Kong
Hong Kong, China
School of Computer Science and Technology
Harbin Institute of Technology (Shenzhen)
Shenzhen, China
smyiu@cs.hku.hk

Kwok Yan Lam
Department of Computer Science
Nanyang Technological University
Singapore
kwokyan.lam@ntu.edu.sg

***Abstract*—As an emerging payment method, bitcoin is receiving growing popularity for the different characteristics it shares with conventional fiat currencies. But the pseudonymous nature of bitcoin brings difficulties for regulators to effectively monitor bitcoin-related financial crimes. In this paper, we present an interactive system to visualize the relationship between bitcoin accounts, namely *BitVis*. With *BitVis*, users can easily filter transactions on demand, interact with the transaction networks to look for useful information, and analyze behavior of bitcoin accounts. Via *BitVis*, financial regulators can conveniently track suspicious accounts, while personal investors can easily investigate the activities of an interested account.**

***Keywords*-Bitcoin; transaction patterns; visualization;**

I. Introduction

Bitcoin, as a representative decentralized cryptographic currency, is famous for its pseudonymous property and irreversibility. However, it is difficult to regulate the bitcoin network effectively and efficiently. Although majority of people trade bitcoin for legal investment, criminals can take advantage of bitcoin for illegal financial activities, unavoidably influencing the ecosystem and discouraging the worldwide legalization process.

Indeed, bitcoin is not truly anonymous. The complete transaction information is recorded in the public ledger and the flow of bitcoins between different addresses can disclose their entities. In a recent work, Change and Svetinovic [12] found that transaction patterns can help to identify bitcoin ownership. Meanwhile, previous researchers explored the possibilities to track money laundering in the bitcoin ecosystem with the perfect knowledge of all transactions. Moser et al. [17] presented possible anti-money laundering strategies by taking advantage of the public transaction graphs and Ranshous et al. [18] proposed potential laundering patterns, short-think-bands (STBs), for further AML investigation. In a word, bitcoin transaction patterns can provide critical clues for bitcoin regulation.

Due to the large volume of bitcoin transactions, an interactive and effective visualization tool that could visualize transaction networks for users to investigate suspicious cases would be desired. In this paper, to facilitate fast and convenient account-based bitcoin activity analysis, we design and present an interactive system, *BitVis*, for users to visualize relationship between bitcoin addresses and transactions. To be clear, we refer a bitcoin acount to either a bitcoin address or a wallet of a group of addresses as in the WalletExplorer [9]. Given a suspicious bitcoin account, users can 1). Analyze its connections. Its relationship map and transaction patterns will be generated automatically with optimized layout and fulfilled filtering options. 2). Infer possible properties via jointly analyzing networks of associated accounts. 3). Explore the transaction history in temporal order within a specified period and check whether the general bitcoin market influences its behavior. 4). Interact with the system with mouse event, such as hovering, clicking, scrolling and dragging to adjust graph settings, change panel size and show graph/transaction/address detailed information.

II. Literature Review

A main category of bitcoin-related visualization aims at displaying information for demonstration purpose and thus cannot provide sufficient hints for account behavior analysis. Projects from many website, companies, and individuals fall in this category. TX HigherWay [4] and TX Street [8] use visualization for concept explanation. TX HigherWay [4] mimics the occurrence of live bitcoincore and bitcoincash transactions as moving cars on a high way for users to compare the two chains while TX Street [8] demonstrates the live bitcoin/bitcoincash transaction broadcasting as a person attempting to board a bus, facilitating customers to understand the principles of mempool and block size. Bitcoin transaction visualization [5], Daily Blockchain [7], Bit Listening [1], BitBonker [2] and Wizbit [10] all aim at visualizing live bitcoin transactions, but use different techniques. Bitcoin transaction visualization [5] adopts unconnected circles; Daily Blockchain [7] uses undirected graph; Bit Listening [1] represents transactions as bubbles; BitBonker [2] rednders 3D falling balls; And Wizbit [10] demonstrates the live transaction with locations on a 3D

978-1-7281-3669-1/19/$31.00 ©2019 IEEE
DOI 10.1109/CVCBT.2019.000-3

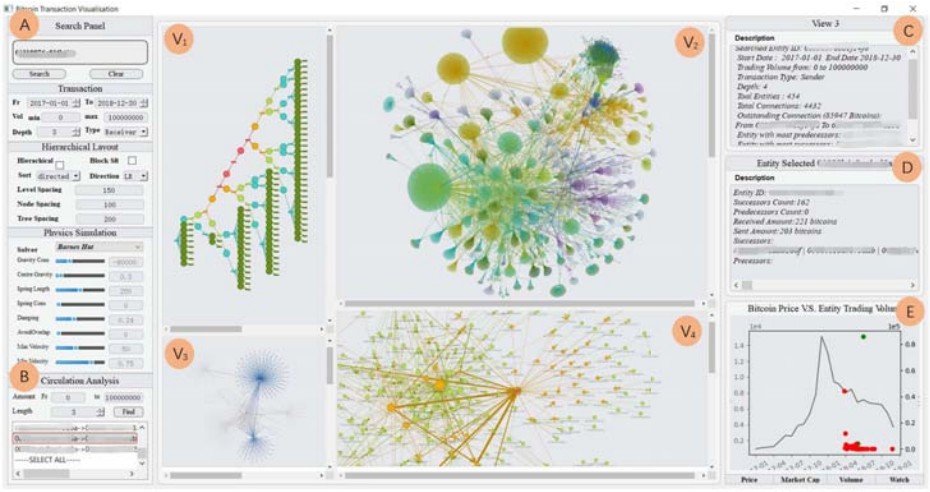


Figure 1: The interface of our *BitVis* visualization tool. (A) Search panel with various filtering options (B) Circulation Analysis (C) View Panel (D) Detail Panel (E) Temporal Display (V1-V4) Relation Explorer

globe. Moreover, the Bitcoin Big Bang [3] provides a gorgeous visualisation of the bitcoin historical data and the BitNodes [6] shows all the full nodes in the bitcoin network that are reachable at the moment. Despite the projects above present interesting and beautiful visualizations, they provide descriptive details only, which are insufficient for account analysis.

Recently, more advanced visualizations are proposed. Researchers attempted to directly visualize content on the block to detect abnormal activities and suspicious users, which normally contains no selected users. For example, Di Battista et al. [13] presented a Bitconeview system with flow charts to infer financial illegal behavior while Mcginn et al. [16] visualized abnormal patterns of transactions. Different from block-level visualization, we rely more on visualizing relationship to detect suspicious cases.

Additionally, a visualization of inter-exchange bitcoin behaviours has been proposed [19], which focused on visualize the trading between exchanges but cannot be used to investigate a particular non-exchange account.

There are also some works on visualizing user-defined bitcoin accounts [15], [14]. However, the previous researches [15], [14] on bitcoin accounts-oriented visualization can only display transactions of a particular account in temporal order but are unable to demonstrate the in-depth relationship between bitcoin accounts as our *BitVis*.

III. System Overview

Our system, namely, *BitVis*, contains a backend and a front-end. The back-end consists of data acquisition module, preprocessing module and storage module, while the front end is composed of an interactive visualisation module. *BitVis* crawls useful bitcoin information from Wallet Explorer [9], such as account ownerships and detailed transactions. Then the acquired data will then be reorganized, stored, processed, and visualized via the interface.

The visualization enables users to analyze behavior of interested bitcoin addresses, entities or transactions from different perspectives. An analysis could be triggered by abnormal transfers, theft, and so on. The system provides two types of graphs, transaction-centered graphs and entity-centered graphs. A user can simultaneously explore different networks of different interested addresses, interact with the graphs, and to view both general network information and specific detailed account/transaction information. One can also adapt graphical features of network, such as layout and physics simulation, and to filter the transaction data based on different conditions, including date, transaction volume, and transaction type. Additionally, users can easily investigate the temporal trading sequence of a searched account in the temporal display and possibly associate its trading behavior with macro bitcoin statistics, such as bitcoin price, overall trading volume and market capitalization.

To ensure efficient and effective, we avoid nodes overlapping and simplify the graphs as much as possible when generating the transaction patterns. Simultaneously, circulation analysis is embedded into the system for advanced pattern analysis.

The whole system is implemented with Python3.7 and PyQt 5.11 on a Windows machine. The Python libraries we used include BeautifulSoup 4.2, Vis.js and matplotlib. Relation database MySQL and graph database Neo4j are used for storage.

IV. Data Preparation

A. Entity Identification

In the research community of cybercurrency, address clustering is of great importance. To some extent, address

clustering can provide crucial clues of characteristics of account owners. Thus, beside address/transaction based analysis, users could be interested in exploring the trading patterns on an entity basis as well.

Currently, we use the clustering results by Wallet Explorer [9] for address grouping. Though the clustering by Wallet Explorer has exceptions caused by mixing services, it is the best open-sourced address grouping results we can find.

B. Data Acquisition and Storage

In our current implementation, bitcoin information is retrieved on demand. When an entity/transaction identifier is entered to the frontend, it will be searched in the storage module. If the identifier is found, the related information will be sent back for further processing and visualization. Otherwise, our web spider will retrieve all the information of the interested identifier on Wallet Explorer [9]. The design of data acquisition to retrieve data on demand can save the downloading time as well the disk space.

Our storage module contains a relation database as well a graph database. The relation database is used to store the detailed information of entities and transactions while the graph database can provide more efficient relationship query than relationship database, benefiting the pattern analysis procedure in our system.

V. Visual Design

Generally, the visualization module of our *BitVis* system contains four modules, namely, search panel, relationship explorer, description panel and temporal display. In order to provide users with an effective, interactive and user-friendly application for bitcoin behavior analysis, we follow three main principles: 1). **User-centered design.** Considering inexperience users, the system is intuitive to use to minimize the learning time, while, at the same time, experts can tackle complicated problems. 2). **Easy visual comparison.** As indicated by [11], it is more convenient to compare abreast views that the ones in memory. Therefore, our system supports multi-view exploration. 3). **User-friendly interaction.** Due to the limited space, it is impossible to show all the detailed information on the screen. Thus, general information is shown first, and details are displayed on demand. Various interactive methods are implemented to fulfil different requirements.

A. Search panel

The search panel in fig. 1 (A) is the main entrance of our system. User can insert an interested entity/address/transaction identifier to retrieve the transaction graphs. Meanwhile, different options for transaction, layout, and graph simulation are provided to improve the visualization.

B. Relationship Explorer

Our relationship explorer intends to offer help for users to visualize inter-accounts behavior via transaction pattern analysis and to understand the potential connections between entities. The multi-view design enables visual analysis of different networks at the same time. When another transaction/entity of interest is found in the current view, its egocentric graph can be shown side by side with previous searched graphs.

Based on the type of the input identifier, the relationship network can be divided into transaction-based graphs and entity-based graphs. In a transaction-based graph, transactions are represented by rectangular node and entities are denoted as circular node. A directed edge can connect nodes of different types, either from transaction to entity or from entity to transaction, indicating the flow direction of bitcoins. Therefore, a complete transaction consists of an input circular entity node, a rectangular transaction node and an output circular entity node. An example of a transaction based graph is shown in fig. 1 (V1). While an entity-based graph reflects the relationship network between entities. In such a graph, different circles represent different entities. A directed edge from entity A to entity B indicates that there are transactions from A to B, the width of which denotes the total trading volumes. The graphs in fig. 1 (V2, V3, V4) are all entity-based graphs. Our node-link based graph design can take advantage of the limited screen space and is user-friendly for analysis.

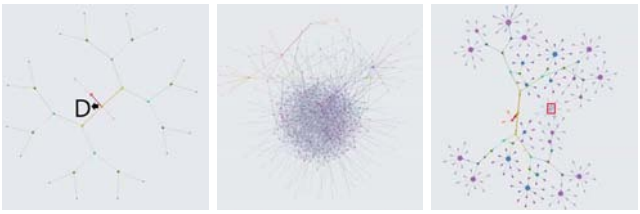
Simultaneously, various interactive functions are embedded to offer useful graph navigation. On one hand, detailed entity and transaction information will be shown on mouse clicking. On the other hand, The size, scale, location, and layout of graph can be easily justified with mouse scrolling, dragging and selecting.

1) Circulation Analysis: is supported in our system. Users can easily retrieve bitcoin circulations in a graph by specifying the range of trading volume and length of the circulation. An exemplary circulation analysis is demonstrated in fig. 1 (V3). The entities that are involved in a selected circulation (marked with red box in fig. 1 (B)) with $length = 3$ as well as the related connections are coloured blue while other entities and connections are greyed out.

C. Description Panel

The description panel consists of two components. One is the *view panel* (fig. 1 (C)), displaying the general information and quantified indices of the selected view and the other is the *detail panel* (fig. 1 (D)), demonstrating the information of the selected identifier.

1) View Panel (VP) : When user selecting a view, VP will first display the filtering options in generating the corresponding graph. Then, quantified indices of the graph, including the total number of connections and the total number of entities, as well as qualitative measures such as



(a) d = 6, v $>$ 10 (b) d = 9, v $>$ 10 (c) d = 9, v $>$ 500

Figure 2: Case study of a silk road-related account. Node size, node color and edge width represent the number of the successors, depth and the total trading volume, respectively. The red node encodes the investigated entity β. Please zoom in for details.

entities with most predecessors, entities with most successors and outstanding connections, will be displayed.

2) Detail Panel (DP) : In both an entity-based graph and a transaction-based graph, DP will display detailed informtion of the selected component whenever an entity/connection/transaction is clicked.

D. Temporal Display

1) Historical Trend: The historical trend (the 2d line chart in fig. 1 (E)) provides a comprehensive overview of historical bitcoin statistics, including price, trading volume and market capitalization, which reflects the evolution of Bitcoin. The 2D line charts of price, volume and market capital will be shown accordingly by clicking the corresponding buttons at the bottom.

2) Temporal Transactions of An Entity: When the 'watch' tablet is selected, the temporal transactions of the selected entity will be displayed in the same figure with historical trend, sharing the time x-axis. The left y-axis and the right-y-axis of the figure represent bitcoin statistics (price/market cap/volume) and entity's trading volume, respectively. A red dot encodes that the entity received bitcoins while a green dot encodes that the entity sent bitcoins. Temporal display integrates the visualization of temporal transaction behavior of a bitcoin entity with that of the bitcoin trading environment. Please refer to fig. 1 (E) for a visual demonstration of temporal display.

VI. Evaluation

In this section, we demonstrate how to use this system for bitcoin behavior analysis with a case study. For privacy protection purpose, we will hide the accounts information.

A. Silk Road

We invited a domain expert X to analyze the silk road related entity β to detect suspicious entities with the assistant of our system.

Expert X easily located an outstanding transaction by looking at β's 1-ring neighbors, in which $11,1114$ bitcoins are transferred to entity D (fig. 2a). By checking the timeslot when the transaction occurred in the temporal display, expert X found that the transaction was confirmed on March 2014, which was after the date when the FBIs took actions, indicating the it is true the the private keys of silk road accounts are managed by other people.

Then, by gradually checking 1-ring neighbors to 5-ring neighbor (increasing the value of $depth$ from 2 to 6 fig. 2a), expert X observed that the silk-road related entity kept decomposing the bitcoins into small values and distributing them into different accounts. However, when $depth > 6$, the entity network becomes complicated and it is difficult to locate suspicious behaviours (fig. 2b). Then, expert X attempted to focus on transactions with big trading volume by set the minimal value of transaction volume to 500 and retrieved a simplified graph (fig. 2c).

In fig. 2c, expert X observed that most 7-ring neighbours have no successors except one marked with a red box. Interesting, this entity is also attracted to the center of the network for its multiple connections with nodes from different branches. After checking the details of this node in the description panel, expert X found that this entity is still trading actively at present. Expert X believes that this entity is probably actively involved in illegal activities and that regulars should watch the entity closely.

Definition 1. ***D-ring neighbors.*** *An account trades with a set of other accounts, each of which has its own trading accounts, and so forth. We say that two accounts are connected if a transaction between the two accounts exist. If denoting an account as A, a D-ring neighbor of A is an account B that are indirect connected to A through $D-1$ intermediate accounts.*

VII. Limitation and Future Work

When a graph gets quite complicated such as fig. 2b, it is difficult for users to get useful clues, which is a limitation of this system. We plan to extend this work by restricting the nodes number of a transaction graph to show important nodes only.

VIII. Conclusion and Limitations

In this paper, by integrating data collection module, data storage module, and data visualization module, we present a *BitVis* system to analyze behavior of arbitrary entities/accounts/transactions. We hope that our system can offer help to users with different objectives, including regulators, investors, as well as researcher to perform the analysis procedure in a more convenient manner.

ACKNOWLEDGMENT

This project is supported by Collaborative Research Fund (CRF) of RGC, Hong Kong (C1008-16G).

REFERENCES

[1] "Bit listen," https://www.bitlisten.com/, accessed: 2019-02-16.

[2] "Bitbonkers," https://bitbonkers.com/, accessed: 2019-02-15.

[3] "Bitcoin big bang," https://www.elliptic.co/, accessed: 2019-02-15.

[4] "Bitcoin cash vs bitcoin core transaction visualizer," https://txhighway.com/#, accessed: 2019-02-16.

[5] "Bitcoin transaction visualization," http://bitcoin.interaqt.nl/, accessed: 2019-02-15.

[6] "Bitnodes.earn.com," https://bitnodes.earn.com/, accessed: 2019-02-15.

[7] "Daily blockchain," http://dailyblockchain.github.io/, accessed: 2019-02-16.

[8] "Txstreet.com," https://txstreet.com/, accessed: 2019-02-16.

[9] "Walletexplorer.com: smart bitcoin block explorer," https://www.walletexplorer.com/., accessed: 2019-02-15.

[10] "Wizbit," https://blocks.wizb.it/, accessed: 2019-02-15.

[11] A. Barsky, T. Munzner, J. Gardy, and R. Kincaid, "Cerebral: Visualizing multiple experimental conditions on a graph with biological context," *IEEE transactions on visualization and computer graphics*, vol. 14, no. 6, pp. 1253–1260, 2008.

[12] T.-H. Chang and D. Svetinovic, "Improving bitcoin ownership identification using transaction patterns analysis," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, no. 99, pp. 1–12, 2018.

[13] G. Di Battista, V. Di Donato, M. Patrignani, M. Pizzonia, V. Roselli, and R. Tamassia, "Bitconeview: visualization of flows in the bitcoin transaction graph," in *Visualization for Cyber Security (VizSec), 2015 IEEE Symposium on*. IEEE, 2015, pp. 1–8.

[14] P. Isenberg, C. Kinkeldey, and J.-D. Fekete, "Exploring entity behavior on the bitcoin blockchain," in *Posters of the IEEE Conference on Visualization*, 2017.

[15] C. Kinkeldey, J.-D. Fekete, and P. Isenberg, "Bitconduite: Visualizing and analyzing activity on the bitcoin network," in *EuroVis 2017-Eurographics Conference on Visualization, Posters Track*, 2017, p. 3.

[16] D. McGinn, D. Birch, D. Akroyd, M. Molina-Solana, Y. Guo, and W. J. Knottenbelt, "Visualizing dynamic bitcoin transaction patterns," *Big data*, vol. 4, no. 2, pp. 109–119, 2016.

[17] M. Möser, R. Böhme, and D. Breuker, "An inquiry into money laundering tools in the bitcoin ecosystem," in *2013 APWG eCrime Researchers Summit*. Ieee, 2013, pp. 1–14.

[18] S. Ranshous, C. A. Joslyn, S. Kreyling, K. Nowak, N. F. Samatova, C. L. West, and S. Winters, "Exchange pattern mining in the bitcoin transaction directed hypergraph," in *International Conference on Financial Cryptography and Data Security*. Springer, 2017, pp. 248–263.

[19] X. Yue, X. Shu, X. Zhu, X. Du, Z. Yu, D. Papadopoulos, and S. Liu, "Bitextract: Interactive visualization for extracting bitcoin exchange intelligence," *IEEE transactions on visualization and computer graphics*, vol. 25, no. 1, pp. 162–171, 2019.