

Privacy-Enhancing Overlays in Bitcoin

Sarah Meiklejohn (University College London)

Claudio Orlandi (Aarhus University)

Anonymity in Bitcoin

Anonymity in Bitcoin

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

Anonymity in Bitcoin

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

Ponzi-Scheme Charge Is Good News for Bitcoin

Anonymity in Bitcoin

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

Ponzi-Scheme Charge Is Good News for Bitcoin

**Estimated 18 percent of US drug users
bought from Silk Road, says study**

Anonymity in Bitcoin

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

Ponzi-Scheme Charge Is Good News for Bitcoin

**Estimated 18 percent of US drug users
bought from Silk Road, says study**

How much anonymity does Bitcoin really provide?

Outline

Outline

Background

Outline

Background

Taint resistance

Outline

Background

Taint resistance

Achieving taint resistance

Outline

Background

Taint resistance

Achieving taint resistance

Conclusions

Outline

Background

How Bitcoin works
Anonymity in Bitcoin
Coinjoin

Taint resistance

Achieving taint resistance

Conclusions

How Bitcoin works

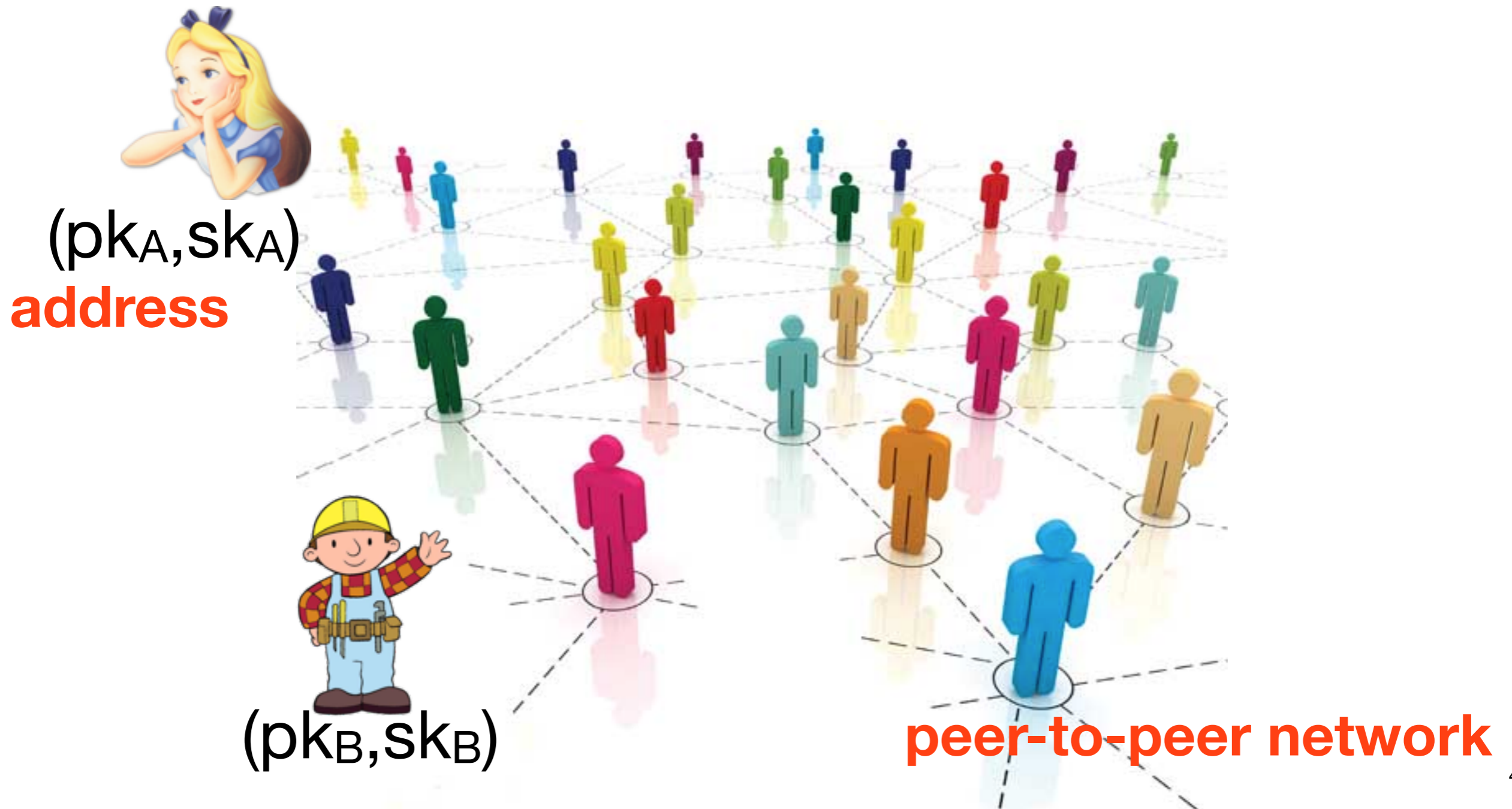
How Bitcoin works



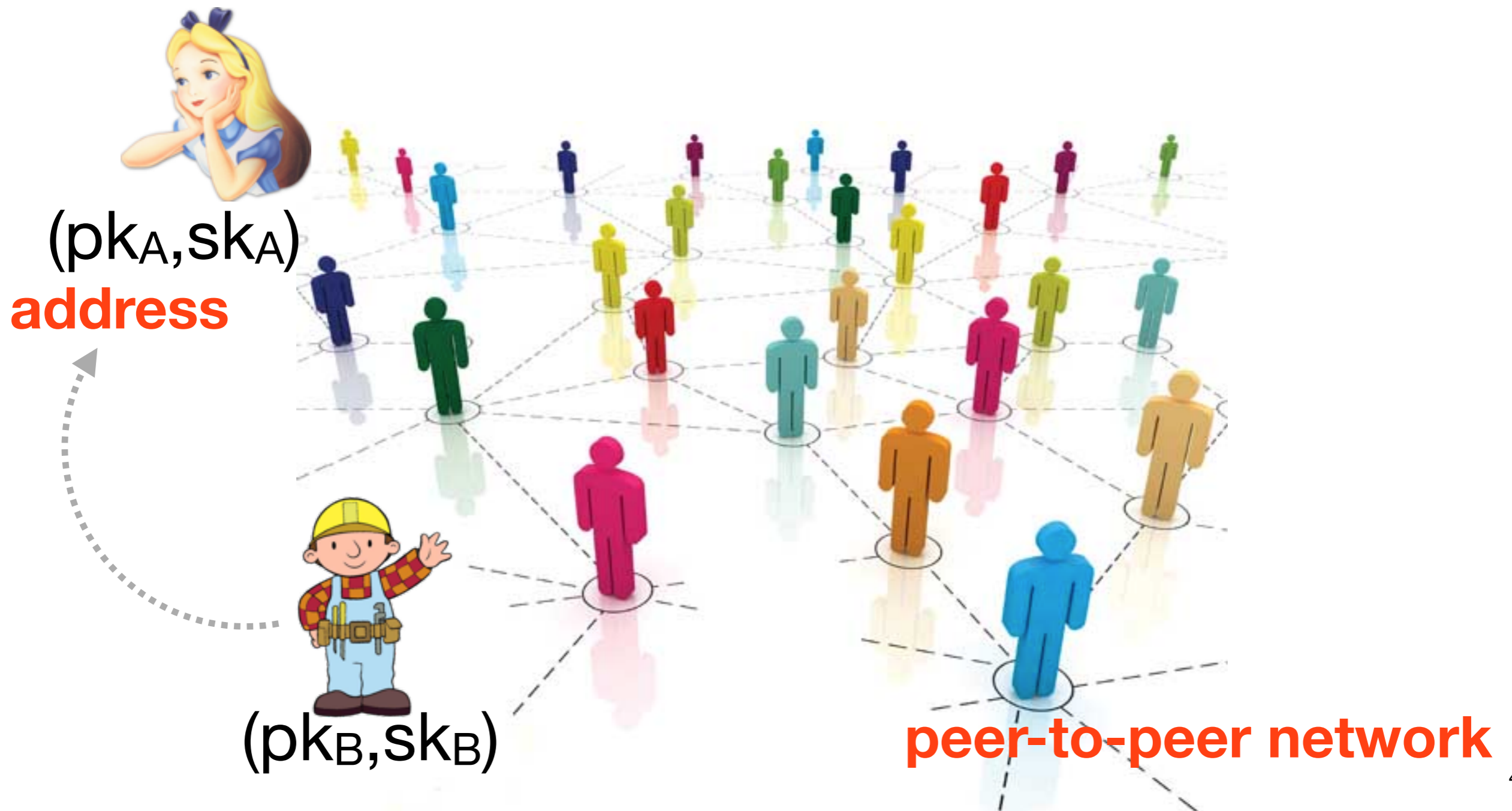
How Bitcoin works



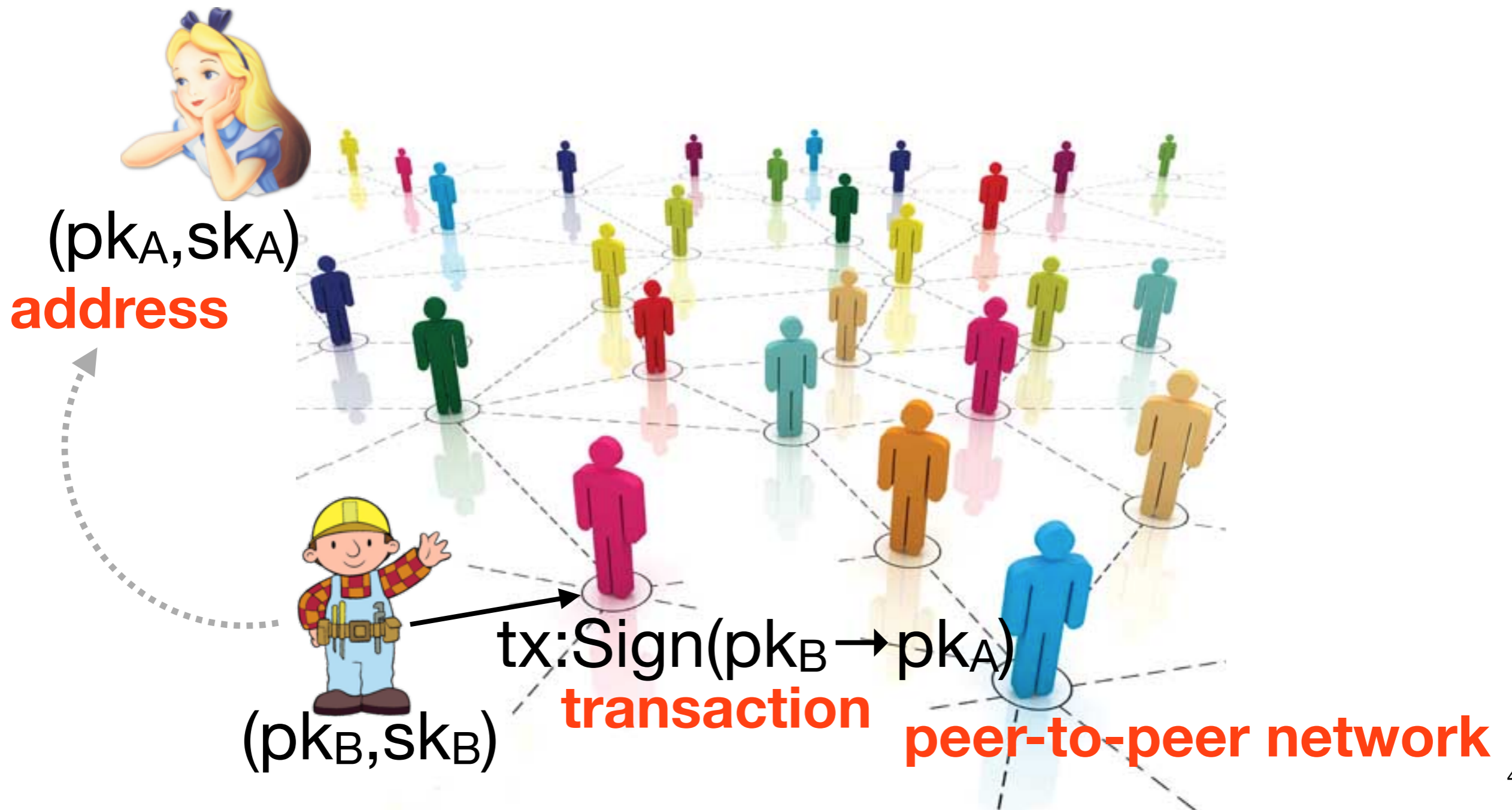
How Bitcoin works



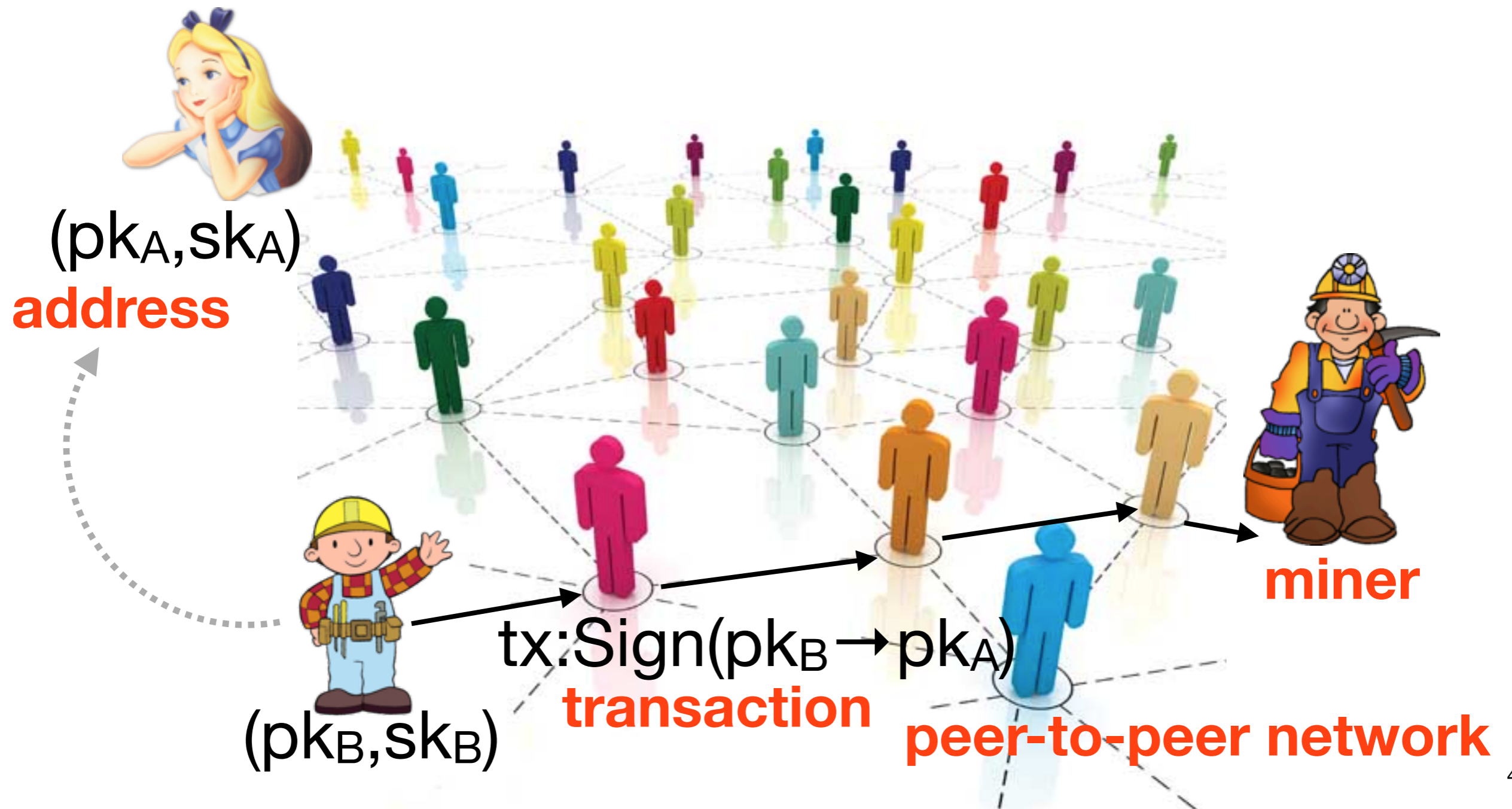
How Bitcoin works



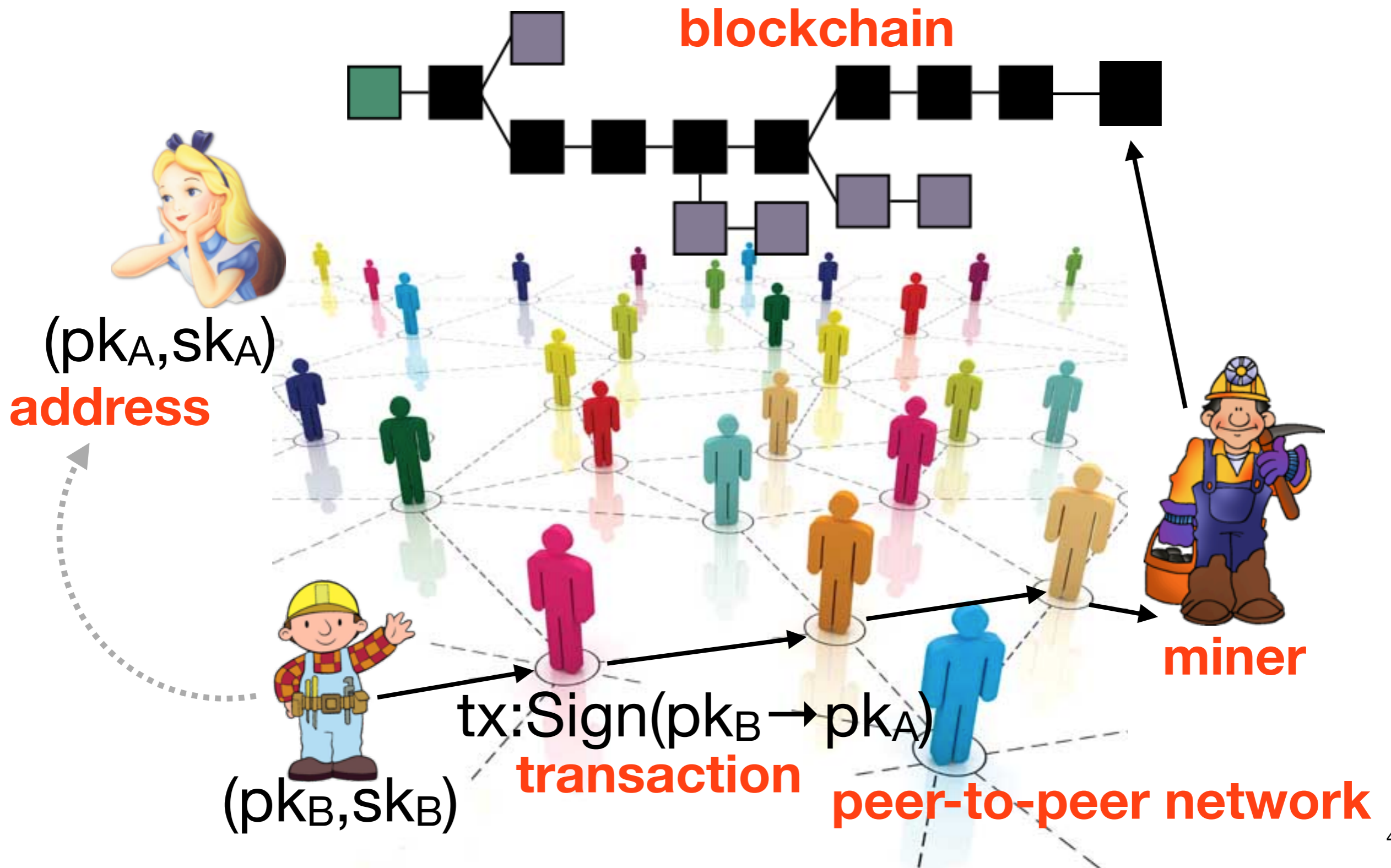
How Bitcoin works



How Bitcoin works



How Bitcoin works



Anonymity in Bitcoin

How much anonymity does Bitcoin really provide?

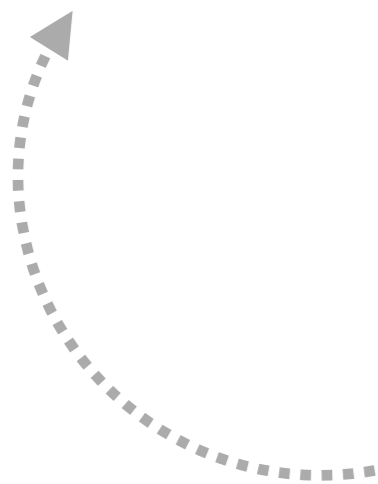


(pk_A, sk_A)

address



(pk_B, sk_B)



Anonymity in Bitcoin

How much anonymity does Bitcoin really provide?



in theory, a lot! addresses are not linked to identity

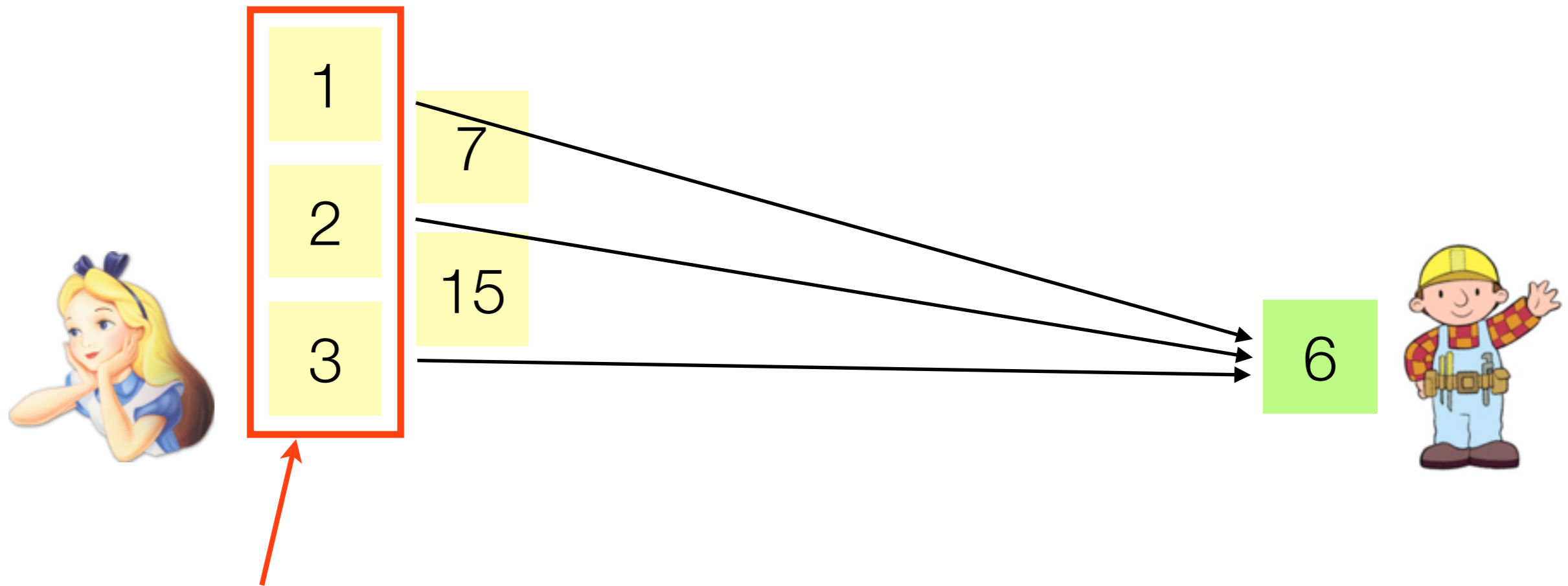
(pk_A, sk_A)

address



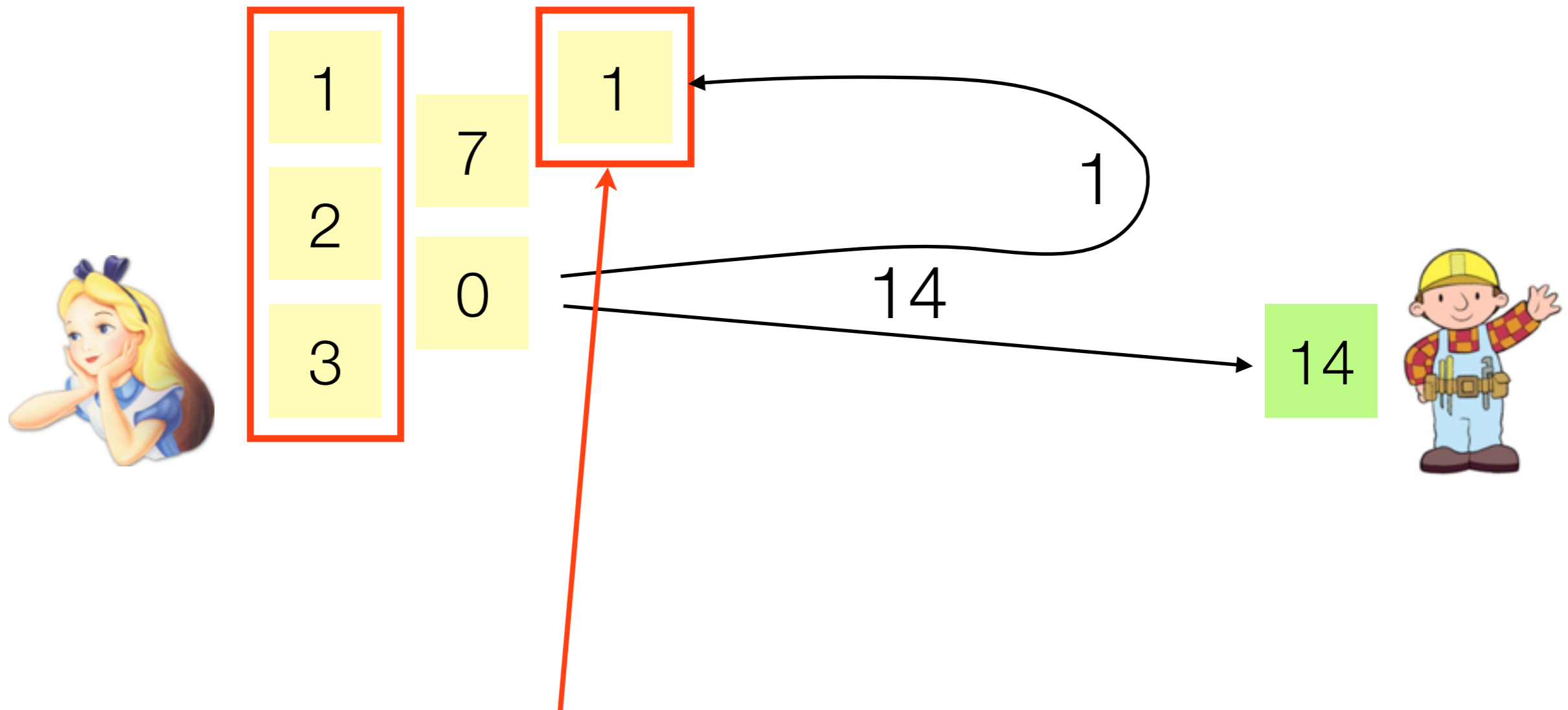
(pk_B, sk_B)

Input clustering [RH13,RS13,A+13,**M**+13,SMZ14]



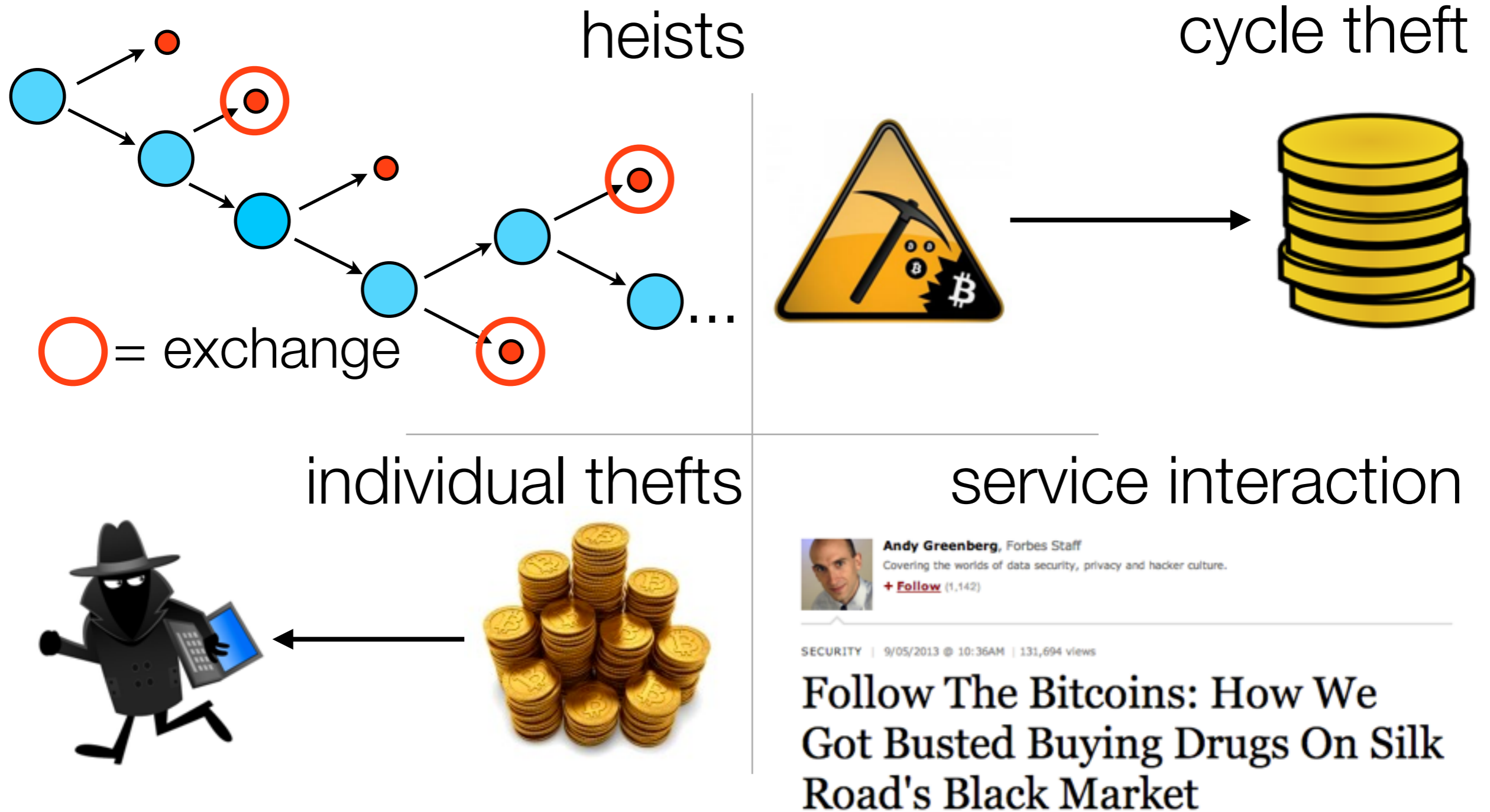
Heuristic: the same user controls these addresses

Change clustering [A+13, **M**+13, SMZ14]



Heuristic: the same user also controls this address

Tracking technique [M+13, HDM+14]



Tracking technique [M+13,HDM+14]



Prosecutors Trace \$13.4M in Bitcoins From the Silk Road to Ulbricht's Laptop

If anyone still believes that bitcoin is magically anonymous internet money, the US government just offered what may be the clearest demonstration yet that it's not.



+ 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

Anonymity in Bitcoin

How much anonymity does Bitcoin really provide?

in theory, a lot! addresses are not linked to identity

in practice, maybe not so much

Privacy-enhancing overlays

Privacy-enhancing overlays

Mixcoin

Anonymity for Bitcoin with accountable mixes
(Full version)

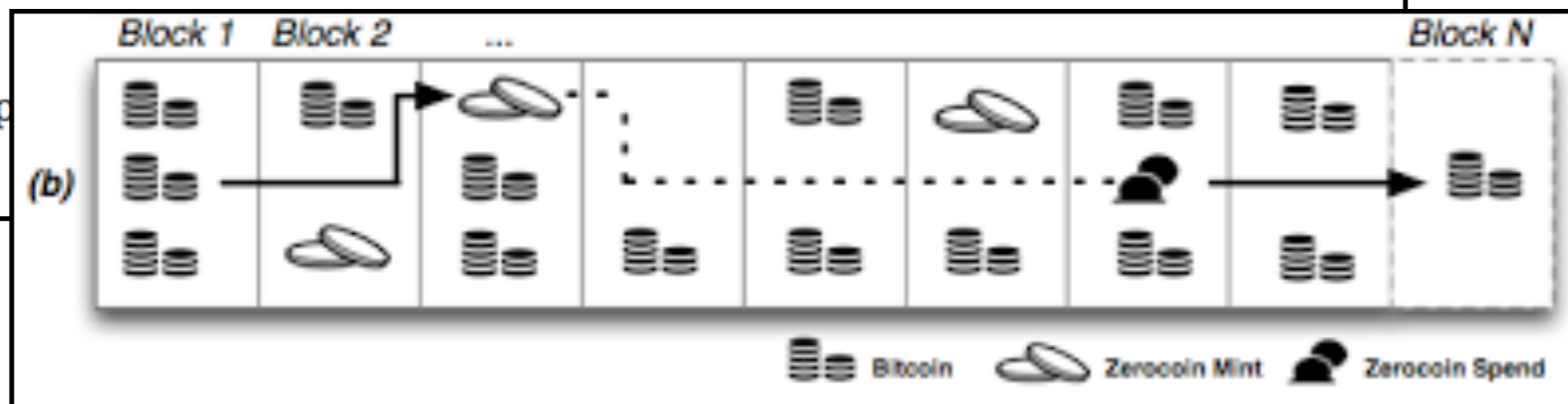
Joseph Bonneau¹, Arvind Narayanan¹, Andrew Miller², Jeremy Clark³, and
Joshua A. Kroll¹ and Edward W. Felten¹

Privacy-enhancing overlays

Mixcoin

Anonymity for Bitcoin with accountable mixes
(Full version)

Josep



Privacy-enhancing overlays

Mixcoin

Anonymity for Bitcoin with accountable mixes
(Full version)



Destination Address Anonymization in Bitcoin

Privacy-enhancing overlays

Mixcoin

Anonymity for Bitcoin with accountable mixes
(Full version)



Destination Address Anonymization in Bitcoin



CoinSwap: Transaction graph disjoint trustless trading

October 30, 2013, 06:43:42 AM

Privacy-enhancing overlays

Mixcoin

Anonymity for Bitcoin with accountable mixes
(Full version)



Destination Address Anonymization in Bitcoin



CoinSwap: Transaction graph disjoint trustless trading

October 30, 2017

CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin*

Tim Ruffing, Pedro Moreno-Sanchez, and Aniket Kate

Privacy-enhancing overlays

Mixcoin

Anonymity for Bitcoin with accountable mixes
(Full version)



Destination Address Anonymization in Bitcoin



CoinSwap: Transaction graph disjoint trustless trading

October 30, 2014

CoinShuffle: Practical Decentralized

Blindcoin

Blinded, Accountable Mixes for Bitcoin

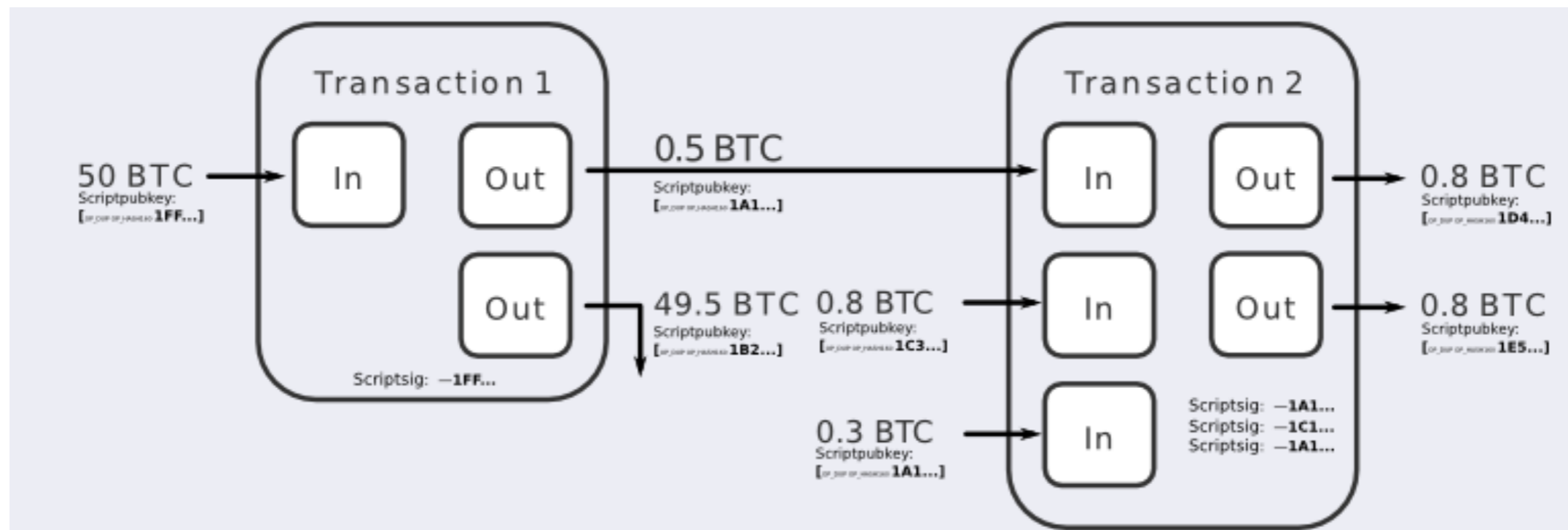
Tim

Luke Valenta¹ and Brendan Rowan² *

Coinjoin

Introduced on August 22 2013 by Gregory Maxwell

“Bitcoin privacy for the real world”



Coinjoin



1

2



3



Coinjoin

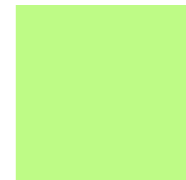


1

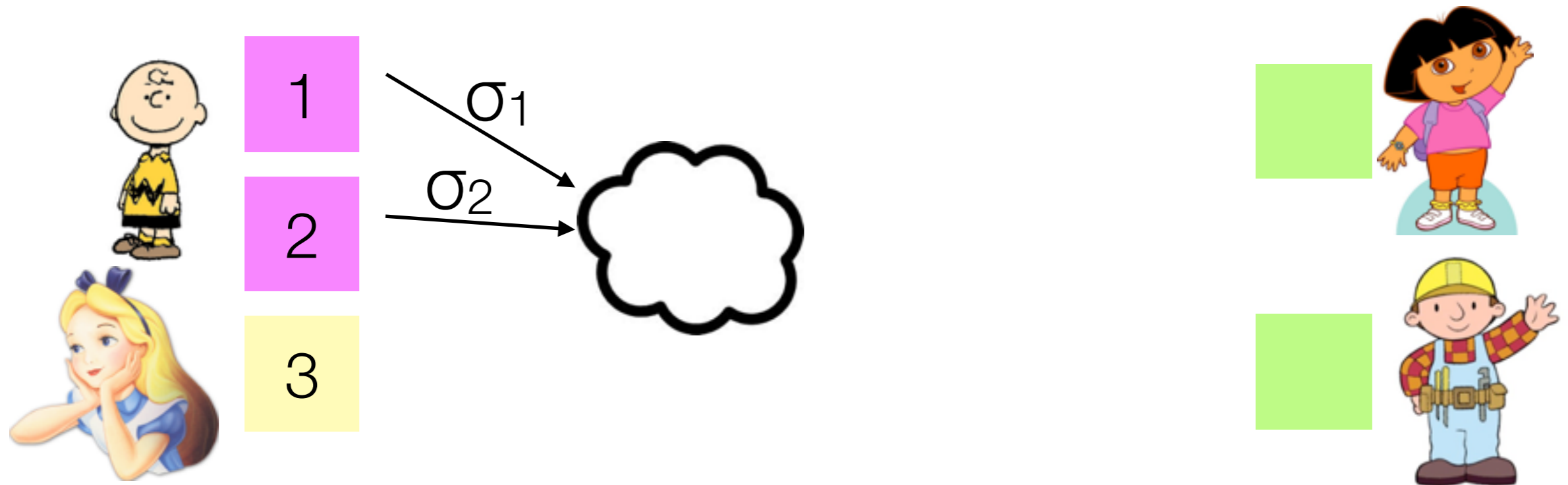
2



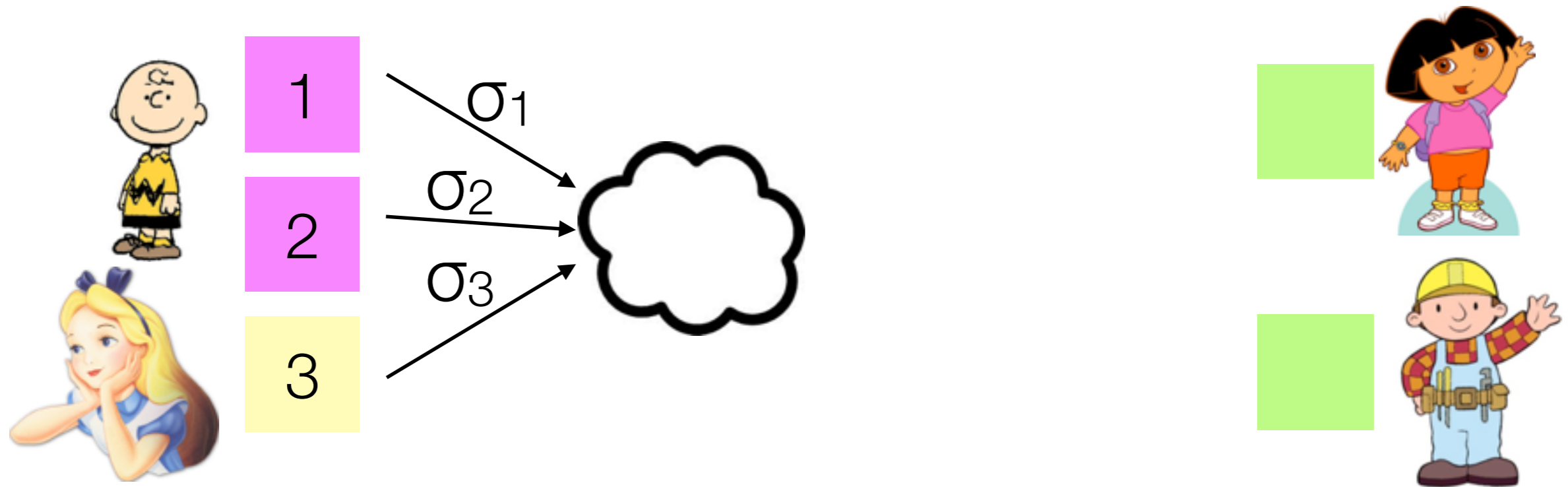
3



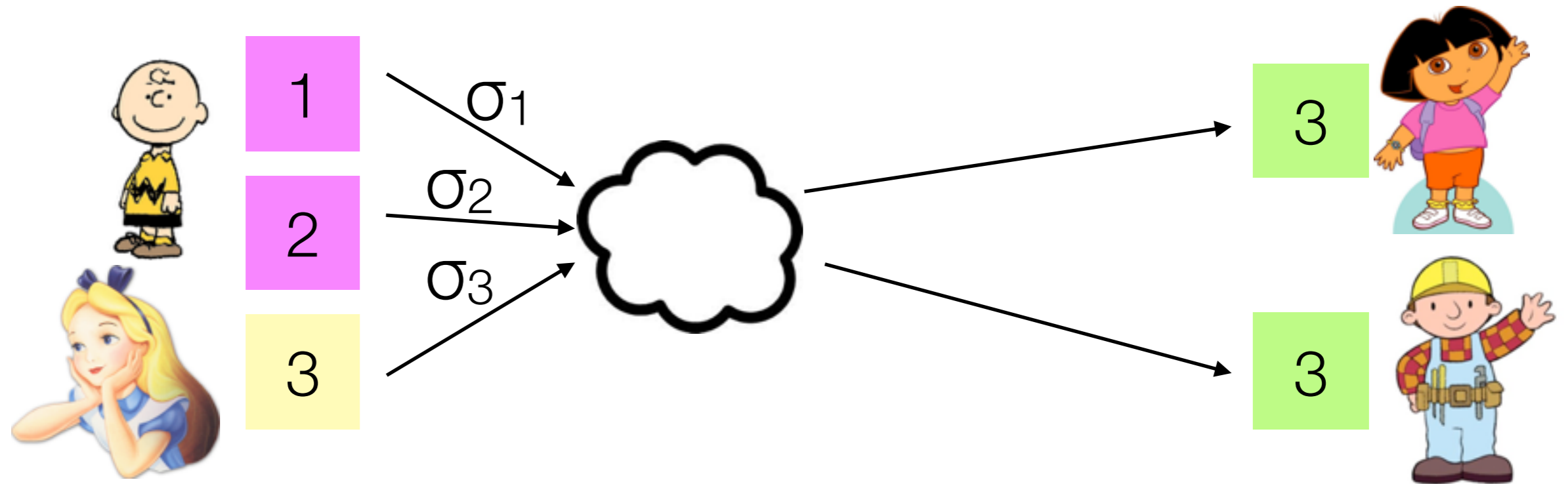
Coinjoin



Coinjoin

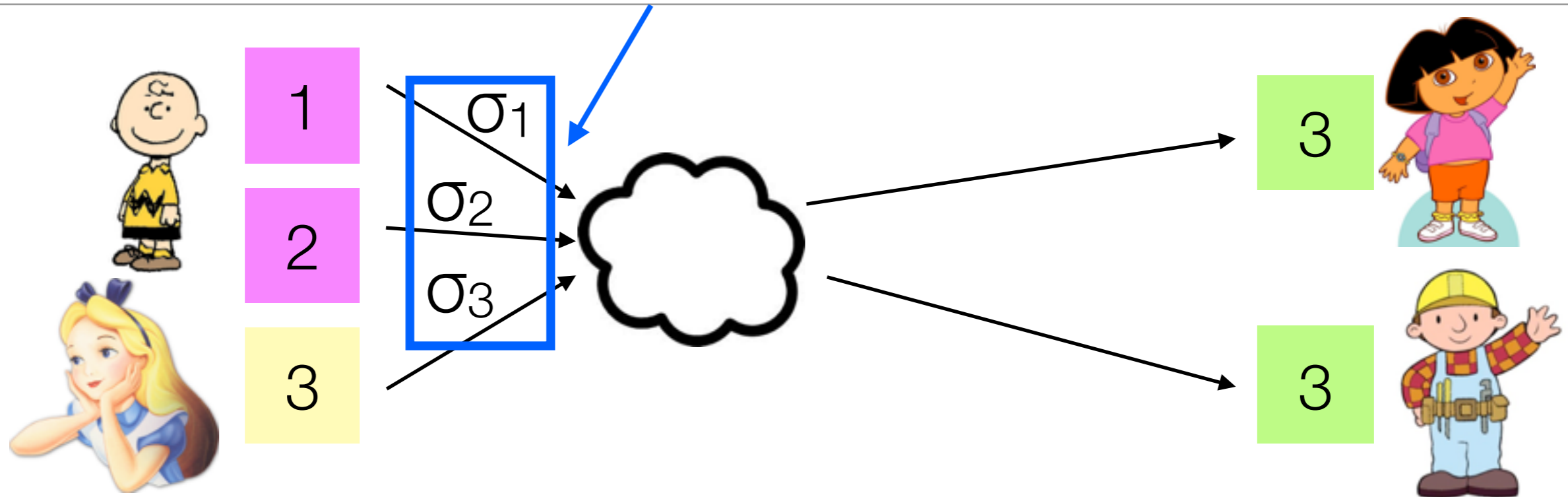


Coinjoin

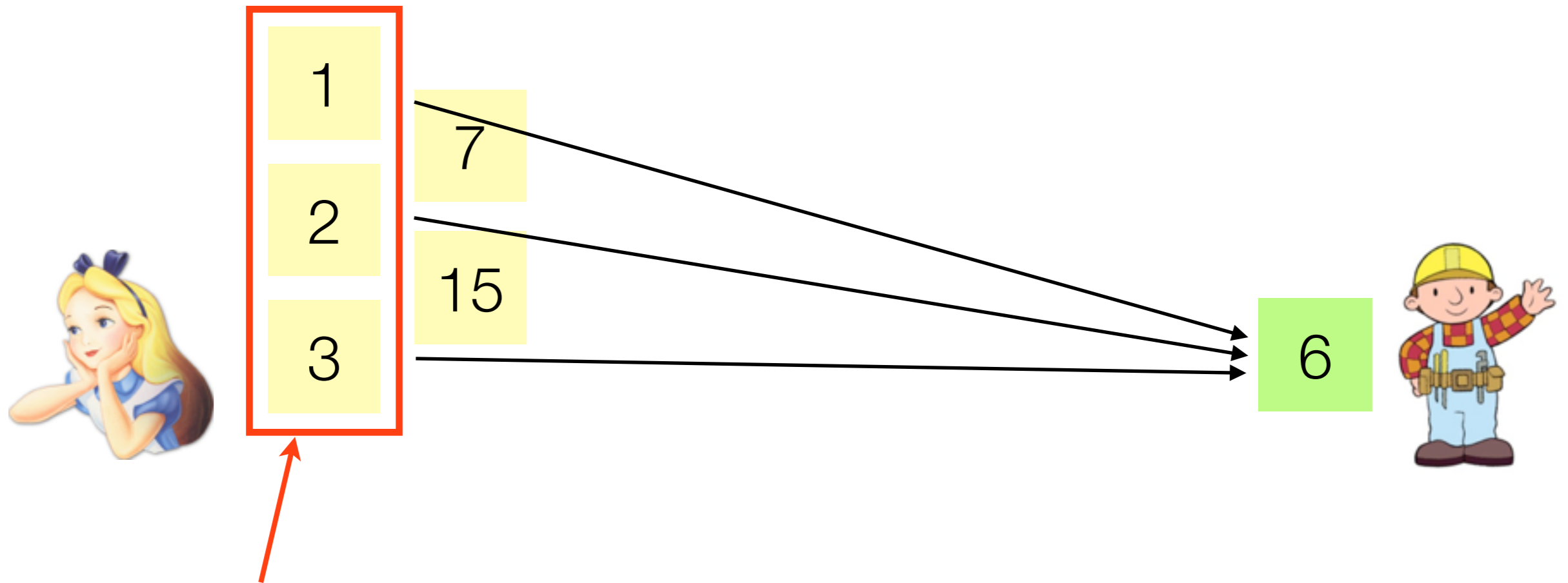


Coinjoin

signatures contributed separately

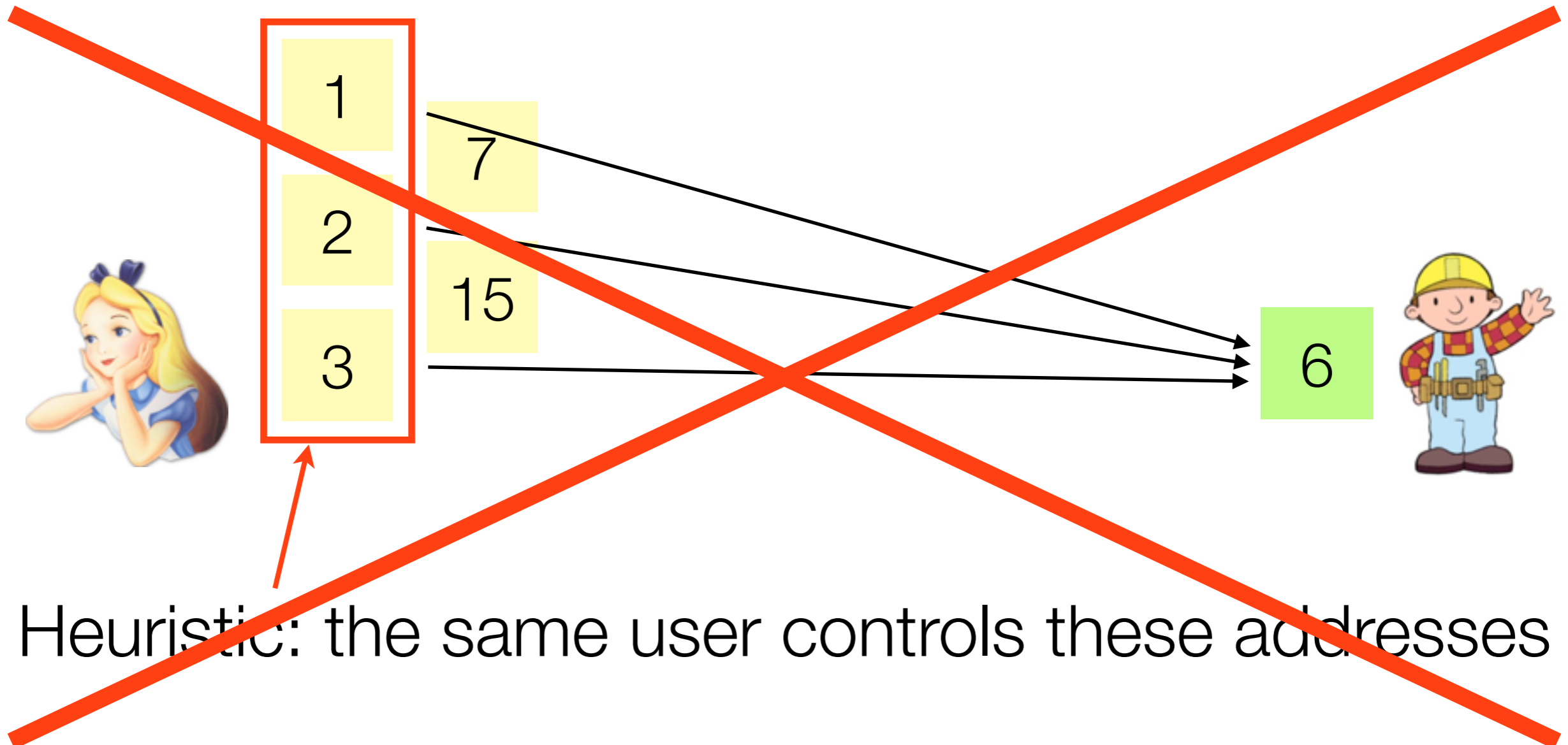


Coinjoin prevents clustering



Heuristic: the same user controls these addresses

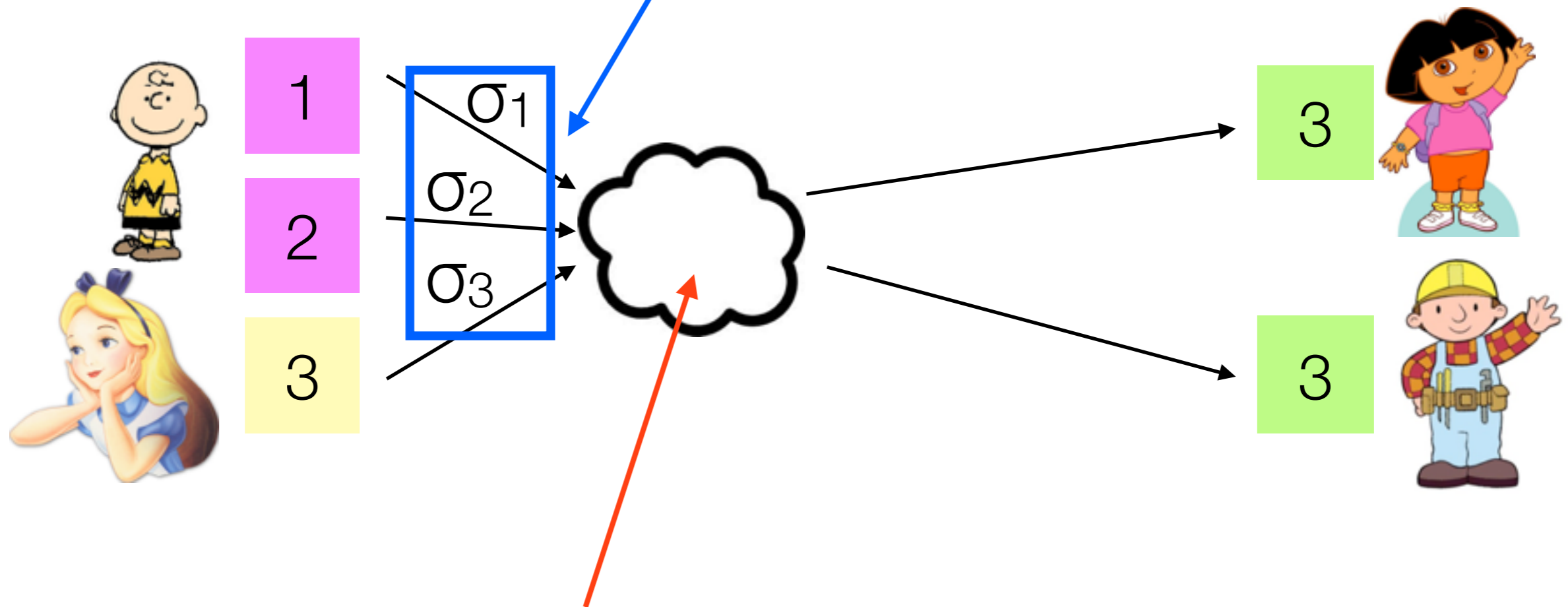
Coinjoin prevents clustering



Heuristic: the same user controls these addresses

Coinjoin

signatures contributed separately



could be:

- private communication
- IRC (+Tor)
- central server (+blind signatures)

Coinjoin

signatures contributed separately



My Wallet Be Your Own Bank.

Wallet Home My Transactions **Send Money** Receive Money Import / Export

TRANSACTION TYPE

- Quick Send
- Custom

Shared Coin

SEND VIA

- Email
- SMS Message

PARTNERS

Gyft.com

TOOLS

Address Book

Shared Coin

Trustless coin mixing using coin join and taint analysis



3



3



could be:

- private communication
- IRC (+Tor)
- central server (+blind signatures)

“Coinjoin” transactions

“Coinjoin” transactions

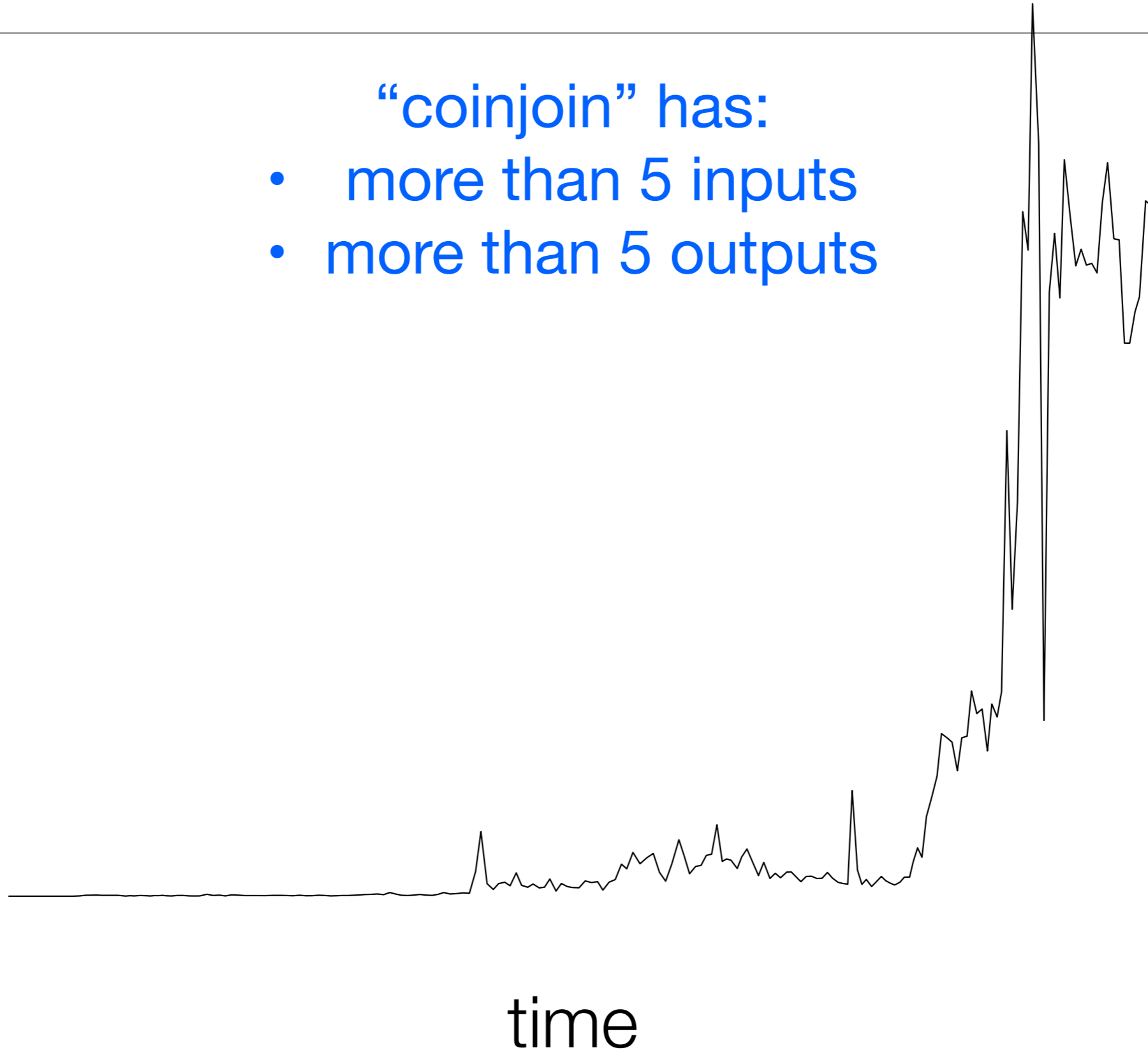
“coinjoin” has:

- more than 5 inputs
- more than 5 outputs

“Coinjoin” transactions

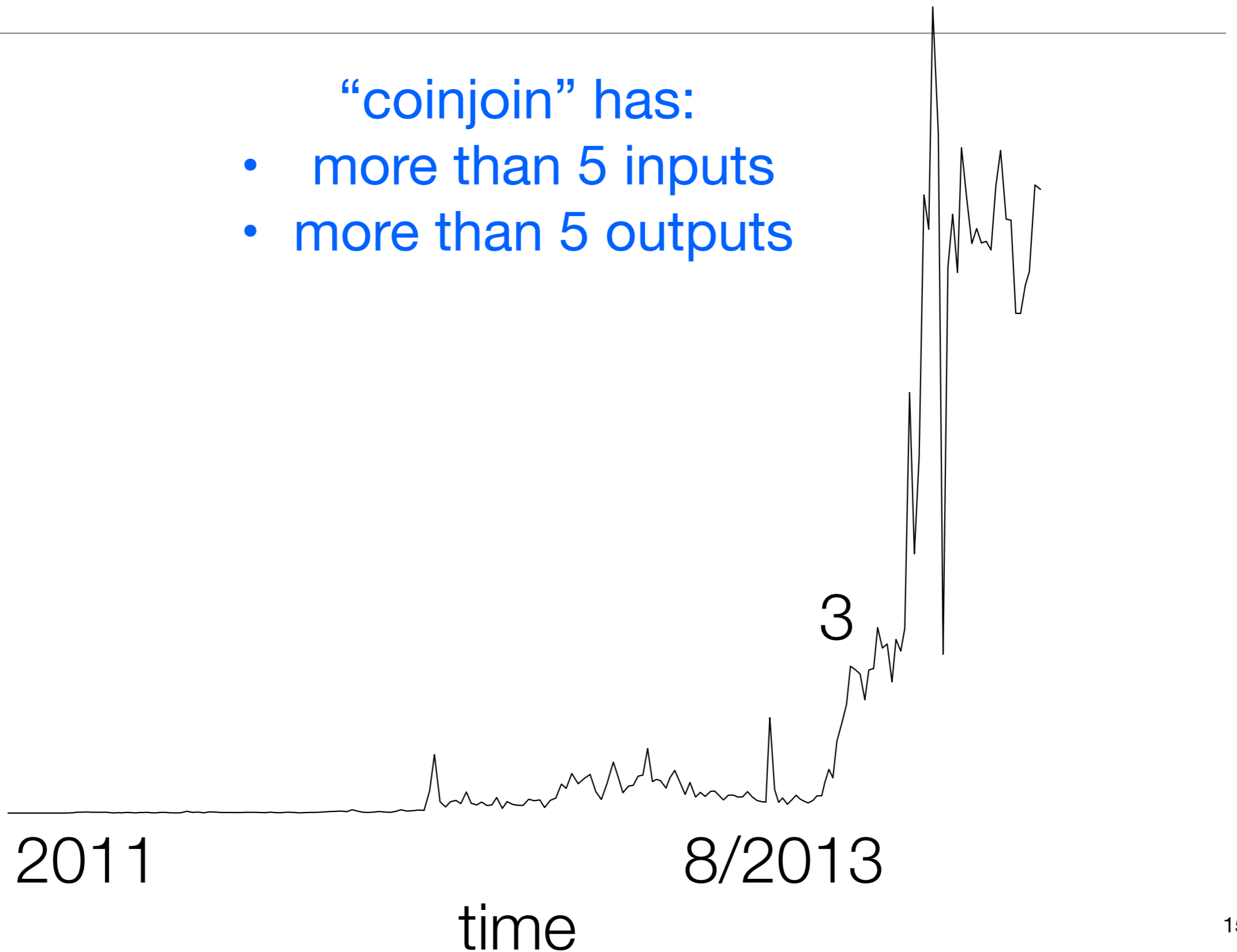
“coinjoins” per block

- “coinjoin” has:
- more than 5 inputs
 - more than 5 outputs



“Coinjoin” transactions

“coinjoins” per block



Anonymity in Bitcoin

How much anonymity does Bitcoin really provide?

in theory, a lot! addresses are not linked to identity

in practice, maybe not so much

Anonymity in Bitcoin

does Coinjoin

How much anonymity ~~does Bitcoin~~ really provide?

in theory, a lot! addresses are not linked to identity

in practice, maybe not so much

Outline

Background

Taint resistance

Accuracy

Taint resistance

Achieving taint resistance

Conclusions

Anonymity in Bitcoin

does Coinjoin

How much anonymity ~~does Bitcoin~~ really provide?

in theory, a lot! addresses are not linked to identity

in practice, maybe not so much

Anonymity in Bitcoin

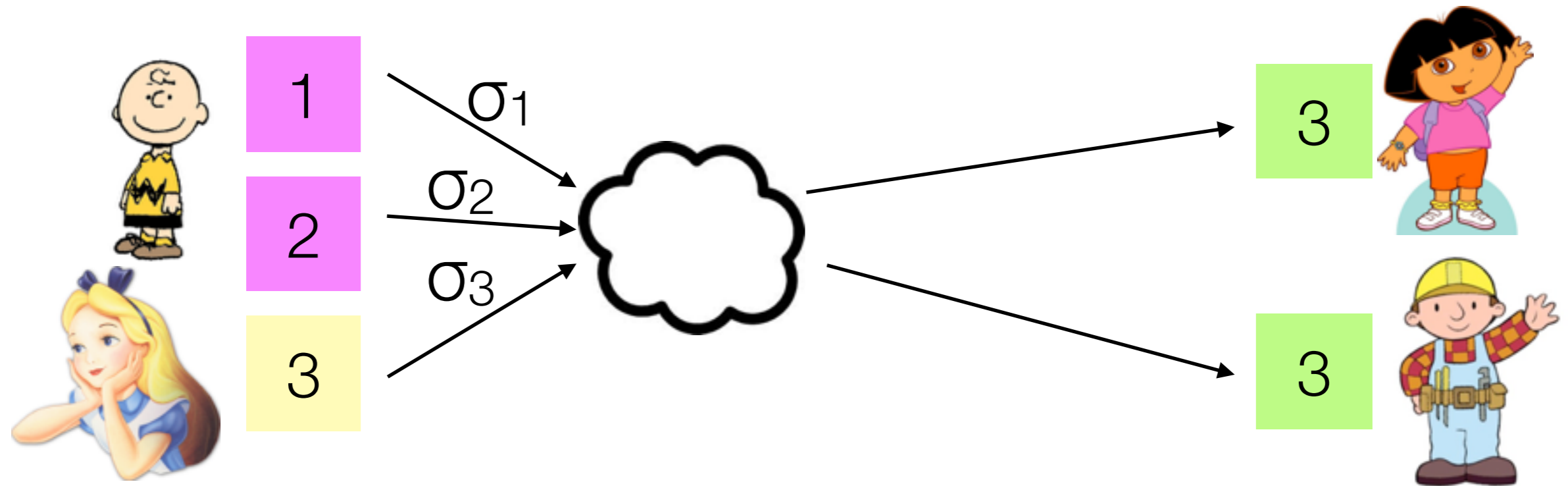
How much ~~anonymity does Bitcoin~~ really provide?

does Coinjoin

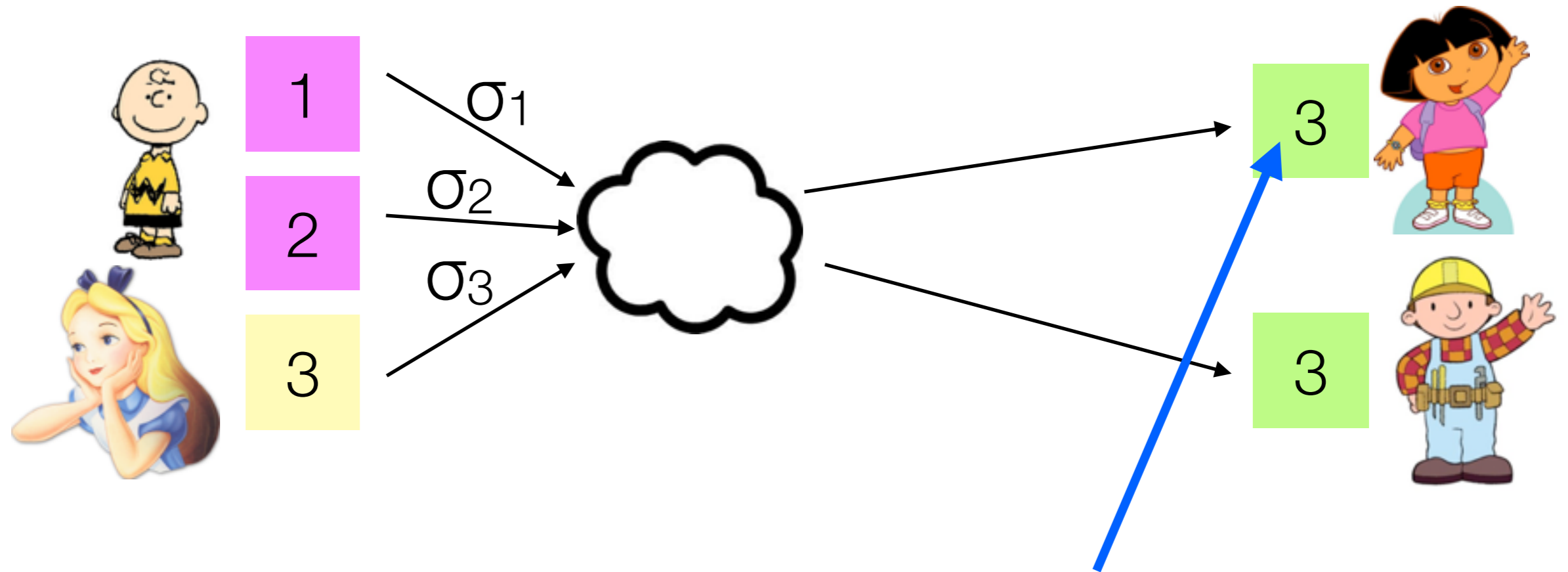
in theory, a lot! addresses are not linked to identity

in practice, maybe not so much

Coinjoin

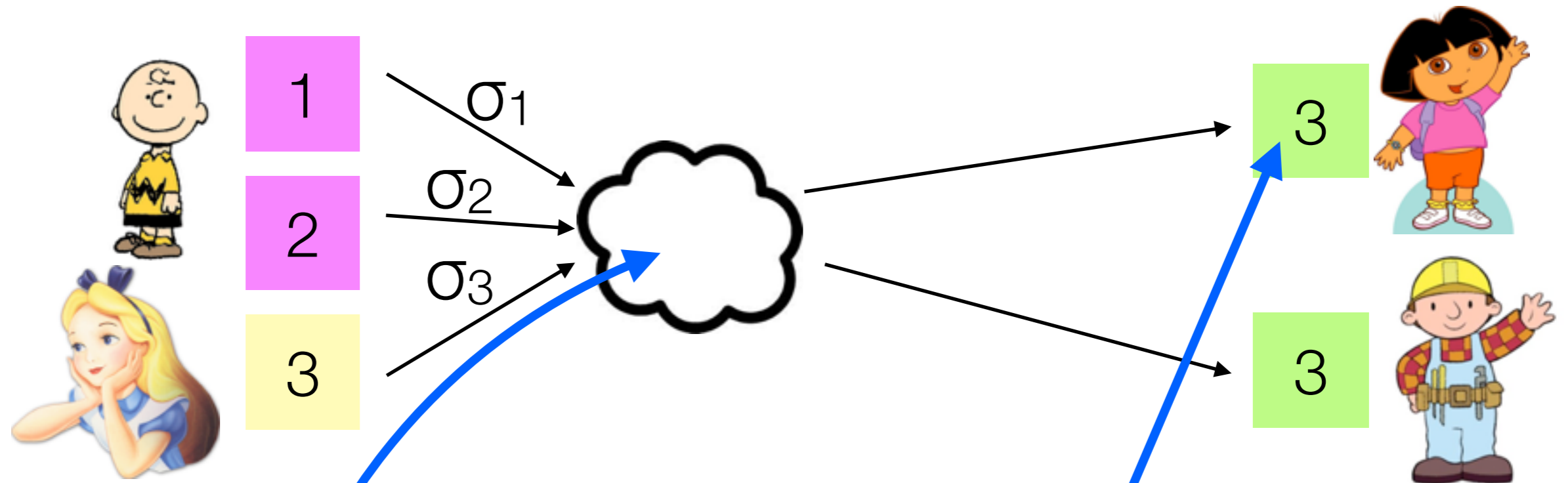


Coinjoin



should be hard to figure out which
input addresses sent to this output address

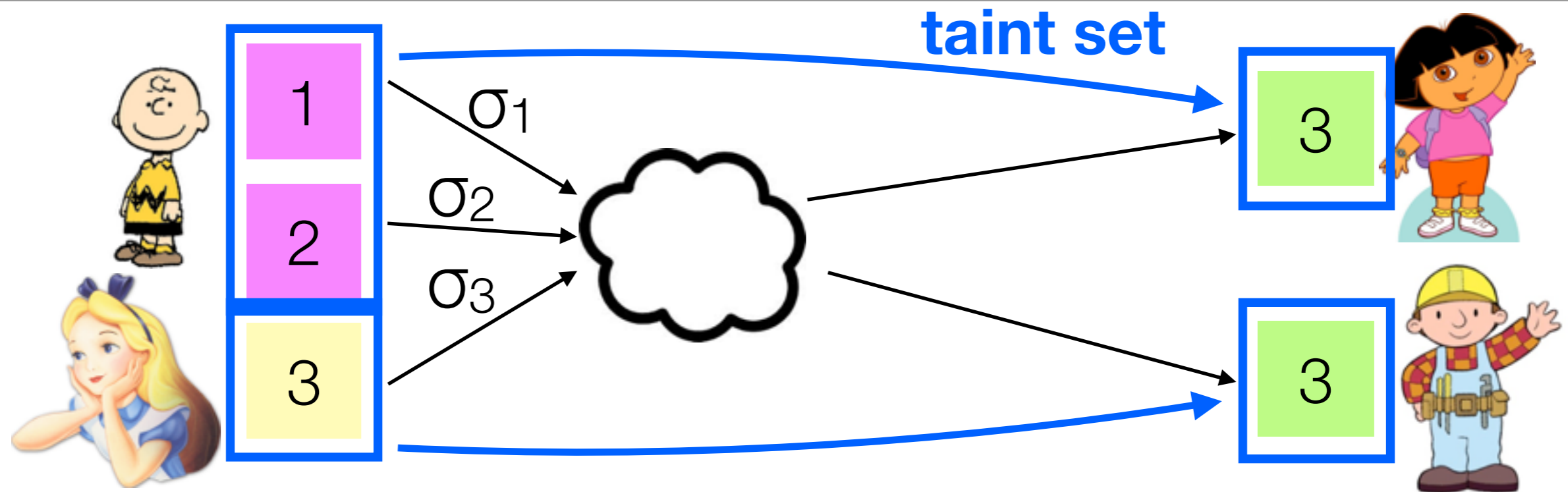
Coinjoin



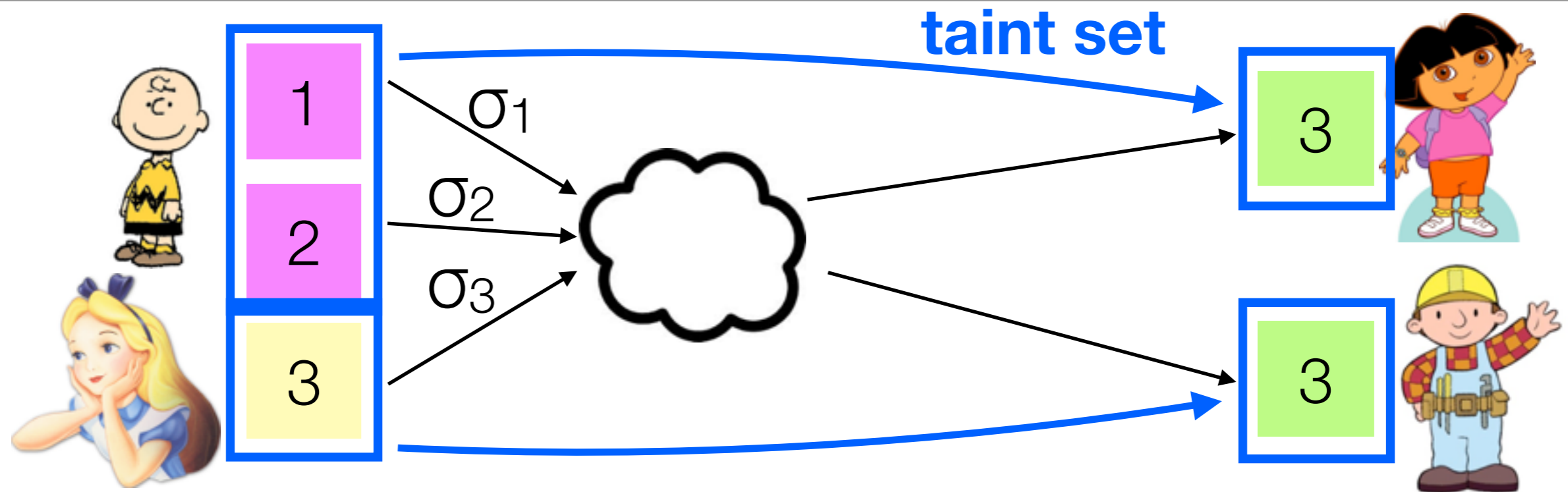
should be hard to figure out which input addresses sent to this output address

should be hard to figure out permutation

Taint resistance

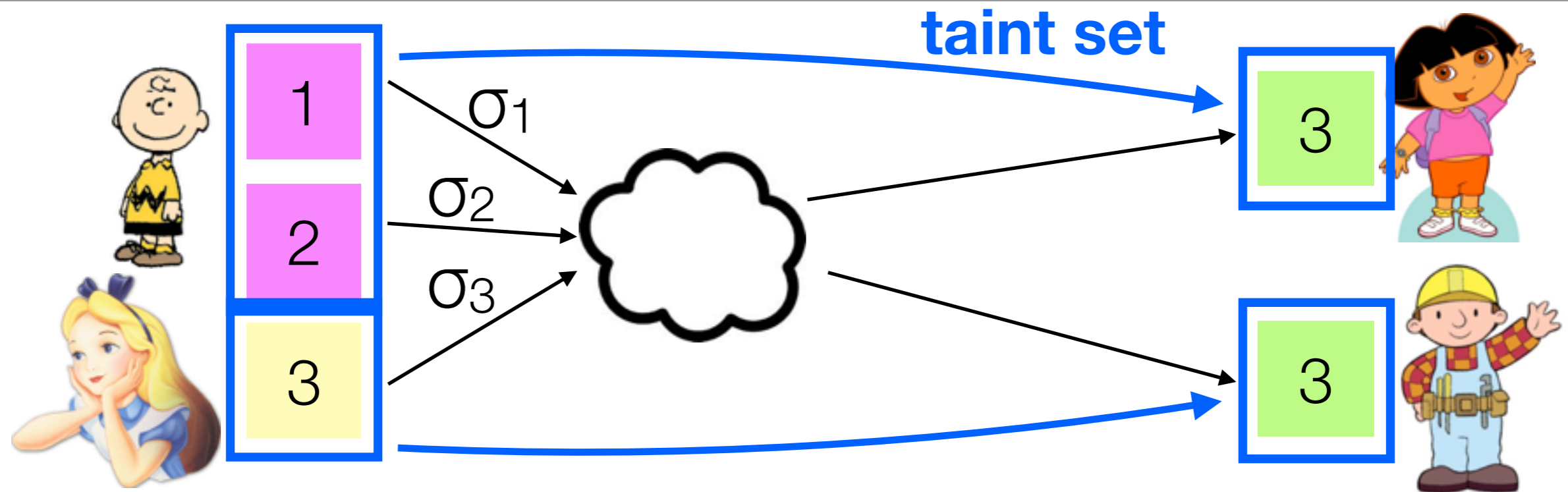


Taint resistance



accuracy: how accurately can one identify taint set?

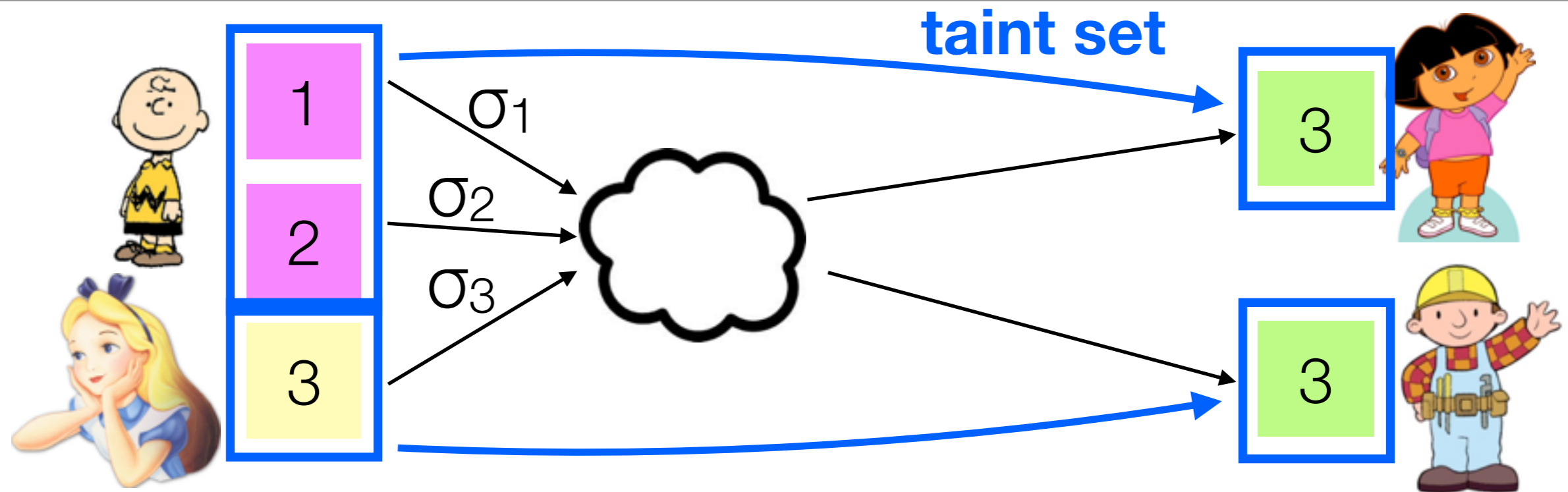
Taint resistance



accuracy: how accurately can one identify taint set?

$$\text{MCC} = \frac{|A \cap T| \times |S \setminus (A \cup T)| - |A \setminus T| \times |T \setminus A|}{\sqrt{(|A| |T| |S \setminus T| |S \setminus A|)}}$$

Taint resistance

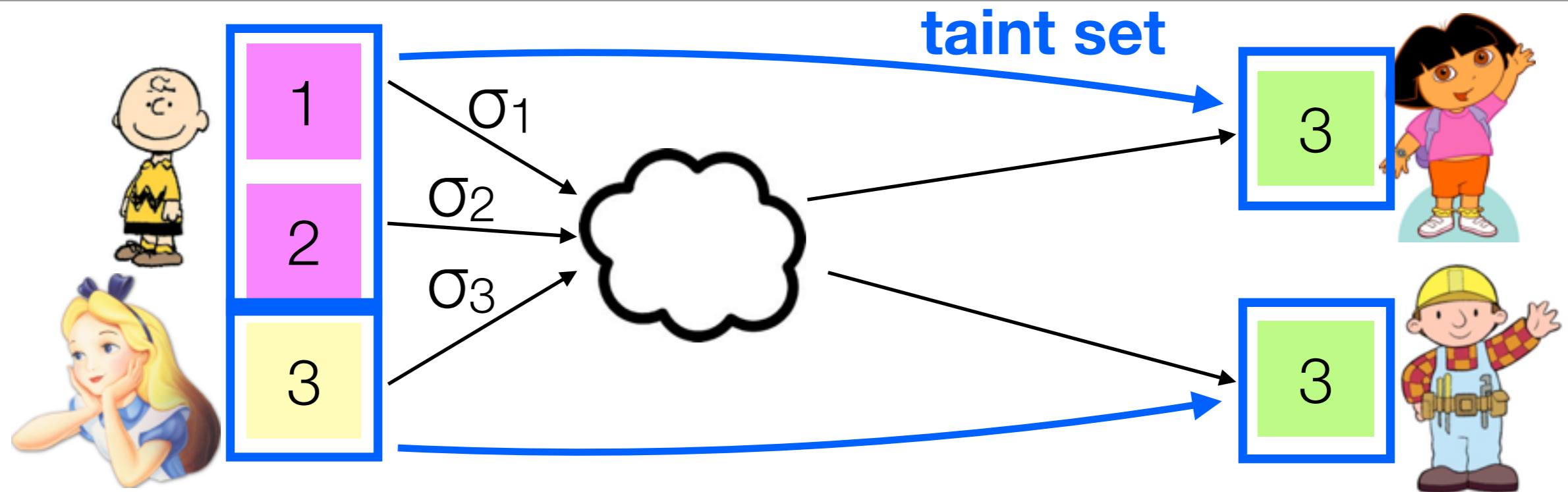


accuracy: how accurately can one identify taint set?

$$\text{MCC} = \frac{|A \cap T| \times |S \setminus (A \cup T)| - |A \setminus T| \times |T \setminus A|}{\sqrt{(|A| |T| |S \setminus T| |S \setminus A|)}}$$

input keys (candidate set) (points to $|S \setminus (A \cup T)|$)
guess for taint set (points to $|A \cap T|$)
(true) taint set (points to $|T \setminus A|$)

Taint resistance



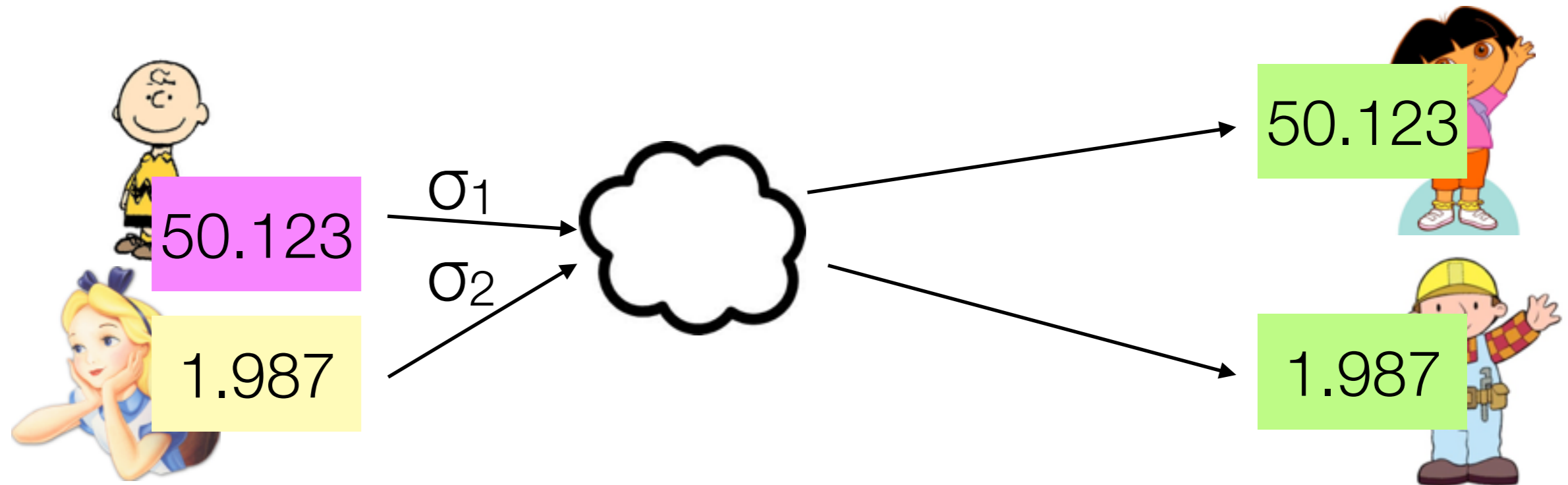
accuracy: how accurately can one identify taint set?

$$\text{MCC} = \frac{|A \cap T| \times |S \setminus (A \cup T)| - |A \setminus T| \times |T \setminus A|}{\sqrt{(|A| |T| |S \setminus T| |S \setminus A|)}}$$

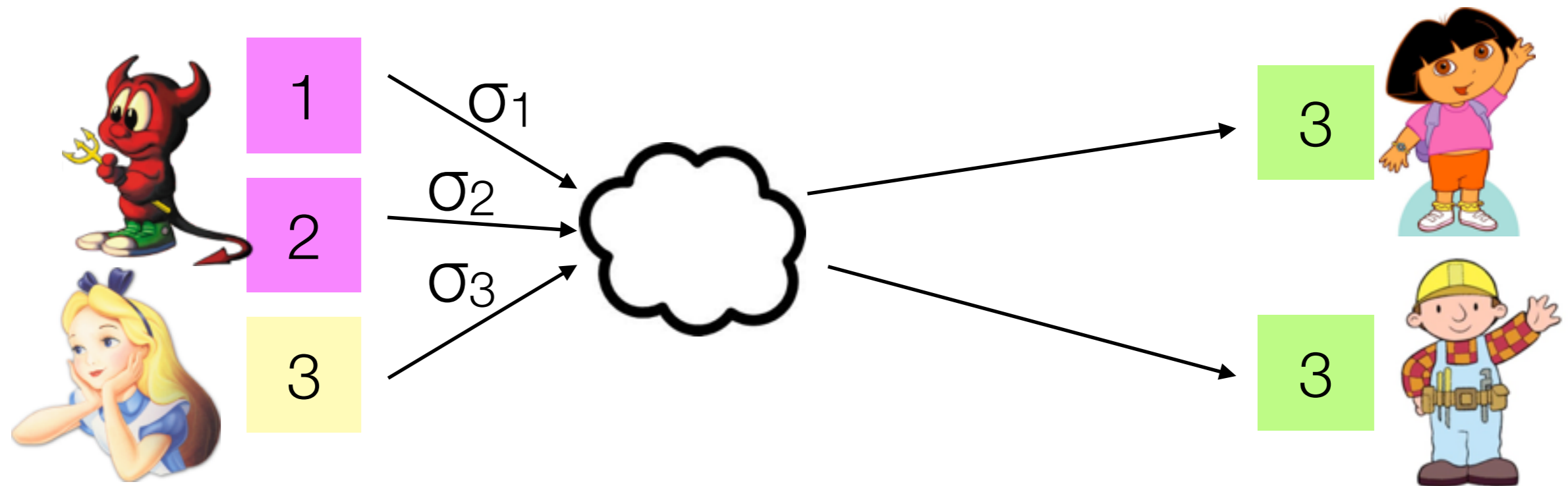
input keys (candidate set)
guess for taint set
(true) taint set

taint resistance: no adversary can have good accuracy

Bad taint resistance: lopsided values



Bad taint resistance: process of elimination



Outline

Background

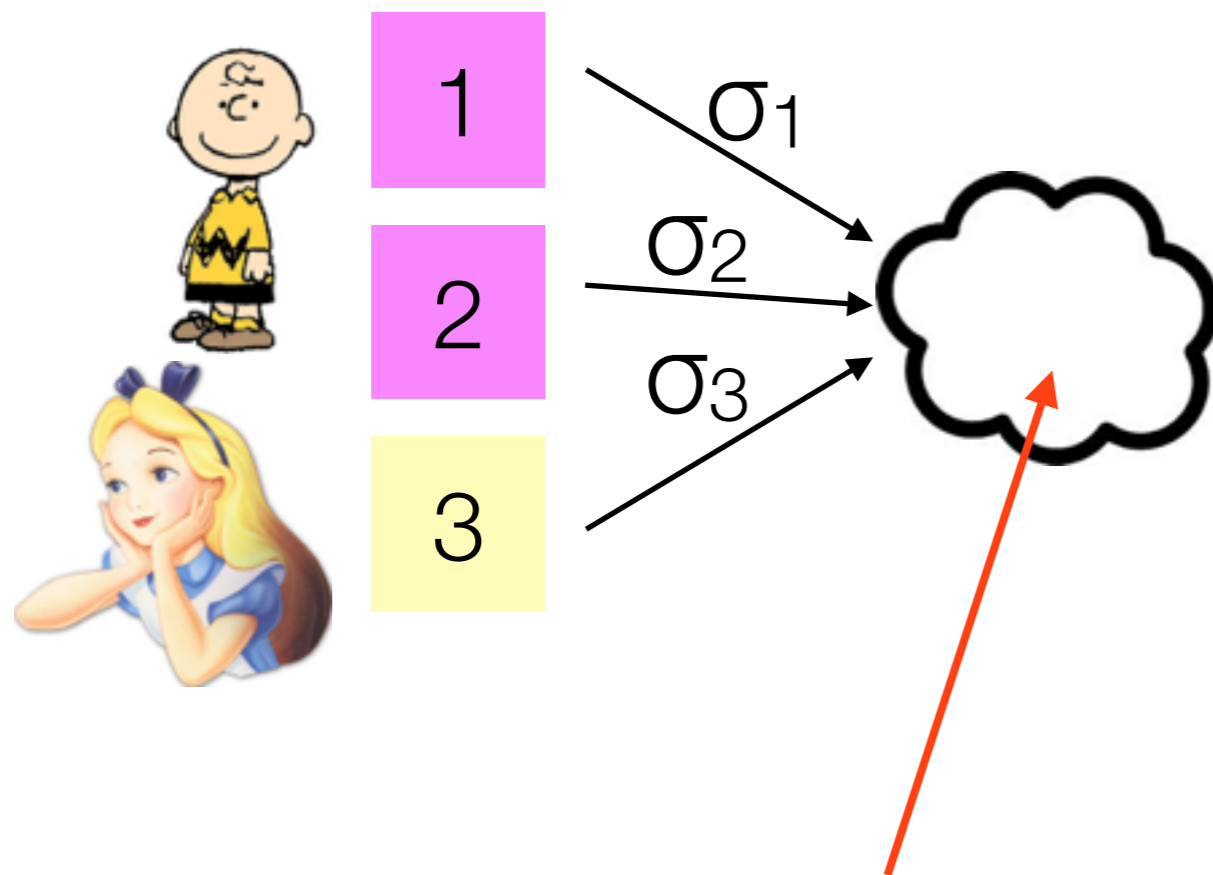
Taint resistance

Achieving taint resistance

Constructive approaches
Is Coinjoin taint resistant?

Conclusions

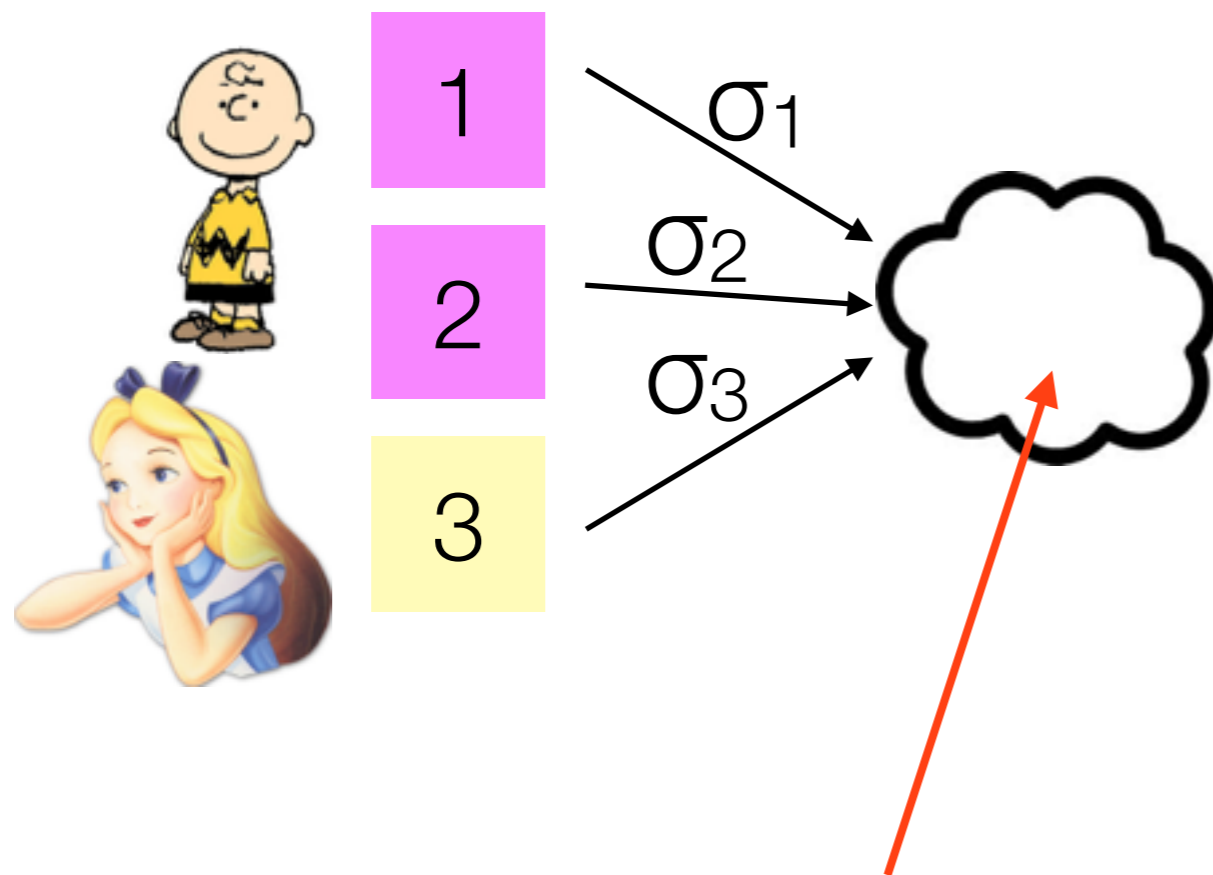
Constructing taint-resistant protocols



could be:

- private communication
- IRC (+Tor)
- central server

Constructing taint-resistant protocols

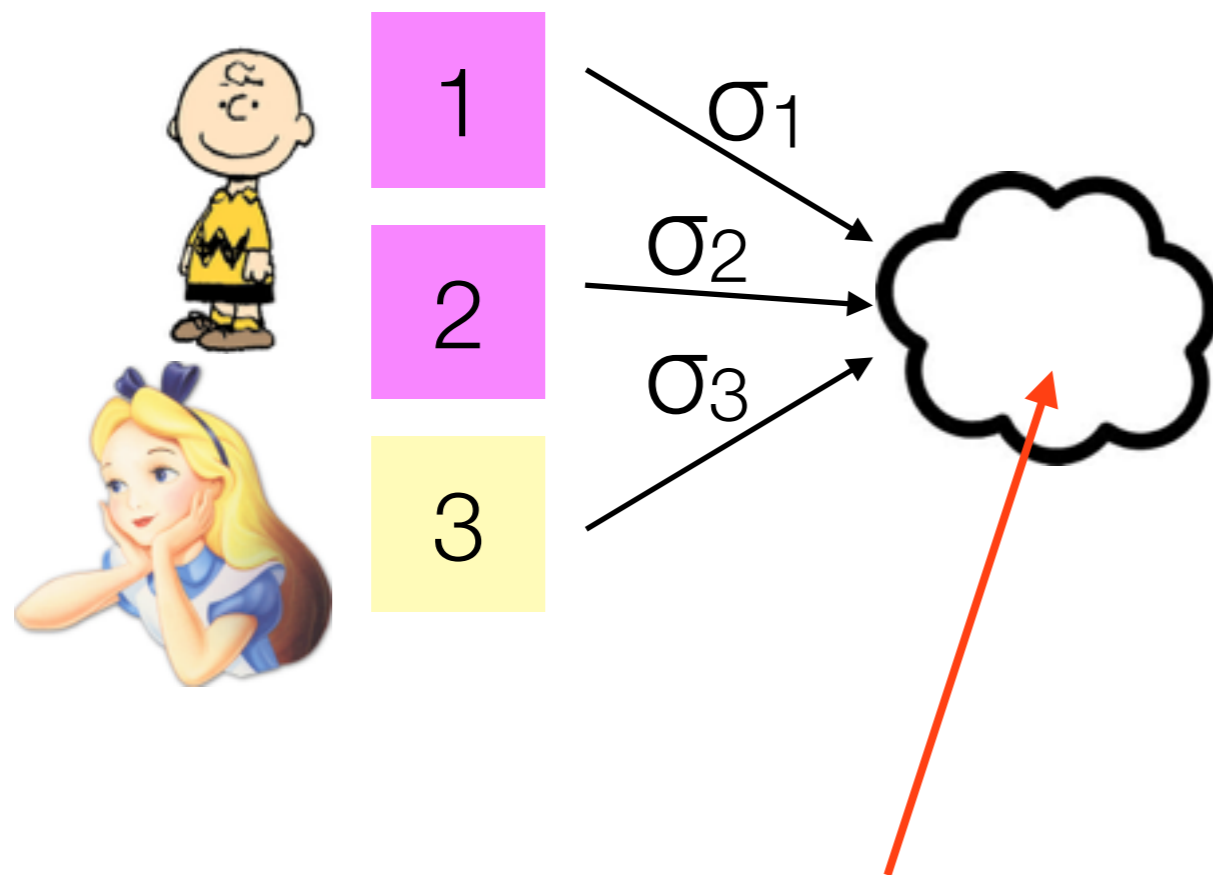


could be:

- private communication
- IRC (+Tor)
- central server

if server is trusted
and A is **passive**
then we can achieve
taint resistance

Constructing taint-resistant protocols



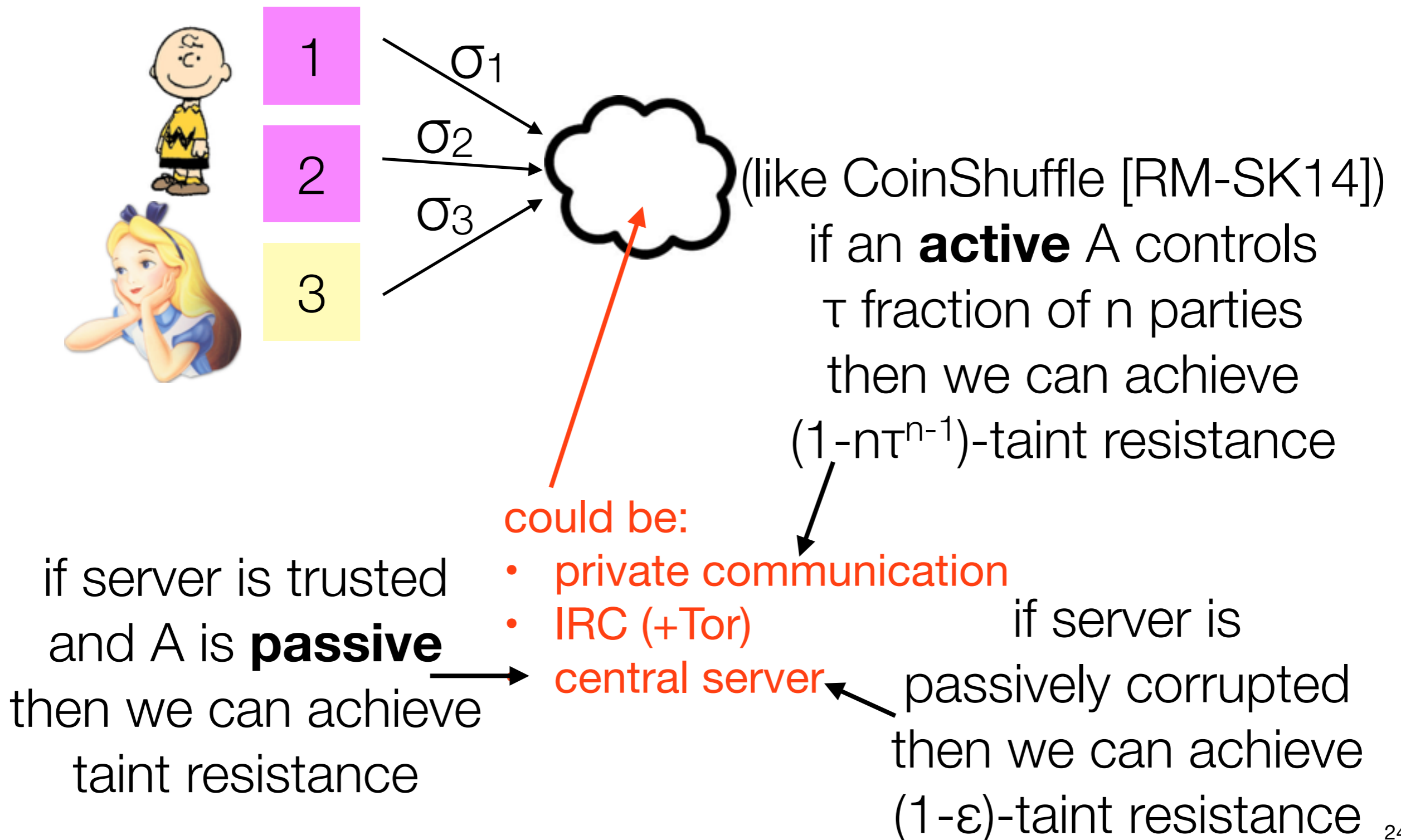
could be:

- private communication
- IRC (+Tor)
- central server

if server is trusted
and A is **passive**
then we can achieve
taint resistance

if server is
passively corrupted
then we can achieve
(1- ϵ)-taint resistance

Constructing taint-resistant protocols



Analyzing taint-resistant protocols

My Wallet Be Your Own Bank.

Wallet Home My Transactions **Send Money** Receive Money Import / Export

TRANSACTION TYPE

- Quick Send
- Custom
- Shared Coin**

SEND VIA

- Email
- SMS Message


PARTNERS

- Gyft.com

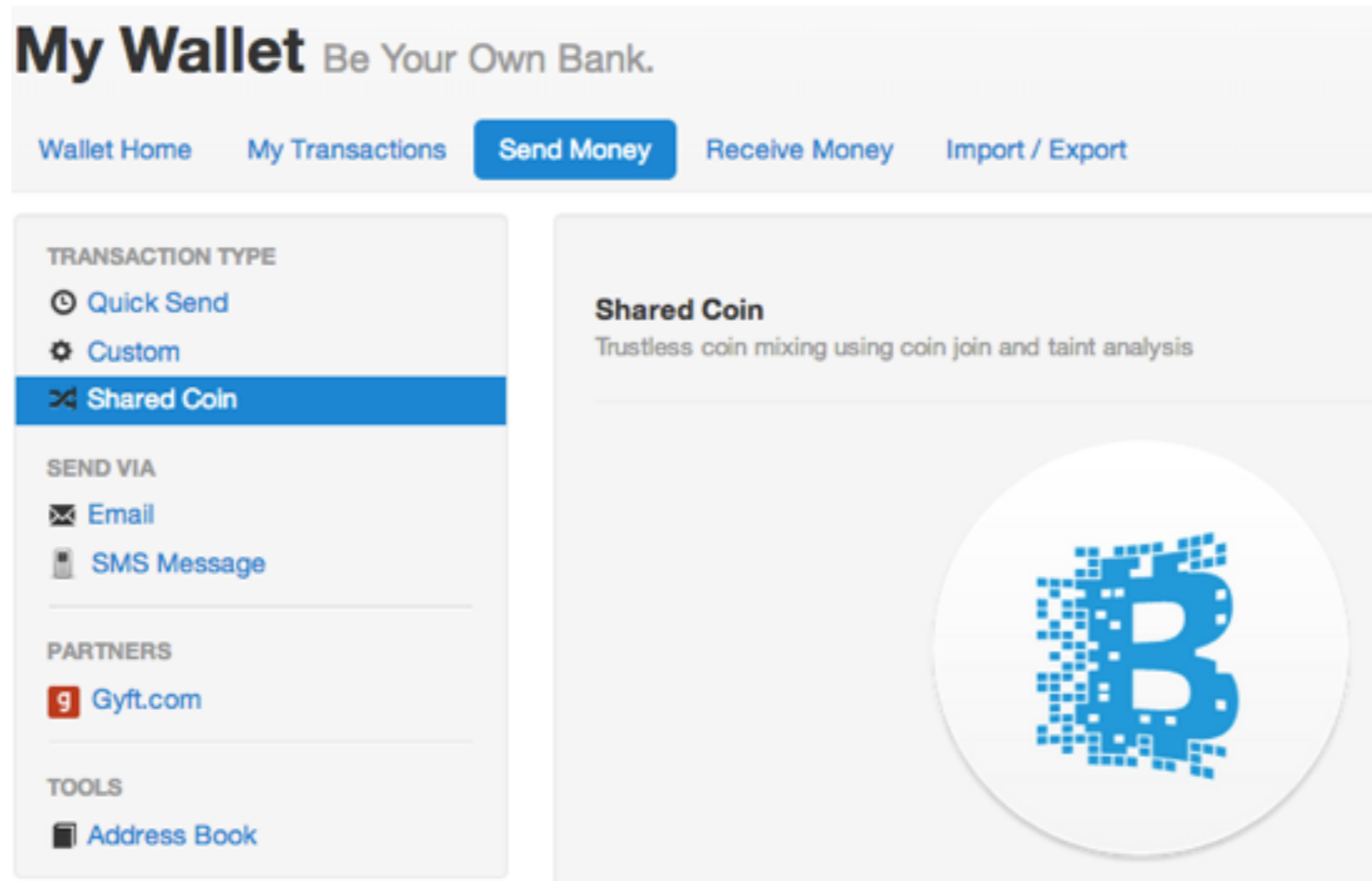
TOOLS

- Address Book

Shared Coin
Trustless coin mixing using coin join and taint analysis



Analyzing taint-resistant protocols



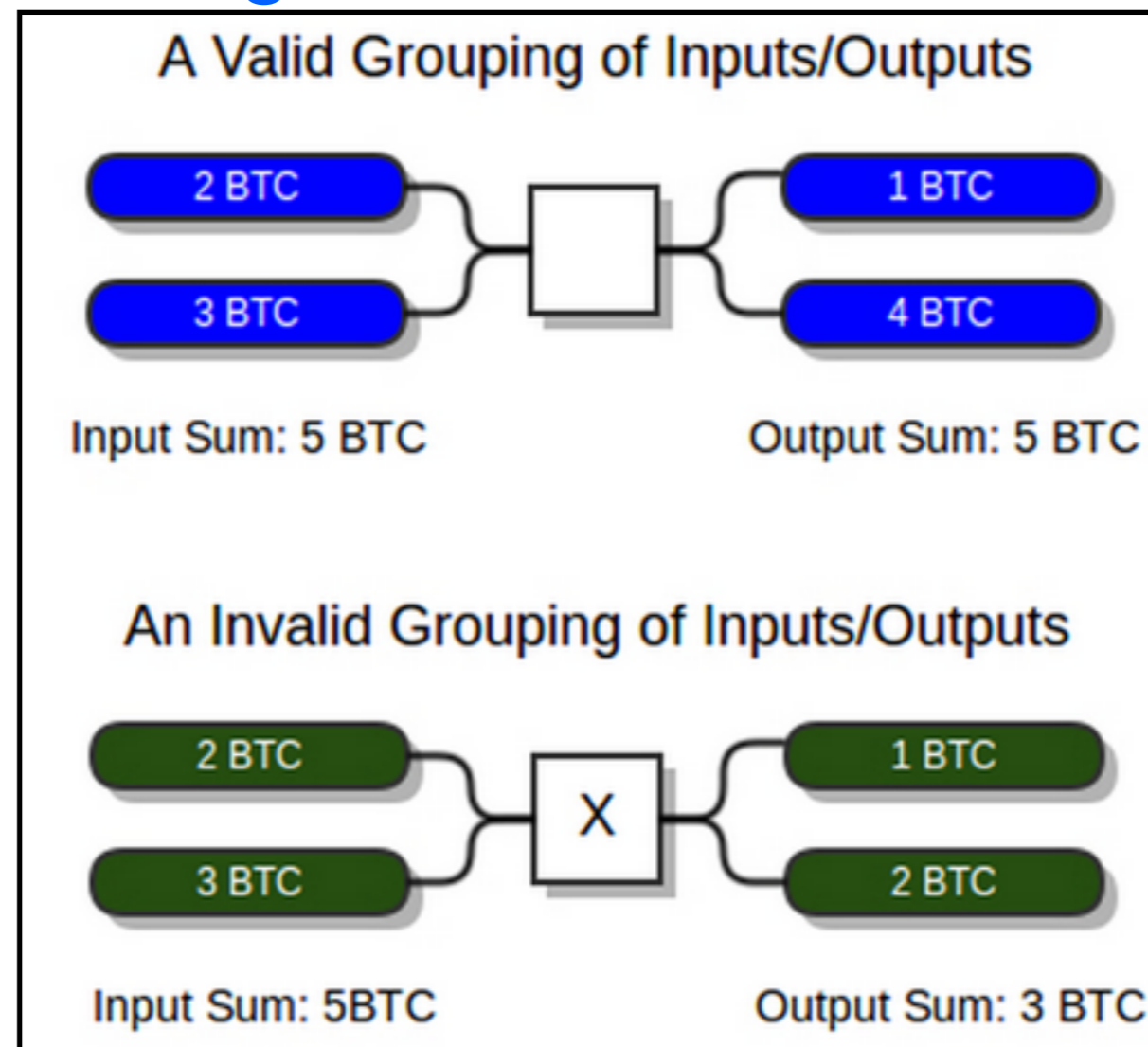
participated in 108 transactions ourselves

Analyzing taint-resistant protocols

implemented simple subset-sum algorithm:
(roughly) if sum of input values is output value,
input addresses might be in taint set for output address

Analyzing taint-resistant protocols

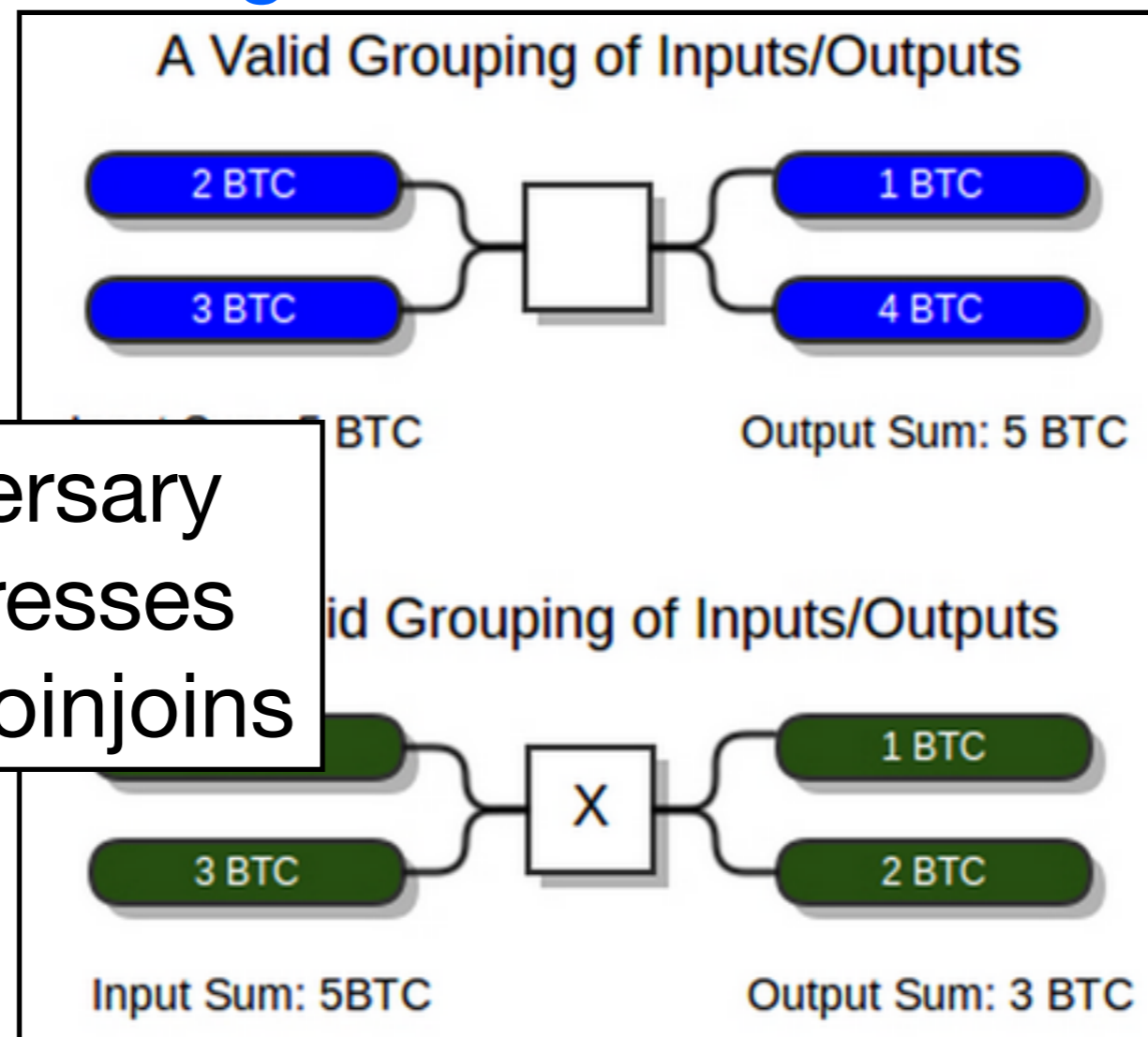
implemented simple subset-sum algorithm:
(roughly) if sum of input values is output value,
input addresses might be in taint set for output address



(Atlas, Coinjoin Sudoku)

Analyzing taint-resistant protocols

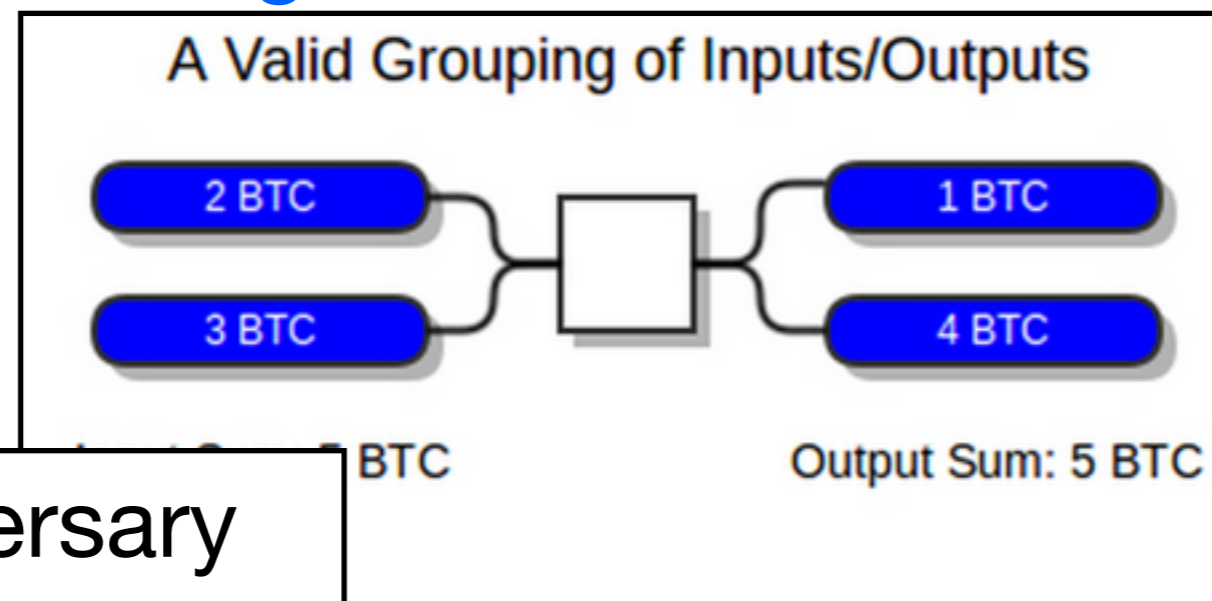
implemented simple subset-sum algorithm:
(roughly) if sum of input values is output value,
input addresses might be in taint set for output address



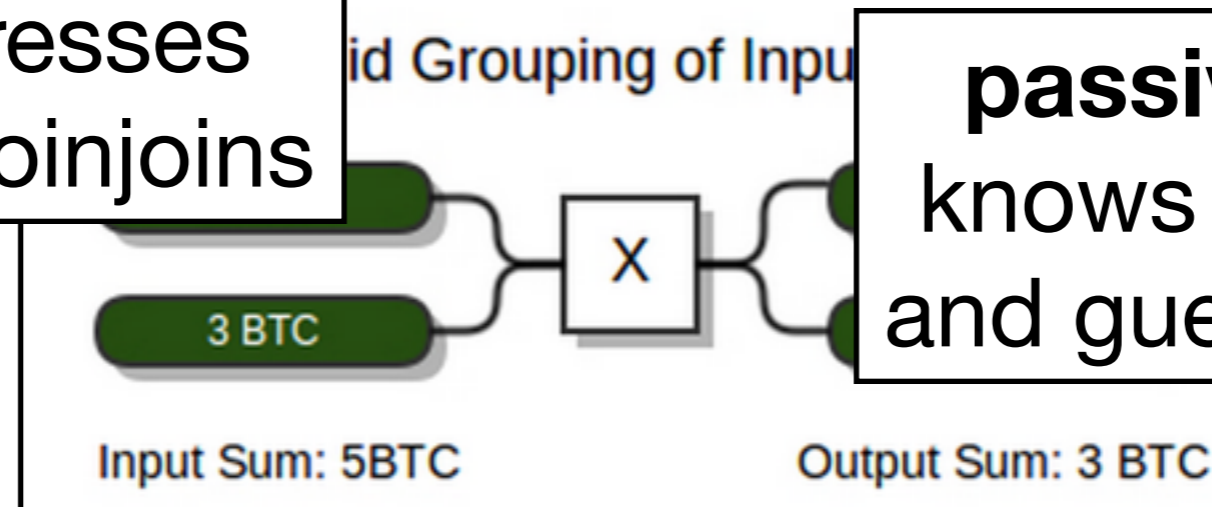
(Atlas, Coinjoin Sudoku)

Analyzing taint-resistant protocols

implemented simple subset-sum algorithm:
(roughly) if sum of input values is output value,
input addresses might be in taint set for output address



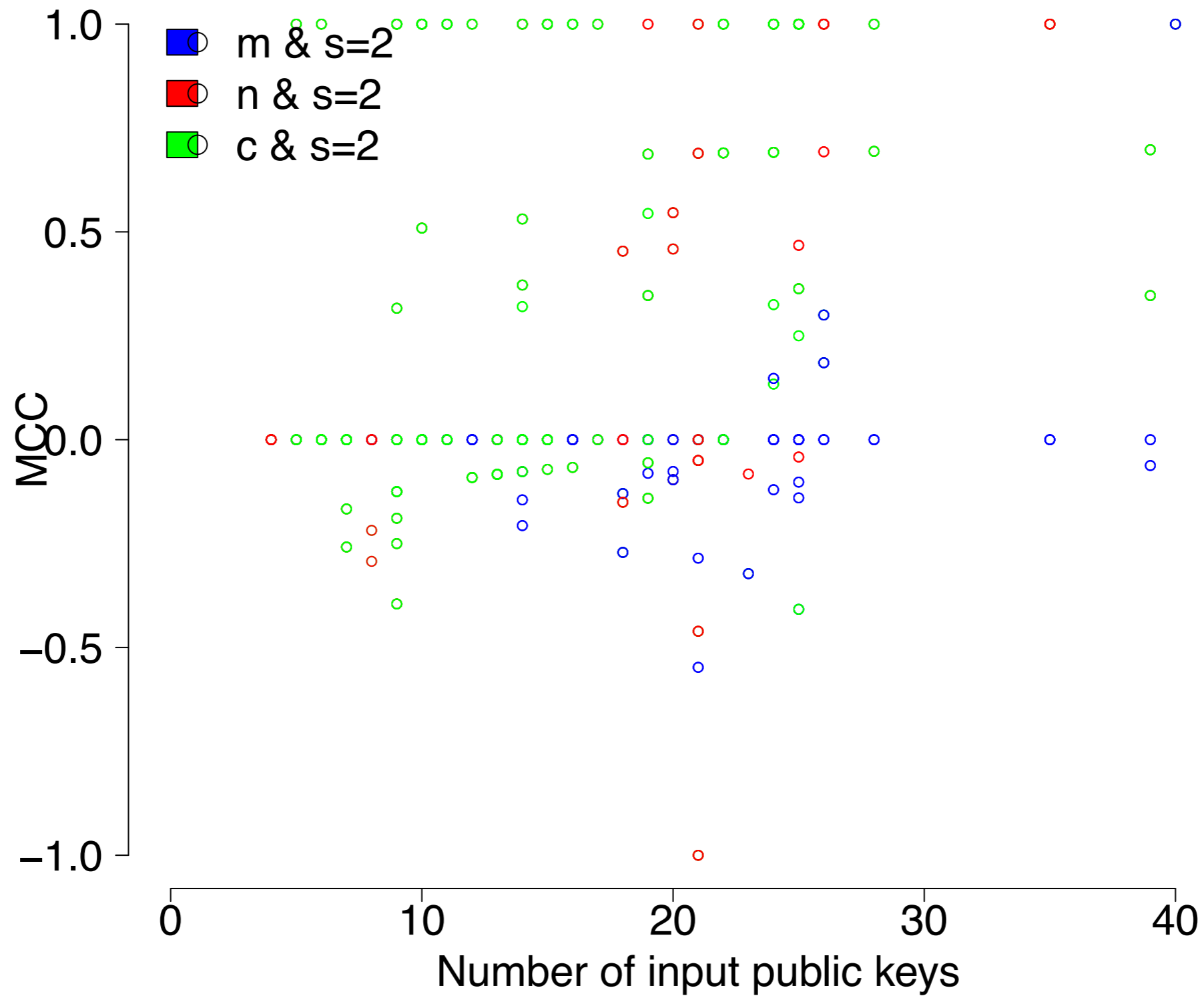
active adversary
knows addresses
and knows coinjoins



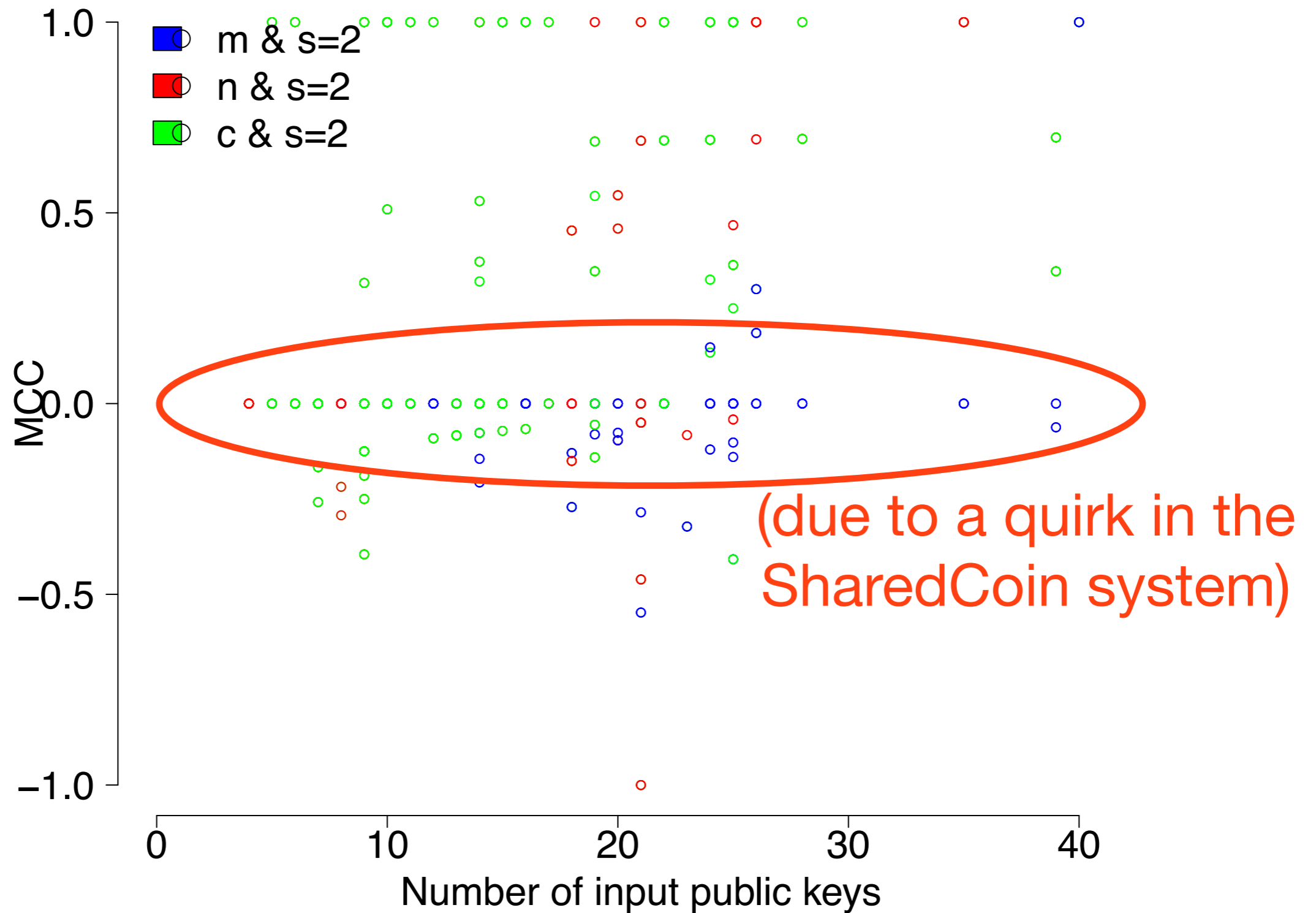
passive adversary
knows no addresses
and guesses coinjoins

(Atlas, Coinjoin Sudoku)

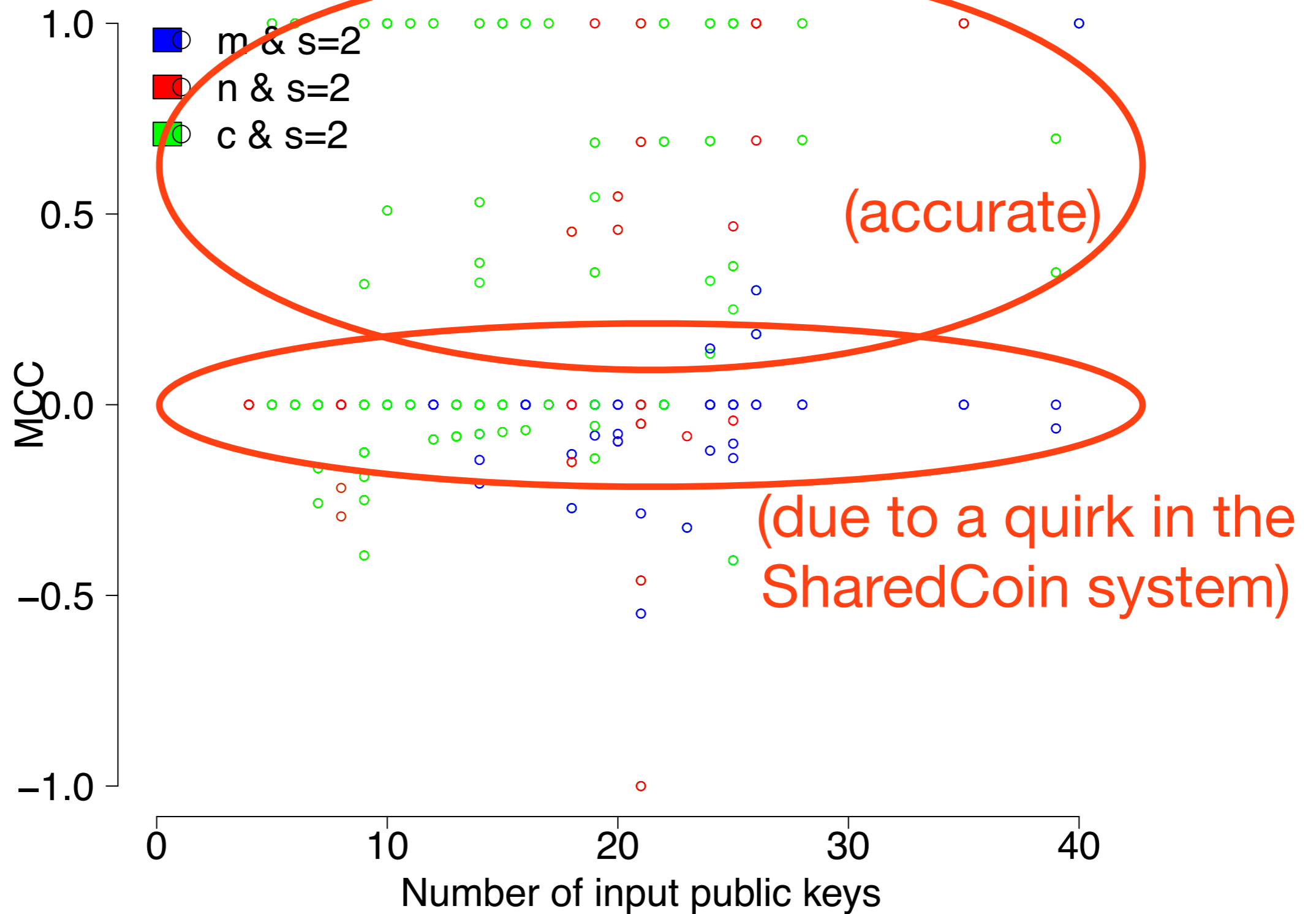
Sanity check: Ground truth output taint



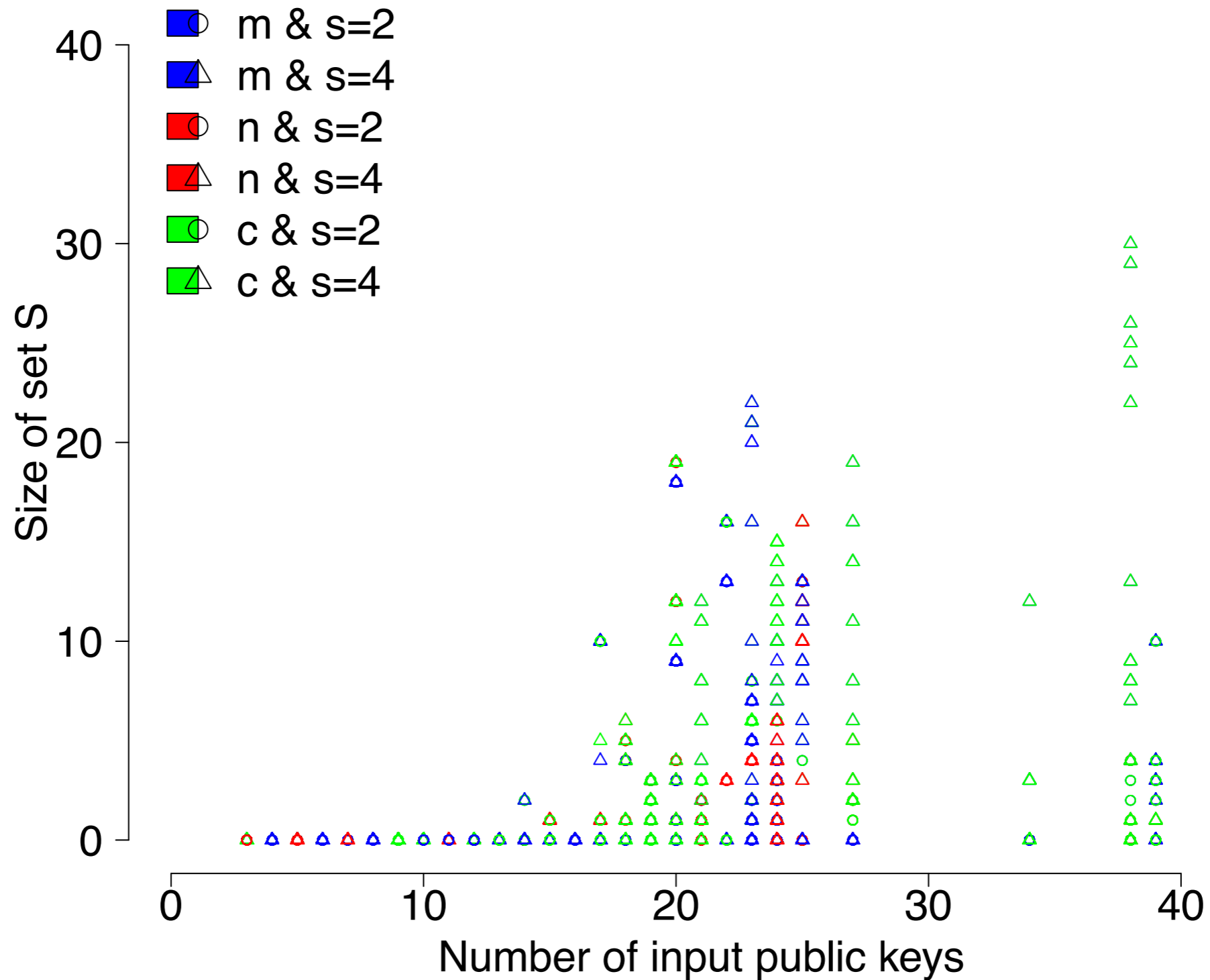
Sanity check: Ground truth output taint



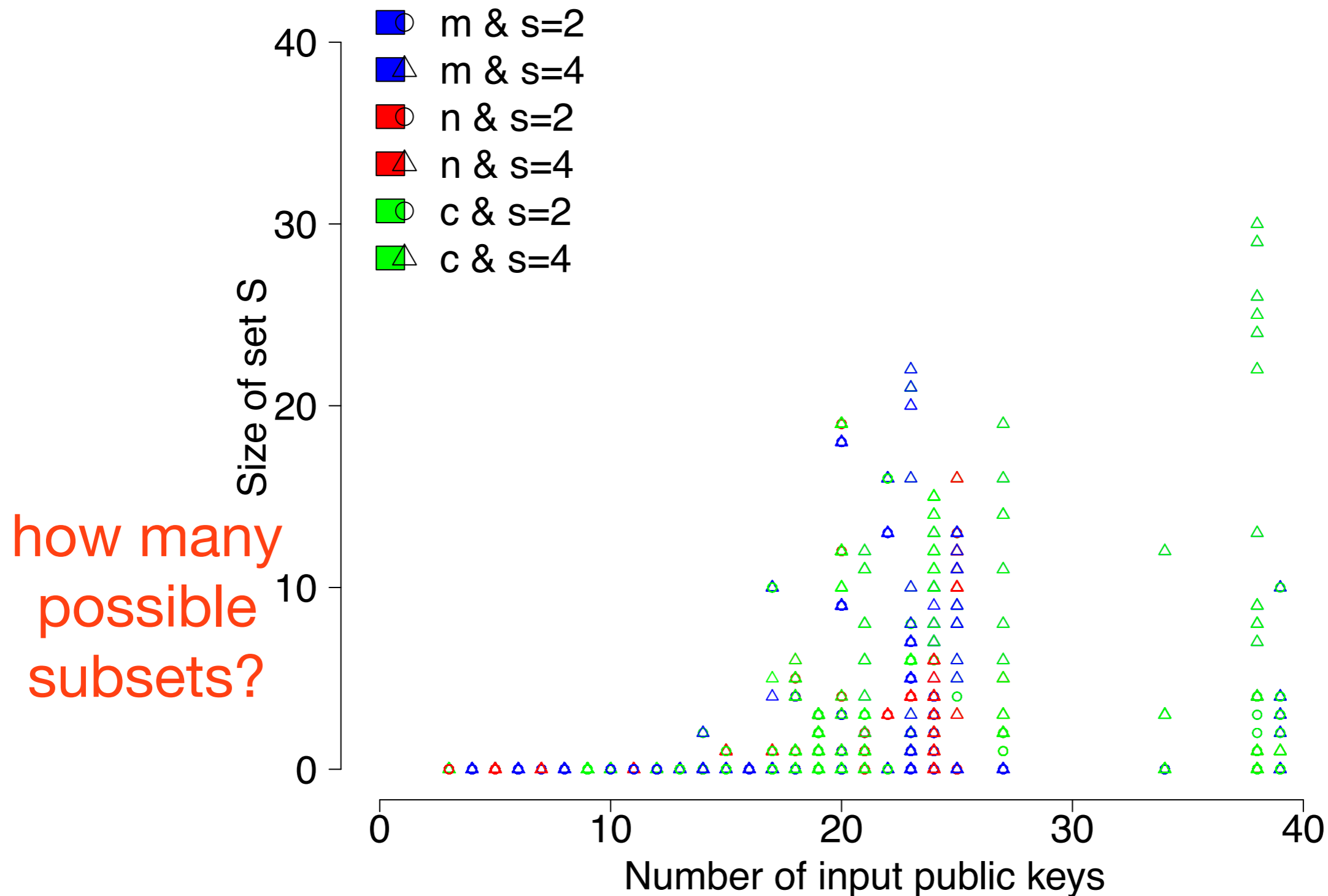
Sanity check: Ground truth output taint



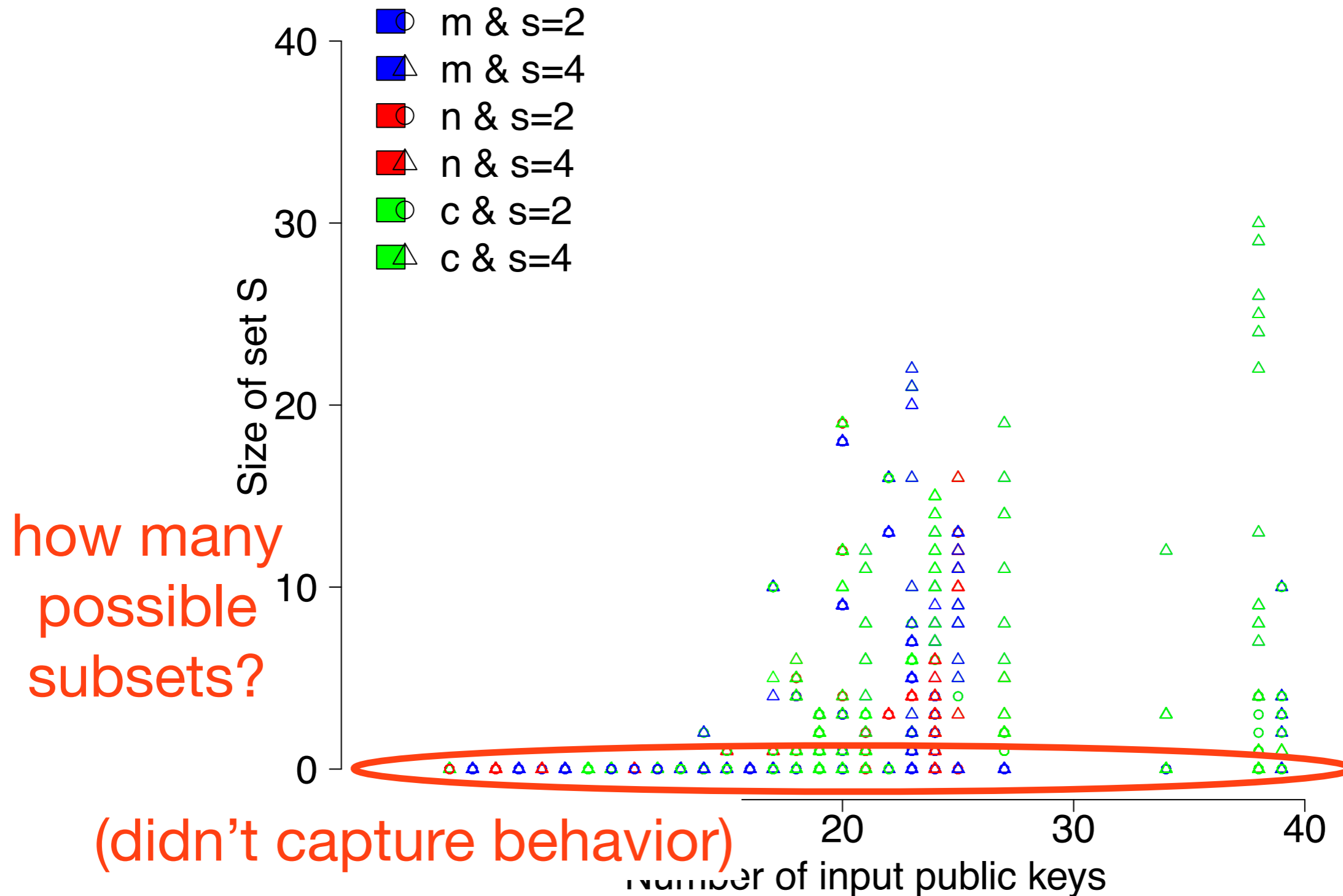
Active adversaries: Coinjoin output taint



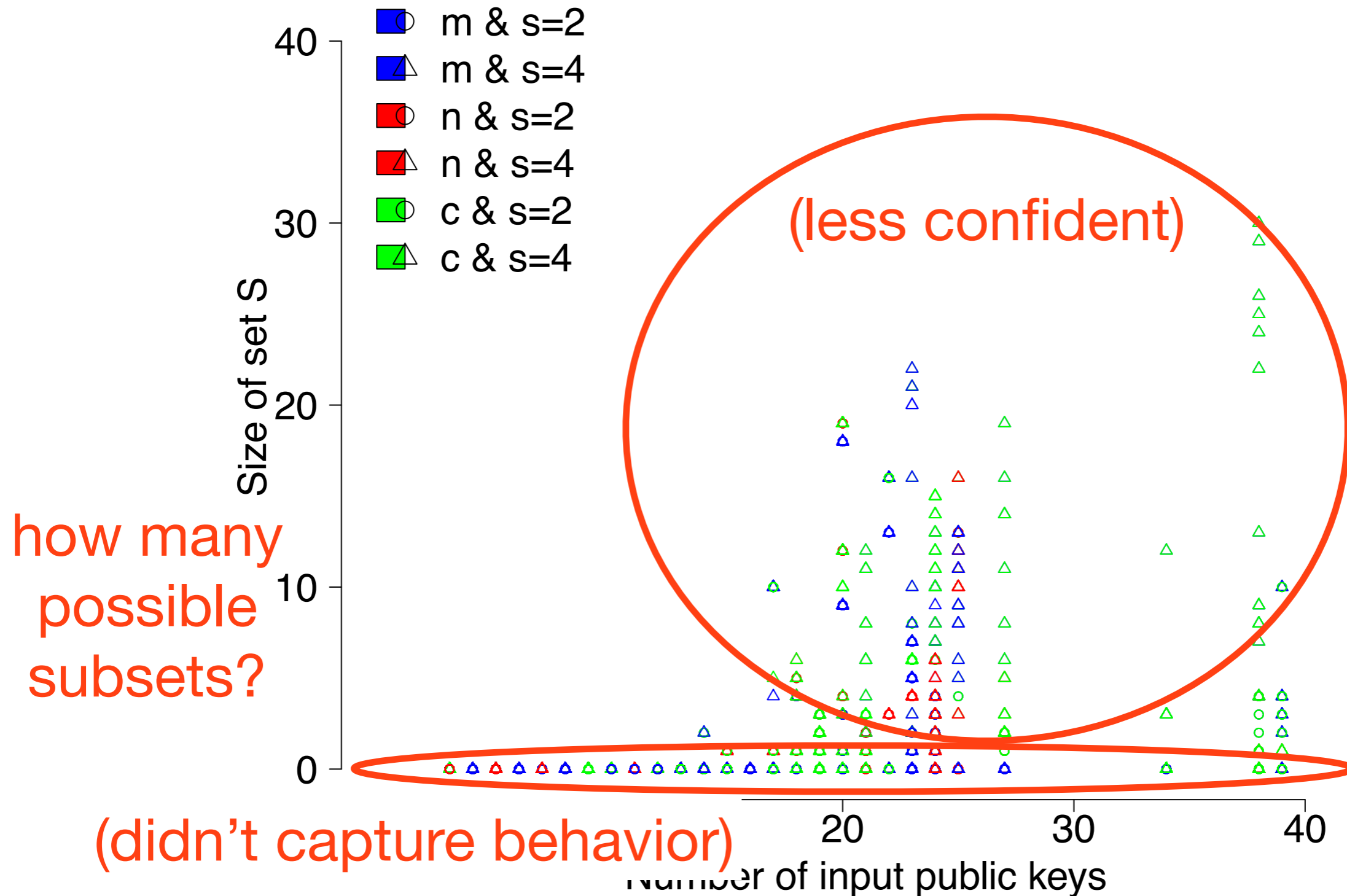
Active adversaries: Coinjoin output taint



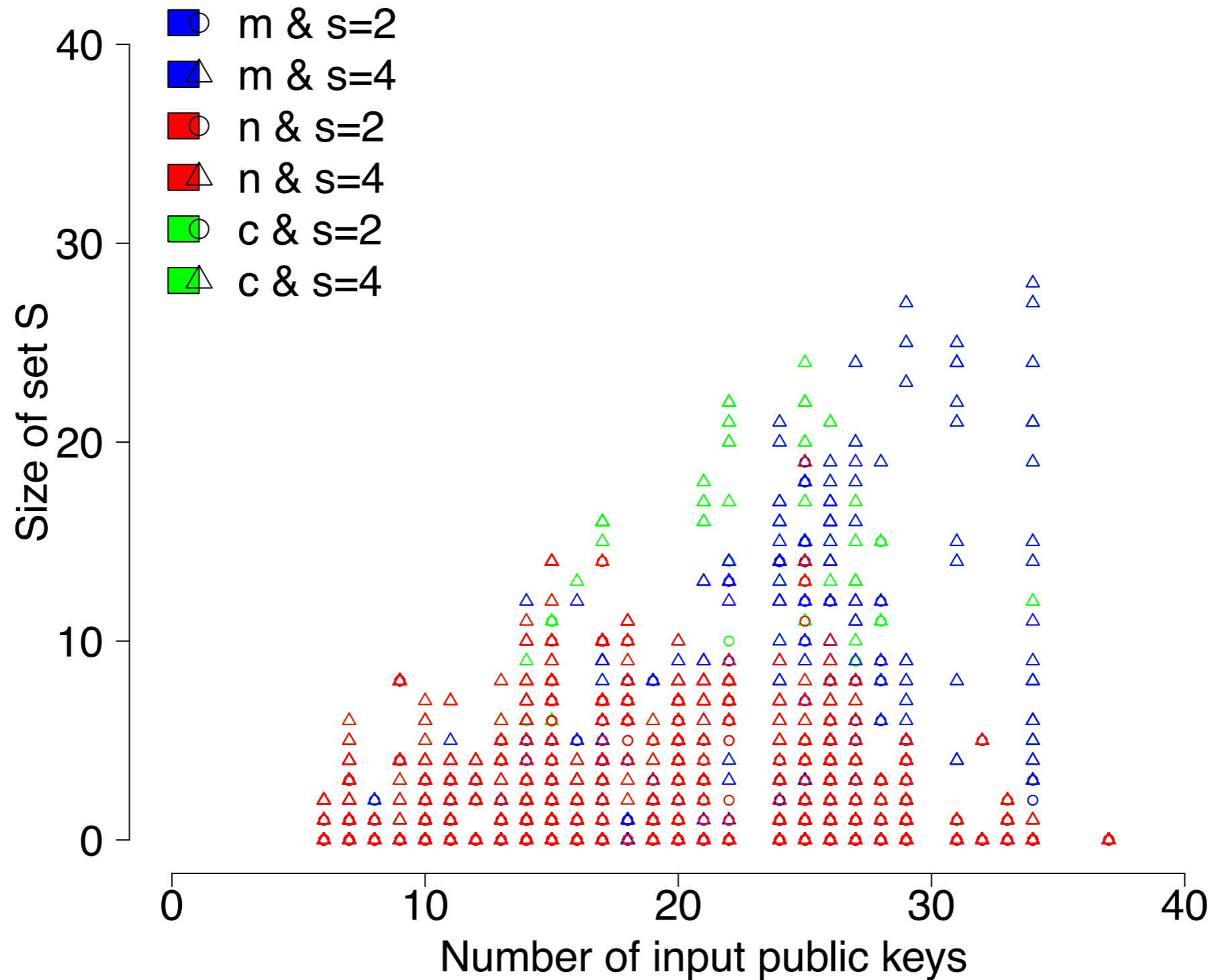
Active adversaries: Coinjoin output taint



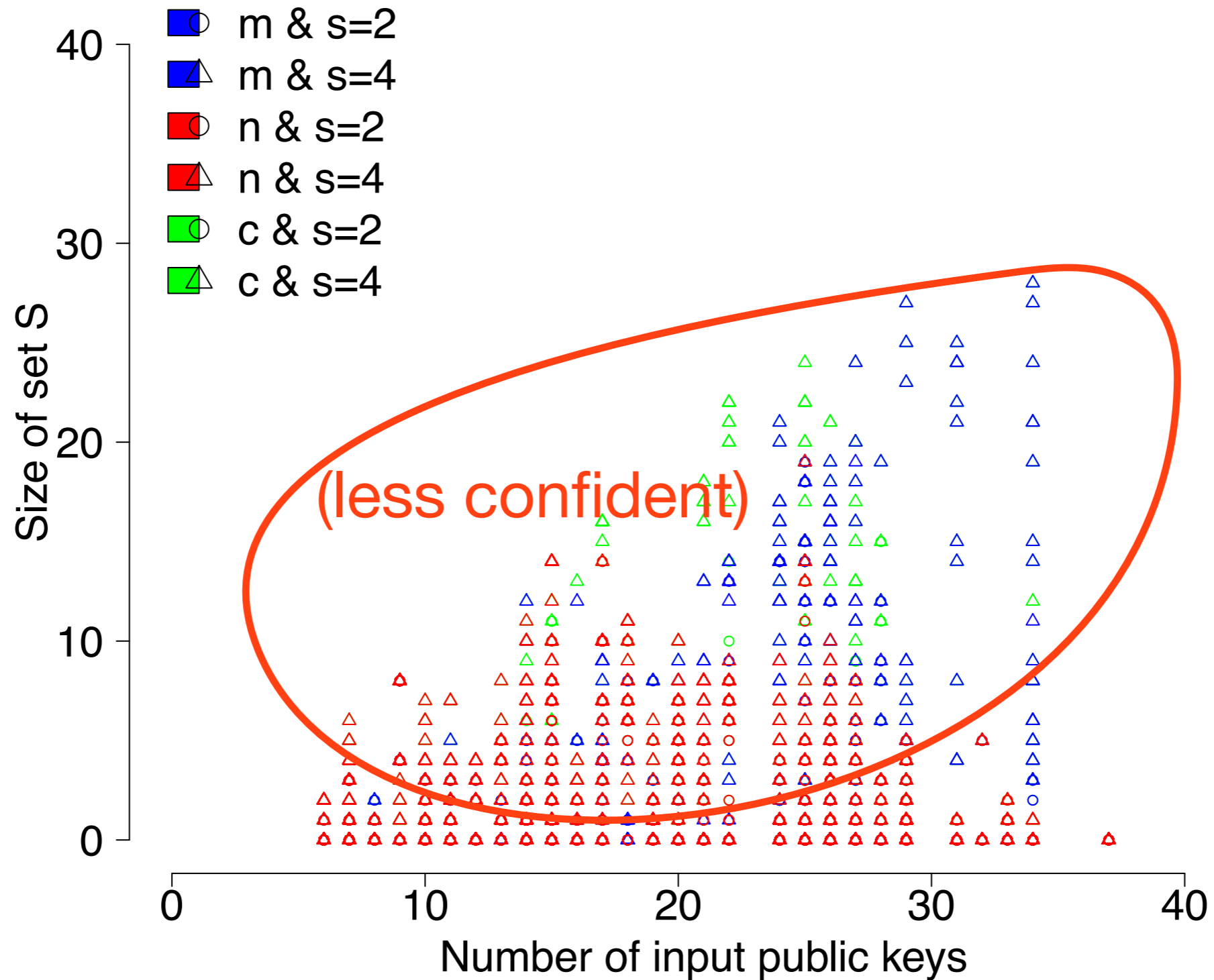
Active adversaries: Coinjoin output taint



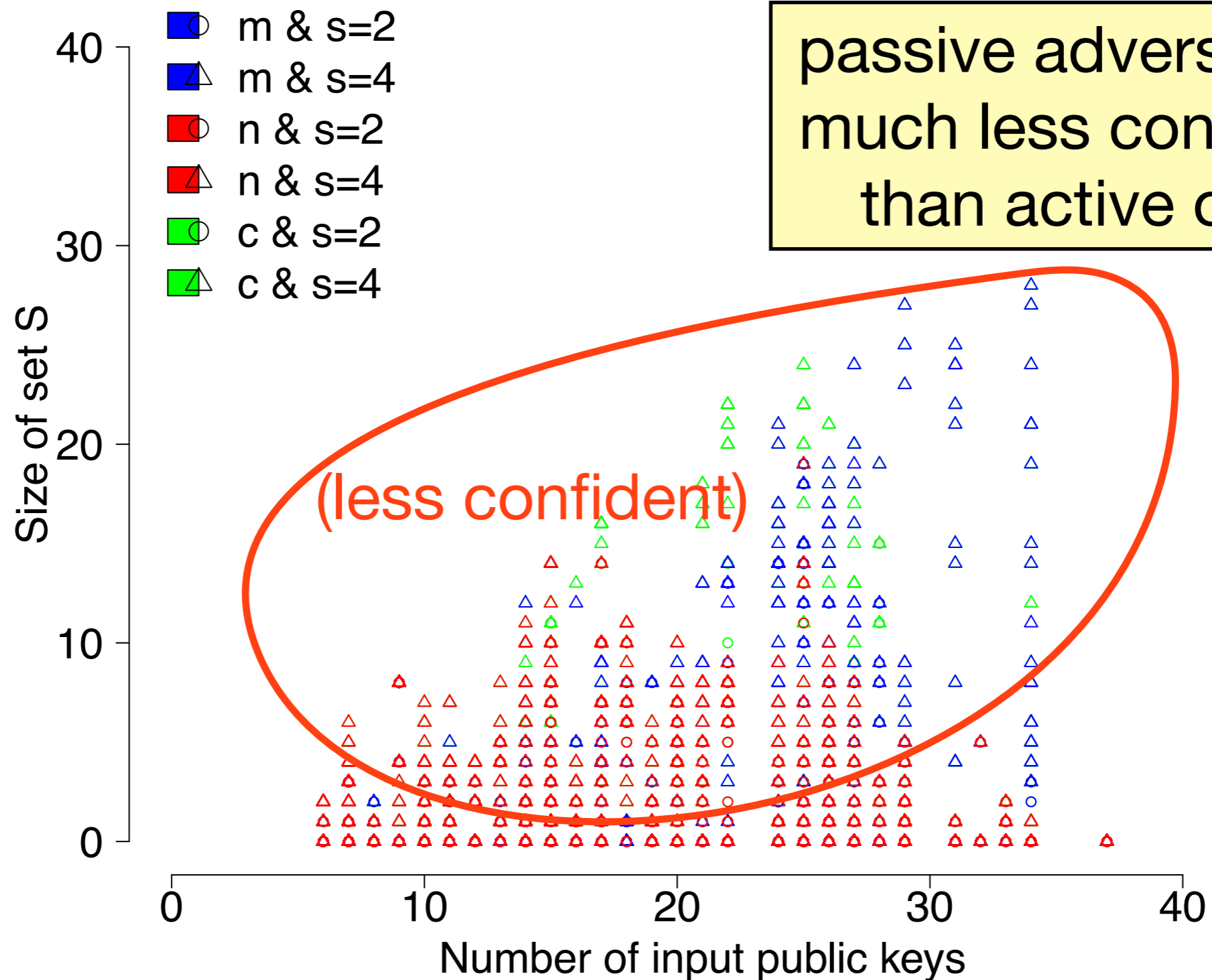
Passive adversaries: “Coinjoin” output taint



Passive adversaries: “Coinjoin” output taint



Passive adversaries: “Coinjoin” output taint



Outline

Background

Taint resistance

Achieving taint resistance

Conclusions

Conclusions

does Coinjoin

How much anonymity ~~does Bitcoin~~ really provide?

in theory, a lot! addresses are not linked to identity

in practice, maybe not so much

Conclusions

does Coinjoin

How much anonymity ~~does Bitcoin~~ really provide?

in theory, a lot! addresses are not linked to identity

in practice, maybe not so much

in theory, can achieve perfect **taint resistance**

Conclusions

does Coinjoin

How much anonymity ~~does Bitcoin~~ really provide?

in theory, a lot! addresses are not linked to identity

in practice, maybe not so much

in theory, can achieve perfect **taint resistance**

in practice, depends on auxiliary information

Conclusions

does Coinjoin

How much anonymity ~~does Bitcoin~~ really provide?

in theory, a lot! addresses are not linked to identity

Thanks! Any questions?

in theory, can achieve perfect **taint resistance**

in practice, depends on auxiliary information