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

Apr 11 2013

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

Apr 11 2013

MtGox Goes Down.. Bitcoin Trading Halted Till Later Today

Posted by **Ron Finberg** in **Bitcoin**

3 Comments

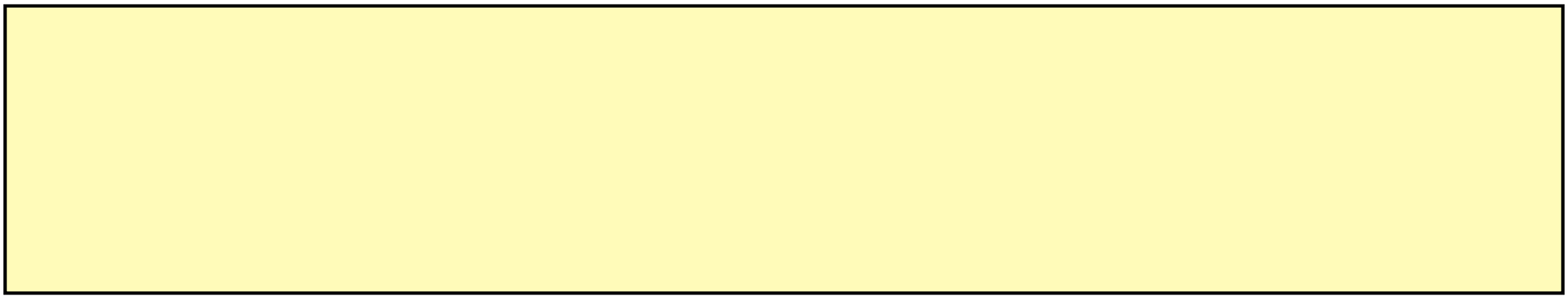
CHART OF THE DAY: Bitcoin Is Going Totally Parabolic Again

MATTHEW BOESLER | OCT. 23, 2013, 4:09 PM | 2,347 | 2

Why study Bitcoin? It's fascinating!

Why study Bitcoin? It's fascinating!

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?

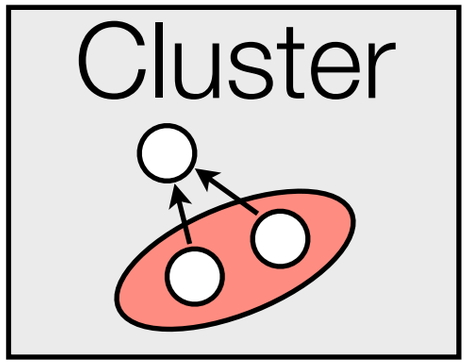
Link pseudonyms to single user using two clustering heuristics

Our paper

What are people using Bitcoin for?

How much anonymity does Bitcoin really provide?

Link pseudonyms to single user using two clustering heuristics

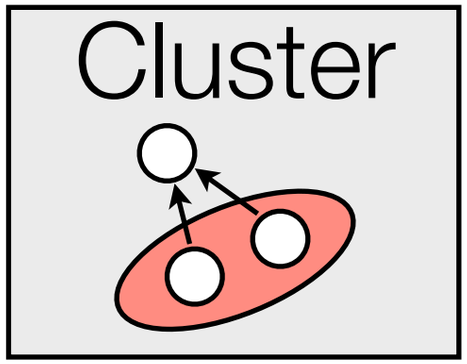


Our paper

What are people using Bitcoin for?

How much anonymity does Bitcoin really provide?

Link pseudonyms to single user using two clustering heuristics



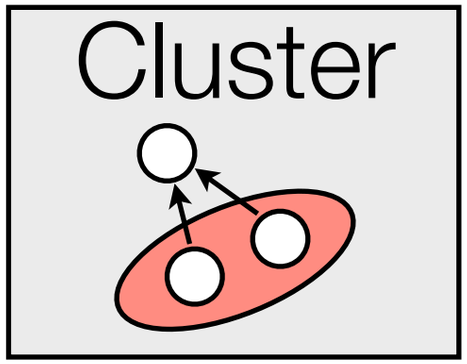
Name users via “re-identification attack” to learn real-world identity

Our paper

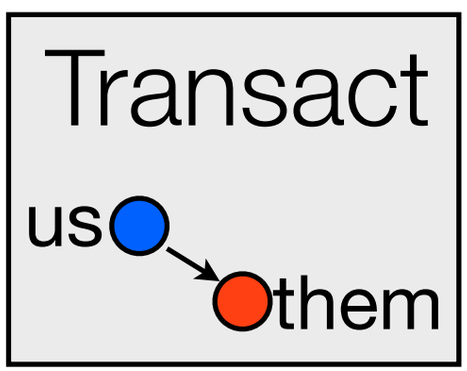
What are people using Bitcoin for?

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

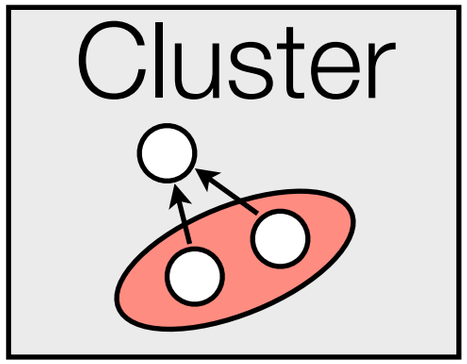


Our paper

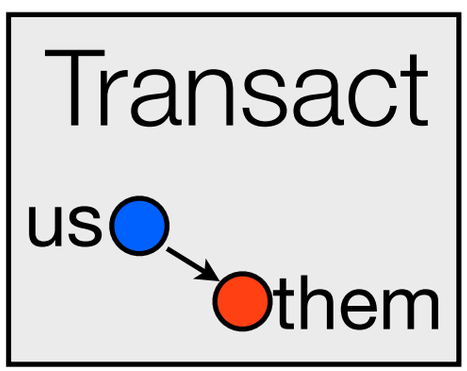
What are people using Bitcoin for?

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

Outline

How does Bitcoin work?

Analysis

Results

Conclusions

Outline

How does Bitcoin work?
Public keys
Transactions
Blocks

Analysis

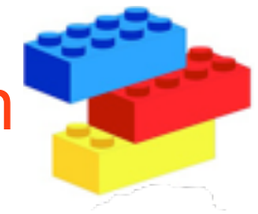
Results

Conclusions

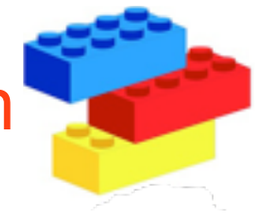
Components of Bitcoin

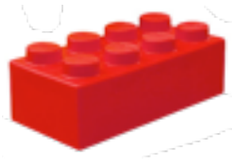
Components of Bitcoin

The global transaction ledger is called the block chain

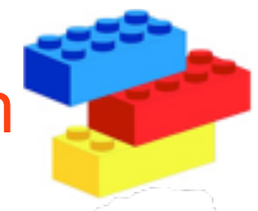


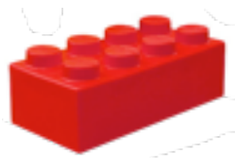
Components of Bitcoin

The global transaction ledger is called the block chain 

A block is a collection of transactions 

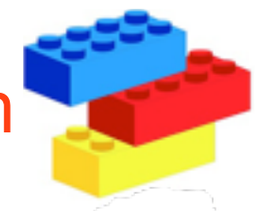
Components of Bitcoin

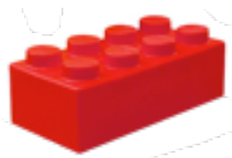
The global transaction ledger is called the block chain 

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?

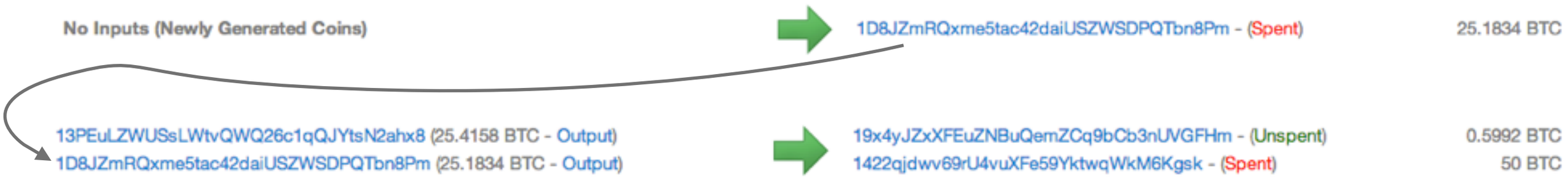
Transactions form a chain

How do bitcoins get spent?

Transactions form a chain

How do bitcoins get spent?

Transactions form a chain



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

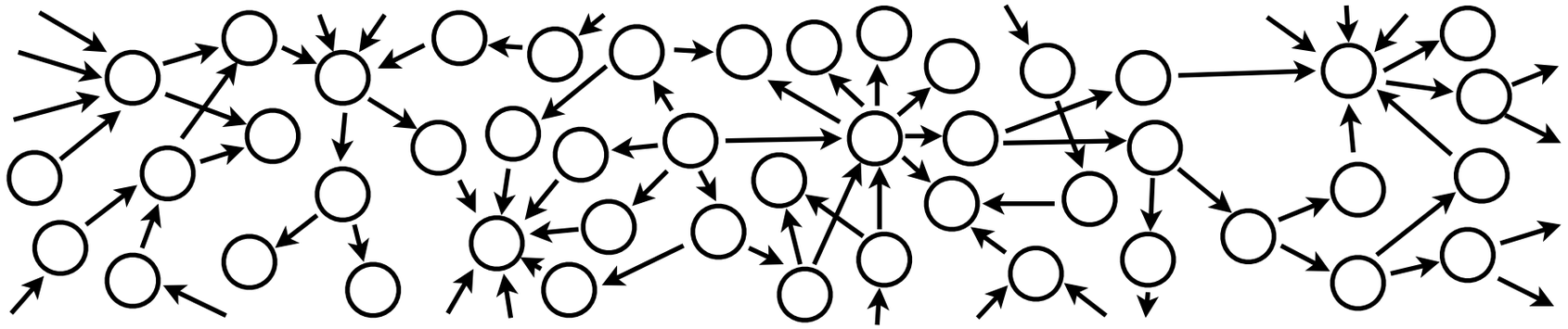
Conclusions

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

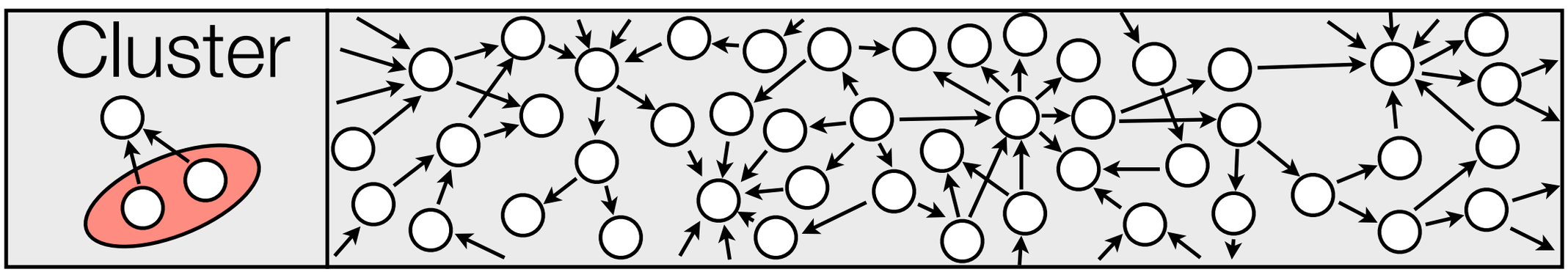
How to identify users?

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



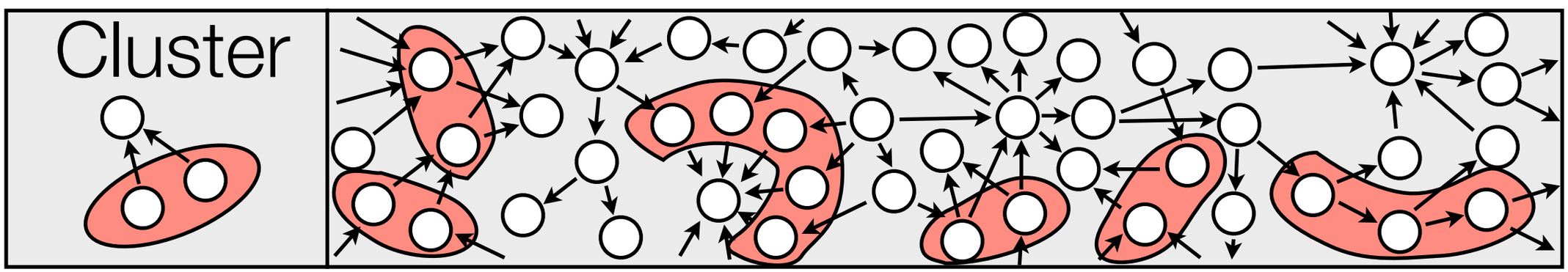
How to identify users?

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?

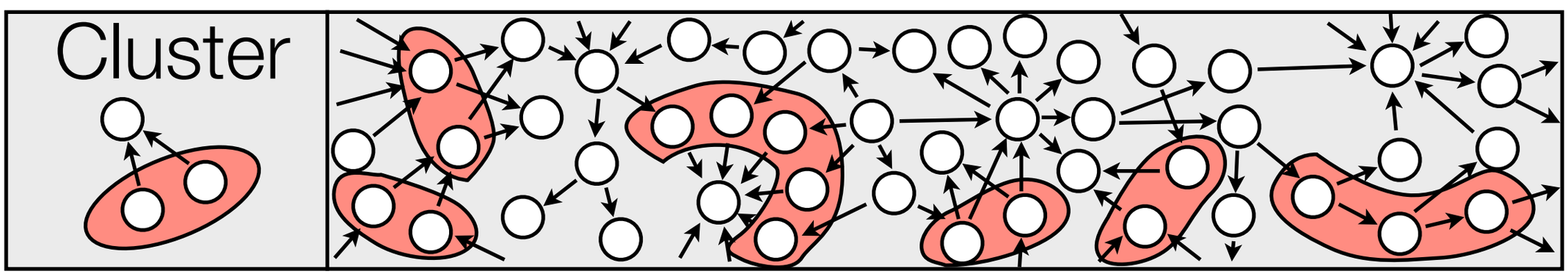
Users can use arbitrarily many public keys (pseudonyms); as a result the Bitcoin graph is complicated and has 12 million public keys



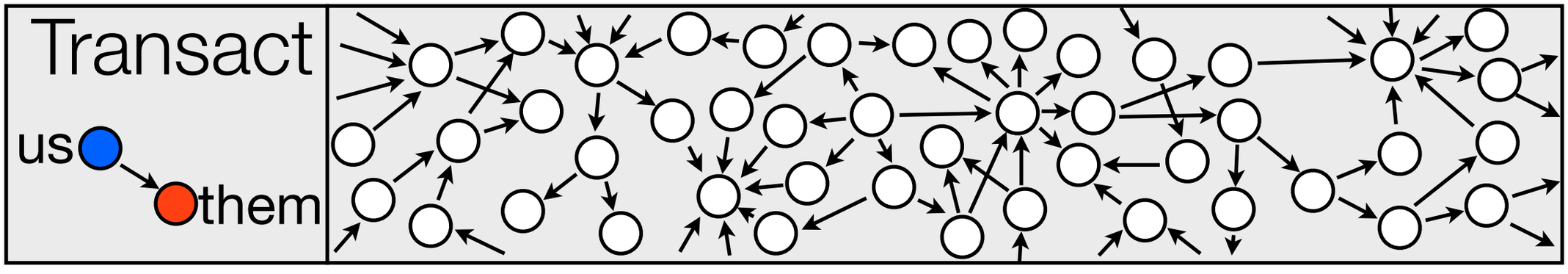
Collapse into a more manageable graph of clusters of public keys representing distinct entities

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

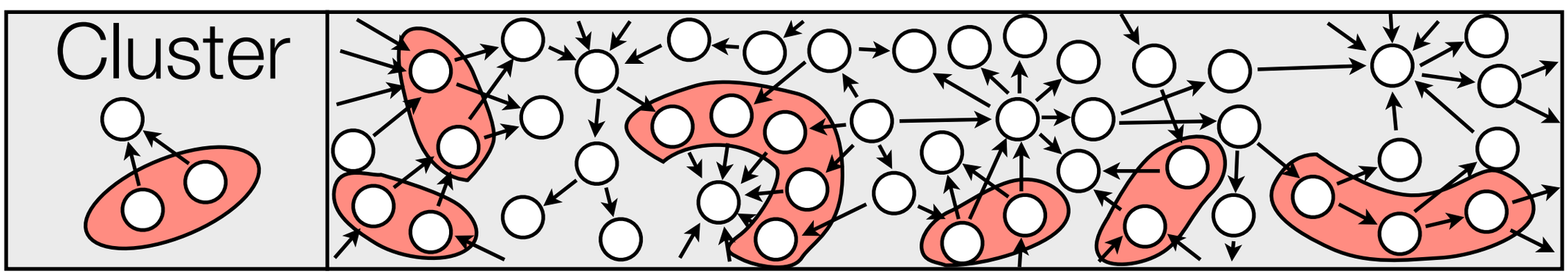


Collapse into a more manageable graph of clusters of public keys representing distinct entities

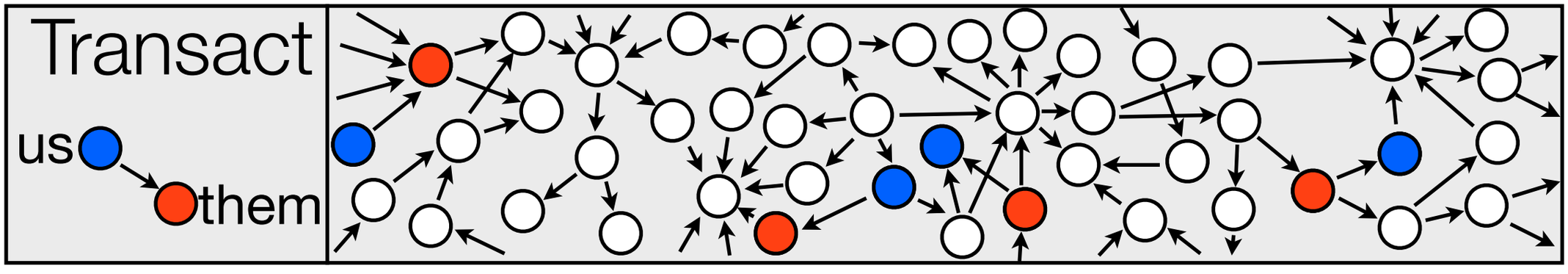


How to identify users?

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

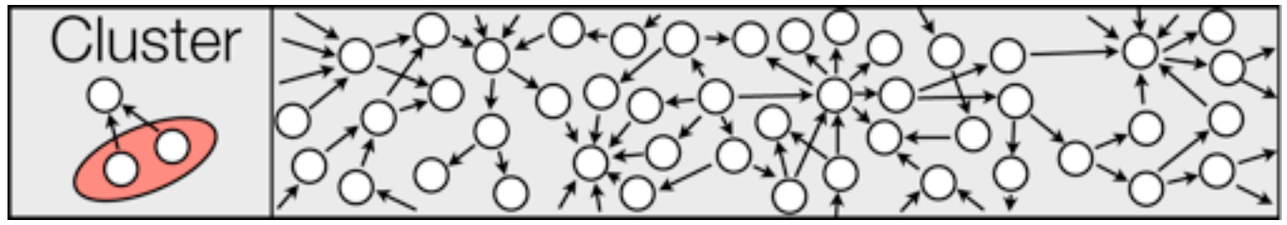


Collapse into a more manageable graph of clusters of public keys representing distinct entities



Collect ground truth data by participating in transactions

Clustering by inputs



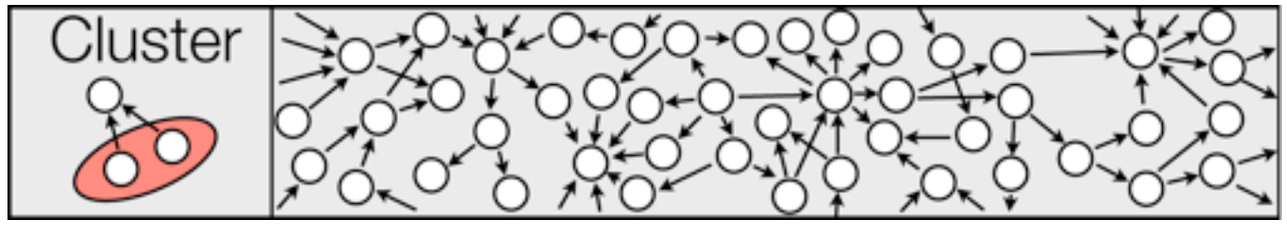
8b6008b2e369499c5c51058f5f09e549c160a84692c00cb97dfa2b4881e9cc27

142Z7VauMVdSV5DADb62DsJ7wvW9ccq18t (30.28851 BTC - Output)
16H9oN1JFXSHEv16X8PLeS77MMF3EKqEiH (30.28851 BTC - Output)
17RHwSeN5Ky8gGwTHCH8j4mZH3eqQNbrav (30.58936 BTC - Output)
13b78oU4oCid4gQw87bvUMUZ1XpnZqwNQ1 (12.9148 BTC - Output)
16BzfEpwF9P6ULmmMcbdag3m2ZaETGgwYN (29.55 BTC - Output)
1CusinkMvW53WtupuspCMDyi8gZ2sb13zv (30.28851 BTC - Output)
1PXA5YNC2MWYtssfsBTBPMWXW8cDkPuMTB (30.28851 BTC - Output)
1Gg2D33ySPndnSELBnmze1QsmycSdeGVkX (30.28851 BTC - Output)
1FdPwjg7XJfrEqdQnduusg2K51UuJDACCi (30.28851 BTC - Output)
178AKou6Q2741uPqt9FQfB26ZUK16f3yDt (29.36578 BTC - Output)
1LZe2eSEKr8ik6ja8k8YNSh1amR2czmwwe (30 BTC - Output)
16ah8vzFqtnyCPtp57Y55bkXwSot7Bd3ic (29.84 BTC - Output)
1Dn92DXHrPNVH7EMrD5oawDedWdk43Jjkk (29.83951 BTC - Output)
1NvC4vQVbwJUjXWHBHKiGKAmKRMkRKe7gv (30.13 BTC - Output)
14kSwoX2cPkwRtKW5KTwBFGtraYpXrYckW (99.45 BTC - Output)
1AkMojTEiUXUa3f9SNjLZcvLtxY54wyC6n (141.9995 BTC - Output)
1KRMiP4uLyy2hm86MRRQv4ghkQthVK6BH6 (29.6 BTC - Output)

1Z9ADFwVMZvgjN3HoNf91XoT2Lpth559F - (Spent) 0.01001 BTC
17iCsx5w55KcNdCRRp9xXFDcMU7btNhqpm - (Unspent) 675 BTC

6 Confirmations | 675.01001 BTC

Clustering by inputs



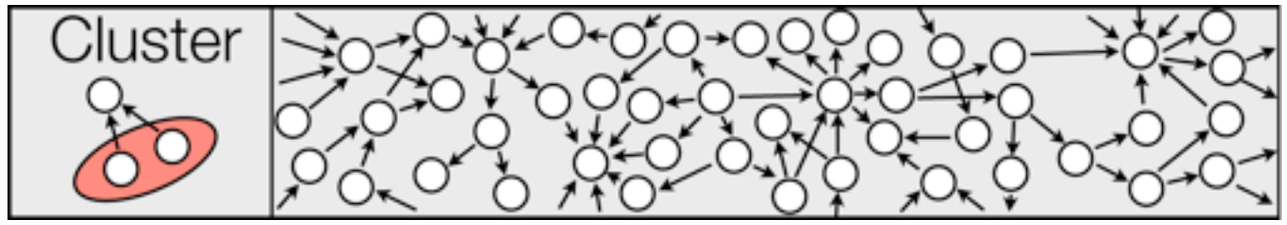
8b6008b2e369499c5c51058f5f09e549c160a84692c00cb97dfa2b4881e9cc27

142Z7VauMVdSV5DADb62DsJ7wvW9ccq18t (30.28851 BTC - Output)
16H9oN1JFXSHEv16X8PLeS77MMF3EKqEiH (30.28851 BTC - Output)
17RHwSeN5Ky8gGwTHCH8j4mZH3eqQNbrav (30.58936 BTC - Output)
13b78oU4oCid4gQw87bvUMUZ1XpnZqwNQ1 (12.9148 BTC - Output)
16BzfEpwF9P6ULmmMcbdag3m2ZaETGgwYN (29.55 BTC - Output)
1CusinkMvW53WtupuspCMDyi8gZ2sb13zv (30.28851 BTC - Output)
1PXA5YNC2MWYtssfsBTBPMWXW8cDkPuMTB (30.28851 BTC - Output)
1Gg2D33ySPndnSELBnmze1QsmycSdeGVkX (30.28851 BTC - Output)
1FdPwjg7XJfrEqdQnduusg2K51UuJDACCi (30.28851 BTC - Output)
178AKou6Q2741uPqt9FQfB26ZUK16f3yDt (29.36578 BTC - Output)
1LZe2eSEKr8ik6ja8k8YNSh1amR2czmwwe (30 BTC - Output)
16ah8vzFqtnyCPtp57Y55bkXwSot7Bd3ic (29.84 BTC - Output)
1Dn92DXHrPNVH7EMrD5oawDedWdk43Jjkk (29.83951 BTC - Output)
1NvC4vQVbwJUjXWHBHKiGKAmKRMkRKe7gv (30.13 BTC - Output)
14kSwoX2cPkwRtKW5KTwBFGtraYpXrYckW (99.45 BTC - Output)
1AkMojTEiUXUa3f9SNjLZcvLtxY54wyC6n (141.9995 BTC - Output)
1KRMiP4uLyy2hm86MRRQv4ghkQthVK6BH6 (29.6 BTC - Output)

1Z9ADFwVMZvgjN3HoNf91XoT2Lpth559F - (Spent) 0.01001 BTC
17iCsx5w55KcNdCRRp9xXFDcMU7btNhqpm - (Unspent) 675 BTC

6 Confirmations | 675.01001 BTC

Clustering by inputs



8b6008b2e369499c5c51058f5f09e549c160a84692c00cb97dfa2b4881e9cc27

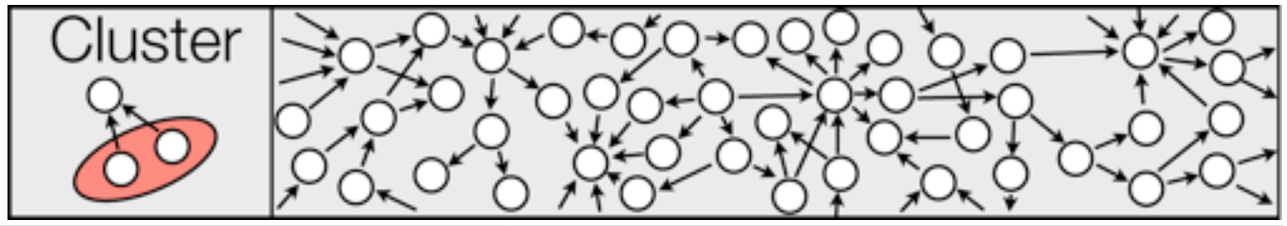
142Z7VauMVdSV5DADb62DsJ7wvW9ccq18t (30.28851 BTC - Output)
16H9oN1JFXSHEv16X8PLeS77MMF3EKqEiH (30.28851 BTC - Output)
17RHwSeN5Ky8gGwTHCH8j4mZH3eqQNbrav (30.58936 BTC - Output)
13b78oU4oCid4gQw87bvUMUZ1XpnZqwNQ1 (12.9148 BTC - Output)
16BzfEpwF9P6ULmmMcbdag3m2ZaETGgwYN (29.55 BTC - Output)
1CusinkMvW53WtupuspCMDyi8gZ2sb13zv (30.28851 BTC - Output)
1PXA5YNC2MWYtssfsBTBPMWXW8cDkPuMTB (30.28851 BTC - Output)
1Gg2D33ySPndnSELBnmze1QsmycSdeGVkX (30.28851 BTC - Output)
1FdPwjg7XJfrEqdQnduusg2K51UuJDACCi (30.28851 BTC - Output)
178AKou6Q2741uPqt9FQfB26ZUK16f3yDt (29.36578 BTC - Output)
1LZe2eSEKr8ik6ja8k8YNSh1amR2czmwwe (30 BTC - Output)
16ah8vzFqtnyCPtp57Y55bkXwSot7Bd3ic (29.84 BTC - Output)
1Dn92DXHrPNVH7EMrD5oawDedWdk43Jjkk (29.83951 BTC - Output)
1NvC4vQVbwJUjXWHBHKiGKAmKRMkRKe7gv (30.13 BTC - Output)
14kSwoX2cPkwRtKW5KTwBFGtraYpXrYckW (99.45 BTC - Output)
1AkMojTEiUXUa3f9SNjLZcvLtxY54wyC6n (141.9995 BTC - Output)
1KRMiP4uLyy2hm86MRRQv4ghkQthVK6BH6 (29.6 BTC - Output)

1Z9ADFwVMZvgjN3HoNf91XoT2Lpth559F - (Spent) 0.01001 BTC
17iCsx5w55KcNdCRRp9xXFDcMU7btNhqpm - (Unspent) 675 BTC

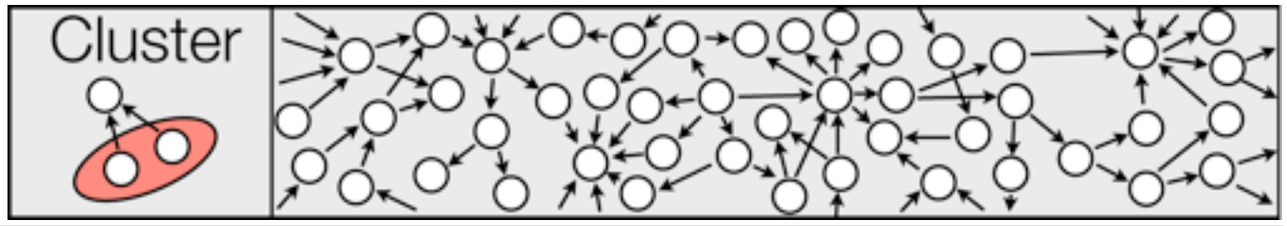
6 Confirmations 675.01001 BTC

Heuristic #1: the same user controls these addresses

Heuristic 1: enough?

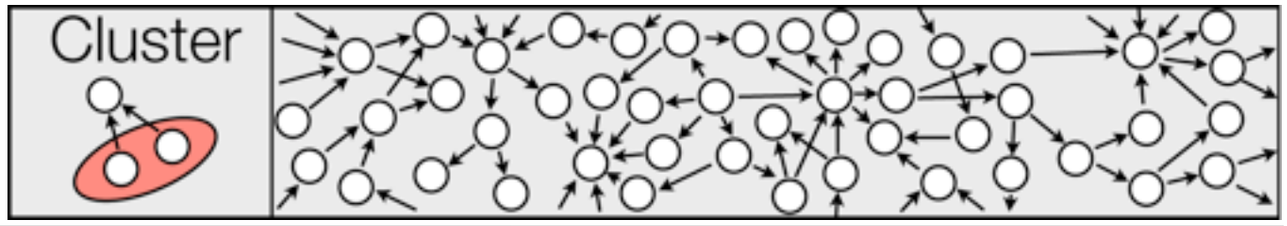


Heuristic 1: enough?



This works because sender must know secret key for each input

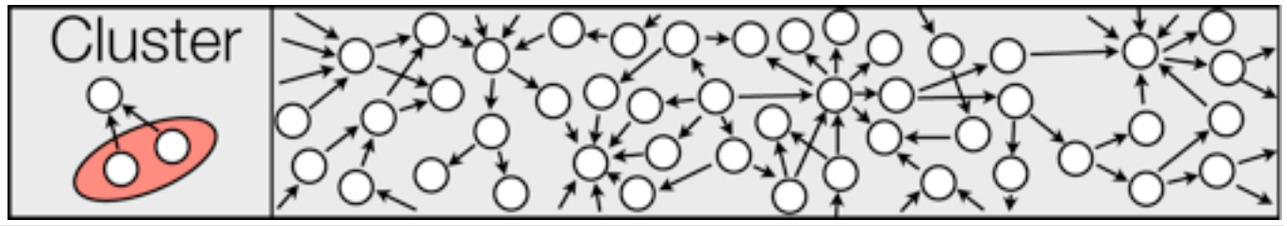
Heuristic 1: enough?



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?

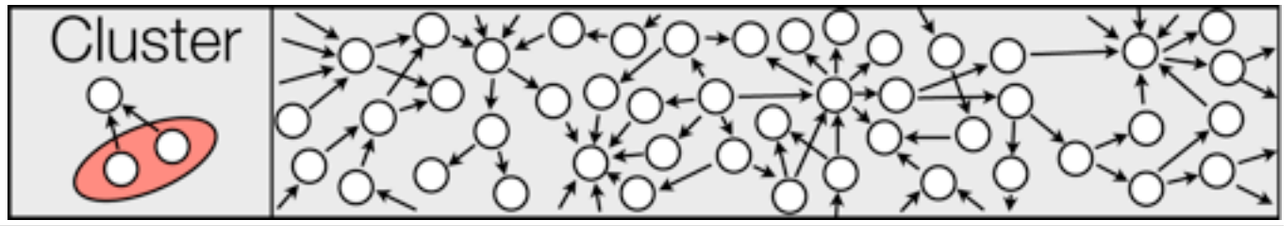


This works because sender must know secret key for each input

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?



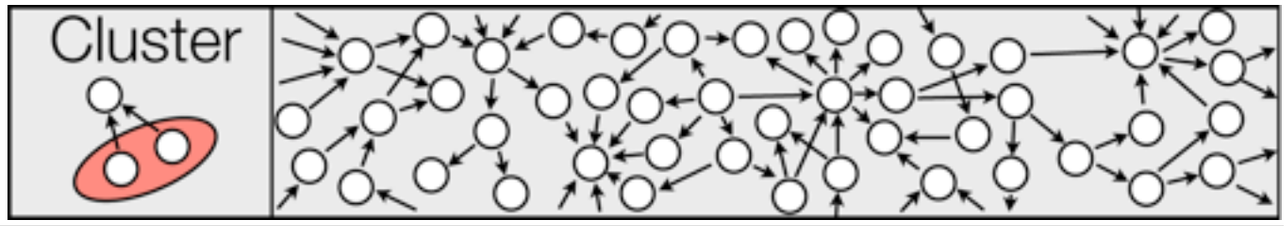
This works because sender must know secret key for each input

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

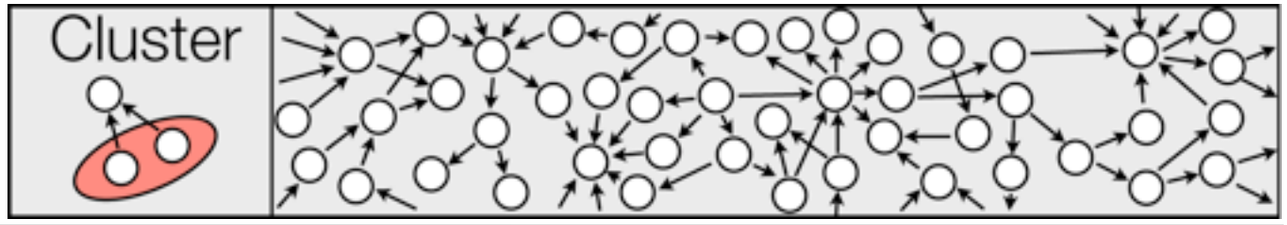
This is established: has been used before [RH13,RS13,A+13] and even acknowledged by Satoshi himself

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

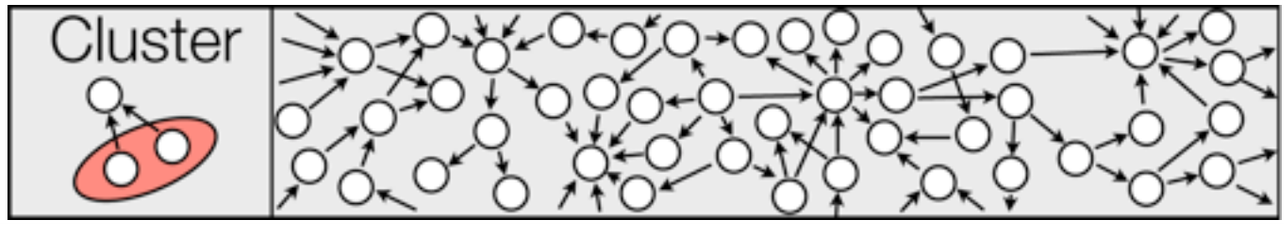


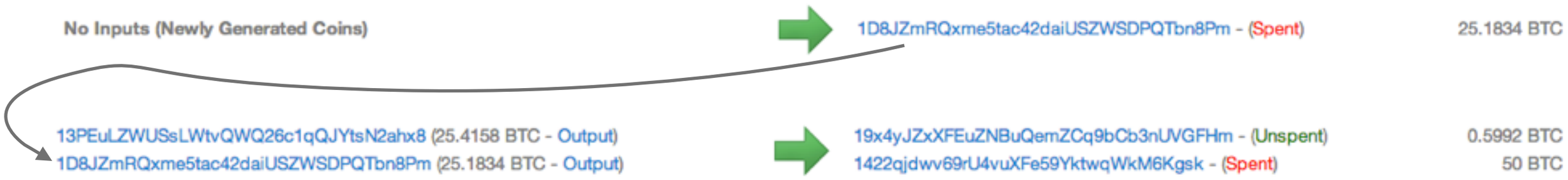
No Inputs (Newly Generated Coins) → 1D8JZmRQxme5tac42daiUSZWSDPQTbn8Pm - (Spent) 25.1834 BTC

13PEuLZWUSsLWtvQWQ26c1qQJYtsN2ahx8 (25.4158 BTC - Output) → 19x4yJZxXFEuZNBuQemZCq9bCb3nUVGFHm - (Unspent) 0.5992 BTC

1D8JZmRQxme5tac42daiUSZWSDPQTbn8Pm (25.1834 BTC - Output) → 1422qjdwv69rU4vuXFe59YktwqWkM6Kgsk - (Spent) 50 BTC

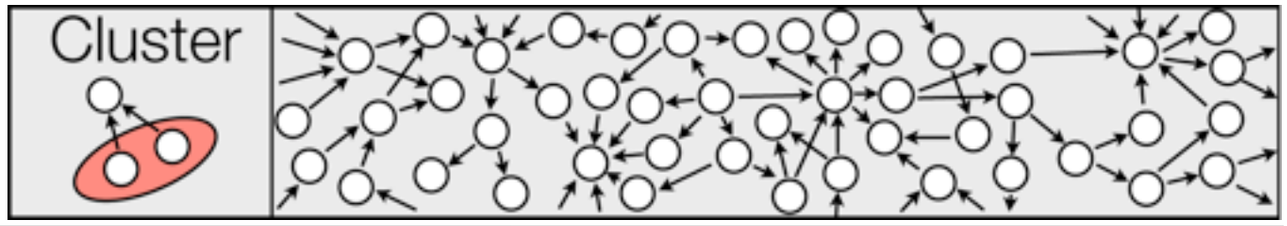
Change addresses

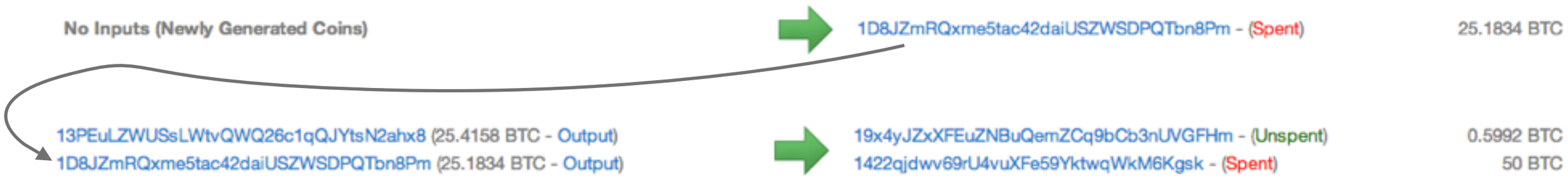




Each transaction must reference a previous transaction, so all bitcoins received must be spent all at once

Change addresses

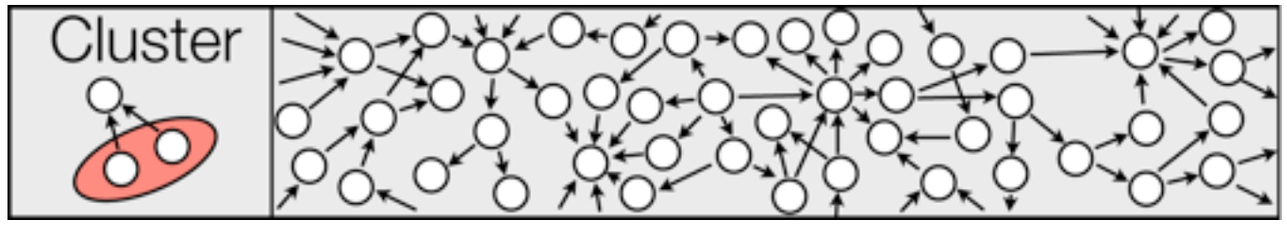


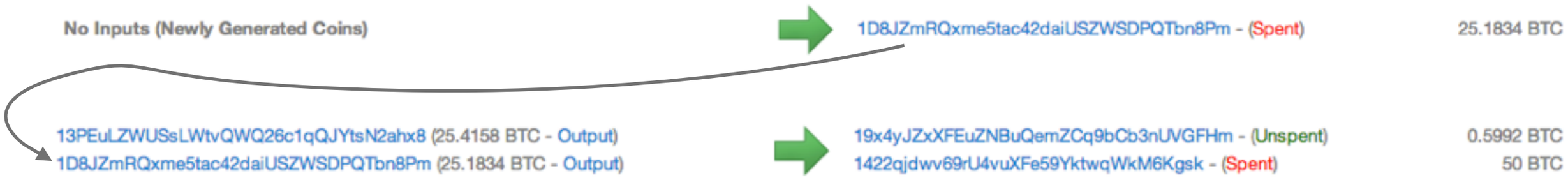


Each transaction must reference a previous transaction, so all bitcoins received must be spent all at once

Change address: used to collect excess bitcoins

Change addresses



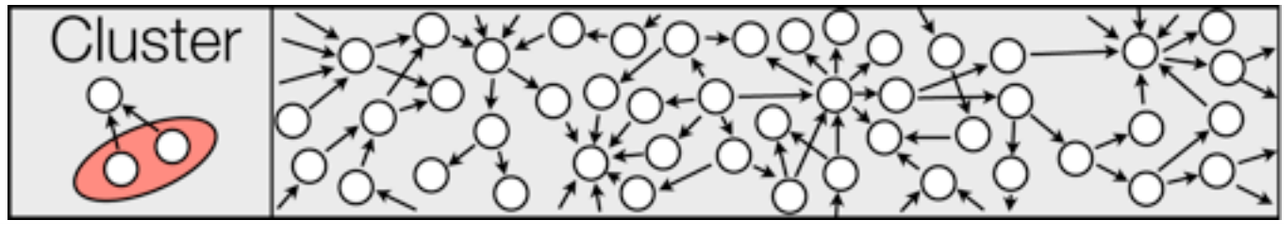


Each transaction must reference a previous transaction, so all bitcoins received must be spent all at once

Change address: used to collect excess bitcoins

In the standard client, change addresses are used at most twice: to receive and to spend

Clustering by change



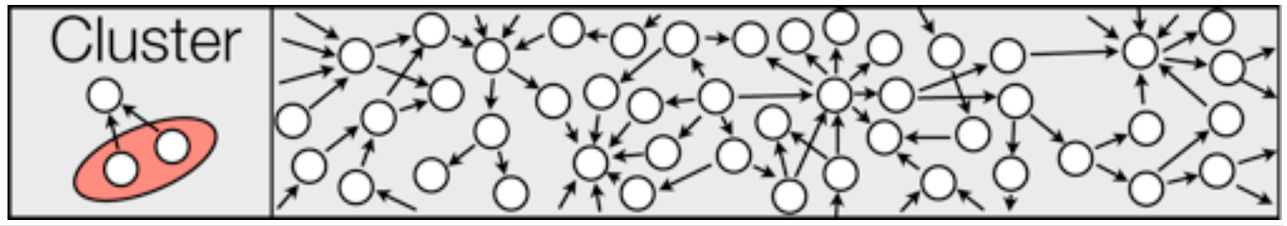
8b6008b2e369499c5c51058f5f09e549c160a84692c00cb97dfa2b4881e9cc27

142Z7VauMVdSV5DADb62DsJ7wvW9ccq18t (30.28851 BTC - Output)
16H9oN1JFXSHEv16X8PLeS77MMF3EKqEiH (30.28851 BTC - Output)
17RHwSeN5Ky8gGwTHCH8j4mZH3eqQNbrav (30.58936 BTC - Output)
13b78oU4oCid4gQw87bvUMUZ1XpnZqwNQ1 (12.9148 BTC - Output)
16BzfEpwF9P6ULmmMcbdag3m2ZaETGgwYN (29.55 BTC - Output)
1CusinkMvW53WtupuspCMDyi8gZ2sb13zv (30.28851 BTC - Output)
1PXA5YNC2MWYtssfsBTBPMWXW8cDkPuMTB (30.28851 BTC - Output)
1Gg2D33ySPndnSELBnmze1QsmycSdeGVkX (30.28851 BTC - Output)
1FdPwjg7XJfrEqdQnduusg2K51UuJDACCi (30.28851 BTC - Output)
178AKou6Q2741uPqt9FQfB26ZUK16f3yDt (29.36578 BTC - Output)
1LZe2eSEKr8ik6ja8k8YNSh1amR2czmwwe (30 BTC - Output)
16ah8vzFqtnyCPtp57Y55bkXwSot7Bd3ic (29.84 BTC - Output)
1Dn92DXHrPNVH7EMrD5oawDedWdk43Jjkk (29.83951 BTC - Output)
1NvC4vQVbwJUjXWHBHKiGKAmKRMkRKe7gv (30.13 BTC - Output)
14kSwoX2cPkwRtKW5KTwBFGtraYpXrYckW (99.45 BTC - Output)
1AkMojTEiUXUa3f9SNjLZcvLtxY54wyC6n (141.9995 BTC - Output)
1KRMiP4uLyy2hm86MRRQv4ghkQthVK6BH6 (29.6 BTC - Output)

1Z9ADFwVMZvgjN3HoNf91XoT2Lpth559F - (Spent) 0.01001 BTC
17iCsx5w55KcNdCRRp9xXFDcMU7btNhqpm - (Unspent) 675 BTC

6 Confirmations | 675.01001 BTC

Clustering by change



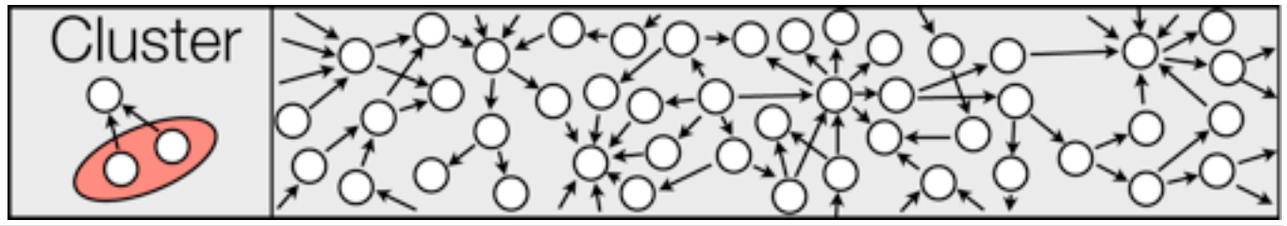
8b6008b2e369499c5c51058f5f09e549c160a84692c00cb97dfa2b4881e9cc27

142Z7VauMVdSV5DADb62DsJ7wvW9ccq18t (30.28851 BTC - Output)
16H9oN1JFXSHEv16X8PLeS77MMF3EKqEiH (30.28851 BTC - Output)
17RHwSeN5Ky8gGwTHCH8j4mZH3eqQNbrav (30.58936 BTC - Output)
13b78oU4oCid4gQw87bvUMUZ1XpnZqwNQ1 (12.9148 BTC - Output)
16BzfEpwF9P6ULmmMcbdag3m2ZaETGgwYN (29.55 BTC - Output)
1CusinkMvW53WtupuspCMDyi8gZ2sb13zv (30.28851 BTC - Output)
1PXA5YNC2MWYtssfsBTBPMWXW8cDkPuMTB (30.28851 BTC - Output)
1Gg2D33ySPndnSELBnmze1QsmycSdeGVkX (30.28851 BTC - Output)
1FdPwjg7XJfrEqdQnduusg2K51UuJDACCi (30.28851 BTC - Output)
178AKou6Q2741uPqt9FQfB26ZUK16f3yDt (29.36578 BTC - Output)
1LZe2eSEKr8ik6ja8k8YNSh1amR2czmwwe (30 BTC - Output)
16ah8vzFqtnyCPtp57Y55bkXwSot7Bd3ic (29.84 BTC - Output)
1Dn92DXHrPNVH7EMrD5oawDedWdk43Jjkk (29.83951 BTC - Output)
1NvC4vQVbwJUjXWHBHKiGKAmKRMkRKe7gv (30.13 BTC - Output)
14kSwoX2cPkwRtKW5KTwBFGtraYpXrYckW (99.45 BTC - Output)
1AkMojTEiUXUa3f9SNjLZcvLtxY54wyC6n (141.9995 BTC - Output)
1KRMiP4uLyy2hm86MRRQv4ghkQthVK6BH6 (29.6 BTC - Output)

1Z9ADFwVMZvgjN3HoNf91XoT2Lpth559F - (Spent) 0.01001 BTC
17iCsx5w55KcNdCRRp9xXFDcMU7btNhqpm - (Unspent) 675 BTC

6 Confirmations | 675.01001 BTC

Clustering by change



8b6008b2e369499c5c51058f5f09e549c160a84692c00cb97dfa2b4881e9cc27

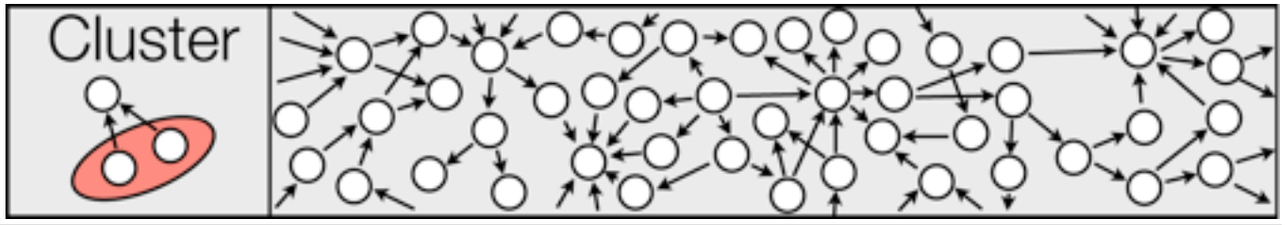
142Z7VauMVdSV5DADb62DsJ7wvW9ccq18t (30.28851 BTC - Output)
16H9oN1JFXSHEv16X8PLeS77MMF3EKqEiH (30.28851 BTC - Output)
17RHwSeN5Ky8gGwTHCH8j4mZH3eqQNbrav (30.58936 BTC - Output)
13b78oU4oCid4gQw87bvUMUZ1XpnZqwNQ1 (12.9148 BTC - Output)
16BzfEpwF9P6ULmmMcbdag3m2ZaETGgwYN (29.55 BTC - Output)
1CusinkMvW53WtupuspCMDyi8gZ2sb13zv (30.28851 BTC - Output)
1PXA5YNC2MWYtssfsBTBPMWXW8cDkPuMTB (30.28851 BTC - Output)
1Gg2D33ySPndnSELBnmze1QsmycSdeGVkX (30.28851 BTC - Output)
1FdPwjg7XJfrEqdQnduusg2K51UuJDACCi (30.28851 BTC - Output)
178AKou6Q2741uPqt9FQfB26ZUK16f3yDt (29.36578 BTC - Output)
1LZe2eSEKr8ik6ja8k8YNSh1amR2czmwwe (30 BTC - Output)
16ah8vzFqtnyCPtp57Y55bkXwSot7Bd3ic (29.84 BTC - Output)
1Dn92DXHrPNVH7EMrD5oawDedWdk43Jjkk (29.83951 BTC - Output)
1NvC4vQVbwJUjXWHBHKiGKAmKRMkRKe7gv (30.13 BTC - Output)
14kSwoX2cPkwRtKW5KTwBFGtraYpXrYckW (99.45 BTC - Output)
1AkMojTEiUXUa3f9SNjLZcvLtxY54wyC6n (141.9995 BTC - Output)
1KRMiP4uLyy2hm86MRRQv4ghkQthVK6BH6 (29.6 BTC - Output)

1Z9ADFwVMZvgjN3HoNf91XoT2Lpth559F - (Spent) 0.01001 BTC
17iCsx5w55KcNdCRRp9xFDcMU7btNhqpm - (Unspent) 675 BTC

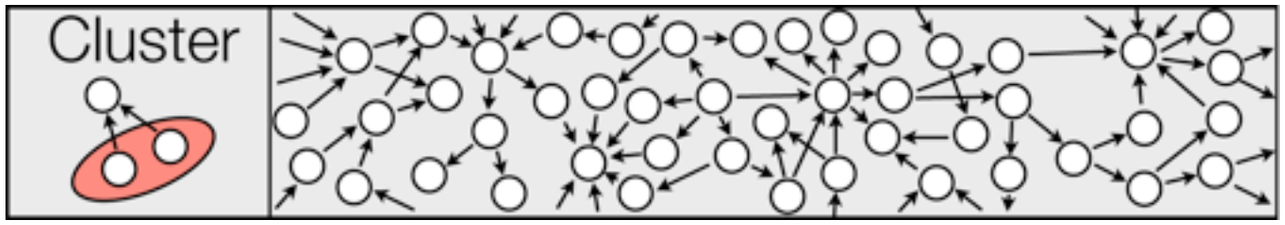
6 Confirmations | 675.01001 BTC

Heuristic #2: the same user also controls this address

Heuristic 2

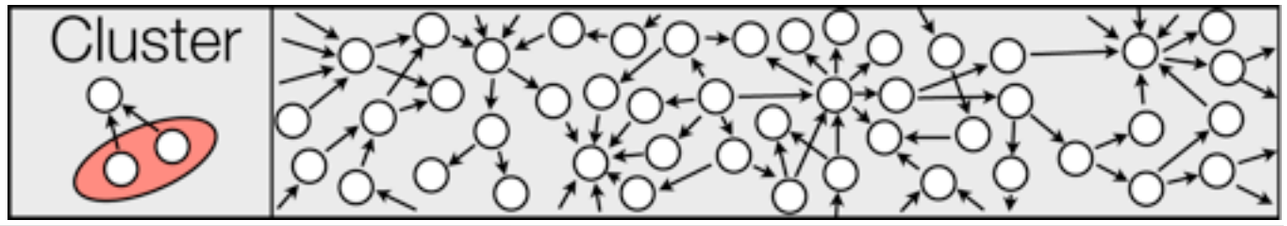


Heuristic 2



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

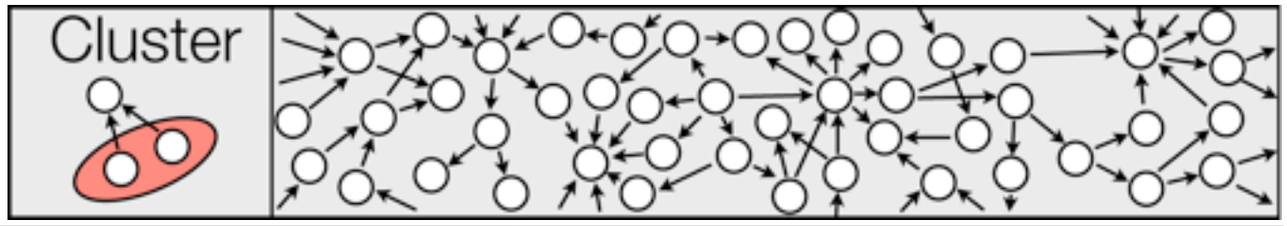
Heuristic 2



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

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

Heuristic 2

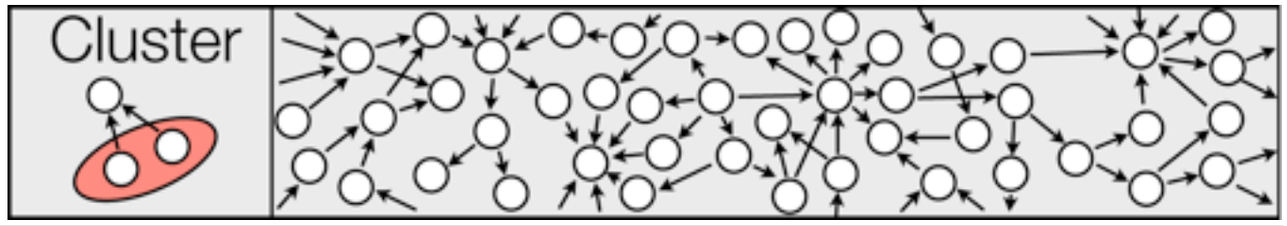


To identify change addresses, look for “one-time” output address

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

This isn’t conservative enough!

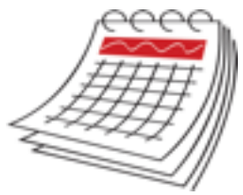
Heuristic 2



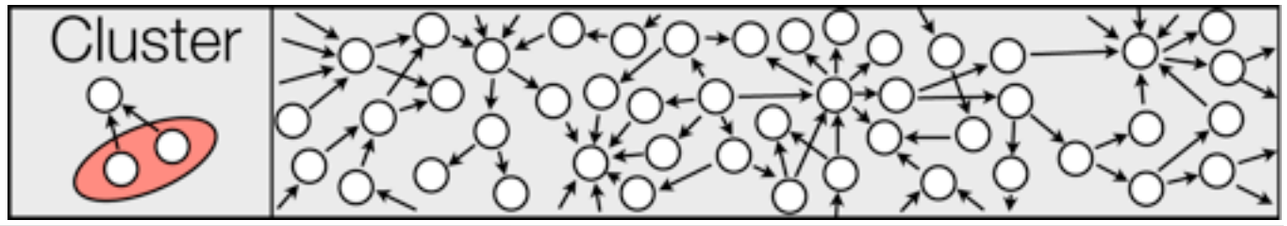
To identify change addresses, look for “one-time” output address

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

This isn’t conservative enough!

- Wait a week before identifying address 

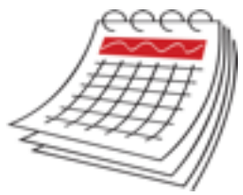
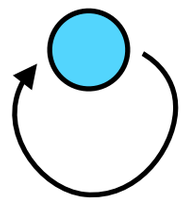
Heuristic 2



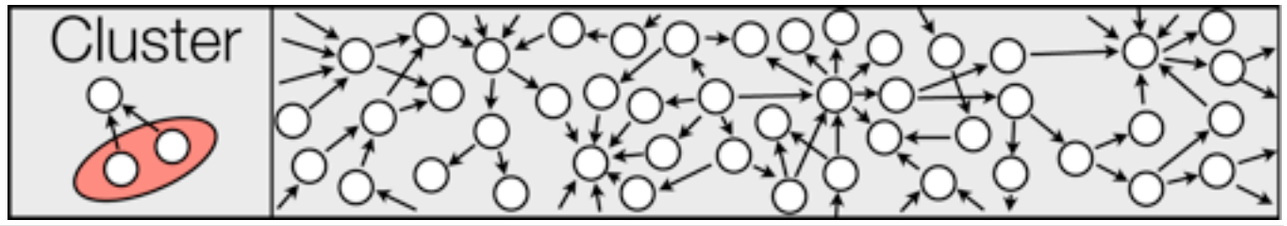
To identify change addresses, look for “one-time” output address

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 

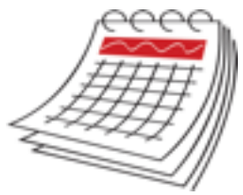
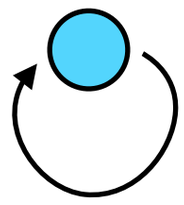
Heuristic 2



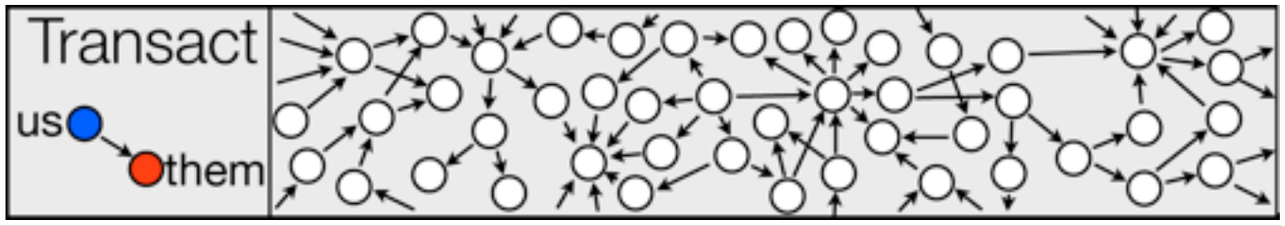
To identify change addresses, look for “one-time” output address

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

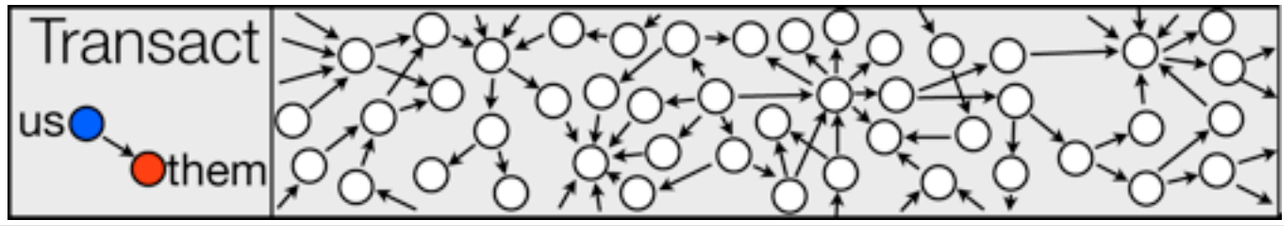
This isn’t conservative enough!

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

Data collection

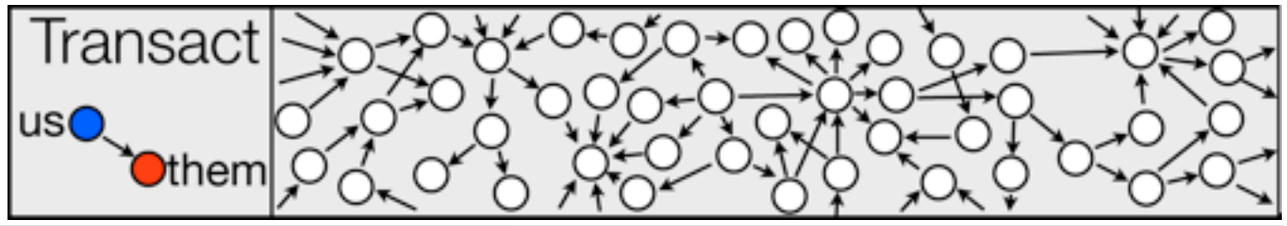


Data collection



Engaged in transactions with:

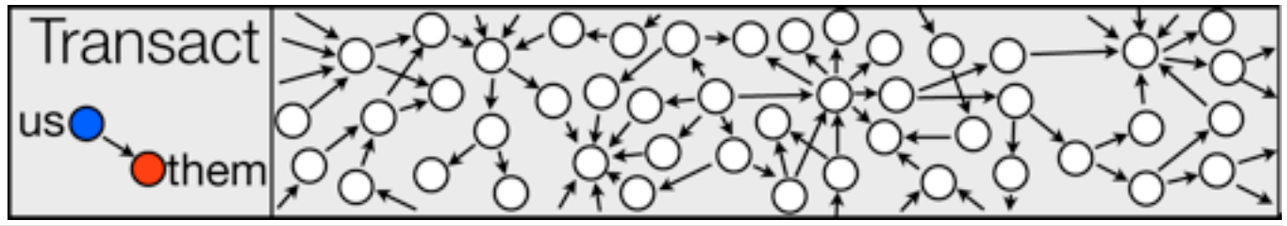
Data collection



Engaged in transactions with:

- Exchanges

Data collection

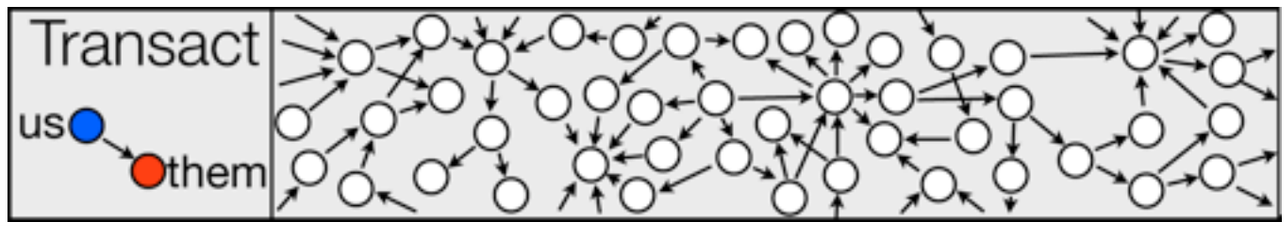


Engaged in transactions with:

- Exchanges

- Vendors

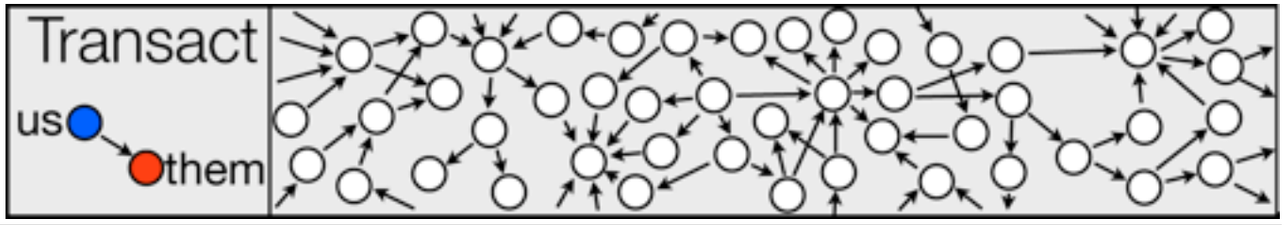
Data collection



Engaged in transactions with:

- Exchanges
- Vendors
- Mining pools

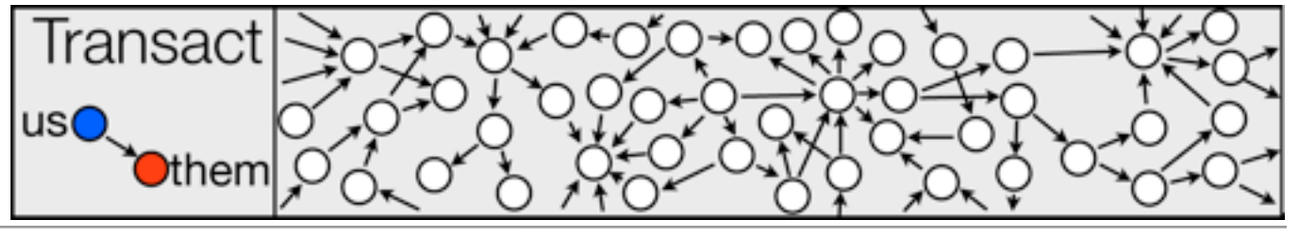
Data collection



Engaged in transactions with:

- Exchanges
- Vendors
- Mining pools
- Gambling sites

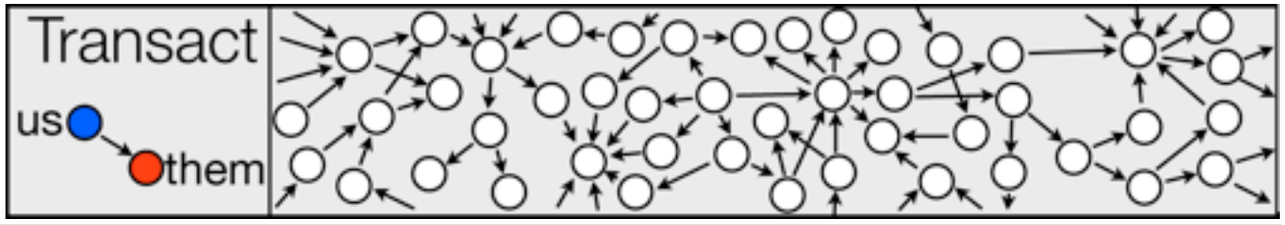
Data collection



Engaged in transactions with:

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

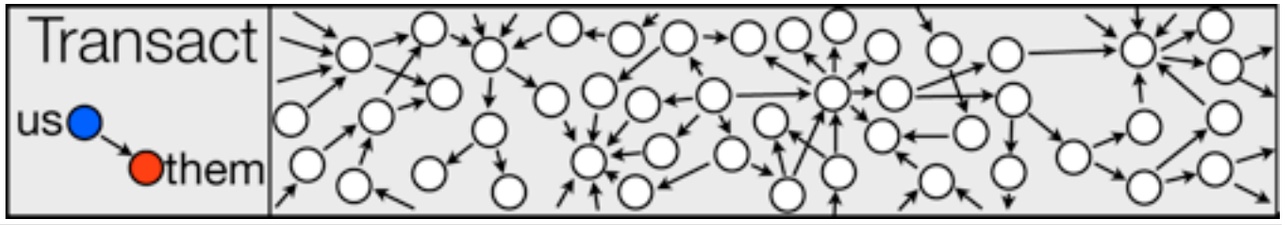
Data collection



Engaged in transactions with:

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

Data collection

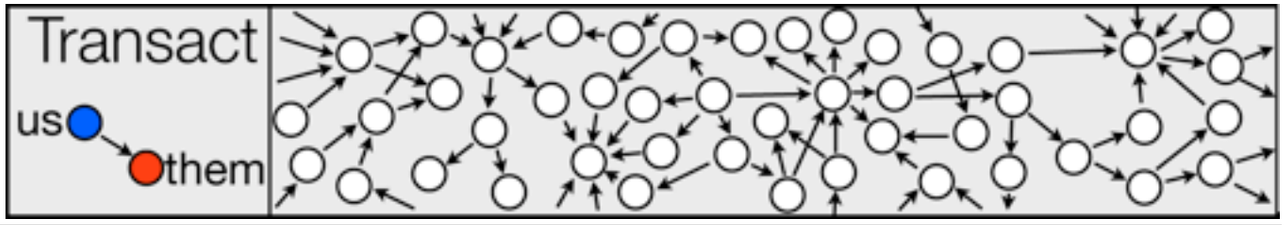


Engaged in transactions with:

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

Scraped published tags

Data collection



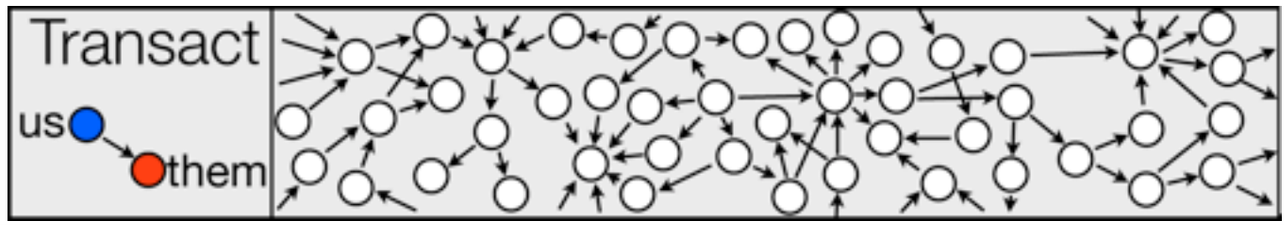
Engaged in transactions with:

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

Scraped published tags

Found addresses discussed on forums

Exchanges



Bitcoin-24

BTC e

aurum exchange

Bitcoin-Central

CAMP BX
BITCOIN TRADING PLATFORM

BitInstant

bitcoin.de
Bitcoin-Marketplace - Made in Germany!

VirtEx
Canadian Virtual Exchange

BITCOIN NORDIC
Bitcoins easy. Bitcoins fast.

Bitcurex
The new age of currency.

ICBIT
Bitcoin Exchange

btcQuick

bitfloor

mercadobitcoin

FastCash4Bitcoins

BitMarket.eu
YOUR PLACE TO EXCHANGE BITCOINS

MT.GOX

LILION TRANSFER
Login | Registration

BITME

TRADING LTD.
THEROCK

NANAIMO GOLD
DIGITAL CURRENCY EXCHANGE

BITSTAMP

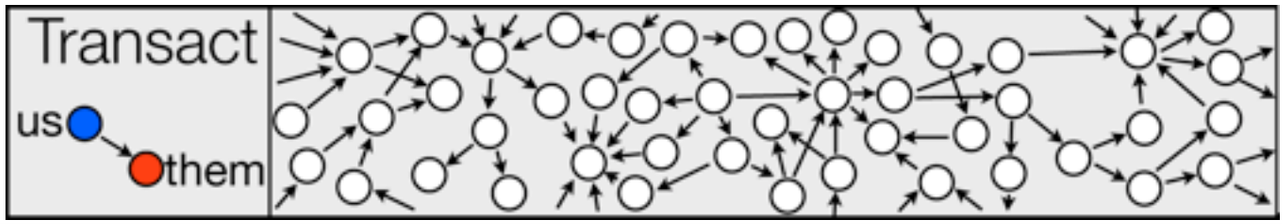
Vircurex

OKPAY payments made easy

Bitcoin China

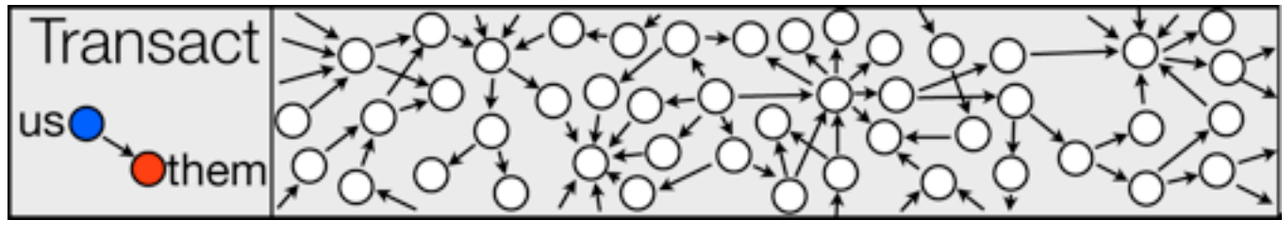
VirWoX
virtual world exchange

Vendors


Transact
us
them

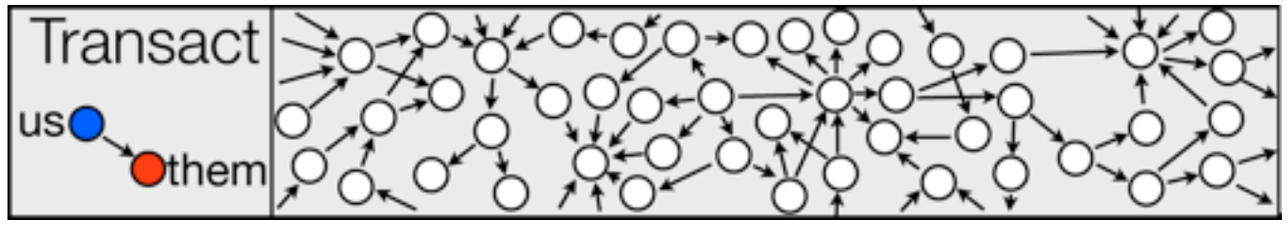

House
SUPER MARIO 3
ubuntu
CASIO
Bitcoin
organic colombian la rochela
Baklava
bitcoin.org
ZYROSTARS
THE LITTLE BOOK OF ANSWERS

Published tags



1LDCRDhNBiTaurUmJKqRef3cGpWLWfEpFk	BitAurum.eu	https://www.bitaurum.eu
1NmduGNyC5XejoysbuioodCN3jR3yf64xM	Electrum	http://electrum.ecdsa.org/community.html
1BTC24yVKQdQNAa4vX71xLUC5A8Za7Rr71	Bitcoin-24.com	https://bitcoin-24.com
14FHqYSgAi39CEJksUJJsK8JzJzyqFpLVk	xkcd	http://xkcd.com/bitcoin/
16xTfttqg6DbvkAGpPvWWpEhEC4e1fCG7G	Genesis2church.org	http://genesis2church.org/donate-with-bitcoin.html
13RcqwggWi9VwcPCZ5BeScxZLWPtt3NVzf	Skeptinerd	http://www.skeptinerd.com/donate-with-bitcoin/
1Kj7V3CYk4TzmE5cgYR7UVbejgFVRbqSwu	WeUseCoins	http://www.weusecoins.com/about.php
1HCMw4nJMT9C6aXaE4EFUb4UbYLg9qpGqw	A Lightning War for Liberty	http://libertyblitzkrieg.com/donate-via-bitcoin-2/

Trolling Bitcoin forums



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

#10

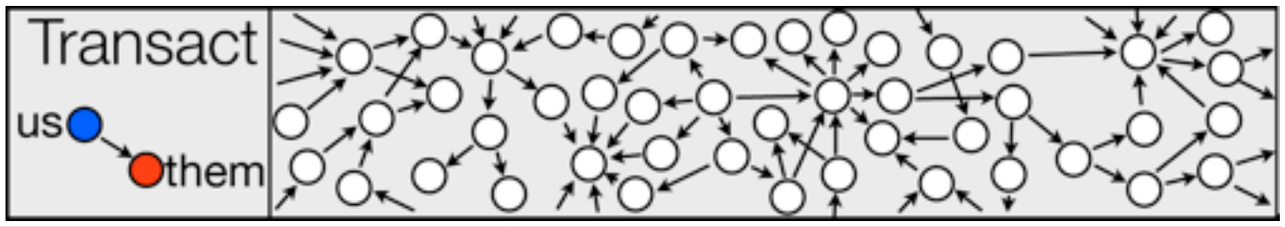
server was hacked brutally. this time - not by stupid site bug, but something else. still looking.

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..

Trolling Bitcoin forums



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

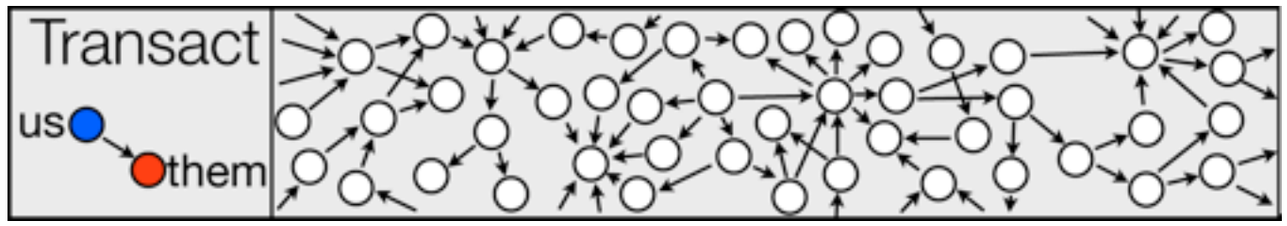
server was hacked brutally. this time - not by stupid site bug, but something else. still looking.

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..

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..

bf70ac1d2b702dbe0e14fbefb3a0cb2ff5ee5aa425cfe4249f16d6ede7b3ff14 **(Fee: 0 BTC - Size: 798 bytes) 2012-04-11 11:14:03**

1FE71fnpTXYbVxZnRXZKxpPvsKBv5ZCJst (10 BTC - Output)		
1FE71fnpTXYbVxZnRXZKxpPvsKBv5ZCJst (4.42577016 BTC - Output)	1HVi6re6zDr5c5v9Sk2mmL9u7svEHfiBt4	0.22895016 BTC
1FE71fnpTXYbVxZnRXZKxpPvsKBv5ZCJst (2 BTC - Output)	1L4kz6BA8mzi8KLV9VQ2pYcW8QQFVihWLg	17 BTC
1Mu4tcypjQ6hypaqQ9x4h8CCs4bg9pH9Zz (0.80318 BTC - Output)		

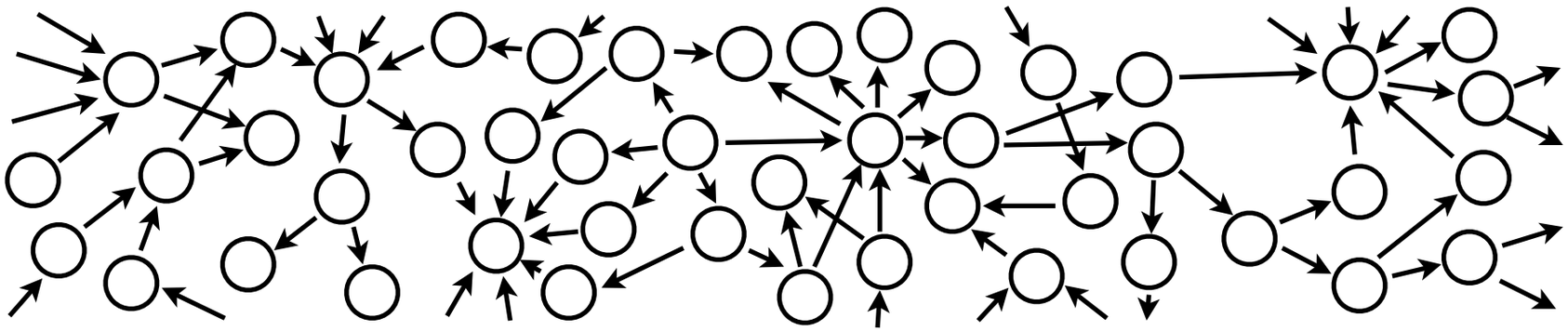
17 BTC

40fc8f6b2f222fb2871a38a245132ed1eada9ff6aec8d46ebe74b29c64fd82a7 **(Fee: 0 BTC - Size: 437 bytes) 2012-04-11 10:51:01**

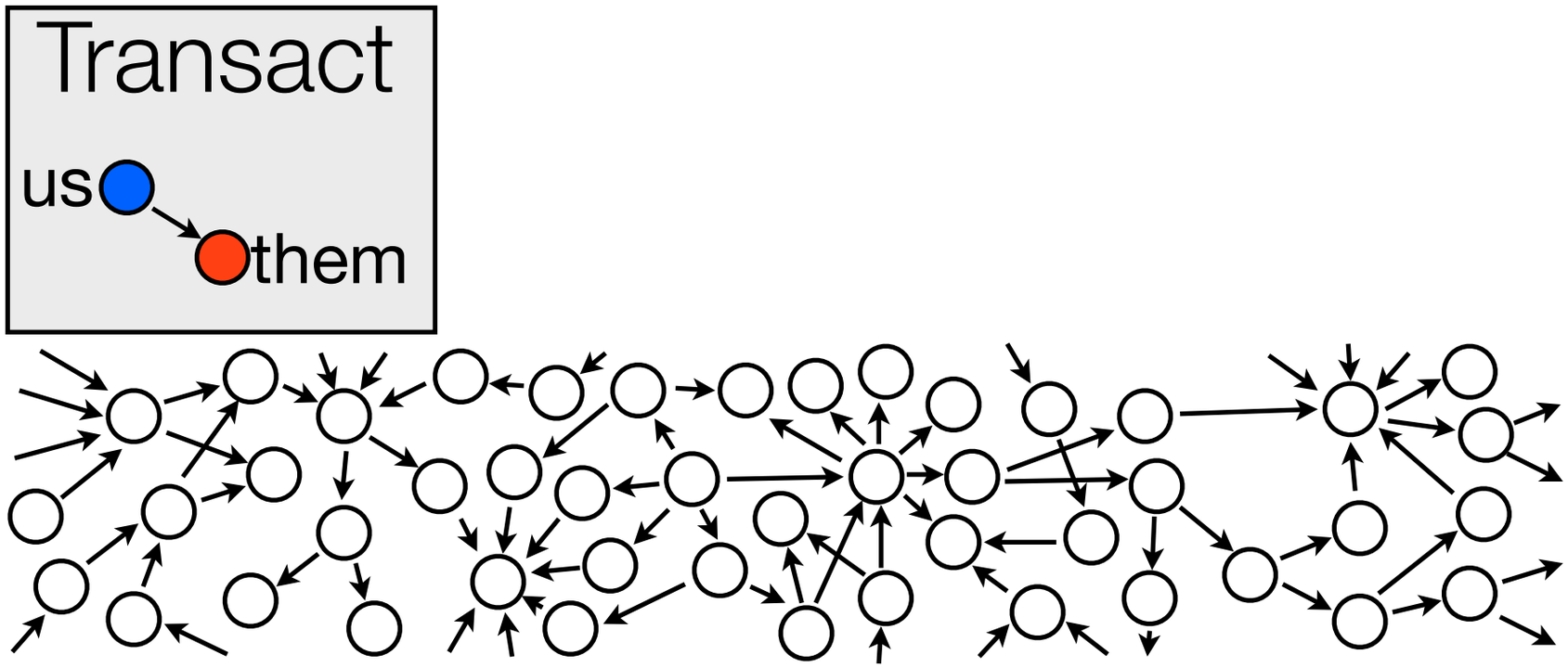
1CcRiHgr3HWK5bHJ38jBwgLVmBUWRzqEu6 (121.258 BTC - Output)	1KPGDc6oHpvWoUSyssxqmRgwtUqsyyey2y	0.038 BTC
1Lgnzb1p9YE3uKwGpspMQZ1NcAD1EMxzSh (43.78 BTC - Output)	1L4kz6BA8mzi8KLV9VQ2pYcW8QQFVihWLg	165 BTC

165 BTC

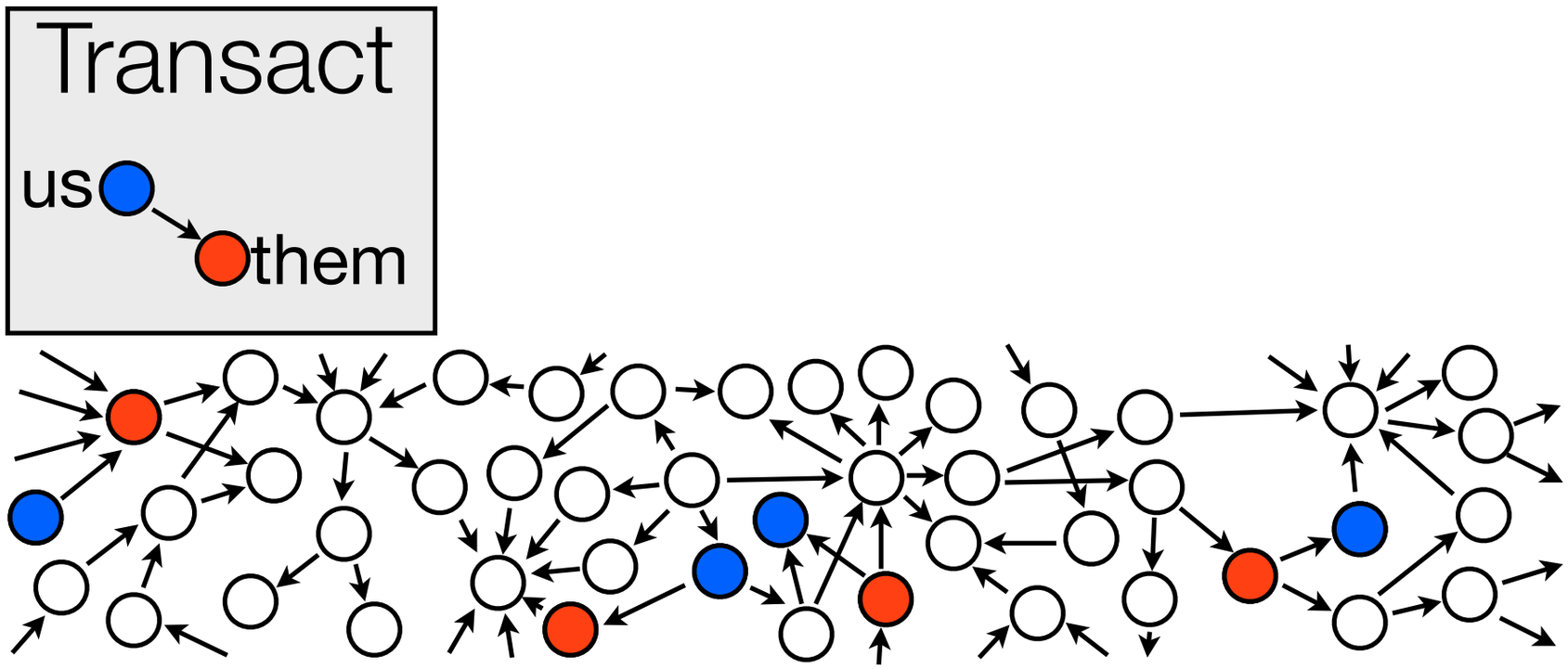
Putting it all together



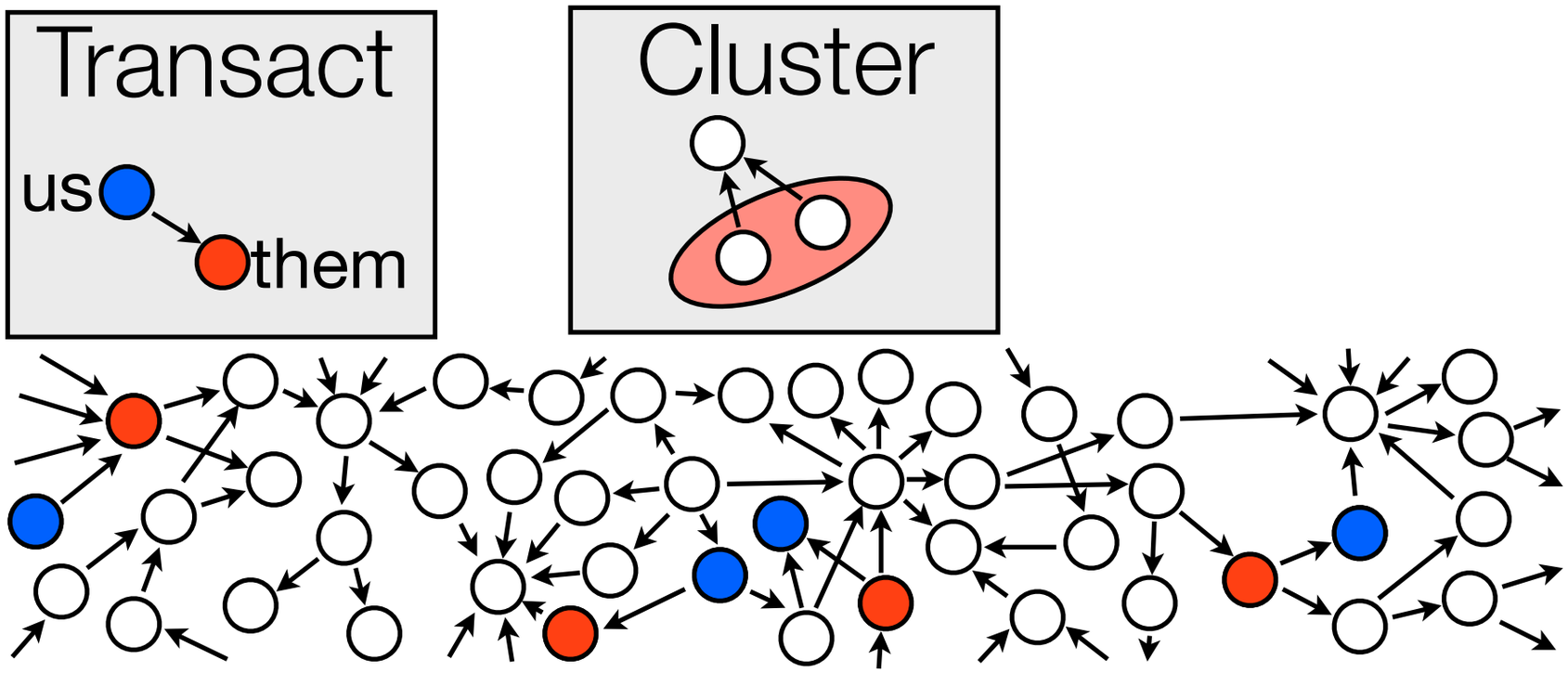
Putting it all together



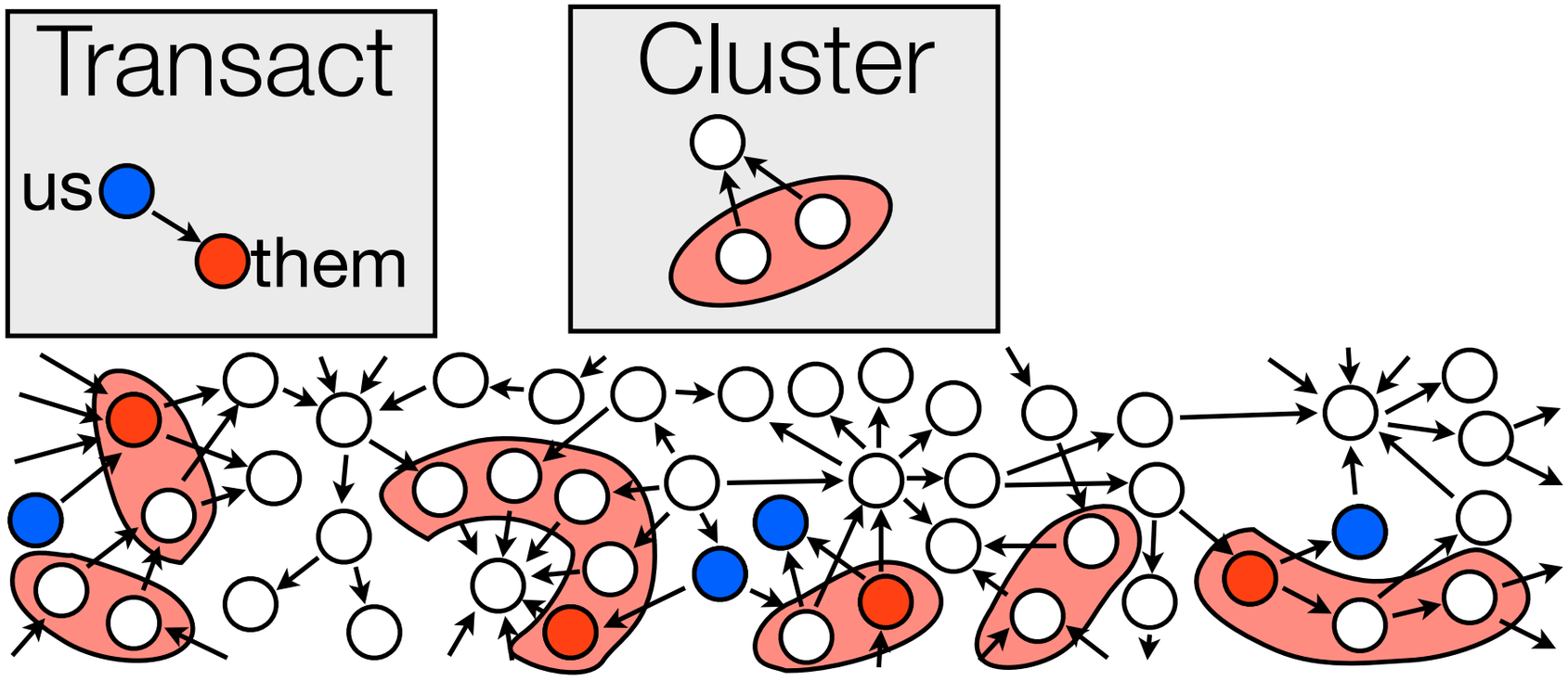
Putting it all together



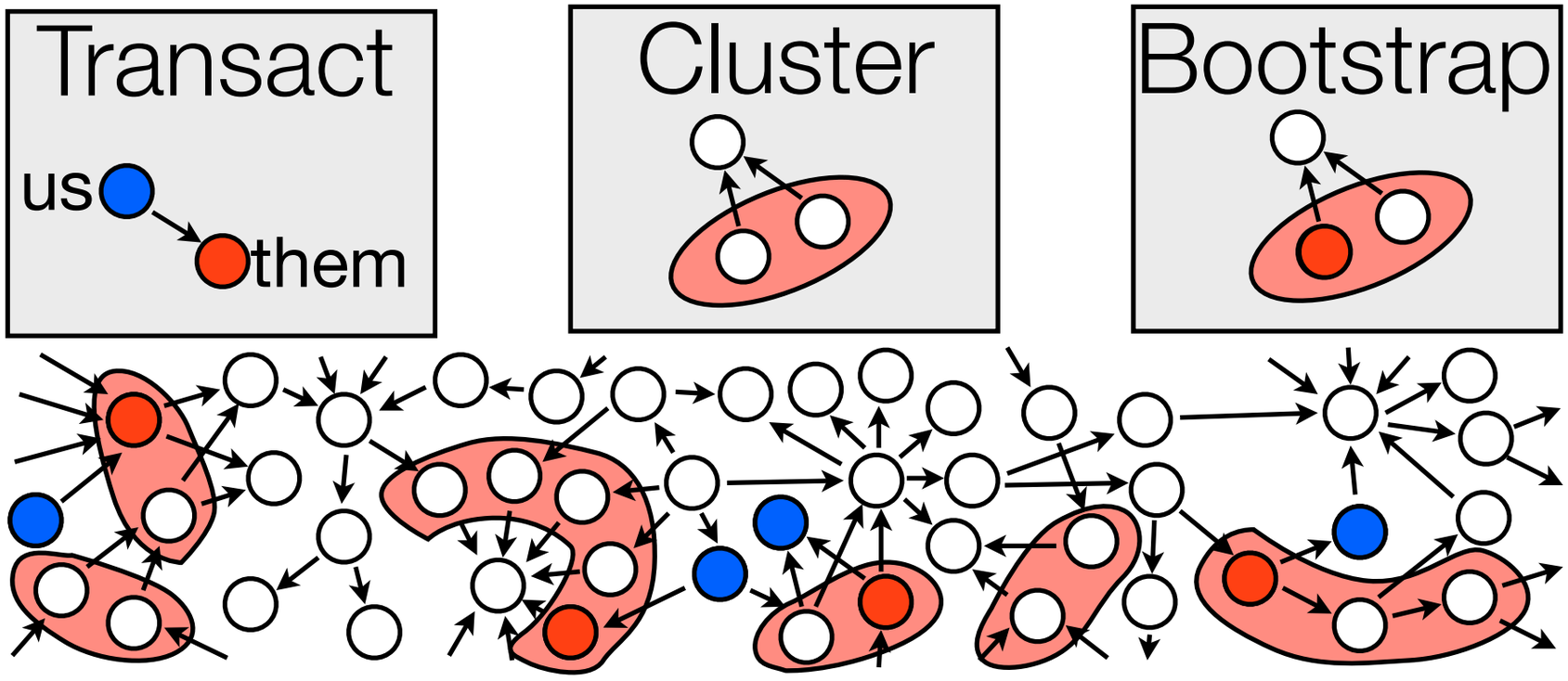
Putting it all together



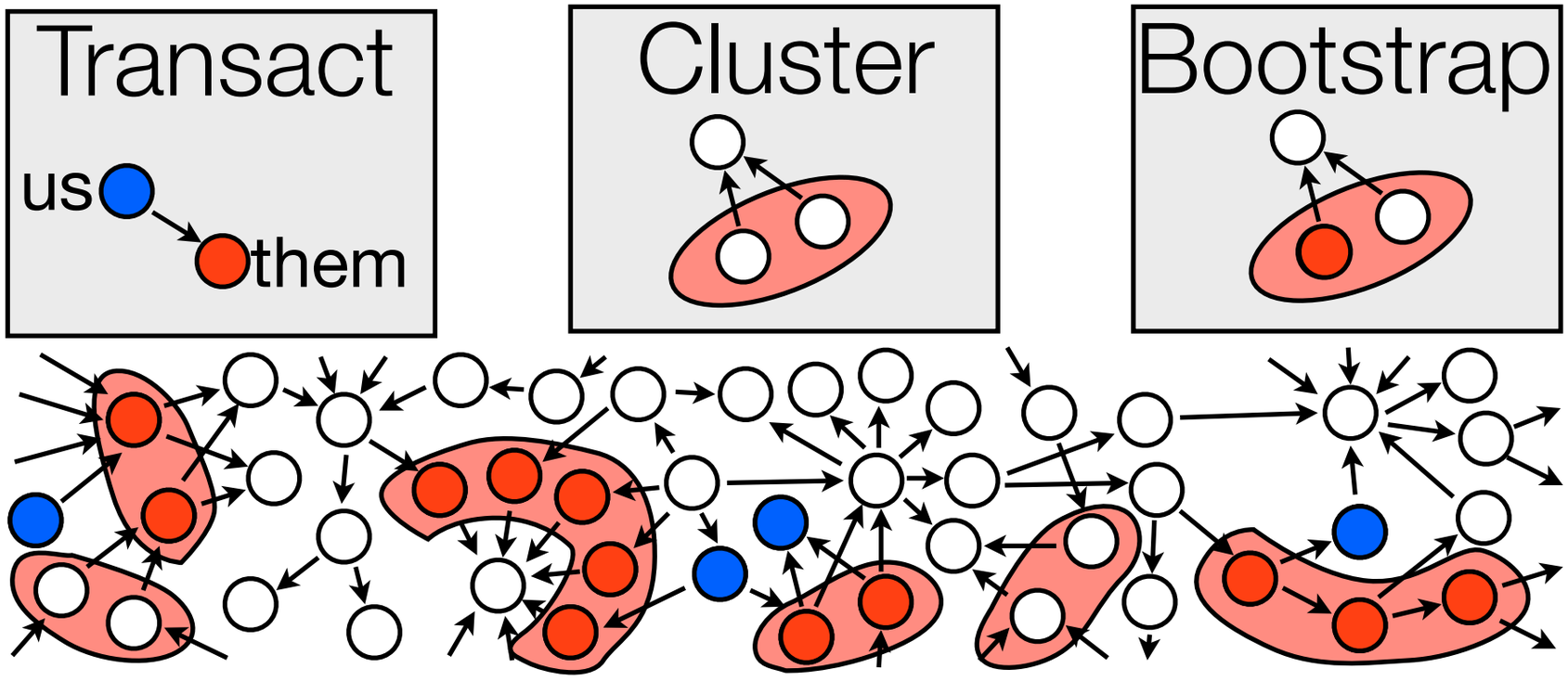
Putting it all together



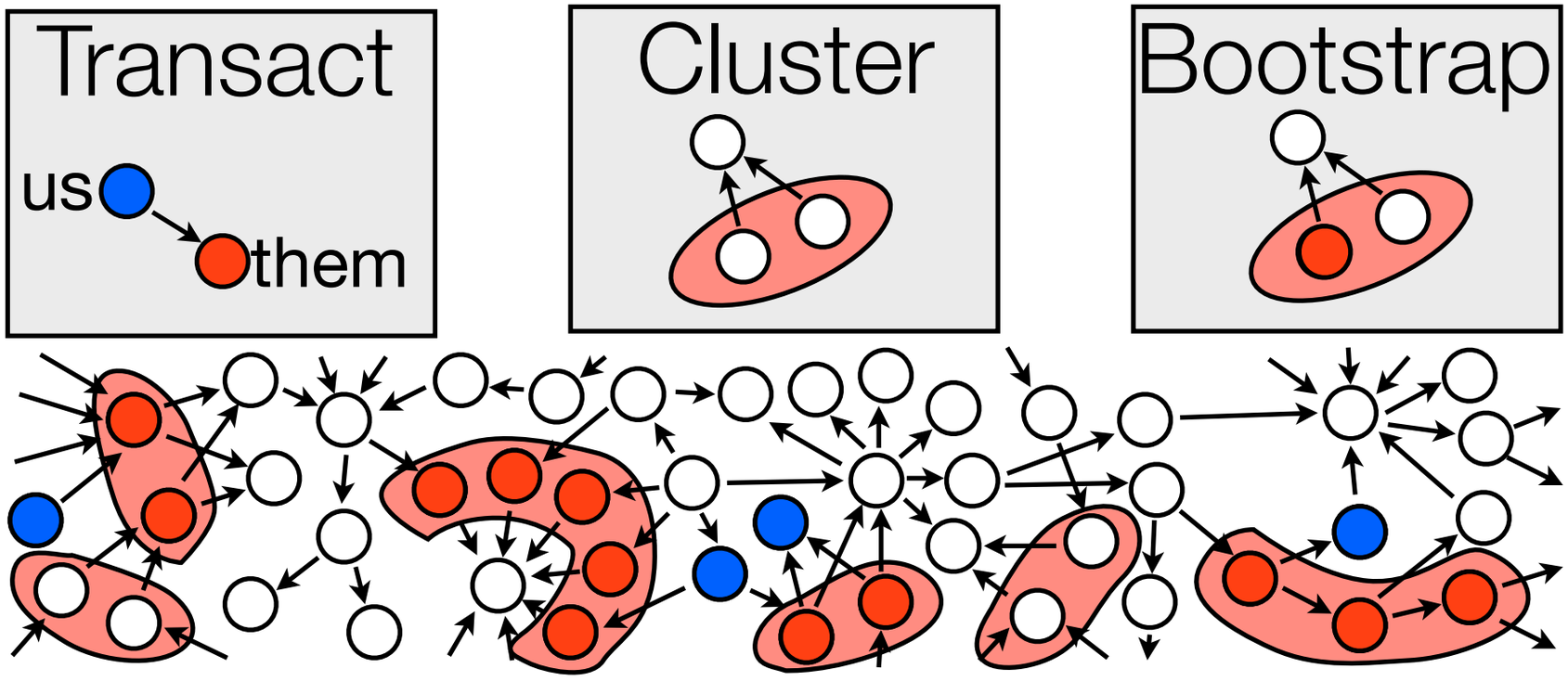
Putting it all together



Putting it all together



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?

Analysis

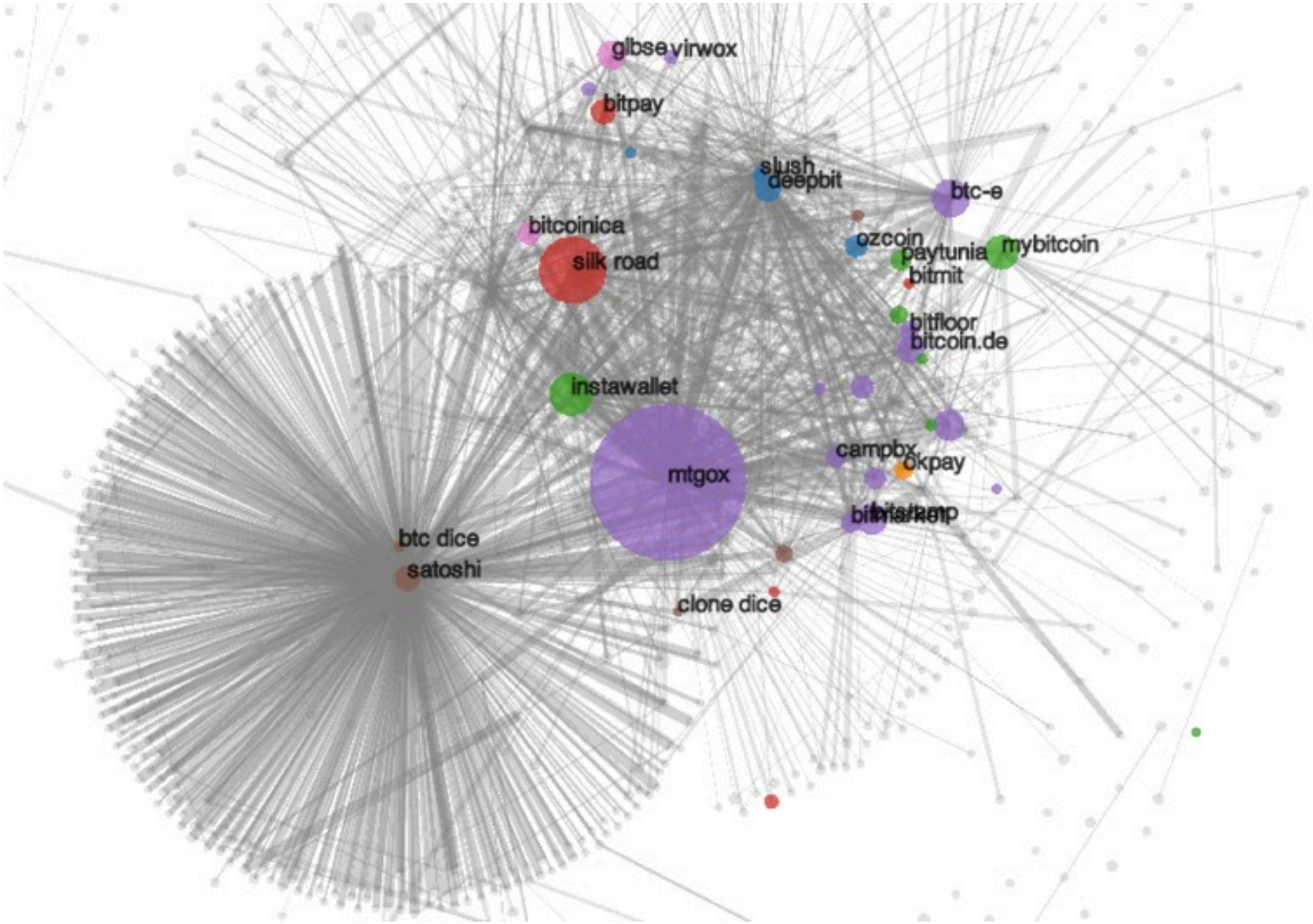
Results

Overall statistics

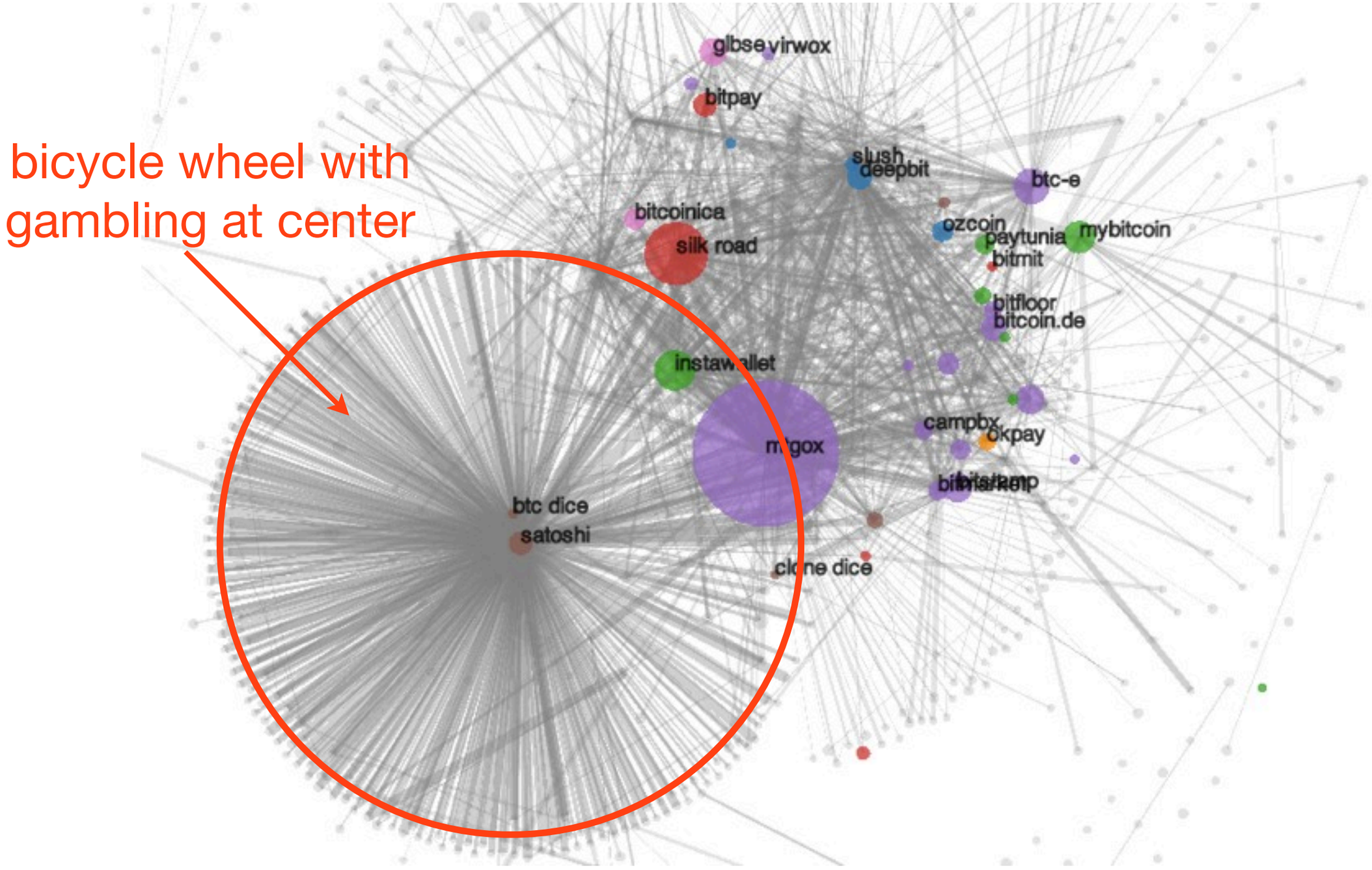
Tracking cluster activity

Conclusions

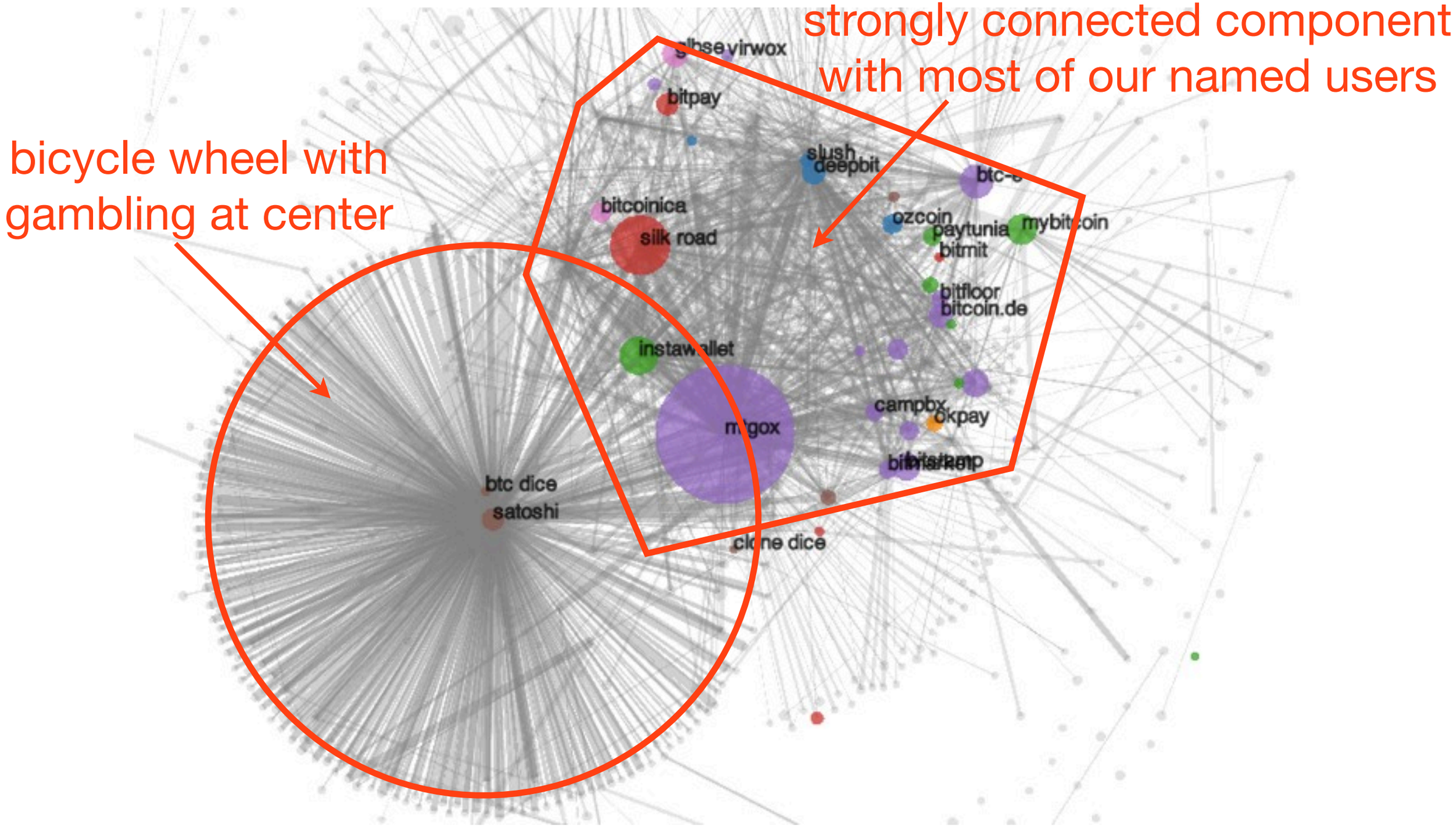
Clustering using our heuristics



Clustering using our heuristics



Clustering using our heuristics



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”

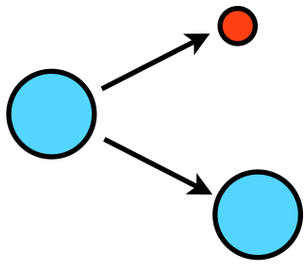
Following bitcoins

Can see when bitcoins meaningfully cross cluster boundaries

1422qjdwv69rU4vuXFe59YktwqWkM6Kgsk (50 BTC - Output)

1GYnR2dWZFsibB8AkjjGKtMNsFCVH6KS21 - (Spent)	48.8325 BTC
1AF2149tLJXQ3JGDpe8gjfrUmmqA9kLNFC - (Unspent)	1.167 BTC

Allows us to systematically follow “peeling chains”



Following bitcoins

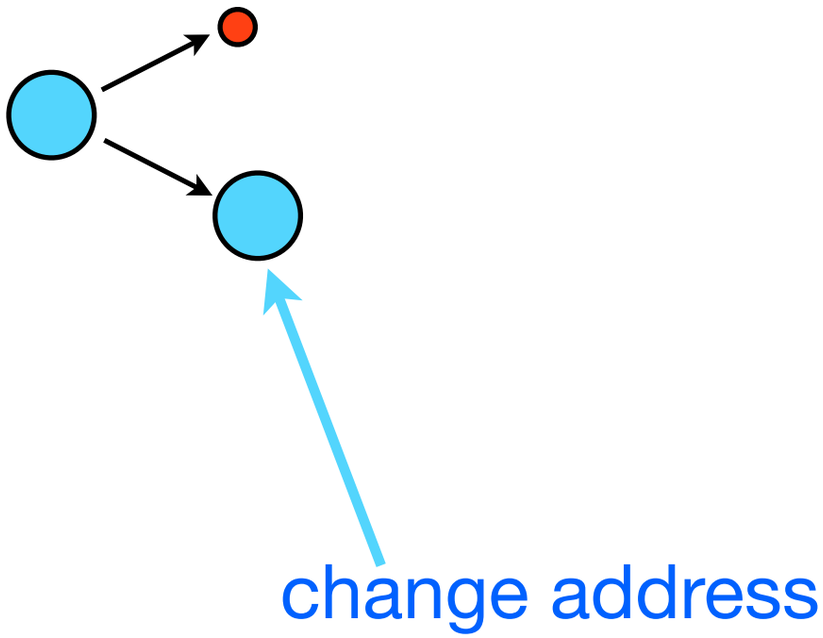
Can see when bitcoins meaningfully cross cluster boundaries

1422qjdwv69rU4vuXFe59YktwqWkM6Kgsk (50 BTC - Output)

1GYnR2dWZFsibB8AkjjGKtMNsFCVH6KS21 - (Spent) 48.8325 BTC

1AF2149tLJXQ3JGDpe8gjfrUmmqA9kLNFC - (Unspent) 1.167 BTC

Allows us to systematically follow "peeling chains"



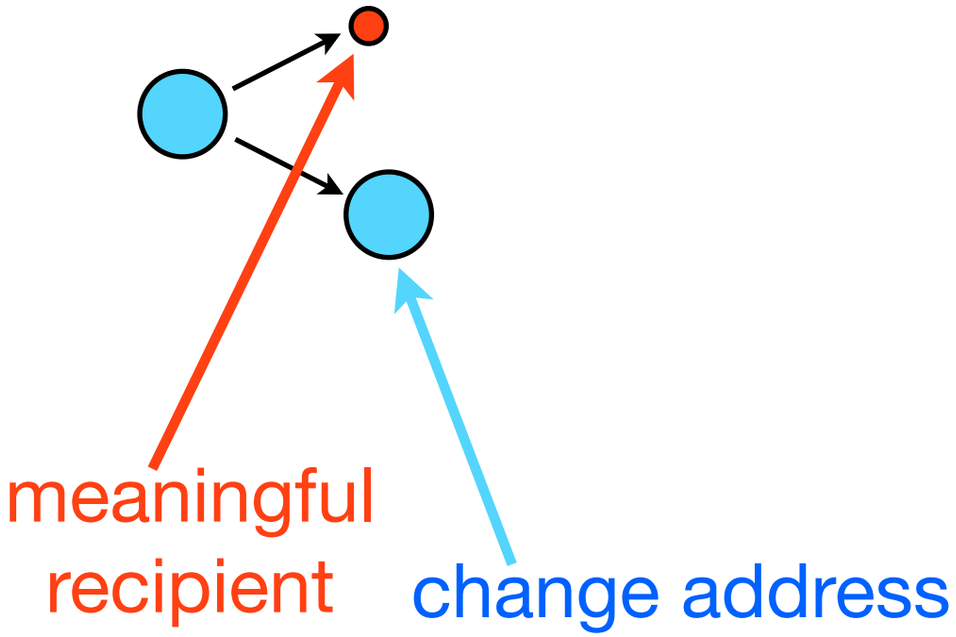
Following bitcoins

Can see when bitcoins meaningfully cross cluster boundaries

1422qjdwv69rU4vuXFe59YktwqWkM6Kgsk (50 BTC - Output)

1GYnR2dWZFsibB8AkjjGKtMNsFCVH6KS21 - (Spent)	48.8325 BTC
1AF2149tLJXQ3JGDpe8gjfrUmmqA9kLNFC - (Unspent)	1.167 BTC

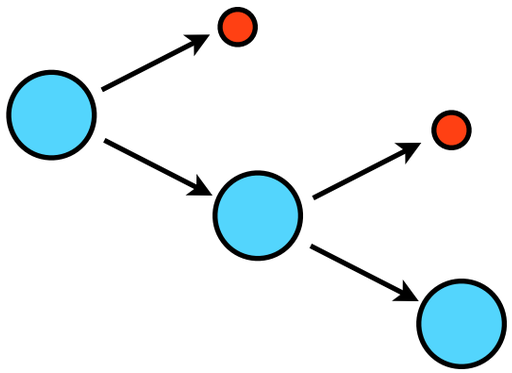
Allows us to systematically follow "peeling chains"



Following bitcoins

Can see when bitcoins meaningfully cross cluster boundaries

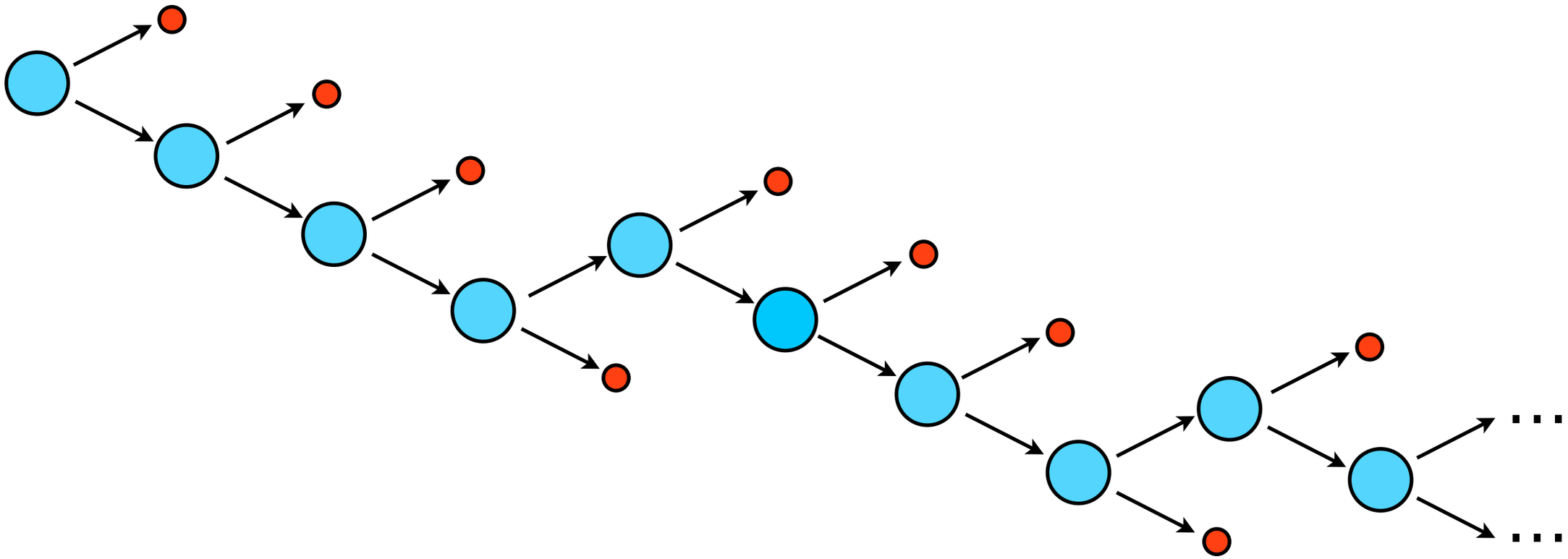
Allows us to systematically follow “peeling chains”



Following bitcoins

Can see when bitcoins meaningfully cross cluster boundaries

Allows us to systematically follow “peeling chains”



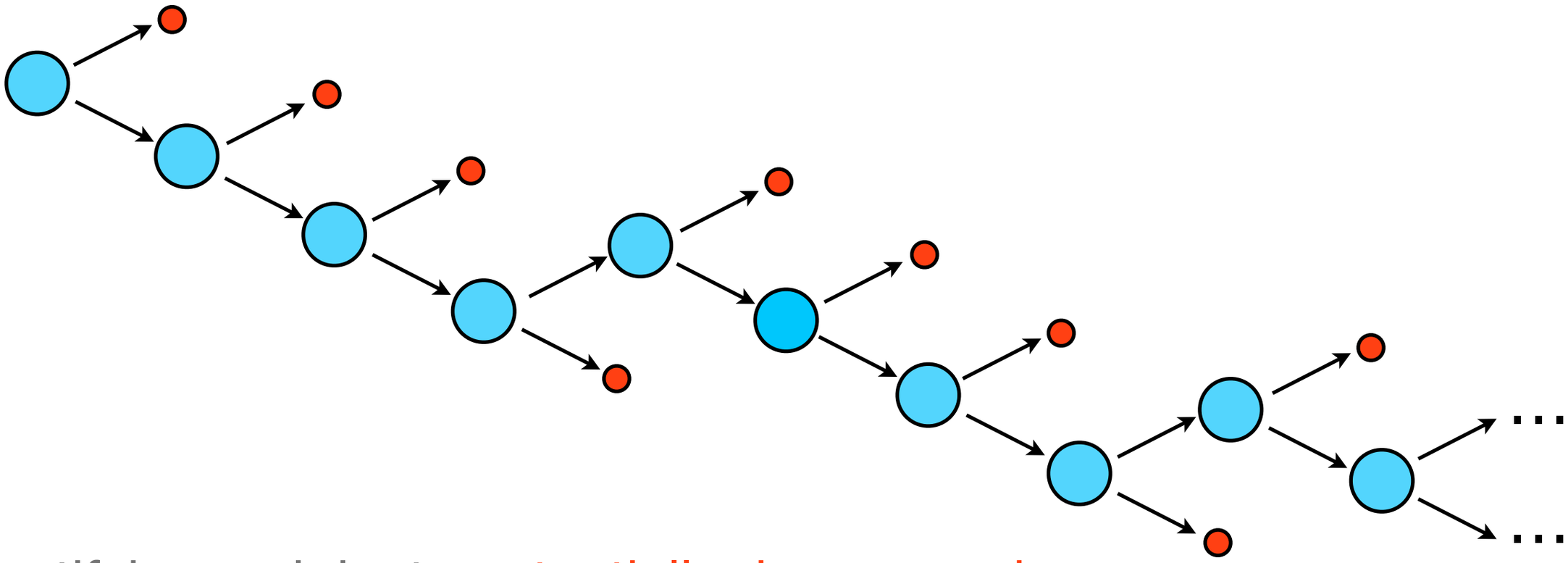
Following bitcoins

Can see when bitcoins meaningfully cross cluster boundaries

1422qjdwv69rU4vuXFe59YktwqWkM6Kgsk (50 BTC - Output)

1GYnR2dWZFsibB8AkjjGKtMNsFCVH6KS21 - (Spent)	48.8325 BTC
1AF2149tLJXQ3JGDpe8gjfrUmmqA9kLNFC - (Unspent)	1.167 BTC

Allows us to systematically follow “peeling chains”



Identifying recipients potentially de-anonymizes user

Tracking illicitly-obtained bitcoins

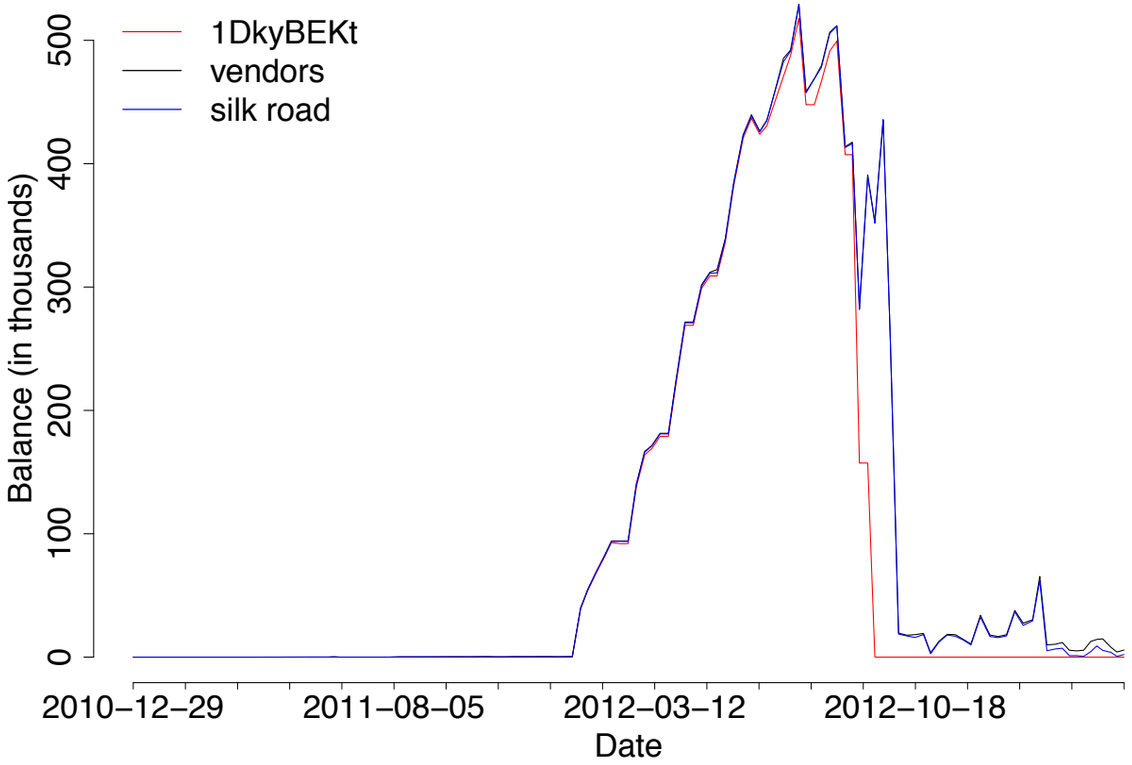
By following peeling chains, we tracked money from known thefts and from one infamous address associated with Silk Road

Tracking illicitly-obtained bitcoins

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

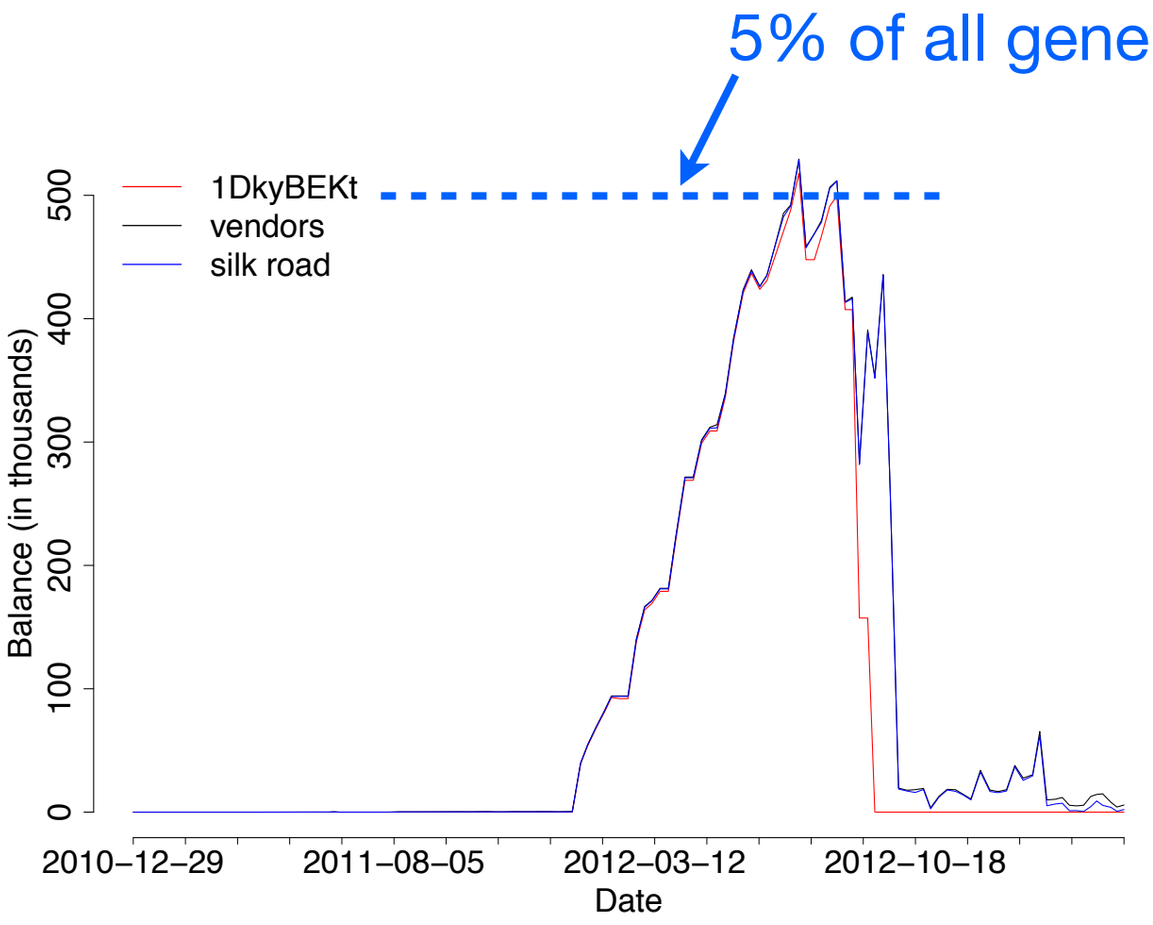
Tracking illicitly-obtained bitcoins

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



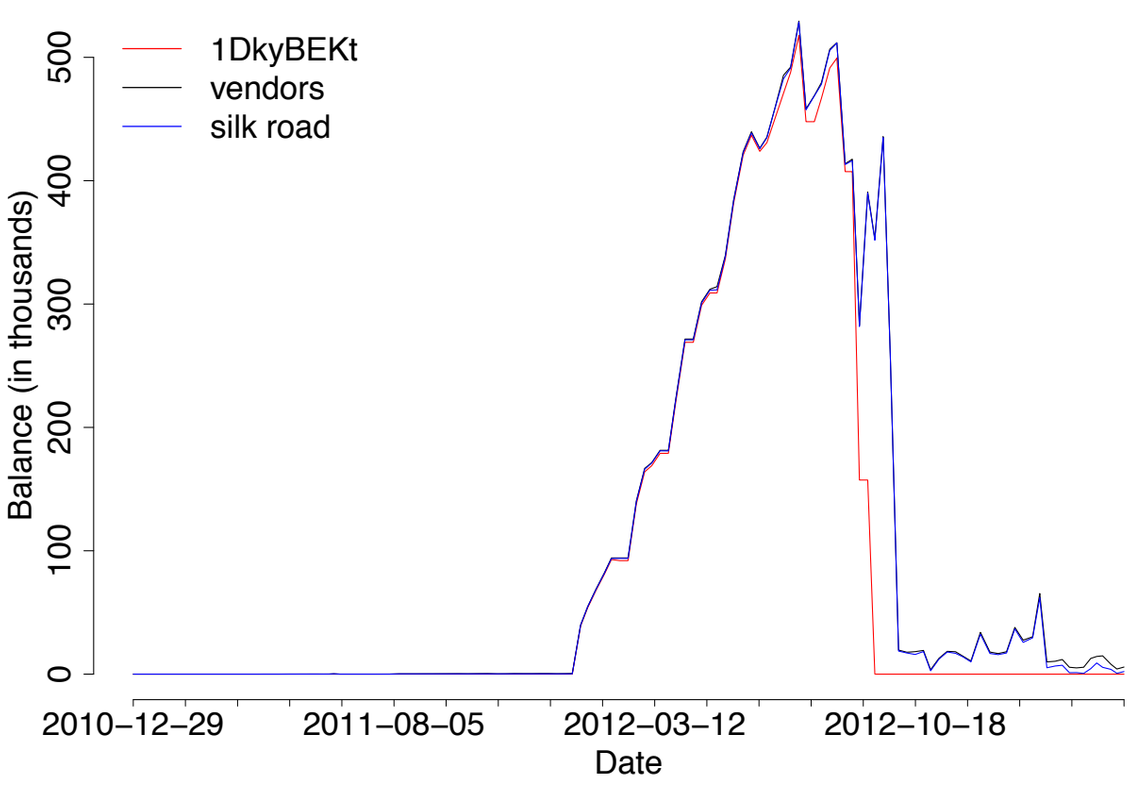
Tracking illicitly-obtained bitcoins

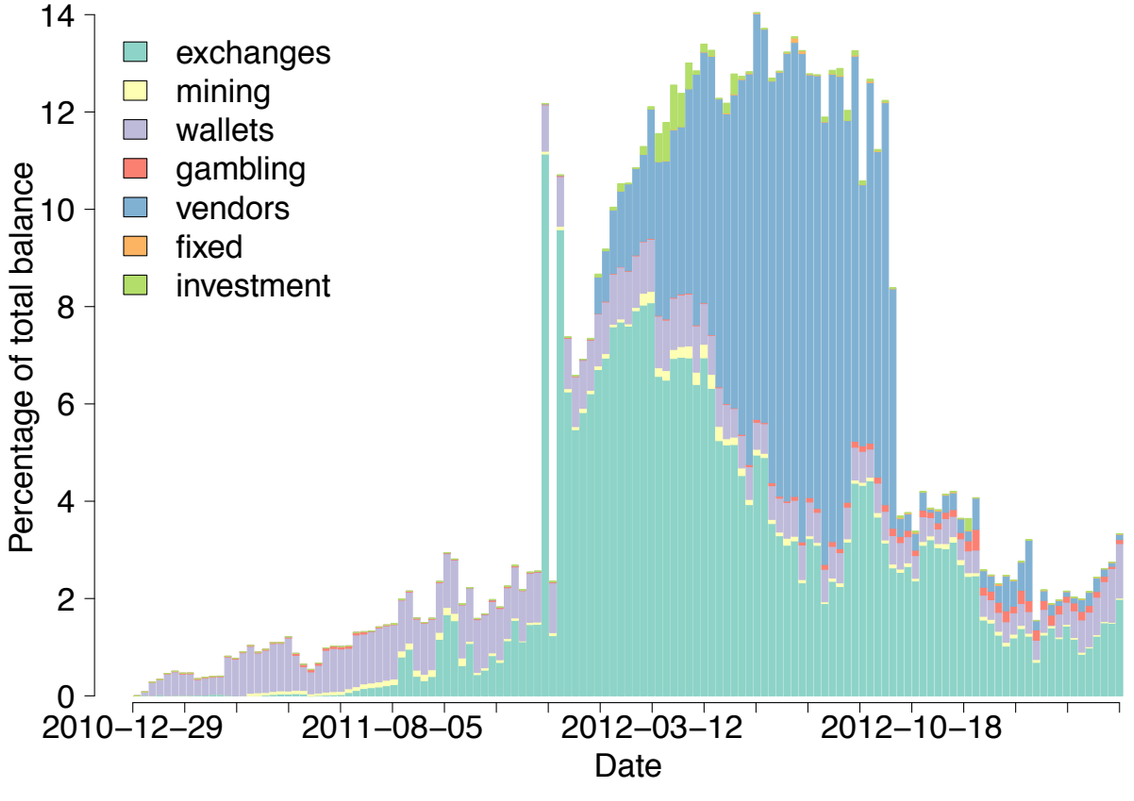
By following peeling chains, we tracked money from known thefts and from one infamous address associated with Silk Road



Tracking illicitly-obtained bitcoins

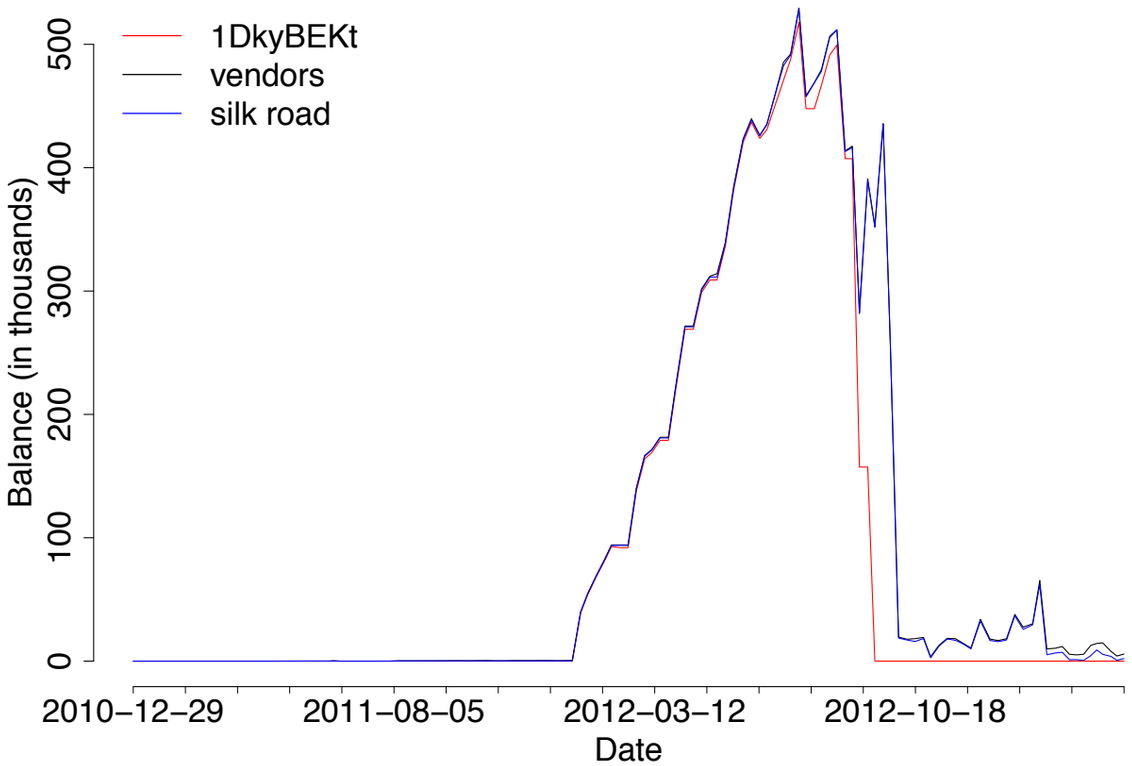
By following peeling chains, we tracked money from known thefts and from one infamous address associated with Silk Road



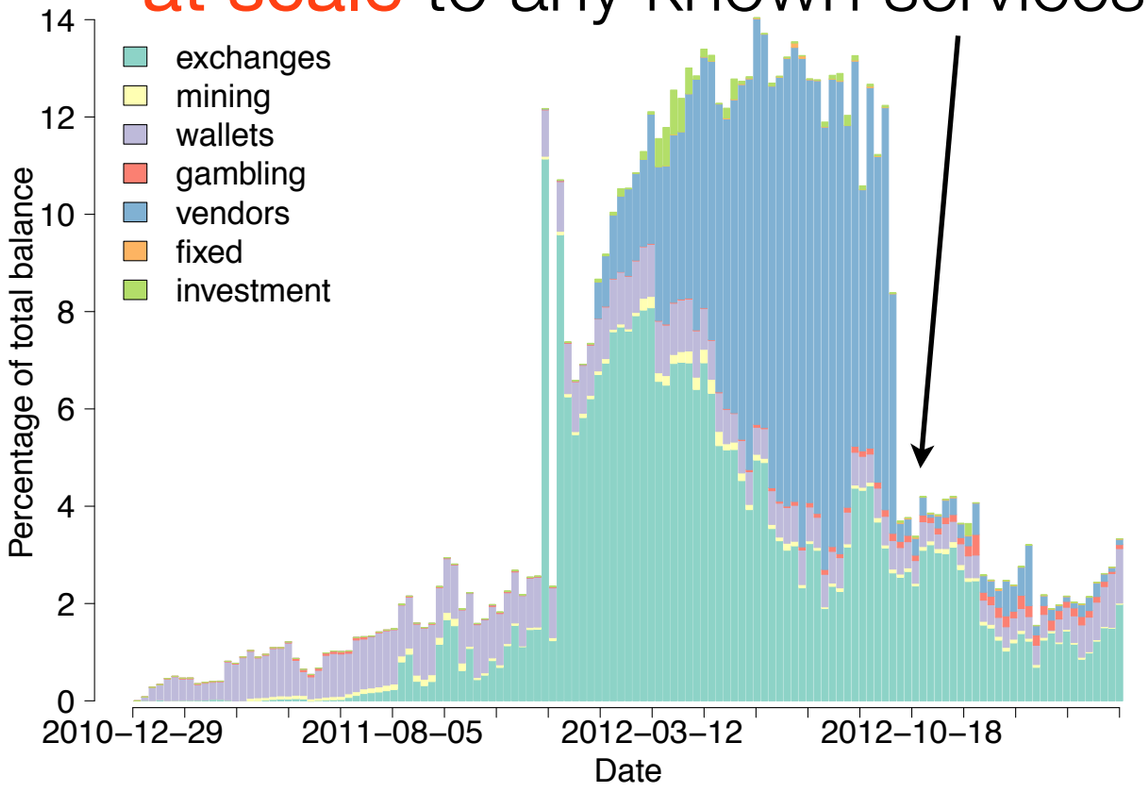


Tracking illicitly-obtained bitcoins

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

	First		Second		Third	
Service	Peels	BTC	Peels	BTC	Peels	BTC
Bitcoin-24			1	2	3	124
Bitcoin Central					2	2
Bitcoin.de					1	4
Bitmarket					1	1
Bitstamp			5	97	1	1
BTC-e					1	250
CA VirtEx	1	3	1	10	3	22
Mercado Bitcoin					1	9
Mt. Gox	11	492	14	70	5	35
OKPay	2	151			1	125

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

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

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

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

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

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

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

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

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

Andy Greenberg, Forbes Staff

Covering the worlds of data security, privacy and hacker culture.

+ Follow (1,142)

SECURITY | 9/05/2013 @ 10:36AM | 131,694 views

Follow The Bitcoins: How We Got Busted Buying Drugs On Silk Road's Black Market

Tracking bitcoins in the real world

Contacted by Andy Greenberg of Forbes to test hypothesis

Got Coinbase addresses; asked to identify drug purchases

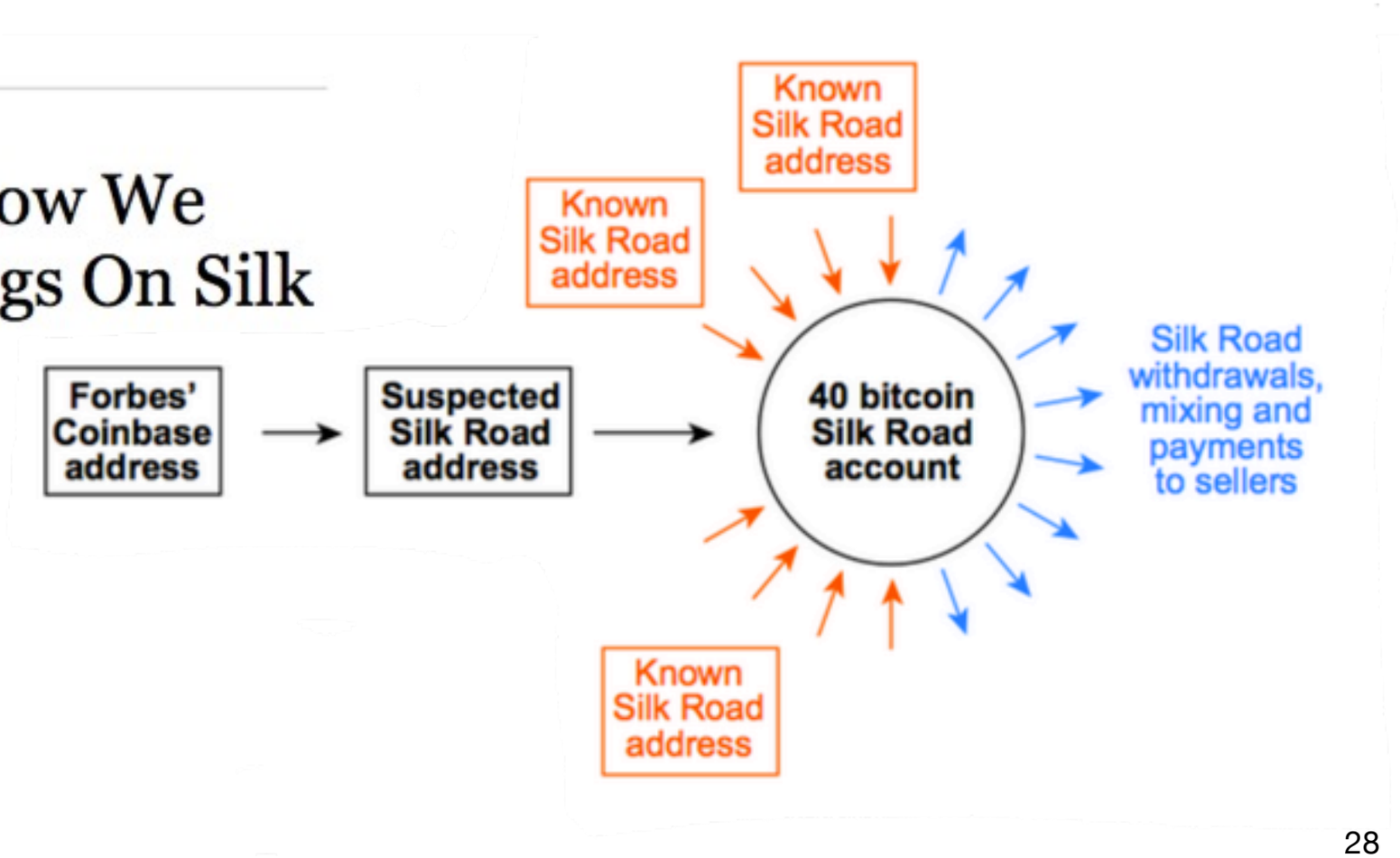
Andy Greenberg, Forbes Staff

Covering the worlds of data security, privacy and hacker culture.

+ Follow (1,142)

SECURITY | 9/05/2013 @ 10:36AM | 131,694 views

Follow The Bitcoins: How We Got Busted Buying Drugs On Silk Road's Black Market



Outline

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?