

The Visualized Analysis of Bitcoin Change Wallets in the Coin Flow Network

Shan-Wen CHEN ^a, Kuan-Po LIU ^a, Fu-Ching TSAI ^a

^a Dept. of Criminal Investigation, Central Police University, Taiwan, ROC.

corresponding author: ftsai@mail.cpu.edu.tw, Tel: +886 3 3282321*5120

Abstract—In recent years, crimes using bitcoin as a tool have brought severe impacts to the social order. Bitcoin has the characteristics of high anonymity, decentralization, peer-to-peer, and the use of asymmetric encryption. These high tech features make bitcoin a new criminal tool which often used by organized criminal groups. Therefore, analyzing bitcoin flow has become critical for law enforcement to conduct a criminal investigation. However, due to its UTXO (Unspent Transaction Output) transaction pattern, many change wallets are generated in analyzing bitcoin flow, which affects the judgment of actual money flow analysis. In this research, we implement input-output differential and temporary rules to detect change wallets by analyzing bitcoin transaction pattern characteristics. Furthermore, we design web crawlers as a tool to collect and parse transactions of highly suspected criminal bitcoin wallets. Micro and macro perspectives of network analysis are provided by social network analysis (SNA) and visualization technology. The experimental results indicate that the proposed rules can detect both clustered and marginal change wallets. By eliminating the noise information caused by change wallets can provide coherent financial flows of interpretation for criminal investigation.

Keywords— Bitcoin Flow Analysis, Social Network Analysis, Visual Analysis

I. INTRODUCTION

In recent years, crimes using bitcoin as a tool have brought many impacts to the social order [1]. Bitcoin has the characteristics of high anonymity, decentralization, peer-to-peer, and the use of asymmetric encryption, and has become a new criminal tool often used in organized crimes. Bitcoin is currently used internationally as a currency of payment and as an investment commodity. It has two characteristics of "currency" and "commodity", making it used in various forms of crime. Also, the transaction process is prone to forming breakpoints in the cash flow, which increases the difficulty for law enforcement investigators to track down the suspicious bank accounts.

The high anonymity of bitcoin has become a widespread criminal tool for criminals, especially for black market transactions on the dark web [2]. Many illegal websites on the dark web trade firearms, drugs, and child pornography in bitcoin. Bitcoin transactions are difficult to trace the true identity of the payer. Therefore, bitcoin has been widely used in illegal goods transactions [3]. However, many law enforcement agencies are not aware of this crisis because of its complicated technology and innovative operating processes [4]. The current strategies or tools for investigating traditional financial crimes are hard to apply to virtual currency crimes.

In investigating bitcoin transactions, tracking the flow is an essential step in the criminal investigation. Although bitcoin transactions are public on the Internet, its UTXO (Unspent Transaction Output) transaction characteristics may produce many change wallets [1]. By observing the bitcoin transaction data, we can find that the sender sent money to the receiver and sent the balance of the original wallet to a new change wallet. In traditional financial transaction records, we treat the wallets on different sides of a transaction, which corresponding to the sender and receiver as two different entities. However, in bitcoin transactions, the owner of the change wallets is identical to the sender. These unique transaction facts will seriously affect the overall understanding of financial flow and make it challenging to discover the crimes [5]. To eliminate the noise caused by change wallets, we implement two rules to detect change wallets from bitcoin transactions and visualize its structural characteristics. The remainder of this paper is organized as follows: Section 2 provides a review of bitcoin and SNA. Section 3 describes the specifics of the research methodology and model development process. Section 4 demonstrates the results achieved by the proposed model. Finally, the last section concludes the paper and makes some suggestions for future work.

II. LITERATURE REVIEW

A. Bitcoin flow analysis

Bitcoin is a virtual currency built on blockchain technology. Therefore, bitcoin is not issued through any countries or financial institutions, but through the algorithms to calculate issuance and conduct transactions. Since there is no specific issuing organization of bitcoin, transactions are generated in the form of a Peer-to-Peer (P2P) network [4], which means that Bitcoin is a decentralized payment system. The bitcoin economy uses a distributed database composed of many nodes in the entire P2P network to confirm and record all transactions. The decentralized nature of P2P and the algorithm itself can ensure that the currency's value cannot be manipulated through the large-scale production of bitcoin. Besides, bitcoin can only be transferred or paid by the actual owner due to the specific encryption design technology which also ensures the anonymity of currency ownership and circulation transactions.

The bitcoin P2P network stores all transaction history in the blockchain. Bitcoin transactions are "booked" on the blockchain ledger, usually with the bitcoin client's assistance. The payer (or input) needs to digitally sign the transaction with

its private key to prove ownership and approve it. The value of the transaction will be recorded on the address of the recipient (or output). Bitcoin transactions are like the way in double-entry bookkeeping. Each transaction contains one or more "inputs", which are the payer of the bitcoin account. On the other side of this transaction, there are one or more "outputs" representing the bitcoin account recipient. The value of these inputs and outputs does not need to be equal. When the cumulative output is slightly less than the input, the difference is the "miner fee", which is actually a "transaction fee." There is no input for a transaction fee but only output because the bitcoin algorithm produces it and be treated as the newly generated coins. After the transaction is broadcasted over the bitcoin network, the miners generate a block containing the transaction and append it to the blockchain. When more and more new blocks are added to the blockchain, the previous blocks will repeatedly be confirmed. Therefore, bitcoin transactions are treated as records that are irreversible and cannot be charged back.

The change wallets in bitcoin are created when the output is not equal to the transaction input. In the traditional financial transaction model, when the input and output are not equal, the unspent money will remain in the original account and become the account balance. Nevertheless, in the bitcoin transaction mode, the balance of the original transaction wallet will be emptied, and the original account balance will be transferred to a new address or the original address where the transaction was initiated. This special model, which deals with the balance in virtual currency, is like transferring money to the sender. However, there is no specific label for this type of bitcoin transaction, so it is impossible to directly observe the change wallet from a large number of transaction records.

In a criminal investigation, the analysis of the financial flow of the suspect is very critical. Nonetheless, the lack of knowledge on bitcoin change wallets will mislead the direction of the investigation. Therefore, determining the change wallet of bitcoin can effectively reduce the noise of financial flow analysis for law enforcement agencies.

B. Social Network Analysis (SNA)

Social Network Analysis (SNA) is a method for analyzing the relationship structure and attributes of social networks [6]. It is also called structural analysis because it mainly analyses the structure and attributes of social relations formed by different social units (individuals, groups, or society). It belongs to a relatively mature analysis method in the field of sociology. From the perspective of social networks, the interaction of people in the social environment can be expressed as a model or rule based on relationships, and the regular model based on this relationship reflects the social structure. The quantitative analysis of this structure is the starting point of SNA. Social network analysis is not only a tool but also a way of thinking in relational theory. Social network analysis can analyze social networks from many different perspectives, including centrality analysis, cohesive subgroup analysis, core-periphery structure analysis, and structural equivalence analysis.

We further introduce the detailed SNA indicators which are adopted in this research with formal mathematical definition as follows.

Size: The indicator describes the scope of the network by summarizing the number of nodes in the entire network. The larger network can cover a wide range of events, but it may also increase the complexity.

Density: The indicator shows the concentrated degree of the entire network. The formula is the ratio of the actual number of connections over all possible number of links. The network with high density represents the frequent interaction and communications among the nodes.

Diameter: The indicator represents the largest geodesic distance between all nodes. If the diameter value is high, the network is treated as a large network. Therefore, previous researches usually use this indicator to define the boundary of the target network.

Degree: It is mainly used to measure the importance of nodes. The mathematical representation is as follows:

$$D_i = \sum_j a_{ij} \quad (1)$$

where D_i represents the degree of node i , and a_{ij} represents the total links of nodes i to the neighboring nodes j in the network. A node with high degree means that the node can connect to a large portion of the node in the whole network, and also indicate the high importance of the node.

Closeness: It is mainly used to measure the tightness of a particular node in the network with other nodes. The mathematical representation is as follows:

$$C_i = \frac{1}{\sum_j d_{ij}} \quad (2)$$

where C_i represents the closeness value of node i , and d_{ij} represents the distance from node i to other nodes j . The total distance from node i to other nodes j is inversely proportional to its closeness value. In other words, the node with smaller distance to other nodes has higher closeness value.

Betweenness: It is mainly used to measure the degree of mediation of a node. The mathematical representation is as follows:

$$B_k = \sum_{i,j} \frac{g_{i,j,k}}{g_{i,j}} \quad (3)$$

where B_k represents the degree of betweenness of node k , $g_{i,j}$ is the shortest path from node i to node j , $g_{i,j,k}$ is the shortest path from node i to node j by node k . The high B_k value of node k indicates its key roles as bridging two isolated groups.

III. RESEARCH FRAMEWORK

Due to the characteristics of the bitcoin UTXO, many change wallets are produced, which makes it difficult to trace the

financial transaction flow. Therefore, this research implements two current change wallet detecting rules and explores the network structure of the change wallets through visual analysis and social network analysis. There are three phases in this research. First, the bitcoin transaction data was collected from the bitcoin trading platform with crawlers. Second, we implement two change wallet detection rules by observing the criteria of bitcoin UTXO characteristics. Finally, we conduct the visualized analysis of the change wallets to find its structural implication regarding social network features. An overview of the proposed model is shown in figure 1. Three main phases, data collection, change wallet extraction, and visualization, are discussed in the following subsections.

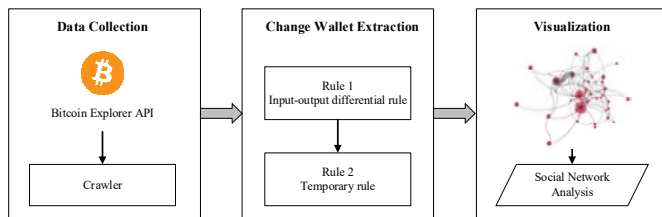


Figure 1. The research framework

A. Data Collection Phase

The bitcoin transaction data of this research is crawled from the Blockchain Explorer platform (<https://www.blockchain.com/explorer>), which is one of the popular crypto trade platforms. Because all the transactions of bitcoins are public, Block Explorer provides a friendly interface to search transaction records of specific accounts. Blockchain Explorer is currently one of the most common tools for analyzing bitcoin financial flows. While entering a specific wallet address or transaction number, the Blockchain Explorer can provide the following information, such as wallet address, transaction history, the total received and sent amount, balance, timestamp, etc. (as shown in figure 2).

This research uses python to implement a website crawler and uses the API (Application Programming Interface) provided by blockchain.com for data collection. The API can responses the structural transaction history with a hash query, which may represent either a wallet address or a transaction ID. Figure 3 shows the transaction history of the wallet 3QR1DpJMNAap42wgSyNvAtPGqrXGhQnEkN. The address on the left are inputs while those on the right are outputs. We further parse the retrieved JSON format data and standardize the features for change wallet detection.

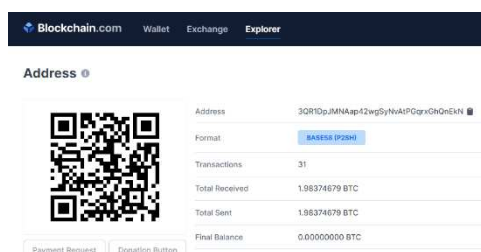


Figure 2. The account information of the bitcoin wallet 3QR1DpJMNAap42wgSyNvAtPGqrXGhQnEkN

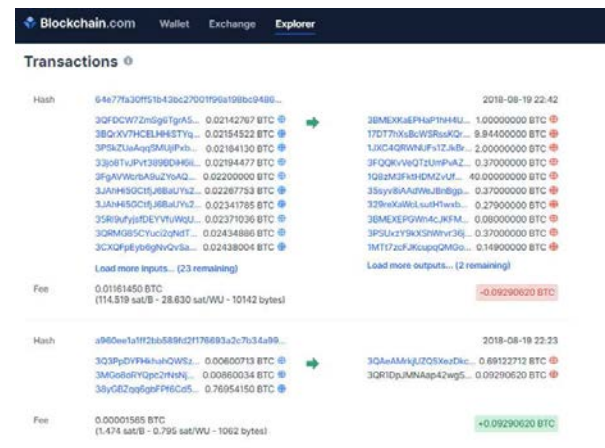


Figure 3. The transaction records of the bitcoin wallet 3QR1DpJMNAap42wgSyNvAtPGqrXGhQnEkN

B. Change wallet extraction Phase

Since the UTXO ledger model is the fundamental mechanism for bitcoin transactions, the balance value has to be calculated based on the inputs and the outputs. Except for the miner fee, the difference between the inputs and the outputs is the balance. The balance, also named unspent money, contributes to the production of change wallets. This means that the new change wallets are designed to store unspent money, and the change wallets owner are still the sender. In traditional flow analysis, we treat the accounts on the different sides belong to different people. However, under the UTXO model, the change wallets appeared on the right still belong to the senders on the left. This phenomenon has become difficult for law enforcement agencies in tracking the bitcoin flow for both upstream and downstream. Therefore, it is necessary to develop and summarize a set of judgment standards for change wallets. We implement two rules for judging bitcoin change wallets in this phase as follows.

Rule1: Input-output differential rule

In bitcoin wallet transactions, the sum of the input's wallets must be equal to the total amount of the output, except for the miner fee. To distinguish a wallet generated for storing the balance but not a wallet-to-wallet transaction, we remove the wallet with the smallest amount on the input side. If the rest of the total amount of wallet on the input side is still less than the largest wallet on the output side, it means that all the wallets on the input side have to pay to the largest wallet on the output side. In other words, there are no extra wallets on the input side to conduct a wallet-to-wallet transaction with the wallets on the output side. Therefore, if there exists a wallet on the output side rather than the largest wallet, it should be the change wallet. We use this rule to exclude any possibilities that the change wallets receive bitcoin from the input wallets.

Rule 2: Temporary rule

The primary function of the change wallet is to store the difference between input and output. Therefore, there is usually no previous transaction records before the change wallet is

generated. Thus, there should usually be two transactions for the change wallets, the first one is the transaction to generate the change wallets, and the second one is the transaction to empty the change wallet for importing the remaining value to the main wallet. Therefore, we implement rule 2 to detect the wallets, which only have two transactions as the change wallets.

C. Visualization Phase

In this phase, we utilize the collected data from the crawler and analyze the transaction network with visualization software [7, 8]. The tool for data visualization is Gephi [9]. This software is an open-source software developed by the University of Technology of Compiègne (UTC), often used for network visualization analysis. Further, we discuss the structure of change wallets with micro and macro perspectives. The macro view focuses on discussing the overall structure. We describe the macro-level information of the network with its averaged SNA statistics to represent the distinctive characteristics of the whole network. On the other hand, the micro view describes the local connections or locations for the specific node. The goal of this phase is to help investigators track the illicit financial flow in an effective and direct way.

IV. EXPERIMENTAL ANALYSIS

We use three bitcoin wallets provided by Criminal Investigation Bureau, Taiwan, as the testbed. The three wallets are highly suspected of committing criminal activities. The three wallets are shown as follows:

- Wallet 1: 3QR1DpJMNAap42wgSyNvAtPGqrxGhQnEkN
- Wallet 2: 3FNZmZ7R8CwKVSDpLtPoDvfPrZ1Nn5ks6h
- Wallet 3: 34FJ1GTBgksEhQEgcwk6iNBGFBEcgMv6wJ

The first wallet has 31 transactions with 284 addresses. The 284 addresses are filtered by the rules implemented in section 3.3. The addresses which fit the criteria of the change wallet rule are shown in Table 1. There are four change wallets detected by rule 1 while 15 wallets are detected by rule 2. Figure 4(a) shows the transaction flow of wallet 1, and figure 4(b) shows the flow of wallet 1 without change wallets. For simplify the name of the wallets, we take the first six digits of the wallet name as the abbreviation of the wallet.

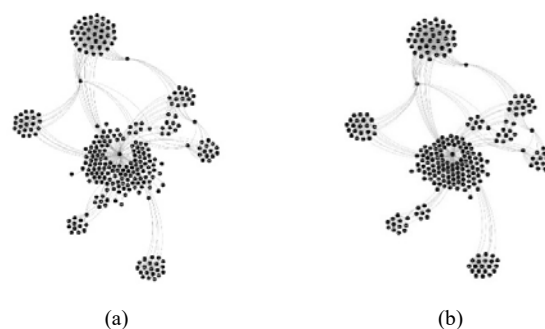


Figure 4. (a) The flow network of wallet 3QR1Dp (b) The flow network of the wallet 3QR1Dp after removing the change wallets

TABLE 1 THE CHANGE WALLET ADDRESS OF BITCOIN ACCOUNT 3QR1DpJMNAap42wgSyNvAtPGqrxGhQnEkN

Target wallet	3QR1DpJMNAap42wgSyNvAtPGqrxGhQnEkN
Wallet address removed by Rule 1	36o9xXTPhhpaxP7MXh2ZmmUuAVqeeWyJE 35Q1Q1eqE6GrJ7oWghCL4vypHpCi49usLy 32AhjHV8jr89yDeX4HsVnNyMfakgVj67Z 38BwzJTn8YeXGjeCQgsixTrCkhhFL7YX3d
Wallet address removed by Rule 2	3KHcRNjRcHnJGTRisBxjMP34a6dBS9YmRA 3JzJ5VUBefNJ3zBPVopNqnSxcCVZERZVR 3J6N2NBmHSHNYeqA9LkY2GPVjUQPu8xRwt 32F4sEvUUPStp9KDcoBeTEGKfqKKKbwW 3EkUbt5vEEkB17v6btPnWuwvvg2xG27ZFV 3Ce4xHxZ79K2VxGH7r98r96tGie6ycKvwE 39YAKmFQKFxkk6RJMALuLhzVCnjTi7sDjH 3DvRY2h2NtrkgixLa7j8h3ibnTko2PpqJr 3DErtgRpUpSgfNdEzBva1QqF8bGZnYSFaT 3BVKydgoye6YGVcdPR4rkwbomzSPkmmfUH 33MLi7nk7BwriiEtqjFXcf4vZrvFoSfSrh 31zAuuG1qBqogjAsJm8dKvjFvUzdUoLSW 3N7qMmroeFf5XLK9BoKNRbRbm5XjBehMPz 38jTqmLvrYnR73UUCRiH4pbCqnxzmpvTic 3KndAntbLFd2StrrHNxBVtQy3wUMXueW3p

In figure 4, the macro view of the two transaction networks is slightly different from each other. However, observing the micro view of change wallets which detected by different rules demonstrates the huge implication of their structure. The change wallets detected by rule1 have high centrality due to its clustered structure. On the contrary, the change wallets which detected by rule 2 usually located on the edge of the group. Figure 5(a) shows that the change wallet 32AhjH is surrounded by several wallets, e.g. 3E26if, 39wuko, 32kiod, 3JBPL7, 32ghxz and 3GXCJW etc., and creates a cluster. Since the change wallet 32AhjH is the center of the cluster, it should play an important role in flow analysis due to its high centrality. On the contrary, change wallets are not important in flow analysis. This incorrect information may lead the misjudgment on explaining the importance of the wallets. When the change wallet 32AhjH is removed, the cluster members show their connection with the target wallet 3QR1Dp .

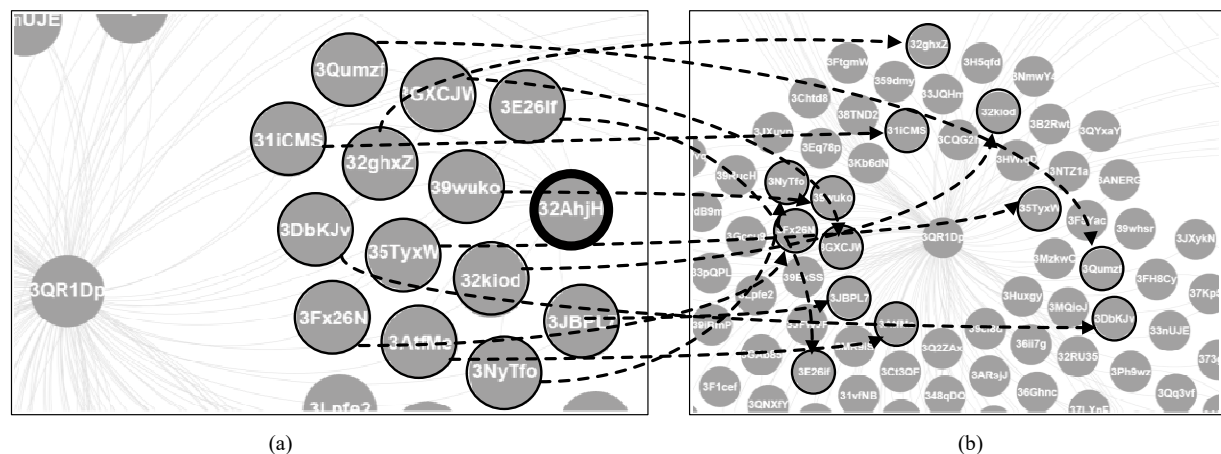


Figure 5. (a) The cluster network of change wallet 32AhjH (b) The clustered wallets decentralized after removing change wallet 32AhjH

Figure 6 shows that the change wallets filtered out by the rule2 are located in the marginal area of the target wallet group. And most of them are in the form of a pair. The rectangles in figure 6 are the change wallets detected by rule 2, and their location demonstrate the paired structures, such as 3KHcRN vs 3JzJ5V and 3KHcRN vs 3JzJ5V. Because the change wallet pairs are less connected to other wallets, the structural difference caused by rule 2 is not as obvious as by rule 1. Therefore, rule 2 produces less impact on the overall transaction structure.

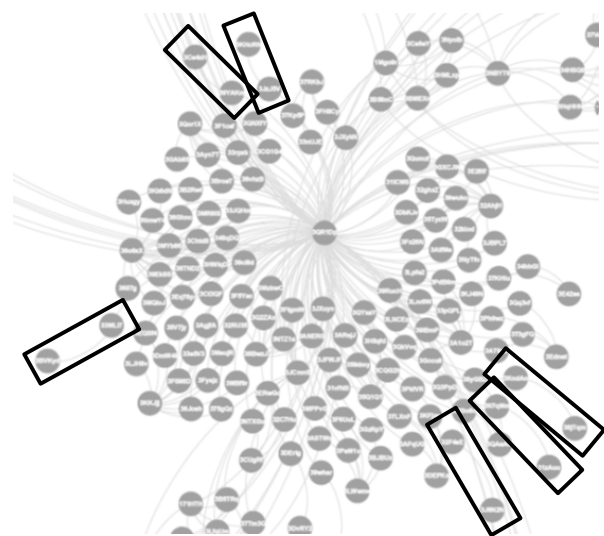


Figure 6. The paired structure of the change detected by rule 2

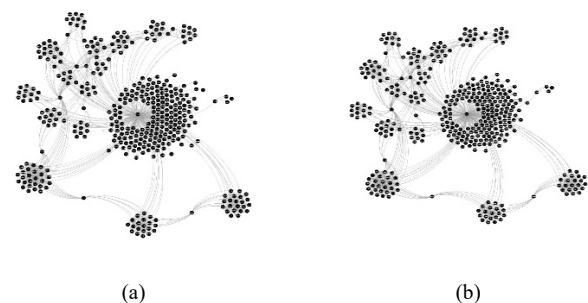
Table 2 demonstrates the results of SNA indicators of the transaction network before and after the change wallets are removed. By comparing the SNA statistics of two networks, the number of links decreases, while the density of the overall transaction scale increases, and the diameter decreases. After the change wallets are reduced, the values of the average degree centrality and the average betweenness centrality are reduced

accordingly. The reason is that by removing the wallets filtered by rule 1, the cluster number also decreases. Moreover, the removed address are the centers of the clusters. The increase in average eigenvector centrality and average closeness centrality shows that the rules can indeed filter the noise transactions and effectively leave qualified transactions for discussion.

TABLE 2. THE SNA STATISTICS OF NETWORK FLOW OF THE WALLET 3QR1DP

	Original network	Network without change wallets
Size	284	265
Edges	1061	990
Density	0.013	0.014
Diameter	5	4
Average Degree Centrality	3.736	3.715
Average Betweenness Centrality	24.19014	22.10227
Average Eigenvector Centrality	0.120024	0.121174
Average Closeness Centrality	0.495405	0.54057

We further analyse two target wallets, i.e. 3FNZmZ7R8CwKVSDpLtPoDvfPrZ1Nn5ks6h and 34FJ1GTBgksEhQEgcwk6iNBGFBEcgMv6wJ. The visualized flow networks are shown in figure 7. The SNA statistics are demonstrated in Tables 3 and 4.



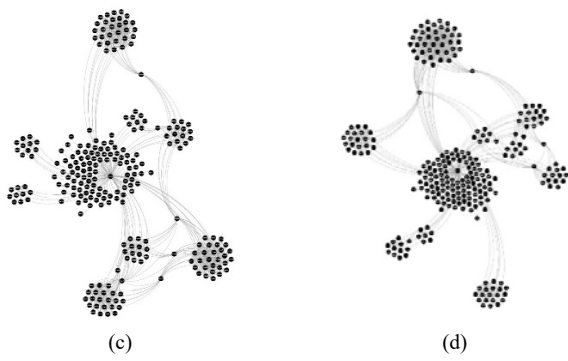


Figure 7. (a) The flow network of wallet 3FNZmZ (b) The flow network of wallet 3FNZmZ after removing the change wallets (c) The flow network of wallet 34FJ1G (d) The flow network of wallet 34FJ1G after removing the change wallets

TABLE 3. THE SNA STATISTICS OF NETWORK FLOW OF THE WALLET 3FNZmZ

	Original network	Network without change wallets
Size	406	395
Edge	1302	1291
Density	0.008	0.008
Diameter	6	6
Average Degree Centrality	3.207	3.268
Average Betweenness Centrality	35.43842	35.45063
Average Eigenvector Centrality	0.13239	0.134714
Average Closeness Centrality	0.471679	0.478396

TABLE 4. THE SNA STATISTICS OF NETWORK FLOW OF THE WALLET 34FJ1G

	Original network	Network without change wallets
Size	248	229
Edge	973	953
Density	0.016	0.018
Diameter	2	2
Average Degree Centrality	3.923	4.162
Average Betweenness Centrality	15.0121	14.25328
Average Eigenvector Centrality	0.188015	0.202016
Average Closeness Centrality	0.545188	0.570352

We have summarized the number of the change wallets filtered by different rules in the 3 wallets, as shown in table 5. The reason why there are more wallets filtered by rule 2 is probably due to the generation mechanism of change wallets. Because the change address is generated by the original wallet during the transaction, a new change address will be automatically created. Unless the original input wallet itself is used as a change wallet or the input money is exactly equal to the output money, a new change wallet will usually be generated during the transaction. As for the stricter conditions to be met by rule1, it is not easy to meet the filter conditions from a large number of input and output wallet transactions, so the number of wallets filtered by rule 1 is less by rule 2.

TABLE 5. THE NUMBER OF CHANGE WALLET REMOVED BY DIFFERENT RULES

	The change wallets which are filtered by rule1	The change wallets which are filtered by rule2
Wallet 1: 3QR1Dp	4	15
Wallet 2: 3FNZmZ	0	11
Wallet 3: 34FJ1G	1	18

We demonstrate the difference between the three wallets in social network analysis statistics, as shown in table 6. From the point of view of the size indicator, the percentage of change wallets removed by wallet 1 and wallet 3 is more, while wallet 2 removed less change wallets. From the edge index, because the wallets filtered by rule1 belong to the cluster structure, the number of edges reduced is more than that of wallet 2 and 3. For density, the value is proportional to the reducing number of change wallets. For diameter, removing more change wallets by rule 1, most are cluster structure, might greatly reduce the value of the diameter. As for the centrality indicators of SNA, because the wallets removed by rule1 are the nodes with higher degree centrality, only the degree centrality value of wallet 1 decreases. Betweenness centrality and closeness centrality are highly related to the number of removed change wallets. Eigenvector centrality is related to neither the number nor types of the change wallets.

TABLE 6. THE DIFFERENCE OF SNA STATISTICS BY FILTERING THE CHANGE WALLET

	Wallet 1: 3QR1Dp	Wallet 2: 3FNZmZ	Wallet 3: 34FJ1G
Size	-7%	-3%	-8%
Edge	-7%	-1%	-2%
Density	8%	0%	13%
Diameter	-20%	0%	0%
Average Degree Centrality	-1%	2%	6%
Average Betweenness Centrality	-9%	0%	-5%
Average Eigenvector Centrality	1%	2%	7%
Average Closeness Centrality	9%	1%	5%

V. CONCLUSIONS

In the current era, when virtual currency is becoming more and more common, criminals will use the virtual currency to commit various financial crimes in order to avoid detection by law enforcement agencies. The previous method of investigating money flow cannot be applied to the trade with virtual currency, mainly because virtual currency generates many change wallets. The noise generated by change wallets will affect the effectiveness of tracing virtual currency. In this study, input-output differential rule and temporary rule are implemented to detect change wallet. This research proceeds the virtual currency flow analysis by designing the web crawler and retrieving the transactions regarding three bitcoin accounts provided by law enforcement agencies, which are highly suspected to involve in criminal activities. From the number of filtered wallets, using the two rules in this study can detect 6% of the address as change wallets. Comparing the filtered wallets by two rules, more wallets are filtered by temporary rule. From the perspective of the network structure, the wallets detected by the input-output differential rule belong to the clusters and with higher degrees of centrality. The wallets filtered by the temporary rule are located at the edge of the network. This type of wallet helps to improve the centrality of the overall transaction. In this research, we conduct the visual analysis of the transaction network, which can provide both the macro and micro view of the complex bitcoin transaction network. Future research directions may include developing more diversified judgment standards of change wallets and collect more transaction records to conclude solid research conclusions.

ACKNOWLEDGEMENT

This research was supported by the Ministry of Science and Technology of the Republic of China under the Grants MOST 109-2410-H-015-007 -. And also partially supported by the Executive Yuan of the Republic of China under the Grants Forward-looking Infrastructure Development Program (Digital Infrastructure-Information Security Project-110).

REFERENCES

- [1] N. Furneaux, *Investigating cryptocurrencies: understanding, extracting, and analyzing blockchain evidence*. John Wiley & Sons, 2018.
- [2] S. Dyson, W. J. Buchanan, and L. Bell, "The challenges of investigating cryptocurrencies and blockchain related crime," *arXiv preprint arXiv:1907.12221*, 2019.
- [3] F. Jobse, "Detecting suspicious behavior in the Bitcoin network," Tilburg University, 2017.
- [4] S. Nakamoto and A. Bitcoin, "A peer-to-peer electronic cash system," *Bitcoin*.—URL: <https://bitcoin.org/bitcoin.pdf>, 2008.
- [5] B. Nikkel, "Fintech forensics: Criminal investigation and digital evidence in financial technologies," *Forensic Science International: Digital Investigation*, p. 200908, 2020.
- [6] R. C. v. d. Hulst, "Introduction to Social Network Analysis (SNA) as an investigative tool," *Trends in Organized Crime*, vol. 12, no. 2, pp. 101-121, 2009.
- [7] 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.
- [8] C. Zhao and Y. Guan, "A graph-based investigation of bitcoin transactions," in *IFIP International Conference on Digital Forensics*, 2015, pp. 79-95: Springer.
- [9] B. M., H. S., and J. M., "Gephi: an open source software for exploring and manipulating networks," presented at the International AAAI Conference on Weblogs and Social Media, 2009.



Shan-Wen Chen is a student at the Department of Criminal Investigation, Central Police University, Taiwan. His research interests include social network analysis, cryptocurrencies, and data mining.



Kuan-Po Liu is a student at the Department of Criminal Investigation, Central Police University, Taiwan. His research interests include python programming, web scraping and cybersecurity.



Fu-Ching Tsai is an Assistant Professor at the Department of Criminal Investigation, Central Police University, Taiwan. He received the MS and Ph.D. degrees in Institute of Information management from National Cheng Kung University, Taiwan, in 2005 and in 2012, respectively. His research interests include data mining, text mining, digital forensics, social network analysis, and cyber criminology.