Anonymity and Privacy in Cryptocurrencies

Instructor: Matthew Green
Fall 2020

Some slides adapted from NBFMG

Housekeeping

- Midterm out yesterday on Gradescope!
    - Midterm due tomorrow (10/29) at 5pm Eastern Time
    - Open book/open notes but it's also a midterm — do not work with anyone else!

News?

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!

Whale Moves $1.16B Bitcoin in Largest-Ever Dollar Transaction

beincrypto.com | 1d

Trending People

Keith Raniere

Keith Raniere is an Americ
entrepreneur best known a

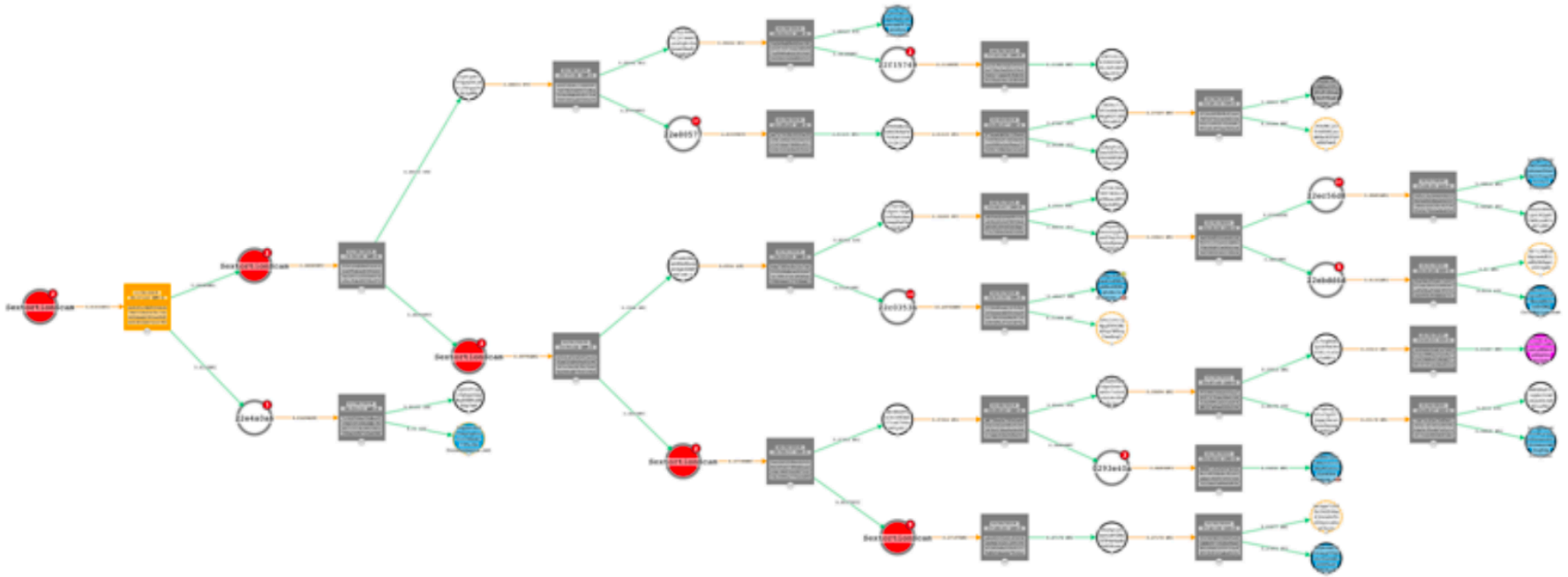
Dez Bryant

Desmond Demond Bryant
American footballer who p

Lindsey Graham

Lindsey Olin Graham (born
1955) is an American polit

Chrissy Teigen



Additionally, 1PXf also sent 0.01359 BTC to GoURL, another 0.0098 BTC to Empire Market (Dark Market), and 0.00507 BTC to Bovada (Gambling). Plus, it sent 0.1405 BTC to 3PFFkzVgbxhwHejFyZeeyXKBFG7dL5gRcj, which still maintained that balance as of December 6.

Several recipients of the emails reported that their payment instructions cited the 1PXf address

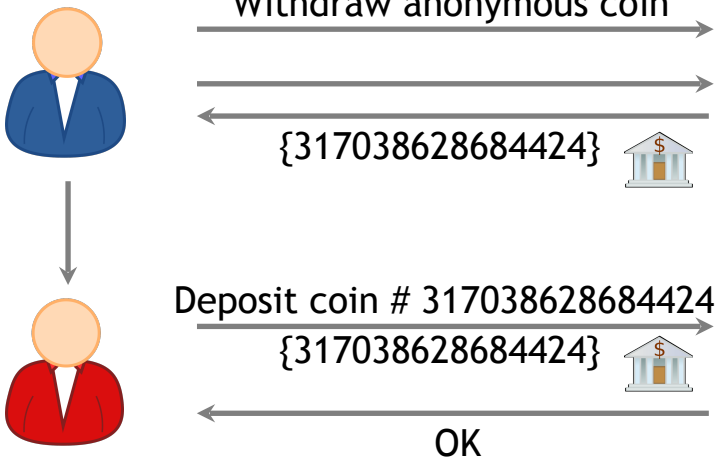
Anonymous e-cash: history

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
…	…
	9
…	…
	6

Spent coins
…
31703862…

Bank cannot link the two users

Anonymity & decentralization: in conflict

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

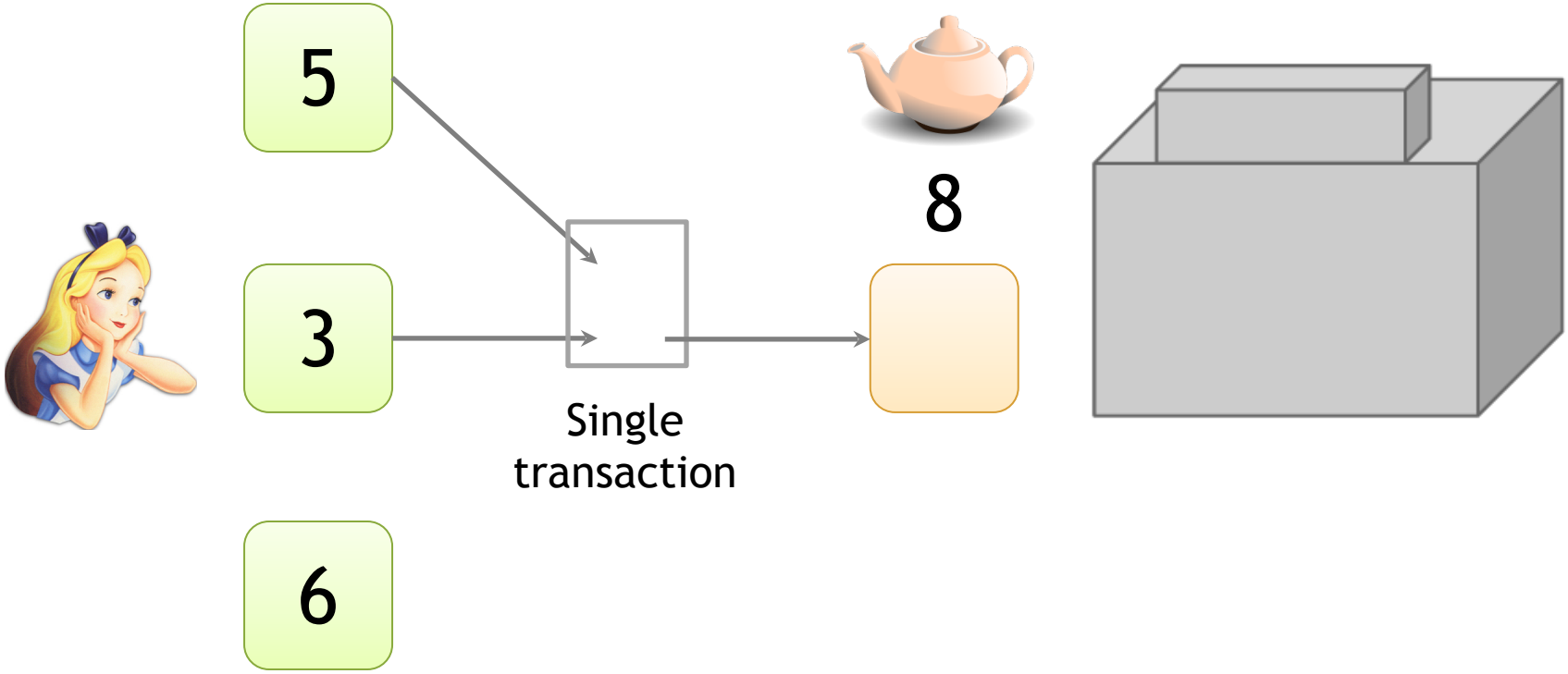
How to de-anonymize Bitcoin

Trivial to create new addresses in Bitcoin

Best practice: always receive at fresh address

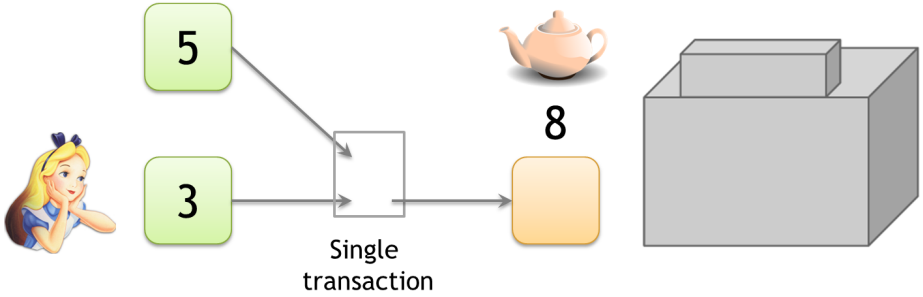
So, unlinkable?

Alice buys a teapot at Big box store



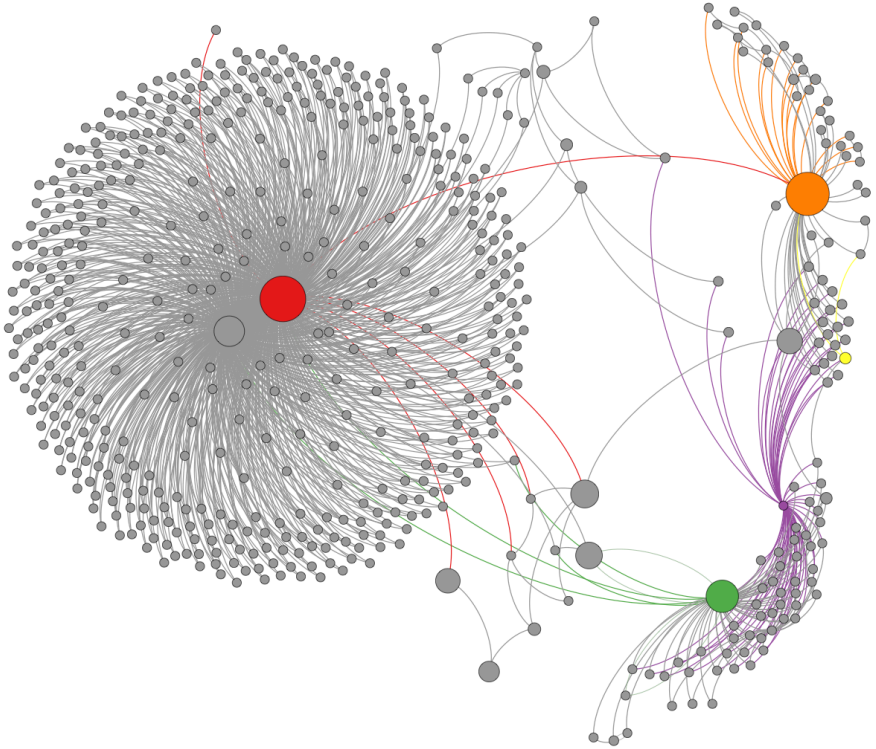
Linking addresses

Shared spending is evidence of joint control



Addresses can be linked transitively

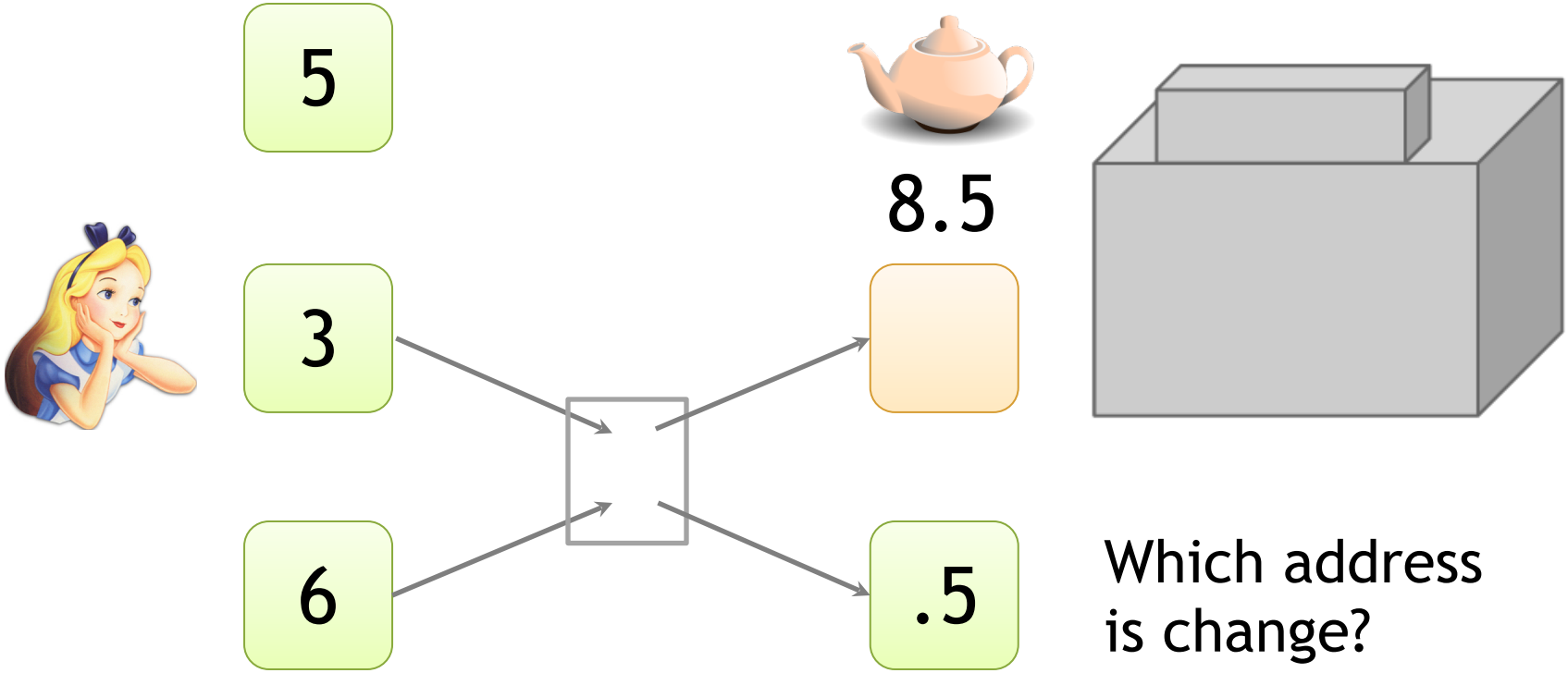
Clustering of addresses



An Analysis of Anonymity in the Bitcoin System

F. Reid and M. Harrigan
PASSAT 2011

Change addresses



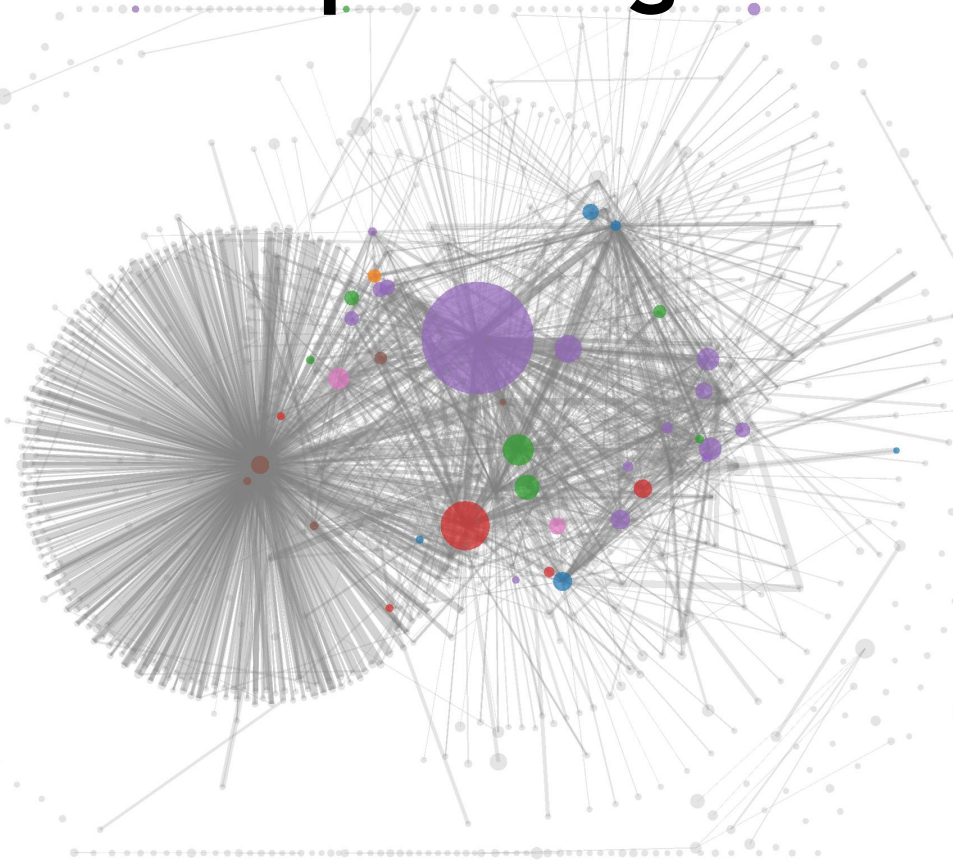
Which address is change?

“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

To tag service providers: transact!

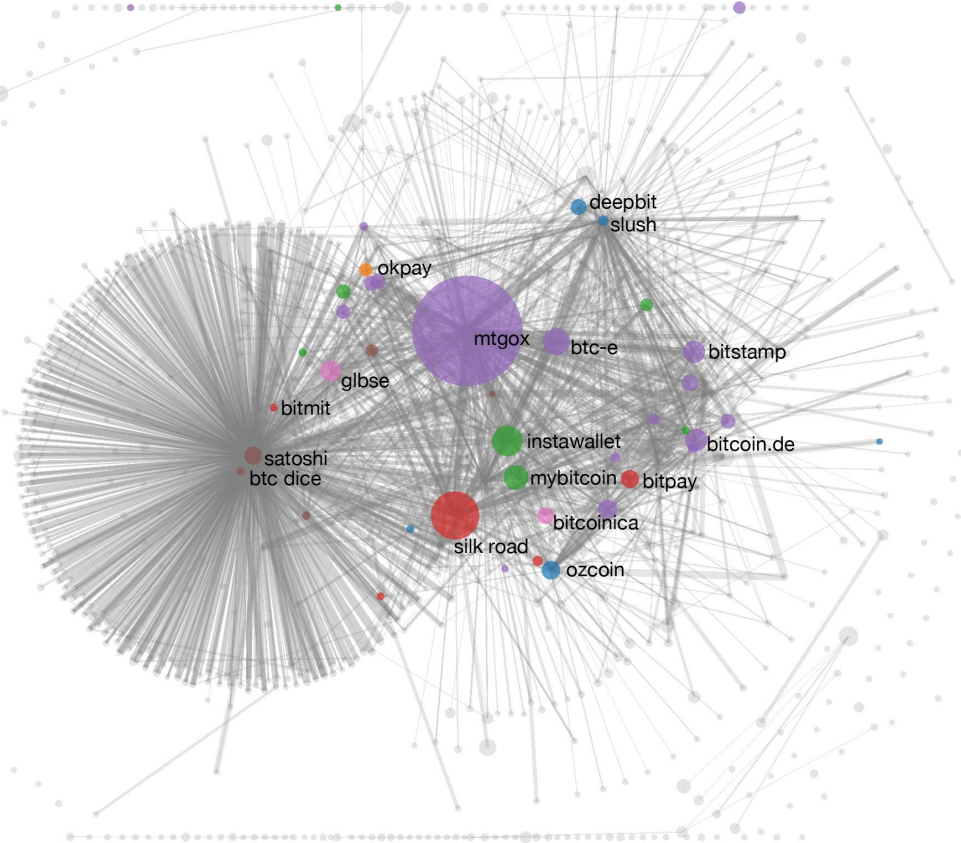
A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

S. Meiklejohn et al.

344 transactions

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

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)