

BitIodine: extracting intelligence from the Bitcoin network



Michele Spagnuolo

Federico Maggi

Stefano Zanero



<http://miki.it>

Is Bitcoin anonymous?

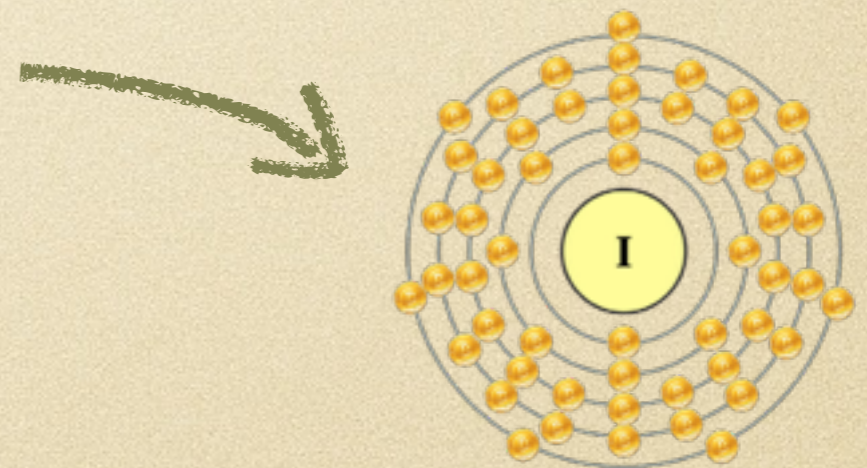
Yes

- No accounts
- No ID required
- Cash-like
- Tor / VPN help

No

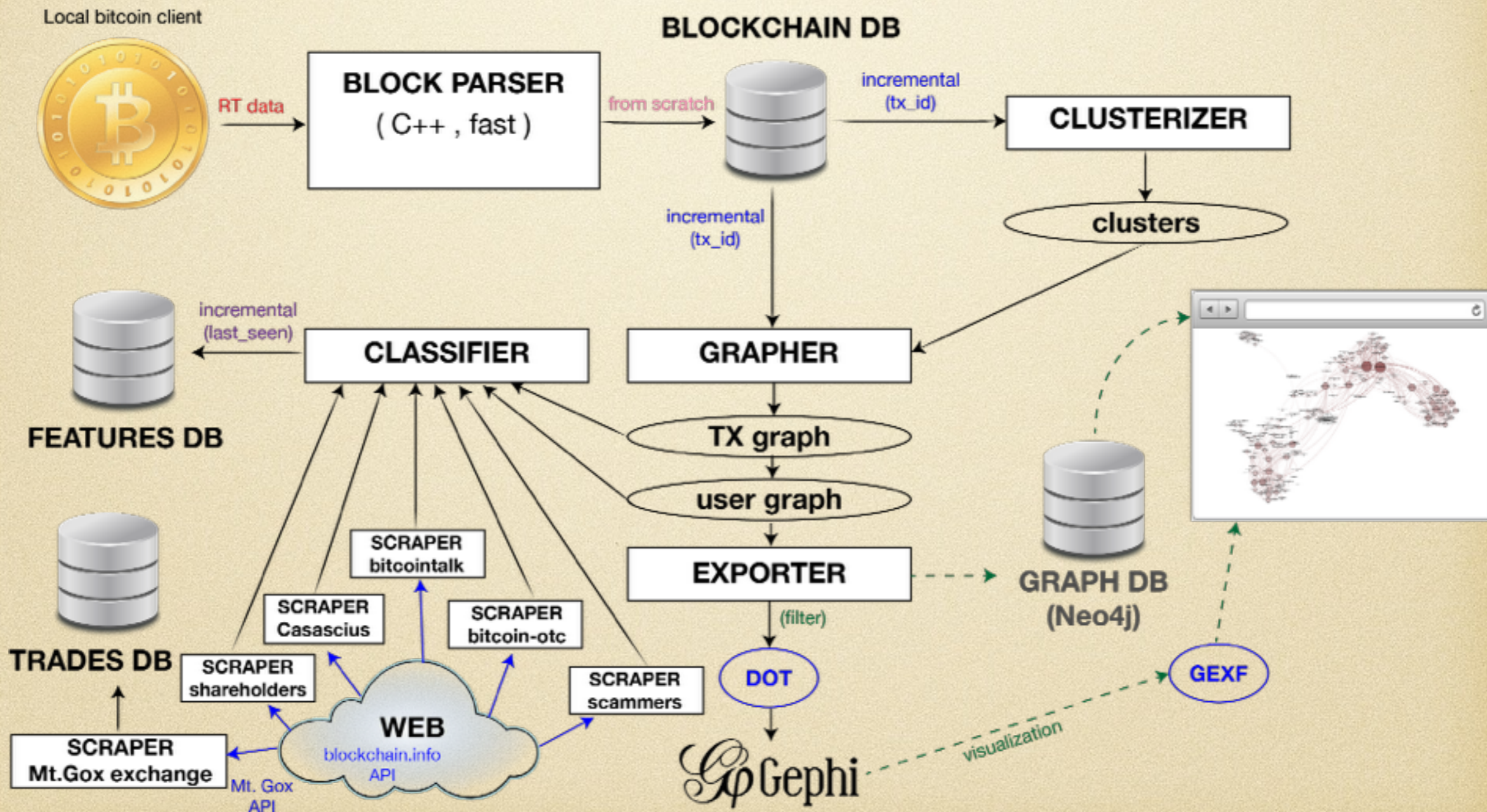
All transactions are public

Analysis of the blockchain can correlate addresses

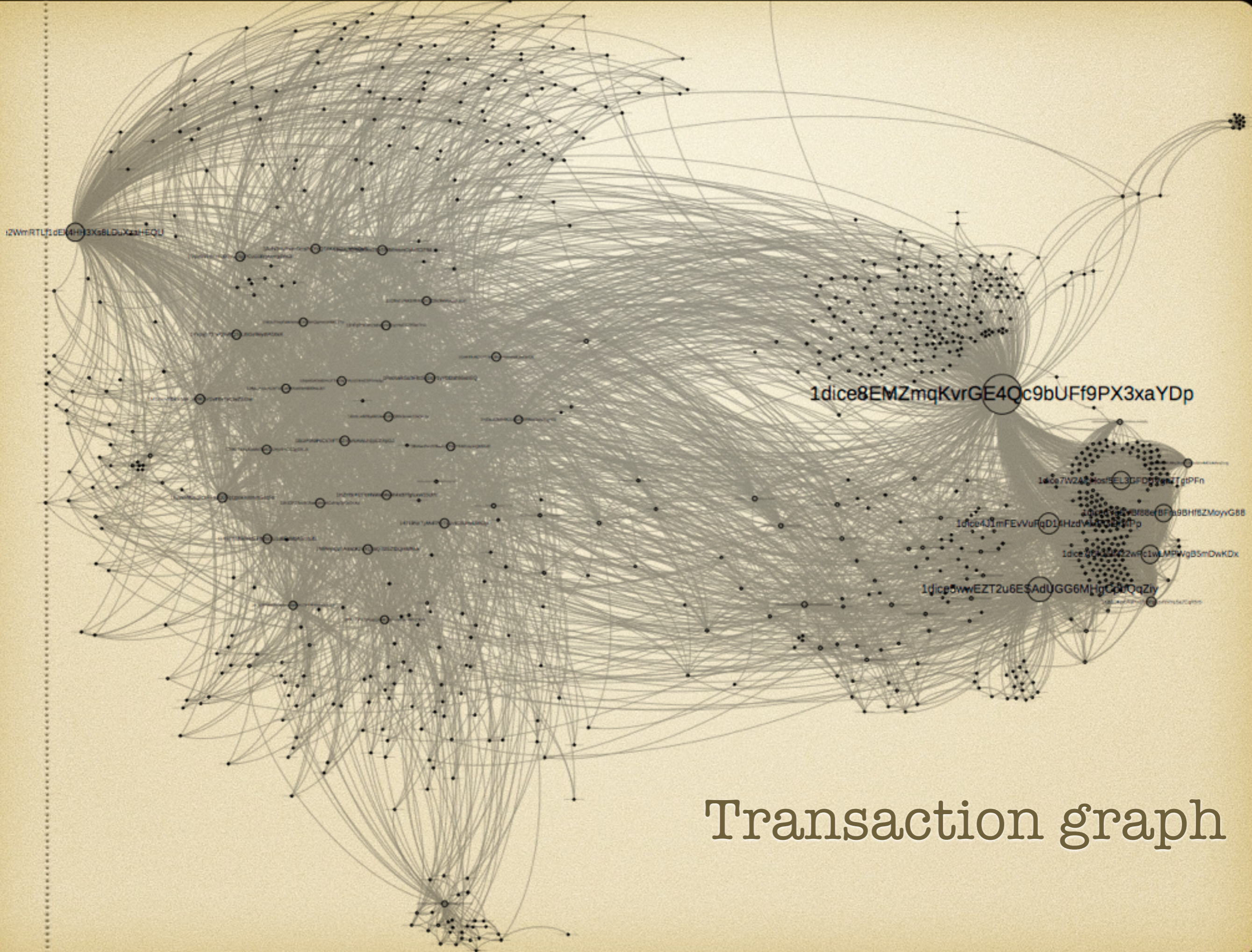


BitIodine

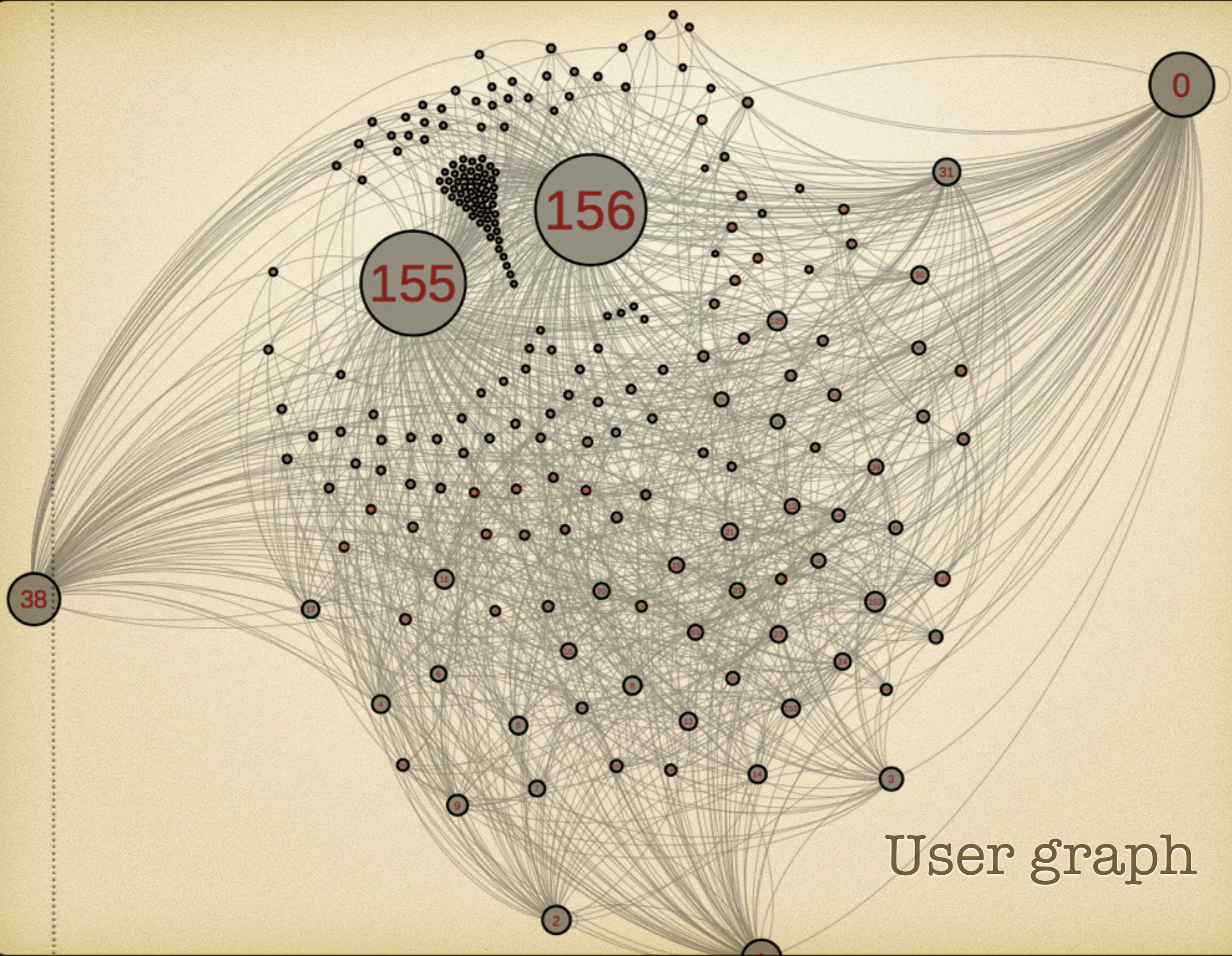
a tool for analyzing and profiling the Bitcoin network







Transaction graph

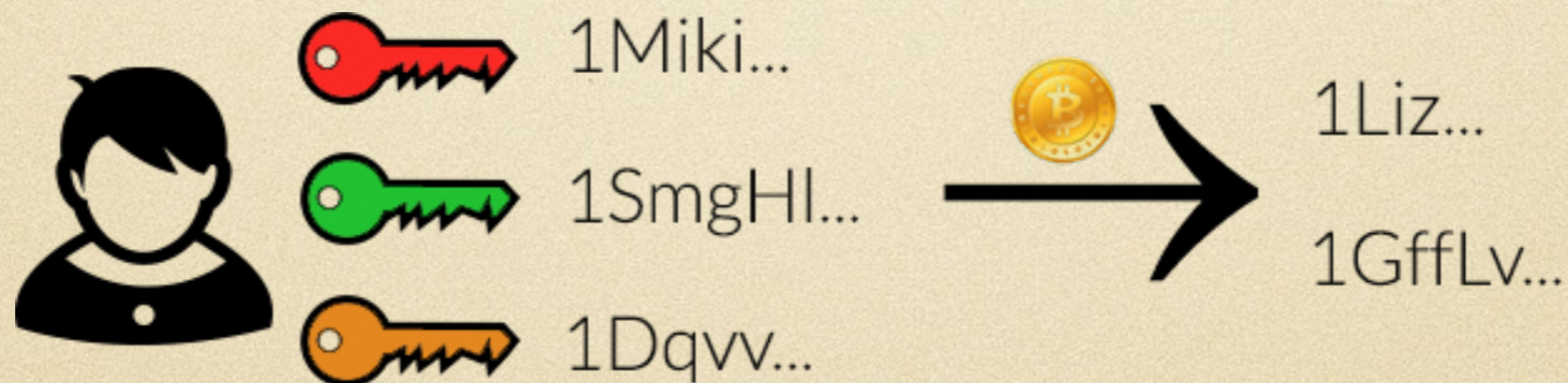


User graph

Multi-input transactions

When a transaction has **multiple input addresses**, we can safely assume that those addresses belong to the same wallet, thus to the **same user**.

Assumption: owners don't share private keys.



Shadow addresses

- Unspent output of a transaction **must be fully used** as input for a new transaction
- A *shadow address* is automatically created and used to collect back the *change*



Shadow addresses

When a Bitcoin transaction has *exactly* two output addresses, O_1 and O_2 , such that O_2 is a **new address** (i.e., an address that has never appeared before), and O_1 corresponds to a previously seen address, we can assume that O_2 constitutes a **shadow address** for input addresses of that transaction.

More than 90% of transactions have *exactly two outputs* (one *payee*, one *shadow address*).

Shadow addresses

The official bitcoin client tries to **randomize** the position of the change output, but **code is flawed**:

File: wallet.cpp

// Insert change txn at random position:

```
vector<CTxOut>::iterator position = wtxNew.vout.begin()+GetRandInt(wtxNew.vout.size());  
wtxNew.vout.insert(position, CTxOut(nChange, scriptChange));
```

Number of payees



← size()+1

If just two outputs (one payee), `GetRandInt(1)` always returns 0.

The change ends up always in the first output.

If multiple outputs, change is never the last output.

Fixed only in January 2013!

Shadow addresses

Given the bug in the official client, **BitIodine** checks transactions with *exactly two outputs*, and also checks that the first address was **new** at the time of the transaction.

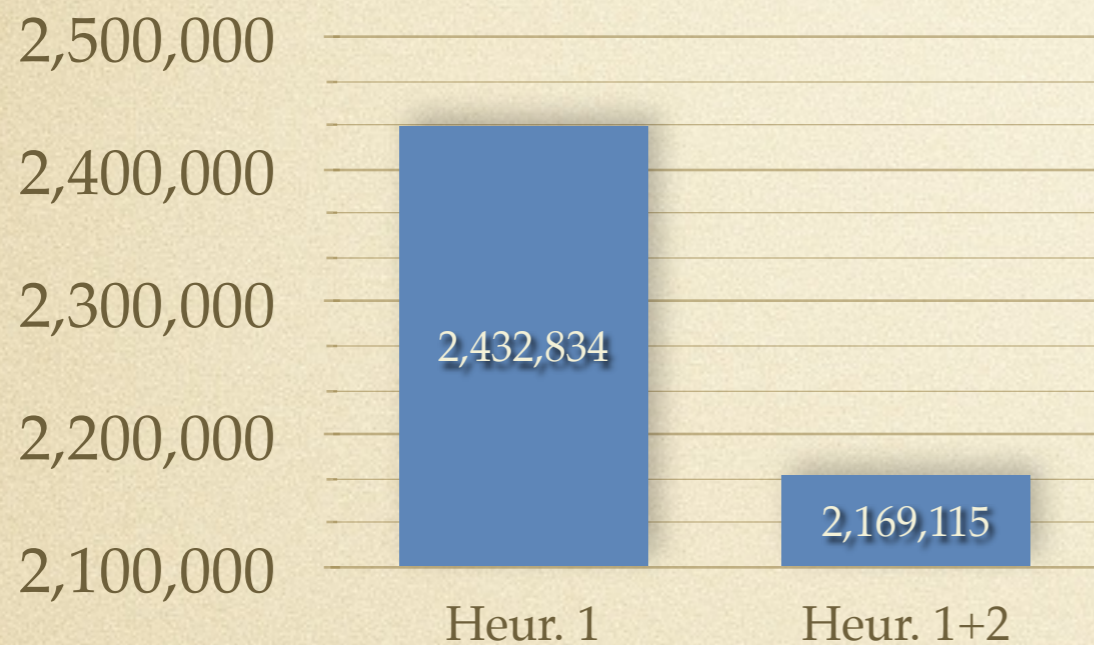
If it is, chances are it's a **shadow address**.

It is a **heuristic** applied to transactions that happened *before the bugfix*.

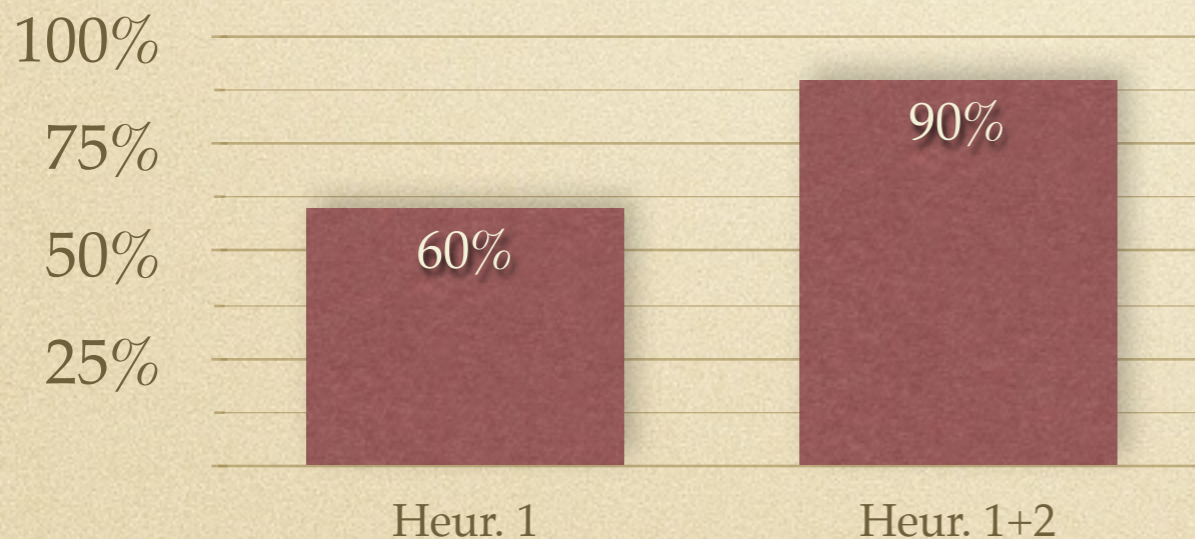


Evaluating heuristics

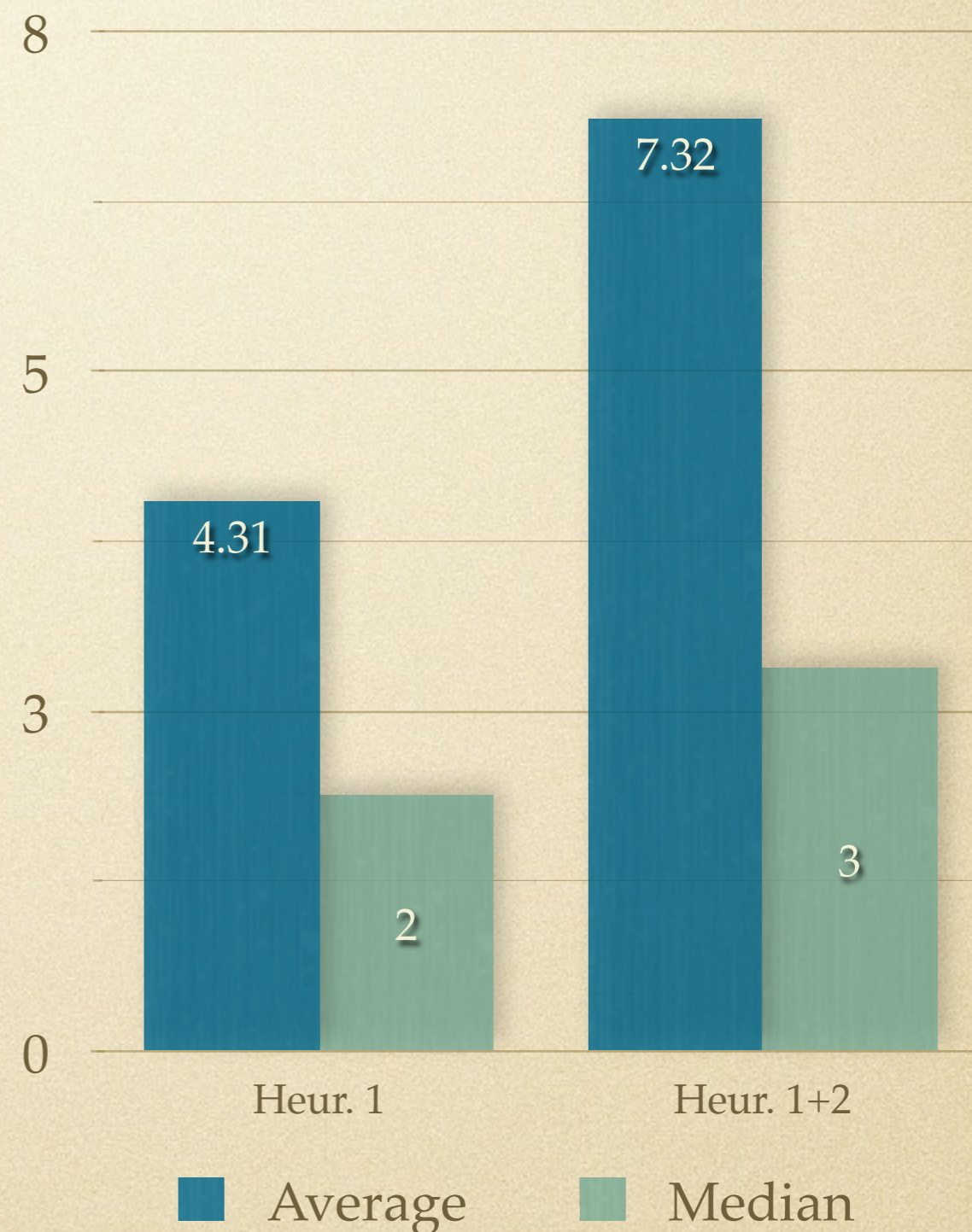
Number of clusters



Addresses clustered



Cluster size



Label	Type	Meaning
first_seen	NUMBER	Timestamp of the first appearance of the address in a transaction
last_seen	NUMBER	Timestamp of the last appearance of the address in a transaction
recv	NUMBER	Total amount received by the address
sent	NUMBER	Total amount sent from the address
balance	NUMBER	Balance of the address
n_tx	NUMBER	Number of transactions in which the address appears
cluster_id	NUMBER	The ID of the cluster the address belongs to
mining	RATIO	Ratio of transactions coming from direct or pooled mining
gambling	RATIO	Ratio of transactions to/from gambling sites
exchanges	RATIO	Ratio of transactions to/from exchanges
wallets	RATIO	Ratio of transactions to/from web wallets
bitcointalk	RATIO	Ratio of transactions to/from known BitcoinTalk users
bitcoinotc	RATIO	Ratio of transactions to/from known Bitcoin-OTC users
freebies	RATIO	Ratio of transactions to/from faucets or other freebies
donations	RATIO	Ratio of transactions to/from known donation addresses
OTA	BOOLEAN	One-Time-Address: appears in just one transaction
OLD	BOOLEAN	Not seen for a long time (<i>tunable</i>)
NEW	BOOLEAN	First appearance is recent (<i>tunable</i>)
EMPTY	BOOLEAN	Balance is close to zero
EXHAUSTED	BOOLEAN	EMPTY and has received more than current balance
RECENTLY_ACTIVE	BOOLEAN	Last activity is recent (<i>tunable</i>)
ZOMBIE	BOOLEAN	Was empty and dormant for a long time, then got used again
SCAMMER	BOOLEAN	The owner is marked as a scammer
DISPOSABLE	BOOLEAN	OLD, a few transactions in a short period of time (<i>tunable</i>)
MINER	BOOLEAN	Related to mining activities
BITCOINTALK_USER	STRING	The BitcoinTalk (forum) username of the owner
BITCOINOTC_USER	STRING	The Bitcoin-OTC (exchange) username of the owner

The Classifier: labels for addresses

Label	Type	Meaning
cluster_id	NUMBER	The ID of the cluster
first_seen	NUMBER	Timestamp of the first appearance of addresses in the cluster
last_seen	NUMBER	Timestamp of the last appearance of addresses in the cluster
recv	NUMBER	Total amount received by addresses in the cluster
sent	NUMBER	Total amount sent from addresses in the cluster
min_balance	NUMBER	Minimum balance of addresses in the cluster
max_balance	NUMBER	Maximum balance of addresses in the cluster
avg_balance	NUMBER	Average balance of addresses in the cluster
n_tx	NUMBER	Number of transactions in which the addresses in the cluster appear
mining	RATIO	Ratio of transactions coming from direct or pooled mining
gambling	RATIO	Ratio of transactions to/from gambling sites
exchanges	RATIO	Ratio of transactions to/from exchanges
wallets	RATIO	Ratio of transactions to/from web wallets
bitcointalk	RATIO	Ratio of transactions to/from known BitcoinTalk users
bitcoinotc	RATIO	Ratio of transactions to/from known Bitcoin-OTC users
freebies	RATIO	Ratio of transactions to/from faucets or other freebies
donations	RATIO	Ratio of transactions to/from known donation addresses
OTA	RATIO	Ratio of One-Time-Addresses in the cluster
OLD	RATIO	Ratio of OLD addresses in the cluster
NEW	RATIO	Ratio of NEW addresses in the cluster
EMPTY	RATIO	Ratio of EMPTY addresses in the cluster
EXHAUSTED	RATIO	Ratio of EXHAUSTED addresses in the cluster
RECENTLY_ACTIVE	RATIO	Ratio of RECENTLY_ACTIVE addresses in the cluster
ZOMBIE	RATIO	Ratio of ZOMBIE addresses in the cluster
SCAMMER	RATIO	Ratio of SCAMMER addresses in the cluster
DISPOSABLE	RATIO	Ratio of DISPOSABLE addresses in the cluster
MINER	RATIO	Ratio of MINER addresses in the cluster
BITCOINTALK_USER	STRING	BitcoinTalk usernames of owners of addresses in the cluster
BITCOINOTC_USER	STRING	Bitcoin-OTC usernames of owners of addresses in the cluster
SCAMMER	BOOLEAN	The owner is marked as a scammer

The Classifier: labels for users

Label	Value
cluster_id	246429
first_seen	Fri, 02 Nov 2012 21:57:06 GMT
last_seen	Mon, 07 Jan 2013 04:25:09 GMT
recv	42.07555841 BTC
sent	42.07555841 BTC
balance	0 BTC
n_tx	84
mining	0%
gambling	0%
exchanges	0%
wallets	0%
bitcointalk	1.4%
bitcoinotc	1.4%
freebies	0%
donations	0%
OTA	🚫
OLD	🚫
NEW	🚫
EMPTY	✅
EXHAUSTED	✅
RECENTLY_ACTIVE	🚫
ZOMBIE	🚫
SCAMMER	✅
DISPOSABLE	🚫
MINER	🚫
BITCOINTALK_USER	xisalty
BITCOINOTC_USER	xisalty-otc

Label	Value
cluster_id	246429
first_seen	Fri, 16 Sep 2011 21:38:13 GMT
last_seen	Mon, 07 Jan 2013 04:25:09 GMT
recv	84.93059065 BTC
sent	84.93053224 BTC
min_balance	0 BTC
max_balance	0.00004598 BTC
avg_balance	0.0000013275 BTC
n_tx	168
mining	0%
gambling	0%
exchanges	0%
wallets	0%
bitcointalk	2.3%
bitcoinotc	2.3%
freebies	0%
donations	0%
OTA	4.5%
OLD	2.3%
NEW	0%
EMPTY	100%
EXHAUSTED	95.5%
RECENTLY_ACTIVE	0%
ZOMBIE	2.3%
DISPOSABLE	0%
MINER	0%
BITCOINTALK_USER	xisalty
BITCOINOTC_USER	xisalty-otc
SCAMMER	✅

Zero-balance address, exhausted in **84 transactions**, belonging to user **xisalty** on BitcoinTalk forum and user **xisalty-otc** on Bitcoin-OTC.

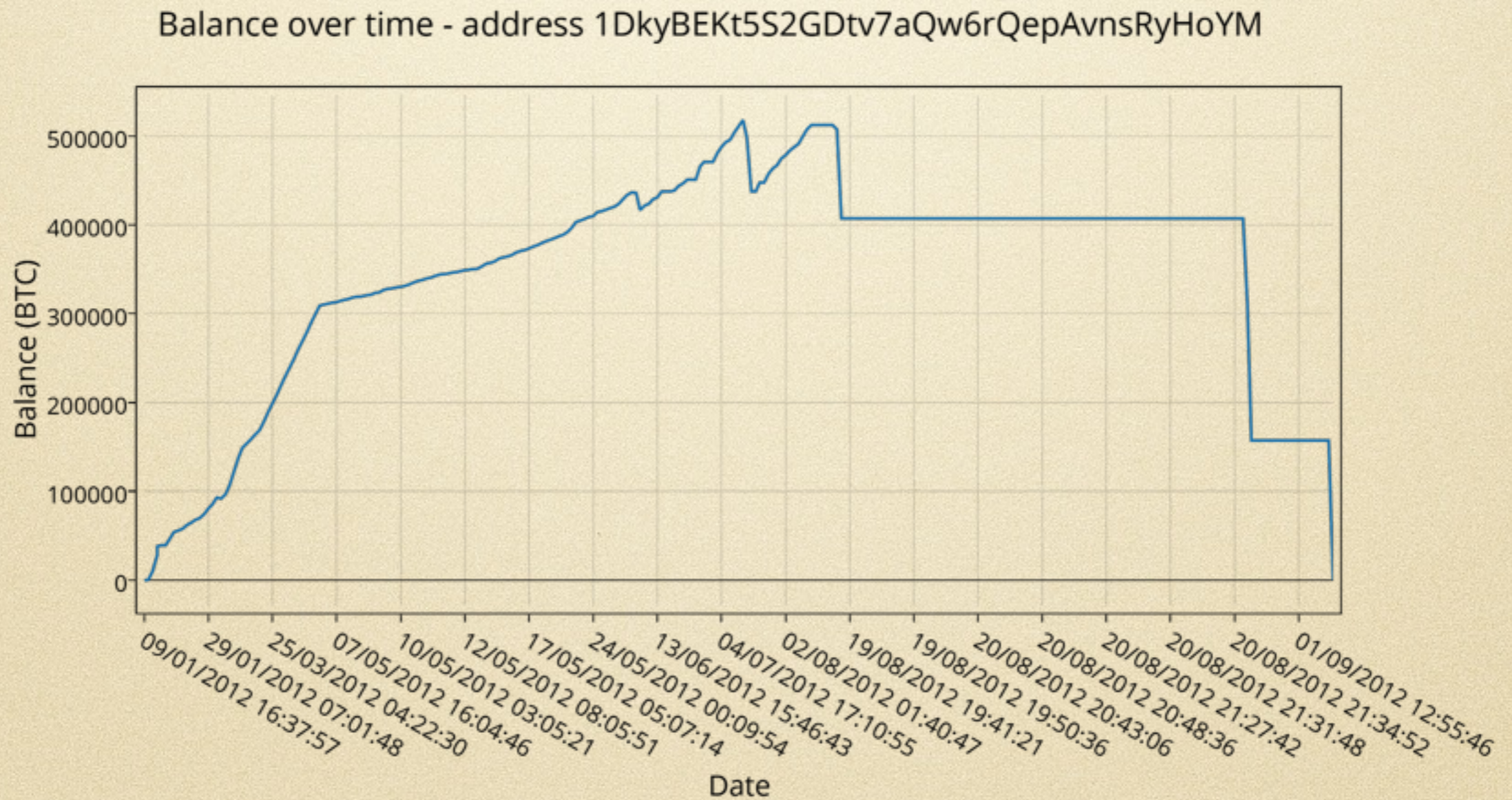
The owner is a **known scammer!**

Every address belonging to the user is **empty**, **4.5%** are **One-Time-Addresses**, **2.3%** are **zombies**.

A real-world case: investigating the Silk Road



We investigate one of the addresses that moved most funds during 2012.



A real-world case: investigating the Silk Road



- Sign up to the Silk Road
- **Deposit 0.001 BTC** to a one-time deposit address
- The coins are mixed: the deposit address is provably in the same wallet as **more than 25,000 other addresses**

A real-world case: investigating the Silk Road



- **Find a connection** between the addresses in the mixer and the large 1Dky... address
- The mixer is a cluster active since June 18, 2012 - more than 80,000 inputs / outputs
- **Follow the flow of coins!**

A real-world case: investigating the Silk Road



Transaction View information about a bitcoin transaction

fc688de6d6bad16a4305f9643a1aa5d2beca56c5d9eef9a9d5df5a05fc1b5f02

1AVMrqGmoJ7Jpjh7FdbHnDwK34VBxtBCcC (21.02949422 BTC - Output)
169WAuvSXLm8R9vwWPbkox16Lacj3MchJc (21.4995 BTC - Output)
1Q6nyjSQ79AAw67xAGHgXxXHRj9erLLqhD (0.001 BTC - Output)
1PhsnkafEiq6DAVZTW2SA4ZGv1BKTsxhw3 (11.98 BTC - Output)
1FySsTNrANq3a7BMBY1XXd2NF85bvjnFAa (0.00008 BTC - Output)
17ihRruptFG2i5sVj4yZg1SwGAuaYwxgvB (35.5 BTC - Output)



14e2mqhV8LdqmqAEW8EC19RTaKZQAxNLz1 - (Spent)
14J3Bm1r9bMhDGpezNybLfoZZZjMftW79k - (Spent)

0.01007422 BTC
90 BTC

90.01007422 BTC

12StkvcnJoob5AYdMYx98S17cy3LxjELP4 (23.3256016 BTC - Output)
13gB1VFgggK1NMT5tDtMzEwPP1rvJyBnPp (327 BTC - Output)
1AA5tGfkBtwucereXbT3WKRj471aYZUxKGG (13 BTC - Output)
14mmFby7pJroJ17f4tzo4irTFF2EaY8v42 (10 BTC - Output)
1JpDXgtStCvm1rjRke7Akrk4oLo9PpQUNb (18 BTC - Output)
1AVMrqGmoJ7Jpjh7FdbHnDwK34VBxtBCcC (31.5258512 BTC - Output)
1H8CiKo4jqatAnjxBBMCqqT9PsvK3qptEoD (11.8 BTC - Output)



1DHrFHDbiMfxxsK2KEKNnEBVeXDQtA5PjV - (Spent) 0.01000333 BTC
1DkyBEKt5S2GDtv7aQw6rQepAvnsRyHoYM - (Spent) 7,000 BTC

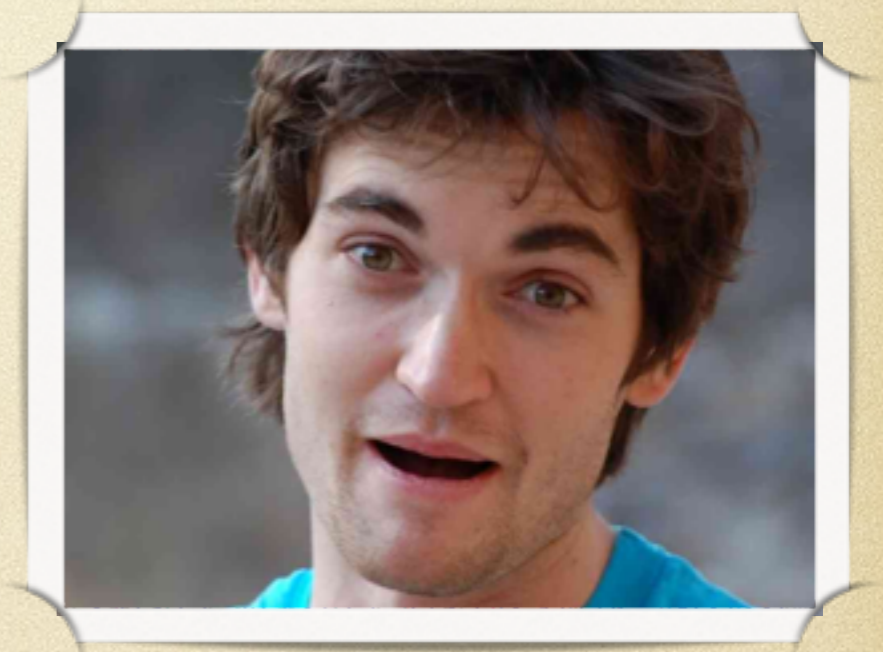
Multi-hop connection found: the 1Dky... address is related to the Silk Road.

FBI Silk Road takedown



- *Dread Pirate Roberts* = **Ross William Ulbricht**

- Charged on *Oct 1 2013* with:
 - *narcotics trafficking conspiracy*
 - *computer hacking conspiracy*
 - *money laundering conspiracy*



- Joint operation - **FBI, DEA, IRS** and **Homeland Security's** investigative unit.

FBI Silk Road takedown in numbers

- 26,000+ BTC seized (blockchain)
- still 600,000 BTC in encrypted wallet
- From *Feb 6, 2011* to *July 23, 2013*:
 - 9,519,664 BTC in 1,229,465 sales
 - 614,305 BTC to Ulbricht in commissions



How to get caught by the FBI



Use **altoid** as nickname on different forums to advertise the Silk Road. Then use it to hire developers using your rossulbricht@gmail.com email address.




Author Topic: IT pro needed for venture backed bitcoin startup (Read 9839 times)

altoid
Member
Activity: 48
Ignore

IT pro needed for venture backed bitcoin startup #1
October 11, 2011, 08:06:22 PM

Hello, sorry if there is another thread for this kind of post, but I couldn't find one. I'm looking for the best and brightest IT pro in the bitcoin community to be the lead developer in a venture backed bitcoin startup company. The ideal candidate would have at least several years of web application development experience, having built applications from the ground up. A solid understanding of oop and software architecture is a must. Experience in a start-up environment is a plus, or just being super hard working, self-motivated, and creative.

Compensation can be in the form of equity or a salary, or somewhere in-between. 

If interested, please send your answers to the following questions to [rossulbricht at gmail dot com](mailto:rossulbricht@gmail.com)

- 1) What are your qualifications for this position?
- 2) What interests you about bitcoin?

From there, we can talk about things like compensation and references and I can answer your questions as well. Thanks in advance to any interested parties. If anyone knows another good place to recruit, I am all ears.

[Report to moderator](#)

How to get caught by the FBI

Using **altoid**, post on BitcoinTalk a piece of code containing an address (1LDNLreKJ6GawBHPgB5yfVLBERi8g3SbQS)



Author Topic: help with Bitcoin development in php (variable parameters) (Read 3040 times)

altoid
Jr. Member
Activity: 48
Posts: 48

[help with Bitcoin development in php \(variable parameters\)](#)
April 25, 2011, 02:17:14 AM

Hi all, I have run into some trouble using the bitcoin api with php. When I issue a command like:

```
$bitcoin->sendfrom($userid, $receiving_address, $amount);
```

I get an error like:

```
fopen(http://...@localhost:8332/): failed to open stream: HTTP request failed! HTTP/1.1 500 Internal Server Error
```

But when I hard code in the parameters:

```
$bitcoin->sendfrom("1", "1LDNLreKJ6GawBHPgB5yfVLBERi8g3SbQS", 10);
```

it works fine.

I did notice that I had to put quotes around the variables in my parameters for other functions to work. For example:

```
$bitcoin->getnewaddress("$userid");
```

But every combination of quotes or no quotes produces the error in the sendfrom function.

Thanks in advance for any help you can give. Let me know if you need more info too.

Looking for the “lost” wallet

- > first input transaction of the address on the right
- > only input transaction of the address on the right
- > only significant input transaction of the address on the right
- > address on the left spent all its coins to address on the right exclusively

1LDNLreKJ6GawBHPgB5yFVLBERi8g3SbQS

->->

1BG9jDV3pA1MsJUnvRyWuA2b7PfGd4MZaw

5000 BTC 2011-04-30 18:32:55

->->

12h6TzwPNBvDnppbsqpyXwW4oo5UUKaKSa

2000 BTC 2011-05-07 14:12:51 in a multi-input TX for 9067.32 BTC

->->->

1EG9HJG9aGqzgGujfNQMiNbyqpKnFxafvE

9067.32 BTC 2011-06-19 23:04:29 in a multi-input TX for 37420.09314115 BTC

->->->

1AHki5AbZYiz4fHkGSTVKN3T1Tv5PwZpnh

37420.09314115 BTC 2011-06-19 23:29:01 in a multi-input TX for 37421.09314115 BTC

->->

15TEAwEMxVS3BK718HhwgJg7nxwyJ2ib9y

37421.09314115 BTC 2011-06-22 02:48:45

->->

1933phfhK3ZgFQNLGSDXvqCn32k2buXY8a

37421.09314115 BTC 2011-07-02 02:42:15 in a multi-input TX for 40954.56541907 BTC

Address 1933phfhK3ZgFQNLGSDXvqCn32k2buXY8a has a balance of 111,114+ BTC.

But wait, there's more!



In March of last year, a SR vendor called *FriendlyChemist* attempted to **extort** DPR via SR's private message system, providing proof that he had the **names and addresses of thousands of vendors.**

He demanded **\$500,000.**

But wait, there's more!



what do u . . . think will happen if thousands of usernames, ordr amounts, addresses get leaked? all those people will leave sr [Silk Road] and be scared to use it again. those vendors will all be busted and all there customers will be exposed too and never go back to sr.

But wait, there's more!



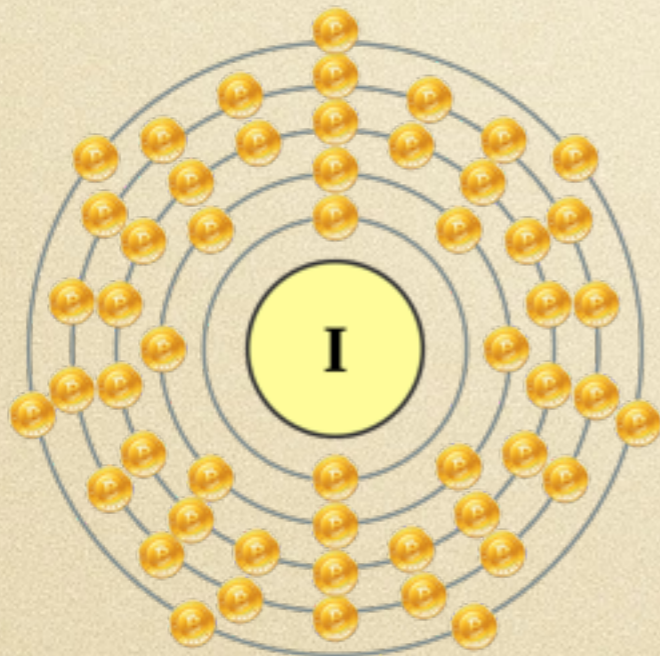
DPR solicited a SR user, *redandwhite* to "execute" FriendlyChemist, supplying him his full name and address. After having agreed on terms, DPR sent redandwhite \$150,000 (1,670BTC) to have FriendlyChemist **killed**.

Redandwhite later provided **photographic proof** of the alleged murder.

But wait, there's more!



We used BitIodine to spot the payment to the hitman.



Scamming pirates...



Investigators could not find any record of anybody in that region being killed around that date or matching that description.

This possibly implies that DPR was **scammed**.

Investigating cybercrime with BitIodine



The screenshot shows a ransomware payment window titled "CryptoLocker". The background is red. On the left, there is a blue shield icon with a white cross. Below it, text reads: "Private key will be destroyed on 10/13/2013 1:21 PM" and "Time left 71 : 33 : 17". The main content area is white and titled "Payment for private key". It contains a dropdown menu with "Bitcoin (most cheap option)" selected. Below the dropdown is the Bitcoin logo and the word "bitcoin". A paragraph explains that Bitcoin is a cryptocurrency based on an open-source cryptographic protocol. Below this, it states: "You have to send 2 BTC to Bitcoin address [redacted] and specify the Transaction ID on the next page, which will be verified and confirmed." There are two links: "Home Page" and "Getting started with Bitcoin". At the bottom, there are two blue buttons: "<< Back" and "Next >>".

CryptoLocker

Payment for private key

Choose a convenient payment method and click «Next»:

Bitcoin (most cheap option)



Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send **2 BTC** to Bitcoin address [redacted] and specify the Transaction ID on the next page, which will be verified and confirmed.

[Home Page](#)
[Getting started with Bitcoin](#)

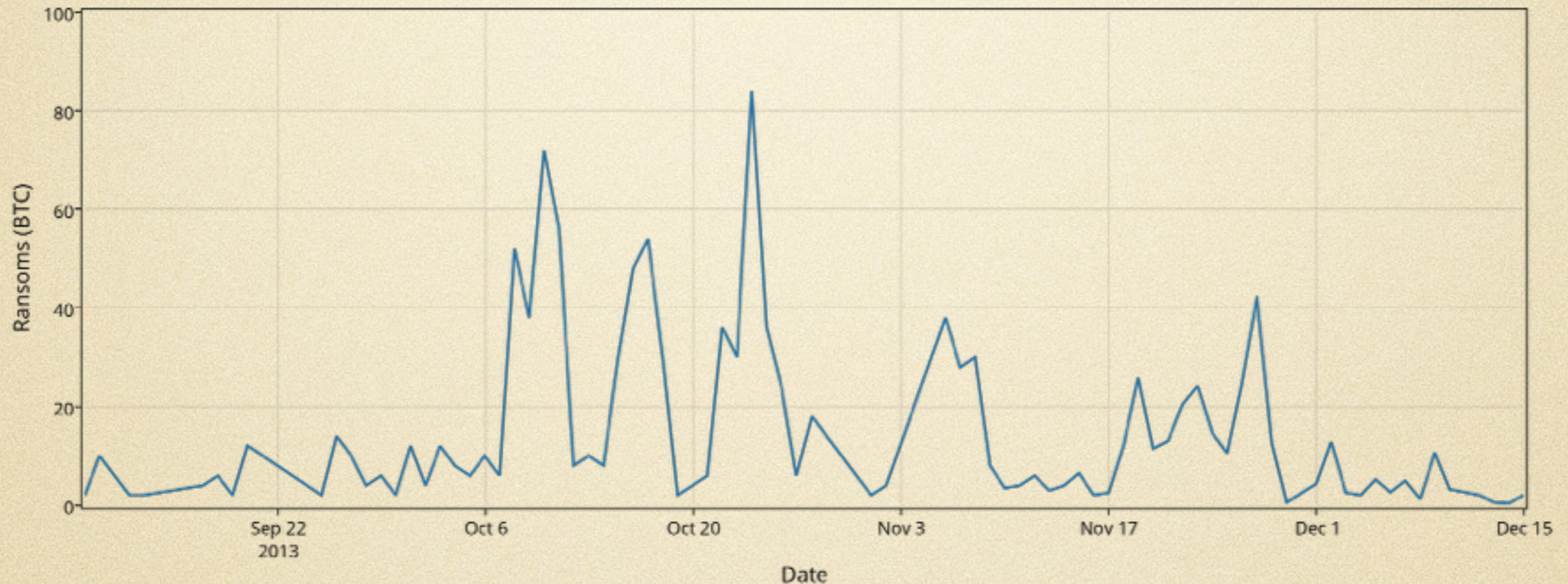
<< Back Next >>

CryptoLocker malware

- Hit the Internet around 5 PM UTC on **5 Sep 2013**
- **Encrypts** victim's documents with strong encryption and **demand**s a ransom in Bitcoin for decrypting them, with a **72h deadline**
- **Ransoms** 10 BTC ➡ 2 BTC ➡ 0.5 BTC ➡ 0.3 BTC

Investigating cybercrime with BitIodine

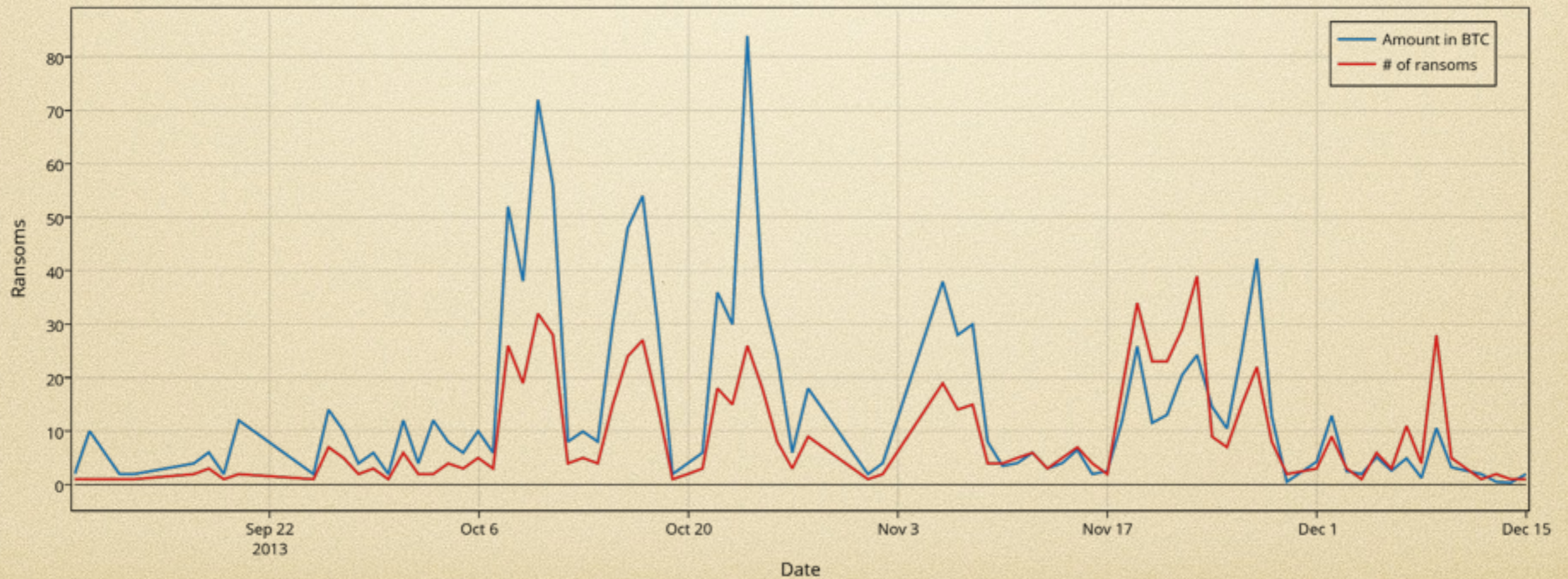
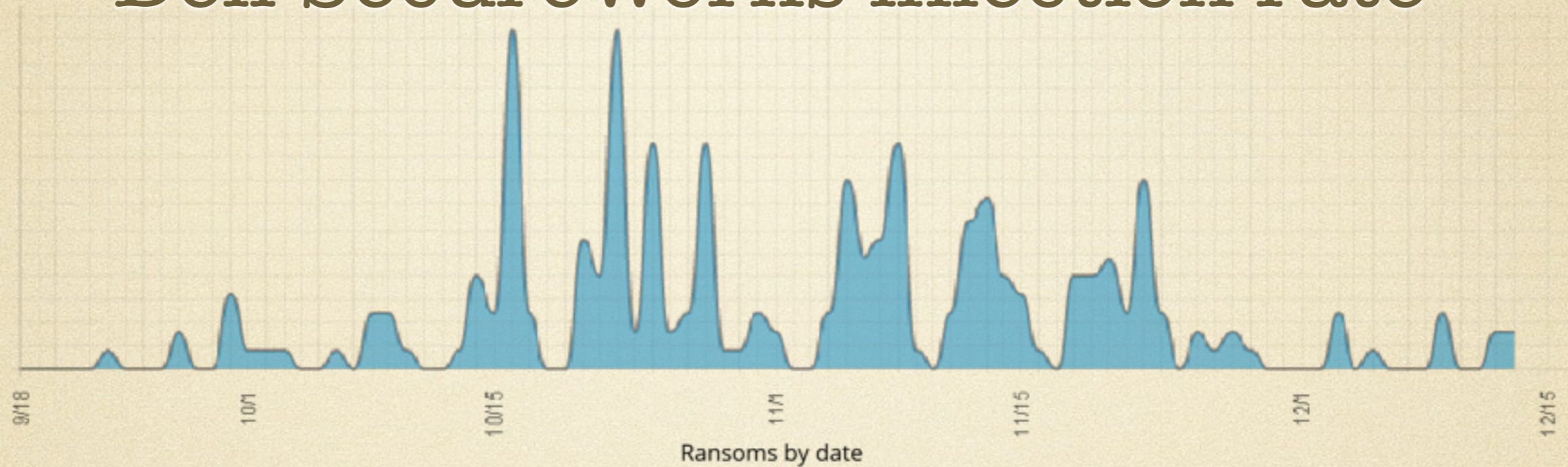
Amount of ransoms paid to CryptoLocker by date



In total, we identified **771** ransoms paid up to Dec 15, for **1226 BTC** (approximately **\$1.2M**).

BitIodine analysis of ransoms and Dell SecureWorks infection rate

Infections



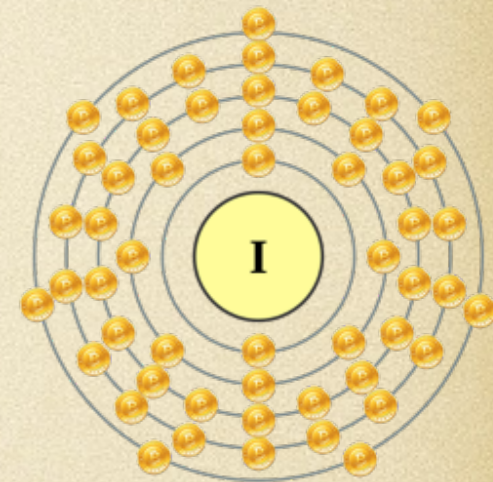
Investigating cybercrime with BitIodine

Estimate is **conservative**.

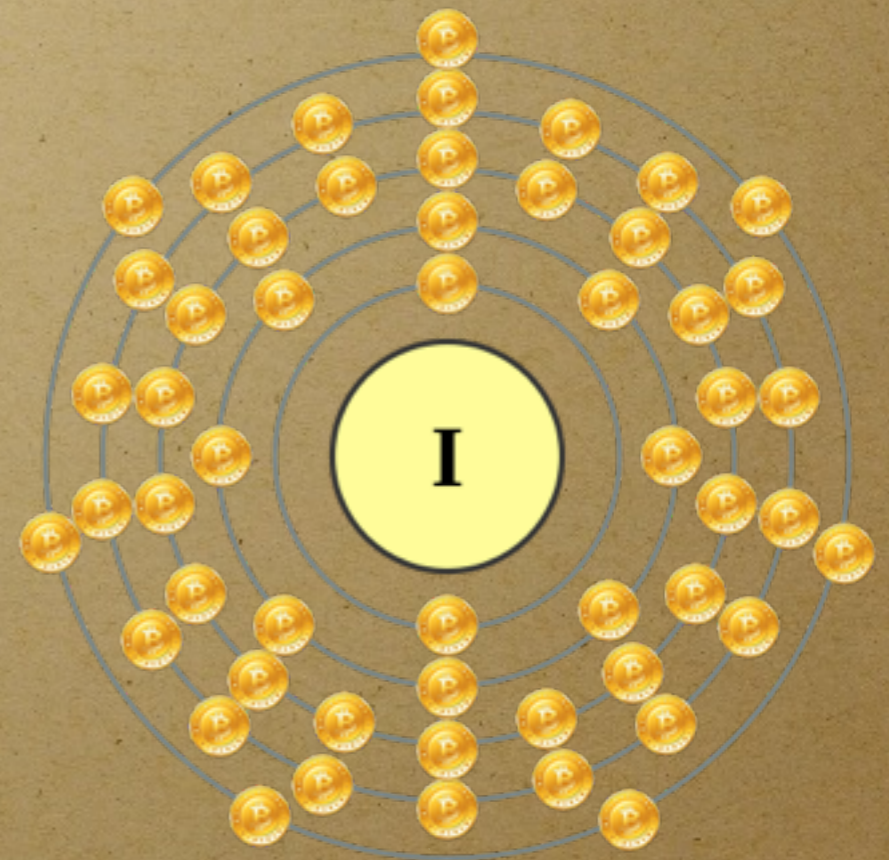
By running the *Classifier* on a **list of addresses of extorted people**, we automatically find out that, for example, BitcoinTalk user **CAESAR09** is among the **victims**.

Conclusions

- We presented BitIodine
 - improved heuristics for clustering
 - automatic labeling of clusters
- We test it on real-world use cases
 - we get insights on the Silk Road
 - we investigate activity related to **cybercrime** in a **novel way**
- Plans for the future
 - add **user-friendly front-end** to the framework
 - improve **performance**



Thank you.



Questions?

