

Lecture 9

Anonymity in Cryptocurrencies

Some say Bitcoin provides anonymity

“ Bitcoin is a secure and anonymous digital currency ”

— WikiLeaks donations page

Others say it doesn't

“ Bitcoin won't hide you from the NSA's prying eyes”

— Wired UK

What do we mean by anonymity?

Literally: anonymous = without a name

Bitcoin addresses are public key hashes rather than real identities

Computer scientists call this pseudonymity

Anonymity in computer science

Anonymity = pseudonymity + unlinkability



Different interactions of the same user with the system should not be linkable to each other

Pseudonymity vs anonymity in forums

Reddit: pick a long-term pseudonym

vs.

4Chan: make posts with no attribution at all

Why is unlinkability needed?

1. Many Bitcoin services require real identity
1. Linked profiles can be deanonymized by a variety of side channels

Defining unlinkability in Bitcoin

- Hard to link different addresses of the same user
- Hard to link different transactions of the same user
- Hard to link sender of a “payment” to its recipient

Quantifying anonymity

Anonymity set: Anonymity set of a transaction T is the set of transactions which an adversary cannot distinguish from T .

To calculate anonymity set:

- define adversary model
- reason carefully about: what the adversary knows, does not know, and cannot know

Why anonymous cryptocurrencies?

Block chain based currencies are totally, publicly, and permanently traceable

Without anonymity, privacy is much worse than traditional banking!

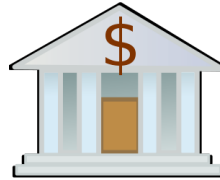
Anonymous e-cash: history



Introduced by David Chaum, 1982

Blind signature: a two-party protocol to create digital signature without signer learning which message is being signed

- An example of secure two-party computation

Anonymous e-cash via blind signatures



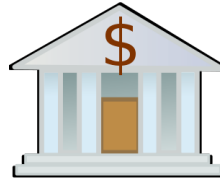
User	Balance
...	...
	10
...	...
	5



Spent coins
...

Anonymous e-cash via blind signatures



Withdraw anonymous coin



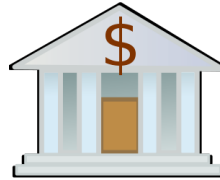
User	Balance
...	...
	10
...	...
	5



Spent coins
...

Anonymous e-cash via blind signatures



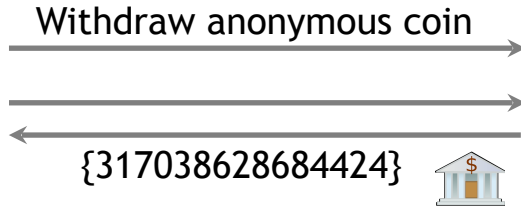
Withdraw anonymous coin





User	Balance
...	...
	9
...	...
	5

Spent coins
...

Anonymous e-cash via blind signatures



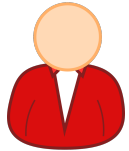
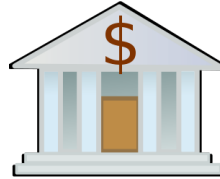
User	Balance
...	...
	9
...	...
	5



Spent coins
...

Anonymous e-cash via blind signatures



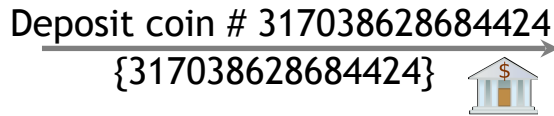
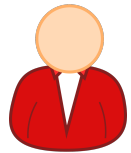
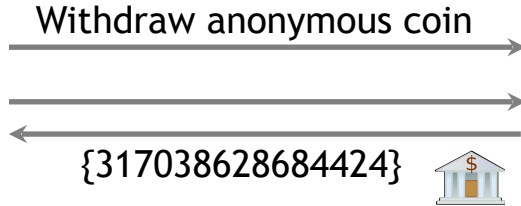
Withdraw anonymous coin →
→
← {317038628684424}



User	Balance
...	...
	9
...	...
	5

Spent coins
...

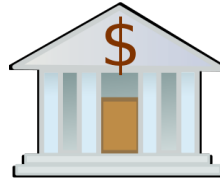
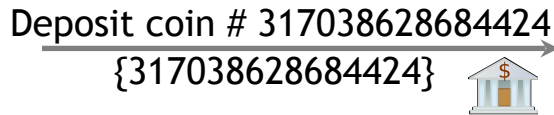
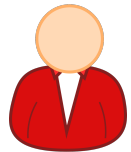
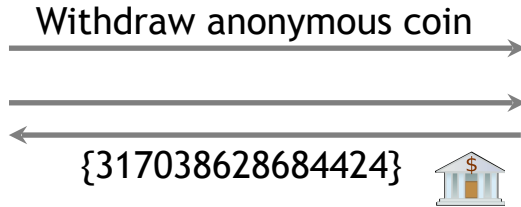
Anonymous e-cash via blind signatures



User	Balance
...	...
	9
...	...
	5

Spent coins
...

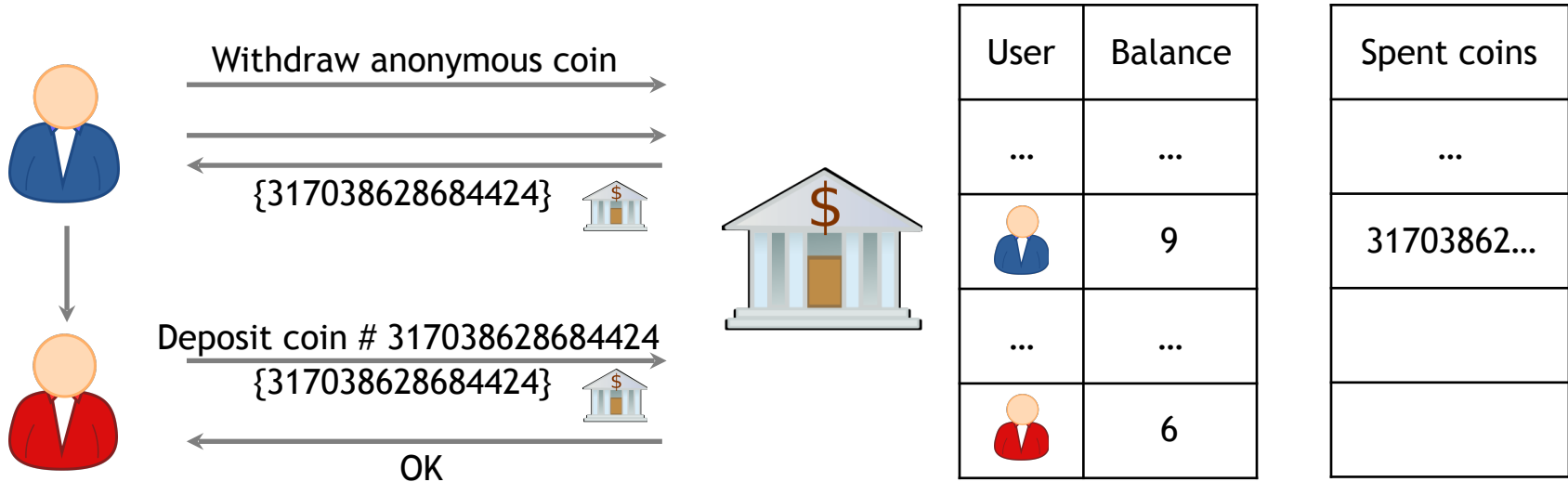
Anonymous e-cash via blind signatures



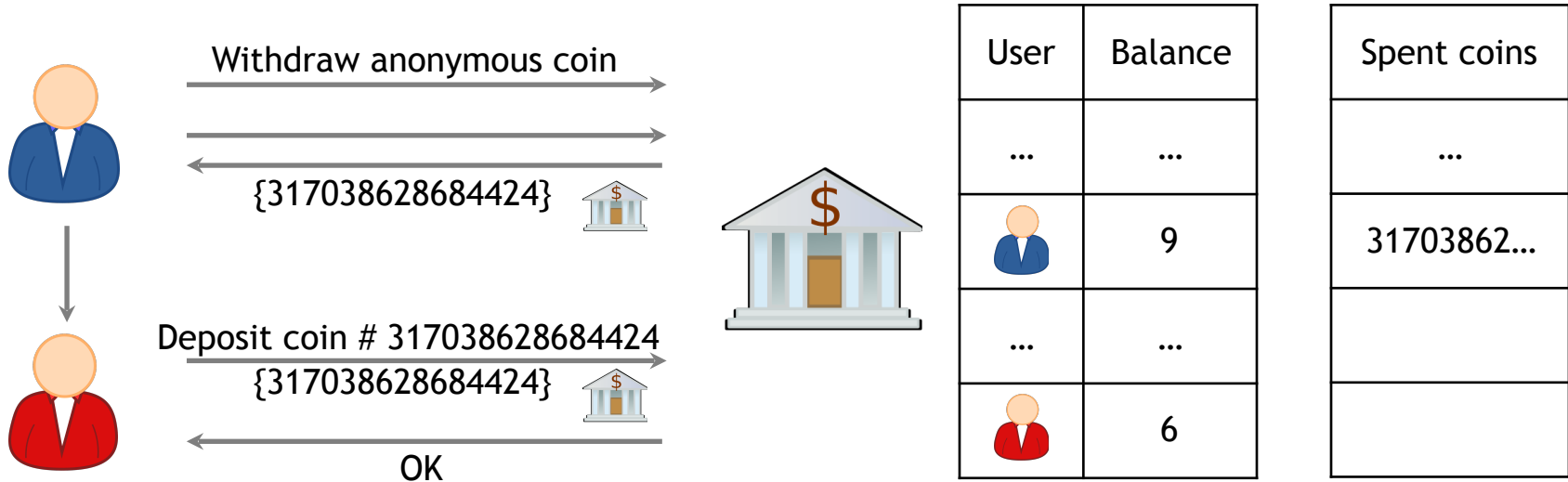
User	Balance
...	...
	9
...	...
	6

Spent coins
...
31703862...

Anonymous e-cash via blind signatures



Anonymous e-cash via blind signatures



Bank cannot link the two users

Anonymity & decentralization: in conflict

- Interactive cryptographic protocols with bank are hard to decentralize
 - Later: Zerocoin and Zerocash overcome this challenge by using non-interactive cryptographic techniques
- Decentralization often achieved via public traceability to enforce security

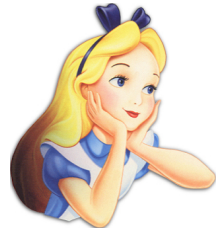
How to de-anonymize Bitcoin

Trivial to create new addresses in Bitcoin

Best practice: always receive at fresh address

So, unlinkable?

Alice buys a teapot at Big box store



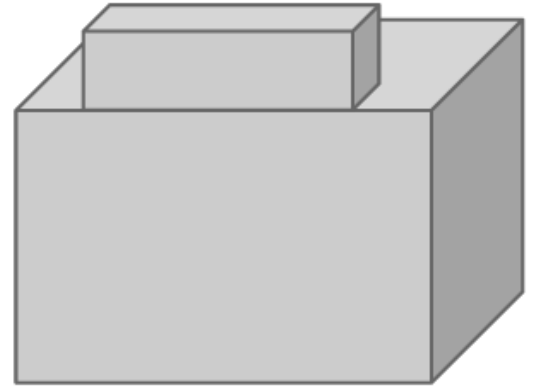
5

3

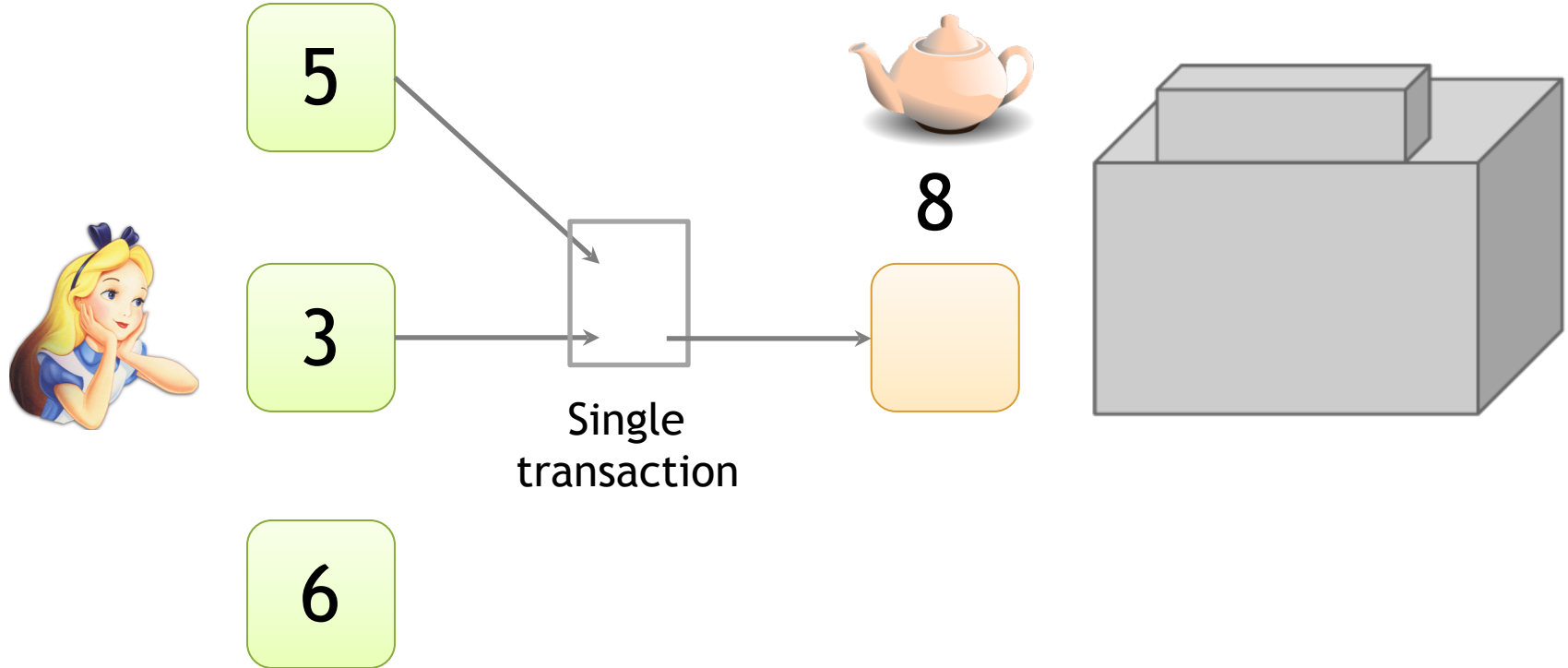
6



8

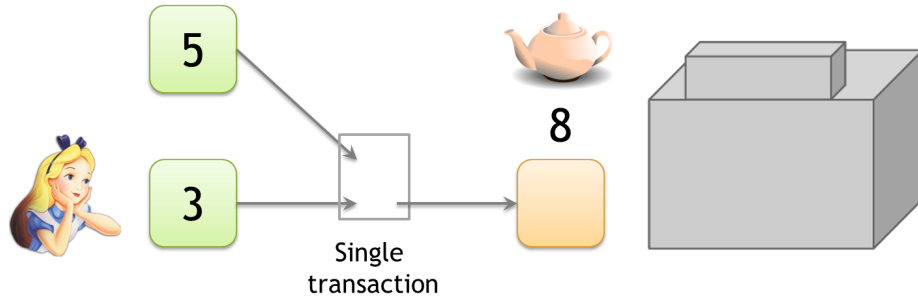


Alice buys a teapot at Big box store



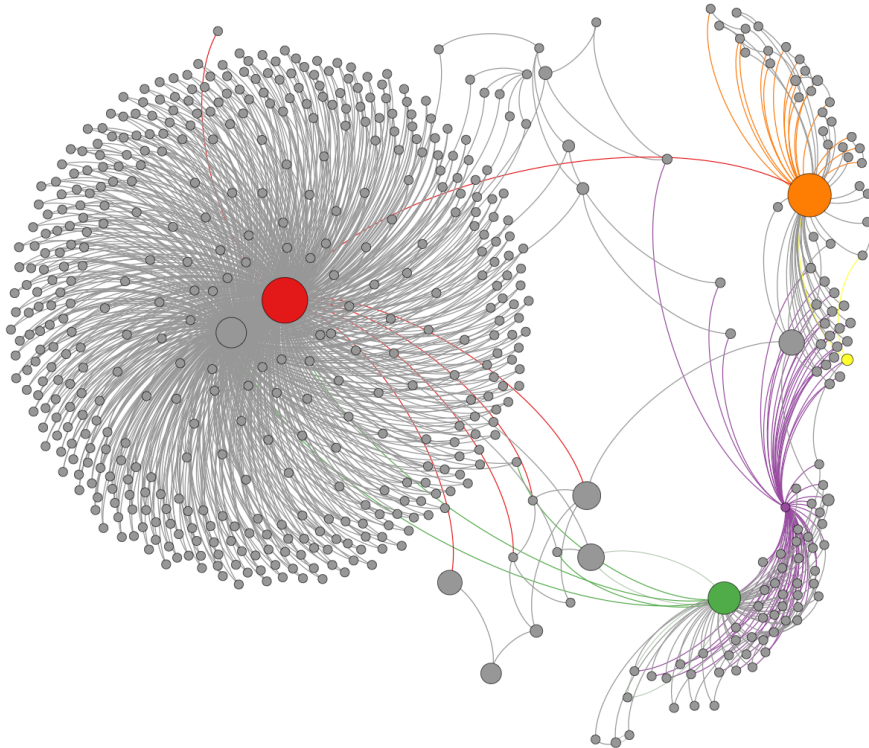
Linking addresses

Shared spending is evidence of joint control



Addresses can be linked transitively

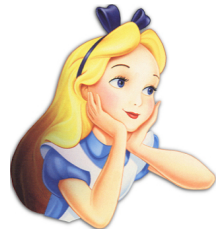
Clustering of addresses



*An Analysis of Anonymity
in the Bitcoin System*

F. Reid and M. Harrigan
PASSAT 2011

Change addresses



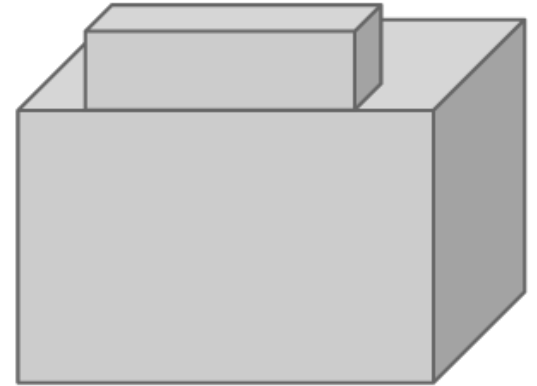
5

3

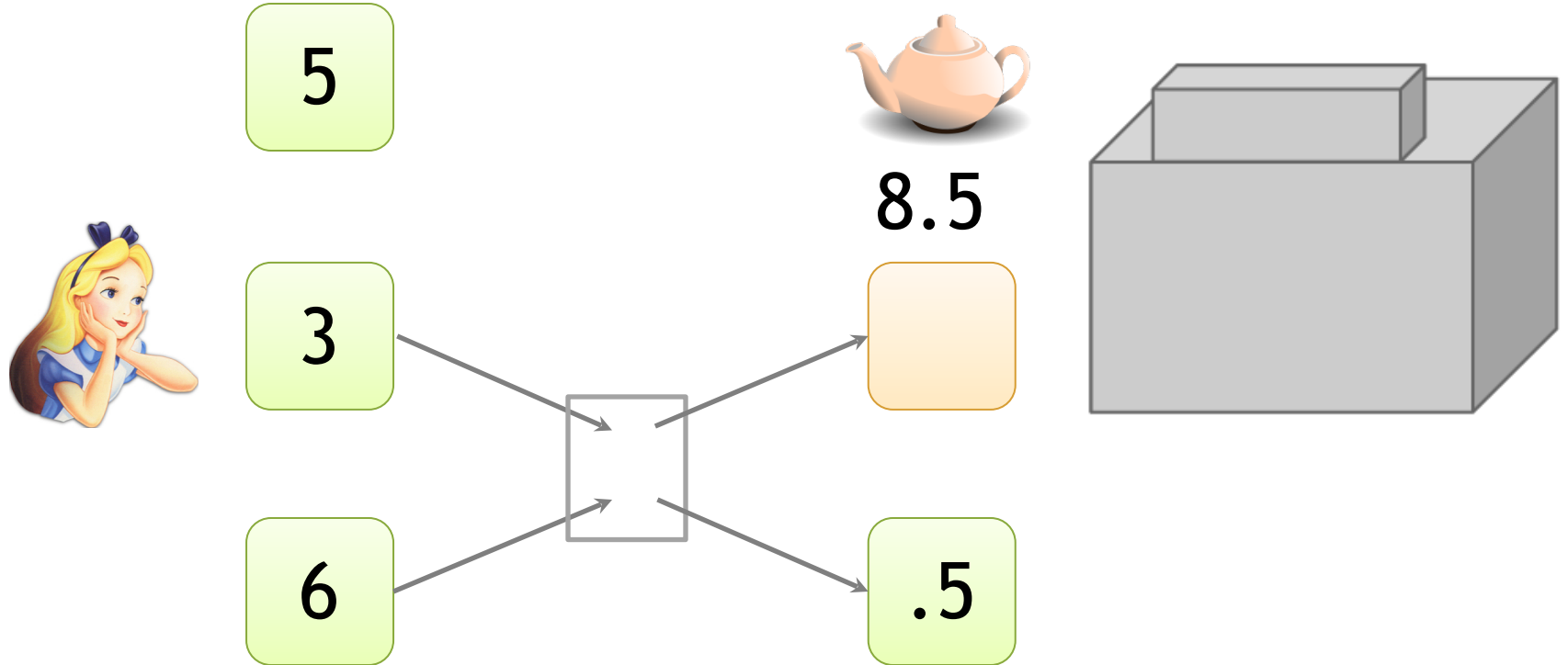
6



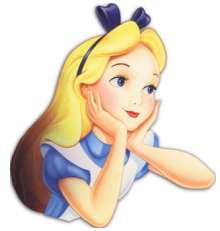
8.5



Change addresses



Change addresses

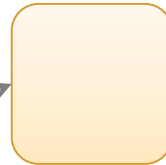


5



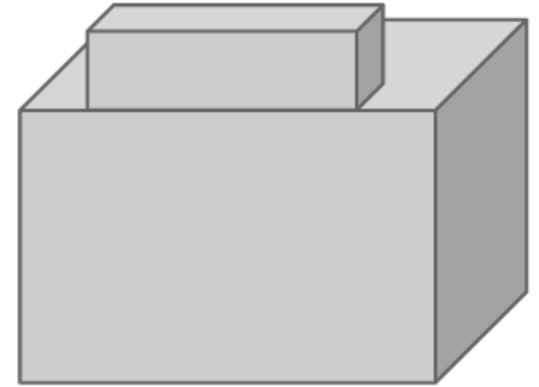
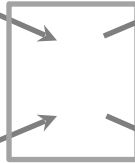
8.5

3



6

.5



Which address is change?

“Idioms of use”

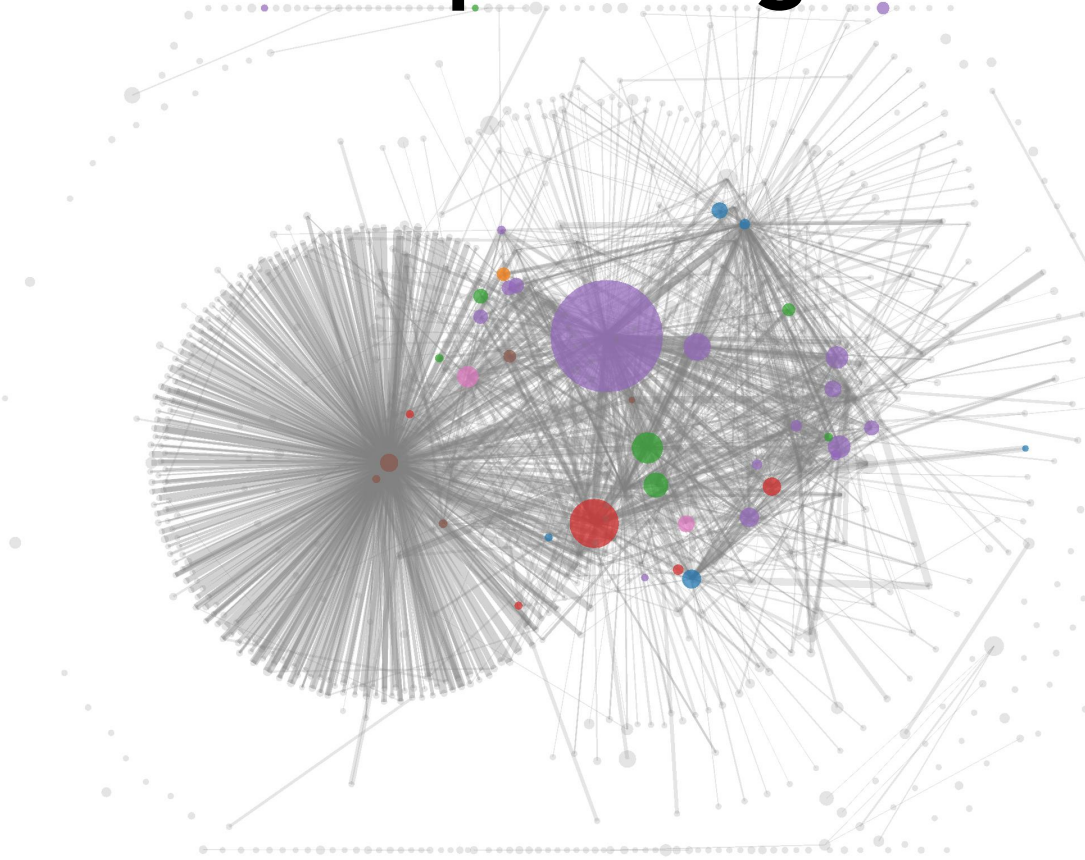
Idiosyncratic features of wallet software

e.g., each address used only once as change

Shared spending + idioms of use

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

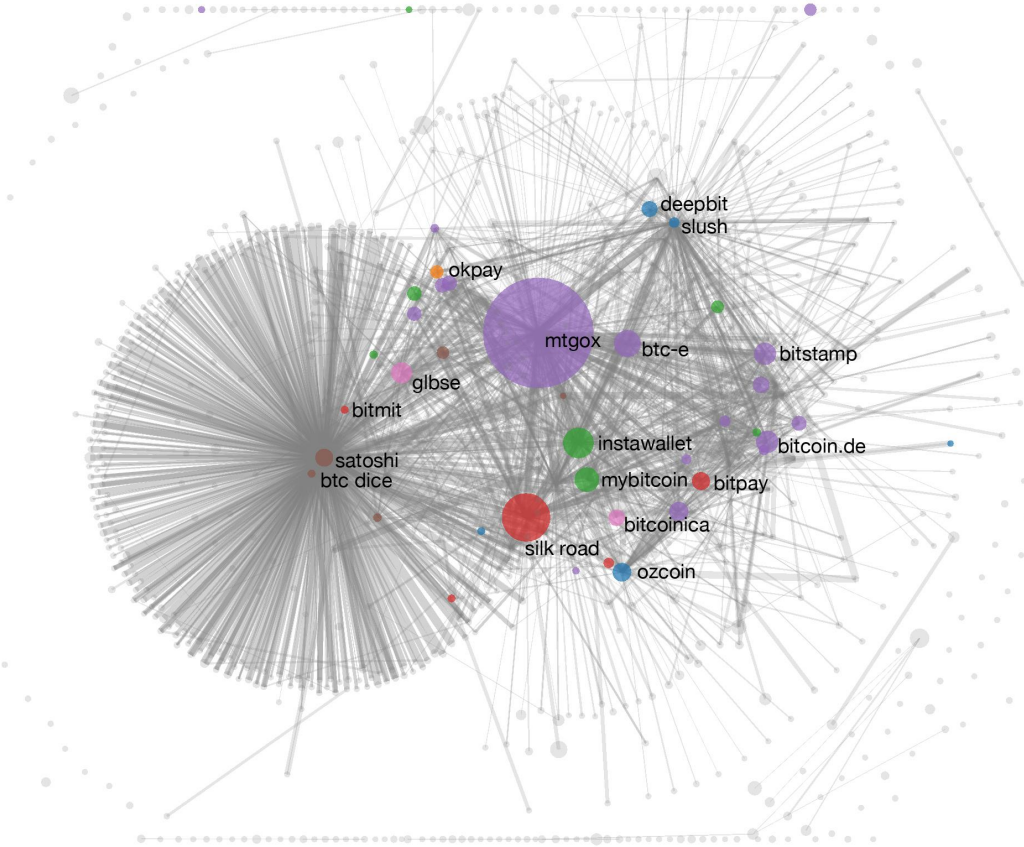
S. Meiklejohn et al.
IMC 2013



Shared spending + idioms of use

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

S. Meiklejohn et al.
IMC 2013



From services to users

1. High centralization in service providers

Most flows pass through one of these – in a traceable way

2. Address – identity links in forums

Achieving Anonymity

Approaches

- **Mixing:** Pool in multiple transactions (ideally same value), and then create new transactions
 - Centralized: E.g., online wallets
 - Decentralized: E.g., CoinJoin
 - Untrusted intermediary using crypto: Tumblebit
- **New cryptocurrencies:**
 - Using Zero-knowledge proofs: Zerocoin and Zerocash
 - Using Ring signatures: Monero

Approaches

- **Mixing:** Pool in multiple transactions (ideally same value), and then create new transactions
 - Centralized: E.g., online wallets
 - Decentralized: E.g., CoinJoin (e.g., implementation: Dash)
 - Untrusted intermediary using crypto: Tumblebit
- **New cryptocurrencies:**
 - Using Zero-knowledge proofs: Zerocoin and Zerocash
 - Using Ring signatures: Cryptonote (e.g., implementation: Monero)