Lecture 6

Bitcoin and anonymity

Lecture 6.1:

Anonymity basics

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 <u>pseudonymity</u>

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

Complete unlinkability (among <u>all</u> addresses/transactions) is hard

<u>Anonymity set</u>: the crowd that one attempts to blend into

To calculate anonymity set:
- define adversary model
- reason carefully about: what the adversary knows, does not know, and <u>cannot</u> know

Why anonymous cryptocurrencies?

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

Without anonymity, privacy is <u>much worse</u> than traditional banking!

What about money laundering?

Legitimate worry

Bottleneck: moving large flows into and out of Bitcoin ("cashing out")

Can we keep only the good uses?

Common conundrum in computer security and privacy:

uses that are very different <u>morally</u> are pretty much the same <u>technologically</u>

Similar dilemma: Tor

Anonymous communication network

Sender and receiver of message <u>unlinkable</u>

The picture can't be displayed.

Used by:
- Normal people
- Journalists & activists
- Law enforcement
- Malware
- Child pornographers

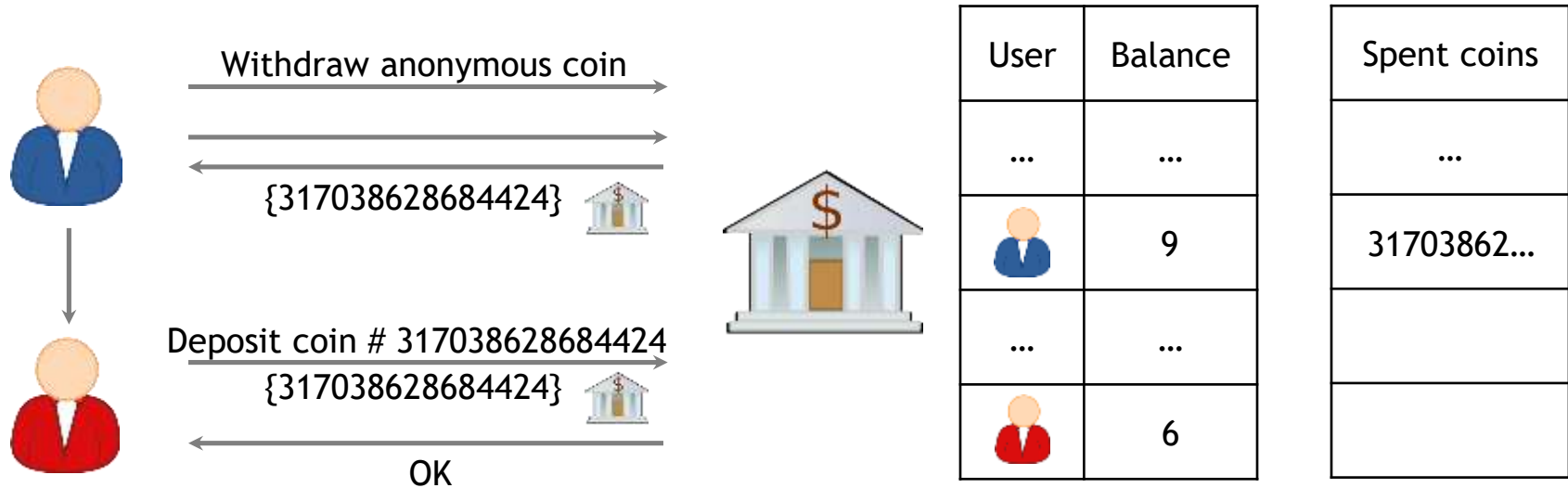Funded by (among others): U.S. State Department

Anonymous e-cash: history

David Chaum, 1982

Crypto magic

Blind signature:
two-party protocol to create digital signature without signer knowing the input

Anonymous e-cash via blind signatures

User	Balance
...	...
👤	9
...	...
👤	6

Spent coins
...
31703862...

Withdraw anonymous coin

{317038628684424}

Deposit coin # 317038628684424

{317038628684424}

OK

Bank cannot link the two users

Anonymity & decentralization: in conflict

- Interactive protocols with bank are hard to decentralize

- Decentralization often achieved via public traceability to enforce security

Lecture 6.2:

How to de-anonymize Bitcoin

Bitcoin

Bitcoin is a secure and anonymous digital currency. Bitcoins cannot be easily tracked back to you, and are safer and faster alternative to other donation methods. You can send BTC to the following address:

13DFamCvSxG8EG16VyXzdpfqxyooifswYx

Various sites offer a service to exchange other currency to/from Bitcoins. There are also services allowing trades of goods for Bitcoins. Bitcoins are not subject to central regulations and are still gaining value. To learn more about Bitcoins, visit the website (http://bitcoin.org) or read more on Wikipedia.

To generate a new, private address for your donation, click the refresh button above.

Bitcoin

Bitcoin is a secure and anonymous digital currency. Bitcoins cannot be easily tracked back to you, and are safer and faster alternative to other donation methods. You can send BTC to the following address:

16nLrMAQma6GJ4AavfxXLaZoeCHBBqqzX3

Various sites offer a service to exchange other currency to/from Bitcoins. There are also services allowing trades of goods for Bitcoins. Bitcoins are not subject to central regulations and are still gaining value. To learn more about Bitcoins, visit the website (http://bitcoin.org) or read more on Wikipedia.

To generate a new, private address for your donation, click the refresh button above.
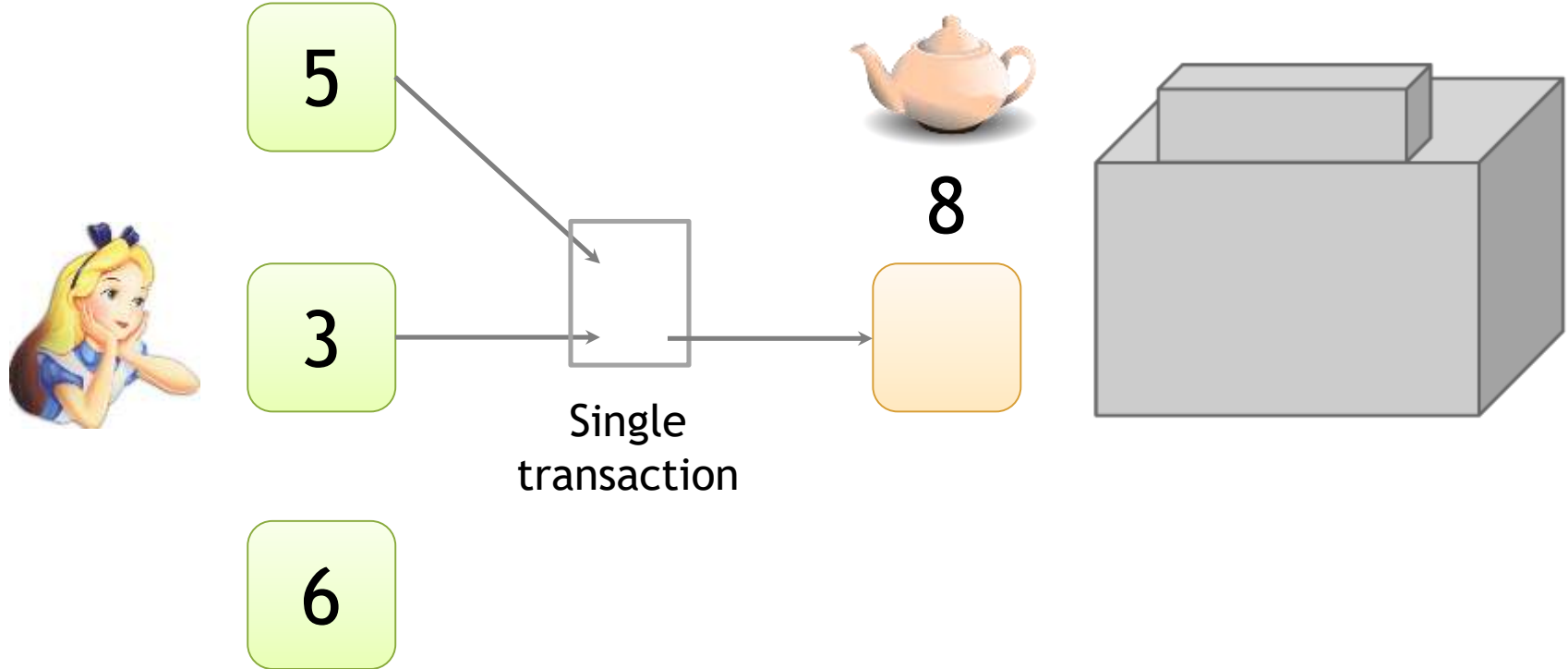
Trivial to create new address

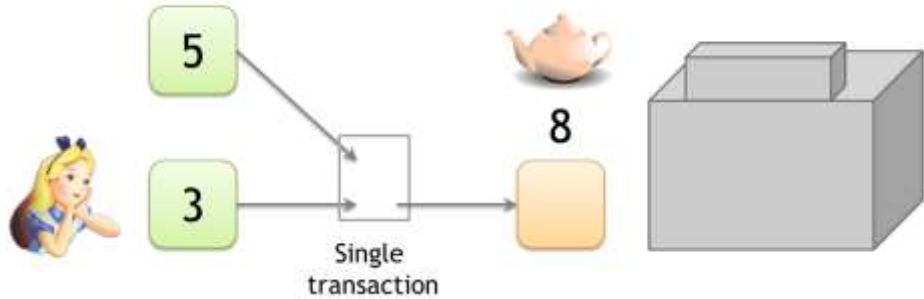Best practice: always receive at fresh address

So, unlinkable?

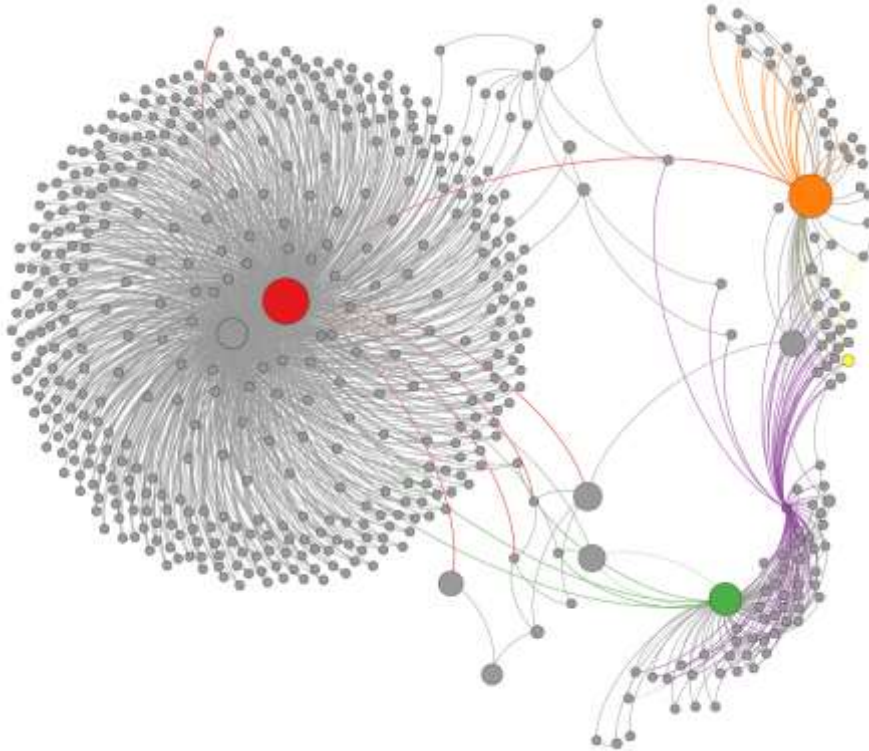# Alice buys a teapot at Big box store

Linking addresses

Shared spending is evidence of joint control

Addresses can be linked transitively
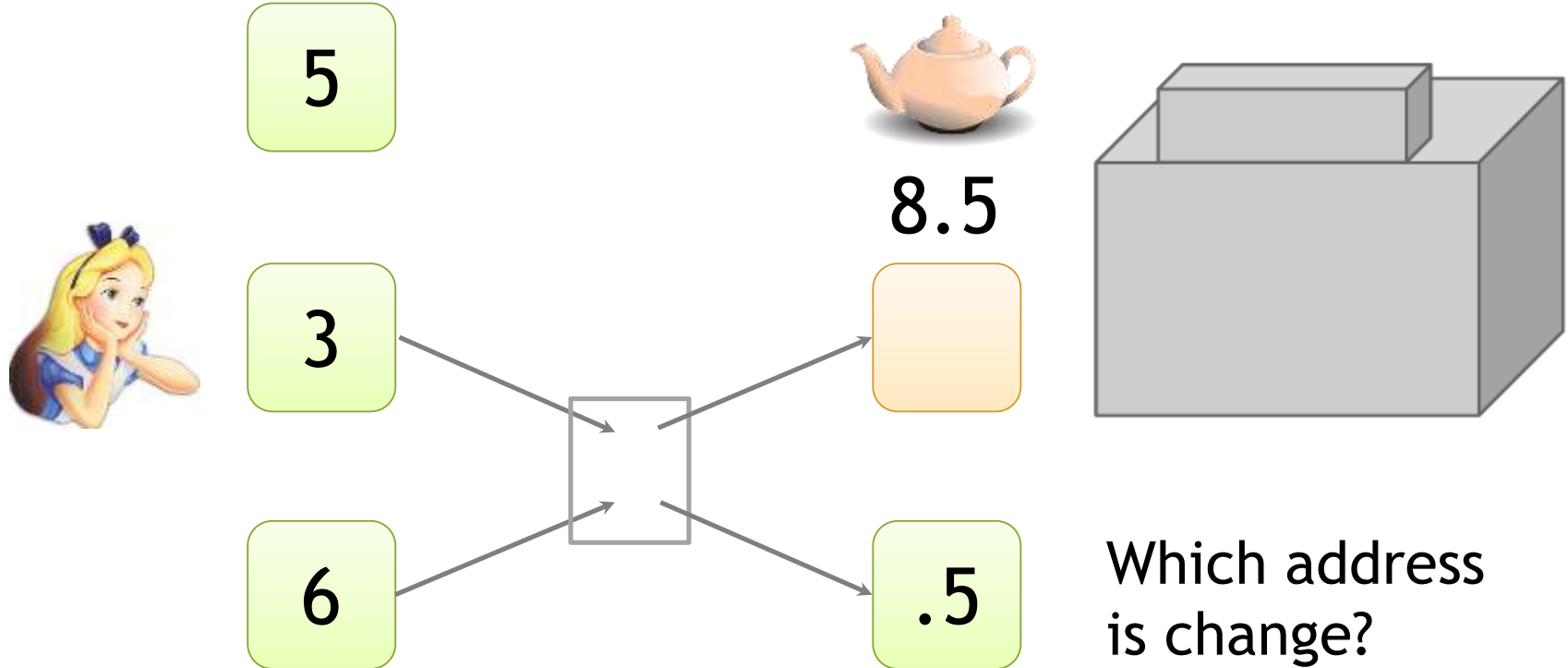
Clustering of addresses

An Analysis of Anonymity in the Bitcoin System

F. Reid and M. Harrigan
PASSAT 2011

Change addresses

5

3

6

8.5

.5

Which address is change?
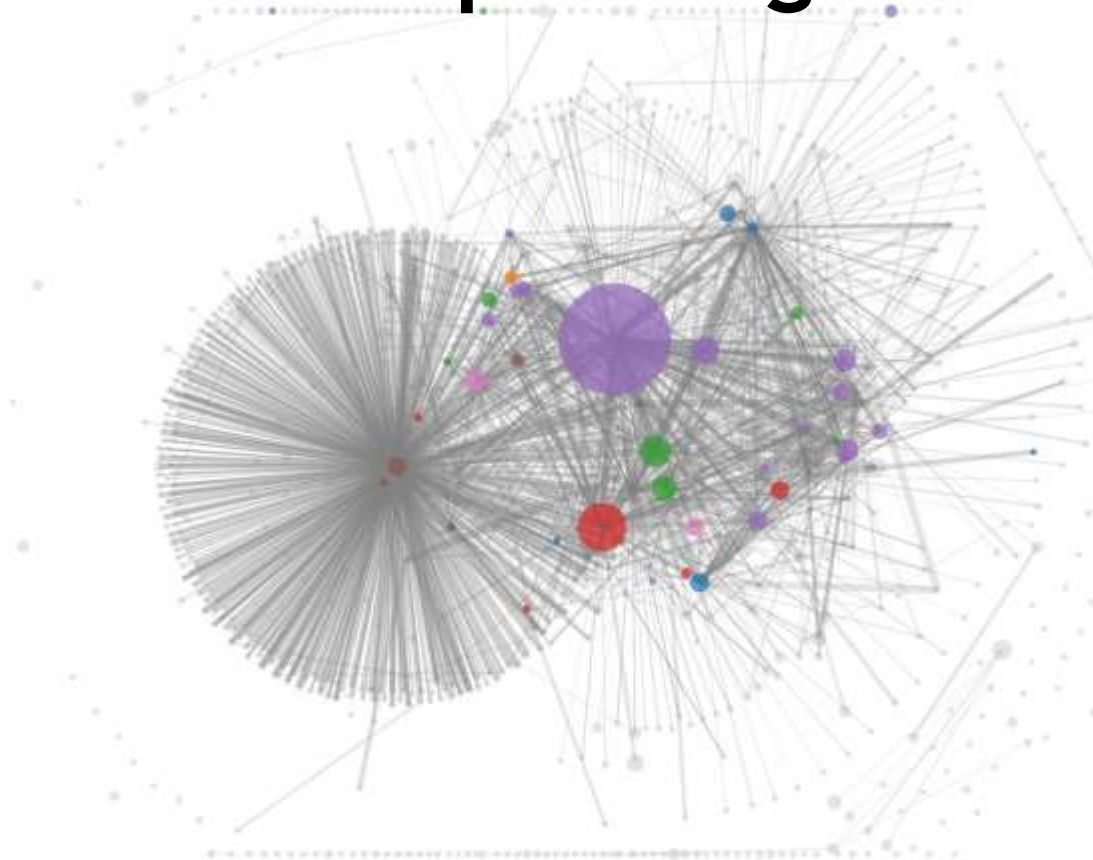
"Idioms of use"

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

To tag service providers: transact!

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names
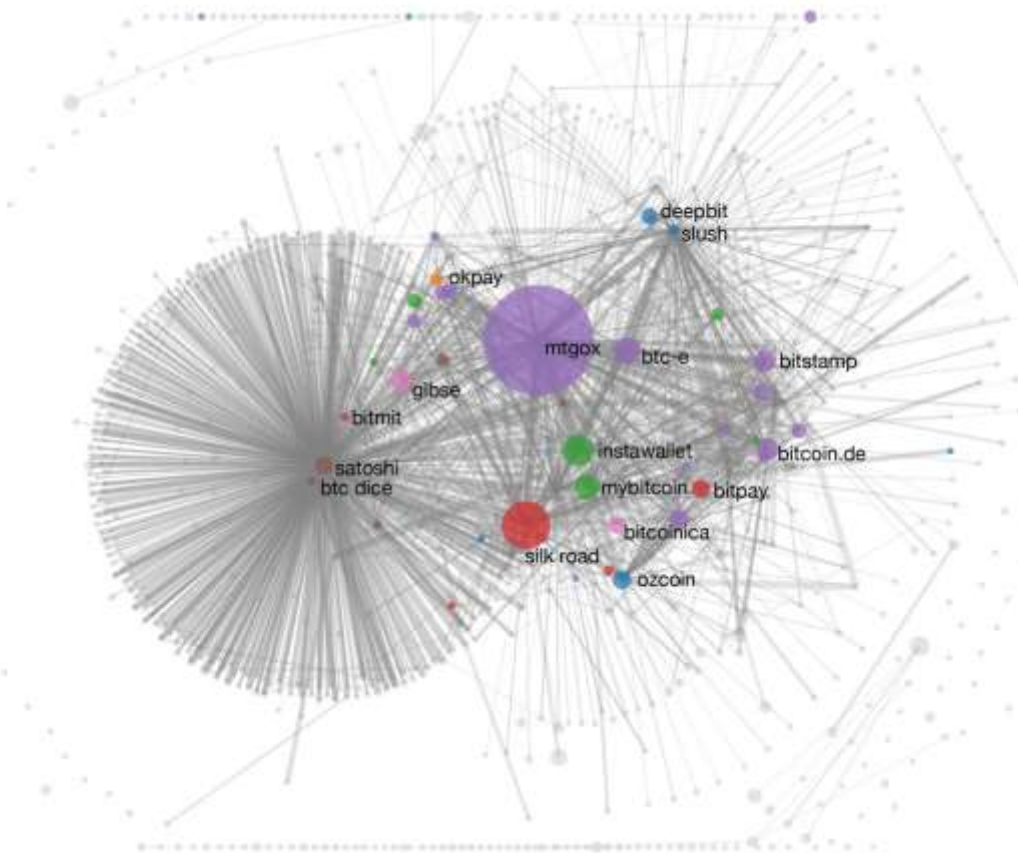
S. Meiklejohn et al.

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

Shared spending + idioms of use

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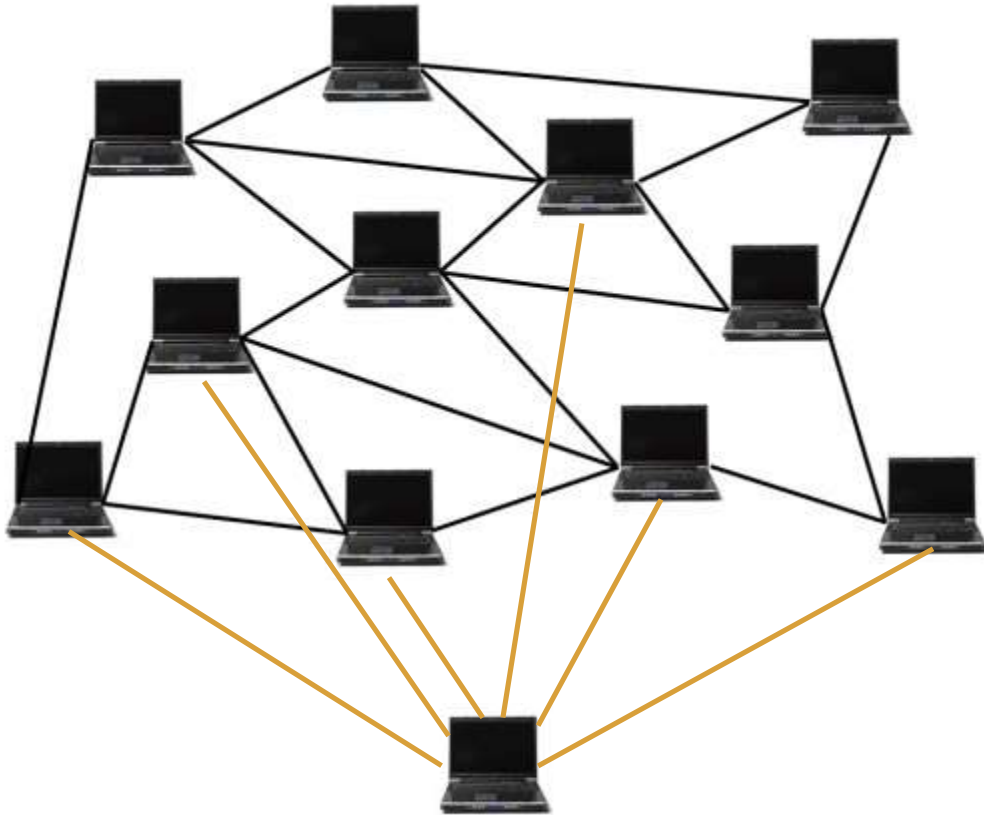*Among Men with No Names*

S. Meiklejohn et al.

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

Network-layer de-anonymization

"The first node to inform you of a transaction is probably the source of it"

Dan Kaminsky
Black Hat 2011 talk

Solution: use Tor

Caveat: Tor is intended for low-latency activities such as web browsing
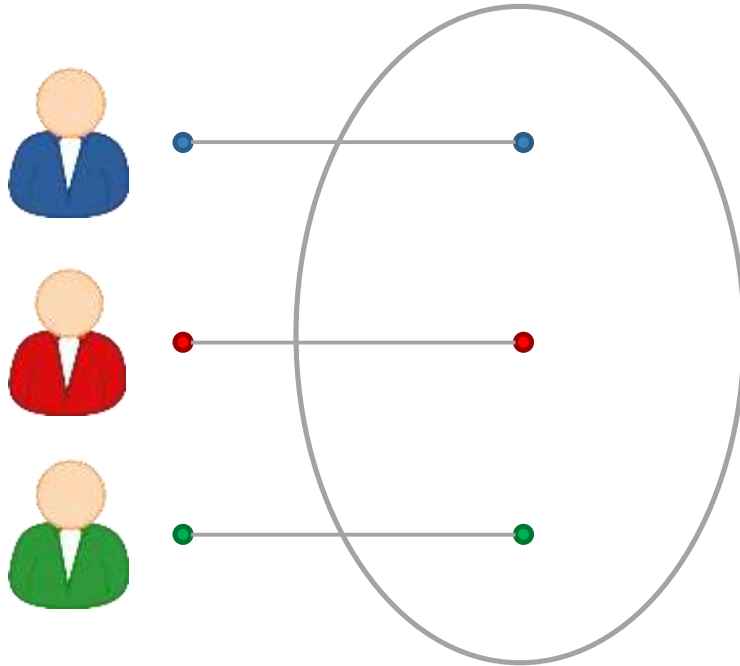
Mix nets might provide better anonymity

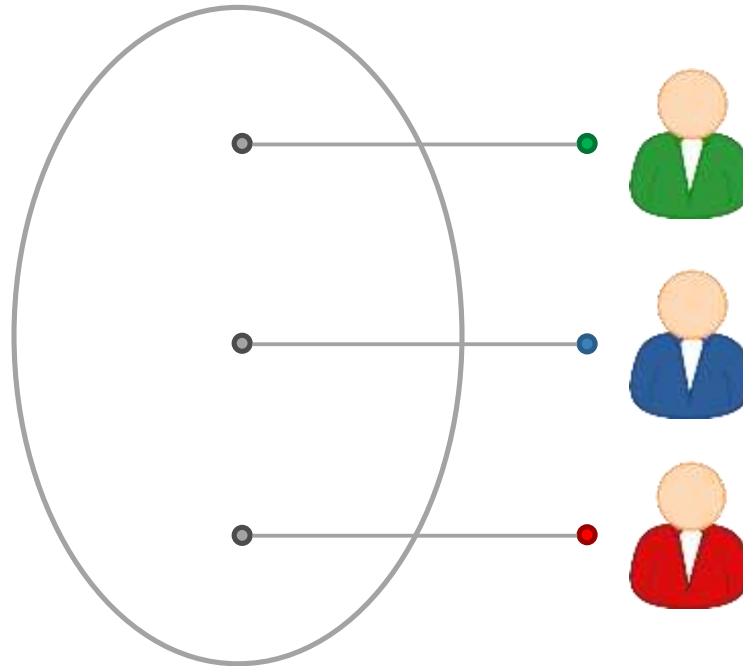BUT Tor is what's deployed and works

Lecture 6.3:

Mixing

To protect anonymity, use an intermediary

To protect anonymity, use an intermediary

Online wallets
do this

Do they provide
anonymity?!

Bits

Study Suggests Link Between Dread Pirate Roberts and Satoshi Nakamoto

By JOHN MARKOFF   NOVEMBER 23, 2013 6:13 PM   23 Comments

E-MAIL

FACEBOOK

TWITTER

SAVE

Two Israeli computer scientists say they may have uncovered a puzzling financial link between Ross William Ulbricht, the recently arrested operator of the Internet black market known as the Silk Road, and the secretive inventor of bitcoin, the anonymous online currency, used to make Silk Road purchases.

Bits

Researchers Retract Report That Linked Bitcoin Creator and Silk Road

By **JOHN MARKOFF**   NOVEMBER 27, 2013 12:45 PM   6 Comments

Two Israeli computer scientists who over the weekend published a paper describing a financial connection between the Bitcoin peer-to-peer transaction system and the operator of Silk Road, an Internet black market, have backed away from the claim after an independent security researcher took responsibility for the puzzling account that generated the transfer.

Dedicated mixing services

- Promise not to keep records

- Don't ask for your identity

Back to online wallets

Reputable, often regulated, businesses

- Typically require identity, keep records ➔
  no anonymity w.r.t. wallet service

- Users trust them with their bitcoins ➔
  keep them for longer ➔
  bigger anonymity set w.r.t. everyone else

Rest of this lecture:

assume a user for whom the trust requirements and anonymity properties of online wallets are unacceptable

Mixing: terminology

Mix vs. mixer

Another term: laundry
Won't use in this lecture
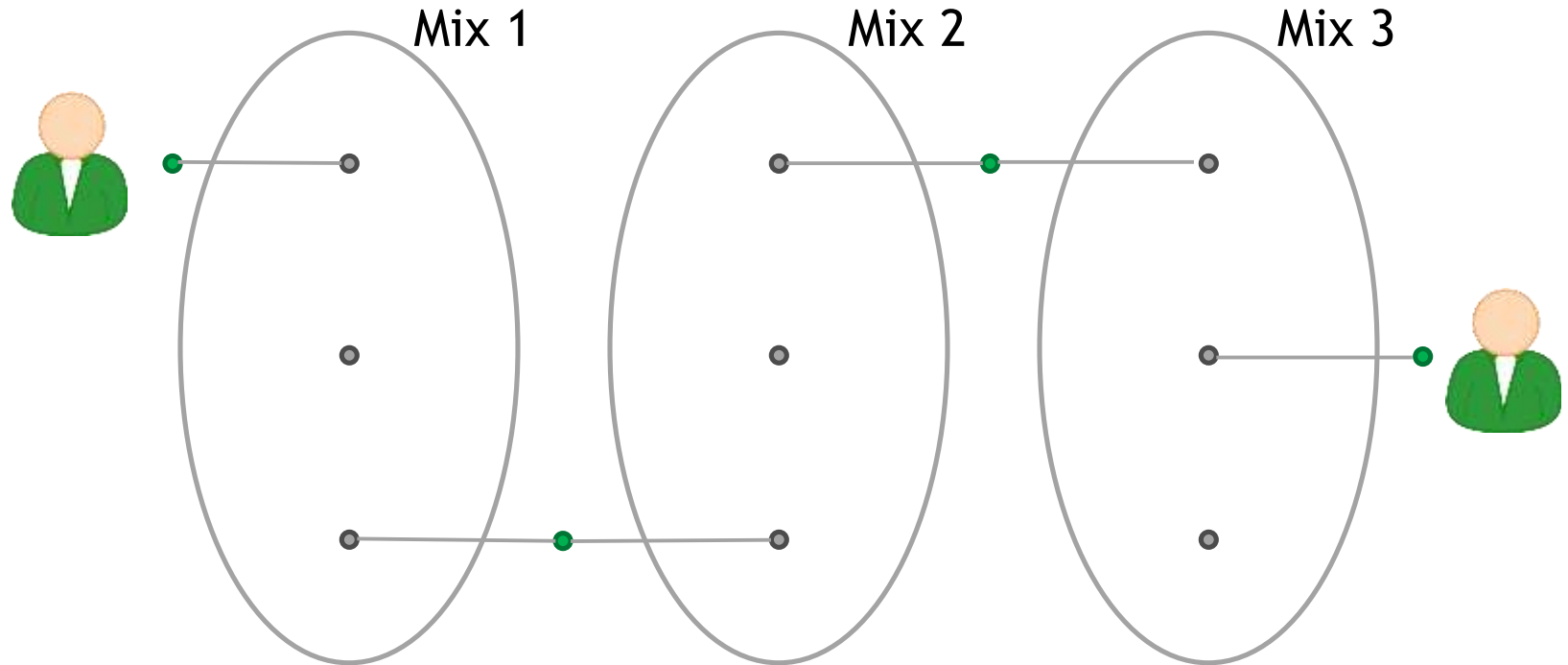
Principles for mixing services

1. Use a series of mixes

   Mixes should implement a standard API to make this easy

Mixcoin: Anonymity for Bitcoin with accountable mixes

J. Bonneau et al. Financial Cryptography 2014

Series of mixes

Principles for mixing services

2. Uniform transactions

In particular: all mix
transactions must have the
same value!

"Chunk size"

*Mixcoin: Anonymity for
Bitcoin with accountable
mixes*

J. Bonneau et al.
Financial Cryptography
2014

Principles for mixing services

3. Client side must be automated

   Desktop wallet software

Mixcoin: Anonymity for Bitcoin with accountable mixes

J. Bonneau et al. Financial Cryptography 2014

Principles for mixing services

4. Fees must be all-or-nothing

Probabilistic fees:
   0.1% mixing fee =
   mix will swallow chunk
   with 0.1% chance

Mixcoin: Anonymity for Bitcoin with accountable mixes

J. Bonneau et al.
Financial Cryptography 2014

Current mixes follow none of these principles

Remaining problem: trusting mixes

1. Stay in business, build up reputation

1. Users can test for themselves

1. Cryptographic "warranties"

Currently no reputable dedicated mix

Caution: Mixing services may themselves be operating with anonymity. As such, if the mixing output fails to be delivered or access to funds is denied there is no recourse. Use at your own discretion.
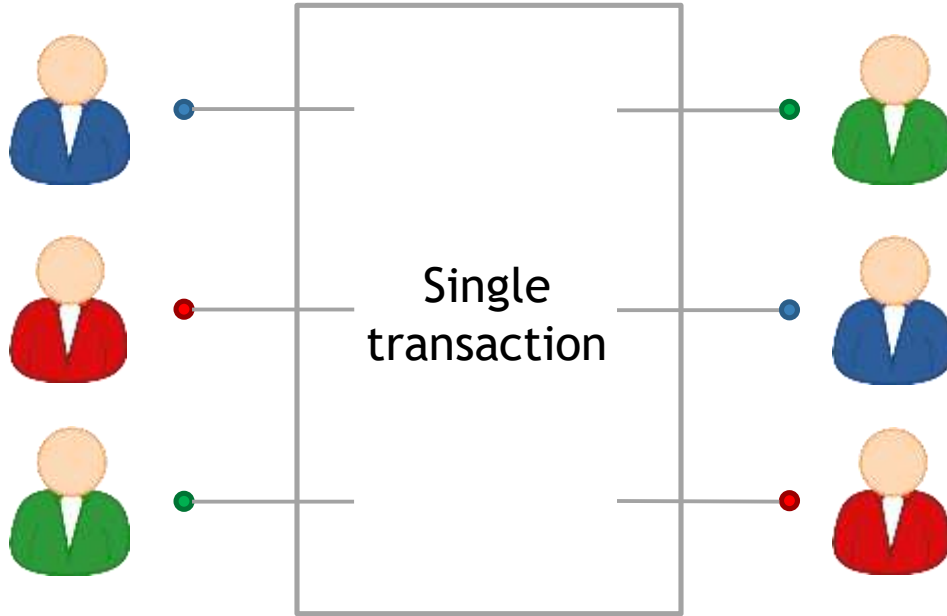
— Bitcoin Wiki

Lecture 6.4:

Decentralized mixing

Why decentralized mixing?

- No bootstrapping problem

- Theft impossible

- Possibly better anonymity

- More philosophically aligned with Bitcoin
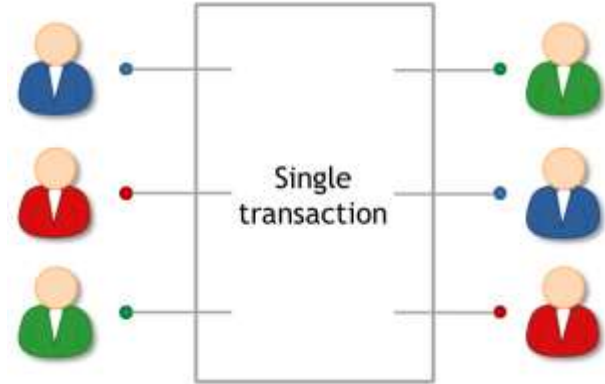
Coinjoin

Each signature is entirely separate

This is 1 mixing round

Mixing principles from before apply on top of basic protocol

Proposed by Greg Maxwell, Bitcoin core developer

Coinjoin algorithm

1. Find peers who want to mix
2. Exchange input/output addresses
3. Construct transaction
4. Send it around, collect signatures (Before signing, each peer checks if her output is present)
5. Broadcast the transaction

Single transaction

Coinjoin: remaining problems

- How to find peers
- Peers know your input-output mapping
(This is a worse problem than for centralized mixes)
- Denial of service
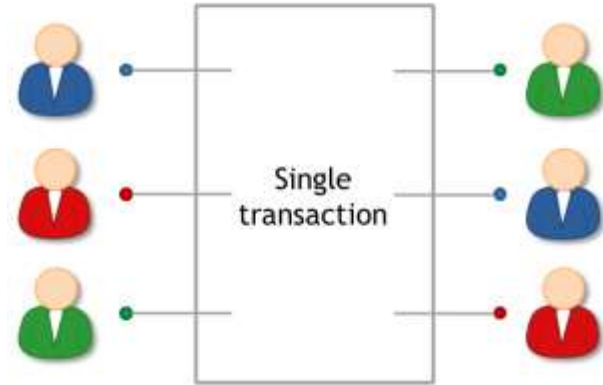
Finding peers

Use an untrusted server

Peer anonymity

Strawman solution:
1. exchange inputs
2. disconnect and reconnect over Tor
3. exchange outputs

Better solution:
special-purpose anonymous routing mechanism

Denial of service

Proposed solutions:
- Proof of work
- Proof of burn
- Server kicks out malicious participant
- Cryptographic "blame" protocol (*CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin* T. Ruffing et al., PETS 2014)

High-level flows could be identifying

Example:
Alice receives 43.12312 BTC / week as income
Always immediately transfers 5% to retirement account

Heuristic: merge avoidance

Instead of a single payment transaction

receiver provides multiple output addresses
sender avoids combining different inputs

(Proposed by Mike Hearn)

Lecture 6.5:

Zerocoin and Zerocash

Zerocoin: protocol-level mixing

Mixing capability baked into protocol

Advantage: cryptographic guarantee of mixing

Disadvantage: not currently compatible with Bitcoin

Zerocoin: Anonymous Distributed E-Cash from Bitcoin

I. Miers et al.
IEEE S&P 2013

Basecoin and Zerocoin

<u>Basecoin</u>: Bitcoin-like Altcoin

Zerocoin: Extension of Basecoin

Basecoins can be converted into zerocoins and back
Breaks link between original and new basecoin

Zerocoins

A Zerocoin is a cryptographic proof that you owned a Basecoin and made it unspendable

Miners can verify these proofs

Gives you the right to redeem a new Basecoin (Somewhat like poker chips)

Two challenges

How to construct these proofs?

How to make sure each proof can only be "spent" once?

Zero-knowledge proofs

A way to prove a statement without revealing any other information

Crypto magic

Example:
- "I know an input that hashes to `da39a3ee5e`"
- "I know an input that hashes to some hash in the following set: … "

Minting zerocoins

Zerocoins come in standard denominations
(Let's assume 1 basecoin)

Anyone can make one!

They have value once put on the block chain
That costs 1 basecoin

Minting a zerocoin: "commitment"

Generate serial number S (eventually made public)

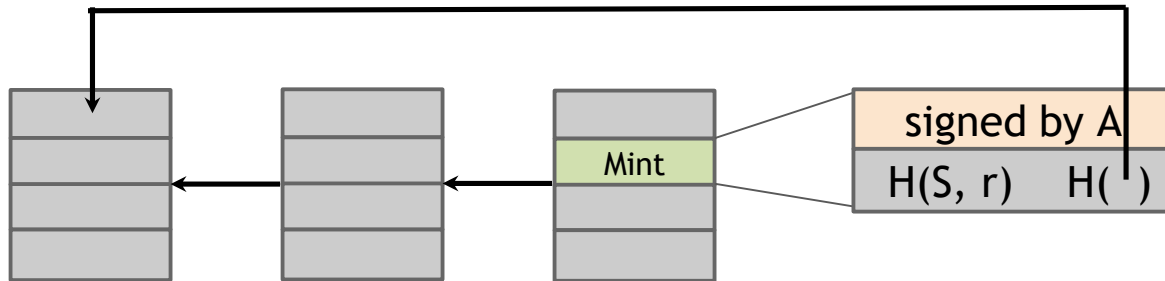and random secret r (never public, ensures unlinkability)

Compute $H(S, r)$ Simplification

Serial number:
317038628684424

Minting a zerocoin

To put *H(S, r)* on block chain

Create Mint Tx with 1 basecoin as input

To spend a zerocoin *S*:

- Reveal *S*
  (miners will verify *S* hasn't been spent before)

- Create zero-knowledge proof that:
  "I know a number *r* such that *H(S, r)* is one of the zerocoins in the block chain"

- Pick arbitrary zerocoin in block chain & use as input to your new transaction

Zerocoin is anonymous

Since *r* is secret, no one can figure out *which* zerocoin corresponds to serial number *S*

H(S, r)

h_1 $\qquad\qquad$ h_2 $\qquad$ ... $\qquad$ h_N

Zerocoin is "efficient"

The proof is a giant disjunction over all zerocoins

Yet the proof is relatively small!

I know r such that

$$H(S, r) = h_1$$

OR

$$H(S, r) = h_2$$

OR

...

OR

$$H(S, r) = h_N$$

Zerocash: Zerocoin without Basecoin

Two differences
- Different crypto for proofs (More efficient)
- Proposal to run system without Basecoin

Zerocash: Decentralized Anonymous Payments from Bitcoin

E. Ben-Sasson et al. Usenix Security 2014

Zerocash: <u>untraceable</u> e-cash

All transactions are zerocoins

Splitting and merging supported
Put transaction value <u>inside the envelope</u>

Ledger merely records existence of transactions

Zerocash: the catch

Random, secret inputs are required to generate public parameters

These secret inputs must then be securely destroyed

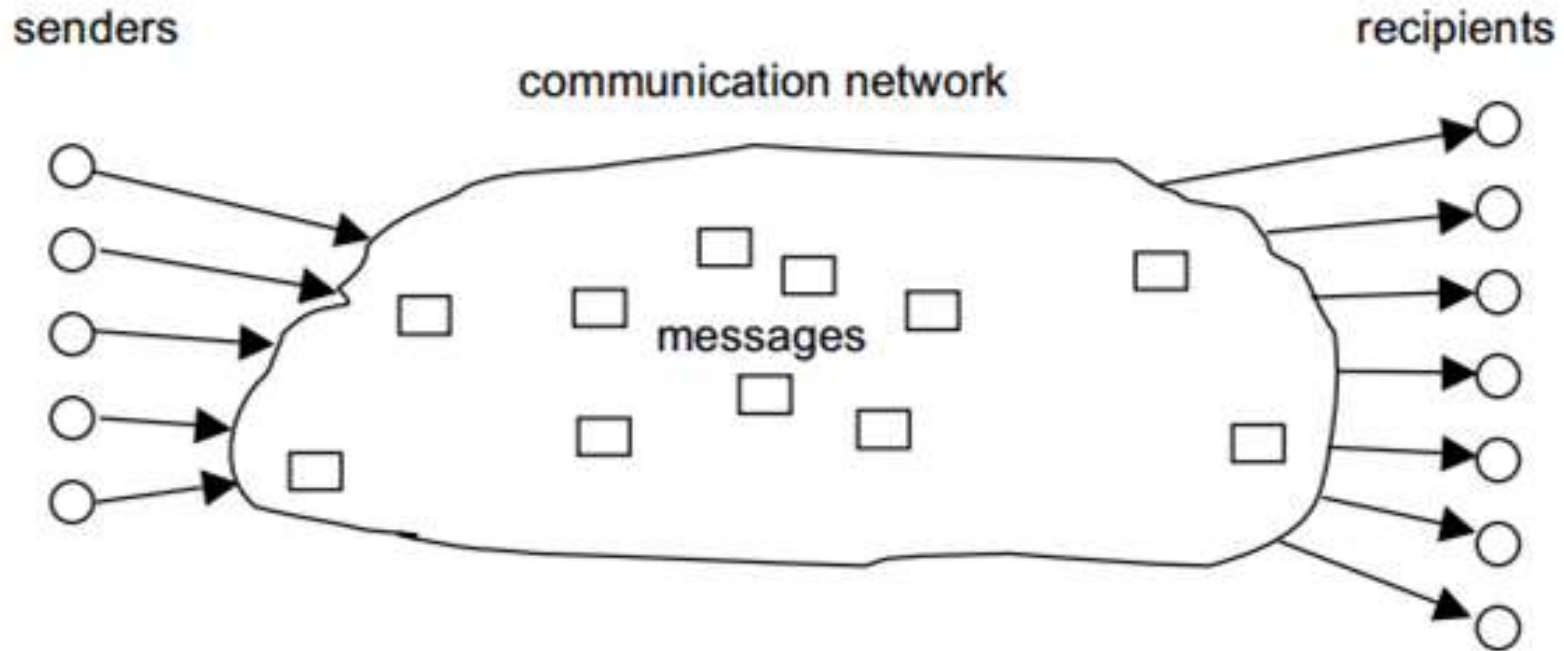No one can know them (anyone who does can break the system)

5 levels of anonymity

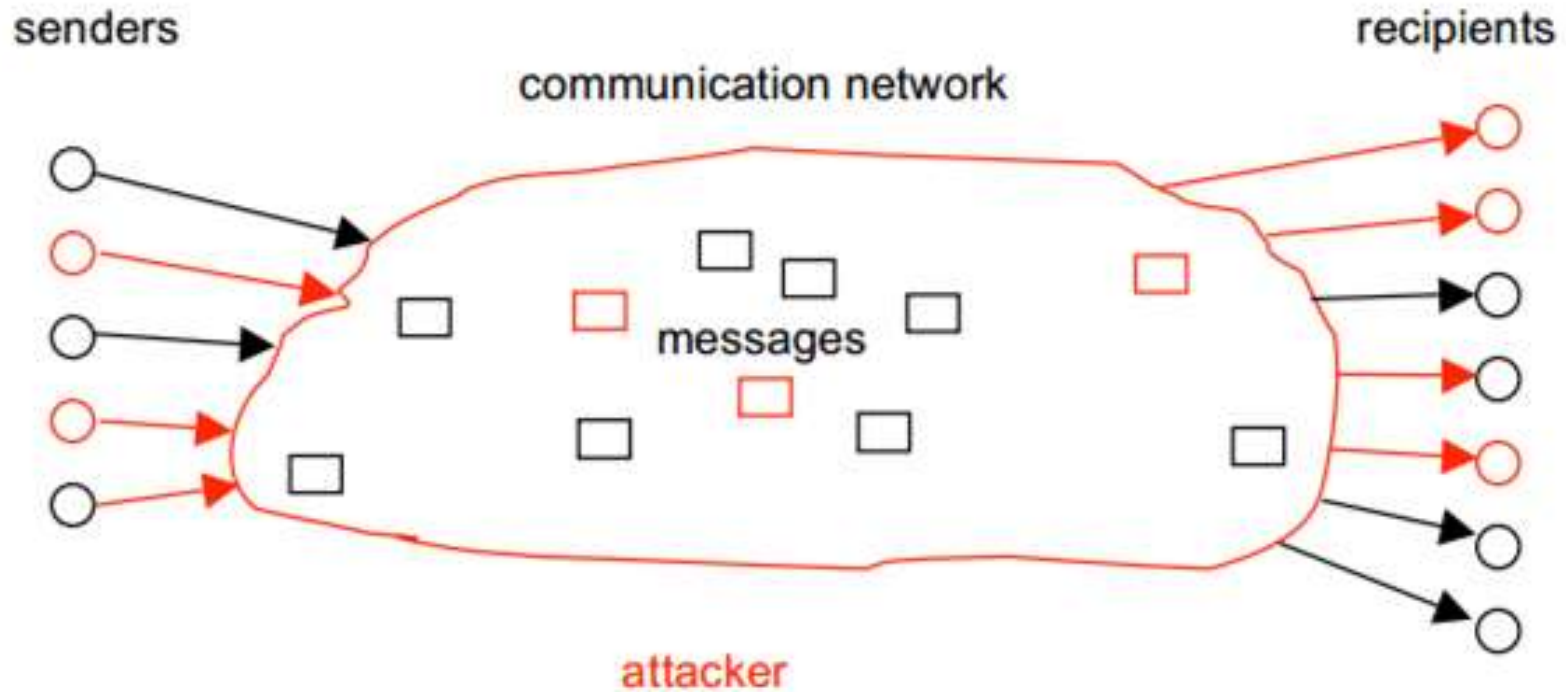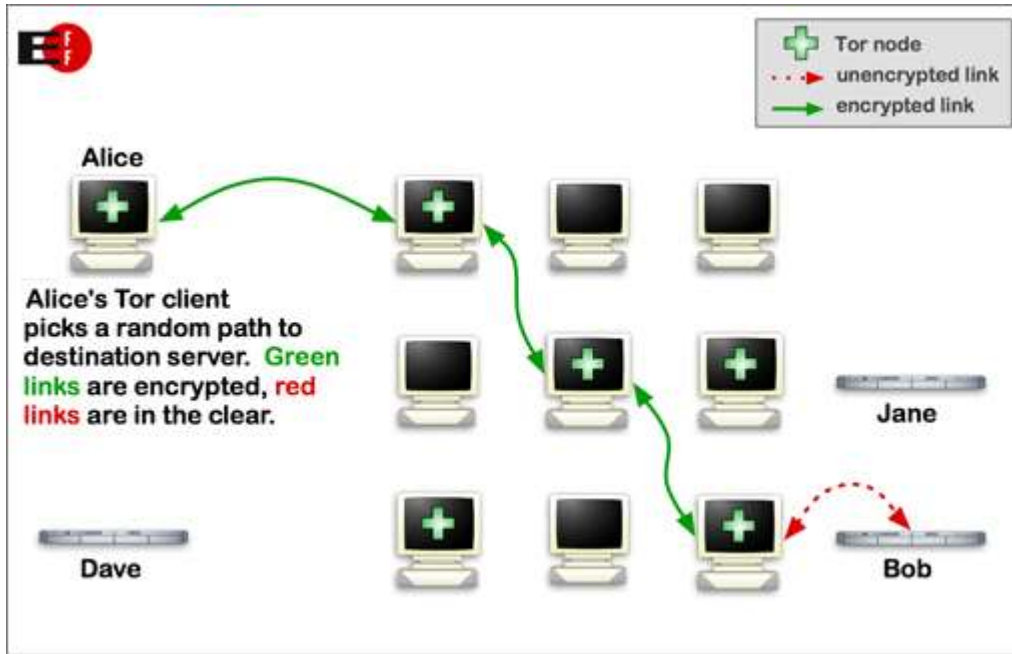| System	Type	Anonymity attacks	Deployability
Bitcoin	Pseudonymous	Tx graph analysis	Default
Single mix	Mix	Tx graph analysis, bad mix	Usable today
Mix chain	Mix	Side channels, bad mixes/peers	Bitcoin-compatible
Zerocoin	Cryptographic mix	Side channels (possibly)	Altcoin
Zerocash	Untraceable	None	Altcoin, tricky setup

Lecture 6.6:

Tor and the Silk Road

Anonymous communication

Threat model

How Tor works

Alice

Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

Tor node
unencrypted link
encrypted link

Jane

Dave

Bob
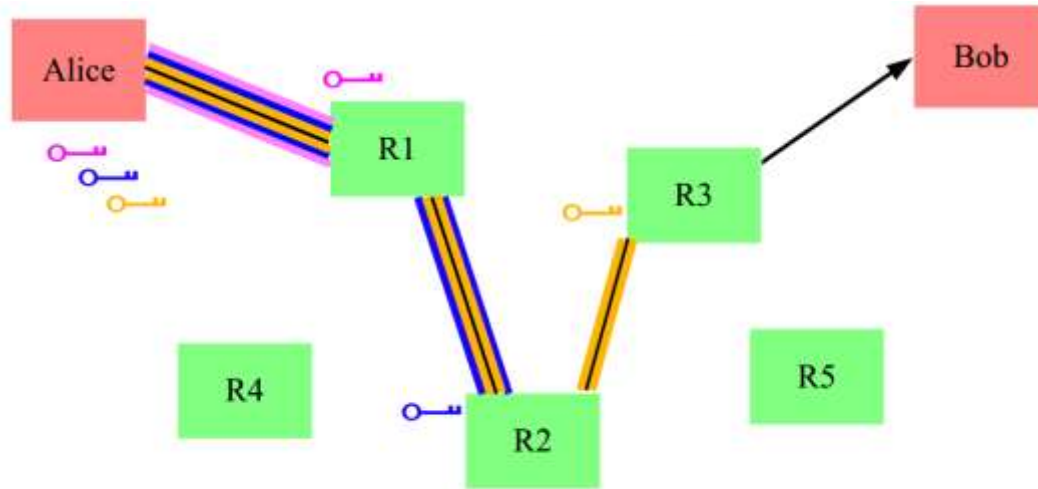
Safe(ish) if at least one router honest

Key challenge: hiding routing information

Solution: layered encryption

Side effect: contents encrypted from Alice to exit node

BUT: Unencrypted from exit node to Bob

Hidden services

What if the <u>server</u> wants to hide its address?

Simplified:
1. Connect to "rendezvous point" through Tor
2. Publish name → rendezvous point mapping
3. Client connects to rendezvous point

Onion address looks like
http://3g2upl4pq6kufc4m.onion/

Silk Road

- Communication: Tor hidden service

- Payment: Bitcoin

- Security?

- Anonymous shipping?