

Market Manipulation of Bitcoin: Evidence from Mining the Mt. Gox Transaction Network

Abstract—The cryptocurrency market is a very huge market without effective supervision. It is of great importance for investors and regulators to recognize whether there are market manipulation and its manipulation patterns. This paper proposes an approach to mining the transaction networks of exchanges for answering this question. By taking the leaked transaction history of Mt. Gox Bitcoin exchange as a sample, we first divide the accounts into three categories according to its characteristic and then construct the transaction history into three graphs. Many observations and findings are obtained via analyzing the constructed graphs. To evaluate the influence of the accounts' transaction behavior on the Bitcoin exchange price, the graphs are reconstructed into series and reshaped as matrices. By using singular value decomposition (SVD) on the matrices, we identify many base networks which have a great correlation with the price fluctuation. When further analyzing the most important accounts in the base networks, plenty of market manipulation patterns are found. According to these findings, we conclude that there was serious market manipulation in Mt. Gox exchange and the cryptocurrency market must strengthen supervision.

Index Terms—Bitcoin, Transaction network, Temporal network, Singular value decomposition

I. INTRODUCTION

Bitcoin has become one of the hottest buzzwords among investors and researchers. It is the first and most famous decentralized digital currency [1], which is secured by cryptography (thus, we call it cryptocurrency). Unlike fiat currencies which usually issued by financial institutions, there is no centralized organization or country controlling the issue and operation of Bitcoin. Furthermore, because of decentralization, users in the Bitcoin system are anonymous. The two characteristics (i.e., decentralization and anonymity) make Bitcoin attract a lot of users since its creation in 2009. It is estimated that there are more than 10 million users in the Bitcoin system [2].

Since the famous “Bitcoin Pizza Day” [3] when a programmer bought two pizzas with 10,000 BTC on May 22, 2010, Bitcoin began to exchange with fiat currencies. Soon afterward, a Bitcoin exchange, Mt. Gox launched. By 2013 and before filing for bankruptcy protection in February 2014, Mt. Gox was the largest bitcoin intermediary and the world's leading Bitcoin exchange [4]. Nowadays, there are more than 1,700 cryptocurrencies inspired by Bitcoin and the daily transaction volume is over \$ 150 billion dollar according to coinmarketcap.com at the moment of writing this paper.

The huge fluctuation of the exchange price of cryptocurrency is an important reason to attract investors' participation. Figure 1 shows the Bitcoin price (i.e., the exchange rate between Bitcoin and USD dollar in this paper) from 2012/12 to 2015/6. During this period, the Bitcoin price rose sharply from

about \$10/BTC to exceeding \$1,000/BTC and then fell back to below \$200/BTC. This extreme price fluctuation has also attracted a large number of researchers to find the determinant factors of the Bitcoin price. Four categories of factors are discussed, including 1) economic factors (e.g., the supply and demand of Bitcoin) [5]; 2) technical factors (e.g., hash rate and difficulty) [6]; 3) interest factors (through proxy variable such as Google trends) [7]; and 4) other financial assets (e.g., gold, stock). In addition, by using the principal component analysis method (analogous to SVD), the paper [8] indicates that the Bitcoin price has a strong correlation with the transactions on the blockchain ledger.

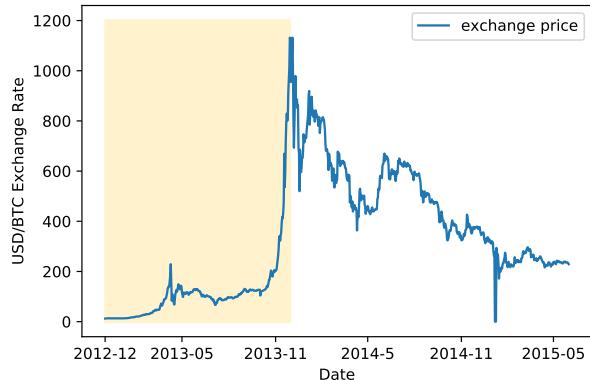


Fig. 1. Bitcoin-USD exchange price at Bitstamp exchange, with the period being studied shaded.

However, these factors are discussed based on data outside the exchanges. Because of the lack of supervision, a nature conjecture is that the extreme fluctuation may be related to the market manipulation of the exchanges. This conjecture is hard to verify as it is very difficult to obtain the detailed trading data from the trading platform. Surprisingly, many transaction histories from April 2011 to November 2013 of the once famous Bitcoin exchange Mt. Gox was leaked in the form of CSV files. These data provide a perfect opportunity for answering the conjecture.

To verify whether there is market manipulation and identify possible manipulation patterns is urgent and of great importance, as plenty of investors who are dreaming of getting rich overnight are attracting to the market. The answer to this question will help investors recognize the potential risks and help to regulate legislation. Based on the leaked data, a recent paper [9] points out that the Mt. Gox exchange manipulated

the Bitcoin price by building a regression model to identify the influence of the activities of some suspicious accounts on the price. We adopt a completely different method compared with it and obtain more results including fake volume, price manipulation, and manipulation patterns.

Figure 2 shows an overview of our analysis. We first verify the leaked data and remove many unreasonable records. Then, by comparing the transaction price with the disclosed Mt. Gox price in quandl.com, we find many abnormal transactions. By using these transactions, we divide the accounts into three categories: extreme high account (EHA), extreme low account (ELA), and normal account (NMA). Next, we construct the extreme high graph (EHG), extreme low graph (ELG) and normal graph (NMG) by seeing the accounts as nodes and transactions as edges. we conduct various graph structure analysis on EHG, ELG, and NMG, such as nodes and edges classification, measuring graph clusters and degree distribution. Such investigation leads to new observations and findings. For example, the abnormal accounts (i.e., EHA and ELA) might be controlled by the exchange and used to provide liquidity and fake volume for the exchange. Finally, by dividing the graphs into daily snapshots and reconstructing it in a matrix, we extract some base graphs through singular value decomposition (SVD). By doing this, we find that the abnormal accounts' transactions strongly related to the Bitcoin price. Furthermore, we find many strange transaction patterns (such as self-loop, bi-direction, triangle etc.) within abnormal accounts. These patterns are considered as evidence of market manipulation in the exchange.

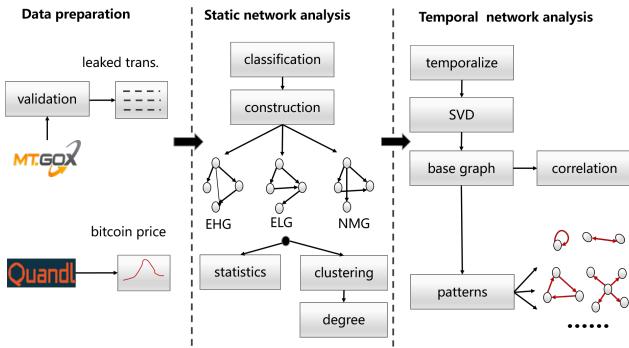


Fig. 2. An overview of our analysis.

In summary, we make the following major contributions.

- To the best of our knowledge, it is the first study on market manipulation of cryptocurrency via graph analysis and SVD. Besides, we prove the effectiveness of the method by applying to the leaked Mt. Gox transaction data.
- We obtain many new observations and findings by characterizing the activities of different accounts (i.e., static network analysis) and adopting SVD on the daily snapshots of the graphs (i.e., temporal network analysis). These findings convinced us that there are many market manipulation behaviors in the exchange.

- We detect many market manipulation patterns which have never been reported in this area. These patterns are strong evidence of market manipulation and can help investors and regulators to recognize the dark side and its severity of the market.

The rest of the paper is organized as follows. After introducing the data set in Section II, we detail the static network analysis in Section III and the temporal network analysis in Section IV. Finally, we provide some related works in Section V and conclude the paper in Section VI.

II. DATA SET

In early 2014, the transaction history from April 2011 to November 2013 of Mt. Gox was leaked in the form of CSV files. Table I reports a segment of the leaked data recorded on 2013/10/01. Two rows with the same *Trade_Id* indicating a complete transaction from the seller (*Type=sell*) to the buyer (*Type=buy*). The volume of the transaction is recorded in *Bitcoins* and the turnover in *Money*, thus the real-time price of Bitcoin at the transaction moment is *Money/Bitcoins*. Each user has a unique identity (*User_Id*) with the FIPS location codes recorded in the country (*User_Country*) and state (*User_State*) fields. These are some other attributes (e.g., transaction fees) not included in the table, as they are not used in this study.

Data Cleaning. As there are many duplicate entries in the leaked data, we adopt a similar way for data cleaning as the previous studies [4], [9]. Specifically, we use the combination of the four key fields: date, user ID, type, and Bitcoins to remove duplicated entries (de-duplication strategy 2 in [4]). After this step, we remove all the single row transaction to make sure that each transaction has the corresponding buyer and seller (i.e., a completed transaction). Then, we remove all duplicated complete transactions. By doing this, the data narrows from approximately 18 million rows to 13.5 million rows (i.e., 6.7 million completed transactions). This method is more strict than the method in [9] as complete transactions with the same *trade_id* are treated as duplicates. We adopt a more strict method in the hope of providing more reliable results.

Advantages. The leaked Mt. Gox data has many advantages in understanding the transaction behaviors in cryptocurrency and its influence in the price. First of all, Mt. Gox was the dominant exchange and Bitcoin has been the main cryptocurrency during the period, thus analyzing the cryptocurrency market based on this data set is more reliable and representative. Second, these data are much more finely grained than data extracted from the blockchain since most trading activity is recorded only in the exchange. Furthermore, users can be identified by their accounts in the leaked data while it is hard in blockchain to identify a user because of its anonymous mechanism.

TABLE I
A SEGMENT OF THE LEAKED DATA.

Trade_Id	Date	User_Id	Type	Currency	Bitcoins	Money	User_Country	User_State
1380587338975940	2013/10/1 0:28:58	125439	buy	USD	0.5	71.69169	US	NC
1380587338975940	2013/10/1 0:28:58	295701	sell	USD	0.5	71.69169	CA	QC
1380739642844790	2013/10/2 18:47:22	609336	buy	USD	0.26177217	33.96631	US	PA
1380739642844790	2013/10/2 18:47:22	36865	sell	USD	0.26177217	33.96631	US	CA

III. STATIC NETWORK ANALYSIS

A. Account Classification

Before delving deeper into the Mt. Gox leaked data, we check the Bitcoin exchange price of each transaction (i.e., Money/Bitcoin) to inspect whether it falls between the highest and lowest exchange price of the disclosed price on the same day. To this end, we first download all the Bitcoin exchange rate (BTC vs. USD) on Mt. Gox from quandl.com (we call this *reference price*). Then, we compare the exchange price of each transaction with the reference price. Surprisingly, we find that there are some abnormal transactions which have a very high or low exchange price. For example, on 2013/08/30, a transaction (trade_ID=1377875127221631) had an exchange price of \$49,338.4/BTC, and another transaction (trade_ID=1377876535345547) had an exchange price of only \$0.81/BTC, whereas, on the same day, the highest and lowest exchange price in the download data are \$142.76/BTC and \$128.56/BTC respectively.

These transactions are abnormal, as the exchange price is clearly out of the reasonable range. In order to distinguish the transaction behavior of different accounts and its influence on the price, we divide all the accounts into three categories: extremely high account (EHA), extremely low account (ELA) and normal account (NMA). As a first step, we apply a simple approach to identify an *abnormal* transaction. For this, suppose the highest and the lowest reference price on day t is H_t and L_t , we regard an transaction with real-time price larger than $1.5 \times H_t$ as an extremely high price transaction (EHT) and with real-time price lower than $0.5 \times L_t$ as an extremely low price transaction (ELT). Both kinds of transactions are referred to as abnormal transactions (ABTs). Please note that we use $(0.5 \times L_t, 1.5 \times H_t)$ instead of (L_t, H_t) to identify an abnormal transaction because there are many exchanges (thus many reference price) at the same time and we cannot make sure the reference price is the real price of the exchange. However, the parameter 0.5 and 1.5 is enough to exclude any normal transaction. Finally, an account is an EHA if it has at least one extremely high price transaction and an ELA if it has at least one extremely low price transaction. Both EHAs and ELAs are referred to as abnormal accounts (ABA). Please note that abnormal accounts could be both an EHA and an ELA if it involves both EHT and ELT. NMA is an account involved in no abnormal transactions, that is to say, all involved transactions are normal transactions (NMT).

Table II shows the number of accounts and all kinds of transactions for each category of account. Four observations can be made from the table: 1) there are 14916 abnormal

TABLE II
STATICS OF ACCOUNTS AND TRANSACTIONS.

Category	#accounts	#Tx	#ABT	#EHT	#ELT
EHA	10702	1406850	179701	138743	40958
ELA	5835	2486807	85784	29737	56047
ABA	14916	3025992	194790	138743	56047
NMA	104427	812865	0	0	0
All	119343	6775117	194790	138743	56047

accounts, which account for 12.5% ($14916/119343$) of all the accounts (please note that the number of ABA is not the sum of the number of EHA and ELA due to the existence of accounts contained in both categories); 2) the proportion of abnormal transactions (#ABT) among ABAs accounts for 2.8% ($\approx 194790/6775117$); 3) the number of normal transactions among ABAs ($3025992-194790=2831202$) account for more than 41% ($2831202/6775117$) of all transactions; and 4) the sum of the number of transactions (#Tx) among ABAs and NMAs is far less than the number of all transactions, thus many transactions occurred between ABA and NMA.

Based on these observations, one can confirm that the abnormal transactions do not occur by accident (observation 2) and the abnormal accounts behave normally in most of their times (observation 3). Thus, the existence of the abnormal accounts must have a certain special purpose. One of the most likely purposes is for providing liquidity (observation 4, Section III-C). Considering the analysis on the recent cryptocurrency market of a trader and investor, which report that in some exchanges most of their disclosed trading volume are fake [10], another possible purpose for these accounts is for fake volume. Besides, price manipulation is also a likely purpose (Section IV). In fact, we find that the abnormal transactions are greatly correlated with the Bitcoin exchange price and there are many abnormal patterns in the transactions.

B. Graph Construction

As each transaction contains a buyer and a seller, we can easily construct a directed graph from the records by considering each account as a node. Specifically, we present the definition of the constructed graph G as follows.

Graph Definition. $G = (V, E, w)$, where V is a set of nodes represent users (denoted by user ID) in the leaked data, E is a set of edges with each represents an *ordered* pair of nodes and w is the function associating each edge to a weight. Each pair indicates that there was at least one transaction between users u (seller) and v (buyer) in the whole dataset. $w : E \rightarrow \mathbb{R}_+$ maps each edge with a weight, which is the

total amount of Bitcoins transferred along the edge by one or more transactions.

In the remainder of this paper, we use the term *account*, *user* and *node* interchangeably. To better compare network characteristics, we construct three graphs according to the nodes' categories as follows:

- EHG. The graph that all nodes are EHAs.
- ELG. The graph that all nodes are ELAs.
- NMG. The graph that all nodes are NMAs.

To construct the graph we adopt the following steps. Since each complete transaction has both a buy and sell record (has the same transaction ID) after data validation, we first construct a set of tuples (S, B, v, t, l) from every complete transaction, where S and B represents the seller and buyer (denoted by user ID), v is the corresponding amount of the transaction in Bitcoin, t is the transaction time and l is a label indicating the category of the transaction (i.e., EHT, ELT or NMT). We call this set as *transaction tuple*, as each tuple corresponds to a unique transaction. Based on the transaction tuple, the aforementioned graphs are easy to construct. For example, to construct the EHG, we select all the tuples in which both the seller and the buyer are EHAs and sum the v entry grouped by S and B . Then, the generated new tuples (S, B, v) is the EHG. Other graphs are constructed as the same except by selecting different tuples according to the nodes' category.

C. Graph Analysis

This subsection investigates the constructed graphs from various metrics in graph analysis. Figure 3 shows the three graphs. We can find that there are more nodes in NMG, indicating the NMG is more sparse in connection (note that we select 5,000 edges for each graph). Furthermore, there are more big nodes in EHG, which means there are more active accounts in EHG. We investigate the statistics and metrics in the following.

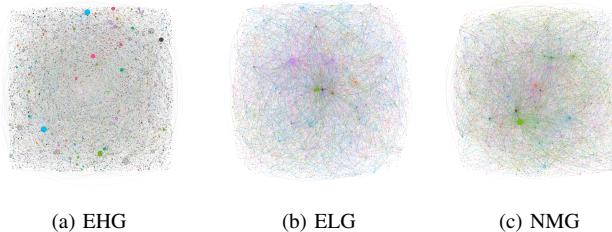


Fig. 3. Visualization of EHG, ELG, and NMG. For the ease of illustration, we randomly select 5000 edges from each graph to draw the figure.

Table III shows all the statistics and metrics for each constructed graph. For comparison, we also constructed the abnormal graph (i.e., the graph of all abnormal accounts, ABG) and the complete graph (i.e., the graph of all accounts, CG). In the following, we first introduce the statistics or metrics and then detail the observations.

The number of nodes in each graph is the number of accounts in each category, which is in accordance with the statistics in Table II. The only exception is that the number of nodes in NMG is less than the number of NMA, because some normal accounts interact with abnormal accounts, thus it is not included the NMG.

TABLE III
STATICS OF GRAPHS.

graph	# nodes	# edges	cluster	avg. degree	avg. wgt. degree
EHG	10702	212900	0.30	19.89	505.43
ELG	5835	413881	0.42	70.93	3107.68
ABG	14916	612885	0.31	41.09	1439.04
NMG	86457	655882	0.03	7.59	76.21
CG	119343	2682719	0.28	22.48	426.54

An edge in the graph indicates a “channel” between two accounts for buying or selling Bitcoin. As can be seen from the table, the number of edges in each graph is far less than the number of transactions, which means that many channels are used more than one times. Another notable result is that the summation of the number of edges in ABG and NMG is greatly less than the number of edges in the CG. This result indicates that many edges are the channels between normal and abnormal accounts and is evidence that the abnormal accounts provide liquidity in the exchange. The number of edges in ABG is slightly larger than the sum of the number of edges in EHG and ELG since there are some edges connecting EHAs and ELAs.

We compute the clustering coefficient of all the graphs in column 4 of Table III. As can be seen, the clustering coefficients are extremely different among EHG, ELG, and NMG. The large clustering coefficients (i.e., 0.3 in EHG and 0.42 in ELG) revealing that if two abnormal accounts A, B trade with abnormal account C , A and B are very likely to trade with each other. In other words, the abnormal accounts are likely to form triangles through transactions. Conversely, the clustering coefficient of NMG is very small (i.e., 0.03), which indicates a normal situation as the probability of three normal accounts forming a triangle is very small. This result indicates that the abnormal accounts behave strangely and herald the existence of market manipulation in the exchange.

The degree of a node is the number of edges connecting to the node. In our case, the degree of a node indicates the number of accounts trading with that node. Figure 4 shows the degree distribution of all the three graphs, all of which approximately follows the power law distribution, meaning that there are few large-degree nodes and many small-degree nodes. We estimate the parameters by using the free statistical software R [11] and the contributed package [12] and plot the fitting line $y \sim x^{-\alpha}$ for each distribution in red. The smaller the α , the more variable of nodes' degree. Thus, the abnormal accounts show less variable as compared with normal accounts. This result probably because the abnormal accounts are controlled by the same organizations.

Column 5 and 6 in Table III show the average degree and the weighted average degree of the graphs. The large

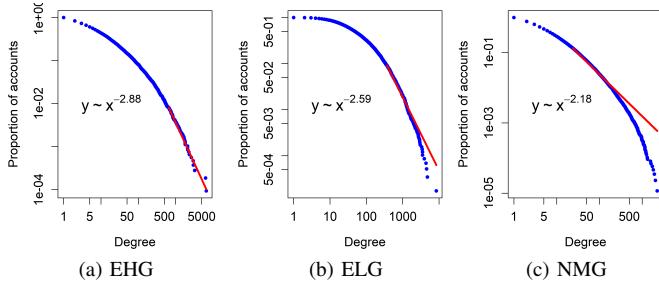


Fig. 4. Degree distribution of EHG, ELG and NMG.

average degree of EHG and ELG indicate that the abnormal accounts are used more frequently than normal accounts. The weighted degree is computed by setting the transaction volume (i.e., Bitcoin) as the weight, thus the average weighted degree represents the average transaction volume for each edge. As can be seen, the average weighted degree of ELG is far larger than it of EHG, one possible reason that the exchange price of transactions in ELG is relatively low, thus the transaction volume is large. Whatever the reason is, an obvious fact remains that the average weighted degree of EHG and ELG are larger than that of NMG, which means the edges between abnormal accounts transfer more Bitcoin than edges between normal accounts.

Based on the results and analysis discussed above, we summarize the findings as follows:

- **Finding 1.** There are some abnormal accounts (12.5%) which trading with very high or low exchange price in some transactions. We consider these accounts abnormal and under control by the exchange for two reasons: 1) the proportion of the abnormal transactions account for 2.8%, thus it is not occurred by accident; 2) the abnormal exchange price is impossible to appear on ordinary users.
- **Finding 2.** Many seemingly normal transactions occurred between abnormal accounts ($> 41\%$). There are two possible purposes for these transactions: 1) these transactions are the fake volume that used to create an illusion of active trading; 2) to provide liquidity for the exchange.
- **Finding 3.** The graphs of abnormal accounts have very large clustering coefficients. One possible reason is that these accounts are controlled by one organization, and thus the trade is not completely random.

These findings indicate that the exchange was likely involved in trading manipulation. As the exchange price is the key factor of trading, in the following section, we will discuss the possibility of price manipulation of the exchange.

IV. TEMPORAL NETWORK ANALYSIS

As discussed above, the transaction network of abnormal accounts (i.e., EHG and ELG) show a great difference from the NMG. We want to know whether these transactions have a correlation with the Bitcoin price and what kind of users and transactions (i.e., graph structure) influence the Bitcoin price greatly. To this end, we calculate the daily snapshots of the

graphs by adopting the method similar to III-B. To detect important changes in the graph structure, we compare successive snapshots of the graphs using singular value decomposition (SVD). The goal is to detect a set of base networks and represents each day's snapshot as a linear combination of these base networks. Unlike in Section III, we focused our study on transaction data after 2012/12/01 in this section. There are many reasons supporting our choice. Firstly, the recent paper which proves the price manipulation of Mt. Gox uses the same transaction history [9]. Secondly, the Bitcoin price experienced a rocket upsurge during this period. Thirdly, Mt. Gox was the main Bitcoin exchange during this period. Finally, more abnormal users and transactions (more than 60%) are found after that day.

A. Extract Base Networks

To evaluate which networks influence the price greatly, we need to construct the daily snapshots of the three graphs: EHG_t , ELG_t and NMG_t . We adopt the same process to construct the graph series. First of all, we construct the *aggregate* networks (i.e., EHG) based on tuples after 2012/12/01. Assume there are n nodes and L edges in the aggregate network, then it can be represented by a $n \times n$ weighted adjacency matrix G , in which there are L non-zero elements. We rearrange G into an L long vector g containing all the non-zero elements. We call this vector as *edge-weight* vector. The vector describes the *graph structure* of the aggregate network as each element represents a possible edge and its weight. To construct the daily snapshots of EHG_t on day t , we recalculate the edge-weight vector g_t (i.e., the graph structure on day t) based on transaction tuples on day t . Please note that we do not change the order of the vector, thus the i -th element of all the edge-weight vectors indicate the same edge, and it may be zero if the edge does not exist on a specific day. For T snapshots, we now build the $T \times L$ graph time series matrix X such that the t -th row of X equals g_t . By doing this, we build a special matrix with T samples and each sample represents a daily graph structure.

To account for the variation of the daily graph structure, we normalize X such that the sum of each row equals 1, and then subtract the column averages from each column. As a result, both the row and column sums in the matrix will be zero. We compute the singular value decomposition of the matrix X :

$$X = U\Sigma V^T, \quad (1)$$

where U is a $T \times T$ unitary matrix, Σ is a $T \times L$ diagonal matrix with non-negative values on the diagonal, and V is a $L \times L$ unitary matrix. The non-negative values on the diagonal are *singular* values and is usually sorted in descending order. The left-singular vectors containing in the column of U are a set of orthonormal eigenvectors of XX^T , and the right-singular vectors containing in the column of V are a set of orthonormal eigenvectors of X^TX . Since in this case $T < L$, there are only T nonzero singular values. We denote the sorted singular values as $(\sigma_1, \dots, \sigma_T)$, the left-singular vectors (u_1, \dots, u_T)

TABLE IV

CORRELATION COEFFICIENTS BETWEEN THE LEFT-SINGULAR VECTORS OF THE NETWORK TIME SERIES MATRIX AND THE BITCOIN EXCHANGE PRICE.

Graph	The 1st base network			The Fitted 10 base networks		
	ρ_P	ρ_S	ρ_K	ρ_P	ρ_S	ρ_K
EHG	0.56	0.60	0.44	0.811	0.807	0.620
ELG	0.58	0.82	0.64	0.871	0.834	0.652
NMG	0.05	0.15	0.12	0.239	0.398	0.289

and the right-singular vectors (v_1, \dots, v_T) , where u_i and v_i are column vectors and satisfy the following equations:

$$u_i^T * u_j = v_i^T * v_j = \delta_{ij}. \quad (2)$$

Based on the special meaning of matrix X , we can interpret the singular vectors and the singular values as 1) the right-singular vectors can be seen as *base networks*, and the element $v_i(l)$ (i.e., the l -th element of the i -th right-singular vector) gives the weight of the l -th edge in the i -th base network; 2) the left-singular vectors account for the temporal variation of the base networks, the t -th value of u_i (denotes as $u_i(t)$) provides the contribution of the i -th base network on day t ; 3) the singular value σ_i , which are the square roots of the non-zero eigenvalues of both $X^T X$ and XX^T , indicates the overall importance of the i -th base network in approximating the whole matrix. Please note that the singular values are sorted in decreasing order, thus give decreasing contribution to the result.

B. Detecting Graph Structural Changes

As the (normalized) weight of the l -th edge in the daily graph structure on day t can be written as:

$$x_{tl} = \sum_{i=1}^T \sigma_i u_i(t) v_i(l), \quad (3)$$

to detect graph structural changes, we need to consider two terms: σ_i (i.e., the importance of the i -th base network) and $u_i(t)$ (i.e., the contribution of the i -th base network on day t).

As a first glance, we consider the daily influence of the first and also the most important base network (i.e., $u_1(t)$). We want to know the correlation between the variation of $u_1(t)$ and the fluctuation of the Bitcoin exchange price. As the range of the price is (12, 1207), we adopt a simple mathematical transform to make sure most of the transformed price falls in the interval (0, 1). Specifically, we adopt the log transform $B(t) = \log_{1000} P(t)$, where $P(t)$ is the close exchange price of Bitcoin on day t . Table IV (left part) shows three commonly used correlation coefficients (i.e., Pearson, Spearman, and Kendall correlation coefficient) between $u_1(t)$ and the log-transformed price $B(t)$. The results show that the daily variation of the first base network in EHG and ELG have a very strong correlation with the Bitcoin exchange price. However, in NMG, there is no correlation between the two variables. The result indicates that the transactions made between abnormal accounts have a great influence on the Bitcoin exchange price.

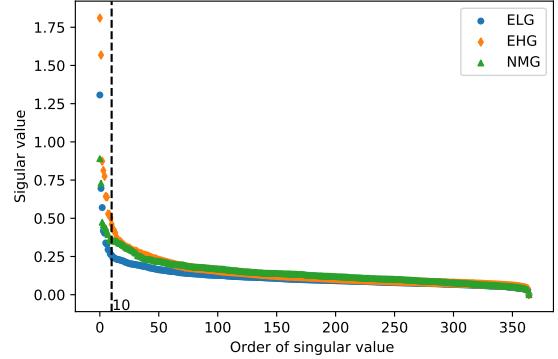


Fig. 5. Singular values in the order of its importance.

Motivated by this result, we want to know, to what extent, the log transferred price can be estimated with the combination of the left-singular vectors, i.e.,

$$B(t) \sim c_0 + \sum_{i=1}^N c_i u_i(t), \quad (4)$$

where c_0 is the mean of $B(t)$ and c_i can be computed as the dot product of $B(t)$ and $u_i(t)$. As the left-singular vectors are orthonormal and span the T -dimensional linear space, $B(t)$ can be reconstructed by $u_i(t)$ when $N = T$. However, this is not what we desire in this case. The purpose of this study is to identify some important base networks and accounts which have a great influence on the Bitcoin price. To proceed, we first try to select some important base networks in the detected base networks. We draw the scree plot of the singular values as shown in Fig. 5. As can be seen from the graph, the curve of the singular values is clearly leveling off at the right side of the dotted line (i.e., the 10th singular value). Thus, we select the first 10 base networks for the following analysis.

Before analyzing accounts in the selected base networks, we approximate $B(t)$ with the selected networks. To evaluate the fitting effect, we calculate the correlation coefficients between the fitted price series and $B(t)$. The right part of Table IV shows the correlation coefficients. Surprisingly, the three correlation coefficients are greatly enhanced as compared with the first left-singular vector. Especially, the Pearson correlation coefficient between ELG and $B(t)$ is 0.87, while only 0.24 between NMG and $B(t)$. The great difference indicates a strong correlation between abnormal accounts' transactions and the Bitcoin exchange price, which is a strong evidence of the price manipulation in Mt. Gox.

Figure 6 shows the trends of $B(t)$ and the fitted price. As can be seen from the graph, though the shape of the peak in April of 2013 is missed, the trends of $B(t)$ has been grasped by the selected base networks of EHG and ELG, whereas the base networks in the NMG have no effect in grasping the trend.

To show the structure variation of the networks, we draw the time-varying contribution $u_i(t)$ of the first four base networks

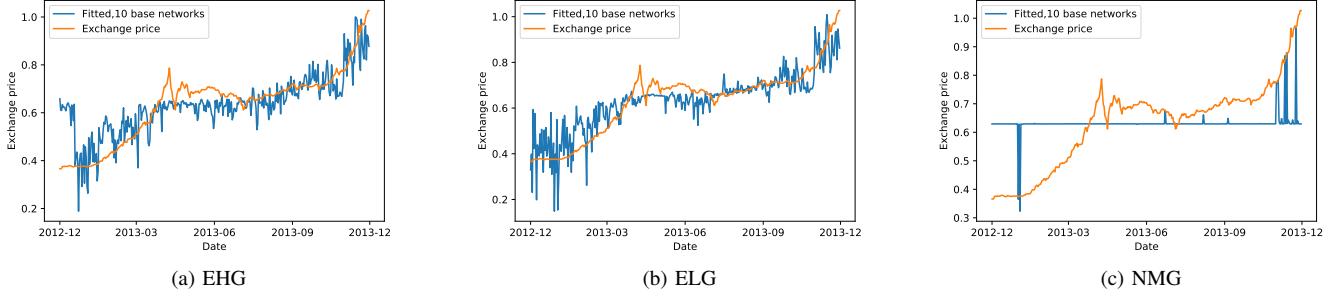


Fig. 6. Approximate the log-transformed Bitcoin price with the linear combination of the selected base networks of EHG, ELG, and NMG.

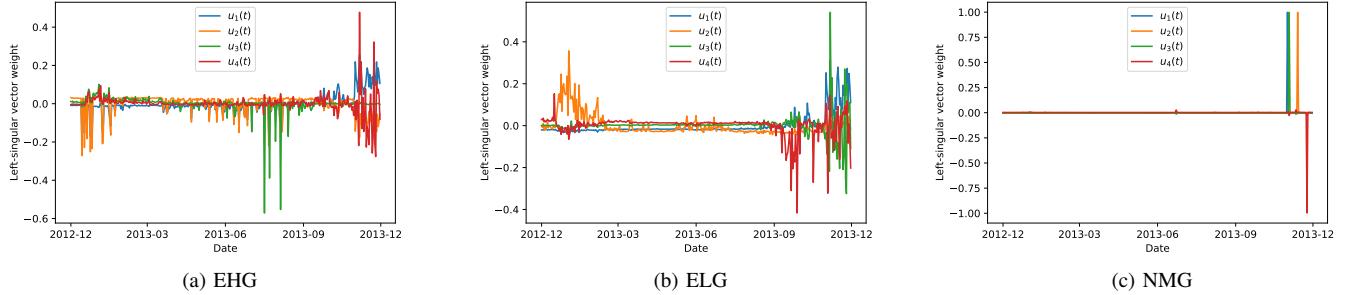


Fig. 7. The time-varying contribution $u_i(t)$ of the first four base networks.

in Fig. 7. In most cases, $u_i(t)$ exhibit a few abrupt changes, partitioning the history of the transaction into separate time periods. The most notable abrupt changes are in December of 2012 when the Bitcoin exchange price is very smooth and the November of 2013 when the price upsurge. During the two periods, the effects of the first four base networks of EHG and ELG are both significant, however, the base networks in NMG have no distinct effect during the smooth period and show effect only a few days during the upsurge period.

C. Abnormal transaction patterns

As discussed above, the transactions between abnormal users have a great correlation with the Bitcoin exchange price. A natural question is which edges (i.e., transactions) and thus accounts are the most influential and whether the transactions show certain patterns during the period. To this end, based on the extracted 10 base networks, we further extract the top-10 ranking edges (by the absolute value of weights) in each base networks. We find only 44 distinct edges instead of the 100 maximally possible, which including a total of 28 accounts in EHG. In ELG, 57 edges and 46 accounts were found. We call these *core abnormal accounts*.

To identify special transaction patterns, we draw the daily subgraph of the core abnormal accounts. We find that there are many abnormal transaction patterns (i.e., market manipulation patterns) in the networks. In order to save space, we show only 6 typical patterns in Fig. 8. These subgraphs are all extracted from ELG on different days. In order to illustrate

more clearly, we fix the layout of the graph (i.e., the position of the accounts in each graph is fixed) and denote the special patterns in red. The size of the line denotes the number of transactions between the two accounts. The number at the right-hand side of the directed edge represents the number of transactions between the two accounts. We simply explain the 6 patterns as follows:

- **Self-Loop.** A pattern that an account made transactions with itself. Figure 8a shows subgraph on 2013/02/07, the account 231 made 749 transactions with itself. Self-Loop is restricted for normal accounts in any exchanges, as it makes no sense. Thus, a reasonable explanation for the self-loop pattern is that the account may belong to the exchange and may be used to increase daily transaction volume or price manipulation.
- **Unidirection.** The unidirectional pattern indicates more than one transaction from account A to B . Figure 8b shows a unidirectional pattern on 2013/08/15, where account 527332 made 322 sell transactions to account 231. It is possible for an account to sell Bitcoin to another account for more than one times, however, it is impossible for two normal accounts to interact with such a large number of times on the same day.
- **Bi-direction.** The bi-directional pattern is a typical market manipulation behavior, especially when the two accounts are controlled by the same user, that two accounts interact with each other many times. Figure 8c shows the bi-direction pattern on 2013/04/14 where account 144834

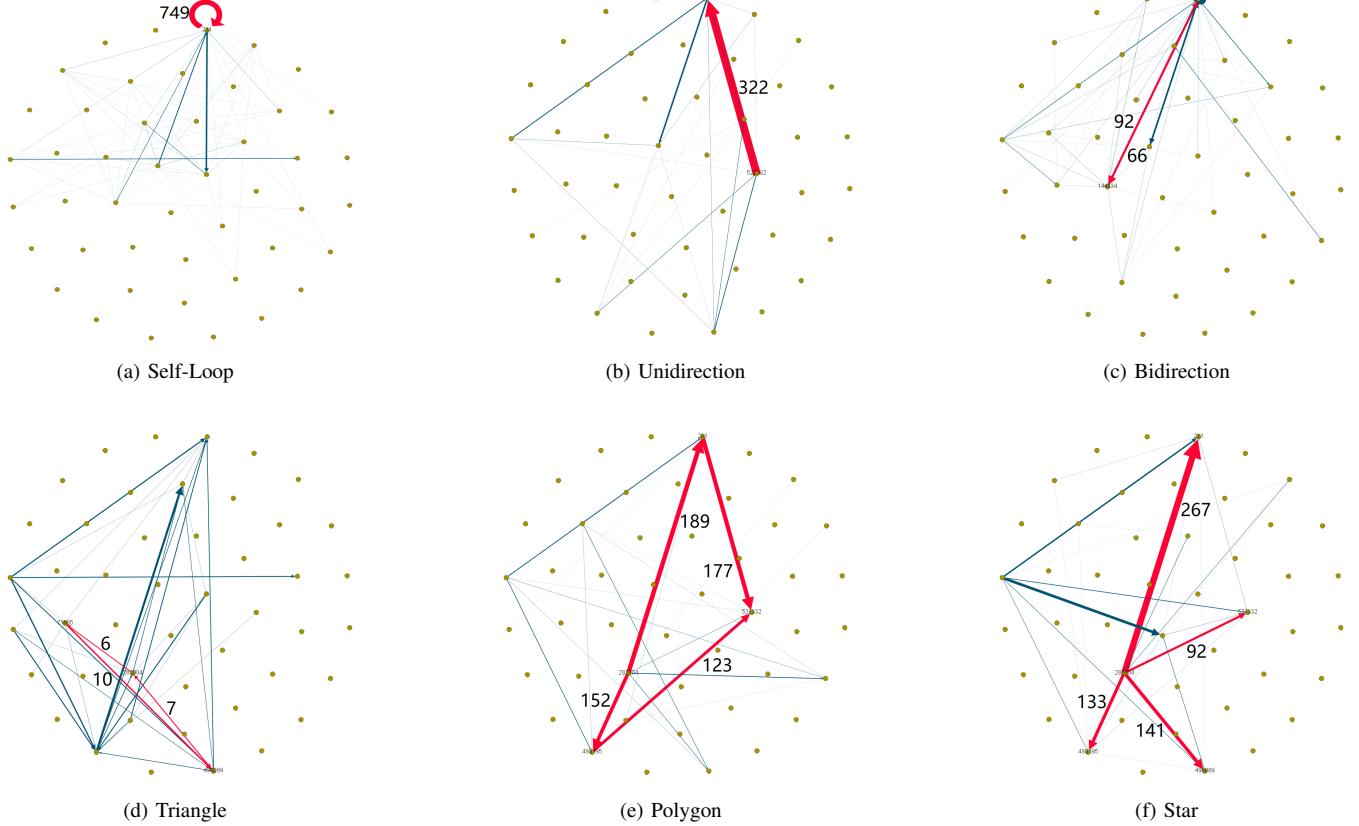


Fig. 8. Some typical abnormal transaction patterns

interact with account 231 for more than 150 times. Same as in unidirection, it is also impossible for two normal accounts to have such a high transaction frequency.

- **Triangle.** The triangle pattern indicates a triangle-like structure between three accounts. It may contain various forms when considering the direction of the edge. Figure 8d shows a special form of triangle pattern on 2013/10/25. It is special because the accounts form a loop through transactions (account 282004 → 71885 → 490089 → 282204). Though the numbers for each edge are not very large, it still large enough to make sure that it is impossible to appear among normal accounts.
- **Polygon.** Polygon pattern is a more complicated transaction pattern where many accounts form a polygon-like group with each edge has more than one transactions. Figure 8e shows a quadrangle pattern on 2013/09/19, it seems that account 282004 sends Bitcoin to account 527332 through the “bridge accounts” 488195 and 231 for more than two hundred transactions.
- **Star.** A star pattern has a core account that buys or sells Bitcoin to many accounts. Figure 8f shows a typical star, where the account 282004 sell Bitcoin to accounts 488195, 490089, 527332 and 231.

Generally speaking, it is not surprising for a transaction network to form a special structure, as transactions are random.

However, in our case, it is impossible as each edge represents far more than one transaction in a single day. Thus, it seems quite possible that these accounts are controlled by a certain group and these transactions have special purposes.

Based on the results, we summarize the findings as follows:

- **Finding 4.** The daily fluctuation of the selected base networks of EHG and ELG have a strong correlation with the Bitcoin exchange price. On the contrary, the daily fluctuation of the base networks of NMG has no correlation with the Bitcoin exchange price. This finding indicates that the behavior of the abnormal accounts’ transaction affects the fluctuation of Bitcoin exchange price.
- **Finding 5.** The trend of the Bitcoin exchange price can be captured by the selected base networks of EHG and ELG. It means that the trend of the price can be predicted by transactions between abnormal accounts.
- **Finding 6.** There are many unusual transaction patterns (e.g., self-loop, bi-direction, star) between abnormal accounts. These patterns imply that these accounts are controlled by the same group and are strong evidence of price manipulation.

V. RELATED WORK

Our research is related to previous work in two areas. The first related area is the study of understanding the big

fluctuation of Bitcoin price. As aforementioned, many driving factors of the price are found. Due to all the related data are time series, the most used method in the analysis is time series based model such as vector space model [13], vector error-correction model [14], ARDL bounds testing method [15], wavelet analysis [6], and vector autoregressive [14]. However, as we have daily transaction records of the most famous exchange, we can do a completely different analysis. Due to the efficiency of graph analysis in understanding the complicated relationship, for example, the recent study adopt graph analysis in analyzing the Ethereum network and obtain many insights [16], we adopt graph analysis to the transaction network. The results show that this method provides a different perspective on this problem. Furthermore, we adopt SVD to the reconstructed daily graph and find that there exists a strong correlation between the abnormal transactions and the Bitcoin price.

Another related area is the study of the blockchain data (i.e., the transaction ledger and other related data of the cryptocurrency) for different topics. Due to the publicly accessible of the blockchain data and users are anonymous in the system, a common topic is to mining the blockchain data to reveal users' privacy [17]–[20]. Because of the relatively lawless nature, blockchain has become an area full of various scams. Thus, mining the blockchain data to detect scams is also a critical topic. Recently, there are many studies on this topic, such as Bitcoin-based scams [21], the smart contract (a program runs on blockchain system [22]) based Ponzi schemes [23], [24], money laundry [25].

VI. CONCLUSION AND FUTURE WORK

We conduct a systematic study to analyze the leaked Mt. Gox transaction data through graph analysis. By comparing the transaction price of the transaction data with the disclosed daily price, many abnormal transactions identified and were used to divide the accounts into three categories. Based on this classification, we construct three graphs (i.e., EHG, ELG, and NMG) and obtain many findings by analyzing these graphs through various metrics. These findings convinced us that there are many market manipulation behaviors in the exchange. In order to reveal the relationship between these behaviors and the Bitcoin price, the graphs are reconstructed into daily graph series and reshaped into matrices. Through adopting SVD to the matrices, some very important base networks are identified. By inspecting the base networks, we find that the daily variation of the abnormal base networks closely related to the Bitcoin price and many market manipulation patterns. Based on these findings and considering Bitcoin is dominant in the market, we propose to strengthen supervision in this market. In the future, we will conduct a more thorough study of the data to reveal the extent to which the market is affected and to discuss the changes in the behavior of investors under the extreme fluctuation price.

REFERENCES

- [1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
- [2] C. Burniske and A. White, "Bitcoin: ringing the bell for a new asset class," *Ark Invest (January 2017)* https://research.ark-invest.com/hubfs/1_Download_Files_ARK-Invest/White_Papers/Bitcoin-Ringing-The-Bell-For-A-New-Asset-Class.pdf, 2017.
- [3] Bitcoin wiki, "Laszlo hanyecz," May 2017. [Online]. Available: https://en.bitcoin.it/wiki/Laszlo_Hanyecz
- [4] A. Feder, N. Gandal, J. Hamrick, and T. Moore, "The impact of ddos and other security shocks on bitcoin currency exchanges: Evidence from mt. gox," *Journal of Cybersecurity*, vol. 3, no. 2, pp. 137–144, 2018.
- [5] M. Buchholz, J. Delaney, J. Warren, and J. Parker, "Bits and bets, information, price volatility, and demand for bitcoin," *Economics*, vol. 312, 2012.
- [6] L. Kristoufek, "What are the main drivers of the bitcoin price? evidence from wavelet coherence analysis," *PloS one*, vol. 10, no. 4, p. e0123923, 2015.
- [7] L. Kristoufek, "Bitcoin meets google trends and wikipedia: Quantifying the relationship between phenomena of the internet era," *Scientific Reports*, vol. 3, p. 3415, 2013.
- [8] D. Kondor, I. Csabai, J. Szűle, M. Pósfai, and G. Vattay, "Inferring the interplay between network structure and market effects in bitcoin," *New Journal of Physics*, vol. 16, no. 12, p. 125003, 2014.
- [9] N. Gandal, J. Hamrick, T. Moore, and T. Oberman, "Price manipulation in the bitcoin ecosystem," *Journal of Monetary Economics*, vol. 95, pp. 86–96, 2018.
- [10] S. Ribes, "Chasing fake volume: a crypto-plague," Mar. 2018. [Online]. Available: <https://medium.com/@sylvainartplayribes/chasing-fake-volume-a-crypto-plague-ea1a3c1e0b5e>
- [11] R Core Team, *R: A Language and Environment for Statistical Computing*, R Foundation for Statistical Computing, Vienna, Austria, 2016. [Online]. Available: <https://www.R-project.org/>
- [12] C. S. Gillespie, "Fitting heavy tailed distributions: The poweRlaw package," *Journal of Statistical Software*, vol. 64, no. 2, pp. 1–16, 2015. [Online]. Available: <http://www.jstatsoft.org/v64/i02/>
- [13] I. Georgoula, D. Pournarakis, C. Bilanakos, D. Sotiropoulos, and M. G. Giaglis, "Using time-series and sentiment analysis to detect the determinants of bitcoin prices," Available at SSRN:<https://ssrn.com/abstract=2607167>, 2015.
- [14] P. Ciaian, M. Rajcaniova, and d. Kancs, "The economics of bitcoin price formation," *Applied Economics*, vol. 48, no. 19, pp. 1799–1815, 2016.
- [15] J. Bouoiyour, R. Selmi *et al.*, "What does bitcoin look like?" *Annals of Economics and Finance*, vol. 16, no. 2, pp. 449–492, 2015.
- [16] T. Chen, Y. Zhu, Z. Li, J. Chen, X. Li, X. Luo, X. Lin, and X. Zhang, "Understanding ethereum via graph analysis," in *IEEE Conference on Computer Communications (INFOCOM 2017)*. IEEE, 2018, pp. 1–9.
- [17] F. Reid and M. Harrigan, "An analysis of anonymity in the bitcoin system," in *Security and Privacy in Social Networks*. Springer, 2013, pp. 197–223.
- [18] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun, "Evaluating user privacy in bitcoin," in *International Conference on Financial Cryptography and Data Security*. Springer, 2013, pp. 34–51.
- [19] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A fistful of bitcoins: Characterizing payments among men with no names." ACM Press, 2013, pp. 127–140.
- [20] S. Athey, I. Parashkevov, V. Sarukkai, and J. Xia, "Bitcoin pricing, adoption, and usage: Theory and evidence," 2016.
- [21] M. Vasek and T. Moore, "There's no free lunch, even using Bitcoin: Tracking the popularity and profits of virtual currency scams," in *International Conference on Financial Cryptography and Data Security*. Springer, 2015, pp. 44–61.
- [22] N. Szabo, "Smart contracts: Building blocks for digital markets," Sep. 1996. [Online]. Available: <http://www.fon.hum.uva.nl/>
- [23] M. Bartoletti, S. Carta, T. Cimoli, and R. Saia, "Dissecting ponzi schemes on ethereum: Identification, analysis, and impact," 2017.
- [24] W. Chen, Z. Zheng, J. Cui, E. Ngai, P. Zheng, and Y. Zhou, "Detecting ponzi schemes on ethereum: Towards healthier blockchain technology," in *Proceedings of the 2018 World Wide Web Conference on World Wide Web*. International World Wide Web Conferences Steering Committee, 2018, pp. 1409–1418.
- [25] M. Moser, R. Bohme, and D. Breuker, "An inquiry into money laundering tools in the bitcoin ecosystem," in *eCrime Researchers Summit (eCRS), 2013*. IEEE, 2013, pp. 1–14.