A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn (UC San Diego)
Marjori Pomarole (UC San Diego)
Grant Jordan (UC San Diego)
Kirill Levchenko (UC San Diego)
Damon McCoy (George Mason University)
Geoff Voelker (UC San Diego)
Stefan Savage (UC San Diego)
What is Bitcoin?
What is Bitcoin?

The first successful, widely adopted form of e-cash
What is Bitcoin?

The first successful, widely adopted form of e-cash

Introduced in 2008 by “Satoshi Nakamoto”
What is Bitcoin?

The first successful, widely adopted form of e-cash

Introduced in 2008 by “Satoshi Nakamoto”

Potential for anonymity via use of pseudonyms
What is Bitcoin?

The first successful, widely adopted form of e-cash

Introduced in 2008 by “Satoshi Nakamoto”

Potential for anonymity via use of pseudonyms

Completely decentralized and unregulated*
What is Bitcoin?

The first successful, widely adopted form of e-cash

Introduced in 2008 by “Satoshi Nakamoto”

Potential for anonymity via use of pseudonyms

Completely decentralized and unregulated*

Every transaction is publicly visible
Why study Bitcoin? It’s fascinating!
Why study Bitcoin? It’s fascinating!

(U) Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity
Why study Bitcoin? It’s fascinating!

(U) Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity

Bitcoin buzz grows among venture investors, despite risks
Why study Bitcoin? It’s fascinating!

(U) Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity

Bitcoin buzz grows among venture investors, despite risks

Ponzi-Scheme Charge Is Good News for Bitcoin
Why study Bitcoin? It’s fascinating!

(U) Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity

Bitcoin buzz grows among venture investors, despite risks

Ponzi-Scheme Charge Is Good News for Bitcoin

MtGox Goes Down.. Bitcoin Trading Halted Till Later Today

Posted by Ron Finberg in Bitcoin

3 Comments
Why study Bitcoin? It’s fascinating!

(U) Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity

Bitcoin buzz grows among venture investors, despite risks

Ponzi-Scheme Charge Is Good News for Bitcoin

MtGox Goes Down.. Bitcoin Trading Halted Till Later Today
Posted by Ron Finberg in Bitcoin
3 Comments

CHART OF THE DAY: Bitcoin Is Going Totally Parabolic Again
MATTHEW BOESLER OCT. 23, 2013, 4:09 PM 2,347 2
Why study Bitcoin? It’s fascinating!
Why study Bitcoin? It’s fascinating!

current market capitalization of > $2B!
Our paper
Our paper

What are people using Bitcoin for?
Our paper

What are people using Bitcoin for?

How much anonymity does Bitcoin really provide?
Our paper

What are people using Bitcoin for?

How much anonymity does Bitcoin really provide?

Link pseudonyms to single user using two clustering heuristics
Our paper

What are people using Bitcoin for?

How much anonymity does Bitcoin really provide?

Link pseudonyms to single user using two clustering heuristics
Our paper

What are people using Bitcoin for?

How much anonymity does Bitcoin really provide?

Link pseudonyms to single user using two clustering heuristics

Name users via “re-identification attack” to learn real-world identity
Our paper

What are people using Bitcoin for?

How much anonymity does Bitcoin really provide?

Link pseudonyms to single user using two clustering heuristics

Name users via “re-identification attack” to learn real-world identity
Our paper

What are people using Bitcoin for?

How much anonymity does Bitcoin really provide?

Link pseudonyms to single user using two clustering heuristics

Name users via “re-identification attack” to learn real-world identity

Combine these techniques to de-anonymize flows of bitcoins
Outline
Outline

How does Bitcoin work?
Outline

How does Bitcoin work?  Analysis
Outline

- How does Bitcoin work?
- Analysis
- Results
- Conclusions
Outline

How does Bitcoin work?
- Public keys
- Transactions
- Blocks

Analysis

Results

Conclusions
Components of Bitcoin
Components of Bitcoin

The global transaction ledger is called the block chain
Components of Bitcoin

The global transaction ledger is called the block chain.

A block is a collection of transactions.
Components of Bitcoin

The global transaction ledger is called the **block chain**.

A **block** is a collection of transactions.

A **transaction** is a collection of ECDSA signatures specifying transfer of bitcoins from one pseudonym to another (or multiple).
Components of Bitcoin

The global transaction ledger is called the **block chain**.

A **block** is a collection of transactions.

A **transaction** is a collection of ECDSA signatures specifying transfer of bitcoins from one pseudonym to another (or multiple).

A **pseudonym** is the hash of an ECDSA public key; owner possesses the corresponding secret key.
How do bitcoins get spent?
How do bitcoins get spent?

Transactions form a chain
How do bitcoins get spent?

Transactions form a chain
How do bitcoins get spent?

Transactions form a chain

No Inputs (Newly Generated Coins) → 1D8JZmRQxme5ac42daiUSZWSDPQTbn8Pm - (Spent) 25.1834 BTC
13PEuLZWUSsLWtvQWQ26c1qQJYtsN2ahx8 (25.4158 BTC - Output) → 1D8JZmRQxme5ac42daiUSZWSDPQTbn8Pm (25.1834 BTC - Output)
19x4yJZxXFEuZN6BuQemZCq9bC3nUVGFHm - (Unspent) 0.5992 BTC
1422qjdwwv69rU4vuXFe59YktwqWkM6Kgsk - (Spent) 50 BTC
How do bitcoins get spent?

Transactions form a **chain**
How do bitcoins get spent?

Transactions form a chain

To **spend the bitcoins**, user signs the hash of the previous transaction and the public key of the intended recipient.
How do bitcoins get spent?

Transactions form a chain

To **spend the bitcoins**, user signs the hash of the previous transaction and the public key of the intended recipient

Each transaction must reference a previous transaction, so all bitcoins received **must be spent all at once**
Outline

How does Bitcoin work?

Analysis
Clustering addresses
Naming clusters

Results

Conclusions
How to identify users?

Users can use arbitrarily many public keys (pseudonyms); as a result the Bitcoin graph is complicated and has 12 million public keys.
How to identify users?

Users can use arbitrarily many public keys (pseudonyms); as a result the Bitcoin graph is complicated and has 12 million public keys.
How to identify users?

Users can use **arbitrarily many public keys** (pseudonyms); as a result the Bitcoin graph is complicated and has **12 million public keys**.
How to identify users?

Users can use arbitrarily many public keys (pseudonyms); as a result the Bitcoin graph is complicated and has 12 million public keys.

Collapse into a more manageable graph of clusters of public keys representing distinct entities.
How to identify users?

Users can use arbitrarily many public keys (pseudonyms); as a result the Bitcoin graph is complicated and has 12 million public keys.

Collapse into a more manageable graph of clusters of public keys representing distinct entities.
How to identify users?

Users can use arbitrarily many public keys (pseudonyms); as a result the Bitcoin graph is complicated and has 12 million public keys.

Collapse into a more manageable graph of clusters of public keys representing distinct entities.

Collect ground truth data by participating in transactions.
Clustering by inputs

<table>
<thead>
<tr>
<th>Transaction Hash</th>
<th>Value (BTC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>8b6008b2e369499c5c51058f5f09e549c160a84682c00cb97df2a2b4881e9cc27</td>
<td>30.28851 BTC</td>
</tr>
<tr>
<td>142Z7VauMvdSV5DADb62DsJ7wvW9ccq18t</td>
<td>30.28851 BTC</td>
</tr>
<tr>
<td>16H9oN1JFXSHEv16X8PLEs77MMF3EKqEIH</td>
<td>30.28851 BTC</td>
</tr>
<tr>
<td>17RHwSeN5iKy8gGwTHCH8j4mZH3eqQNbrav</td>
<td>80.58936 BTC</td>
</tr>
<tr>
<td>13b78oU4OdI4dQw87bvUMUZ1XpnZqwNQ1</td>
<td>12.9148 BTC</td>
</tr>
<tr>
<td>16Bz7E5PpF9P8ULmmMcbdag3mZzETGwYN</td>
<td>29.55 BTC</td>
</tr>
<tr>
<td>1Cus inkMvW53WtupuspCMDyigZ2s13zv</td>
<td>30.28851 BTC</td>
</tr>
<tr>
<td>1PVA5YNc2mWYtssfsBTBPMWX8CdKuM7B</td>
<td>30.28851 BTC</td>
</tr>
<tr>
<td>1Gg2D33ySPhdnSElBnmze1QsmycSdeGvkX</td>
<td>30.28851 BTC</td>
</tr>
<tr>
<td>1FdPwjg7XJfrEqdOnduus2KS1uuDAGCI</td>
<td>30.28851 BTC</td>
</tr>
<tr>
<td>178AKou6Q2741uPqt9FGj826ZUK18f3yDx</td>
<td>29.36578 BTC</td>
</tr>
<tr>
<td>1LZe2eSEKr6ikijI8k8YNSh1amR2czmww</td>
<td>30 BTC</td>
</tr>
<tr>
<td>1bah8vzFqtynCtip57Y5btkXwS6t7Bd3ic</td>
<td>29.84 BTC</td>
</tr>
<tr>
<td>1Dr92DXHrPYNV7EMrD0awDedWdk43Jikk</td>
<td>28.83951 BTC</td>
</tr>
<tr>
<td>1hV4C4vQwvJUjXWHBkIGKMkRKe7gv</td>
<td>30.13 BTC</td>
</tr>
<tr>
<td>14kSwoX2cPkwRtkW5TkTwFgtraYpYcKcW</td>
<td>99.45 BTC</td>
</tr>
<tr>
<td>1AkMojTE1UXUs3fS8N1LCzvtBx54wyoOn</td>
<td>141.9995 BTC</td>
</tr>
<tr>
<td>1KRMIP4uLy2hm86MRQRQv4ghkQthVK6BH6</td>
<td>29.6 BTC</td>
</tr>
</tbody>
</table>

Cluster diagram showing transaction connections.
Heuristic #1: the same user controls these addresses
Heuristic 1: enough?
Heuristic 1: enough?

This works because sender must know **secret key** for each input.
Heuristic 1: enough?

This works because sender must know secret key for each input.

This is established: has been used before [RH13, RS13, A+13] and even acknowledged by Satoshi himself.
Heuristic 1: enough?

This works because sender must know **secret key** for each input.

This is **established**: has been used before [RH13, RS13, A+13] and even acknowledged by Satoshi himself.

Already yields a fairly **robust graph**: 5.5 million distinct clusters.
Heuristic 1: enough?

This works because sender must know secret key for each input.

This is established: has been used before [RH13, RS13, A+13] and even acknowledged by Satoshi himself.

Already yields a fairly robust graph: 5.5 million distinct clusters.

Our goal is to track flows of bitcoins.
Heuristic 1: enough?

This works because sender must know secret key for each input.

This is established: has been used before [RH13, RS13, A+13] and even acknowledged by Satoshi himself.

Already yields a fairly robust graph: 5.5 million distinct clusters.

Our goal is to track flows of bitcoins.

Lots of flow remains in these clusters because of change addresses.
Change addresses

No Inputs (Newly Generated Coins)

13PEulZWUSsLWtvWQ26c1qQJYtsN2ahx8 (25.4158 BTC - Output)
1D8JZmRQxme5iac42daiUSZWDQbTbn8Pm (25.1834 BTC - Output)

1D8JZmRQxme5iac42daiUSZWDQbTbn8Pm - (Spent) 25.1834 BTC
19x4yJZxXFeuZNBuQemZCq9bCb3nUVGFHm - (Unspent) 0.5992 BTC
1422qjdvv69rU4vuXFe59YktwqWkM6Kgsk - (Spent) 50 BTC
Change addresses

Each transaction must reference a previous transaction, so all bitcoins received **must be spent all at once**
Change addresses

Each transaction must reference a previous transaction, so all bitcoins received must be spent all at once

Change address: used to collect excess bitcoins
Each transaction must reference a previous transaction, so all bitcoins received must be spent all at once.

**Change address**: used to collect excess bitcoins.

In the standard client, change addresses are used at most twice: to receive and to spend.
Clustering by change
Clustering by change
Heuristic #2: the same user also controls this address
Heuristic 2
Heuristic 2

To identify **change addresses**, look for “**one-time**” output address

```
  pk
```

Cluster
To identify change addresses, look for “one-time” output address

If there is exactly one such address, label it the change address
Heuristic 2

To identify change addresses, look for “one-time” output address

If there is exactly one such address, label it the change address

This isn’t conservative enough!
Heuristics 2

To identify change addresses, look for “one-time” output address

If there is exactly one such address, label it the change address

This isn’t conservative enough!

• Wait a week before identifying address
Heuristic 2

To identify change addresses, look for “one-time” output address

If there is exactly one such address, label it the change address

This isn’t conservative enough!

• Wait a week before identifying address

• Ignore “self-change” addresses
To identify change addresses, look for “one-time” output address

If there is exactly one such address, label it the change address

This isn’t conservative enough!

- Wait a week before identifying address
- Ignore “self-change” addresses
- Manually inspect some remaining addresses
Data collection
Data collection

Engaged in transactions with:
Data collection

Engaged in transactions with:

- Exchanges
Engaged in transactions with:

- Exchanges
- Vendors
Data collection

Engaged in transactions with:

- Exchanges
- Mining pools
- Vendors
Data collection

Engaged in transactions with:

- Exchanges
- Mining pools
- Vendors
- Gambling sites
Data collection

Engaged in transactions with:

- Exchanges
- Mining pools
- Wallet services
- Vendors
- Gambling sites
Data collection

Engaged in transactions with:

- Exchanges
- Mining pools
- Wallet services
- Vendors
- Gambling sites
- Mix services
Data collection

Engaged in transactions with:

- Exchanges
- Mining pools
- Wallet services
- Vendors
- Gambling sites
- Mix services

Scraped published tags
Engaged in transactions with:

- Exchanges
- Mining pools
- Wallet services
- Vendors
- Gambling sites
- Mix services

Scraped published tags

Found addresses discussed on forums
Exchanges

- Bitcoin-24x
- Bitcoin-Central
- bitcoin.de
- Bitcurex
- bitfloor
- BitMarket.eu
- BITME
- BITSTAMP
- Bitcoin China
- BTC e
- Camp BX
- VirtEx
- iCBIT
- mercadobitcoin
- MT.GOX
- THE ROCK
- Transact
- aurum
- BitInstant
- BITCOIN NORDIC
- btcQuick
- FastCash4Bitcoins
- LILION TRANSFER
- Nanaimo Gold
- OKPAY
Vendors
## Published tags

<table>
<thead>
<tr>
<th>Address</th>
<th>Sender</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>1LDCRDhNBiTaurUmJKqRef3cGpWLWfEpFk</td>
<td>BitAurum.eu</td>
<td><a href="https://www.bitaurum.eu">https://www.bitaurum.eu</a></td>
</tr>
<tr>
<td>1NmduGNyC5XEjoysbuioodCN3jR3yf64xM</td>
<td>Electrum</td>
<td><a href="http://electrum.ectds.org/community.html">http://electrum.ectds.org/community.html</a></td>
</tr>
<tr>
<td>1BTC24yVKQdQNAa4vX71xLUC5A8Za7Rr71</td>
<td>Bitcoin-24.com</td>
<td><a href="https://bitcoin-24.com">https://bitcoin-24.com</a></td>
</tr>
<tr>
<td>14FHqYSgAi39CEJksUJJJsK8JzJzyqFpLVk</td>
<td>xkcd</td>
<td><a href="http://xkcd.com/bitcoin/">http://xkcd.com/bitcoin/</a></td>
</tr>
<tr>
<td>16xTfttqg6DbvkAGpPvWWpEHEC4e1fCG7G</td>
<td>Genesis2church.org</td>
<td><a href="http://genesis2church.org/donate-with-bitcoin.html">http://genesis2church.org/donate-with-bitcoin.html</a></td>
</tr>
<tr>
<td>13RcqwggWi9WwcPCZ5BeScxZLWPtt3NVzf</td>
<td>Skeptinerd</td>
<td><a href="http://www.skeptinerd.com/donate-with-bitcoin/">http://www.skeptinerd.com/donate-with-bitcoin/</a></td>
</tr>
<tr>
<td>1Kj7V3CYk4TzmE5cgYR7UVbejgFVRbqSwu</td>
<td>WeUseCoins</td>
<td><a href="http://www.weusecoins.com/about.php">http://www.weusecoins.com/about.php</a></td>
</tr>
<tr>
<td>1HCMw4nJMT9C6aXaE4EFUb4UbYlg9qpGqw</td>
<td>A Lightning War for Liberty</td>
<td><a href="http://libertyblitzkrieg.com/donate-via-bitcoin-2/">http://libertyblitzkrieg.com/donate-via-bitcoin-2/</a></td>
</tr>
</tbody>
</table>
server was hacked brutally. this time - not by stupid site bug, but something else. still looking.

it would be fine, since I never keep all coins on server, but hacker was able somehow to hack into my laptop and desktop through vpn i have between my home and server and wiped all wallets i had in there.. have no clue how it was done yet. all machines uses different passwords and different ubuntu distro versions.

still investigating. all money went there - http://blockexplorer.com/address/1L4kz6BA8mzi8KLV9VQ2pYcW8QQFVihWLg almost in the same time.

this was quite sophisticated attack i must say..
server was hacked brutally. this time - not by stupid site bug, but something else. still looking.

it would be fine, since I never keep all coins on server, but hacker was able somehow to hack into my laptop and desktop through vpn i have between my home and server and wiped all wallets i had in there.. have no clue how it was done yet. all machines uses different passwords and different ubuntu distro versions.

still investigating. all money went there - http://blockexplorer.com/address/1L4kz6BA8mzl8KLV9VQ2pYcW8QQFVihWLg almost in the same time.

this was quite sophisticated attack i must say..
Trolling Bitcoin forums

Re: betco.in's a ghost town now?
April 13, 2012, 12:19:17 AM #10

server was hacked brutally. this time - not by stupid site bug, but something else. still looking.

it would be fine, since I never keep all coins on server, but hacker was able somehow to hack into my laptop and desktop through vpn i have between my home and server and wiped all wallets i had in there.. have no clue how it was done yet. all machines uses different passwords and different ubuntu distro versions.

still investigating. all money went there - http://blockexplorer.com/address/1L4kz6BA8mzi8KLV9VQ2pYcW8QQFVihWLg almost in the same time.

this was quite sophisticated attack i must say..

bf70acz1d2b702d9e0e14f3efb93a0cf2ff5e6a5a425cfe4249f166ede71b3ff14
1FE71fnpTXYbVzXnRXZKxpmV8KBv5ZCJst (10 BTC - Output)
1FE71fnpTXYbVzXnRXZKxpmV8KBv5ZCJst (4.4257016 BTC - Output)
1FE71fnpTXYbVzXnRXZKxpmV8KBv5ZCJst (2 BTC - Output)
1Mu4topyQ6hpyaqQ6x4hCCs4bg9p9Wz2 (0.80318 BTC - Output)

1Hvi6re6zDr55v9Sk2mmL9u7svEHiBl4
1L4kz6BA8mzi8KLV9VQ2pYoW8QQFVihWLg
0.22895016 BTC
17 BTC

40fd8f6b2f2222f2b2871a3a8245132ed1eadaf9f6aee8d46ebe74b29c64fd82a7
1CcRihgr3iHVkwBiJ338jBwglLvmBUWRzqEuE (121.258 BTC - Output)
1Lgnzb1p9YE3uKwGpspMQZ1NcAD1EnmzSH (43.78 BTC - Output)

1KPGDc6oHpvW0SyssxqmRgwU7sy4y2y
1L4kz6BA8mzi8KLV9VQ2pYoW8QQFVihWLg
0.038 BTC
165 BTC

(Fee: 0 BTC - Size: 798 bytes) 2012-04-11 11:14:03

(Fee: 0 BTC - Size: 437 bytes) 2012-04-11 10:51:01
Putting it all together
Putting it all together
Putting it all together
Putting it all together
Putting it all together

Transact

Cluster

us -> them
Putting it all together
Putting it all together

Transact

us -> them

Cluster

Bootstrap
Putting it all together

Interacted with **31** MtGox addresses, tagged **518,723**!

Participated in **344** transactions and tagged **1.3M** public keys
Outline

How does Bitcoin work?  

Results  
Overall statistics  
Tracking cluster activity

Analysis

Conclusions

22
Clustering using our heuristics
Clustering using our heuristics

bicycle wheel with gambling at center
Clustering using our heuristics

bicycle wheel with gambling at center

strongly connected component with most of our named users
Following bitcoins
Following bitcoins

Can see when bitcoins meaningfully **cross cluster boundaries**
Following bitcoins

Can see when bitcoins meaningfully cross cluster boundaries
Following bitcoins

Can see when bitcoins meaningfully cross cluster boundaries

Allows us to systematically follow “peeling chains”
Following bitcoins

Can see when bitcoins meaningfully cross cluster boundaries

Allows us to systematically follow "peeling chains"
Following bitcoins

Can see when bitcoins meaningfully **cross cluster boundaries**

Allows us to systematically follow “**peeling chains**”
Following bitcoins

Can see when bitcoins meaningfully **cross cluster boundaries**

Allows us to systematically follow "peeling chains"

change address
Following bitcoins

Can see when bitcoins meaningfully cross cluster boundaries

Allows us to systematically follow “peeling chains”
Following bitcoins

Can see when bitcoins meaningfully cross cluster boundaries

Allows us to systematically follow “peeling chains”
Following bitcoins

Can see when bitcoins meaningfully **cross cluster boundaries**

Allows us to systematically follow “**peeling chains**”
Following bitcoins

Can see when bitcoins meaningfully cross cluster boundaries

Allows us to systematically follow “peeling chains”

Identifying recipients potentially de-anonymizes user
Tracking illicitly-obtained bitcoins

By following peeling chains, we tracked money from known thefts and from one infamous address associated with Silk Road
Tracking illicitly-obtained bitcoins

By following peeling chains, we tracked money from known thefts and from one infamous address associated with Silk Road.
Tracking illicitly-obtained bitcoins

By following peeling chains, we tracked money from known thefts and from one infamous address associated with Silk Road.
Tracking illicitly-obtained bitcoins

By following peeling chains, we tracked money from known thefts and from one infamous address associated with Silk Road.

5% of all generated bitcoins!

<table>
<thead>
<tr>
<th>Date</th>
<th>Balance (in thousands)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010-12-29</td>
<td>-</td>
</tr>
<tr>
<td>2011-08-05</td>
<td>-</td>
</tr>
<tr>
<td>2012-03-12</td>
<td>-</td>
</tr>
<tr>
<td>2012-10-18</td>
<td>-</td>
</tr>
</tbody>
</table>

- 1DkyBEKt
- vendors
- silk road
Tracking illicitly-obtained bitcoins

By following peeling chains, we tracked money from known thefts and from one infamous address associated with Silk Road.
Tracking illicitly-obtained bitcoins

By following peeling chains, we tracked money from known thefts and from one infamous address associated with Silk Road.

Dissipated bitcoins did not flow at scale to any known services.
Tracking illicitly-obtained bitcoins
Tracking illicitly-obtained bitcoins

By following peeling chains, we tracked money from known thefts and from one infamous address associated with Silk Road.
Tracking illicitly-obtained bitcoins

By following peeling chains, we tracked money from known thefts and from one infamous address associated with Silk Road.

But we saw peels to known exchanges.

<table>
<thead>
<tr>
<th>Service</th>
<th>First Peels</th>
<th>First BTC</th>
<th>Second Peels</th>
<th>Second BTC</th>
<th>Third Peels</th>
<th>Third BTC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bitcoin-24</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>124</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bitcoin Central</td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bitcoin.de</td>
<td>1</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bitmarket</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bitstamp</td>
<td>5</td>
<td>97</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BTC-e</td>
<td>1</td>
<td>250</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CA VirtEx</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>10</td>
<td>3</td>
<td>22</td>
</tr>
<tr>
<td>Mercado Bitcoin</td>
<td>1</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mt. Gox</td>
<td>11</td>
<td>492</td>
<td>14</td>
<td>70</td>
<td>5</td>
<td>35</td>
</tr>
<tr>
<td>OKPay</td>
<td>2</td>
<td>151</td>
<td></td>
<td></td>
<td>1</td>
<td>125</td>
</tr>
</tbody>
</table>
Tracking illicitly-obtained bitcoins
Tracking illicitly-obtained bitcoins

By following peeling chains, we tracked money from known thefts and from one infamous address associated with Silk Road.

Again, saw many peels to known exchanges.

<table>
<thead>
<tr>
<th>Theft</th>
<th>BTC</th>
<th>Date</th>
<th>Movement</th>
<th>Exchanges?</th>
</tr>
</thead>
<tbody>
<tr>
<td>MyBitcoin</td>
<td>4019</td>
<td>Jun 2011</td>
<td>A/P/S</td>
<td>Yes</td>
</tr>
<tr>
<td>Linode</td>
<td>46,648</td>
<td>Mar 2012</td>
<td>A/P/F</td>
<td>Yes</td>
</tr>
<tr>
<td>Betcoin</td>
<td>3171</td>
<td>Mar 2012</td>
<td>F/A/P</td>
<td>Yes</td>
</tr>
<tr>
<td>Bitcoinica</td>
<td>18,547</td>
<td>May 2012</td>
<td>P/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Bitcoinica</td>
<td>40,000</td>
<td>Jul 2012</td>
<td>P/A/S</td>
<td>Yes</td>
</tr>
<tr>
<td>Bitfloor</td>
<td>24,078</td>
<td>Sep 2012</td>
<td>P/A/P</td>
<td>Yes</td>
</tr>
<tr>
<td>Trojan</td>
<td>3257</td>
<td>Oct 2012</td>
<td>F/A</td>
<td>No</td>
</tr>
</tbody>
</table>
Tracking illicitly-obtained bitcoins

By following peeling chains, we tracked money from known thefts and from one infamous address associated with Silk Road

Again, saw many peels to known exchanges

<table>
<thead>
<tr>
<th>Theft</th>
<th>BTC</th>
<th>Date</th>
<th>Movement</th>
<th>Exchanges?</th>
</tr>
</thead>
<tbody>
<tr>
<td>MyBitcoin</td>
<td>4019</td>
<td>Jun 2011</td>
<td>A/P/S</td>
<td>Yes</td>
</tr>
<tr>
<td>Linode</td>
<td>46,648</td>
<td>Mar 2012</td>
<td>A/P/F</td>
<td>Yes</td>
</tr>
<tr>
<td>Betcoin</td>
<td>3171</td>
<td>Mar 2012</td>
<td>F/A/P</td>
<td>Yes</td>
</tr>
<tr>
<td>Bitcoinica</td>
<td>18,547</td>
<td>May 2012</td>
<td>P/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Bitcoinica</td>
<td>40,000</td>
<td>Jul 2012</td>
<td>P/A/S</td>
<td>Yes</td>
</tr>
<tr>
<td>Bitfloor</td>
<td>24,078</td>
<td>Sep 2012</td>
<td>P/A/P</td>
<td>Yes</td>
</tr>
<tr>
<td>Trojan</td>
<td>3257</td>
<td>Oct 2012</td>
<td>F/A</td>
<td>No</td>
</tr>
</tbody>
</table>

2857 BTC (87%) hadn’t moved
Tracking illicitly-obtained bitcoins

By following peeling chains, we tracked money from known thefts and from one infamous address associated with Silk Road.

Again, saw many peels to known exchanges.

<table>
<thead>
<tr>
<th>Theft</th>
<th>BTC</th>
<th>Date</th>
<th>Movement</th>
<th>Exchanges?</th>
</tr>
</thead>
<tbody>
<tr>
<td>MyBitcoin</td>
<td>4019</td>
<td>Jun 2011</td>
<td>A/P/S</td>
<td>Yes</td>
</tr>
<tr>
<td>Linode</td>
<td>46,648</td>
<td>Mar 2012</td>
<td>A/P/F</td>
<td>Yes</td>
</tr>
<tr>
<td>Betcoin</td>
<td>3171</td>
<td>Mar 2012</td>
<td>F/A/P</td>
<td>Yes</td>
</tr>
<tr>
<td>Bitcoinica</td>
<td>18,547</td>
<td>May 2012</td>
<td>P/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Bitcoinica</td>
<td>40,000</td>
<td>Jul 2012</td>
<td>P/A/S</td>
<td>Yes</td>
</tr>
<tr>
<td>Bitfloor</td>
<td>24,078</td>
<td>Sep 2012</td>
<td>P/A/P</td>
<td>Yes</td>
</tr>
<tr>
<td>Trojan</td>
<td>3257</td>
<td>Oct 2012</td>
<td>F/A</td>
<td>No</td>
</tr>
</tbody>
</table>

2857 BTC (87%) hadn’t moved.

Exchanges know the real-world identity of the account owner.
Tracking illicitly-obtained bitcoins

By following peeling chains, we tracked money from known thefts and from one infamous address associated with Silk Road. Again, saw many peels to known exchanges.

<table>
<thead>
<tr>
<th>Theft</th>
<th>BTC</th>
<th>Date</th>
<th>Movement</th>
<th>Exchanges?</th>
</tr>
</thead>
<tbody>
<tr>
<td>MyBitcoin</td>
<td>4019</td>
<td>Jun 2011</td>
<td>A/P/S</td>
<td>Yes</td>
</tr>
<tr>
<td>Linode</td>
<td>46,648</td>
<td>Mar 2012</td>
<td>A/P/F</td>
<td>Yes</td>
</tr>
<tr>
<td>Betcoin</td>
<td>3171</td>
<td>Mar 2012</td>
<td>F/A/P</td>
<td>Yes</td>
</tr>
<tr>
<td>Bitcoinica</td>
<td>18,547</td>
<td>May 2012</td>
<td>P/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Bitcoinica</td>
<td>40,000</td>
<td>Jul 2012</td>
<td>P/A/S</td>
<td>Yes</td>
</tr>
<tr>
<td>Bitfloor</td>
<td>24,078</td>
<td>Sep 2012</td>
<td>P/A/P</td>
<td>Yes</td>
</tr>
<tr>
<td>Trojan</td>
<td>3257</td>
<td>Oct 2012</td>
<td>F/A</td>
<td>No</td>
</tr>
</tbody>
</table>

2857 BTC (87%) hadn’t moved

Exchanges know the real-world identity of the account owner.

Hypothesis: if you subpoena the exchange, you can identify the thief.
Tracking bitcoins in the real world
Tracking bitcoins in the real world

Contacted by Andy Greenberg of Forbes to test hypothesis
Tracking bitcoins in the real world

Contacted by Andy Greenberg of Forbes to test hypothesis

Got Coinbase addresses; asked to identify drug purchases
Tracking bitcoins in the real world

Contacted by Andy Greenberg of Forbes to test hypothesis

Got Coinbase addresses; asked to identify drug purchases
Tracking bitcoins in the real world

Contacted by Andy Greenberg of Forbes to test hypothesis

Got Coinbase addresses; asked to **identify drug purchases**
How does Bitcoin work?

Analysis

Results

Conclusions
Conclusions

What are people using Bitcoin for?

How much anonymity does Bitcoin really provide?
Conclusions

What are people using Bitcoin for?

How much anonymity does Bitcoin really provide?

Bitcoin is used mostly for gambling, currency exchange, to a (much) lesser extent buying drugs.
Conclusions

What are people using Bitcoin for?

How much anonymity does Bitcoin really provide?

Bitcoin is used mostly for gambling, currency exchange, to a (much) lesser extent buying drugs

Our analysis provides a real-world way to track flows of bitcoins
Conclusions

What are people using Bitcoin for?

How much anonymity does Bitcoin really provide?

Bitcoin is used mostly for gambling, currency exchange, to a (much) lesser extent buying drugs.

Our analysis provides a real-world way to track flows of bitcoins.

 Seems hard to launder significant quantities of money.
Conclusions

What are people using Bitcoin for?

How much anonymity does Bitcoin really provide?

Bitcoin is used mostly for gambling, currency exchange, to a (much) lesser extent buying drugs.

Our analysis provides a real-world way to track flows of bitcoins.

Seems hard to launder significant quantities of money.

Thanks! Any questions?