

Blockchains & Cryptocurrencies

Anonymity



Image from cryptonomad.info

Instructor: Abhishek Jain
Johns Hopkins University - Spring 2021

*Some slides based on NBFMG

Housekeeping

- Course Project Idea Due on 02/26

Today

- New Thread: **Anonymity**

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
2. 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!

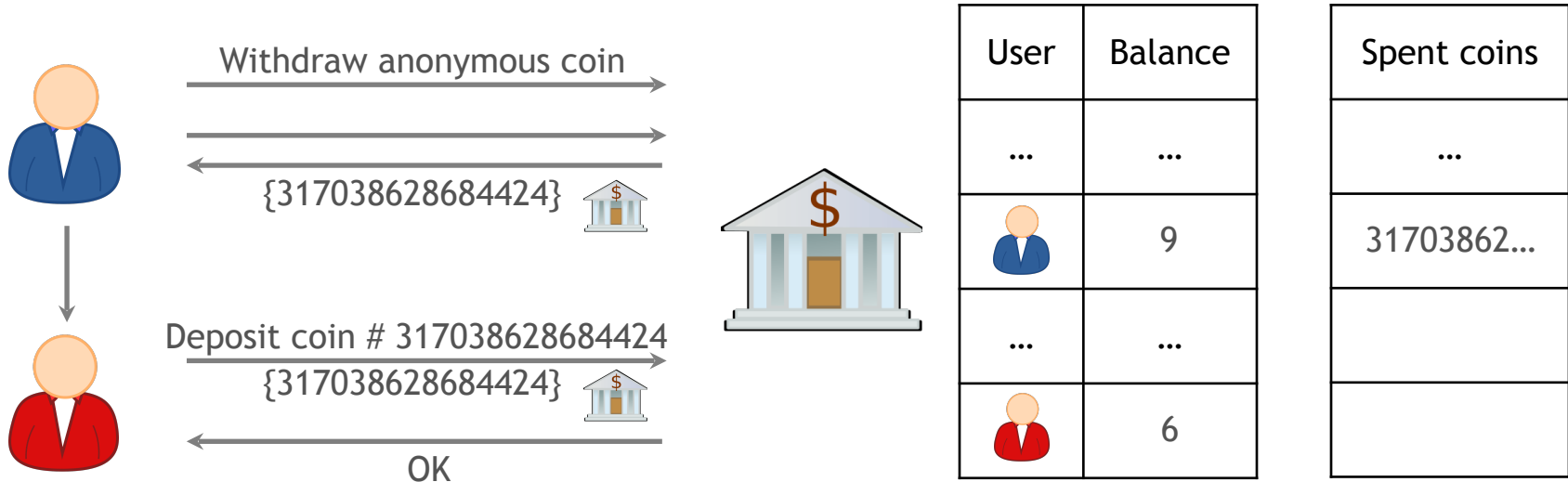
Anonymous e-cash: history

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



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

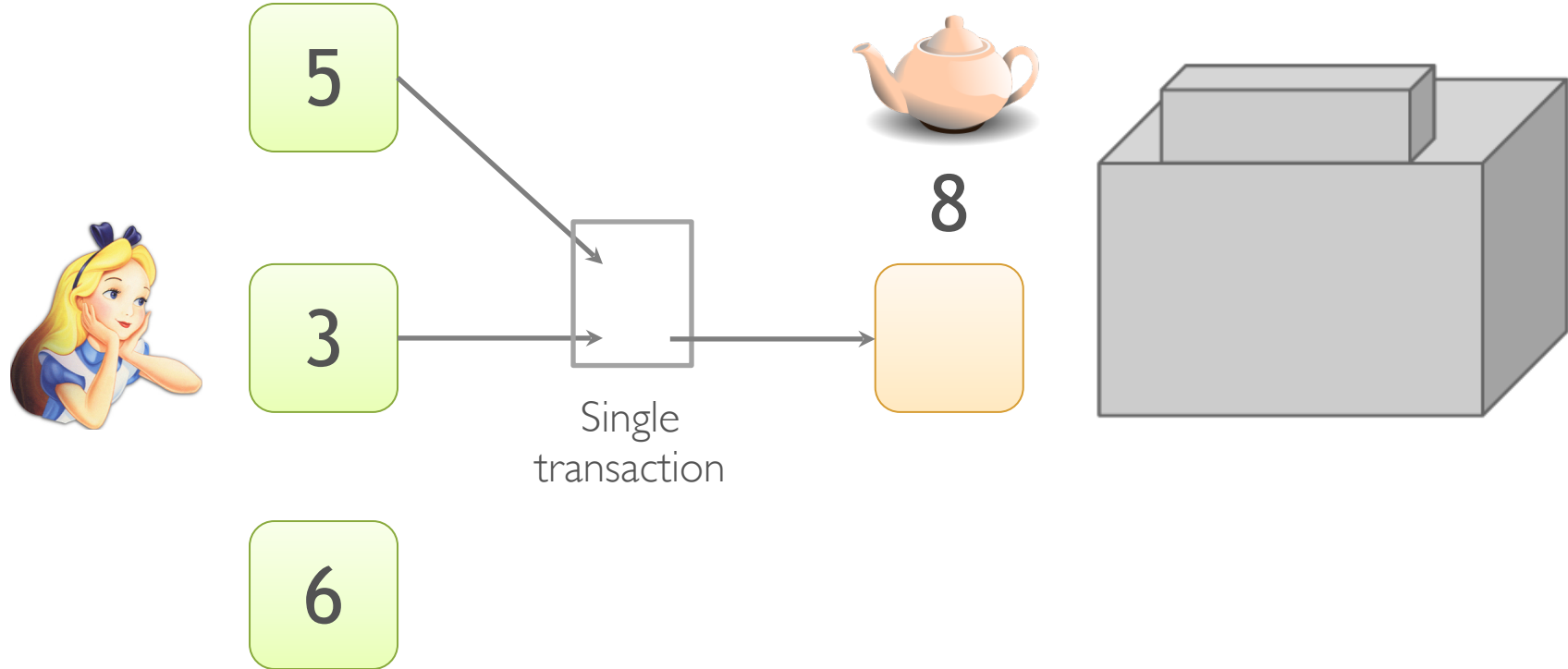
How to de-anonymize Bitcoin

Trivial to create new addresses in Bitcoin

Best practice: always receive at fresh address

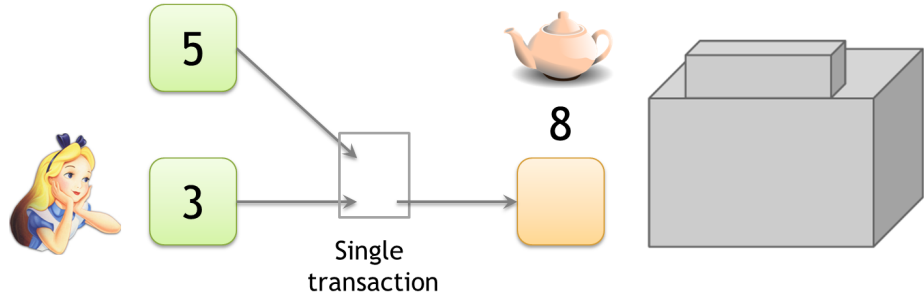
So, unlinkable?

Alice buys a teapot at Big box store



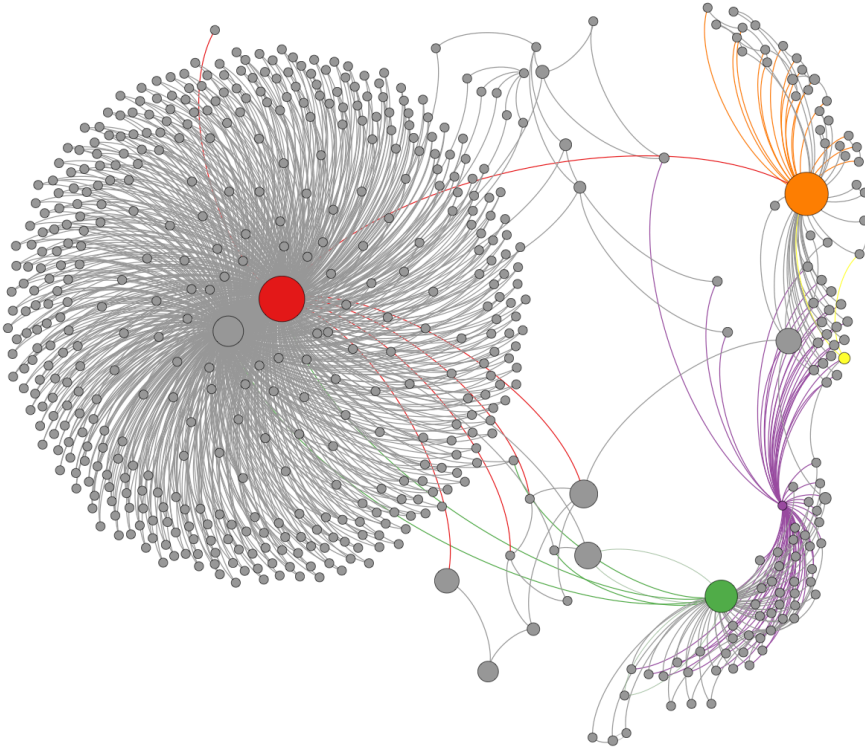
Linking addresses

Shared spending is
evidence of joint cont



Addresses can be linked transitively

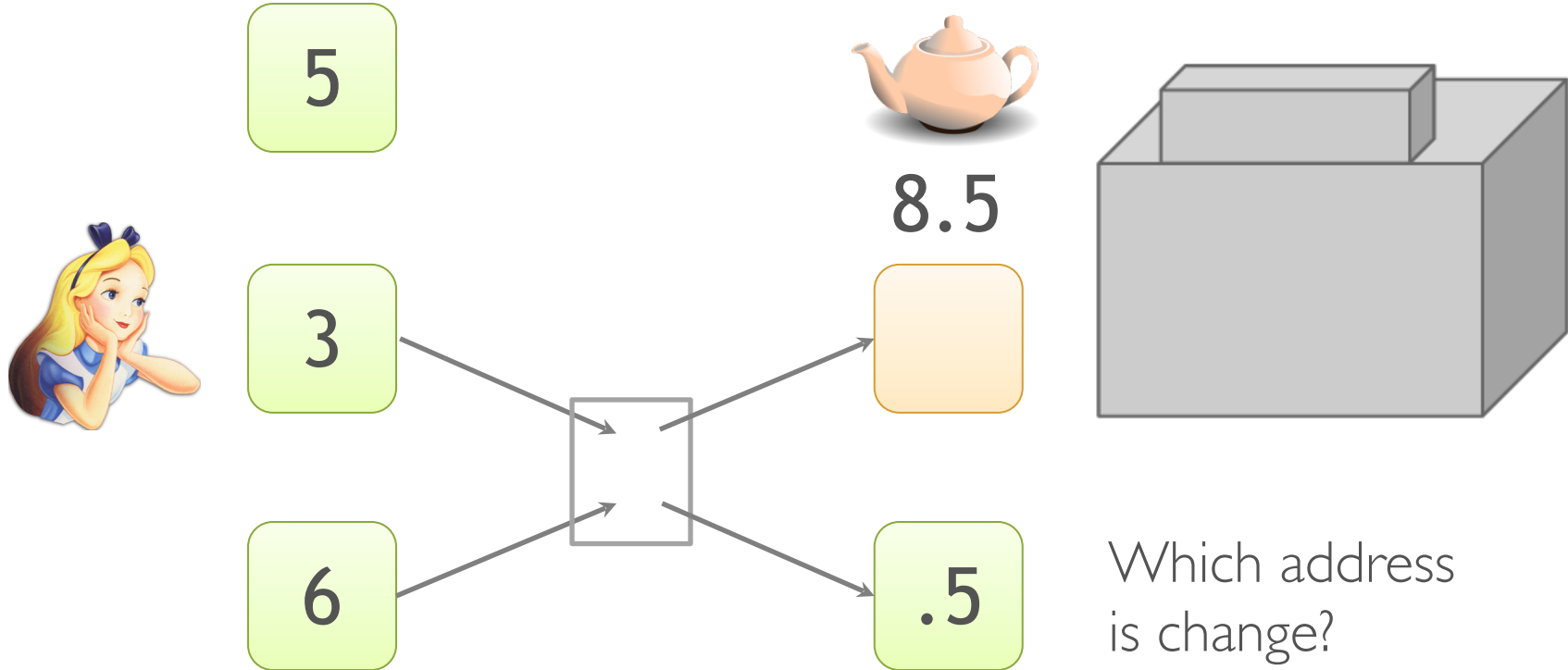
Clustering of addresses



An Analysis of Anonymity in
the Bitcoin System

F. Reid and M. Harrigan
PASSAT 2011

Change addresses



“Idioms of use”

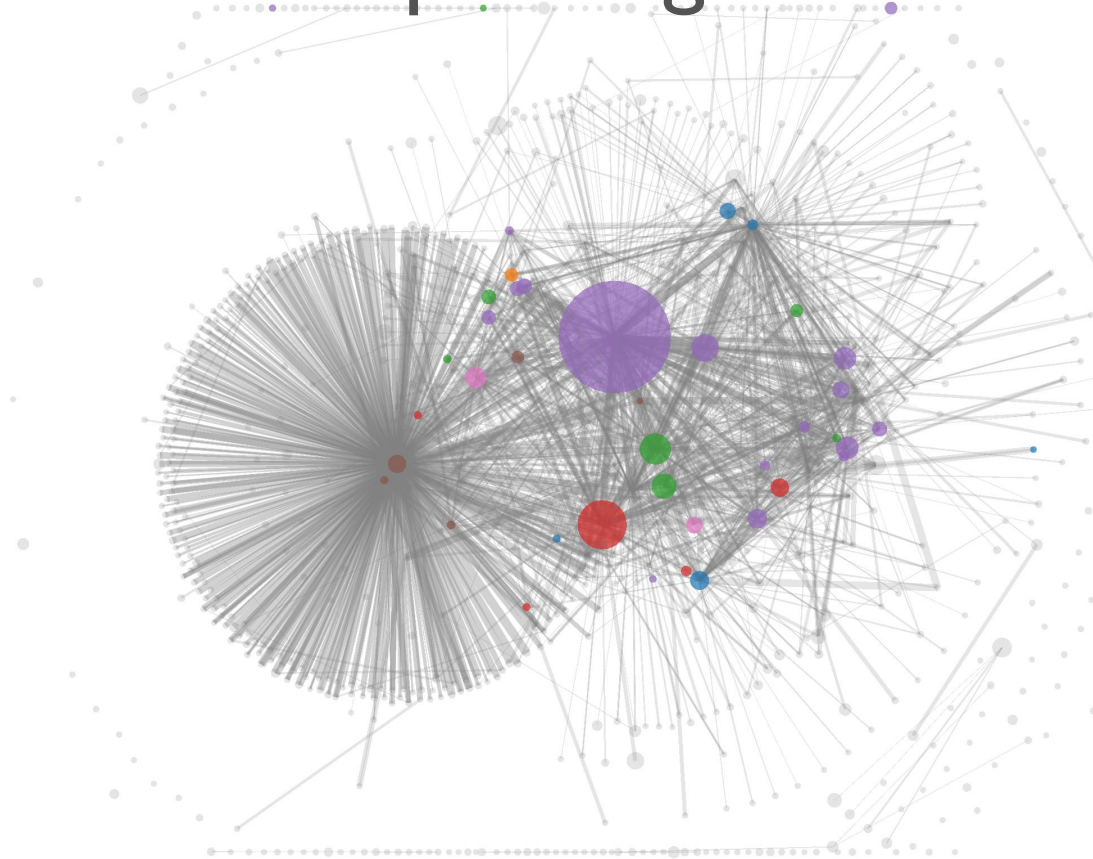
Idiosyncratic features of wallet software

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.

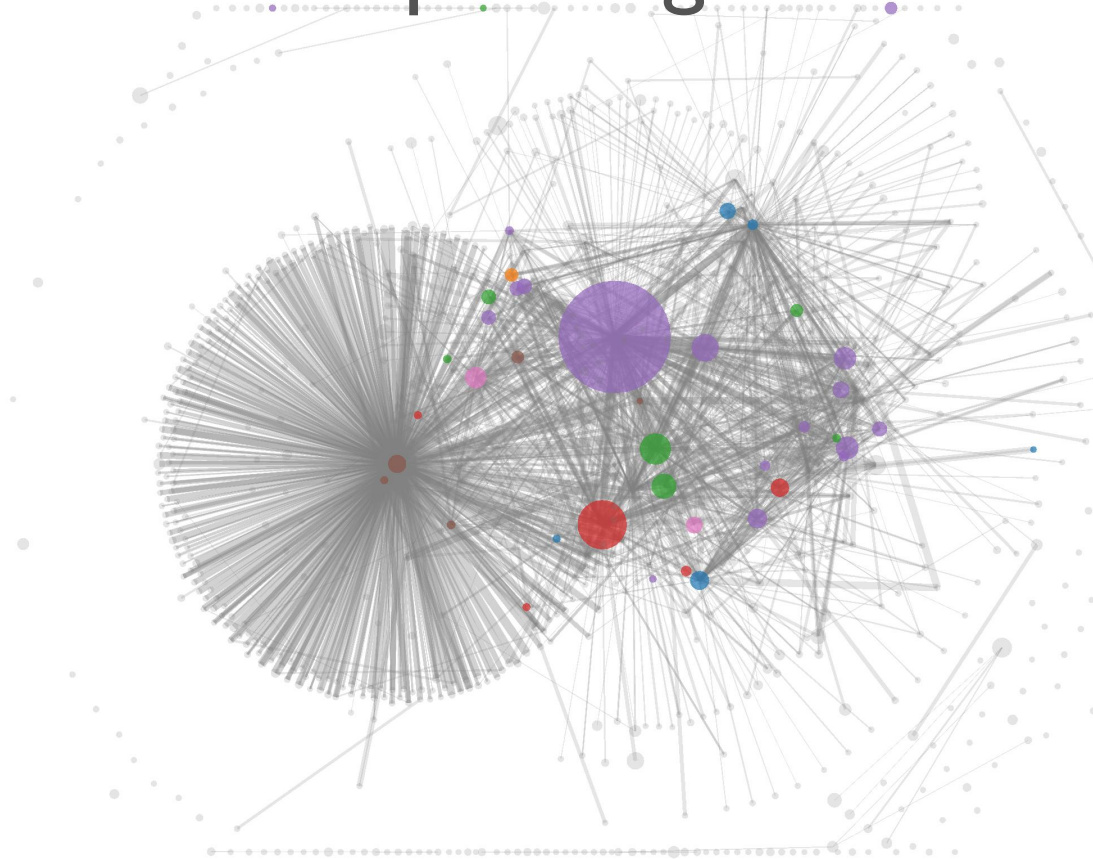
344 transactions

- 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

Early solutions

- **Mixes**

- Create a centralized server, many people send coins
- Mixer shuffles those together, sends the right amount back to each user (less a fee), thus unlinking the sources of transactions
 - Risk 1: Mixer can “exit” and steal your cash
 - Risk 2: Mixer keeps track of the sources/destinations
 - Risk 3: Low volume of mixing can make tracing easy

Early solutions

- **CoinJoin**

- Proposed by Maxwell; variants even earlier by “killerstorm” on BitcoinTalk*
- Solves the “scamming mixer” problem
- Idea: each transaction has multiple inputs and outputs
 - Have a mixer author one single transaction that consumes
N equal-value inputs, produces N outputs

CryptoNote & RingCT

- 2012: CryptoNote (“Nicolas van Saberhagen”)
 - Originally launched as part of the ByteCoin currency
 - Anonymous creator, did a pre-mine
 - Was forked multiple times into many different currencies, including bitmonero -> Monero
 - Protocol ideas later improved into RingCT, which hid amounts as well as inputs (used in Monero today)

CryptoNote idea

- I want to make a transaction with (e.g.,) one input
 - But I don't want to reveal which transaction is my input
 - Standard Bitcoin transactions do reveal this, and it leads to privacy problems
 - I could mix with other people (e.g., CoinJoin) but they would have to participate with me online, and that's annoying

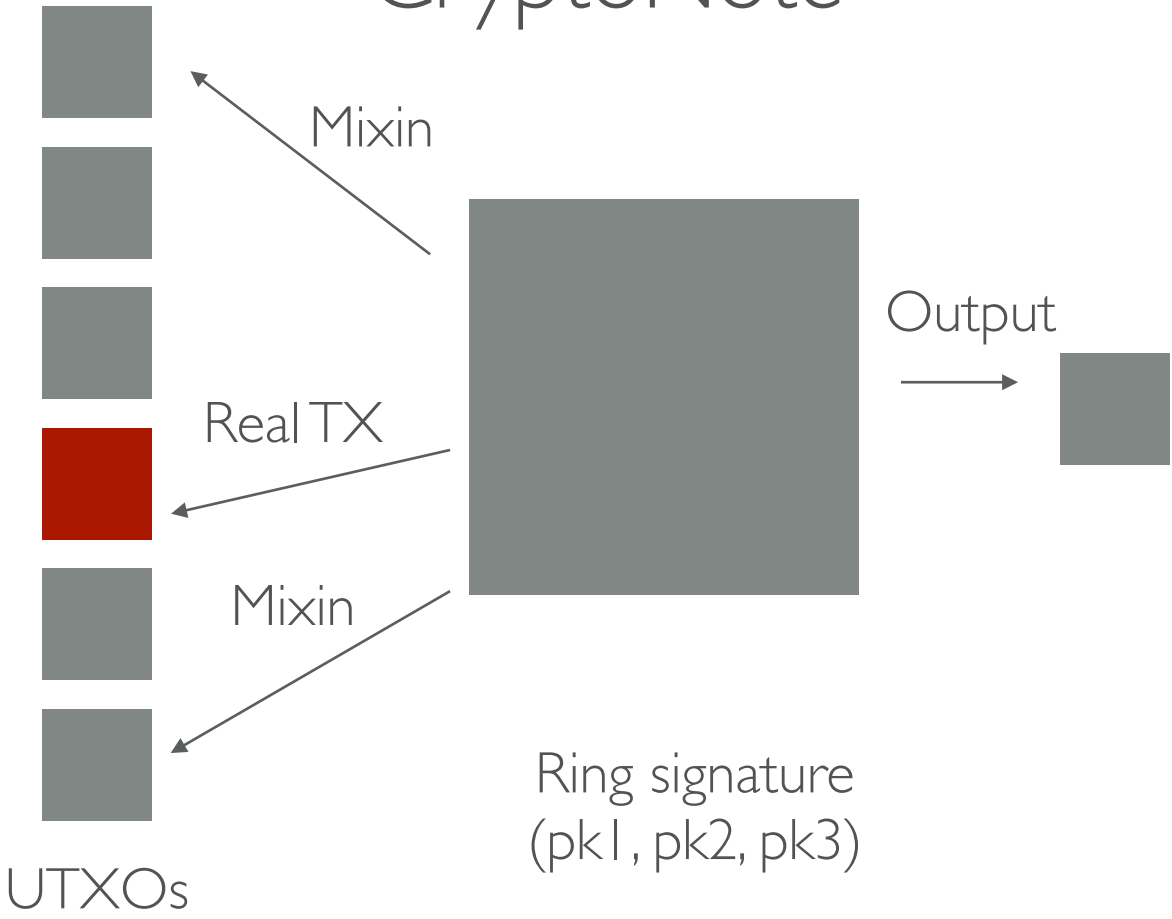
Ingredient: Ring Signatures

- Normal signature: sign with sk , verify with pk
- **Ring signature:**
 - Sign with my secret key + $N-1$ other people's public keys
(Signer does not have to know the other secret keys!)
 - Verifier verifies with all N public keys (she must know them)
 - **Privacy:** verifier does not learn which signer actually made the signature! (It could be any of the key owners!)

CryptoNote idea

- Make all transactions the same value (e.g., 1 ByteCoin)
- Make all addresses single-use (auto-generated)
- Assume (for simplicity) that spender has one “real” input
 1. Identify $N-1$ unrelated “cover” transactions from the UTXO set, get those public keys (“mixins”)
 2. Make a ring signature on her transaction, using her secret key and the $N-1$ public keys for the mixing
 3. Post signature plus a “key image” (function of the real secret key) to prevent the real transaction being spent twice

CryptoNote



CryptoNote Limitations

- CryptoNote ring signatures grow as $O(N)$ where N is number of inputs (including Mixins)
 - Ditto signing time and verification time
 - In practice this limits Mixin number to something modestly small (1-7)
 - Original CryptoNote required all input transactions be the same value, requiring multiple “denominations” (RingCT fixes this)
 - Surprisingly advanced crypto, surprisingly advanced code