Blockchain Explorer: An Analytical Process and Investigation Environment for Bitcoin

Hiroki Kuzuno*†
*SECOM Co., Ltd., Japan
Email: h-kuzuno@secom.co.jp

Christian Karam†‡
†INTERPOL Global Complex for Innovation, Singapore
‡UBS Cyber Threat Intelligence

Abstract—**Bitcoin is the most famous cryptocurrency currently operating with a total marketcap of almost 7 billion USD. This innovation stands strong on the feature of pseudo anonymity and strives on its innovative de-centralized architecture based on the Blockchain. The Blockchain is a distributed ledger that keeps a public record of all the transactions processed on the bitcoin protocol network in full transparency without revealing the identity of the sender and the receiver.Over the course of 2016, cryptocurrencies have shown some instances of abuse by criminals in their activities due to its interesting nature. Darknet marketplaces are increasing the volume of their businesses in illicit and illegal trades but also cryptocurrencies have been used in cases of extortion, ransom and as part of sophisticated malware modus operandi. We tackle these challenges by developing an analytical capability that allows us to map relationships on the blockchain and filter crime instances in order to investigate the abuse in law enforcement local environment. We propose a practical bitcoin analytical process and an analyzing system that stands alone and manages all data on the blockchain in real-time with tracing and visualizing techniques rendering transactions decipherable and useful for law enforcement investigation and training. Our system adopts combination of analyzing methods that provides statistics of address, graphical transaction relation, discovery of paths and clustering of already known addresses. We evaluated our system in the three criminal cases includes marketplace, ransomware and DDoS extortion. These are practical training in law enforcement, then we determined whether our system could help investigation process and training.**

I. Introduction

Bitcoin is currently the most popular math based cryptocurrency [1]. Cryptocurrencies differ from government-issued currencies by (1) depending on decentralized trust network in its protocol and system architecture, (2) not having a central authority that can monitor the transactions and issue the units themselves. What cryptocurrencies offer as well is pseudo-anonymity based on the public-key cryptography and peer-to-peer (P2P) network without the existence of a trusted third party.

Bitcoins biggest innovation is the Blockchain, a distributed ledger that provides verification and integrity for transaction history. The model of Blockchain transaction models users can transfer bitcoin's anonymously from a Bitcoin address (address) to another address as a value payment for any business, service or trade activity.

Bitcoin and other cryptocurrencies are used in daily trading activities on marketplaces in the darknet, some of which are dealing with illicit and illegal trading. Bitcoins pseudo anonymous nature satisfies their requirement to become the adopted currency for this crime model. Marketplace users and ransomware operators would then keep their identities protected.

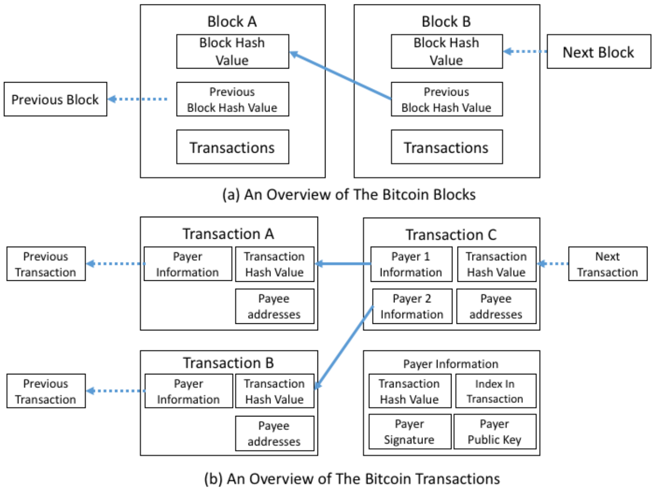
Identifying this type of activity is crucial in order to prevent money laundering and to counter terrorism financing. Researchers have been analyzing transactions and try to reveal relationships in between addresses, then showed connectivity and Bitcoin flow to graph structure for further understanding of Blockchain interactions [2], [3], [4], [5]. A few web sites and software have already started indexing whole sets of transactions and addresses to cluster them under a specific group [6], [7], [8], [9], [10].

These research and sites are extremely useful since they allow the Blockchain to become more readable. These lead to unveil the relation of multiple addresses, even though it does not provide sufficient investigation requirements for law enforcement. They requires additional analyzing features with local environment for utility training and investigation system that has combination of multiple methods to easily make a investigation report in each organization. In order to tailor a law enforcement analysis linked to specific acquired suspicious addresses' real time activity and provide on demand training in specific criminal cases from already known addresses. We propose a bitcoin analytical process and practical system that stands alone environment. These are used to be at training provides combination of analysis methods lead to effective tracing of address activity and relations. This is based on statistics of specific address, graphical representation of transaction relations, the discovery of new address relations and the clustering of addresses.

During the evaluation phase, our system analyzed a whole subset of transactions are based on analytical process. We were able to explain and draw the relationship in between addresses suspiciously linked to activities in illegal marketplaces, ransomware and DDoS extortion.

We consider the main contributions of this paper to be:

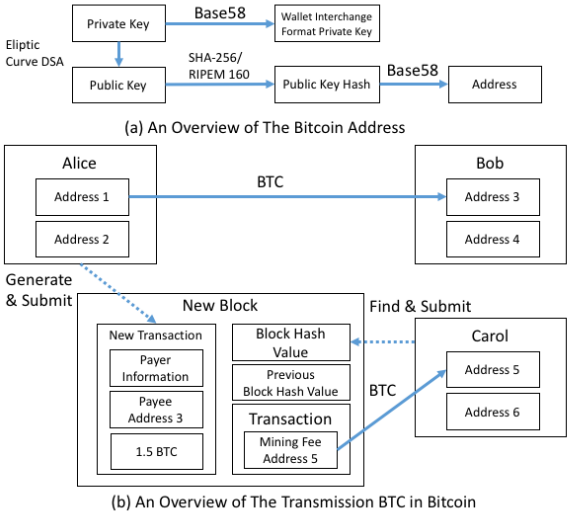
- An analytical process for discovering activity of addresses in Bitcoin to law enforcement investigation and training;
- Proposed system for providing combination of multiple analyzing methods through interaction at the local envi-



(a) An Overview of The Bitcoin Blocks

(b) An Overview of The Bitcoin Transactions

Fig. 1. (a) An overview of the Bitcoin blocks. A Block contains block hash value, a previous block hash value, and transactions. Each block refers to the next block and is referred to by the previous block in the chain. (b) An overview of the Bitcoin transactions. A transaction contains transaction hash value, senders information, and receivers information. A senders information has a transaction hash value, index of the transaction, senders public key, and the private key signature issuing the payment by the sender.



(a) An Overview of The Bitcoin Address

(b) An Overview of The Transmission BTC in Bitcoin

Fig. 2. (a) An overview of the Bitcoin address. A Bitcoin client generates a private key and a public key using Elliptic Curve DSA, an address is base58 encoded from public key SHA-256, RIPEMD-160 hash value. (b) An overview of the transmission BTC. Alice is payer, Bob is payee, and Carol is miner. First, Alice generates new transaction and submits it to Bitcoin network. Second, Carol finds specific block hash value for a new block inside Alices transaction. If it is to be accepted in the Bitcoin network, Carol could get a mining fee. Finally, Alices bitcoin payment will be sent to Bob.

ronment;

The rest of this paper introduces Bitcoin overview and anonymity in section II. In section III, we present Bitcoin analytical process and our system allowing the analysis of transactions and addresses. We evaluate our process and system using suspicious addresses at known cases to trace transmitting activity in section IV. In section V, we discuss related works, and suggest future work of our process and system. We conclude in section VI.

II. Overview of Bitcoin

Bitcoin is based on a decentralized architecture. It survives thanks to the Blockchain and P2P network. The Blockchain attributes include a block ID, a transaction ID, a Bitcoin address and the use of cryptographic techniques for validation of the transactions. Figure 1 shows an overview of the block and transaction. A block contains the hash of a previous block as well as the hosted transactions. A transaction shows a Bitcoin transfer between two entities. A transaction contains the senders signature, the public key, the hash value of the previous transaction, the receivers address and the Bitcoin amount value. The series of blocks and the transaction history are part of a chain in the Blockchain. The Blockchain requires specific 256 bit hash value when every new block is added, if a client finds it, the client can be rewarded with Bitcoins. This is called the mining process.

Figure 2 shows an overview of an address and the transaction in Bitcoin. The client must have a Bitcoin wallet that will manage any number of addresses that are generated from the public key and private key pair. In the transaction case, Alice is the sender, Bob is the receiver, and Carol is the miner. First, they setup a client separately in their environments in order to generate their wallet addresses. Next, each client will join the Bitcoin network. When Alice sends a Bitcoin payment from Alices address to Bobs address, Alice generates a transaction, which will be submitted to the Bitcoin network. If Carol finds a specific unique hash value for an incomplete block to include Alices transaction, Carol could submit the hash result to the Bitcoin network, assigning the transaction to the block and therefore claiming a mining fee. If the block is full, a new block is created. After signing the transaction, Bob will have the Bitcoin value transferred to his address.

A. *Anonymity of Bitcoin*

Bitcoin provides pseudo-anonymity for users. Therefore, all of the transaction history is publically published in the Blockchain. A client only requires the users address, the public and private key pair in order to issue and receive a transaction. If clients only use the same address to issue every payment, we could trace the activity in Bitcoin and understand deeply the type of activity undertaken under the wallet.

In some cases, a client might manage a persistent address. A persistent address is usually associated to a business, a marketplace vendor or a specific entity requiring payments to be deposited in its address such as public donations. The address has to be made public in order to receive funds. This is common in cybercrime related cases such as ransomware and DDoS extortion where hackers will display a cash-out addresses to collect Bitcoins from victims.

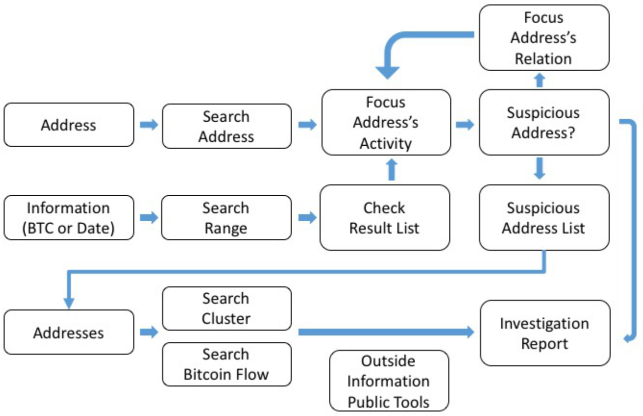


Fig. 3. The Bitcoin analytical process. This chart explains that the series of flow obtains whether specific address activity is suspicious or not using our proposed system. Finally, user can get an investigation report of the relation of target address.

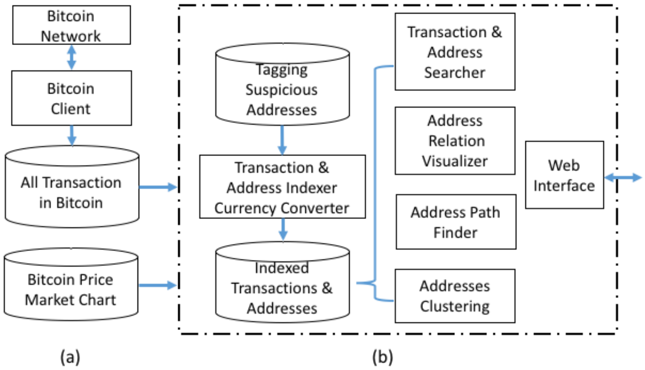

Bitcoin Network
Bitcoin Client
All Transaction in Bitcoin
Bitcoin Price Market Chart
(a)
Tagging Suspicious Addresses
Transaction & Address Indexer Currency Converter
Indexed Transactions & Addresses
Transaction & Address Searcher
Address Relation Visualizer
Address Path Finder
Addresses Clustering
Web Interface
(b)

Fig. 4. (a) A Bitcoin client joins the network and stores the transaction history, and Bitcoin price market chart in order to search in another currency. (b) The architecture of the Blockchain explorer system. It has three parts. First is an indexer for transactions and addresses. Second, analysis components and features for investigation about address information. Third is the web interface for users.

III. Approach

In this section, we present a Bitcoin analytical process and combination of methods to (1) analyze the transaction history of a address, (2) search specific known address activities, (3) identify relations between two addresses, and (4) cluster sets of known addresses. Our objective is to provide practical analytical process that derives useful information using analysis methods of known addresses for investigation and training in law enforcement. By focusing on finding characteristic activity and relations, we postulate that the system allows the user to profile and reveal details of a known address owner.

The Bitcoin analytical process is showned in Figure 3. It is step by step flow that takes activity information from known address or bitcoin remittance is acquired from criminal cases. Investigators trace address relation and activity in Bitcoin using combination of methods in our system. Finally they determine finding address is suspicious or not to support their investigation.

The relation of our system and the Bitcoin client is showed in Figure 4. The Bitcoin client joins the network and in real time downloads blocks that are issued. It is important to keep the ledger updated since Bitcoins have a price value comparison to fiat currencies fluctuating depending on the market charts.

Our system covers three parts. The first part is an indexer that builds an index of transactions and addresses, then adds a tag from suspicious addresses reported to our system from law enforcement. Second part the analysis features: a search function that provides statistics and information in relation to an address, a visualizer that shows addresses relationships by transaction, and a finder that discovers the transaction path in any addresses while clustering multiple addresses that may belong to one wallet. The third part is web interface for the system user.

A. Bitcoin Analytical Process

We lead the Bitcoin analytical process that is derived from practical investigation scenes. It refers to working knowledge in some criminal cases (e.g. Illegal trading or Pay off Ransom).

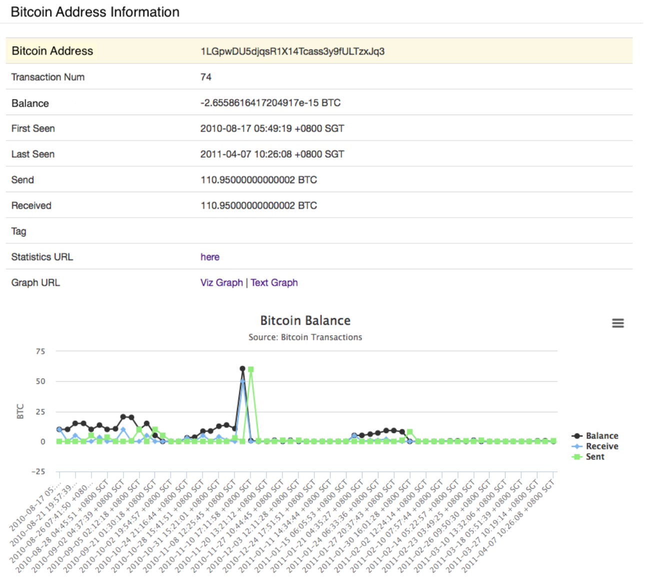
The chart has two starting point to finally make a report that shows an investigation result in Bitcoin. First, we postulate that target address is already known. User can get its balance and relations of other address, iterative trace whether focused transmission is suspicious or not. Second, if users only know the amount of transmission, they can search the whole of transactions have target transmission with specific date range. Finally, in order to locate the detail of addresses have linkability each other to make an investigation report, they use system features that automatically find bitcoin flow path and clustering of multiple addresses are whether managed on the same wallet or not.

If users could use public tool that shows related information of target addresses, it is an important complement to third party knowledge for an investigation report. This process helps for users to easily find an activity of target address, then trace relations of other addresses from target one in investigation process and training.

B. Indexing and Searching

The indexer of our system is designed to be able to real time monitor and convert the transactions in the original database of the Bitcoin client to our relational database. The searcher provides specific address information and transactions to users from it's database.

Typical client bitcoind [11] provides some API that are accessed by block and transaction hash amount, but it does not handle a specific address or any currency. Additionally, some researcher has already provided indexing information[8], [9]. Although these are useful and easily accessed from user environment, they do not respond to develop software for



Bitcoin Address Information

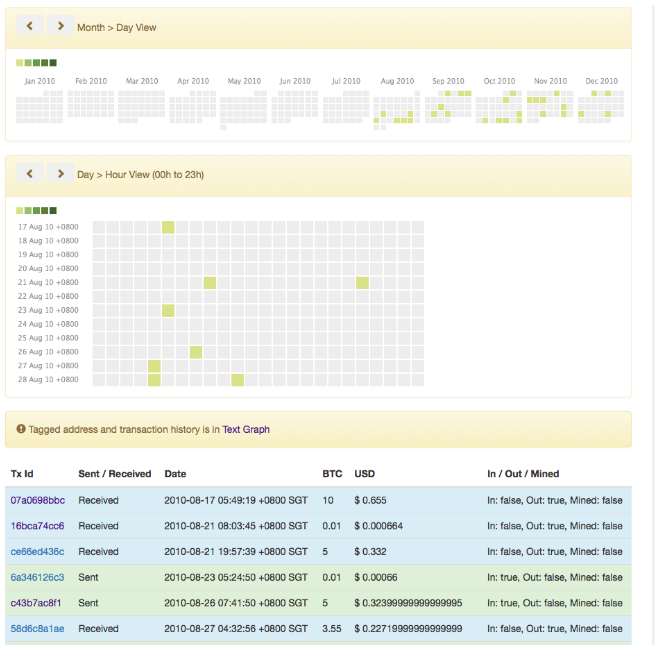
Bitcoin Address	1LGpwDU5djqsR1X14Tcass3y9fULTzxJq3
Transaction Num	74
Balance	-2.6558616417204917e-15 BTC
First Seen	2010-08-17 05:49:19 +0800 SGT
Last Seen	2011-04-07 10:26:08 +0800 SGT
Send	110.95000000000002 BTC
Received	110.95000000000002 BTC
Tag	
Statistics URL	here
Graph URL	Viz Graph | Text Graph

Bitcoin Balance

Source: Bitcoin Transactions

75
50
25
0
-25
BTC
Balance
Receive
Sent
2010-08-17 05:...
2010-08-21 19:57:39...
2010-08-26 07:41:50 +080...
2010-08-28 04:45:51 +0800 SGT
2010-09-02 04:37:39 +0800 SGT
2010-09-05 02:12:18 +0800 SGT
2010-09-21 01:30:18 +0800 SGT
2010-10-02 19:54:57 +0800 SGT
2010-10-24 21:16:44 +0800 SGT
2010-10-28 15:41:51 +0800 SGT
2010-10-31 15:21:01 +0800 SGT
2010-11-08 12:25:45 +0800 SGT
2010-11-10 17:11:58 +0800 SGT
2010-11-20 13:21:12 +0800 SGT
2010-11-27 10:44:45 +0800 SGT
2010-12-03 12:11:28 +0800 SGT
2010-12-24 17:51:51 +0800 SGT
2011-01-11 14:34:44 +0800 SGT
2011-01-15 06:05:53 +0800 SGT
2011-01-21 04:35:27 +0800 SGT
2011-01-24 06:33:36 +0800 SGT
2011-01-27 20:37:43 +0800 SGT
2011-01-30 16:01:28 +0800 SGT
2011-02-02 12:24:14 +0800 SGT
2011-02-10 07:57:44 +0800 SGT
2011-02-14 05:22:57 +0800 SGT
2011-02-23 03:49:25 +0800 SGT
2011-02-26 09:50:30 +0800 SGT
2011-03-10 13:32:06 +0800 SGT
2011-03-18 05:51:39 +0800 SGT
2011-03-27 10:19:14 +0800 SGT
2011-04-07 10:26:08 +0800 SGT

Fig. 5. A specific address information, which contains the number of transactions, balance amount, first seen date and last seen date. A chart shows balance, sent and received history.



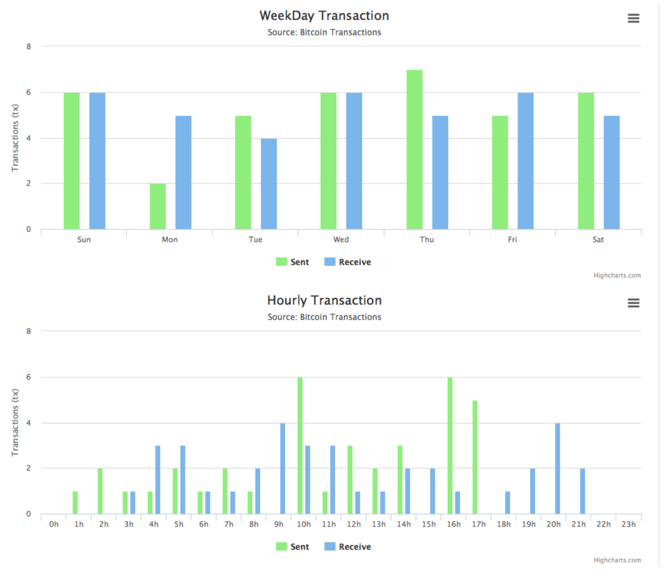
Tagged address and transaction history is in Text Graph

Tx Id	Sent / Received	Date	BTC	USD	In / Out / Mined
07a0698bbc	Received	2010-08-17 05:49:19 +0800 SGT	10	$ 0.655	In: false, Out: true, Mined: false
16bca74cc6	Received	2010-08-21 08:03:45 +0800 SGT	0.01	$ 0.000664	In: false, Out: true, Mined: false
ce66ed436c	Received	2010-08-21 19:57:39 +0800 SGT	5	$ 0.332	In: false, Out: true, Mined: false
6a346126c3	Sent	2010-08-23 05:24:50 +0800 SGT	0.01	$ 0.00066	In: true, Out: false, Mined: false
c43b7ac8f1	Sent	2010-08-26 07:41:50 +0800 SGT	5	$ 0.32399999999999995	In: true, Out: false, Mined: false
58d6c8a1ae	Received	2010-08-27 04:32:56 +0800 SGT	3.55	$ 0.22719999999999999	In: false, Out: true, Mined: false

Fig. 6. Monthly, weekly transactions and each transaction detail for a specific address.

recent transaction volume, then sometimes stop to support the API features.

In order to quickly pull the address information and Bitcoin flow in the local environment, the indexer iteratively parallel accesses the first block to the latest block in the original database, and stores each transaction ID and Block ID in our private database.



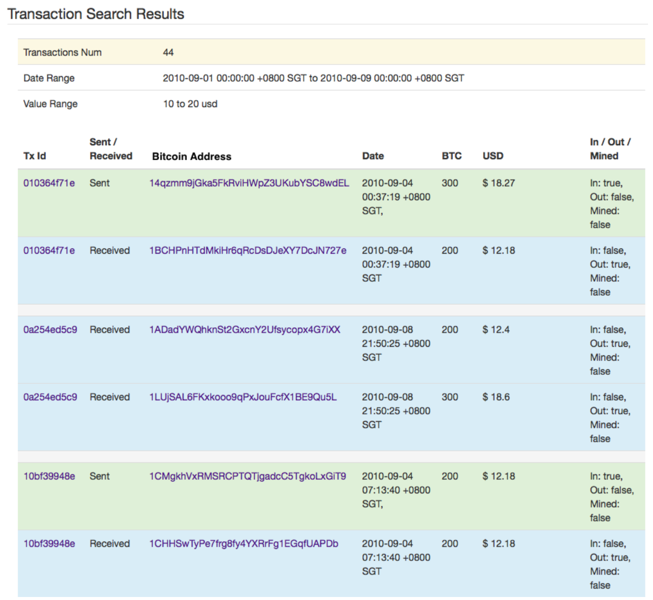
WeekDay Transaction

Source: Bitcoin Transactions

Hourly Transaction

Source: Bitcoin Transactions

Fig. 7. Statistics of weekday and hourly transactions for a specific address. The system separately shows sent and received Bitcoin transactions.



Transaction Search Results

Transactions Num	44
Date Range	2010-09-01 00:00:00 +0800 SGT to 2010-09-09 00:00:00 +0800 SGT
Value Range	10 to 20 usd

Tx Id	Sent / Received	Bitcoin Address	Date	BTC	USD	In / Out / Mined
010364f71e	Sent	14qzmm9jGka5FkRviHWpZ3UKubYSC8wdEL	2010-09-04 00:37:19 +0800 SGT,	300	$ 18.27	In: true, Out: false, Mined: false
010364f71e	Received	1BCHPnHTdMkiHr6qRcDsDJeXY7DcJN727e	2010-09-04 00:37:19 +0800 SGT	200	$ 12.18	In: false, Out: true, Mined: false
0a254ed5c9	Received	1ADadYWQhknSt2GxcnY2Ufsycopx4G7iXX	2010-09-08 21:50:25 +0800 SGT	200	$ 12.4	In: false, Out: true, Mined: false
0a254ed5c9	Received	1LUjSAL6FKxkooo9qPxJouFcfX1BE9Qu5L	2010-09-08 21:50:25 +0800 SGT	300	$ 18.6	In: false, Out: true, Mined: false
10bf39948e	Sent	1CMgkhVxRMSRCPTQTjgadcC5TgkoLxGiT9	2010-09-04 07:13:40 +0800 SGT,	200	$ 12.18	In: true, Out: false, Mined: false
10bf39948e	Received	1CHHSwTyPe7frg8fy4YXRrFg1EGqfUAPDb	2010-09-04 07:13:40 +0800 SGT	200	$ 12.18	In: false, Out: true, Mined: false

Fig. 8. A result is searched by U.S dollar. This shows 44 transactions are exists at amount range is USD 10 to USD 20, date from 2010.09.01 to 2010.09.09.

The searcher provides (1) Address Identifier, Block and Transaction hash value, (2) A transactions of Bitcoin amount or official currencies of the country (e.g. U.S. dollar).

An address search result contains an overview of address activity in Bitcoin and statistics related to the transactions. The overview also shows the number of transactions, balance history, first/last seen date, transaction amounts, tag information, and monthly. Additionally, weekly sending and receiving patterns appeared in a calendar view. A statistic shows the number of transactions on weekday and hourly. These are separately counted by sent and received.

Users promptly understand the whole context of target

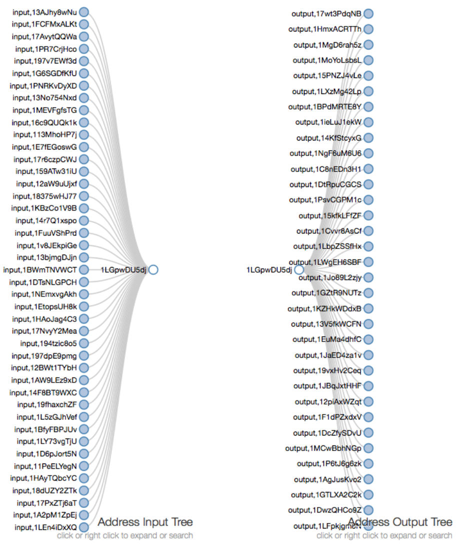


Fig. 9. A tree visualization of specific address relation. An address input tree shows a Bitcoin flow from the sender address to a target address. An address output tree shows a Bitcoin flow from target address to receiver address.

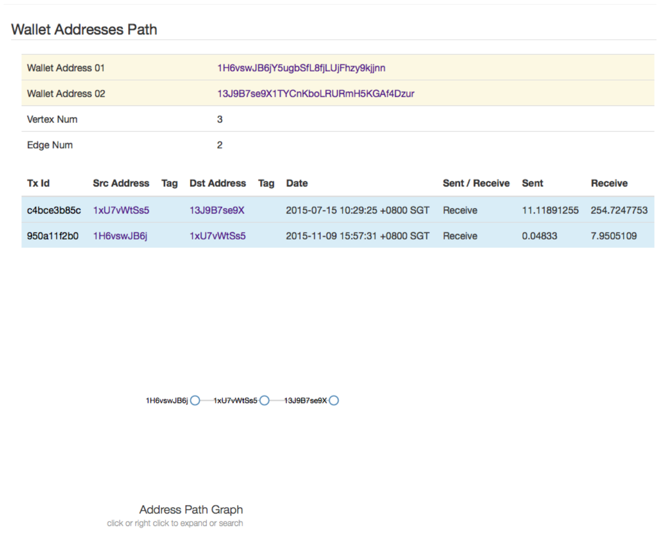
address type to make a reasonable guess about the number of victim at a ransom case or active timezone of address owner. The result of sample address information is shown in Figure 5 , Figure 6, and the statistics is shown in Figure Figure 7.

An other search type finds any transactions at specific date range with Bitcoin amount or official currencies. As an example in Figure 8. This feature is important for an investigation, since it allows us to identify victims by searching for ransom values in between specific dates where crimes have been reported. As an example, Figure 8 shows 44 transactions at amount range is $10 to $20, date from 2010.09.01 to 2010.09.09.

C. Visualizing and Path Finding

The visualizer displays a relation of addresses that shows a Bitcoin flow between one address and another address. Some addresses appeared in several transactions making them key for further analysis and cross match with investigative data. The visualization of this flow helps the investigator to zoom in on the address behavior and situation in an investigation target. Figure 9 shows graphical relations of specific addresses. Received and sent transactions are separated, user could track input and output transaction history from each address.

The path finder discovers a relation of one address to other address. A relation is a Bitcoin currency flow, the finder automatically links the sender and the receiver through any intermediate addresses to determine a connection of each target address. The path of “1H6vsw” to “13J9B7” in Figure 10. This path shows “1H6vsw” sent 0.04 Bitcoin to “1xU7vW”, then it sent 11.11 Bitcoin to “13J9B7”. If specific addresses are related or connected, we could easily identify them using the path finder. In the investigation field, user acquires multiple addresses. The finder supports the discovering multiple path between each addresses. It leads to determine what address is exchange point of Bitcoin in a criminal cases.

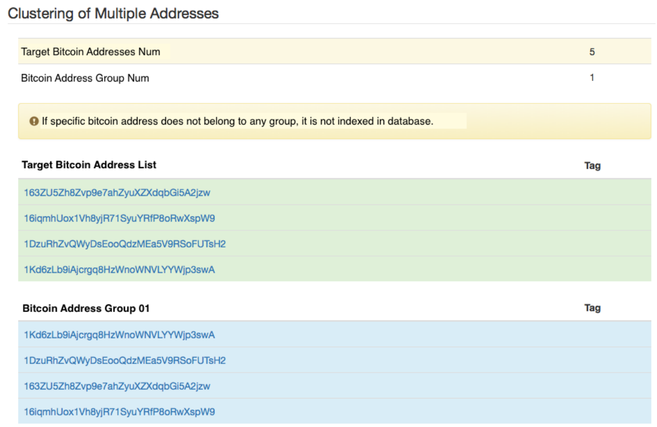


Wallet Addresses Path

Wallet Address 01	1H6vswJB6jY5ugbSfL8fjLUjFhzy9kjjnn
Wallet Address 02	13J9B7se9X1TYCnKboLRURmH5KGAf4Dzur
Vertex Num	3
Edge Num	2

Tx Id	Src Address	Tag	Dst Address	Tag	Date	Sent / Receive	Sent	Receive
c4bce3b85c	1xU7vWtSs5		13J9B7se9X		2015-07-15 10:29:25 +0800 SGT	Receive	11.11891255	254.7247753
950a11f2b0	1H6vswJB6j		1xU7vWtSs5		2015-11-09 15:57:31 +0800 SGT	Receive	0.04833	7.9505109

Fig. 10. A relation between two addresses. This shows that Bitcoin flow exists from one address to other address.



Clustering of Multiple Addresses

Target Bitcoin Addresses Num	5
Bitcoin Address Group Num	1

❶ If specific bitcoin address does not belong to any group, it is not indexed in database.

Target Bitcoin Address List	Tag
163ZU5Zh8Zvp9e7ahZyuXZXdqbGi5A2jzw	
16iqmhUox1Vh8yjR71SyuYRfP8oRwXspW9	
1DzuRhZvQWyDsEooQdzMEa5V9RSoFUTsH2	
1Kd6zLb9iAjcrgq8HzWnoWNVLYYWjp3swA	

Bitcoin Address Group 01	Tag
1Kd6zLb9iAjcrgq8HzWnoWNVLYYWjp3swA	
1DzuRhZvQWyDsEooQdzMEa5V9RSoFUTsH2	
163ZU5Zh8Zvp9e7ahZyuXZXdqbGi5A2jzw	
16iqmhUox1Vh8yjR71SyuYRfP8oRwXspW9	

Fig. 11. A clustering of multiple addresses. A clustering determines multiple addresses are in one transaction as payee or not. This result shows four addresses belong to the same wallet.

D. Clustering

The clustering of our system iteratively associates a known address with other addresses that might be owned by the same wallet operator. It might unveil multiple addresses that belong to specific wallet[4]. The iterative clustering assumes that a senders addresses in same transaction, these are managed by one wallet. It goes through all transactions related to addresses, then if some addresses re-appear in the same transaction, these are flagged as managed by the same client.

The clustering is fundamental method to analyze a relation of required addresses. In the investigation process, users create suspicious address list, then they have to unveil the detail of relevance to each other. The clustering helps their process to find the management of suspicious holder has how many

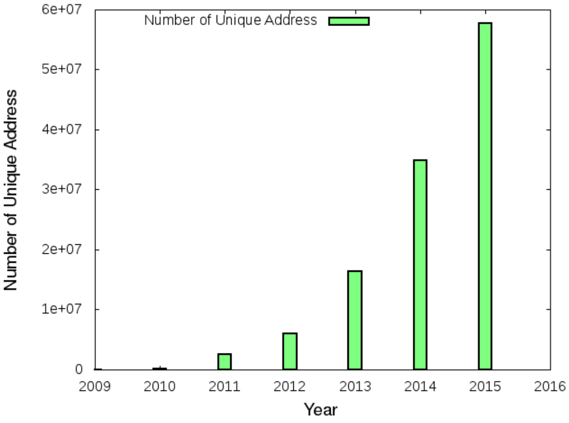


Fig. 12. The number of unique address for 2009 to 2015. This result shows explosive increase in address.

address in environment. Figure 11 shows result that four addresses belong to one wallet. This means possibility of multiple addresses are managed in the one wallet or one client. It is reference information to understand the relation of multiple addresses in Bitcoin.

IV. Evaluation

In this section, we show the statistics of the number of yearly address and investigation result of specific addresses in known cases. These results help to grasp the trend of Bitcoin and the effectiveness of our proposed process and system.

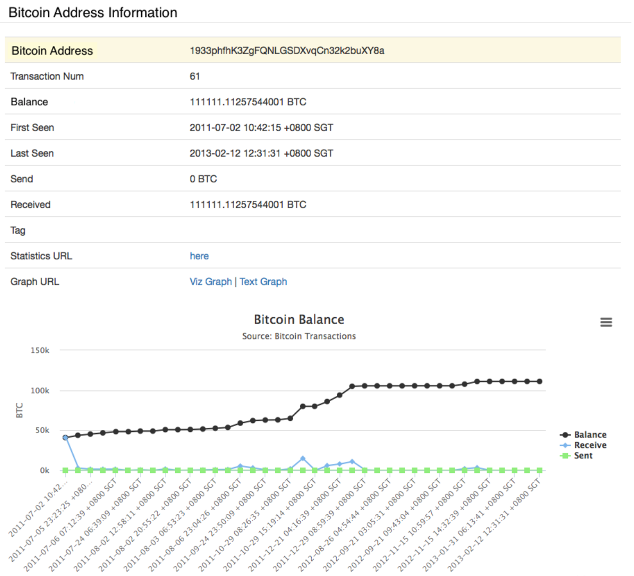
A. *Statistics of Address*

Bitcoin transactions are rapidly increased in the recent years, thus many addresses are generated. The number of unique address for period from 2009 to the 2015 in Figure 12. It shows over 1,700 times as many as in 2015 from 2009. This trend becomes an obstacle to the flow of analyzing the transaction history, because a system handles a lot of relations of address in a realistic time. If we identify new threats, a system should iterative find a detail of information regarding these transactions or Bitcoin flows of addresses. The indexing and other features prepare for this problem based on parallel tracking latest block in our proposed system.

B. *Addresses Investigation*

We revisited the investigating detail of suspicious addresses in threecybercrime cases [10], [12], [13] : (1) "Silk Road" market place owner's address, (2) CryptoLocker ransomware's addresses, and (3) DD4BC extortion case's addresses. We evaluate our system features' capabilities acquire useful information to make an investigation report is based on Bitcoin analytical process.

1) Silk Road Case: Silk Road case shows Bitcoin flow exists between address "1LDNLr" [1] and "1933ph" [2]. Both addresses were managed by site owner. User refers analytical process that searching feature finds specific address "1LDNLr" activity, then iterative trace remittance to "1933ph" on the visualizing and path finder determine it. Finally, investigation report includes the balance of "1933ph". It is Figure 13 shows the history of receiving to 111,111 BTC.

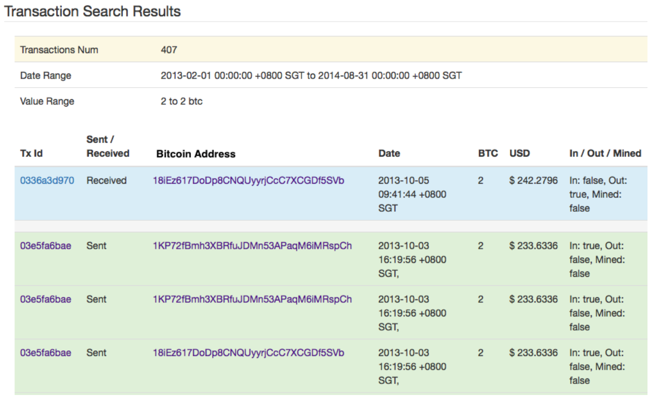


Bitcoin Address Information

Bitcoin Address	1933phfhK3ZgFQNLGSDXvqCn32k2buXY8a
Transaction Num	61
Balance	111111.11257544001 BTC
First Seen	2011-07-02 10:42:15 +0800 SGT
Last Seen	2013-02-12 12:31:31 +0800 SGT
Send	0 BTC
Received	111111.11257544001 BTC
Tag	
Statistics URL	here
Graph URL	Viz Graph | Text Graph

Bitcoin Balance
Source: Bitcoin Transactions
BTC
150k
100k
50k
0k
Balance
Receive
Sent
2011-07-02 10:42...
2011-07-05 23:23:25 +080...
2011-07-06 07:12:39 +0800 SGT
2011-07-24 06:39:09 +0800 SGT
2011-08-02 12:58:11 +0800 SGT
2011-08-02 20:55:22 +0800 SGT
2011-08-03 06:53:23 +0800 SGT
2011-08-06 23:04:26 +0800 SGT
2011-09-24 23:50:09 +0800 SGT
2011-10-29 08:26:35 +0800 SGT
2011-10-29 15:19:14 +0800 SGT
2011-12-21 04:16:39 +0800 SGT
2011-12-29 08:59:39 +0800 SGT
2012-08-26 04:54:44 +0800 SGT
2012-09-21 03:05:31 +0800 SGT
2012-09-21 09:43:04 +0800 SGT
2012-11-15 10:59:57 +0800 SGT
2012-11-15 14:32:39 +0800 SGT
2013-01-31 06:13:41 +0800 SGT
2013-02-12 12:31:31 +0800 SGT

Fig. 13. The balance of SilkRoad address "1933ph". It appeared from 2011.07 to 2013.02 in Bitcoin network and still has unspent 111,111 BTC.



Transaction Search Results

Transactions Num	407
Date Range	2013-02-01 00:00:00 +0800 SGT to 2014-08-31 00:00:00 +0800 SGT
Value Range	2 to 2 btc

Tx Id	Sent / Received	Bitcoin Address	Date	BTC	USD	In / Out / Mined
0336a3d970	Received	18iEz617DoDp8CNQUyyrjCcC7XCGDf5SVb	2013-10-05 09:41:44 +0800 SGT	2	$ 242.2796	In: false, Out: true, Mined: false
03e5fa6bae	Sent	1KP72fBmh3XBRfuJDMn53APaqM6iMRspCh	2013-10-03 16:19:56 +0800 SGT,	2	$ 233.6336	In: true, Out: false, Mined: false
03e5fa6bae	Sent	1KP72fBmh3XBRfuJDMn53APaqM6iMRspCh	2013-10-03 16:19:56 +0800 SGT,	2	$ 233.6336	In: true, Out: false, Mined: false
03e5fa6bae	Sent	18iEz617DoDp8CNQUyyrjCcC7XCGDf5SVb	2013-10-03 16:19:56 +0800 SGT,	2	$ 233.6336	In: true, Out: false, Mined: false

Fig. 14. The result is searched by 2 BTC, date from 2013.02.01 to 2014.08.31. Our system showed 407 Bitcoin flows are found, few transactions related to Cryptlocker's address "1KP72f" and "18iEz6".

2) Cryptolocker Case: CryptoLocker case shows that ransomware author managed a lot of addresses that have relations to victims' address. User could search the amount of Bitcoin (e.x. 2.0 BTC) is base on the analytical process. The searching feature automatically extracts the list of transactions from whole of transmitting history. In this case, two addresses were easily pointed out, because of these addresses received 2.0 BTC from many other address. Figure 14 shows two address

[1] 1LDNLreKJ6GawBHPgB5yfVLBERi8g3SbQS
[2] 1933phfhK3ZgFQNLGSDXvqCn32k2buXY8a

“1KP72f” [3] and “18iEz6” [4] have a lot of 2.0 BTC transactions. It is evidence to explain that these received Bitcoin from victims. user could estimate the number of victims in this case, then easily traces ranwomware author sent it to other suspicious address on the features of our system.

3) DD4BC Case: DD4BC is DDoS Extortion group. They required Bitcoin for stopping DDoS attack to private companies. This case, user could investigate few addresses and the amount of Bitcoin are base on the analytical process. It is provided the searching feature of our system. They used address “1H2bst” [5] and “17WQov” [6] for e-mail extortion. User could identify these address have relations of “1FsVcd” [7] on the visualizing and path finder features. Finally, their BTC was sent to address “3Bgk1o” [8], next is “3Q5r9g” [9].

Our system shows the Bitcoin flow relation between address “1FsVcd” and “3Bgk1o” on the visualizing. Figure 15 shows the Bitcoin flow relation between address “1FsVcd” and “3Bgk1o”. Figure 16 shows address “3Bgk1o” has a lot of connection to other address at tree visualization, both addresses are provided by a mixing service. User could see the Bitcoin flow of “3Q5r9g” sent BTC to other address that probably shows exchanging of Bitcoin to other currency (Figure 17).

In this case, user could identify that the extortion group collect ransom to specific address, transmit flow is complicated at intermediary service that camouflages with other transactions to hide relations of each address.

These are investigation result of cryptocurrencies forensics in Bitcoin at known cases. Our proposed analytical process supports manual investigation works, user use our system to make the report that could easily build from transaction history and relations about known addresses in our training for law enforcement.

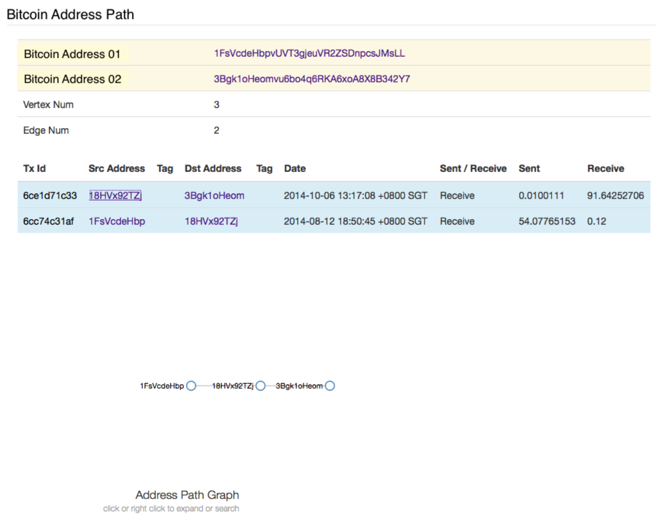
V. Related Works and Discussion

There has been extensive work on the subject of cryptocurrencies [5], [14]. Bitcoin is used in many businesses such as online gambling [15], exchanges [16], etc.

Law enforcement mentions an array of illegal activities currently proliferating from the Bitcoin technology [17], [18]. In the case of online marketplaces in Darknet (e.g. Silk Road [19], Evolution [20]), users traded illegal items for Bitcoin. Ransomware (e.g. CryptoLocker [21]) or DDoS extortion groups (e.g. DD4BC [22]) demand Bitcoin as ransom from their victims since it is an easy verified way to issue anonymous payments as well as handling them in cash-outs.

Bitcoin transaction analysis, address clustering and tracking could unveil connections between Bitcoin services [23], [3], [2], [4], it also narrows the range of suspicious addresses considerably. Although changing addresses leads to false positive cases, we might determine the targets behavior from the relation between other identified addresses. Its a cascaded identification process.

Bitiodine proposed a practical architecture for analyzing Bitcoin data [10], BlockChain.info and Chainalytics provide a sophisticated interface and a quick response system [24], [6]. These target automatic classification of addresses, and allow users to pull information from graphical visualization results. WalletExplorer.com is also one to mention since it labels in real time addresses based on a smart clustering method



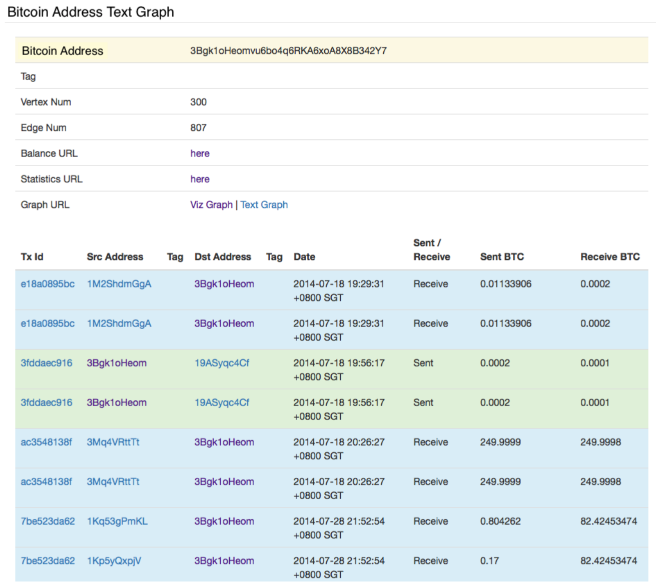
Bitcoin Address Path

Bitcoin Address 01	1FsVcdeHbpvUVT3gjeuVR2ZSDnpcsJMsLL
Bitcoin Address 02	3Bgk1oHeomvu6bo4q6RKA6xoA8X8B342Y7
Vertex Num	3
Edge Num	2

Tx Id	Src Address	Tag	Dst Address	Tag	Date	Sent / Receive	Sent	Receive
6ce1d71c33	18HVx92TZj		3Bgk1oHeom		2014-10-06 13:17:08 +0800 SGT	Receive	0.0100111	91.64252706
6cc74c31af	1FsVcdeHbp		18HVx92TZj		2014-08-12 18:50:45 +0800 SGT	Receive	54.07765153	0.12

Address Path Graph
click or right click to expand or search

Fig. 15. The relation path of DD4BC suspicious address between “1FsVcd” and “3Bgk1o”. It showed the mixing characteristic relation. The one of bitcoin flow is connected to “3Bgk1o” via one address.



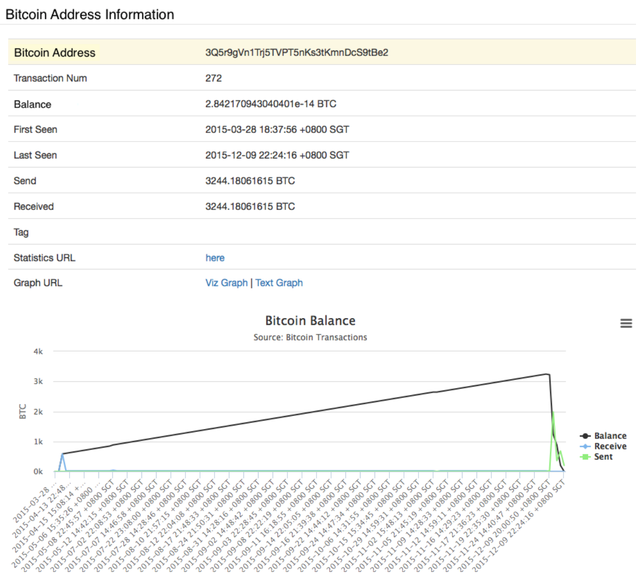
Bitcoin Address Text Graph

Bitcoin Address	3Bgk1oHeomvu6bo4q6RKA6xoA8X8B342Y7
Tag	
Vertex Num	300
Edge Num	807
Balance URL	here
Statistics URL	here
Graph URL	Viz Graph | Text Graph

Tx Id	Src Address	Tag	Dst Address	Tag	Date	Sent / Receive	Sent BTC	Receive BTC
e18a0895bc	1M2ShdmGgA		3Bgk1oHeom		2014-07-18 19:29:31 +0800 SGT	Receive	0.01133906	0.0002
e18a0895bc	1M2ShdmGgA		3Bgk1oHeom		2014-07-18 19:29:31 +0800 SGT	Receive	0.01133906	0.0002
3fddaec916	3Bgk1oHeom		19ASyqc4Cf		2014-07-18 19:56:17 +0800 SGT	Sent	0.0002	0.0001
3fddaec916	3Bgk1oHeom		19ASyqc4Cf		2014-07-18 19:56:17 +0800 SGT	Sent	0.0002	0.0001
ac3548138f	3Mq4VRttTt		3Bgk1oHeom		2014-07-18 20:26:27 +0800 SGT	Receive	249.9999	249.9998
ac3548138f	3Mq4VRttTt		3Bgk1oHeom		2014-07-18 20:26:27 +0800 SGT	Receive	249.9999	249.9998
7be523da62	1Kq53gPmKL		3Bgk1oHeom		2014-07-28 21:52:54 +0800 SGT	Receive	0.804262	82.42453474
7be523da62	1Kp5yQxpjV		3Bgk1oHeom		2014-07-28 21:52:54 +0800 SGT	Receive	0.17	82.42453474

Fig. 16. The relation of DD4BC suspicious address “3Bgk1o” received BTC from many addresses. It sents BTC to three addresses include “3Q5r9g”.

[3] 1KP72fBmh3XBRfuJDMn53APaqM6iMRspCh
[4] 18iEz617DoDp8CNQUyyrjCcC7XCGDf5SVb
[5] 1H2bstU3yCpqJyrNzHSrnperZnTMSwLa5K
[6] 17WQov8BTXJAemWmqn5XJ8ibiq13SNoaqs
[7] 1FsVcdeHbpvUVT3gjeuVR2ZSDnpcsJMsLL
[8] 3Bgk1oHeomvu6bo4q6RKA6xoA8X8B342Y7
[9] 3Q5r9gVn1Trj5TVPT5nKs3tKmnDcS9tBe2



Bitcoin Address Information

Bitcoin Address	3Q5r9gVn1Trj5TVPT5nKs3tKmnDcS9tBe2
Transaction Num	272
Balance	2.842170943040401e-14 BTC
First Seen	2015-03-28 18:37:56 +0800 SGT
Last Seen	2015-12-09 22:24:16 +0800 SGT
Send	3244.18061615 BTC
Received	3244.18061615 BTC
Tag	
Statistics URL	here
Graph URL	Viz Graph | Text Graph

Bitcoin Balance
Source: Bitcoin Transactions
4k
3k
2k
1k
0k
BTC
Balance
Receive
Sent
2015-03-28 ...
2015-04-13 22:48...
2015-04-15 15:08:14 +...
2015-05-06 15:35:26 +0800 ...
2015-05-08 22:45:57 +0800 SGT
2015-05-12 14:42:15 +0800 SGT
2015-07-02 22:08:53 +0800 SGT
2015-07-07 14:46:58 +0800 SGT
2015-07-22 23:08:00 +0800 SGT
2015-07-28 14:28:46 +0800 SGT
2015-08-10 21:57:15 +0800 SGT
2015-08-12 22:04:08 +0800 SGT
2015-08-17 21:48:33 +0800 SGT
2015-08-24 21:50:31 +0800 SGT
2015-08-31 14:28:16 +0800 SGT
2015-09-02 14:48:42 +0800 SGT
2015-09-03 22:28:45 +0800 SGT
2015-09-08 22:22:19 +0800 SGT
2015-09-11 16:18:55 +0800 SGT
2015-09-14 22:05:05 +0800 SGT
2015-09-16 21:39:38 +0800 SGT
2015-09-22 14:44:12 +0800 SGT
2015-09-24 14:47:34 +0800 SGT
2015-10-06 14:31:55 +0800 SGT
2015-10-15 15:34:45 +0800 SGT
2015-10-29 14:59:31 +0800 SGT
2015-11-02 15:48:13 +0800 SGT
2015-11-05 21:45:19 +0800 SGT
2015-11-09 14:28:33 +0800 SGT
2015-11-12 14:59:11 +0800 SGT
2015-11-16 14:29:23 +0800 SGT
2015-11-17 21:36:23 +0800 SGT
2015-11-19 22:35:30 +0800 SGT
2015-11-24 14:40:47 +0800 SGT
2015-12-09 20:00:50 +0800 SGT
2015-12-09 22:24:16 +0800 SGT

Fig. 17. The balance of DD4BC suspicious address “3Q5r9g”. It collected 3,244 BTC, then finally sent it to other address at the end of 2015.

[7]. Law enforcement has already gathered many addresses information for investigation and training, in order to support manually investigation process, our system supports almost features except for Web API, because of it focuses on local environment. We combine these sites’ features and our original features are based on analytical process to analyze already known addresses using public and private information.

Additionally, we consider information sharing with other stakeholders and researchers to be key for the evolution of our system, then we provide the system and source code in the future.

VI. Conclusions

Bitcoin technology is an innovative rebranding of e-payments but also has taken an important position in the criminal modus operandi, being used for trading or ransom payment. In order to prevent and detect these cases, we need to develop a practical methods, and suitable set of solutions at the local environment for the investigation process and training. We have proposed the Bitcoin analytical process and the practical system that can stand alone and provide effective Bitcoin analyzing result for the investigation field and training. In our evaluation, we could analyze the specific known addresses relate to suspicious activities in marketplace, ransomware and DDoS extortion case. We believe that the proposed analytical process and system can help throughout making investigation report at law enforcement. Additionally, we will be pushing for cooperation with other sites and researchers for better understanding and sharing of techniques, source code and data.

Acknowledgment

We would like to thank Pieter Hartel from University of Twente and Costel Ion from INTERPOL Global Complex for Innovation for discussions and feedback, the anonymous reviewers for their helpful comments.

References

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” in *https://bitcoin.org/bitcoin.pdf*, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, “A fistful of bitcoins,” in *The Internet Measurement Conference 2013*, 2013.

[3] D. Ron and A. Shamir, “Quantitative Analysis of the Full Bitcoin Transaction Graph.” *Financial Cryptography*, vol. 7859, no. Chapter 2, pp. 6–24, 2013. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-39884-1_2

[4] F. Reid and M. Harrigan, “An Analysis of Anonymity in the Bitcoin System,” in *Security and Privacy in Social Networks*, 2013.

[5] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, “Sok: Research perspectives and challenges for bitcoin and cryptocurrencies,” in *36th IEEE Symposium on Security and Privacy*, 2015.

[6] Chainalysis Inc. (2014) Chainalysis reactor. [Online]. Available: https://chainalysis.com/

[7] A. Janda. (2013) Walletexplorer.com: smart bicoin block explorer. [Online]. Available: https://www.walletexplorer.com/

[8] P. Stevens. (2016) Blockbin. [Online]. Available: http://blockbin.com/blog/

[9] I. Brugere. (2013) Bitcoin Transaction Network Dataset. [Online]. Available: http://compbio.cs.uic.edu/data/bitcoin/

[10] M. Spagnuolo, F. Maggi, and S. Zanero, “BitIodine: Extracting Intelligence from the Bitcoin Network,” in *Eighteenth International Conference Financial Cryptography and Data Security*, Mar. 2014.

[11] The Bitcoin Foundation. (2011) Bitcoin core. [Online]. Available: https://bitcoin.org/

[12] ASERT, “ASERT Threat Intelligence Brief 2015-04 DD4BC DDoS Extortion Activity,” Tech. Rep., Jun. 2015.

[13] K. Liao, Z. Zhao, A. Doupé, and G.-J. Ahn, “Behind closed doors - measurement and analysis of CryptoLocker ransoms in Bitcoin.” *eCrime*, pp. 1–13, 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7487938/

[14] F. Tschorsch and B. Scheuermann, “Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies,” in *eprint.iacr.org*, May 2015.

[15] SatoshiDice. (2012) The original blockchain-based bitcoin dice game. [Online]. Available: https://www.satoshidice.com/

[16] BitStamp. (2013) buy and sell bitcoins. [Online]. Available: https://www.bitstamp.net/

[17] FBI, “Bitcoin Virtual Currency: Intelligence Unique Features Present Distinct Challenges for Deterring Illicit Activity ,” May 2012.

[18] E. C. Bank, “Virtual currency schemes - a further analysis,” Feb. 2015.

[19] R. W. Ulbricht. (2011) Silk road. [Online]. Available: http://silkroad6ownowfk.onion

[20] Verto. (2014) Evolution. [Online]. Available: http://k5zq47j6wd3wdvjq.onion

[21] KrebsonSecurity. (2013) Cryptolocker crew ratchets up the ransom. [Online]. Available: http://goo.gl/V32ncu

[22] Europol. (2016) International action against dd4bc cybercriminal group. [Online]. Available: https://goo.gl/Ei6bbx

[23] T. Moore and N. Christin, “Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk.” *Financial Cryptography*, vol. 7859, no. Chapter 3, pp. 25–33, 2013. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-39884-1_3

[24] Blockchain.info. (2011) Blockchain.info. [Online]. Available: https://blockchain.info/