Practical Analyzing the Relation of Wallet Addresses in Bitcoin

Hiroki Kuzuno[a,b], Christian Karam[b]
[a]SECOM Co., Ltd.,
[b]Research and Innovation, INTERPOL, IGCI

Goal and Contributions

- Goal and Contributions
  - Tracing suspicious activity of crime in Cryptcurrencies
  - Providing useful information and analyzing infrastructure
    - Supporting Cryptocurrencies forensics for law enforcement
    - Easily finding specific wallet address (address) relations
- Evaluation: Practical investigation process in Bitcoin
  - Rethinking at some cybercrime cases
    - Market Place: Bitcoin information in SilkRoad
    - Ransomware: Address relations in cryptolocker
    - DD4BC: Address relations and limitation
- Discussion: Analyzing limitation in Cryptocurrencies

Outline

- Background and Problem
  - Cryptocurrencies Trend
  - Bitcoin information and relation of cybercrime
- Analyzing Overview
  - Scope and purpose for cryptocurrencies forensics
- Related Works
  - Practical tools and methods from private sector and academic
- Approach
  - Bitcoin analyzing methods : Address, Transaction, Block relations
  - Graphical viewing : useful information for law enforcement
- Evaluation
  - Showing Some cybercrime cases at our analyzing result
- Discussion
  - Limitation of Cryptocurrencies forensics
- Summary and Future Trend

Background and Problem

- Cryptocurrencies Trends
  - The number of cryptocurrencies：643 currencies, 1986 Markets

643 Currencies / 59 Assets / 1986 Markets Market Cap: $11,289,337,349 / 24h Vol: $90,960,784 / BTC Dominance: 80.9% Follow @CoinMKTCap

Crypto-Currency Market Capitalizations

Market Cap ▾ | Trade Volume ▾ | Trending ▾ | Tools ▾ | Search Currencies

All ▾ | Currencies ▾ | Assets ▾ | USD ▾ | Next 100 → | View All

#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$ 9,135,982,668	$ 584.53	15,629,675 BTC	$ 68,560,800	0.21 %	
2	Ethereum	$ 1,131,040,257	$ 14.00	80,779,358 ETH	$ 9,338,460	1.38 %	
3	Litecoin	$ 226,015,464	$ 4.90	46,114,876 LTC	$ 2,115,210	-0.37 %	
4	Ripple	$ 201,179,728	$ 0.005770	34,868,679,462 XRP *	$ 831,828	-0.00 %	
5	The DAO	$ 151,615,200	$ 0.129279	1,172,775,159 DAO *	$ 1,039,320	-0.56 %	
6	Dash	$ 50,856,773	$ 7.82	6,505,836 DASH	$ 324,569	0.48 %	
7	Lisk	$ 44,178,300	$ 0.441783	100,000,000 LSK *	$ 2,309,010	-7.95 %	
8	MaidSafeCoin	$ 26,508,348	$ 0.058575	452,552,412 MAID *	$ 417,148	-5.54 %	

Fig1. https://coinmarketcap.com

Fig 2 http://money.visualcapitalist.com/tag/bitcoin/

Background and Problem

- Cryptocurrencies' Problem in Bitcoin case
  - Bitcion becomes defects currency in cybercrime

Fig.3 Cryptolocker case
http://arstechnica.com/security/2013/10/youre-infected-if-you-want-to-see-your-data-again-pay-us-300-in-bitcoins/

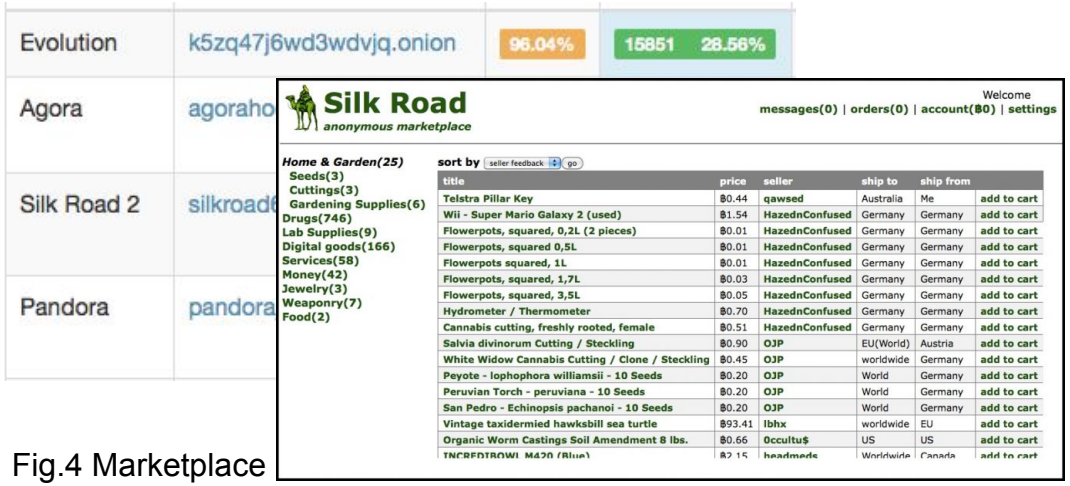
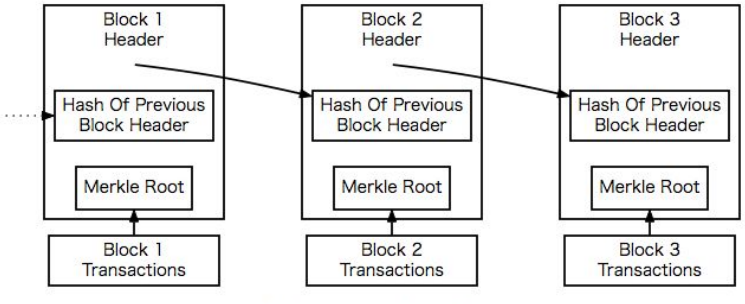


Fig.4 Marketplace
https://www.bestvpnz.com/silk-road-shut-down-by-fbi/

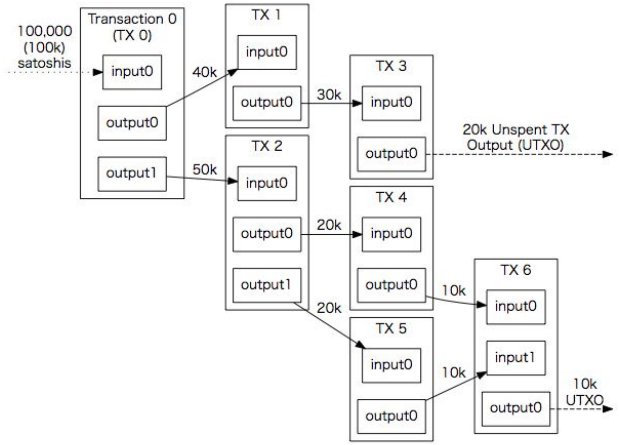
Fig.5 DD4BC https://www.neustar.biz/blog/ddos-extortion-and-bitcoin

Background and Problem

- Many advantages for users
  - Complex architecture : Blockchain, Peer-to-Peer network



Simplified Bitcoin Block Chain



Triple-Entry Bookkeeping (Transaction-To-Transaction Payments) As Used By Bitcoin

Fig. 6 Blockchain
https://bitcoin.org/en/developer-guide

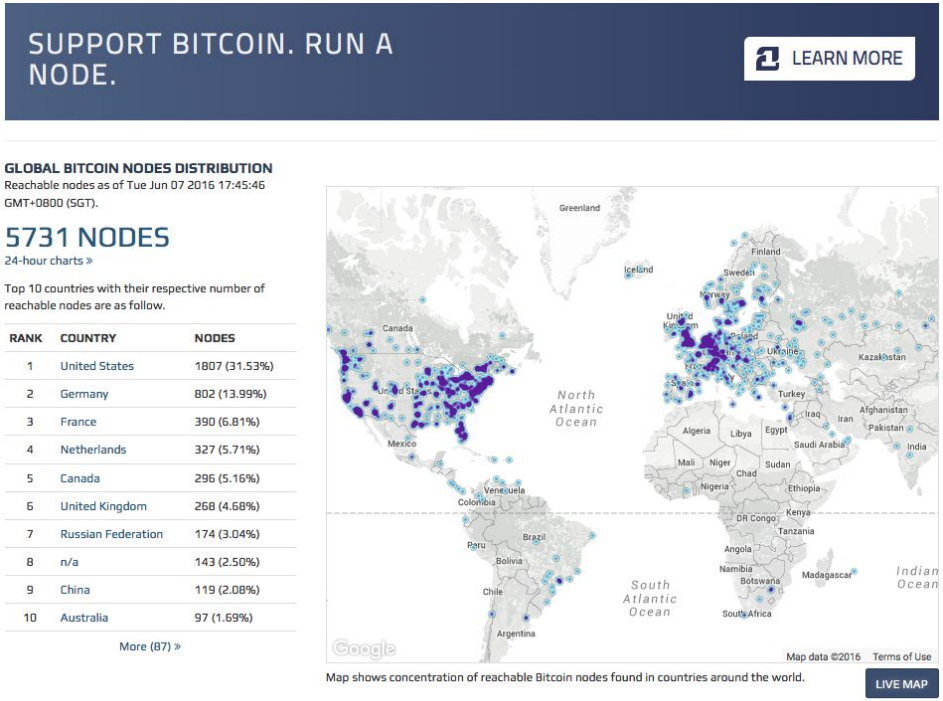


Fig.7 **Global Bitcoin Nodes Distribution**
https://bitnodes.21.co/

Background and Problem

- Many advantages for users
  - Pseudo anonymity : wallet address (address), exchange

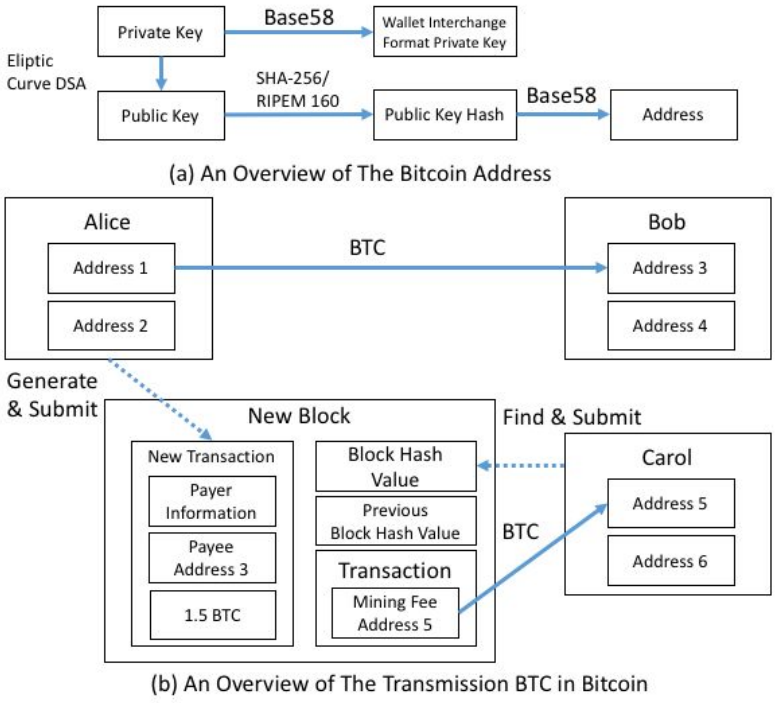


Fig.8 Sample case of address and payment

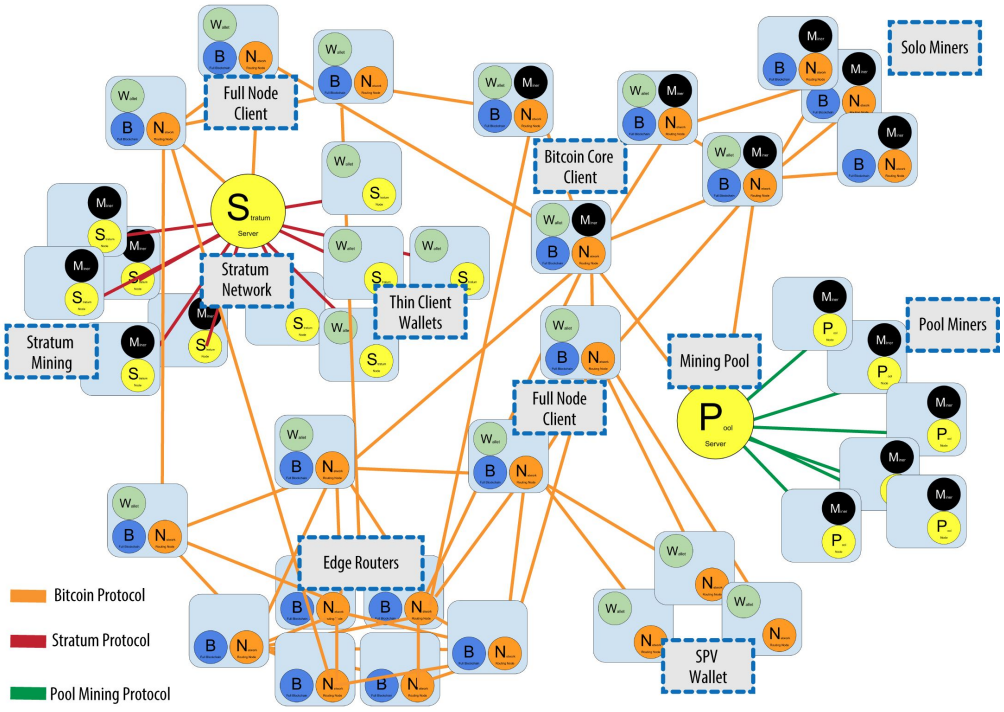


Fig.9 The extended bitcoin network showing various node types, gateways, and protocols
http://chimera.labs.oreilly.com/books/1234000001802/ch06.html

Analyzing overview

- Scope and Purpose
  - Tracing suspicious activity of crime in Cryptcurrencies
  - Providing useful information and analyzing infrastructure
- Motivations
  - Support practical cryptocurrencies investigation process
    - Easily investigate address relation without knowledge
- Goal
  - Detect the relations of addresses and point of exchange
- Approach : Practical Analyzing
  - Real time creating whole indexed data of Blockchain
  - Graphical and user friendly interface for investigator

Related Works

- Practical tools and methods from private sector and academic

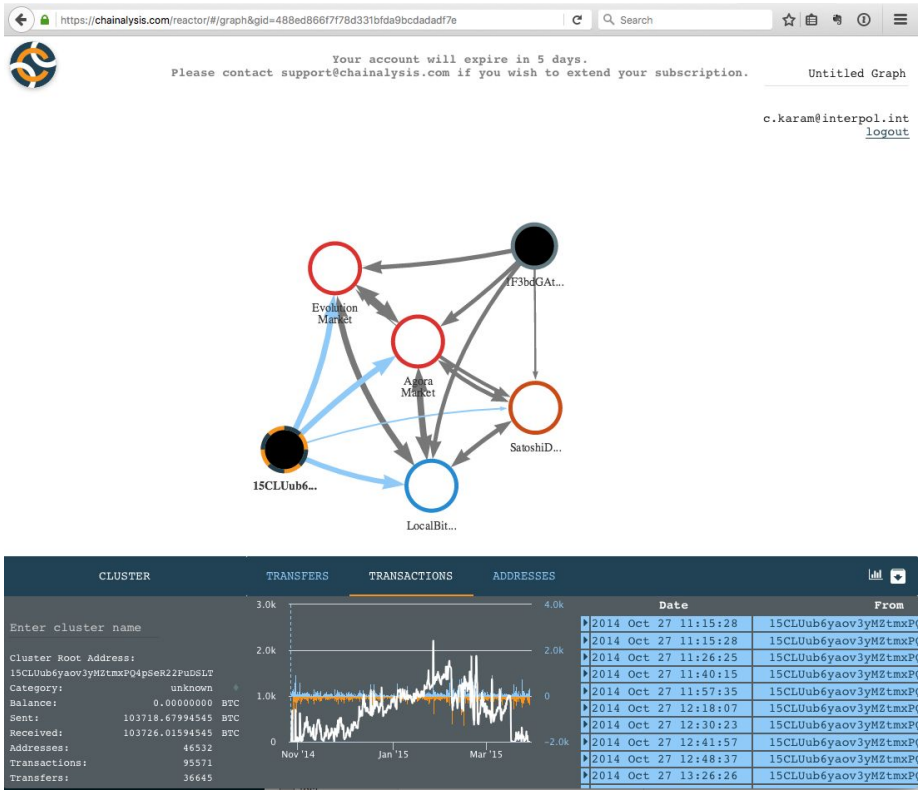


Fig.10 Sample of Chainalysis

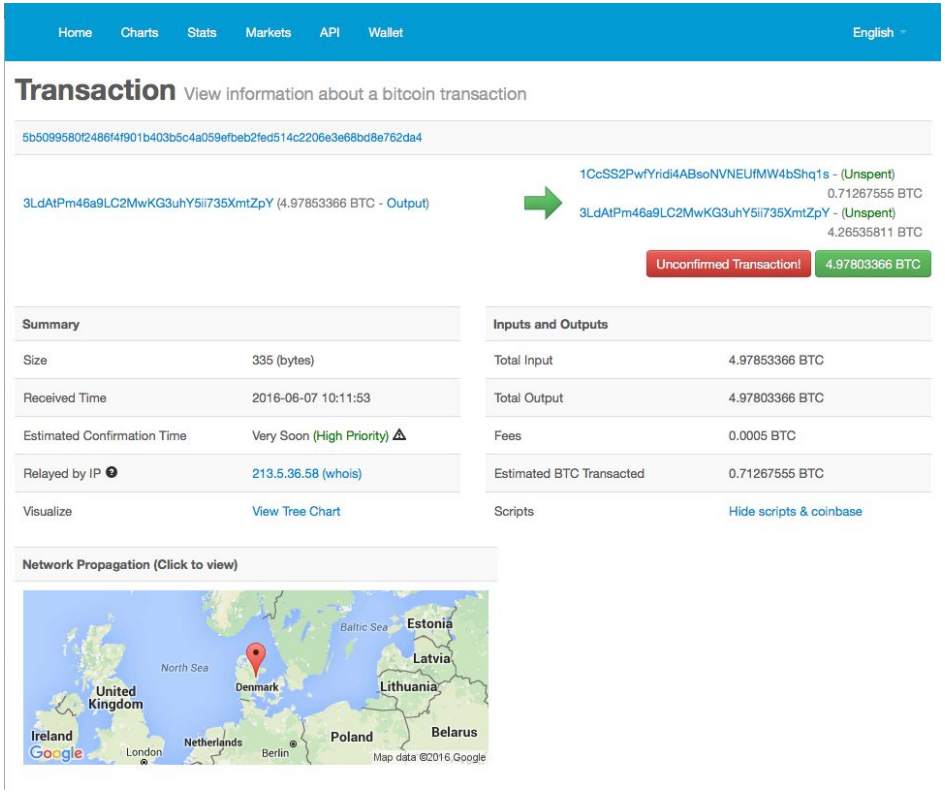


Fig.11 Sample of Blockchain.info

Related Works

- Practical tools and methods from private sector and academic

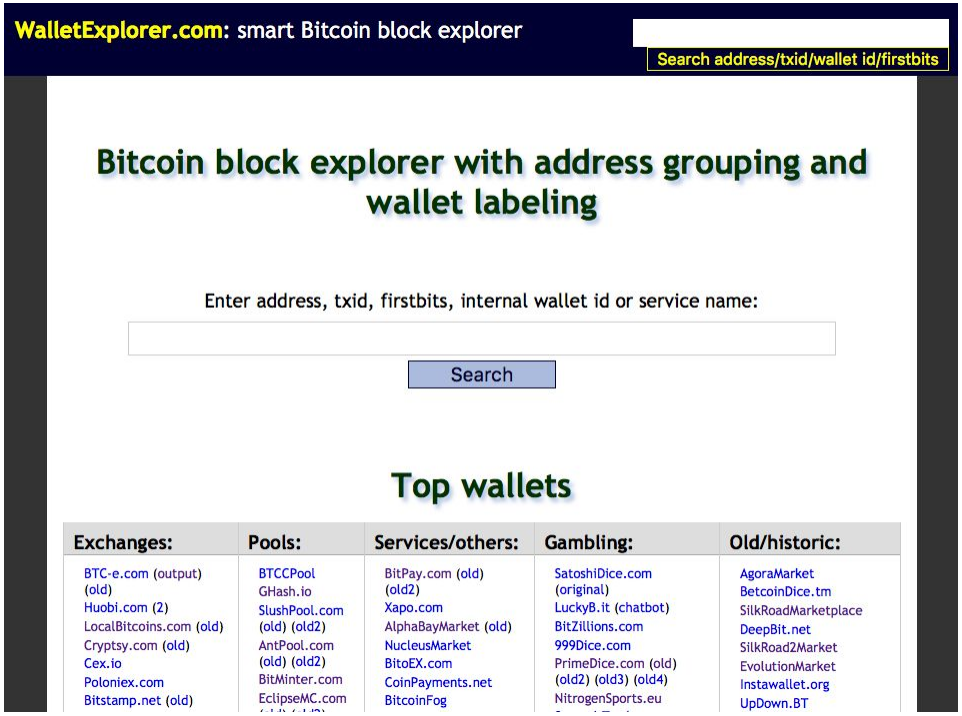


Fig.12 walletexplorer.com

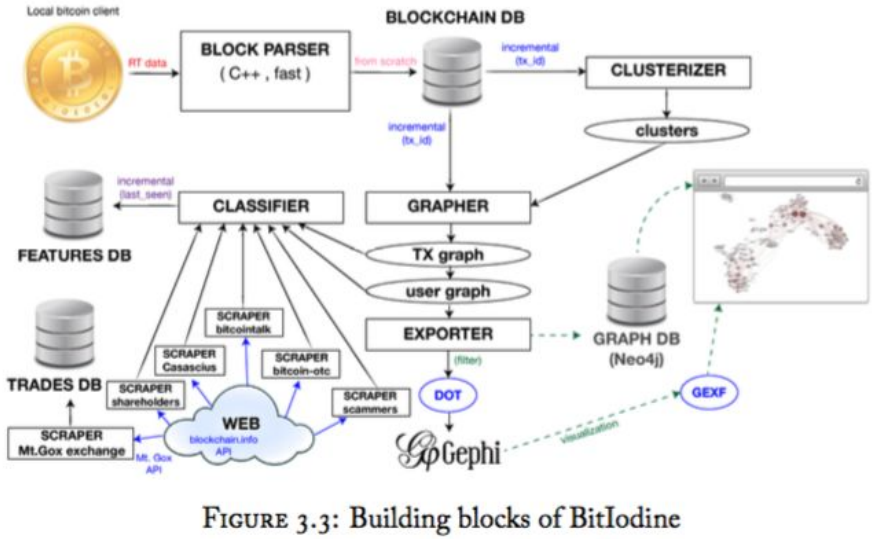


FIGURE 3.3: Building blocks of BitIodine

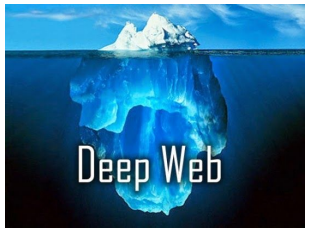
Fig.13 BitIodine

M. Spagnuolo, “BitIodine: Extracting Intelligence from the Bitcoin Network,” 2013.

Approach : Practical Analyzing in Our System

- Target
  - Wallet Address, Transaction, Block relation
- Bitcoin Analyzing method
  - Search: target, Bitcoin flow, specific date and amount (BTC,USD)
  - Statistics: weekly, hourly, yearly activity
  - Tagging: attribution of address
  - Clustering: group of addresses (transaction input based)
- Graphical viewing
  - Cluster Relation
    - Understanding each group connection, trend
  - Address Relation
    - Handling Bitcoin flow in each address

Bitcoin Analyzing Process Overview



Collecting Phase

Public / Private Data

Bitcoin Indexed Data

Original Tools

Analyzing Phase

Report

Public Tools

Address information
- Bitcoin flow
- Related addresses
- Activity time
- Exchange sites

Complementary
- IP address
- Related sites
- Other information

Evaluation: Case Study 01, SilK Road

- Silk Road Market Place: Shut down by FBI October 2013
- Addresses: leaked at forum
  - 1LDNLreKJ6GawBHPgB5yfVLBERi8g3SbQS, 6 hops -> 1933 …
  - 1933phfhK3ZgFQNLGSDXvqCn32k2buXY8a

Wallet Address Information

Wallet Address	1933phfhK3ZgFQNLGSDXvqCn32k2buXY8a
Transaction Num	61
Wallet 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

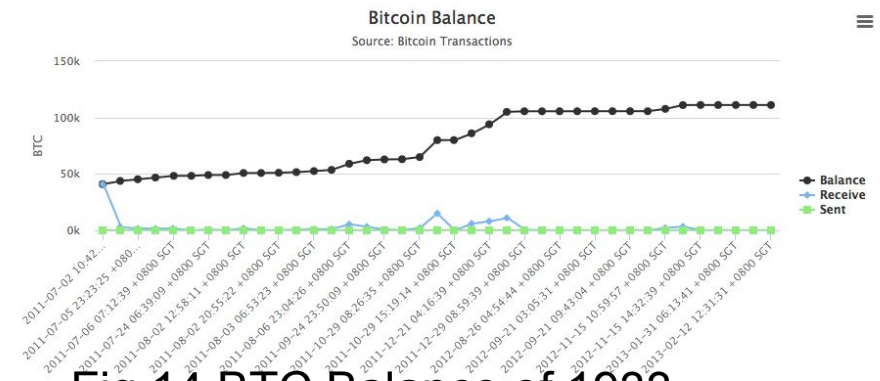


Fig.14 BTC Balance of 1933.

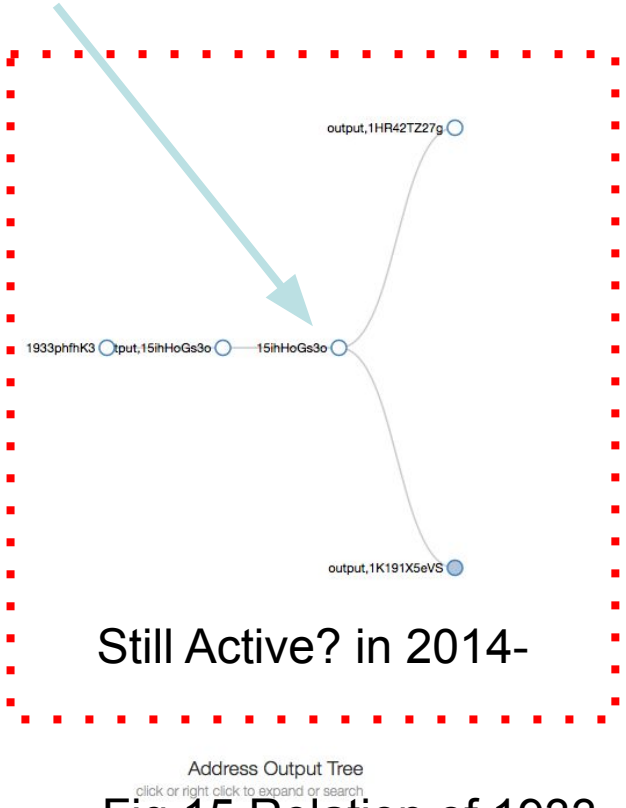
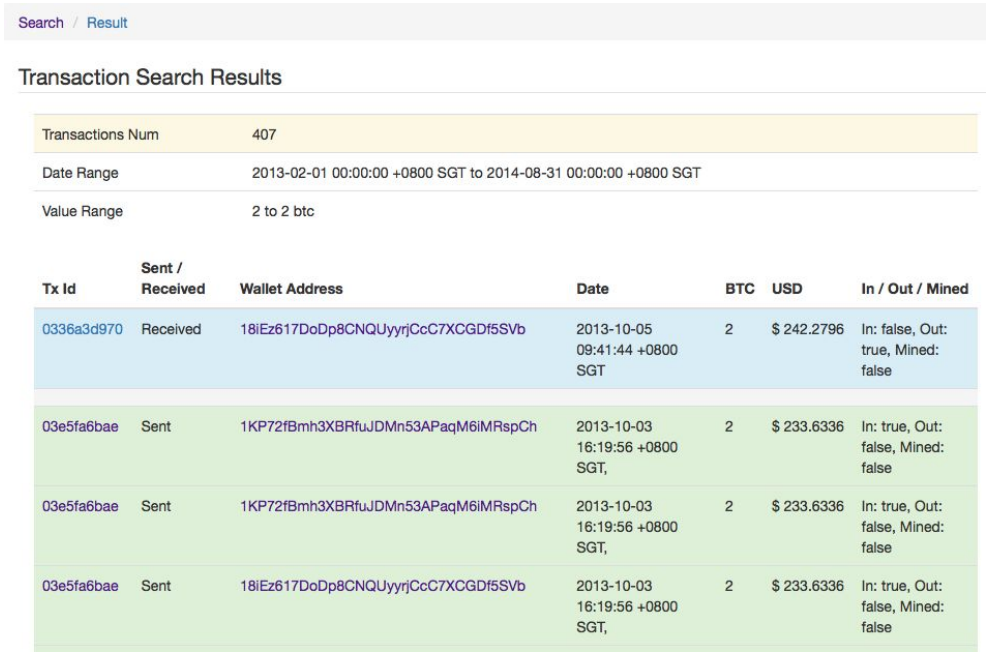


Fig.15 Relation of 1933..

Evaluation: Case Study 02, CryptoLocker

- Ransomware : CryptoLocker requires 2 BTC to victims
- Address
  - 1KP72fBmh3XBRfuJDMn53APaqM6iMRspCh
  - 18iEz617DoDp8CNQUyyrjCcC7XCGDf5SVb



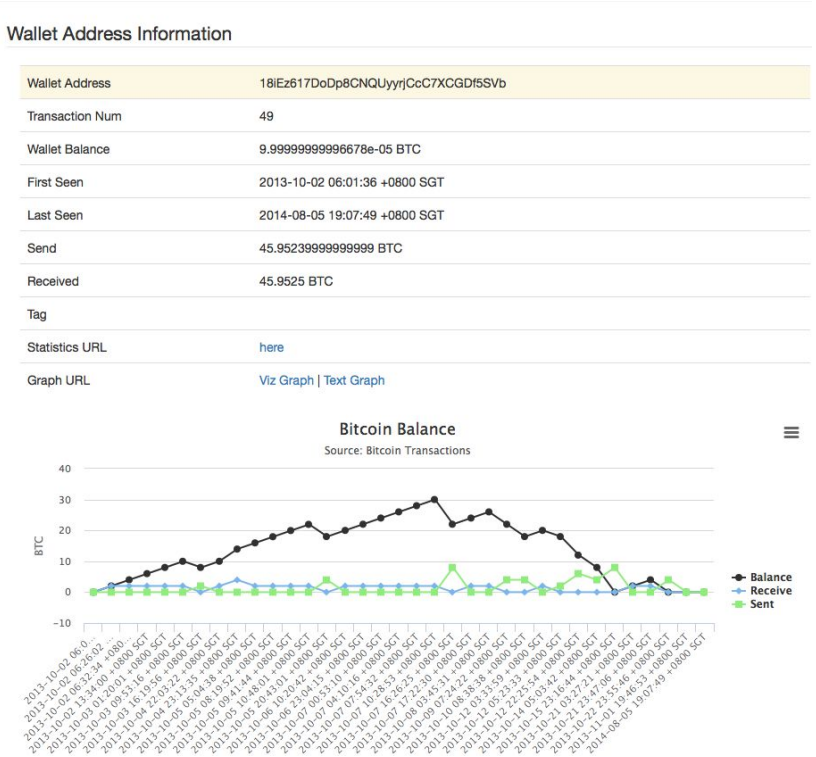
Search / Result

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	Wallet 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.16 Search Result of 2.0 BTC



Wallet Address Information

Wallet Address	18iEz617DoDp8CNQUyyrjCcC7XCGDf5SVb
Transaction Num	49
Wallet Balance	9.99999999996678e-05 BTC
First Seen	2013-10-02 06:01:36 +0800 SGT
Last Seen	2014-08-05 19:07:49 +0800 SGT
Send	45.95239999999999 BTC
Received	45.9525 BTC
Tag	
Statistics URL	here
Graph URL	Viz Graph | Text Graph

Fig.17 BTC Balance of 18iE…

Evaluation: Case Study 02, CryptoLocker

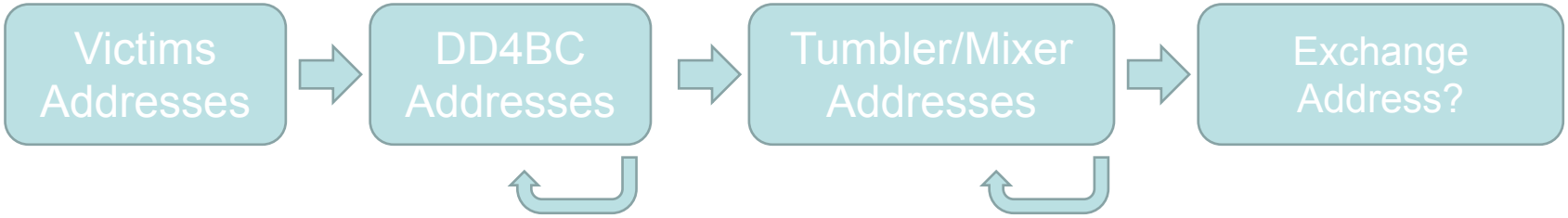
- Ransomware : CryptoLocker requires 2 BTC to victims
- Address
  - 1KP72fBmh3XBRfuJDMn53APaqM6iMRspCh
  - 18iEz617DoDp8CNQUyyrjCcC7XCGDf5SVb

Fig.18 Transaction Stats of 1KP7…

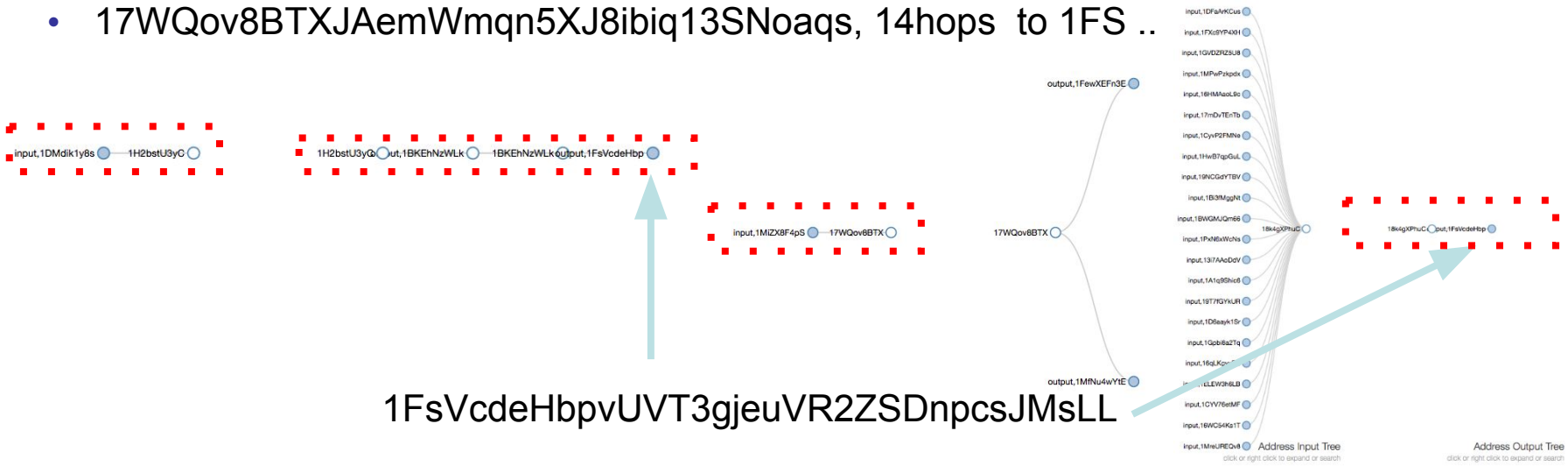
Fig.19 Relation of 1KP7…

Evaluation: Case Study 03, DD4BC

- Extortion: DD4BC (DDoS for Bitcoin)
- Relation Overview



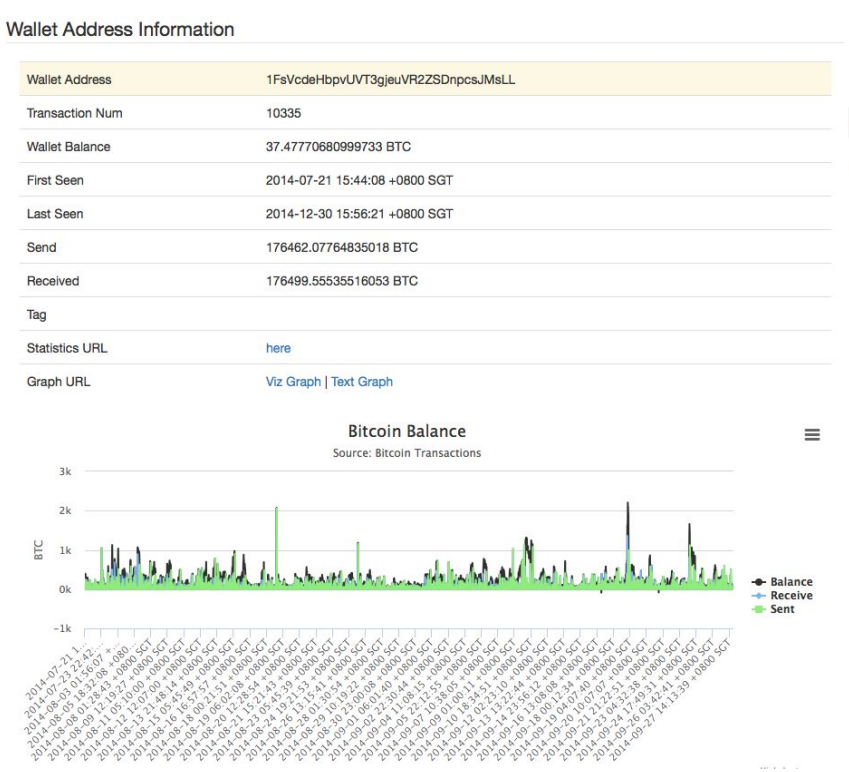
- DD4BC Addresses -> 1FsVcdeHb…
  - 1H2bstU3yCpqJyrNzHSrnperZnTMSwLa5K, 3hops to 1Fs…
  - 17WQov8BTXJAemWmqn5XJ8ibiq13SNoaqs, 14hops to 1FS ..

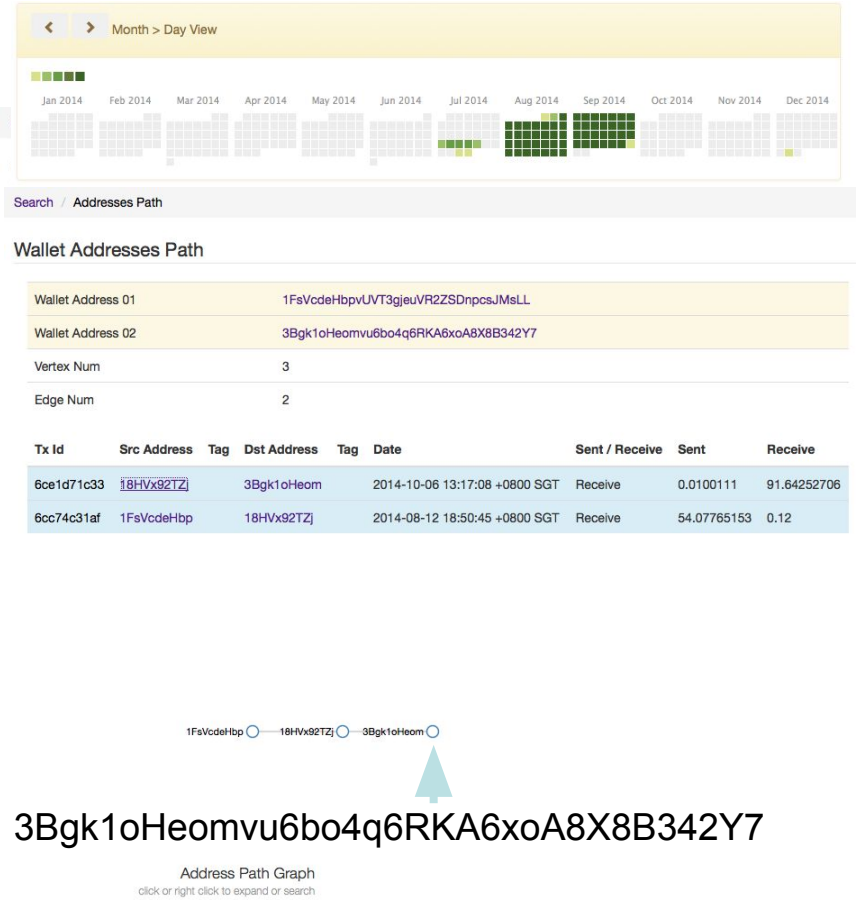


1FsVcdeHbpvUVT3gjeuVR2ZSDnpcsJMsLL

Evaluation: Case Study 03, DD4BC

- Extortion: DD4BC (DDoS for Bitcoin)
- Tumbling / Mixing Address
  - 1FsVcdeHbpvUVT3gjeuVR2ZSDnpcsJMsLL -> 3Bgk1oHeo…





Evaluation: Case Study 03, DD4BC

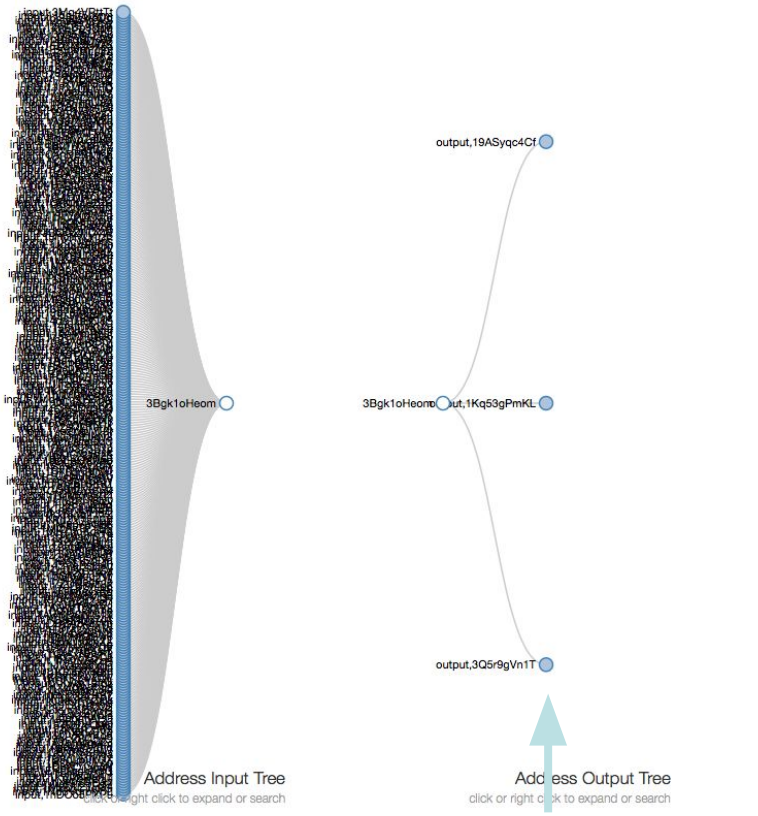
- Tumbling / Mixing Address
  - 3Bgk1oHeomvu6bo4q6RKA6xoA8X8B342Y7 -> 3Q5r9gVn….

Search / Wallet Address / Viz Graph / Text Graph

Wallet Address Text Graph

Wallet 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



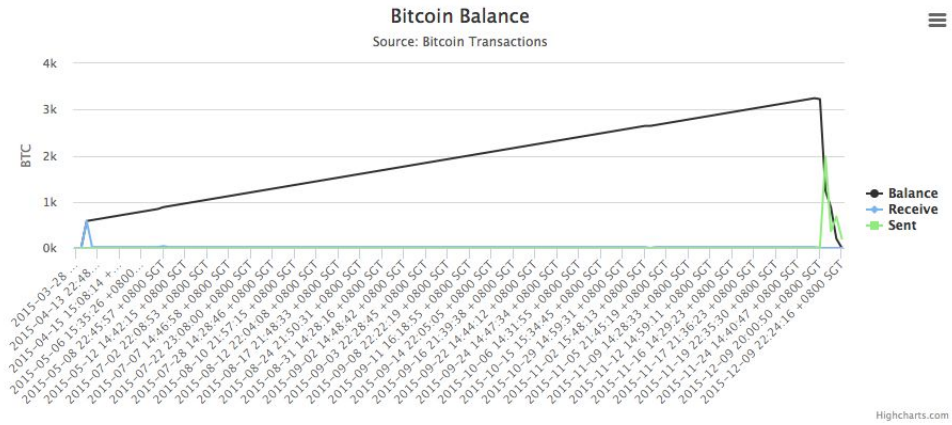
3Q5r9gVn1Trj5TVPT5nKs3tKmnDcS9tBe2

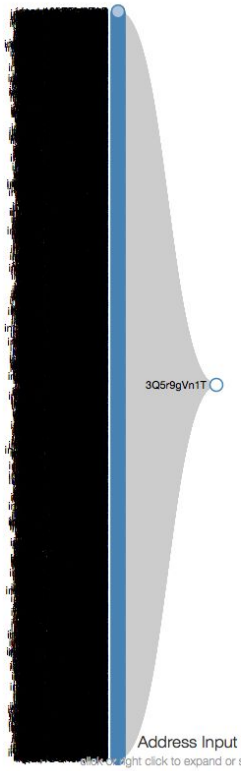
Evaluation: Case Study 03, DD4BC

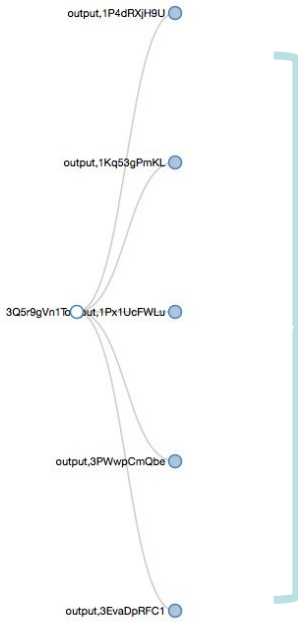
- Exchange Address?
  - 3Q5r9gVn1Trj5TVPT5nKs3tKmnDcS9tBe2

Wallet Address Information

Wallet Address	3Q5r9gVn1Trj5TVPT5nKs3tKmnDcS9tBe2
Transaction Num	272
Wallet 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





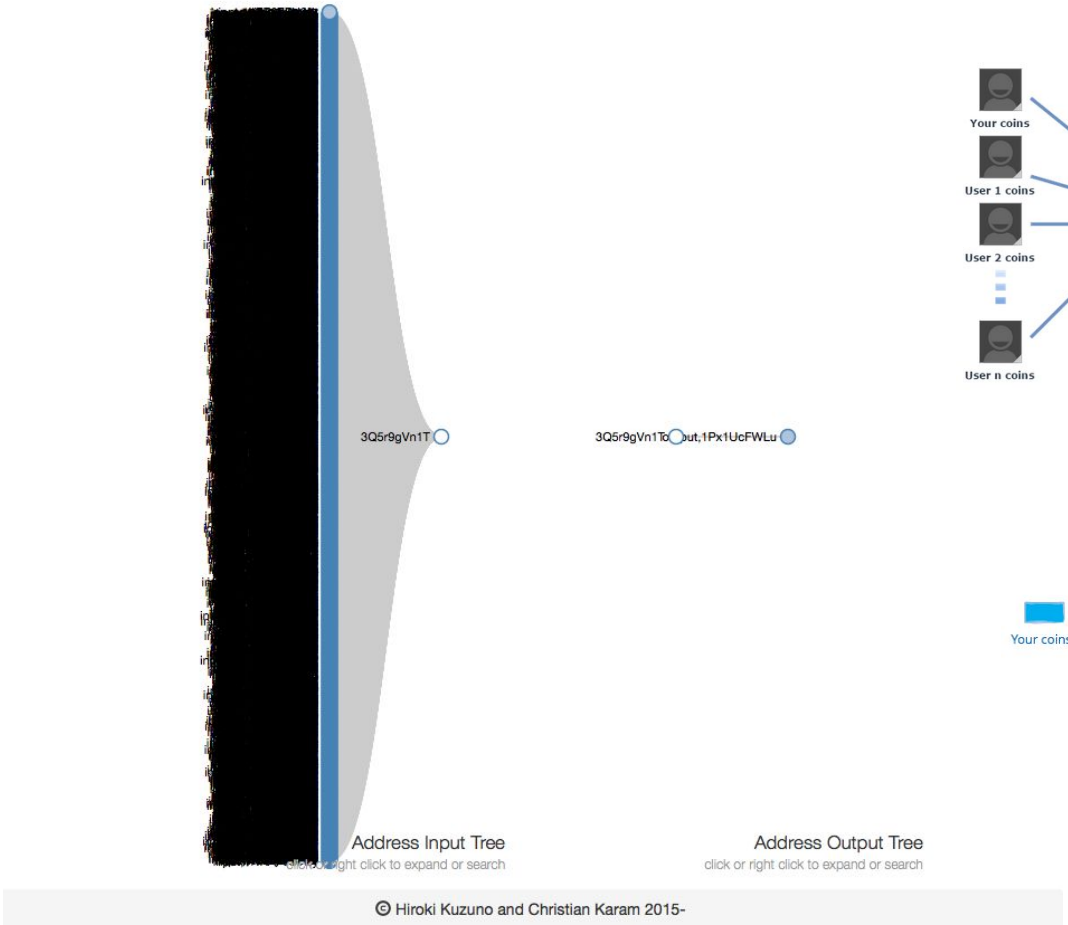


Discussion

- Limitation of Cryptocurrencies Forensics
  - Knowledge Requirement
    - Cryptography: Hash, Signature, Public Key Crypt, …
    - Network: TCP/IP, P2P, Tor, VPN, ...
    - Bitcoin : Blockchain, address / transaction mechanism
  - Tumbling / Mixing Service
    - It breaks up any Bitcoin flow and address relations
  - Data size
    - The number of unique address is increasing
    - Total Transaction is huge

Discussion

- Tumbling / Mixing Service



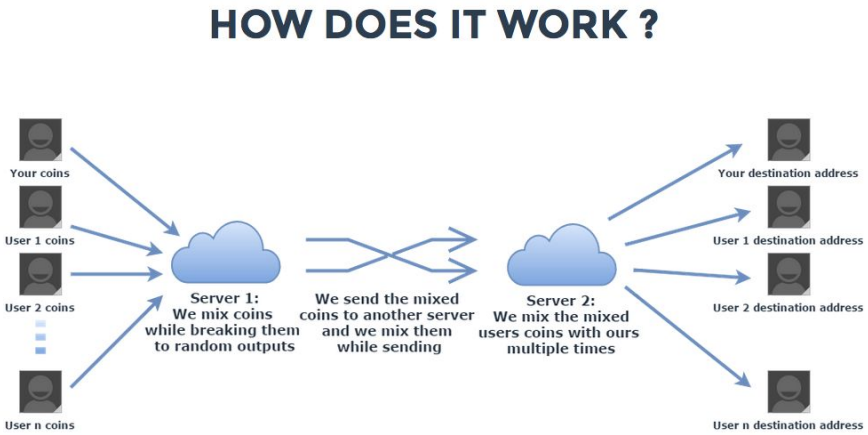


Fig.20 https://www.fogify.net/

Fig.21 https://bitmixer.io/

Discussion

- Data size: Over 60GBytes (raw db size)
  - Address (2009-2015): 32,611 -> 57,723,195
  - Transaction (2016.06) : 134,449,708

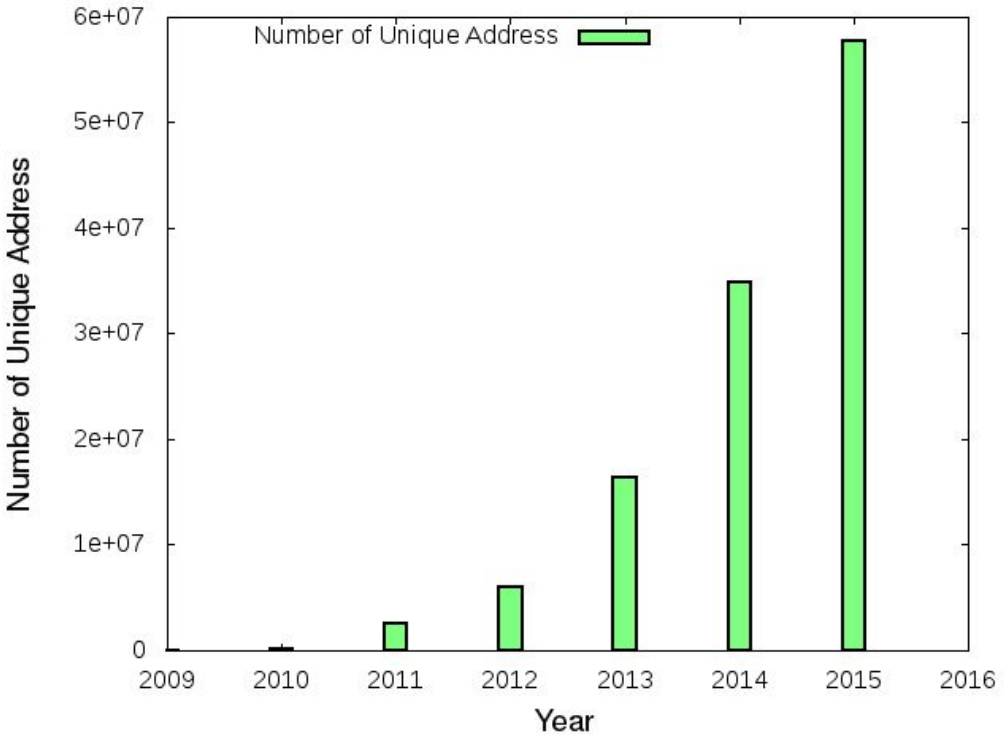


Fig.22 The number of unique address

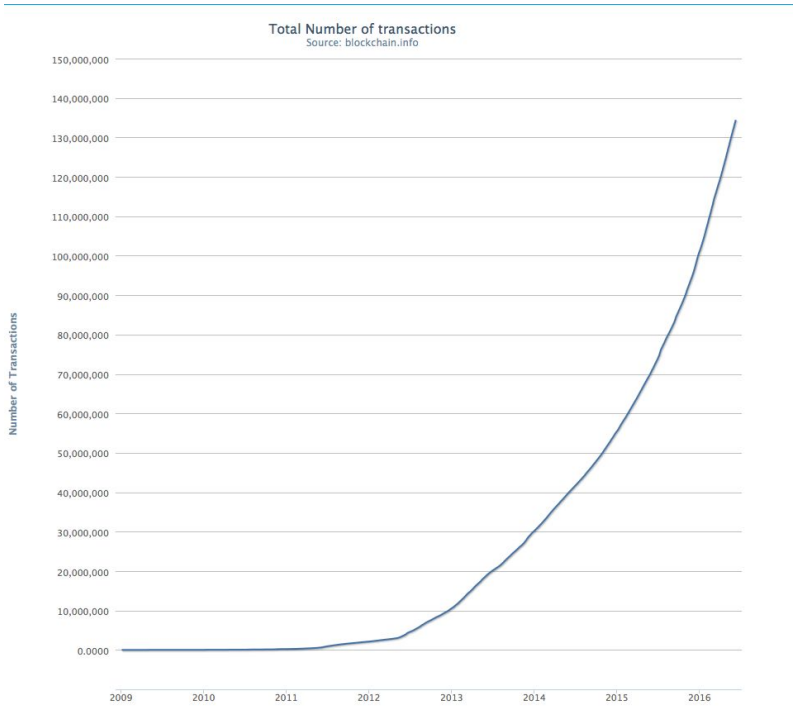


Fig.23 Total number of transactions
https://blockchain.info/charts/n-transactions-total

Summary and Future Trend

- Cryptocurrencies is new field of Forensics
  - In cybercrime, Bitcoin becomes de fact currency
  - No silver bullet and no one solution
- Our approach of investigation
  - Focusing macro / micro information of Bitcoin flow
  - Using outside information: Forum, Marketplace, Chat, and so on
  - Practical methods are important
    - Combine public tools and private tool
    - Collaboration with private, public sectors and academic people

⇒We continue to tackle with detection and tracing “suspicious” activity

- Future Trend
  - Cryptocurencies forensics: Tumbling, Exchange, Miner analyzing
  - Bitcoin Transaction Pattern Recognition, Big Graph Handling

Clustering of Addresses

- Assumption
  - If sender wallet addresses in same transaction input, these are managed by one user
    - e.x. Addr1 and Addr2 sent BTC to Addr3 in Tx1
    - One user has Addr1 and Addr2
- Reason
  - Bitcoin client supports multi wallet addresses (public/private key)
  - Bitcoin client requires a private key to sent BTC to other wallet address
    - Transaction input is signed by wallet address's private key
  - Bitcoin client doesn't support other Bitcoin client's BTC sending
    - It needs wallet address's private key
  - Sender wallet addresses in same transaction, these are managed by one user
    - These wallet addresses' private key are in same environment