Winter 12-6-2018

Structural Pattern Recognition of Fraudster Groups in P2P Transaction Websites

Jinya Hu

Feng Li

Yanfeng Wang

Dong Zhuang

Hu, J.Y., Li, F., Wang, Y.F. & Zhuang, D. (2018). Structural pattern recognition of fraudster groups in P2P transaction websites. In *Proceedings of The 18th International Conference on Electronic Business* (pp. 604-613). ICEB, Guilin, China, December 2-6.

Structural Pattern Recognition of Fraudster Groups in P2P Transaction Websites

(Full Paper)

Jinya Hu*, School of Business Administration, South China University of Technology, China, bmhujinya@mail.scut.edu.cn
Feng Li, School of Business Administration, South China University of Technology, China, fenglee@scut.edu.cn
Yanfeng Wang, School of Business Administration, South China University of Technology, China, bmyfwang@mail.scut.edu.cn
Dong Zhuang, School of Business Administration, South China University of Technology, China, dzhuang@scut.edu.cn

ABSTRACT

The advent of online platform economy has increased online fraudsters. To detect them, most research explored to recognize characteristics from behavioral data of online users. In those works, each user was regarded as an individual subject, while relationship between users was underestimated. This paper introduced methodology of social network analysis to mine characteristics of relationship among online fraudsters. Using dataset from a Bitcoin trading website, a weighted signed network is constructed. By removing normal user nodes from the network, relationships between fraudsters are clarified. Then, major structural patterns of the snipped network are uncovered by way of community partitioning method. Based on real data from the Bitcoin trading website, 3 typical structures of fraudster groups are found: star-shaped structure, double-core structure and reticular structure.

Keywords: Platform economy, fraudster detection, structural pattern, weighted signed network

*Corresponding author

INTRODUCTION

An Online Platform Economy (OPE) refers to a kind of virtual marketplace that facilitates transactions between buyers and sellers (Farrell & Greig, 2016). It is an emerging form of e-commerce, as business model of eBay, Airbnb and Uber is increasingly popular. The remarkable success of OPE is derived from its peer-to-peer (P2P) transaction model. Compared to the traditional transaction model, the P2P platform facilitates a marketplace allowing individual buyers and sellers to interact with each other directly. In this way, both buyers and sellers would benefit from the decreasing of transaction cost.

However, P2P transactions have increased online fraudsters because the transactions are without participation or intermediation from the platform. Fraudsters may take advantage of the P2P mechanism and extract money from the innocent users. So, users need to take the responsibility themselves to avoid being cheated. To help users to be aware of counterparty risk, the platform usually introduced a credit rating mechanism. For example, eBay presents the total number of positive and negative feedback ratings for transactions for users that ended in the last 12 months. Similar credit rating system in Bitcoin trading platform Bitcoin-OTC is named 'web of trust'. By this way, users can access others' trade history and credit record. Nevertheless, this mechanism cannot overcome the problem of singularity standard as it only pays attention to the total number of ratings and ignored the users' internal relationships, which makes it difficult to recognize fraudster groups. The description above can be verified from disclaimers of Bitcoin-OTC: "...a scammer creates a bunch of bogus accounts who all inter-rate each other."

At present, the credit rating system treats user as an individual person, ignoring inter-relationship between users. So, characteristics of group fraudsters are underestimated for detecting fraudsters. This paper use methodology of social network analysis to represent the relationship between users as a weighted signed network, and analyze internal structures among fraudsters.

The rest of this paper is organized as follows: A brief introduction of related works will be given in section 2. Section 3 is devoted to the basic aspects of the Bitcoin exchange website Bitcoin-OTC and the dataset used in this research. Section 4 first demonstrates the five-step approach that is used in this paper to detect fraudster groups: constructing the weighted signed network from dataset, classifying nodes of the network, filtering nodes, detecting communities and pruning the network. In section 5 of this paper, the structural analysis is performed based on the results above. Finally, the conclusion of the whole paper is discussed in the last section.

RELATED WORKS

Credit Model

With the emerging of online platform economy, the problem of trading risks becomes an important issue. There has been a rising interest in design of credit rating mechanism. These researches mainly focused on building the quantitative model. Marsh (1994) first tried to introduce trust relationship into the Internet environment, who proposed a model based on social properties of trust. The model focuses on the personal experiences and tried to integrate many aspects related to trust. However, the model is too impractical and inaccessible. Later, Abdul-Rahman and Hailes (2000) simplified some obscure concepts proposed by Marsh. Based on Marsh's work, they divided trust into "direct" and "indirect" trusts. The direct trust refers to an agent feeling towards another agent. According to the extent of trust, the direct trust can be classified into 4 levels. As for the indirect trust, Abdul-Rahman and Hailes (2000) believe indirect trust generated from word-of-mouth. After that, Josang and Ismail (2002) proposed Beta model based on Bayesian theory where credit scores are statistically updating beta probability density functions. The Beta method uses probability density function to calculate credit ratings and increase the weights of recent transactions, which accords with characteristics of human memory. Beside researches in literature, the pioneer eBay also practiced a well-known credit rating system. In eBay, buyers and sellers can rate each other after transactions. And the overall credit of a user is computed as the sum of these ratings over the last six months auction site. Buyers and sellers on eBay can open access users' credit. What's more, many other models are proposed from scholars (Beth, Borcherding, & Klein, 1994; Zacharia, Moukas, & Maes, 2000; Xiong & Liu, 2004). Although many studies of credit model have been reported and it is effective of using model to detect fraudsters, limited by the research method, little is known about the internal structures of fraudster groups.

Social Network Analysis

The technique we applied is referred to as Social Network Analysis (SNA), which is a method of quantitative research on social relationships based on mathematical tools such as graph theory and matrix (Wasserman & Faust, 1994). Assuming that relationships are important, social network analysis takes actors and their mutual relationships as the research content. It maps formal and informal relations between the actors and analyzes the relationship contained in the network through several indicators. In a social network, the nodes represent individuals, and an edge or arc between nodes indicates a direct relationship between the individuals.

During past decades, there has been an increasing interest in applying SNA to information science (Otte & Rousseau, 2002), innovation system (Cantner & Graf, 2006), biological questions (Croft, James, & Krause, 2008) and other fields. One of the most popular concepts in SNA is the small world whose most famous manifestation is the "six degrees of separation" concept proposed by Travers and Milgram (1967). After that, Boccaletti *et al.* (2006) proposed that our brain networks are small-world networks whether at macro or micro scales. In the case of social media, a research such as that conducted by Li and Du (2014) have proposed a framework to investigate the persuasiveness of opinion leaders in twitter bases on SNA where results show the framework can identify opinion leaders and their opinions effectively. As for the animal ecology field, Farine and Whitehead (2015) conduct an interesting research where SNA is applied to analyze animal social systems and test hypotheses and prove the SNA model could be used to explore how the rules influence group joining and leaving drive social structure.

Despite the numerous contributions of applied SNA, efforts in the direction of applying SNA to online user credit evaluation are very limited. Consequently, this paper is based on SNA to detect communities and explore the internal structures of fraudster groups. Some basic indicators often used in SNA are listed below.

(1) Degree: The degree k_i of a node i is the number of edges incident with the node, and is defined in terms of the adjacency matrix A as:

$$k_i = \sum_{j \in N} a_{ij} \tag{1}$$

If the graph is directed, the degree of the node has two components: the number of outgoing links (or arcs) $k_i^{out} = \sum_j a_{ij}$ (referred to as the out-degree of the node), and the number of ingoing (or arcs) $k_i^{in} = \sum_j a_{ij}$ (referred to as the in-degree of the node). The total degree is then defined as $k_i = k_i^{out} + k_i^{in}$ (Boccaletti *et al.*, 2006).

(2) The diameter characterizes the ability of two nodes to communicate with each other: the smaller the diameter is, the shorter is the expected path between them. Networks with a very large number of nodes can have a rather small diameter.

(3) A measure of the typical separation between two nodes in the graph is given by the average shortest path length, also known as characteristic path length, defined as the mean of geodesic lengths over all couples of nodes (Boccaletti *et al.*, 2006).

$$L = \frac{N}{N(N-1)} \sum_{i,j \in N, i \neq j} d_{ij} \tag{2}$$

(4) Network density refers to the proportion of direct ties in a network relative to the total number possible (Intanagonwiwat *et al.*, 2002). It equals to the ratio between the actual number of edges or arcs in the network and the upper limit of the number of edges

or arcs that can be accommodated. Network density describes the overall level of interaction of network nodes. The density of an undirected network with *N* nodes and *L* actual edges is

$$d(G) = \frac{2L}{N(N-1)} \tag{3}$$

(5) Network centralization refers to an index demonstrating the overall centrality of the network graph based on the degree centrality of a node; it measures the connectivity of the whole network and dependence on few actors. Centralization reflects the extent to which interactions are concentrated in a small number of individuals rather than distributed equally among all members. The numerator of network centralization is

$$C = \frac{\sum_{i=1}^{n}[C_{max} - C_i]}{\max[\sum_{i=1}^{n}(C_{max} - C_i)]} \tag{4}$$

C_{max} is the maximum point of degree centrality in the graph. C_i is the degree centrality of node *i* (Freeman, 1978).

THE BITCOIN EXCHANGE WEBSITE AND DATASET

Introduction Of Bitcoin Trading Website

The P2P transaction website researched in this paper is Bitcoin-otc (https://www.Bitcoin-otc.com). The dataset used was published by a network analysis project from Stanford University. Like other P2P transaction websites, Bitcoin-otc does not have prescribed membership and strict transaction rules, where users trade through negotiation. Also, according to the site policy, the website does not conduct user qualification examination or take any responsibility for transactions. The individual buyers and the sellers shall take all transaction risks. Therefore, users on the website may be either normal users or fraudsters.

A credit rating mechanism is also set up to reduce transaction risks. Users can rate the trading objects after transactions and ratings can vary from -10 to +10 (integral and cannot be 0). As shown in table 1, the website gives guidelines for users to rate different people.

Table 1: Rating Guidelines from Bitcoin-otc

Rating	Guideline
10	You trust this person as you trust yourself. Reserve this for close friends and associates you know in person.
8	Large number of high-value transactions, long period of association, very trustworthy.
5	You've had a number of good transactions with this person.
1	One or two good transactions with this person
-1	Person strikes you as a bit flaky. Unreasonable/unexpected delays in payment, etc.
-10	Person failed to hold up his end of the bargain, took payment and ran, fraudster.

To summary, the credit rating mechanism is mainly based on the following rules:
(1) The higher ratings are given to the users, the better are their credit, and transaction risk is lower.
(2) If negative ratings are given to the users, their credit is worse, transactions might be risky.
(3) If positive and negative ratings are given, their credit is uncertain, and transactions may also be risky.

Therefore, if a user receives high ratings, it can be "initially" considered that the user is trust worthier than other users and the transaction credibility is high.

Risks And Vulnerabilities Of Current Mechanism

It is acknowledged that Bitcoin is a digital currency with no central authority. Bitcoin exchanges do not explicitly distinguish the payer or the payee. Therefore, the exchanges are in a cryptographic way and private keys are needed to authorize a fund transfer in transactions. Because of this form of Bitcoin transaction, there is a lag time between payment and delivering. The lag time causes remarkable risks vulnerabilities, as fraudsters can take the money or the private keys and disappear forever.

The credit rating mechanism is set up to reduce this transaction risks. However, since not all users are honest, there are still risks and vulnerabilities in Bitcoin-otc's credit rating mechanism. For example, several shills can give high ratings to a fraudster account first, thus improving the total rating of the fraudster account. Then, the fraudster account can defraud innocent users of their money. As shown in figure 1, the fraudster account received several positive ratings from 8 shill accounts (whose total ratings are negative) until 13:31 in September 10, 2012. However, several ratings of minus 10 were given to this user after 2 hours. The credit rating mechanism failed in the above-mentioned situation. We tend to consider the shills and fraudsters in the above situations are in close cooperation. In other words, they are in a fraudster group.

id	rater nick	rater total rating	rated nick	created at (UTC)	rating	notes
[redacted]	[redacted]	-14	[redacted]	2012-09-10 12:32:19	6	Good Seller
[redacted]	[redacted]	-11	[redacted]	2012-09-10 12:33:15	8	Sold me Btc for paypal
[redacted]	[redacted]	-17	[redacted]	2012-09-10 12:40:10	1	good seller
[redacted]	[redacted]	-3	[redacted]	2012-09-10 12:48:05	2	loaned me 4.5 bitcoins at 6% int. ty
[redacted]	[redacted]	-7	[redacted]	2012-09-10 12:51:30	1	bought btc for dwolla
[redacted]	[redacted]	-19	[redacted]	2012-09-10 13:27:43	1	bought btc for mp
[redacted]	[redacted]	-29	[redacted]	2012-09-10 13:29:40	1	loaned me 2 btc at 8% interest
[redacted]	[redacted]	-20	[redacted]	2012-09-10 13:31:57	2	bought btc pp
[redacted]	[redacted]	252	[redacted]	2012-09-10 15:27:36	-10	WARNING: Obvious shill account. Known Scammer AKA: dragonx cecil Bitman dknys dkny toocool ezekiell ninjaD ninjaA
[redacted]	[redacted]	109	[redacted]	2012-09-10 15:28:16	-10	Obvious shill account. Known Scammer AKA: dragonx cecil Bitman dknys dkny toocool ezekiell ninjaD ninjaA
[redacted]	[redacted]	353	[redacted]	2012-09-10 16:45:17	-10	WARNING: Obvious shill account. Known Scammer AKA: dragonx cecil Bitman dknys dkny toocool ezekiell ninjaD ninjaA
[redacted]	[redacted]	191	[redacted]	2012-09-10 22:06:09	-10	

Figure 1: A Typical Fraud Group and Victims

COMMUNITY DETECTION

Framework Of Community Detection

Figure 2 illustrates the process of detecting fraudster groups. Step 1 is the preparation stage where a weighted signed network is constructed based on the data collection extracted from Bitcoin-otc. This step allows us to analyze the data by taking advantage of Social Network Analysis in the following steps. After that, we conduct classification according to whether the nodes are rated negatively by other users. In Step 3, the nodes that were not classified as fraudsters were filtered. In this way, the network was snipped to a fraudster network, where nodes were all related with fraudsters. Once the normal user nodes are filtrated from the network, a community detection algorithm was applied to partition the fraudster groups. To discover the core fraudsters in each fraudster group, the snipped fraudster network is handled and optimized through pruning redundant nodes in the last step.

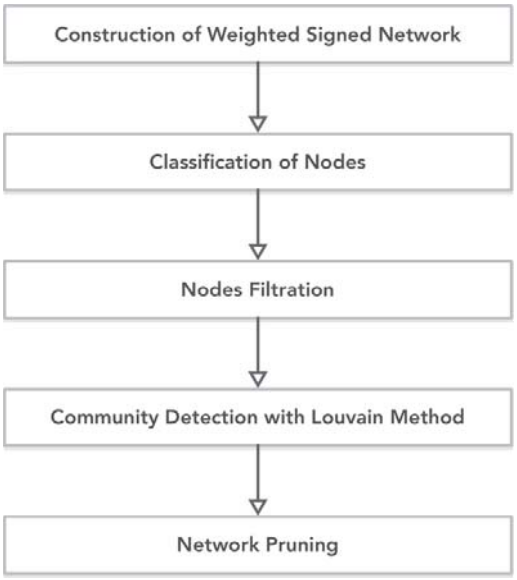


Figure 2: Five-step Approach to Detect Fraudster Groups

Construction Of A Weighted Signed Network

Many complex relationships in the real world can be modeled as social network and community detection algorithm can be used to find the fraudster groups. Firstly, we construct a weighted signed network from the rating dataset. In the network, each node represents a user on Bitcoin-otc platform, and each arc describes a user's rating action toward another user. The weights of arcs are positive or negative ratings received by the ratees. The data collection of Bitcoin-otc gives 35,592 comments, involving 5,881 users. Each data includes four aspects: Source, Target, Rating and Time. To avoid making the analysis more complicated, this paper ignores the evaluation time and only constructs the weighted signed network based on Source, Target, and Rating. Figure 3 shows the final weighted signed we constructed in Kamdam-Kawai layout. It can be observed that there is a lumping tendency within the network.

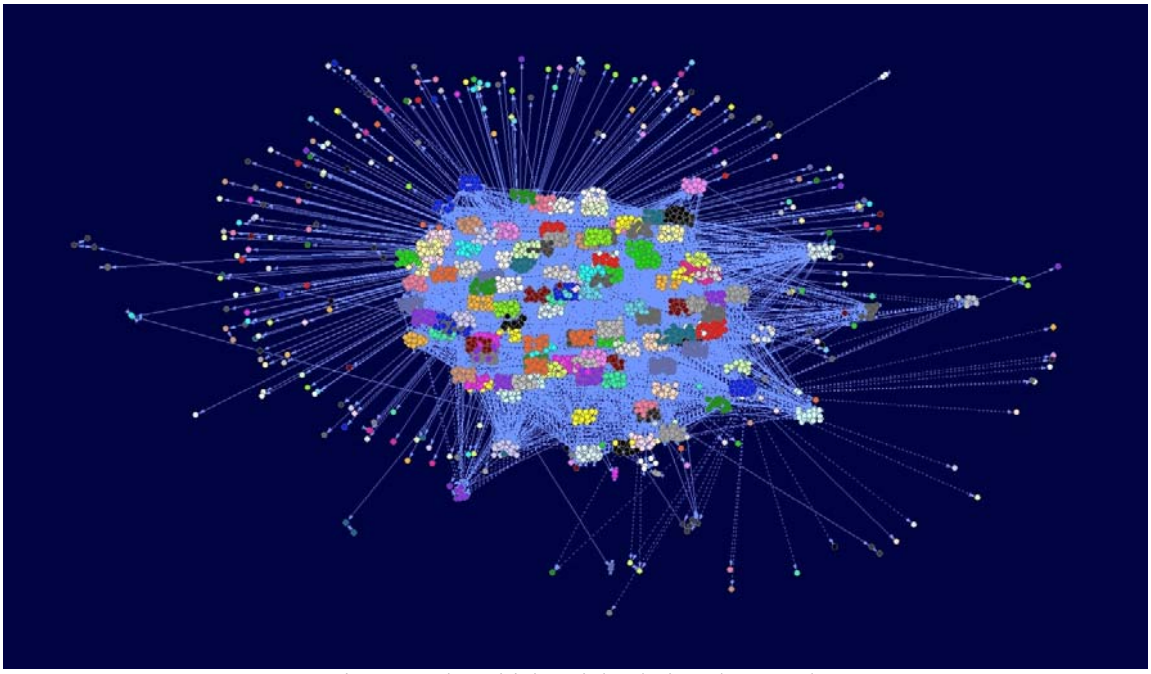


Figure 3: The Initial Weighted Signed Network

Table 2 gives the basic statistical data of the initial weighted signed network whose total number of nodes is 5881 and total number of arcs is 35592. The average degree of this large network is 12.1040, which reflects a relatively high exchanging frequency in the whole network. What's more, an equal relationship between average in-degree and average out-degree can be seen in table 1. At last, close relations between nodes are found in conjunction with the network diameter of 11 and the average path length of 3.7189.

Table 2: Basic Information of the Initial Weighted Signed Network

Indicators	Value
Total number of nodes	5,881
Total number of arcs	35,592
Average degree	12.1040
Average in-degree	6.0520
Average out-degree	6.0520
Network diameter	11
Average path length	3.7189

Classification Of Nodes

According to the website's description, when a user is negatively rated by other users, it indicates that the user is "abnormal" in the transaction. If users choose to trade with such users, the transaction might be risky. Instead, when a user receives positive ratings from other users, it indicates that the user performed "well" in the transaction. If a user chooses to trade with such a user, the transaction risk might be low. Therefore, we divided nodes into 2 classes according to whether the users are negatively rated by other users.

After classification, the number of nodes that have been rated negatively by other users is 1,254 (class-A nodes for short), while the number of nodes that have not been rated negatively by other users is 4,604 (class-B nodes for short). Also, users have not rated 23 nodes, that is, these nodes have ever rated other users, but have never been rated by other users (class-C nodes for short).

Nodes Filtration

Based on the analysis result in 3.2, we know that most "fraudster" users are in close cooperation. They form their fraudster groups and cheat the unwitting users together. Thus the fraudsters fall into 2 categories: core fraudsters and shills. Core fraudsters are main actors to cheat unwitting users while shills are those who are disguising themselves as normal users and assisting the core fraudsters. In fact, core fraudsters are the core nodes of the fraudster groups and other users have rated them negatively. Shills are the marginal nodes of the fraudster groups who are not rated negatively by other users, but give the "core fraudster" users positive ratings. Moreover, in order to extract money from innocent users, the members of the fraudster groups will rate positively to each other within the groups to improve their total ratings.

To filtrate all fraudster nodes, we first need to extract a sub-network composed of both core fraudsters and shills. According to the definition in the last paragraph, that means the end points of arcs in the new sub-network must be class-A nodes. Therefore, the sub-network is an extended A network containing all class-A nodes and some class-B nodes, so we named it "A+ network."
As the next step, according to the fact that the members of the fraudster groups will rate positively to each other within the groups to improve their total ratings, there is no denying that the weights inside the "A+ network" must be positive. Consequently, we deleted the 607 arcs with negative weights and 370 isolated nodes generated, and finally get a new network containing 15969 arcs and 3492 nodes.

Community Detection In The Network
Louvain Method is an algorithm based on modularity optimization, which is a simple but effective method to extract communities from initial network (Blondel *et al.*, 2008). In this part, Louvain Method is utilized to detect fraudster groups in the A+ network where resolution parameter is set to 50 and the number of random restarts is set to 1. After creating partitions by using Pajek (a free program for large network analysis), 574 communities were extracted. To improve the showing effect, the arcs between different communities are removed (figure 3). Figure 4 demonstrates a complete structure (including both core fraudster nodes and shill nodes) of each fraudster group.

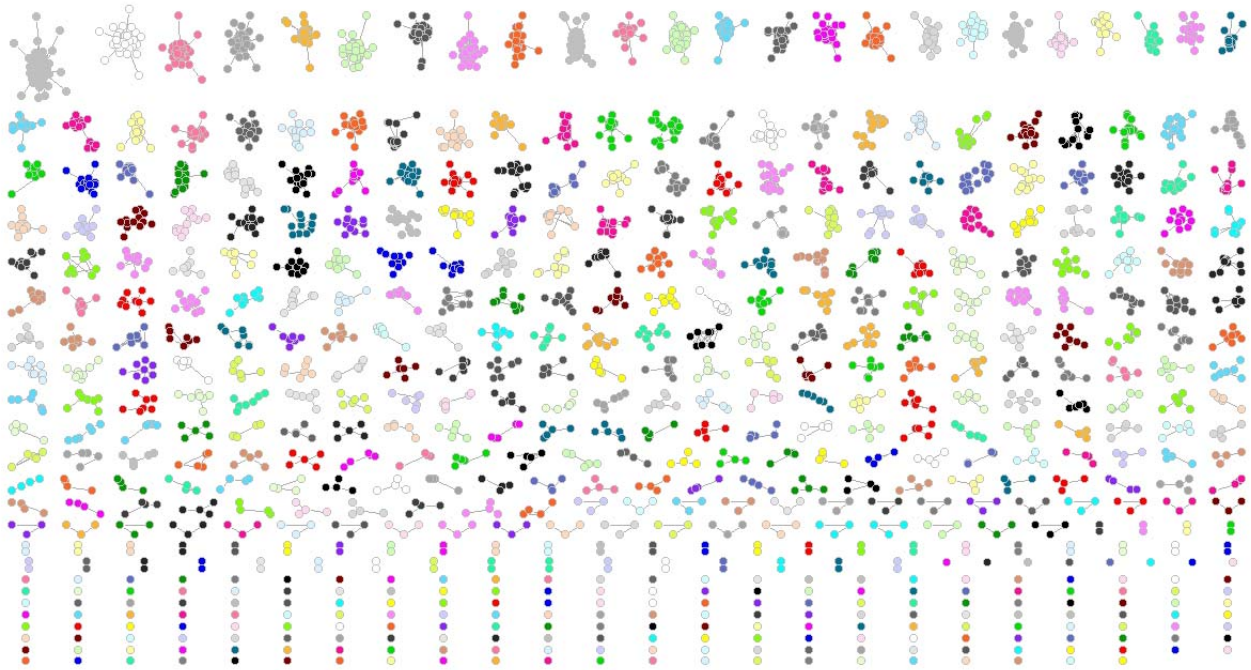


Figure 4: Separate fraudster groups in A+ network

Network Pruning
Next, according to the hypothesis in 4.2 that the fraudsters can be divided into 2 categories, the shill nodes refer to those who do not belong to class-A but give positive ratings to class-A nodes need to be pruned from the "A+ network". Therefore, to explore the core structure of fraudster network, the new sub-network should only contain the class-A nodes as we consider the class-A nodes as core fraudster nodes. Having known that class-A users are those who have been rated negatively by other nodes, the starting point and ending point of each arc in the new sub-network must be both class-A nodes. Consequently, arcs whose ending points are class-A nodes while the starting points are not class-A nodes are removed in this step.

The Louvain Method (Blondel *et al.*, 2008) is also used to identify communities from the new network. 268 communities were extracted where the resolution parameter is set to 50 and the number of random restarts is set to 1. To improve the showing effect, arcs between different communities are removed. Figure 5 demonstrates the core nodes (core fraudsters) of each fraudster group.

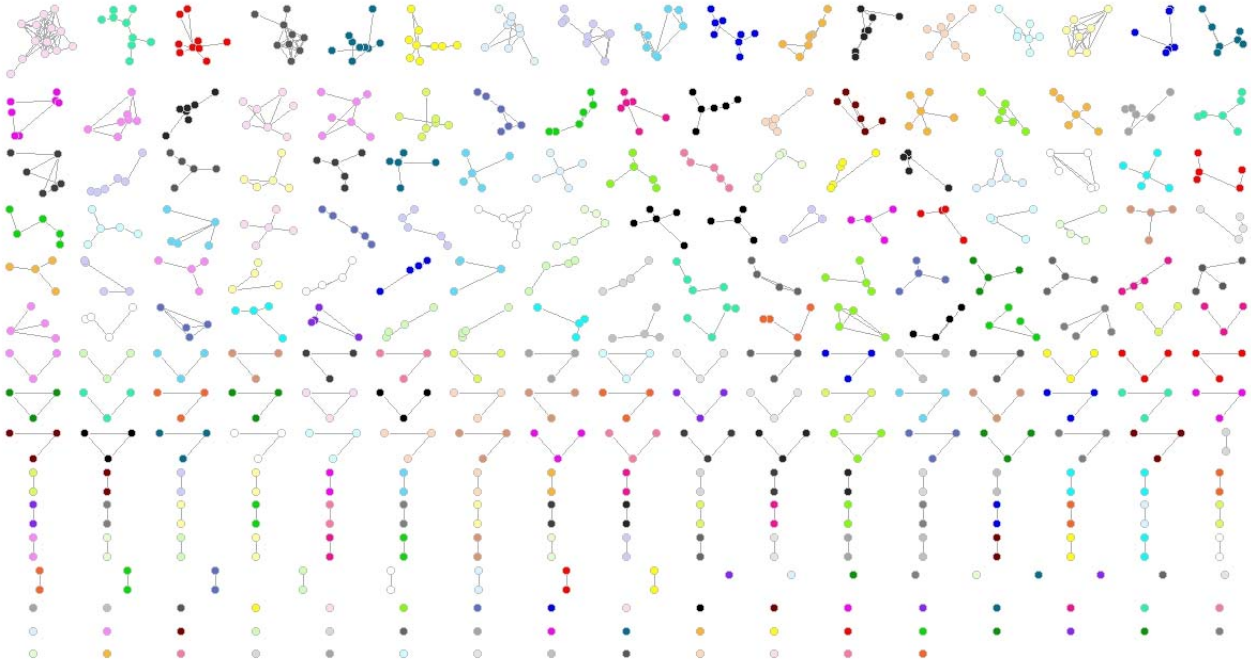


Figure 5: Separate Fraudster Groups in A Network

The basic statistical data of 2 sub-networks (A+ network and A network) are shown in the following table.

Table 3: Basic Information of the 2 Sub-networks

Indicators	A+ network	A network
Total number of clusters	574	268
Total number of nodes	3492	876
Total number of arcs	6920	2013
Average number of nodes	6.08	3.26
Average number of arcs	12.05	4.23
Average degree	1.96	2.58

As shown in table 3, total number of clusters, total number of nodes and total number of arcs all decrease sharply vary from "A+ network" to "A network". These changes indicate that the core fraudsters are only a small percentage of fraudster groups. As for the change happened in average number of nodes and average number of arcs, it could be known that the core fraudster groups are much smaller in scale. However, the average degree of "A network" is much higher than the "A+ network", which shows a highly close cooperation relationship and high exchange frequency within the core fraudsters.

An example will be given to explain details further. If we zoom out and focus on the same fraudster group in A and A+ network respectively, a very clear distinction between 2 sub-networks will be found (Figure 6). It can be seen from the figure 5 that all nodes in "A network" actually act as core nodes in "A+ network". The core nodes are at the center and marginal cores rated positively towards the core nodes, where the core nodes refer to the core fraudster and the marginal nodes refer to the shills.

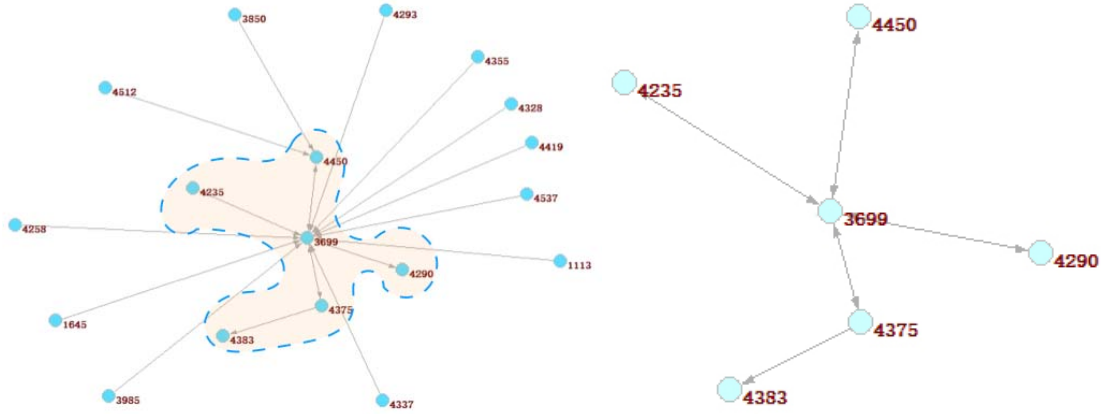


Figure 6: The Same Fraudster Group in A and A+ Network

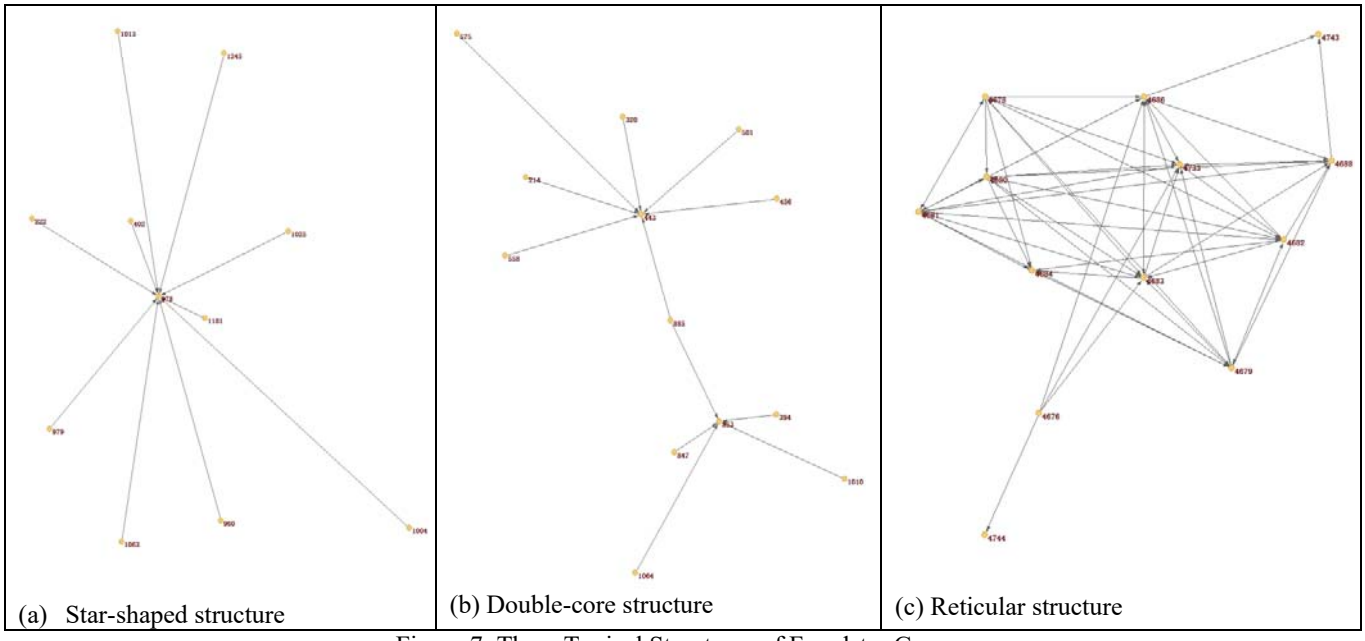
EXPLORING STRUCTURES

In order to explore the characteristics of the fraudster groups further, we observed their network structure. Our observation shows that there are three typical network structures of fraudster groups: star-shaped, double-core and reticular.

1) Star-shaped structure (Figure 7 (a)) refers to the topological structure with one core node at the center of the structure and all other nodes' arcs pointing towards the core node.

2) Double-core structure (Figure 7 (b)) refers to the topology structure in which two core nodes are in the center of the structure, and all other nodes have arcs pointing towards two core nodes.

3) Reticular structure (Figure 7 (c)) is a kind of topology in which the nodes in the groups are nearly fully connected.



(a) Star-shaped structure (b) Double-core structure (c) Reticular structure

Figure 7: Three Typical Structures of Fraudster Groups

To explore the internal rules of the network structure of fraudster groups further, we try to draw a scatter diagram based on several indexes in SNA.

Table 4: Model Summary and Parameter Estimation

	Model Summary					Parameter Estimates		
Equation	R Square	F	df1	df2	Sig.	Constant	b1	b2
Linear	0.436	255.469	1	330	0.000	19.611	-69.276	
Logarithmic	0.757	1028.813	1	330	0.000	-15.004	-11.824	
Inverse	0.953	6618.637	1	330	0.000	-0.063	1.000	
Quadratic	0.682	352.697	2	329	0.000	29.500	-205.206	368.474

Cubic	0.815	480.446	3	328	0.000	42.029	-474.105	1829.215
Compound	0.630	561.253	1	330	0.000	20.485	0.001	
Power	0.829	1604.903	1	330	0.000	0.954	-1.005	
S	0.700	769.349	1	330	0.000	1.372	0.070	
Growth	0.630	561.253	1	330	0.000	3.020	-6.758	
Exponential	0.630	561.253	1	330	0.000	20.485	-6.758	
Logistic	0.630	561.253	1	330	0.000	0.049	860.889	

We find that network density is negatively correlated the number of nodes and carried out analyses using SPSS. We select several fitting methods to deal with the correlation between the number of nodes and network density. Compared with the linear, logarithmic and other fitting method, the inverse matching effect-fitting method is preferable (Table 4) as it has an excellent performance in goodness-of-fit (R^2) and regression test (F) (R^2= 0.953, $F = 6618.637$). Adopting an inverse fitting, equation of the number of nodes and network density is built in (3) where "y" represents network density and "x" represents the number of nodes.

$$y = -0.063 + 1/x \tag{5}$$

The figure 8 clearly demonstrates the inverse correlation between the number of nodes and network density further. Network density describes the overall level of interaction of network nodes. It is believed that a Star-shaped structure is sparser than a reticular structure. It means there are structure preferences among the fraudster groups: the bigger the scale of fraudster groups, the more likely the fraudsters are to choose star-shaped structure; the smaller the scale of fraudster groups, the more likely the fraudsters are to choose reticular structure.

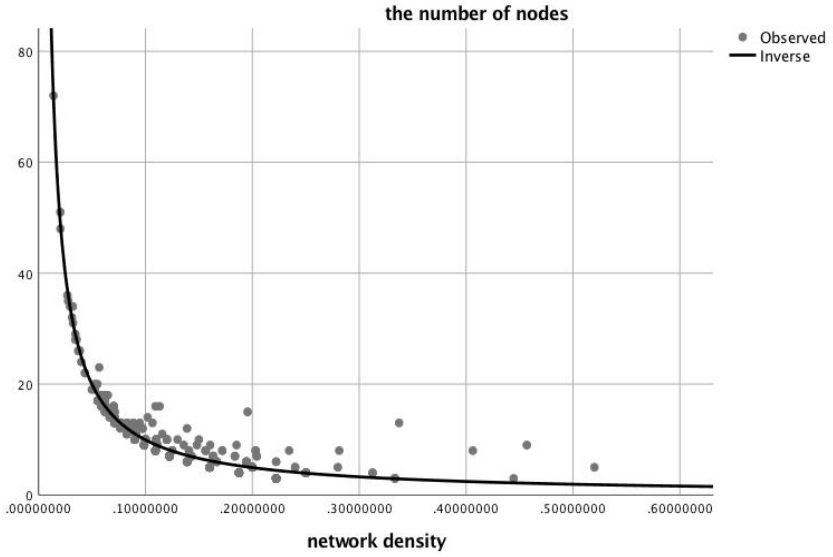


Figure 8: A Scatter Diagram of the Number of Nodes and Network Density

CONCLUSIONS

This paper builds a weighted signed network based on a Bitcoin transaction website. Nodes with different characteristics in the network are classified into 2 classes. According to the results of classification, fraudster groups are detected through community detection algorithm. Next, several typical structures of fraudster groups are found. Then, we find the number of nodes and network density move in opposite directions. At last, a mathematical formula of the number of nodes and network density has been obtained by fitting analysis and structure preferences among the fraudster groups have been found.

ACKNOWLEDGEMENT

This work is partially supported by Education and Teaching Reform Project of the South China University of Technology (Y9161010).

REFERENCES

[1] Abdul-Rahman, A., & Hailes, S. (2000). Supporting trust in virtual communities. In *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences* (pp. 6007). IEEE, Hawaii, HI, USA, January 4-7.

[2] Beth, T., Borcherding, M., & Klein, B. (1994). Valuation of trust in open networks. In *Proceedings of Third European Symposium on Research in Computer Security* (pp. 1-18). Brighton, UK, November 7-9.
[3] Blondel, V. D., Guillaume, J. L., Lambiotte, R., & Lefebvre, E. (2008). Fast unfolding of communities in large networks. *Journal of Statistical Mechanics: Theory and Experiment, 2008*(10), 10008.
[4] Boccaletti, S., Latora, V., Moreno, Y., Chavez, M., & Hwang, D. U. (2006). Complex networks: Structure and dynamics. *Physics Reports, 424*(4-5), 175-308.
[5] Cantner, U., & Graf, H. (2006). The network of innovators in Jena: An application of social network analysis. *Research Policy, 35*(4), 463-480.
[6] Croft, D. P., James, R., & Krause, J. (2008). *Exploring Animal Social Networks*. Princeton, New Jersey: Princeton University Press.
[7] Farine, D. R., & Whitehead, H. (2015). Constructing, conducting and interpreting animal social network analysis. *Journal of Animal Ecology, 84*(5), 1144-1163.
[8] Farrell, D., & Greig, F. (2016). Paychecks, paydays, and the online platform economy: Big data on income volatility. Working paper, JP Morgan Chase Institute, Japan, February.
[9] Freeman, L. C. (1978). Centrality in social networks conceptual clarification. *Social Networks, 1*(3), 215-239.
[10] Intanagonwiwat, C. , Heidemann, J. , Estrin, D. , & Govindan, R. (2002). Impact of network density on data aggregation in wireless sensor networks. In *Proceedings of the 22nd International Conference on Distributed Computing Systems* (pp. 457-458). IEEE, Washington, DC, USA, July 2-5.
[11] Josang, A., & Ismail, R. (2002). The beta reputation system. In *Proceedings of the 15th BLED Electronic Commerce Conference E-Reality: Constructing the E-Economy* (pp. 2502-2511). Bled, Slovenia, June 17-19.
[12] Li, F., & Du, T. C. (2014). Listen to me—Evaluating the influence of micro-blogs. *Decision Support Systems, 62*, 119-130.
[13] Marsh, S. P. (1994). Formalising trust as a computational concept (Doctoral dissertation, University of Stirling, Scotland, UK).
[14] Otte, E., & Rousseau, R. (2002). Social network analysis: A powerful strategy, also for the information sciences. *Journal of Information Science, 28*(6), 441-453.
[15] Travers, J., & Milgram, S. (1967). The small world problem. *Phychology Today, 1*(1), 61-67.
[16] Wasserman, S., & Faust, K. (1994). *Social Network Analysis: Methods and Applications*. Cambridge, England: Cambridge University Press.
[17] Xiong, L., & Liu, L. (2004). Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities. *IEEE Transactions on Knowledge and Data Engineering, 16*(7), 843-857.
[18] Zacharia, G., Moukas, A., & Maes, P. (2000). Collaborative reputation mechanisms for electronic marketplaces. *Decision Support Systems, 29*(4), 371-388.