BitAnalysis: A Visualization System for Bitcoin Wallet Investigation

Yujing Sun, Hao Xiong, Siu Ming Yiu, *Member, IEEE*, and Kwok Yan Lam

Abstract—Bitcoin is gaining ever increasing popularity. However, professional skills are required if people want to check bitcoin transaction information from the blockchain. As pointed out in a recent study, there is a lack of tools to support effective interactive investigation of bitcoin transactions. Therefore, we present a novel visualization system, *BitAnalysis*, for interactive bitcoin wallet investigation. The analytical and visualization functions of *BitAnalysis* are defined and developed by following the advice and requirements of a group of entrepreneurs and regulators of bitcoin-related business. *BitAnalysis* provides a rich set of functions and intuitive visual interfaces for the users, such as law-enforcement officers and regulators, to effectively visualize and analyze the transactions of a bitcoin wallet (i.e., a cluster of bitcoin addresses) and its related wallets, to track the flow of bitcoins, and to identify wallet correlation using our novel clustering functions. To achieve these functions, we have designed new visualization techniques for presenting bitcoin transactions information and introduced the *connection diagram* and *bitcoin flow map* as new ways of analyzing, tracking and monitoring the trading activities of a cluster of closely related wallets. We also present an extensive user study that validated the effectiveness and usability of *BitAnalysis*.

Index Terms—Bitcoin, FinTech, transaction data, visualization

1 Introduction

At the first, bitcoin was invented by Satoshi Nakamoto in 2008 as a payment method that people would use to make purchases through bitcoin transactions, which has become a reality. For example, people routinely purchase daily necessities with bitcoins as a means to fight inflation in Venezuela. With the tremendous increase in adoption of bitcoin for transactions, there is a corresponding increased demand to monitor and analyze bitcoin transactions, either for investment or for criminal investigation. The goal of the present paper is to meet this demand by developing a complete interactive system for intuitive visualization and effective analysis of bitcoin transactions. Note that a person, also called an *entity*, can possess multiple bitcoin addresses, like the way a person has multiple bank accounts. To be clear, in this paper, we refer a wallet w to be a collection of addresses clustered by Wallet Explorer [2] as owned by the same entity and a *trader* of w to be any wallet that have transactions with w.

Although bitcoin wallets and bank accounts are similar, they are different in terms of anonymity. As centralized institutions, banks know the owner identity of every bank account in the world using fiat currency. When a conventional financial transaction occurs, such as a wire transferring or a credit transferring, the Know-Your-Customer (KYC) principle must be strictly enforced so that customer identities are validated. This allows banks to conveniently monitor and investigate bank accounts, reducing the risk of having transactions with untrustworthy people.

In contrast, bitcoin is designed to be pseudonymous. In the world of bitcoin, no centralized institutions exist to check and validate the identities of the owners of bitcoin wallets. Therefore, no one knows the true identity of a bitcoin owner. This anonymity brings about a difficulty for both parties of a bitcoin transaction – We do not know whether we are trading with a dishonest company, a con man or a criminal in money laundry business. So in practice, for exchanging bitcoins with other individuals/institutions or making a purchase using bitcoin, checking the attributes of a bitcoin wallet in question is the only way to minimize the risk of trading with "bad guts".

Indeed, due to the anonymity and decentralization, criminal organizations are naturally interested in using bitcoin for settlement. The last step of a crime is often accomplished by the transaction of money. Hence, governments all over the world find it necessary to monitor and analyse suspicious bitcoin transactions and the associated wallets. Intuitive software tools for wallet investigation are therefore important for regulators.

Despite the anonymity of bitcoin ownership, there are certain trading patterns that can be used to characterize the behaviour of the unknown entity. For example, a newly founded company should have only a limited number of transactions, small businesses normally should not have transactions with a large bitcoin volume, and entities intentionally hiding the origins of their bitcoins are likely

- *Yujing Sun, Hao Xiong, and Siu Ming Yiu are with the Department of Computer Science, University of Hong Kong, Hong Kong. E-mail: 1990tangtang@gmail.com, xionghao0011@126.com, smyiu@cs.hku.hk.*
- *Kwok Yan Lam is with the Department of Computer Science, Nanyang Technological University, Singapore 639798. E-mail: kwokyan.lam@ntu.edu.sg.*

Manuscript received 10 January 2022; revised 27 June 2022; accepted 30 June 2022. Date of publication 5 July 2022; date of current version 14 March 2023. This work was supported by the HKU-SCF FinTech Academy, the University of Hong Kong.
(Corresponding authors: Yujing Sun; Siu Ming Yiu.)
Recommended for acceptance by R. Hong.
Digital Object Identifier no. 10.1109/TBDATA.2022.3188660

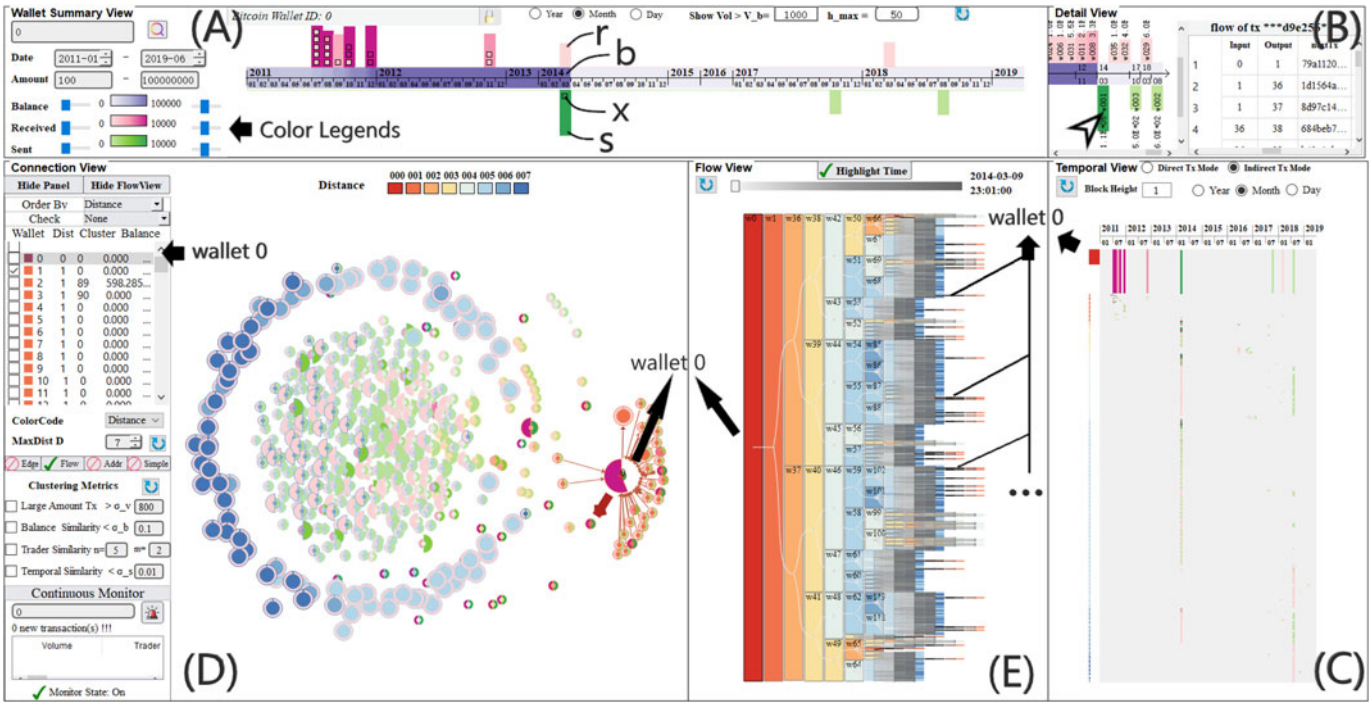


Fig. 1. The interface of *BitAnalysis* system. (A) The summary view summarizes the transactions of an interested wallet w. (B) The detail view shows user-selected wallet/transaction details. (C) The temporal view enables wallet temporal analysis. (D) The connection view facilitates wallet connection analysis. (E) The flow view visualizes a user-selected bitcoin flow. Wallet 0 is highlighted simultaneously in different views. Note that in this paper, we hide the original wallet ids and use regenerated ids instead to protect privacy.

involved in illegal activities. Our *BitAnalysis* system explores these traits for effective analysis in bitcoin transaction investigation.

There have been active studies and software systems for bitcoin-related query and examination [3], [4], [5], [6], [7], [8], [9]. Among the existing works, there are only two online systems that are commonly used for exploration of individual bitcoin addresses/wallets – Wallet Explorer [2] and Blockchain.info [10]. However, both systems are only for primitive data query as they only display transaction records in a list format without an intuitive visualization or summarization, and support no high-level summary, analysis, or interactions. When using such a system to investigate a bitcoin wallet involved in many transactions, it becomes very onerous to trace all the transactions: One has to keep clicking on the next button to view pages after pages of transactions shown in lists of numerical values.

More recently, wallet-based visualizations were studied in [9], [11], [12], [13]. However, these methods cannot demonstrate the complex relationship among trading wallets with intuitive visualizations. As pointed out by a recent review on existing online bitcoin visualization tools [1], there is a stark lack of effective visualization and analysis tools that allow the user to easily and interactively investigate bitcoin transaction data for various potential users.

A bitcoin wallet under investigation can be involved in thousands of transactions in a short period of time. It is therefore a challenging task to develop a visualization and analysis system for bitcoin wallet investigation that is capable of visualizing all the involved transactions, related wallets and activities in a clear, ordered, and efficient manner. To understand the requirements for the functions of such an interactive visualization system for bitcoin wallet analysis, we have conducted interviews with numerous bitcoin experts, entrepreneurs in cryptocurrency, and regulators investigating bitcoin-oriented money laundering. Based on these interviews, we summarize the requirements as follows: (1) visually intuitive browsing of wallet summary; (2) efficient analysis of transactions patterns; (3) tracking of bitcoin flows; and (4) continuous monitoring of suspicious transactions.

We have designed and developed our *BitAnalysis* system base on these requirements. The main interface of *BitAnalysis* is shown in Fig. 1. *BitAnalysis* facilitates bitcoin wallet investigation by providing the following functions: (1) Easy browsing and visualization of a wallet summary from different perspectives, such as the top trading wallets, period of peak trading activities, balance variations, etc; (2) Visualization, analyzing and clustering wallets based on transaction patterns; (3) Tracking how bitcoins flow between wallets; and (4) Monitoring interested wallets in real time and alerting the user to new suspicious transactions.

We have conducted a user study to validate the efficacy of the system *BitAnalysis* . 15 participants have been recruited. Among whom, five have helped us perform the needs assessment. The user study strongly indicates that our system meets the requirements of the domain experts. The details of the user study will be discussed in Section. 9.1.

Our contributions are summarized as follows:

- We present a visualization system,*BitAnalysis*, for bitcoin wallets analysis. This system facilitates efficient wallet preview, new transactions alerting, wallets analysis and bitcoin flow tracking. Interactive functions are also provided to assist the wallet investigation procedure.

- We present a novel connection diagram to demonstrate the connections between wallets as well as design several clustering methods based on bitcoin characteristics. These methods can be used to identify wallet similarity and infer wallet ownership.
- We present a novel flow map to clearly trace and visualize bitcoin flows among a cluster of related wallets.

We provided an accompanying video in the supplementary materials to help illustrate the visualization functions of *BitAnalysis* .

2 Related Work

2.1 Bitcoin Analysis

With the wider spread of bitcoin, researchers have a stronger interest in its economic impact, potential risks, and technological limitations. Bitcoin related researches appear across various disciplines. The topics range from bitcoin property [14], anomaly detection [15], [16], [17], [18], regulation [19], [20], privacy analysis [21], [22], to trend prediction [23], [24]. However, most of the existing works on bitcoin analysis focused on the macro characteristics of bitcoin. On the contrary, our system aims at assisting exploration and investigation of specific bitcoin wallets.

We also observe that an important category of researches on bitcoin analysis relies on transaction pattern analysis. Moser *et al.* [17] provided a systematic inquiry on evaluating bitcoin as a money laundering tool and presented outlines of anti-money laundering strategies based on bitcoin transaction information. Reid and Harrigan [25] analysed the anonymity of bitcoin by investigating bitcoin flow. Ranshous *et al.* [26] constructed directed hyper-graphs of exchange-centred transactions to understand potential money-laundering behaviour. Most recently, Wu *et al.* [27] proposed a bitcoin transaction network analytic method for facilitating Blockchain forensic investigation based on an extended safe Petri Net. Our system also provides transaction pattern analysis. But note that the existing works mentioned above mainly focus on the analytical process of network patterns rather than visualization capabilities to facilitate the analysis.

2.2 Bitcoin Visualization

A main category of bitcoin-related visualizations aims at displaying information for demonstration purpose [3], [4], [5], [28], [29], [30], [31], [32], [33]. TxhighWay [28] and TxStreet [31] intend to educate people about the mechanism of bitcoin blockchain; Bitbonkers [3], BitTxVis [4], BitListen [5], daily blockchain [29] and WIZBIT [30] mimic the real occurrence of bitcoin transactions; Bitnodes [32] estimates the relative size of the bitcoin peer-to-peer network by finding all of its reachable nodes. Meanwhile, bitcoin big bang [33] shows the emergence over time of the largest entities on the Bitcoin blockchain, and their interconnectivity. Despite the interesting and vivid visualizations shown, the above works do not provide adequate interactive visualization and analytical functions for analysis purpose.

Recently, analysis-oriented visualization becomes an active research direction. Christin *et al.* [34] investigated Silk Road related data via a comprehensive measurement analysis. Battista *et al.* [7] and McGinn [8] provided block-level visualizations for anomaly detection. Bistarelli [35] presented to find specific transactions or addresses with customizable filters. Besides, Kondofr *et al.* [36] and Maesa *et al.* [37] proposed to analyse the overall bitcoin transaction network by measuring the network characteristics and visualize the results. Meanwhile, a visualization for analysing inter-exchange behaviour has been proposed as well [6]. More recently, Zhong *et al.* [9] proposed a SilkViser system to visualize cryptocurrency transaction data from the blockchain perspective.

Our *BitAnalysis* are different from the above works from different aspects. SilkRoadTravel [34] only focused on the specific silk road analysis, but *BitAnlaysis* is design to support custom wallet analysis. BlockChainVis [35] proposed predefined filters to filter out undesired information for transactions visualization while we emphasize on wallet relationship analysis and find out their relevance. Different from block-based anomaly detection [7], [8], we rely more on visualizing transaction patterns for analysis. Different from overall blockchain visualizations from the macro perspective [36], [37], we aims at bitcoin investigation from the micro perspective. Compared with the exchanges-oriented visualization [6], our *BitAnalysis* can be applied to analyse wallets not limited to those belonged to exchanges. Though SilkViser [9] also visualized transaction data, it focused on demonstrating transaction data on a block-basis rather than emphasizing the relationship analysis between wallets as our *BitAnalysis* . In Addition, comparing to the existing wallet-based visualizations [11], [12], *BitAnalysis* can facilitate wallet analysis from the temporal dimension as well as the relationship dimension, providing more advanced investigations.

2.3 Network Visualization

Network visualization is another related area which has been actively studied. In [38], Heer and Boyd used a node-link diagram to represent the relation between end-users in online social networks. Wang and Mueller [39] visualized causal networks with path diagrams. Christina *et al.* [40] adopted a Sankey diagram to visualize dynamic network for data journalists. Besides layout design, researchers also attempted to adopt different technologies to better illustrate a network. Some previous works [41], [42] used edge bundling to simplify a graph. Wang *et al.* [43] proposed a visual technique to reveal ambiguities. Langevin [44] presented a visual analytical approach to leverage cluster computing by retrieving hierarchical communities from the input data. However, despite of the exist techniques, a network will be hardly readable with increasing complexity. Therefore, we design a connection diagram to adaptively visualize transaction network and a flow map to clearly show the bitcoin flows between wallets.

2.4 Community Detection

In network analysis, an important topic is community detection. Duch and Arenas [45] took advantages of extremal optimization. Yang *et al.* [46] made use of node attributes. Pizzuti [47] proposed a genetic-based approach to detect communities in social networks. More recently, community detection for multi-layer networks has begun to emerge. Wilson *et al.* [48] presented a multilayer extraction procedure

which could identify densely connected vertex-layer sets in multiplex networks. Li *et al.* [49] designed a random walk based LART (Locally Adaptive Random Transitions) algorithm to discover communities in a multi-layer network. Clustering is also important for our system to measure wallet similarity. However, the existing clustering strategies cannot be applied directly to bitcoin analysis. Therefore, based on the features of bitcoin, we design specific metrics for bitcoin wallet clustering.

2.5 Visual Analysis of Financial Data

Although bitcoin is different from fiat currency, research on visual analysis of traditional financial data is also relevant to our work.

Anomaly detection is known as financial fraud detection. Fraud investigators have realized that visualizations are very helpful for anomaly detection and various visualization techniques have been developed to help solve the problem. Kirkland *et al.* [50] proposed an ADS system on financial anomaly detection by combining the visualization techniques as well as the AI techniques. Based on a set of predefined keywords, Chang *et al.* [51] presented a WireVis system to facilitate banks to discover abnormal wire transactions. Huang *et al.* [52] designed a framework of visual analysis for stock market security, with a 3D tree-map to monitor the real time stock market and a node-link network to discover unusual trading pattern. Leite *et al.* [53] implemented a visual analytic approach (EVA) to help financial institutions conduct fraud transaction detection.

Correlative analysis can bring new insights for investors, analysts and financial institutions. Marketanalyzer [54] presented an interactive system for market and competitor analysis, providing side-by-side comparisons for sales, trends, and growth rates. Malik *et al.* [55] proposed a visual analytical approach to explore spatial-temporal correlations. Badam *et al.* [56] presented a system, Timefork, for prediction of multivariate time series data. Note that most traditional financial visual analysis, using macro financial data for macro analysis, are quite different from our work.

3 Needs Assessment

In order to develop a visualization system that is useful for practical bitcoin transaction investigation, we conducted interviews with bitcoin experts, entrepreneurs and regulators. Among the interviewees, one was the former CTO of a national Stock Exchange, one is an executive of a world-leading Cryptocurrency Exchange, one is a senior researcher specialized in cryptocurrency and financial technology, and two are police for cyber security crime. According to their feedbacks, we summarize the following needs:

T1. Quick wallet overview. The entrepreneurs are interested in the trading activities of the wallet that they will trade with, including active trading periods and top trading wallets, etc. They stated that they would pay more attention if unusual behaviours are detected, such as transactions of unusually large volume, or wallets trading with those wallets known to be unwanted. Therefore, it is important to provide a quick wallet overview. They complained that the well-known websites for bitcoin wallet query, including Blockchain.info [10] and Wallet Explorer [2], display transactions of a wallet in an unintuitive manner, using a list format. Our interviewees overall wish to use a system that can provide a visual and intuitive summary of transaction information.

T2. Detail examination. The interviewees suggest that an effective system should enable them to check detailed information when necessary. For example, when there are many transactions occurring in one month, the user wants to browse the transaction summary as well as to view the details of some of the transactions if needed.

T3. Transaction pattern analysis. What regulators are concerned most about is whether wallets directly or indirectly trading with a criminal's wallet w are suspects as well. However, regulators are unable to confirm the identity information of wallets as they can do for bank accounts. Therefore, transaction pattern analysis becomes the only way to identify such suspicious wallets. A typical situation is that when a criminal organization is destroyed, the police can only acquire the IDs of a limited number of bitcoin wallets but need to know whether related wallets of a suspicious w is suspect as well. Meanwhile, entrepreneurs also point out that understanding partners is a key rule in business. Examining the transaction pattern of business partners' wallet w is the best way to know about their partners.

a). Connection analysis. Transaction patterns of w can be treated as the network of wallets trading with w directly or indirectly. Both regulators and entrepreneurs desire to make use of this network to analyze wallet connections. Also, they hope the system could provide metrics that can automatically detect characteristic transaction patterns to facilitate the investigation process.

b). Temporal analysis. The interviewees are also interested in whether two wallets have the similar transaction pattern in the time dimension, that is whether they are active during the same specified period. Both regulators and experts believe that the similarity in trading periods is a key clue to find suspicious wallets related to a suspicious w. The system should support checking temporal trading activities of wallets related to w simultaneously.

T4. Bitcoin flow tracking. Meanwhile, both regulators and entrepreneurs concern about dirty bitcoins, that were ever possessed by criminals: Regulators focus on where the dirty money went to while entrepreneurs do not want to receive dirty bitcoins. Since every bitcoin keeps the log file about who has previously owned it, the interviewees hope to clearly visualize the bitcoin flow among wallets. In Wallet Explorer [2], the flow of bitcoin is kept in a format of linked URLs. In such a way, the user can only see one transaction at a time, which does not provide an overall view of the sequence of transactions for a good understanding of bitcoin flow. Hence, there is a need for a more convenient way to track bitcoin flows among wallets.

T5. User-friendly interactions should be provided to make the investigation procedure easy and efficient.

T6. Real time monitoring. All the interviewees want to be alerted when new transactions happen to an interested wallet so as to keep being updated about its status.

4 System Overview

Design challenges. During the design and implementation of our system, a main challenge comes from the huge amount

of transaction information, resulting in complicated wallet relationship and bitcoin flows. Hence, it is important to have a design that balances between high-level overviews and detailed information of involved wallets and transactions. The design should also support quick overview of a wallet, related transaction patterns, and user-selected bitcoin flows, as well as to support essential detailed examination when needed. Furthermore, we also need to present the transaction pattern clearly and to demonstrate a user-selected bitcoin flowing intuitively, even when a large number of wallets and transactions are involved.

System outline. To accomplish the tasks formulated in Section. 3, we have designed and developed a system, *BitAnalysis* , which is composed of a front-end module for visualization (Fig. 1) and a back-end module for bitcoin data representation and management. The bitcoin data representation and management module stores wallets and transactions information while the front-end assists with wallet investigation by visualizing the information of a user-selected wallet or bitcoin flow. Please refer to the supplemental material for a video demonstration of our system.

BitAnalysis system is implemented on a DELL window machine with Intel Core i7-11700, 64 GB DDR4 2933 MHz and GTX1080Ti GPU. Under most situations, the user spends about 5-30 minutes in investigating an interested wallet.

4.1 Bitcoin Data Representation and Management

We collect data from Wallet Explorer [2] to build up the SQL Server storage module. The data storage consists of a wallet database and a transaction database. The *transaction database* records information of each transaction. Meanwhile, to assist bitcoin flow tracking, it keeps the next transactions of each transaction where the bitcoins went to. The transaction database records each transactions' original transaction ID, timestamps (when it happened), input wallet ID, output wallet IDs, bitcoin amount, and next transaction IDs. The *wallet database* maintains the statement of each wallet, which records transaction IDs it was involved and the corresponding balances afterwards.

4.2 Design Principles

We follow the following principles when designing our system:

P1. Overview first and details on demand. A wallet can involve many transactions and traders. Meanwhile, the transaction pattern and bitcoin flows can be very complicated. To adapt to this complexity, our system provides an overview first and supports detail examination when necessary.

P2. Different views are responsible for different tasks but they cooperate when necessary. To make the functionalities clear to the user, we use different views for different tasks. Besides, cross-view interactions are integrated to facilitate investigation that cannot be done within a single view.

P3. Make parameters user-adjustable. The difference between wallets can be huge. For example, the maximum amount of bitcoins of a transaction may be 10 in one wallet and 10000 in another. So we allow the user to adjust some key parameters for the best visualization effects, depending on the complexity of the data involved. Meanwhile, the parameters are all set with reasonable initial default values, allowing wallet investigation without parameter fine-tuning in common cases.

P4. Intuitive visual designs. The target users of this system may have little experience with visualization systems. Therefore, we strive to make the system functions easy to use and the visualization interface intuitive to help the user better understand the data displayed.

4.3 Visualization Interface

Interface overview. The main interface (Fig. 1) of *BitAnalysis* contains three fundamental views and two advanced views. The fundamental views are the *summary view* (A), the *detail view* (B), and the *temporal view* (C). The advanced views are the *connection view* (D) and the *temporal view* (E). Here A, B, C, D and E refer to the views in Fig. 1.

- A The summary view summarizes the transactions of an interested wallet w.
- B The detail view shows user-selected wallet/transaction details.
- C The temporal view enables wallet temporal analysis.
- D The connection view facilitates wallet connection analysis.
- E The flow view visualizes a user-selected bitcoin flow.

Workflow of bitcoin investigation. One starts investigating a wallet w by entering its ID in the summary view, with a specified time period (t_s, t_e), and a transaction amount range (v_{min}, v_{max}). Then, *BitAnalysis* will enquire the database to retrieve related transaction and wallet data, to generate the summary, connection and temporal views. The user can then investigate the wallet w and choose to monitor a wallet related to w if needed. Also, when the user selects to track an interested flow, relevant data will be retrieved from the transaction database to generate the flow view.

5 Fundamental Views

In this section we will introduce the fundamental views, laying the foundation for introducing the advanced views in the following sections.

5.1 Summary View

A wallet w can have plenty of transactions, making it inconvenient for the user to go through one by one. Hence, it is important that the user can browse the transaction summary first and focus on details of transactions and traders occurring during more interested periods when necessary. Besides, the user may want to check the transaction summary from the perspective of traders. For example, wallets trading with a given wallet w with a large amount of bitcoins are more important than those with a small amount of bitcoins. Such summarized information is hard to collect in lists provided by Wallet Explorer [2] and BlockChain.info [10]. Therefore, a summary view (Fig. 1 A) is provided to visualize aggregated trading activities. (*T1*)

Main Features. Based on the feed-backs from the needs study (See Section. 3), we identify and visualize four types of information important for characterizing a wallet w: (1) outgoing transactions from w; (2) incoming transactions to

w; (3) traders; and (4) balances. The summary view is designed to aggregate and visualize these four kinds of information clearly in a compact manner.

Visual Design. Specifically, we aggregate transactions in a user-specified time period, such as day, month and year. Then the aggregated transactions in each period are shown in the temporal order, which are displayed by a combination of a vertical incoming transactions bar (r in Fig. 1), a vertical outgoing transaction bar (s in Fig. 1), a horizontal balance bar (b in Fig. 1), and a number of wallet blocks (x in Fig. 1). The incoming (outgoing, resp.) transaction bar represents the aggregated incoming (outgoing, resp.) transactions in the time period. The height and colour of the bar encode the total amount of bitcoins received (or sent). The balance bar shows the balance changing during the corresponding time period, with colour encoding wallet balance. Simultaneously, wallet blocks encode those traders (wallets) that trade with w an amount of bitcoin greater than a user-specified threshold v_b during the specified period.

Bar Height Normalization. The height of an incoming/outgoing transaction bar encodes the total incoming/outgoing bitcoin amount within the corresponding time period. Since trading bitcoin amounts can vary dramatically, we choose to use a logarithmic function instead of linear functions to compute height of transaction bars. Specifically, given a trading bitcoin amount v, the height $h(v)$ of the corresponding transaction bar is computed as

$$h(v) = \frac{log(1+v)}{log(1+v_{max})} \cdot h_{max} \quad (1)$$

where h_{max} is the user-defined max height of a transaction bar and v_{max} is the maximum received/sent bitcoins.

Bar Colour Encoding. We use three colour schemes, which are colour-blindness-safe, print friendly and photocopy safe, to encode balance, received bitcoins and sent bitcoins, respectively. The colour legends are displayed within the summary view (Fig. 1 A) and the user can adjust the minimum and maximum values. Note that, for consistency, the colour encoding of received and sent bitcoins in the other views is the same as that in the summary view.

Alternative Designs. Let us use two specific scenarios in bitcoin analysis to illustrate the advantages of our design of the summary view over the line chart and the bar chart. Suppose that the user is interested in studying the variation of the bitcoins received by a particular wallet over a period of time. (1) *Comparison with the bar chart* : It is inconvenient to use the bar chart (Fig. 2a) to examine the variation of the received bitcoins, which are presented by the red bars, because they are separated from each other by other kind of bars (green and purple). However, with our design, it is easier to examine the variation because the red bars are placed next to each other (Fig. 2c). Similarly, it is easier to use our design to visualize the other two features, i.e., sent bitcoins and balances, than using the bar chart. (2) *Comparison with the line chart* : Our design shows not only the variation of the received bitcoins but also the contributing wallets, i.e. the wallet boxes in each red bar in Fig. 2c. In contrast, the line chart (Fig. 2a) cannot represent these contributing wallets. Hence, our design provides a summary view that is more complete, compact and intuitive than the line chart and the bar chart.

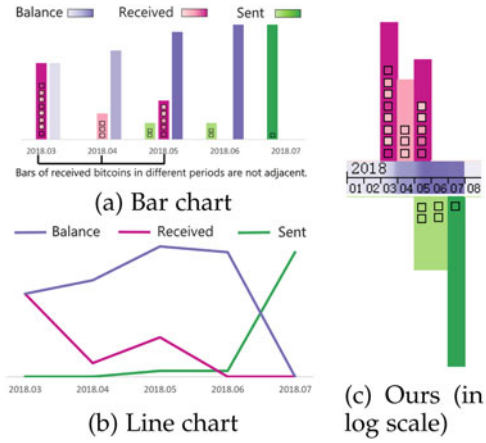


Fig. 2. Alternative designs for the summary view.

5.2 Detail View

One often needs to check the details of a particular transaction or wallet. For that purpose, we provide a table representation and a visual representation in the detail view (Fig. 1 B), which are both desired by the people interviewed in our user needs study. (*T2* , *T5*)

Tablet Representation. When one selects an element in any other view, information of related transactions and wallets will be displayed in this view with a table format.

Visual Representation. For visual representation of the detailed information, we adopt a visual design similar to that used in the summary view. All the involved transactions are displayed in the temporal order.

Cross-View Interactions. The detail view and the other views are coordinated to enable the user to examine transaction detail. When the user clicks on an element, i.e., a transaction or a wallet, in any other view, the detailed information of the element will be shown in the detailed view. Please refer to the accompanying video for a more clear demonstration.

5.3 Temporal View

The trading activities of those wallets related to a given wallet w reflect the characteristics of w. Hence, we design a temporal view (Fig. 1 C) to help understand the temporal aspects of the trading activities of the wallets trading with w. The following two modes are provided to fulfill the requirement *T1* and *T3.b* – the *direct transaction mode* and the *indirect transaction mode* .

5.3.1 Direct Transaction Mode

When browsing the transaction summary of an interested wallet w in the summary view, the user may also care about its trading activities from the perspective of each trader, to find out information such as which traders that they traded most bitcoins with or traded most frequently during the searched period (Fig. 3). In this case, the user can choose the direct mode to explore the transactions between w and every trader e. (*T1*)

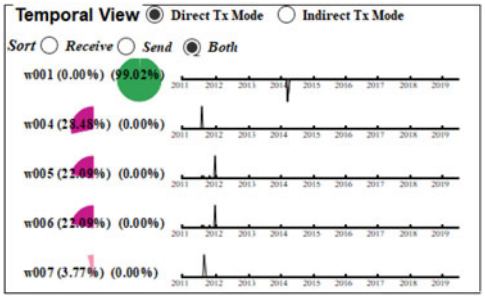


Fig. 3. Visual design of the direct transaction mode.

Visual Design. The traders of the wallet w are displayed in a user-defined order, by received bitcoins, sent bitcoins or both. The wallet w's total received bitcoins from trader e and sent bitcoins to trader e are represented by received pie slices and sent pie slices, respectively, whose area and colour encode total received/sent bitcoins. The colour encoding for received/sent bitcoins is the same as that in the summary view. Note that a bar chart is another option. Compared to pie charts, bar charts take more space. Therefore, we choose the pie chart to save space.

Besides total traded bitcoins between w and e, the user may also be interested in trader e's temporal trading activities with w. Thus, for every e, we also visualize its temporal trading behaviour with w in a line chart, with sent and received trading behaviour drawn downwards and upwards, respectively.

5.3.2 Indirect Transaction Mode

The temporal view (Fig. 1 C) of *BitAnalysis* also provides an indirect transaction mode to simultaneously investigate the trading activity of wallets ω indirectly related to w, for finding out whether wallets ω have similar trading frequency or are active during the same period as w, to name a few. We will have a detailed discussion in Section. 6.1 about wallets that trade indirectly with a given wallet w.

Design Rationale. When the user chooses this mode, they focus on the temporal similarity among ω rather than on specific transaction details. Therefore, the visual design should enable fast and convenient comparisons. Different from in the direct mode, in the indirect mode, we design the visual encoding of each wallet to be placed with that of other wallets in a more compact manner, enabling trading activity comparison among a large number of indirect related wallets.

Visual Design. Specifically, we use a horizontal colour bar, temporalTx, to aggregate temporal transaction data of wallet ω, as demonstrated in Fig. 4. In the temporalTx bar of ω, the transactions of ω are grouped by a user-defined time period, year, month or day. The total incoming (X_t^r) and outgoing (X_t^s) transactions occurring during the period t are represented as a txBlock b_r and b_s, whose height encodes the total received (v_r) and sent (v_s) bitcoins, respectively.

Fig. 4. Visual design of the indirect transaction mode.

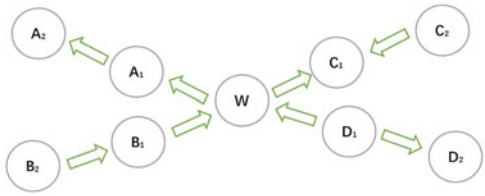


Fig. 5. Illustration of a connection network.

TxBlock b_r and b_s are aligned vertically. The height of b_r and b_s are computed as $H_s = \frac{v_s}{v_s+v_r} \cdot H$ and $H_r = \frac{v_r}{v_s+v_r} \cdot H$, respectively, where H is specified by the user. The user can adjust the value of H to compress or expand temporalTx bars. For consistency, the colour encoding of received (b_r) and sent (b_s) txBlocks is the same as that of the incoming/outgoing transaction bars in the summary view.

Meanwhile, we learn from the experts that inactive periods are as important as active periods, both of which together reflect the temporal activity of a wallet ω. Therefore, we use a gray block to encode the period t when no transactions occur.

6 Connection View

6.1 Connection Network

In the world of bitcoin, the relation of wallets is defined by the transactions between them. It is therefore important to use the network connecting the wallets trading with a given wallet w to understand the trading behavior of w. In the following we will first introduce some basic concepts and notations, and then present our method for analysing and visualizing this network of transactions.

Connected Wallets and Connection Network. Given a time period T, we define the *universal connection graph* $G(T) = \{V, E\}$, where the vertex set is composed of all the wallets and the edge set is composed of all the transactions between the wallets in V. Given a wallet w, an i-connected wallet of w, denoted as ω_w^i, is a wallet whose shortest path to w in $G(T)$ goes through i edges (transactions), or equivalently, has $i-1$ intermediate vertices (wallets). For an integer $D > 0$, we define the *D-distance connection network* of wallet w to be the network of all the wallets trading with w through D transactions or less. Specifically, this network, denoted as $\mathcal{N}_w^D = (V,' E')$, is the subgraph of the universal connection graph $G(T) = \{V, E\}$ such that $V' \subset V$ consists of all the i-connected wallets of w, $0 \leq i \leq D$, and $E' \subset E$ consists of all the transactions between the wallets in V'. Note that wallet w itself is ω_w^0 and that the traders of w are wallets ω_w^1.

Shortest Path. Note that, although the D-distance connection network $\mathcal{N}_w^D$ is a directed graph upon wallets and transactions, in the definition of an i-connected wallet of w, the shortest path between two wallets in $\mathcal{N}_w^D$ is computed without considering the edge directions. As an illustration, see Fig. 5, the shortest path length between the wallet w and each of the four wallets A_2, B_2, C_2 and D_2 is 2. The edge direction is ignored here because, according to bitcoin investigation experts, the connections between wallets are complicated and that it is important to discover their similarities and relations even if they do not trade directly with other.

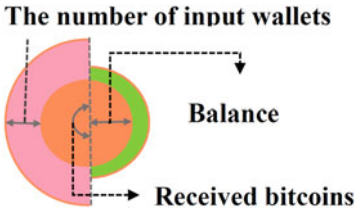


Fig. 6. Visual design of wallet glyph.

6.2 Connection Diagram

In the connection view (Fig. 1 D), we display the D-distance connection network in the form of a *connection diagram* , which is a novel visual presentation for clearly showing the relationship between a wallet w and its trading wallets, directly or indirectly. (*T3* , *T5*)

The value of D is specified by the user. All the involved wallets ω_w^i ($i \in [0, D]$) are listed on the left of the connection view (Fig. 1 D). Each wallet is displayed with its ID, its distance to w, and its belonged cluster, together with its last balance during the searching period. The user can choose to order the wallets by distance, cluster, or balance.

Wallet Glyph. The main element of a connection diagram is the *wallet glyph* , which encodes the main features of the trading activities of each wallet ω_w^i in the connection network $\mathcal{N}_w^D$ of wallet w. These features include the balance b, the total sent bitcoins v_s, the total received bitcoins v_r, the number of input wallets n_r that ω_w^i received bitcoins from, and the number of output wallets n_s that ω_w^i sent bitcoins to.

Fig. 6 shows the visual design of a wallet glyph. Here, the balance b is encoded by circle in the center, whose radius is proportional to the corresponding balance value. Two annular sectors are used to encode the total received bitcoins v_r and sent bitcoins v_s, respectively. The central angle and thickness of the annular sections are proportional to the received (v_r) (sent v_s, resp.) bitcoins, and the number of input (n_r) (output n_s, resp.) wallets, respectively. When a wallet glyph is selected in the connection diagram, the glyph itself and its incident connection edges will be highlighted. Besides, the same wallet will be highlighted in other views as well.

Colour Encoding. The center balance circle is coloured according to the wallet's trading distance to w. The colouring scheme for distances is colour-blindness-safe and different from those used in the summary view, which is shown on the top of the connection view (Fig. 1 D). Meanwhile, to be consistent, the colour encoding of the sent and received annular sectors is the same as that of sent and received bitcoins in the summary view, respectively.

Design logic. The glyph is designed to support feature comparisons across different wallets as well as within the same wallet, which are both important for users. Users can focus on different parts of the glyph for different purposes. For example, if users want to compare inputs and outputs of the same wallet, they can focus on the annular angles. While if users want to compare different wallets on features such as input or output, they can focus on the corresponding colors for comparison.

Full mode v.s. simple mode. By default, the full mode is enabled to show full wallet glyphs (Fig. 7a). We also provide a simple mode (Fig. 7b) to show the center balance circle only when the user wants to hide glyph details to focus on the connection network as a whole.

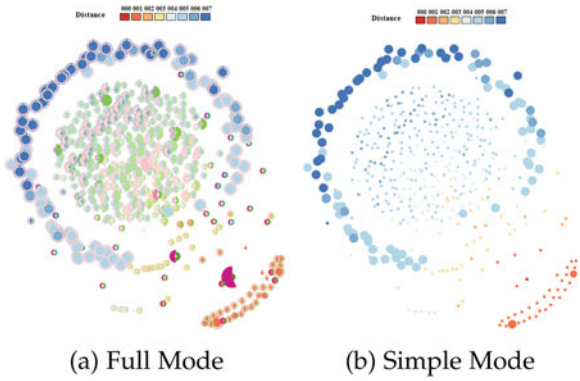


Fig. 7. Full mode v.s. simple mode of the connection diagram.

Wallet Placement. In the connection diagram, the wallets, displayed as wallet glyphs, are placed in the view panel using the graph-layout method by Kamada [57], which places closely wallets trading with each other. While the edges encode the connections (transactions) between wallets, showing all edges would make the visualization of a connection network cluttered and incomprehensible in practice since there are often a large number of active wallets in the connection network. Hence, we choose to display only the edges incident to a particular wallet chosen for investigation while hiding all the connections. This selective approach to display the edges of the connection diagram is a trade-off between diagram clarity and expressing wallet connections. Note that, although many edges are not displayed, it is still easy to visualize the trading distances between the wallets because the distances from the wallets to the central wallet w in the view panel are generally correlated to their trading distances. Further, the wallet glyphs are coloured in a way to indicate their distances to the wallet w. See Fig. 7.

When needed, the user can zoom in on the diagram with mouse scrolling, translate the diagram with the arrow keys, and rotate the diagram with the 'R' key. Meanwhile, the user can also reposition a wallet glyph with mouse dragging. (*T5*)

6.3 Similarity-Based Transaction Patterns of Wallet

When analysing a connection network $\mathcal{N}_w^D$, regulators and entrepreneurs are often interested in how the i-connected wallets ω_w^i of w are related to each other and whether they display similar characteristics, because such similarities can be used to characterize the behavior pattern of the wallet w. Hence, we propose to cluster similar wallets using the following four clustering metrics: *temporal similarity* , *trader similarity* , *balance similarity* , and *similarity of large-amount transactions* . Note that parameters in this section can be adjusted and the visual effects of each metric will be demonstrated later in the evaluation section. The user can choose to colour the center circle of wallet glyph based on belonging clusters. If a wallet is not clustered with any other wallets, it will be coloured gray, indicating that it is not successfully clustered. (*T3*)

Temporal Similarity. By this metric, two wallets are regarded to be highly related if they are active during the

same time period. For each wallet w_j in $\mathcal{N}_w^D$, we first retrieve its total trading amount, i.e., the sum of sent and received bitcoins, in every time period, and order them chronically to form a time series $\mathcal{S}_j$. Then we apply the fast dynamic time wrapping algorithm (DTW) [58] to compute temporal similarity between w_p and w_q. Wallets with the temporal similarity less than a user specified threshold σ_s with be grouped in the same cluster $\mathcal{C}_{time}$. That is, every two wallets w_p and w_q in $\mathcal{C}_{time}$ satisfy

$$DTW(\mathcal{S}_p, \mathcal{S}_q) < \sigma_s.$$

Briefly Speaking, DTW computes temporal similarity between w_p and w_q with the summed euclidean distance between the optimal shape-matched corresponding data points on $\mathcal{S}_p$ and on $\mathcal{S}_q$.

Trader Similarity. The trader similarity metric measures the degree in which two wallets contain similar traders. The user can choose the set of top n traders of each wallet w_j, denoted as $R^n_{w_j}$, and then group together wallets such that the number of their common traders is greater than a user specified integer $m > 0$. Denote a trader cluster as $\mathcal{C}_{trader}$,

$$\|R^n_{w_p} \cap R^n_{w_q}\| > m, \quad w_p, w_q \in \mathcal{C}_{trader}.$$

In this way, wallets having a certain number of common traders are clustered together.

Balance similarity. The balance similarity metric measures the similarity of the latest balances of two wallets. Using this metric, we group wallets w_j with their balance difference less than a threshold σ_b into the same cluster $\mathcal{C}_{balance}$. Let $\mathcal{B}_{w_j}$ denote the balance of wallet w_j. Then for two wallets w_p and w_q in the same cluster, we have

$$|\mathcal{B}_{w_p} - \mathcal{B}_{w_q}| < \sigma_b, \quad w_p, w_q \in \mathcal{C}_{balance}.$$

Similarity of large amount transactions. When a large-amount transaction occurs, the investigating agents should be alerted for further investigation. Based on this need, we introduce the large-amount transaction (greater than σ_v) metric to cluster the wallets involved in large amount transactions. Denote a large transaction cluster as $\mathcal{C}_{large}$, If w_i^{in} and w_i^{out} are the input and output of a large amount transaction $X_i^{\sigma_v}$, then $w_i^{in}, w_i^{out} \in \mathcal{C}_{large}$. Moreover, If w_j^{in} and w_j^{out} are the input and output of another large amount transaction $X_j^{\sigma_v}$ with $w_i^{out} = w_j^{in}$, then $w_j^{out} \in \mathcal{C}_{large}$ as well.

6.4 Continuous Wallet Monitoring

When a wallet attracts attention for any reason, besides examining its previous trading activities, the investigator also wishes to keep monitoring the wallet and be informed when any new transaction occurs to the wallet. Hence, we provide a monitoring module at the bottom-left of the connection view (Fig. 1 D) to meet this requirement. When selecting a wallet from the wallet list, the user can set the monitoring state to "On". In this case, our system will continuously monitor the selected wallet and record all the new transactions occurring to it. For every monitored wallet, *BitAnalysis* checks its transaction information in Wallet Explorer [2] every 30 minutes. Whenever new transactions are detected, the user will receive a notification via email or communication applications. (*T7*)

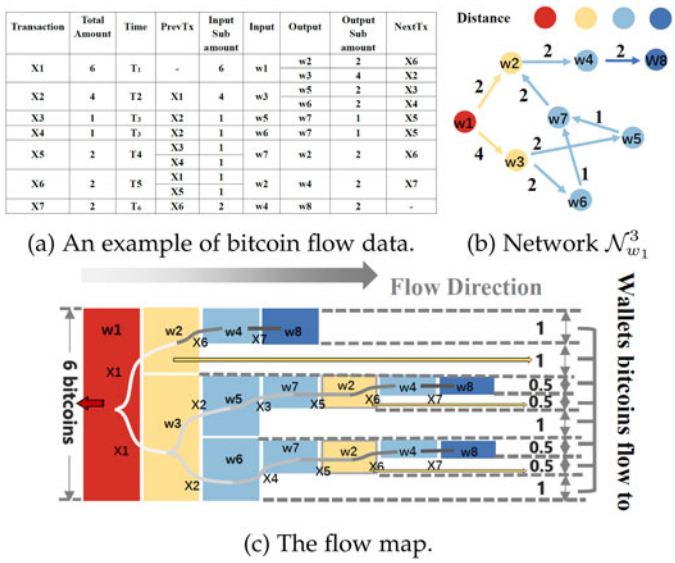


Fig. 8. An illustrative example of a flow map.

7 Flow View

The bitcoin flow is a process that some amount of bitcoins is transferred from a wallet to a group of wallets through a chain of transactions. Besides the trading activities of individual wallets, bitcoin investigators often also need to track whether the wallets are involved in a bitcoin flow and where the bitcoins end up. Hence, in this section we will present some new techniques in *BitAnalysis* for visualizing the bitcoin flow process. Fig. 8 uses a simple example to illustrate how a bitcoin flow process is visualized. (*T3* , *T4* , *T5*)

7.1 Bitcoin Flow Map

We have designed a new structure for visual presentation of the bitcoin flow originated from a given wallet w. In general, bitcoins flow from w to multiple wallets (i.e., the traders of w). Then the bitcoins continue flow from these traders to other wallets via new transactions. Hence, in general the flow of bitcoin has a tree structure. However, it often happens that a wallet may be involved multiple times in the flow. In this case they will appear multiple times in the tree structure of the flow map.

Visual Design. The visual presentation of an illustrative flow map is illustrated in Fig. 8c, based on the hypothetical bitcoin flow data tabulated in Fig. 8a.

Wallet Representation. Here, each wallet involved in the flow is represented by a rectangular box of a fixed width, whereas its height indicates the amount of bitcoins received from its preceding wallet, with the exception for the root wallet from which the flow starts; the height for the root wallet is the amount of bitcoins flowing out of it. Specifically, in this example, the box of the root wallet w_1 is placed left most of the flow map. Then the wallets receiving bitcoins from w_1, which are w_2 and w_3, are stacked and placed next to w_1. In general, the output wallets of a transaction are placed next to the input wallet to define a branching structure of the flow map tree. The colour of each box indicates the trading distance of the corresponding wallet to the root wallet w_1. Note that multiple transactions may share the

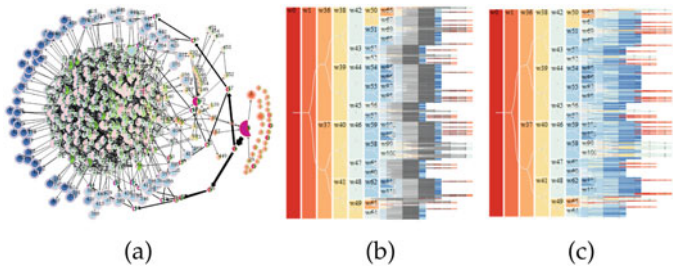


Fig. 9. Connection diagram v.s. flow map. (a) Connection Diagram. (b) Flow map with highlighted time. (c) Flow map w/o highlighted transaction time.

same output wallets. For example, in Fig. 8a, w_7 is the output wallet of transactions X_3 and X_4. Then, w_7 will appear twice in the flow map, leading to two identical sub-trees. A flow map based actual bitcoin transaction data is shown in Fig. 9b.

Transaction Representations. In addition, there is a curved path tracing from each wallet back to the root wallet in the flow map, encoding the involved transactions. The graduate colour change of the path represents the times when the transactions along the path take place. However, when the height of wallet boxes decreases, the curved paths may occlude the corresponding wallet boxes as shown in Fig. 9b. Therefore, we provide another non-time-highlight mode (Fig. 9c) when time is not the user's main focus.

Note that bitcoins will not disappear by the UTXO model. In our flow map, a blank space does not mean the disappearing of bitcoins; It means that certain bitcoins remain unspent in certain wallets after certain transactions. For the example in Fig. 8c, before transactions X_1, 6 bitcoins are all in wallet w_1. But after transactions X_1-X_7, bitcoins flow to other wallets and finally remain in w_2, w_5, w_6, and w_8. For example, totally 2 bitcoins remain in w_2, with 1 bitcoin unspent in the first branch of w_2, and 0.5 bitcoin unspent in both the second and third branches of w_2 (marked by the yellow arrow for illustration). In total, after transaction X_1-X_7, 2 bitcoins remain in w_2 and w_8, respectively while 1 bitcoin remains in w_5 and w_6, respectively. And all other wallets have a zero balance.

Comparison With Connection Diagram. Compared with the connection diagram (Fig. 9b), the flow map (Fig. 8c) more clearly shows the process how wallets are involved along the flow direction. As shown in the flow map (Fig. 8c), the bitcoins involved in transaction X_1 are finally distributed into and maintained by w_2, w_5, w_6, and w_8. But it is difficult for the user to tell which wallets the bitcoins finally end to in the connection diagram (Fig. 9b). Besides, it is also intuitive to see that whether circulations exist. For example, 1-connected wallet w_2 appears on the right of 2-connected wallets w_5, w_6 and w_7, indicating that bitcoins are circulated between w's 1-connected and 2-connected wallets.

Note that the advantage of a flow map over a connection diagram will be more noticeable with the increased complexity of involved wallets and transactions. For example, in Fig. 9c, when the flow process is complex, the flow map is still clear and the user can clearly see the circulation pattern: Certain bitcoins flow out of the w_0, the leftmost red box, and afterwards flow back to w_0, the red boxes on the right side of the map. However, the user can hardly tell the connections between wallets and the circulation pattern in the connection diagram with all edges set visible (Fig. 9a).

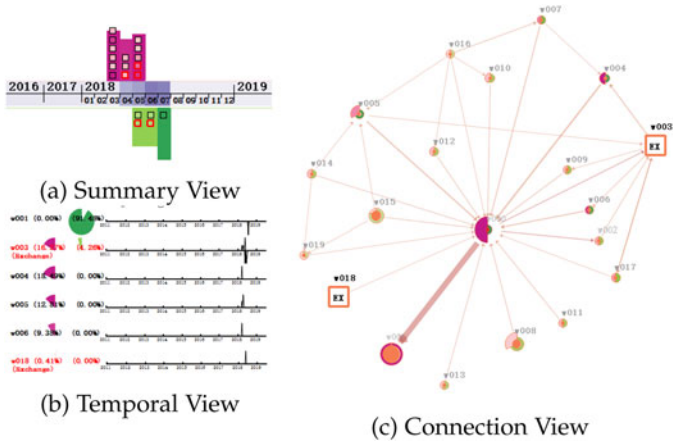


Fig. 10. Tagging known wallet types if exist.

7.2 Track Bitcoin Flow

Workflow. One starts to track where bitcoins traded in a transaction X flow to by clicking a transaction X (marked in Fig. 1 B) in the detail view. And the involved transaction information will be retrieved from the transaction database, displayed in the table of the detail view (Fig. 1 B). Then, the flow process is shown in the flow view (Fig. 1 E), illustrating how bitcoins flow among wallets $\omega_w^i (i \in [0, D])$ involved in the connection network $\mathcal{N}_w^D$.

BitAnalysis provides the following interactive operations to support convenient examination of bitcoin flows. Please refer to the video for a more clear demonstration.

- *Correlation of flow view to other views.*When one selects a wallet in the connection view, the flow view, or the temporal view, the same wallet will be highlighted in other views as well.

  As an example, wallet 0 is selected in Fig. 1.
- *Bitcoin flow animation.* The process of bitcoin flow involves a series of flow steps and the user may want to review the process dynamically. When the user scrolls the time axis slider-bar in the flow view, the process how bitcoin flows will be animated in the flow map as well as in the connection diagram.
- *Zooming up.* The flow map is initially displayed as an overview. When the user wants to check wallet boxes in detail, he can scroll the mouse wheel to increase the height of boxes.

8 Tag Wallets With Known Types

Meanwhile, we have retrieved tags, including exchanges, mixers, services, and gambling games from Wallet Explorer to exhibit wallet types. To be specific, when users choose to highlight wallets with known types in BitAnalysis,

- The summary view will highlight outstanding wallet blocks with known tags (Fig. 10a).
- The temporal view will display traders of a wallet along with their tags (Fig. 10b).

TABLE 1
Evaluation Questionnaire

Q1:	Is it easy for you to quickly browsing the transaction summary of a wallet in the summary view?
Q2:	Is it easy for you to find the outstanding traders (transactions) via the summary view and the direct Tx mode of the temporal view?
Q3:	Is it easy for you to analyze wallets relationship via the connection diagram and the provided metrics in the connection view?
Q4:	Is it easy for you to examine the temporal activity of i-connected wallets of w in the indirect Tx mode of temporal view?
Q5:	Is it easy for your to track bitcoin flow with the flow map in flow view and the interactions (e.g., flow animation)?
Q6:	Is it easy for you to set real time monitoring alarms for interested wallets?
Q7:	Is it easy for you to examine details of interested transactions?
Q8:	Is it easy for you to learn how to use *BitAnalysis*?
Q9:	Overall, is it easy for you to understand the visual designs of *BitAnalysis*?
Q10:	Do you think *BitAnalysis* is more effective than Wallet Explorer [2] and Blockchain.info [10] in accomplishing the tasks described in Q1-Q7? ?
Q11:	Do you think *BitAnalysis* is more effective than BlockChainVis [35] in accomplishing the tasks described in Q1-Q7?
Q12:	Do you think *BitAnalysis* is more effective than Bitcoin Big Bang [33] in accomplishing the tasks described in Q1-Q7?
Q13:	Do you think *BitAnalysis* is more effective than BitExtract [6] in accomplishing the tasks described in Q1-Q7?
Q14:	Do you think *BitAnalysis* is more effective than SilkViser [9] in accomplishing the tasks described in Q1-Q7?

- In the connection view, wallets with known types will be rendered distinguished from others along with the abbreviation of their tags (Fig. 10c).
- In the flow view, if a transaction involves wallets of specific types, such as exchange or mixer, the tracking of bitcoin flow in the flow map will be stopped automatically, since in such transactions, the inputs and outputs obviously do not relevant and thus require no further flow tracking.

9 Evaluation

9.1 User Study

To evaluate *BitAnalysis* , we conducted a user study to assess its effectiveness and usability. The details of the user study are presented in this section.

9.1.1 User Study Setup

Participants. We recruited 25 participants for the user study. Among them, 5 have helped us perform the needs study described in Section. 3 and the rest 20 participants (4 females, aged 29 to 65 years) are interested in or have bitcoin investment experience. Meanwhile, all the participants have no background of either HCI or visualization and no conflict of interests.

Procedure. We first briefly explained to all the participants the main features of the *BitAnalysis* system, by demonstrating commons visualization functions with a wallet investigation example. Then, the participants were asked to utilize *BitAnalysis* to analyze a wallet by accomplishing six tasks as shown below, which will be explained shortly. After the participants finished all the tasks, we asked them to express their view on the effectiveness and usability of *BitAnalysis* both verbally and in a post-study questionnaire (Table 1), which consists of 14 five-point Likert scale survey questions. For each question, participants needed to choose from strongly disagree (1) to strongly agree (5). The entire procedure took about 60 minutes

R1 Browse the historical transactions of a wallet w. (*T1*,*T5*)
R2 Identify the most prominent traders and transactions of a wallet w. (*T1*,*T2*)
R3 Examine the bitcoin flow originating from a wallet w. (*T4*,*T5*)
R4 Detect circulations in a bitcoin flow. (*T3*)
R5 Identify wallets that share similar transaction patterns to that of a given wallet w. (*T3*,*T5*)
R6 Set the monitoring function for a wallet w to monitor its future transactions. (*T6*)

9.1.2 In-Depth Wallet Examination

In this section, we describe the procedure how participants investigated a wallet w in the user study.

Basic Tasks. All the participants (p_{1-25}) started the analysis by searching the w and looking at its transaction summary from the summary view (Fig. 1 A), from which they noticed that w kept accumulating bitcoins until March 2014, which are all sent out afterwards (*R1*). Then, some participants ($15/25$) clicked on the transaction bar of time unit 2014.03 to check transaction details from the detail view (Fig. 1 B) while some ($20/25$) examined from the direct mode of the temporal view (Fig. 3), who all found that 111114 (99%) bitcoins were send to wallet $w001$ in one single transaction X (*R2*).

Track Bitcoin Flow. Then, the participants attempted to investigate the bitcoin flow of X. Most participants ($21/25$) immediately decided to focus on $w001$ and leave alone other traders $\omega_w^1(\neq w001)$ of w since the majority of bitcoins in w were sent to $w001$. And they increased D of the connection network $\mathcal{N}_w^D$ in the connection view by expanding wallet $w001$ only. The remaining 4 participants (p_{10}, p_{14}, p_{18} p_{19}) started to ignore wallet $\omega_w^1(\neq w001)$ after $D > 3$. The participants kept increasing D while at the same time checked the bitcoin flow of X. They observe that when $D < 6$, all wallets $\omega_w^i(i \in [2, D])$ maintain a zero balance. This phenomenon stops when $D = 7$ (Fig. 1 D).

Afterwards, all the participants ($25/25$) used the provided flow tracking animation to examine the time-varying bitcoin flow process (Fig. 11), with which the participants can watch the live bitcoin flow process in the connection diagram (a) - (c), and in the flow maps (d) - (f) simultaneously.

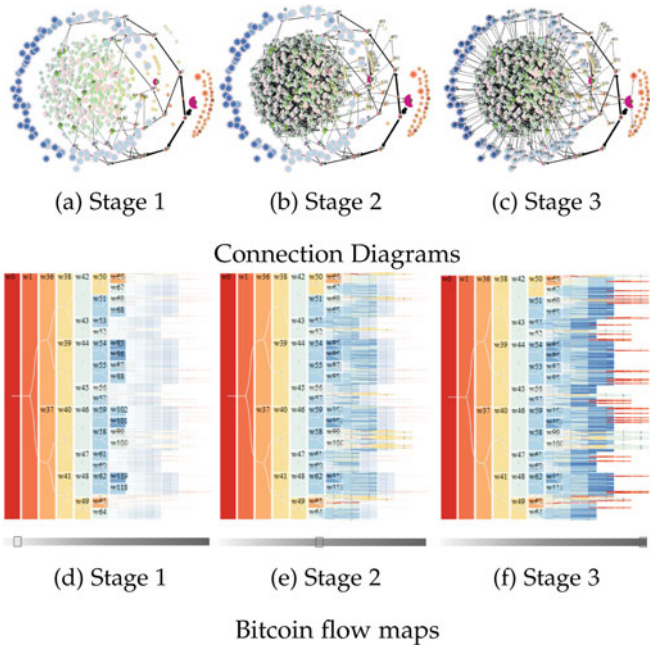


Fig. 11. Analysis of bitcoin flow in the user study.

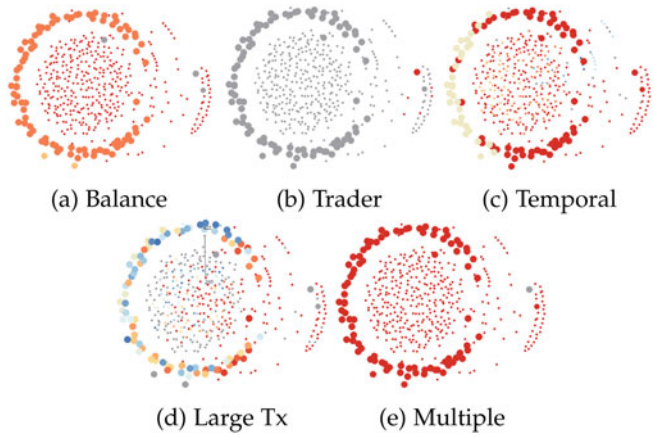


Fig. 12. Analysis of wallet similarity using different metrics. The wallets in the same cluster have the same colour.

Note that the flow maps are set not to highlight time and please refer to Fig. 1 E for the time-highlighted version.

In the first stage, Figs. 11a, 11b, 11c, and 11d, the bitcoins were sent to more wallets distributively. In the second stage, Figs. 11b, 11c, 11d, and 11e, bitcoins were traded between many intermediate wallets back and forth, which leads to the complex connectivity of the connection diagram. In the last stage, Figs. 11c, 11d, 11e, and 11f, the bitcoins were concentrated from the intermediate wallets to the final wallets, which are the wallet boxes on the rightmost side of the flow map (Fig. 11f) and the wallet glyphs with a larger balance (or inner) circle radius in the connection diagram (Fig. 11c). Notice that among the final wallets, most are dark blue wallets or light blue wallets but one is an orange wallet. (*R3*)

21 (out of 25) participants noticed the appearance of red rectangles on both the left and right sides of the flow map (Fig. 11f), which represent the wallet w_0 itself, indicating the existence of bitcoin circulations that some bitcoins flow back to w_0. Though 4 participants (p_8, p_{10}, p_{14}, p_{21}) did not notice this phenomenon at first but realized it right away after a quick hint. (*R4*)

Identify Wallet Similarity. Next, the participants used the four similarity metrics and the temporal view to investigate wallet $\omega_w^i (i \in [2,7])$ similarity. The clustering results of different metrics, balance, trader, temporal, large-amount transaction, and combining them all are shown in Fig. 12. The findings are

- Wallets have great balance similarity (Fig. 12a) but little trader similarity (Fig. 12b). Meanwhile, the indirect Tx mode of the temporal view (Fig. 1 C) and the temporal similarity (Fig. 12c) metric both demonstrate the temporal similarity between wallets. (25/25 participants)
- In Fig. 12d, many wallets belonging to the red balance cluster of Fig. 12a transferred a large volume of bitcoins to wallets belonging to the orange balance cluster of Fig. 12a. This phenomenon indicates that the wallets also have great similarity in terms of the large-amount transaction metric from the perspective of balance clusters. ($20/25$ participants)
- Wallets are clustered into a single group if combining the balance, temporal, and large transaction metrics (Fig. 12e), indicating their same ownership. ($24/25$ participants)

In a word, $w001$ and all wallets $\omega_w^i (i \in [2,7])$ probably belong to the same owner of wallet w. (*R5*)

Set Monitoring Alarms. Finally, all participants easily set a monitoring alarm for wallet w. (*R6*)

9.1.3 Results

Overall, the user study indicates that *BitAnalysis* can effectively help the user examine a bitcoin wallet. Meanwhile, it is easy to use for the user with little knowledge of visualization and HCI.

Effectiveness. Fig. 13 shows the scores for each question in the post-study questionnaire (Table 1). The participants usually started an investigation from the summary view. All participants appreciated the summary view which enables them to get an overview first with the intuitive encoding of outstanding wallets and transactions ($Q1$ and $Q2$). Many participants verbally commented that the summary view releases them from having to go through pages of transactions (p_{3-5}, p_{17-19}, p_{20}, p_{23-25}), and that it is intuitive to locate the outstanding traders (p_{3-5}, p_8, p_{11-13}, p_{16-19}, p_{20}, p_{22-25}). Meanwhile, $24/25$ participants can easily examine details of interested transactions ($Q7$ of Fig. 13).

More importantly, most participants praised the analysis functions provided. i.e., the temporal view and the connection view, as well as the convenient manner to track bitcoin flows in the flow view, as shown in $Q3$, $Q4$ and $Q5$ of Fig. 13. They noted that such advanced functions are unavailable in other existing tools. Specifically, $23/25$ participants expressed their satisfaction with the connection view ($Q3$). All participants agreed that the temporal view provides an effective way to observe wallet temporal similarity ($Q4$). $24/25$ participants appreciated the flow map and bitcoin flow tracking animation, which enabled them to easily go through the bitcoin flow process among wallets ($Q5$).

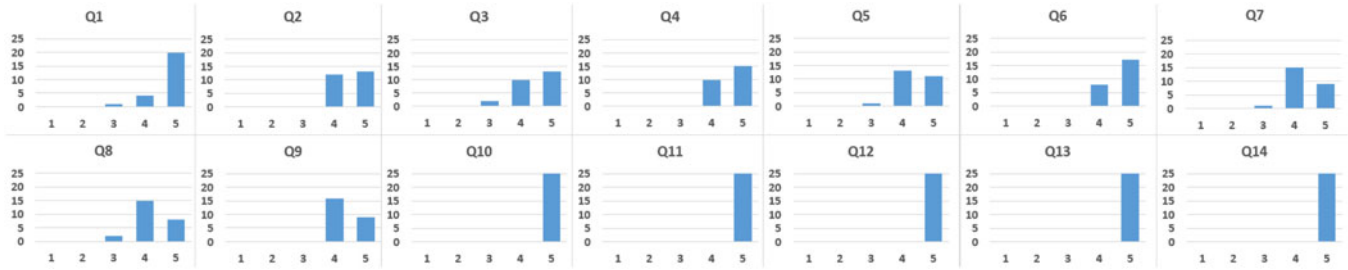


Fig. 13. The participants' scores on the 14 questions (from 1-strongly disagree to 5-strongly agree).

Meanwhile, many participants verbally commented that the design of wallet glyph is very helpful in providing a quick overview, and facilitate visually wallet similarity checking (p_{1-5}, p_8, p_{10-13}, p_{15}, p_{17}, p_{19}, p_{20}, p_{22-25}); that the proposed bitcoin characteristics based metrics are useful for wallet similarity measurement (p_{1-5}, p_{8-11}, p_{13}, p_{15}, p_{16}, p_{19-20}, p_{22-23}); that the newly designed flow map can show the paths of bitcoin flow in a more clean and clear way comparing to the widely used node-link diagrams, in which the paths can easily overlap with each other and are much more unintuitive to investigate (p_1, p_3, p_5, p_{10}, p_{12}, p_{19-22}, p_{24}); and that the time-axis in the flow map is useful for investigating flow process from the temporal perspective (p_3, p_5, p_{11}, p_{15}, p_{17}, p_{23}).

Finally, all participants encountered no difficulties in setting the monitoring alarms for interested wallets ($Q6$).

Usability. $Q8$ and $Q9$ of Fig. 13 show that the participants had no difficulty in learning and understanding *BitAnalysis* . Meanwhile, the participants' verbal feedback indicates that the integrated cross-view interactions are helpful during the wallet investigation.

Comparison With Existing Tools. Note that it would be informative to compare our system with existing wallet analytical tools. However, a formal comparison between our system and existing tools is probably unfair and inappropriate because the existing tools do not provide visualization functions (e.g., BlockChain.info [10] and Wallet Explorer [2]), do not support advanced analysis functions (e.g. Bitcoin Big Bang [33]), or have different objectives as *BitAnalysis* (e.g., BlockChainVis [35], BitExtract [6], and SilkViser [9]). Hence, we just introduce the most relevant existing tools to them and asked the participants to try their best to finish the same tasks with the existing tools and collected their comments on the comparison between *BitAnalysis* and the existing tools in questions $Q10$-$Q14$ of the questionnaire (Table 1).

All the participants commented that the BlockChain.info [10] and Wallet Explorer [2] are useful for primitive transaction examination but are ineffective for advanced tasks, such as bitcoin flow tracking and wallet analysis, due to their lack of visualization functions and other advanced analysis tools. Moreover, many participants (p_{1-5}, p_{7-13}, p_{16-19}, p_{21-25}) pointed out that BlockChain.info [10] and Wallet Explorer [2] do not support transactions filtering as *BitAnlysis* does, so they always have to go through a wallet's transactions of all time, which is very inconvenient when there are many transactions under consideration. All the participants asserted that the *BitAnalysis* system is more effective than Wallet Explorer and Blockchain.info (Fig. 13 $Q10$).

Moreover, all the participants commented that BitExtract [6], SilerViser [9], BlockChainVis [35], and Bitcoin Big Bang [33] have different objectives as ours and thus cannot accomplish the main tasks our system aims to solve (Fig. 13 $Q11$-$Q14$).

9.2 Comparative Analysis

We also provide a detailed comparison between *BitAnalysis* and existing works from different aspects, including the advantages, disadvantages, techniques, objectives, and experimental environments (Table 2). Most related works focus on bitcoin analysis and visualization from different perspectives as ours and thus have different objectives. The different functionalities mean that their techniques are quite different from ours. Please refer to Table 2 for details.

9.3 Mathematical Analysis

Time Complexity. In theory, without using any provided filtering, the time complexity of our system is $O(m \cdot n^D)$, where n is the average number of traders of a wallet, m is the average number of transactions of a wallet, and D is the max distance of the connection network. Because of the high time complexity, when using the system, the user should filter out unimportant transactions and increase value of D in the connection diagram by expanding user-specified wallets only. if the provided filtering function is used, the time complexity can be reduced to $O(\hat{m} \cdot \hat{n}^D)$, where $\hat{m} \ll m$ and $\hat{n} \ll n$, and if user-specified wallet expanding strategy is further adopted, the time complexity could be reduced to $O(\hat{m} \cdot \hat{n} \cdot D)$ to the greatest extent.

Theory Analysis of System Design. The design of flow map is piece-wise linear in the 2-dimensional screen space, following a tree structure and demonstrating a series of related bitcoin flows in a consistent direction. While the connection diagram is not, demonstrating the flows in random directions of the 2-dimensional screen space. Therefore, theoretically, it is much easier for users to track the flows in the flow map than in the connection diagram. Meanwhile, the advantage of a flow map over a connection diagram will be more noticeable with the increased complexity of involved wallets and transactions.

In the connection diagram, we propose the design of wallet glyphs. Without the glyphs, a wallet node in the connection diagram can only demonstrate one feature, enabling feature comparison from 1 dimension. While in a wallet glyph, we fully take advantage of the screen space to demonstrate multiple features of bitcoin wallets, including received/sent center angles, input/output thickness, concentric circles for different

TABLE 2
Comparison With Existing Works

	Objectives	Experimental Enviroment	Advantages	Disadvantages	Techniques
Bitbonkers [3] BitTxVis [4] BitListen [5] dailybchain [29] WIZBIT [30]	-Mimic the real occurrence of bitcoin transactions to bitcoin newbies who wants to know about bitcoin transactions .	-Webpage	✓ Vivid visualizations	-Support no analysis	-Graphical rendering
TxhighWay [28] TxStreet [31]	-Demonstrate to bitcoin newbies who wants to grasp the machanism of bitcoin blockchain,.	-Webpage	✓ Vivid visualizations	-Support no analysis	-Graphical rendering
Bitcoin Big Bang [33]	-Show the emergence of large bitcoin entities and their connectivity to people who want to know the evolvement of large bitcoin entities.	-Webpage	✓ Vivid visualizations ✓ Support to check the connectivity between predefined large bitcoin entities.	-Support no custom analysis ✗ Wallet summary preview ✓ Predefined wallet relationship analysis ✗ Wallet similarity analysis ✗ Bitcoin flow tracking ✗ Wallet monitoring	-Node-link diagrams
Wallet Explorer [2] BlockChain.info [10]	-Enable people to check basic information of bitcoin wallets/addresses and transactions.	-Webpage	✓ Simple table visualization for easy understanding	-Support no analysis ✗ Wallet summary preview ✗ Wallet relationship analysis ✗ Wallet similarity analysis ✓ Weak Bitcoin flow tracking ✗ Wallet monitoring	-Table -Linked list
BlockChainVis [35]	-Help professionals to analyze transactions by filtering out undesired information.	-PHP -JSON -OrientDB	✓ Visualize transaction network by eliminating undesired information	-Support no wallet-based analysis ✗ Wallet summary preview ✓ Weak Wallet relationship analysis ✗ Wallet similarity analysis ✓ Weak Bitcoin flow tracking ✗ Wallet monitoring	-Node link diagram -Predefined custom filtering
BitExTract [6]	-Help professionals to explore the evolutionary transaction patterns and relationship of bitcoin exchanges	-Web based -Python3 -MongoDB	-Support exchange-based analysis ✓ Observe the transactions between exchanges ✓ Depict the temporal transaction distribution among exchanges ✓ Compare the evolution patterns of transactions between exchanges	-Support no non-Exchange analysis ✗ Wallet summary preview ✗ Wallet relationship analysis ✗ Wallet similarity analysis ✗ Bitcoin flow tracking ✗ Wallet monitoring	-An ego-centered node-link diagram -Multiple parallel bars on a timeline
Blockchain Forensics [27]	-Facilitate professionals to conduct blockchain forensic investigations	-A virtual machine with 8 core CPU and 64G RAM -SQL Server Database	-Support macro transaction pattern analysis ✓ Find addresses that satisfy a given pattern. ✓ Analyze marginal distribution to eliminate false positive samples.	- Not applicable to compare with the functions BitAnalysis provided since BitAnalysis is for micro-level wallet analysis	-Extended safe Petri Net
SilkViser [9]	-Provide a block and blockchain-oriented explorer for novice user and experienced users to check transactions.	HTML5	✓ Support block-level transaction checking	✗ Wallet summary preview ✗ Wallet similarity analysis ✗ Wallet relationship analysis ✗ Bitcoin flow tracking ✗ Wallet monitoring	-A paper ledger-inspired block and blockchain visual design -An ancient copper coin-inspired transaction visual design
BitAnalysis	-Provide an interactive bitcoin wallet investigation tool to facilitate 1. newbies to check basic information of custom bitcoin wallets 2. regulators and professionals to perform advanced wallet analysis	-PyQt5 -Python3 -SQL Server Database	-Support micro advanced wallet analysis ✓ Wallet summary preview ✓ Wallet relationship analysis ✓ Wallet similarity analysis ✓ Bitcoin flow tracking ✓ Wallet monitoring	✓ Less vivid visualization ✗ Block-level analysis ✗ Exchange-oriented analysis ✗ Macro analysis from the perspective of the whole bitcoin network	-A novel connection diagram to demonstrate wallet connections -A set of clustering metrics designed based on bitcoin features -A novel flow map to demonstrate bitcoin flows

features. Meanwhile, we also use consistent color schemes to display absolute received/sent bitcoins. Totally, a wallet glyph can exhibit 7 different features at the same time, enable users to compare wallets from 7 dimensions in a connection diagram.

9.4 Contribution & Novelty Discussion

To summarize, the main contribution of this paper is the BitAnalysis system for advance bitcoin wallet analysis, which provides four main functions, efficient wallet preview via a novel designed summarization chart, wallets analysis with a newly proposed wallet glyph and connection diagram, bitcoin flow tracking with a novel designed flow map, as well as new transactions alerting. The functions are carefully designed based on the requirements raised in needs assessment (Section. 3). To be more specific, from the perspective of each proposed technique:

- Compared with line charts and bar charts, the design of our summary view is for more convenient comparison between different features of a wallet. And its advantages over line charts and bar charts are demonstrated in section 5.1 (alternative designs).
- Compared with node-link diagrams, our connection diagram uses novel wallet glyphs to summarize the features of wallets. Meanwhile, the placement of wallets in the diagram is designed to reflect wallet trading distances, which is shown in Section 6.2.
- Compared with existing clustering metrics, our wallet similarity metrics are specifically designed based on the characteristics of bitcoins, which are shown in section 6.3.
- Bitcoin flow map in section 7 is a newly design structure to illustrate how bitcoin flows between wallets, in with each graphical element is designed to encode different wallet/transaction features.

Experimental Justification. Meanwhile, to justify that the proposed functions and designs are effective, in our experiment (section 9.1), we have invited 25 participants to conduct a rigorous case study for wallet investigation and let them accomplish six tasks (Section. 9.1.1, R1-R6) that cover different aspects of the proposed functions. The detailed procedure of the case study (section. 9.1.2) and the feedbacks from the participants (section 9.1.3) together indicate the effectiveness and usefulness of the proposed functionalities of BitAnalysis. Generally speaking, the participants are satisfied with the proposed system design, and they claimed that the functions provided by our system are helpful for bitcoin wallet analysis.

9.5 Limitations and Future Works

Processing Time and System Upgrade. Although the proposed system is useful and effective, it has a potential limitation, which is the processing time. When an investigation involves too many wallets, for example, a wallet contains many transactions or users specify a large distance value in the connection view, the data retrieval time and visualization rendering time will be long. To mitigate this problem, the user can filter out unimportant transactions and increase value of D in the connection diagram by expanding user-

specified wallets only. As we tested, with the filtering functions enabled, the processing time to generate a 7-distance connection diagram with 450 wallets and 67,000 transactions is less than a minute.

To make the system more applicable for the industry, in the future work, we want to include more computational power and use parallel computing to speed up the data loading and rendering process.

Privacy-Oriented Cryptocurrencies . Since our system takes advantages of the transactions between wallets to perform the analysis, As a result, it cannot be used to analyze privacy-oriented cryptocurrencies such as Zcash, Dash and Monero, which are anonymous. However, in the future, we can still extend the system to support analysis of more non-privacy-oriented cryptocurrencies.

Beginners Need Some Efforts to Learn the System. Inevitably, our system consists of relatively complicated visual design in order to fulfill the requirement of advanced bitcoin analysis. Therefore, it takes some time for users who are inexperienced in bitcoin to understand and to user our system. In the future, we will attempt to develop a simpler version of the current system as a complement for beginners with less advanced analytical needs.

Environment Settings. At present, *BitAnalysis* is a desktop system. In the future, we are considering migrating our system to a web engine to make it a web-based application, enabling BitAnalysis to be more easily accessible by users with no need to configure system settings.

Heterogeneous Systems. During the design process of BitAnalysis, we did not fully consider how it will work in the case of heterogeneous systems. Therefore, we list it as a limitation and would like to explore the possibility to integrate this feature in the future work.

10 Conclusion

In this paper, we have presented the first visualization system, *BitAnalysis* , to facilitate investigation of a user-selected wallet. The newly designed connection diagram, similarity metrics and bitcoin flow map greatly help analyze the trading activities of related wallets. Our system has been validated by an extensive user study, which indicates that *BitAnalysis* is effective for wallet investigation. We hope that our work can inspire more research on bitcoin analysis systems and promote the global legalization of bitcoin.

References

[1] N. Tovanich, N. Heulot, J.-D. Fekete, and P. Isenberg, "A systematic review of online bitcoin visualizations," in *Proc. Posters Eur. Conf. Visual.*, 2019, pp. 69–72.

[2] Walletexplorer.com: Smart bitcoin block explorer, 2019. Accessed: Feb. 15, 2019. [Online]. Available: https://www.walletexplorer.com/

[3] Bitbonkers, 2019. Accessed: Feb. 15, 2019. [Online]. Available: https://bitbonkers.com/

[4] Bitcoin transaction visualization, 2019. Accessed: Feb. 15, 2019. [Online]. Available: http://bitcoin.interaqt.nl/

[5] Bit listen, 2019. Accessed: Feb. 16, 2019. [Online]. Available: https://www.bitlisten.com/

[6] X. Yue *et al.*, "BitExTract: Interactive visualization for extracting bitcoin exchange intelligence," *IEEE Trans. Visual. Comput. Graph.*, vol. 25, no. 1, pp. 162–171, Jan. 2019.

[7] 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 *Proc. IEEE Symp. Visual. Cyber Secur.*, 2015, pp. 1–8.

[8] 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.

[9] Z. Zhong *et al.*, "SilkViser: A visual explorer of blockchain-based cryptocurrency transaction data," in *Proc. IEEE Conf. Vis. Analytics Sci. Technol.*, 2020, pp. 95–106.

[10] Blockchain.info, 2019. Accessed: Feb. 15, 2019. [Online]. Available: https://blockchain.info/tree/114688199

[11] C. Kinkeldey, J.-D. Fekete, and P. Isenberg, "BitConduite: Visualizing and analyzing activity on the bitcoin network," in *Proc. EuroVis Eurographics Conf. Visual.*, 2017, Art. no. 3.

[12] P. Isenberg, C. Kinkeldey, and J.-D. Fekete, "Exploring entity behavior on the bitcoin blockchain," in *Proc. IEEE Conf. Visual.*, 2017, pp. 1–2.

[13] Y. Sun, H. Xiong, S. M. Yiu, and K. Y. Lam, "Bitvis: An interactive visualization system for bitcoin accounts analysis," in *Proc. IEEE Crypto Valley Conf. Blockchain Technol.*, 2019, pp. 21–25.

[14] D. Yermack, "Is bitcoin a real currency? an economic appraisal," in *Handbook of Digital Currency*. New York, NY, USA: Elsevier, 2015, pp. 31–43.

[15] T. Pham and S. Lee, "Anomaly detection in bitcoin network using unsupervised learning methods," 2016, *arXiv:1611.03941*.

[16] P. Monamo, V. Marivate, and B. Twala, "Unsupervised learning for robust bitcoin fraud detection," in *Proc. IEEE Inf. Secur. South Afr.*, 2016, pp. 129–134.

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

[18] R. Stokes, "Virtual money laundering: The case of bitcoin and the linden dollar," *Inf. Commun. Technol. Law*, vol. 21, no. 3, pp. 221–236, 2012.

[19] R. Böhme, N. Christin, B. Edelman, and T. Moore, "Bitcoin: Economics, technology, and governance," *J. Econ. Perspectives*, vol. 29, no. 2, pp. 213–38, 2015.

[20] J. Brito, H. Shadab, and A. Castillo, "Bitcoin financial regulation: Securities, derivatives, prediction markets, and gambling," *Colum. Sci. Tech. L. Rev.*, vol. 144, pp. 2014–2015, 2014.

[21] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, "Mixcoin: Anonymity for bitcoin with accountable mixes," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, 2014, pp. 486–504.

[22] 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.*, 2014, pp. 469–485.

[23] S. McNally, J. Roche, and S. Caton, "Predicting the price of bitcoin using machine learning," in *Proc. 26th Euromicro Int. Conf. Parallel Distrib. Netw.-Based Process.*, 2018, pp. 339–343.

[24] J. Almeida, S. Tata, A. Moser, and V. Smit, "Bitcoin prediciton using ANN," *Neural Netw.*, vol. 7, pp. 1–12, 2015.

[25] F. Reid and M. Harrigan, "An analysis of anonymity in the bitcoin system," in *Security and Privacy in Social Networks*. Berlin, Germany: Springer, 2013, pp. 197–223.

[26] S. Ranshous *et al.*, "Exchange pattern mining in the bitcoin transaction directed hypergraph," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, 2017, pp. 248–263.

[27] Y. Wu *et al.*, "A bitcoin transaction network analytic method for future blockchain forensic investigation," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1230–1241, Apr.–Jun. 2020.

[28] Bitcoin cash vs bitcoin core transaction visualizer, 2019. Accessed: Feb. 16, 2019. [Online]. Available: https://txhighway.com/#

[29] Daily blockchain, 2019. Accessed: Feb. 16, 2019. [Online]. Available: http://dailyblockchain.github.io/

[30] Wizbit, 2019. Accessed: Feb. 15, 2019. [Online]. Available: https://blocks.wizb.it/

[31] Txstreet.com, 2019. Accessed: Feb. 16, 2019. [Online]. Available: https://txstreet.com/

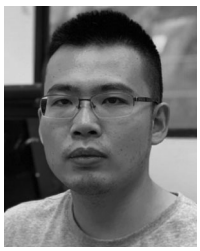
[32] Bitnodes.earn.com, 2019. Accessed: Feb. 15, 2019. [Online]. Available: https://bitnodes.earn.com/

[33] Bitcoin big bang, 2019. Accessed: Feb. 15, 2019. [Online]. Available: https://www.elliptic.co/

[34] N. Christin, "Traveling the silk road: A measurement analysis of a large anonymous online marketplace," in *Proc. 22nd Int. Conf. World Wide Web*, 2013, pp. 213–224.

[35] S. Bistarelli and F. Santini, "Go with the-bitcoin-flow, with visual analytics," in *Proc. 12th Int. Conf. Availability Rel. Secur.*, 2017, pp. 1–6.
[36] D. Kondor, M. Pósfai, I. Csabai, and G. Vattay, "Do the rich get richer? an empirical analysis of the bitcoin transaction network," *PLoS One*, vol. 9, no. 2, 2014, Art. no. e86197.
[37] D. Di Francesco Maesa, A. Marino, and L. Ricci, "Data-driven analysis of bitcoin properties: Exploiting the users graph," *Int. J. Data Sci. Analytics*, vol. 6, no. 1, pp. 63–80, 2018.
[38] J. Heer and D. Boyd, "Vizster: Visualizing online social networks," in *Proc. IEEE Symp. Inf. Visual.*, 2005, pp. 32–39.
[39] J. Wang and K. Mueller, "Visual causality analysis made practical," in *Proc. IEEE Conf. Vis. Analytics Sci. Technol.*, 2017, pp. 151–161.
[40] C. Stoiber *et al.*, "netflower: Dynamic network visualization for data journalists," *Comput. Graphis Forum*, vol. 38, no. 3, pp. 699–711, 2019.
[41] D. Holten and J. J. Van Wijk, "Force-directed edge bundling for graph visualization," in *Computer Graphics Forum*, vol. 28, no. 3. Hoboken, NJ, USA: Wiley, 2009, pp. 983–990.
[42] R. Bourqui, D. Ienco, A. Sallaberry, and P. Poncelet, "Multilayer graph edge bundling," in *Proc. IEEE Pacific Visual. Symp.*, 2016, pp. 184–188.
[43] Y. Wang *et al.*, "Ambiguityvis: Visualization of ambiguity in graph layouts," *IEEE Trans. Vis. Comput. Graphics*, vol. 22, no. 1, pp. 359–368, Jan. 2015.
[44] D. Jonker, S. Langevin, D. Giesbrecht, M. Crouch, and N. Kronenfeld, "Graph mapping: Multi-scale community visualization of massive graph data," *Inform. Vis.*, vol. 16, no. 3, pp. 190–204, 2017.
[45] J. Duch and A. Arenas, "Community detection in complex networks using extremal optimization," *Phys. Rev. E*, vol. 72, no. 2, 2005, Art. no. 027104.
[46] J. Yang, J. McAuley, and J. Leskovec, "Community detection in networks with node attributes," in *Proc. IEEE 13th Int. Conf. Data Mining*, 2013, pp. 1151–1156.
[47] C. Pizzuti, "Ga-Net: A genetic algorithm for community detection in social networks," in *Proc. Int. Conf. Parallel Problem Solving From Nature*, 2008, pp. 1081–1090.
[48] J. D. Wilson, J. Palowitch, S. Bhamidi, and A. B. Nobel, "Community extraction in multilayer networks with heterogeneous community structure," *J. Mach. Learn. Res.*, vol. 18, no. 1, pp. 5458–5506, 2017.
[49] X. Li, G. Xu, and M. Tang, "Community detection for multi-layer social network based on local random walk," *J. Vis. Commun. Image Representation*, vol. 57, pp. 91–98, 2018.
[50] J. D. Kirkland, T. E. Senator, J. J. Hayden, T. Dybala, H. G. Goldberg, and P. Shyr, "The NASD regulation advanced-detection system (ADS)," *AI Mag.*, vol. 20, no. 1, pp. 55–55, 1999.
[51] R. Chang *et al.*, "Wirevis: Visualization of categorical, time-varying data from financial transactions," in *Proc. IEEE Symp. Vis. Analytics Sci. Technol.*, 2007, pp. 155–162.
[52] M. L. Huang, J. Liang, and Q. V. Nguyen, "A visualization approach for frauds detection in financial market," in *Proc. IEEE 13th Int. Conf. Inf. Visualisation*, 2009, pp. 197–202.
[53] R. A. Leite *et al.*, "EVA: Visual analytics to identify fraudulent events," *IEEE Trans. Visual. Comput. Graph.*, vol. 24, no. 1, pp. 330–339, Jan. 2017.
[54] S. Ko, R. Maciejewski, Y. Jang, and D. S. Ebert, "Marketanalyzer: An interactive visual analytics system for analyzing competitive advantage using point of sale data," in *Computer Graphics Forum*, vol. 31, no. 3. Hoboken, NJ, USA: Wiley, 2012, pp. 1245–1254.
[55] A. Malik, R. Maciejewski, N. Elmqvist, Y. Jang, D. S. Ebert, and W. Huang, "A correlative analysis process in a visual analytics environment," in *Proc. IEEE Conf. Vis. Analytics Sci. Technol.*, 2012, pp. 33–42.
[56] S. K. Badam, J. Zhao, S. Sen, N. Elmqvist, and D. Ebert, "TimeFork: Interactive prediction of time series," in *Proc. CHI Conf. Hum. Factors Comput. Syst.*, 2016, pp. 5409–5420.
[57] T. Kamada *et al.*, "An algorithm for drawing general undirected graphs," *Inf. Process. Lett.*, vol. 31, no. 1, pp. 7–15, 1989.
[58] S. Salvador and P. Chan, "Toward accurate dynamic time warping in linear time and space," *Intell. Data Anal.*, vol. 11, no. 5, pp. 561–580, 2007.

Yujing Sun received the bachelor's degree from University of Minnesota, Twin Cities, in 2013 and the PhD degree in computer science from the University of Hong Kong, in 2018. She is currently a research assistant Professor with the University of Hong Kong, under supervision of Prof. Wenping Wang. Her research interests include financial data analysis, computer graphics, image processing, and biometrics.



Hao Xiong received the bachelor's degree from Sun Yat-Sen University, in 2010 and the PhD degree in computer science from the University of Hong Kong, in 2013. He is an adjunct assistant professor with the University of Hong Kong. His research interests include cryptography and blockchain.

Siu Ming Yiu (Member, IEEE) received the PhD degree in computer science from the University of Hong Kong. He is a full professor with the University of Hong Kong. He has Published more then 100+ papers in referred journals and conferences (Citations (8627), h-index (41), i10-index (98)) and is Conference/programme chairs in prestigious conferences in both areas of cryptography and bioinformatics.

Kwok Yan Lam received the BSc from the University of London, in 1987 and the PhD from the University of Cambridge, in 1990. He is a full professor with the Nanyang Technological University. He is a renowned Cyber Security Researcher and practitioner. He has collaborated extensively with law-enforcement agencies, government regulators, telecommunication operators and financial institutions in various aspects of Infocomm and Cyber Security in the region. He is the Lead P.I. of the SPIRIT Programme, an 11,000,000 programme on smart nation research funded by NRF. Prior to joining NTU, he has been a Professor of the Tsinghua University, PR China (2002–2010) and a faculty member of the National University of Singapore and the University of London since 1990.