

Bitcoin and Anonymity

- Anonymity Basics
 - How to de-anonymize Bitcoin
 - Mixing
 - Decentralized Mixing
 - Zerocoin and Zerocash
 - Tor and the Silk Road
-

Bitcoin and Anonymity

- Anonymity Basics
 - How to de-anonymize Bitcoin
 - Mixing
 - Decentralized Mixing
 - Zerocoin and Zerocash
 - Tor and the Silk Road
-

Some say Bitcoin provides Anonymity

CAPABLE MEN
PERSONAL DEVELOPMENT STRATEGY

HOME CATEGORIES START HERE DONATE WRITE FOR US ALL

DONATE

Capable Men remains committed to producing quality content each and every month which requires many hours of research and writing. We continuously seek solutions to help us fund this platform while keeping this experience free of intrusive advertisements or the awful click-bait junk that has become commonplace online.

If you find yourself benefiting from the content that we provide here at Capable Men, please consider a small donation as a token of your appreciation. This truly helps us keep the lights on while we look to develop and move forward in a sustainable and virtuous way.

DONATE NOW

Rather pay with digital currency? We also accept Bitcoin - our address:

1Gjxtb8PFjGubWA22NkmgdYpBnQgBj58v

Bitcoin is a secure and anonymous digital currency.

Others say it doesn't

WIRED BITCOIN

Bitcoin

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


By KADHIM SHUBBER
11 Jun 2013

Let's get the Terminology straight

- Literally: **anonymous** = "without a name"
 - Recall: Bitcoin **addresses** are **public key hashes** rather than **real identities**
 - Computer scientists call this **pseudonymity**
-

Anonymity in Computer Science

$\text{anonymity} = \text{pseudonymity} + \text{unlinkability}$



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

Pseudonymity vs. Anonymity: Examples

Reddit: pick a long-term pseudonym

vs.

4Chan: make posts with no attribution at all

Why care about Unlinkability?

1. Many Bitcoin services require real identity.
 2. Linked profiles can be de-anonymized 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

Observation: **Complete unlinkability** (among all addresses/ transactions) is **hard**!

Vanilla Measure for "partial" Anonymity:

Anonymity Set: The crowd that one attempts to "blend" into.

Q: How to **calculate** anonymity set?

- Define **adversary model**.
 - Reason carefully about **what** adversary **knows**, does **not know**, and **cannot know**.
-

Why Worry about Anonymity?

Observation: Block chain based currencies are **totally, publicly, and permanently traceable**

Without **anonymity**, privacy in such currencies is **much worse** than **traditional banking!**

So, what about Money Laundering?!

Money Laundering is a **legitimate worry**.

So, why is not more done about it?!

"Cashing-Out" Problem: bottleneck is with moving large flows **into and out of** Bitcoin.

Not unique to Bitcoin!

Improving Anonymity does **not solve** cashing-out problem.

Can we keep only the good Uses?

Observation:

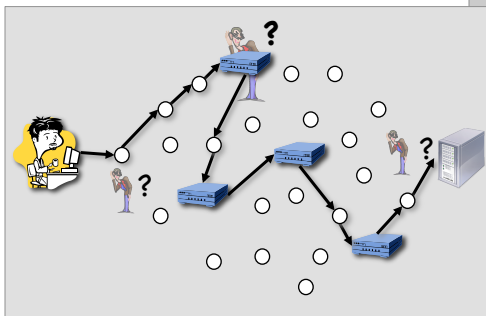
Uses that are very **different morally** are pretty much **the same technologically**.

This is a **common problem** in computer **security** and **privacy**.

Similar Dilemma:

Anonymous communication network

Sender and receiver of message are **unlinkable**



Used by:

- Normal people
- Journalists & activists
- Law enforcement
- Malware
- Child pornographers

Coming to you **courtesy of the U.S. Government:**

- U.S. State Dept.
- ONR
- others . . .

Anonymous e-Cash: History

Proposed by David Chaum in 1982

Crypto
magic!

Based on **Blind Signatures**:

Two-party protocol to create digital signature
without signer knowing what she signs.

Under the Hood: Blind Signatures with RSA

Recall:

- public key (e, N)
- private key (d, N)
- N is public modulus

- plaintext m
- cyphertext c

Encryption:

$$c = m^e \pmod{N}$$

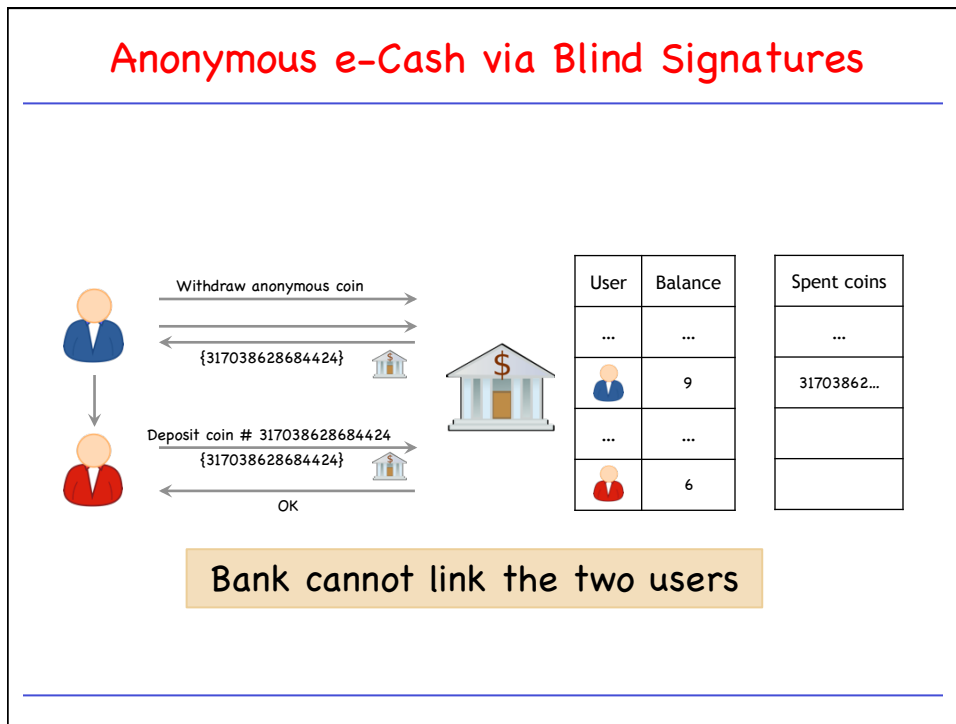
Decryption/signing

$$m = c^d \pmod{N}$$

Blind RSA Signature:

- pick random blinding factor r
(detail: $\gcd(r, N) = 1$)
- compute
 $m' = mr^e \pmod{N}$
- signing authority signs m'
 $s' = (m')^d \pmod{N}$
- extract signature:
 $s = s' * r^{-1} \pmod{N}$
- why?!

$$s = s' * r^{-1} = (m')^d r^{-1} = m^d r^{ed} r^{-1} = m^d r r^{-1} = m^d \pmod{N}$$



Anonymity & Decentralization

Q: How to "de-scroogify" e-Cash?

Interactive Protocols with bank are **hard to decentralize**.


Decentralization often achieved via **public traceability** to enforce security

- e.g., publicly **post transactions** to avoid **double-spending**.

Bitcoin and Anonymity

- Anonymity Basics
- **How to de-anonymize Bitcoin**
- Mixing
- Decentralized Mixing
- Zerocoin and Zerocash
- Tor and the Silk Road

Example: Wikileaks


WikiLeaks

Shop
Donate
Submit

Leaks
News
About
Partners


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:


1HB5XMLmzFVj8ALj6mfBsbfRoD4miY36v
↻

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 (<https://bitcoin.org>) or read more on [Wikipedia](#).


For a more private transaction, you can click on the refresh button above to generate a new address



Example: Wikileaks





WikiLeaks

Search  Shop Donate Submit

Leaks News About Partners


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:

1Q3q1HTVuFGR5nWhbD4q6APonCLDg39E1E  

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 (<https://bitcoin.org>) or read more on [Wikipedia](#).

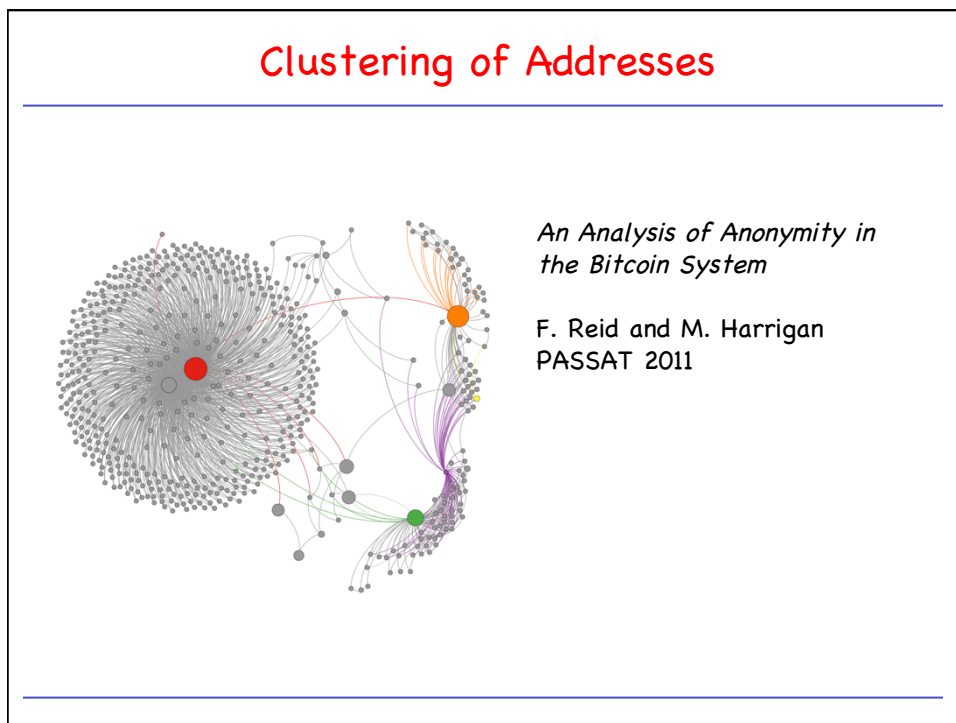
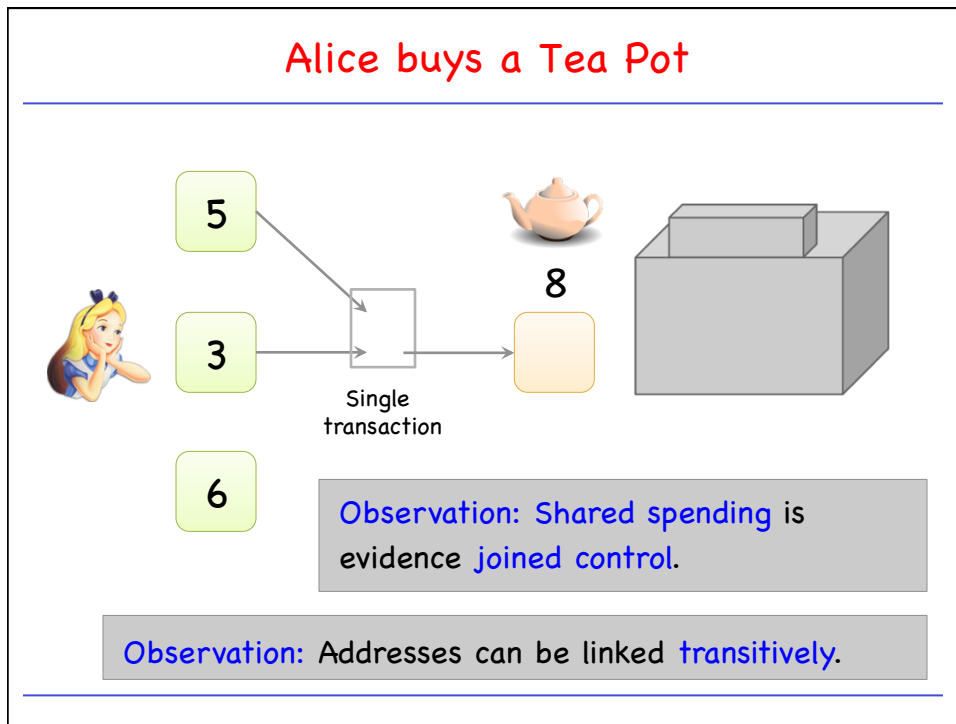
For a more private transaction, you can click on the refresh button above to generate a new address



Recall: It is easy to generate new Addresses!

So, **always** receive at a **fresh** address.
It's easy!

Q: Are the transactions now **unlinkable**?



Change Addresses

The diagram shows a transaction process. On the left, a woman icon is next to three green boxes containing the numbers 5, 3, and 6, representing inputs. Arrows from these boxes point to a central white square representing a transaction. From this square, two arrows point to the right. The top arrow points to an orange box containing 8.5, with a teapot icon above it. The bottom arrow points to a green box containing .5. To the right of the 8.5 box is a grey box icon. Below the diagram, there is a grey box with the text: "Observation: One of the outputs (change) jointly controlled with the inputs." To the right of this box is another grey box with the text: "Which address is change?"

Observation: One of the outputs (change) jointly controlled with the inputs.

Which address is change?

"Idioms of Use"

Idioms of Use: Idiosyncratic features of wallet software


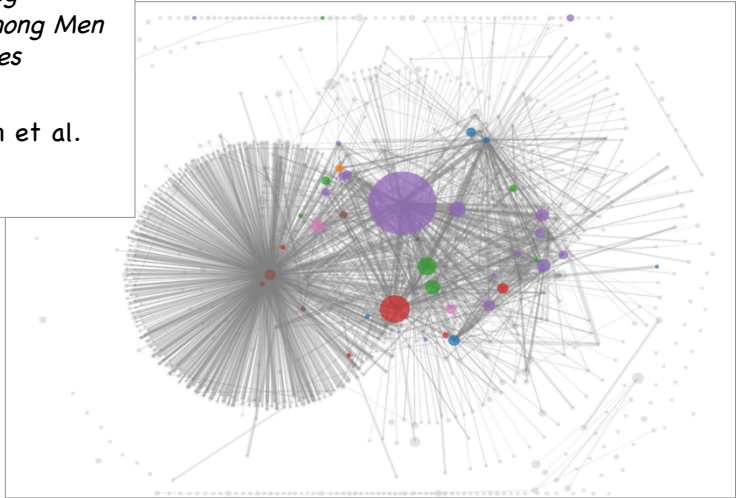
Examples:

- each address is **used only once** as change
- bug: change is **first output** of transaction
- etc.

Shared Spending + Idioms of Use

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


S. Meiklejohn et al.
IMC 2013


Tagging Service Providers: transact!

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

S. Meiklejohn et al.
IMC 2013



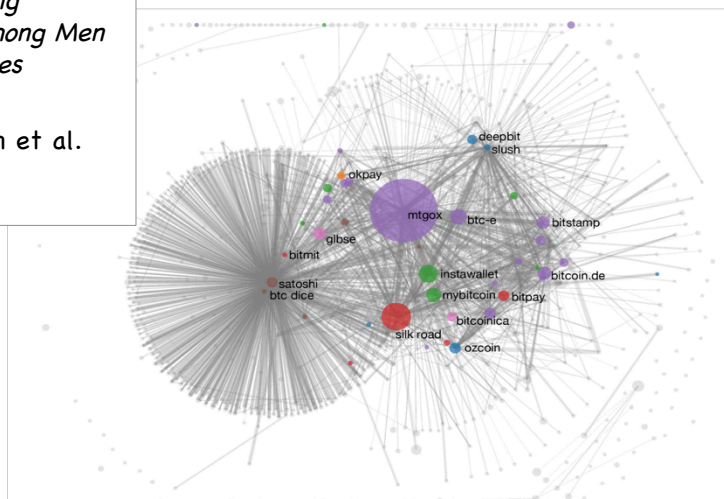
- 344 transactions
- Mining pools
- Wallet services
- Exchanges
- Vendors
- Gambling sites



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

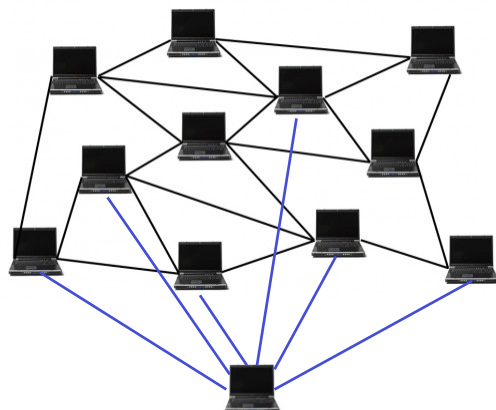
High **centralization** in service providers

- Service providers are **identifiable**
- Most **flows pass through one of these** – in a traceable way

Addresses often **posted** in forums

- **Address – identity link** becomes traceable

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.

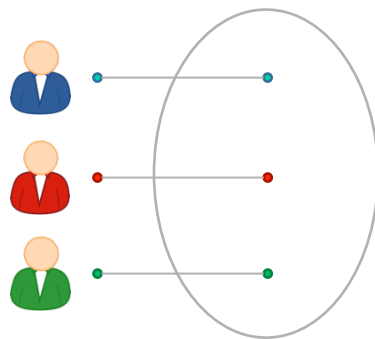
Mix nets might provide **better anonymity**

BUT Tor is what's deployed and works

Bitcoin and Anonymity

- Anonymity Basics
 - How to de-anonymize Bitcoin
 - **Mixing**
 - Decentralized Mixing
 - Zerocoin and Zerocash
 - Tor and the Silk Road
-

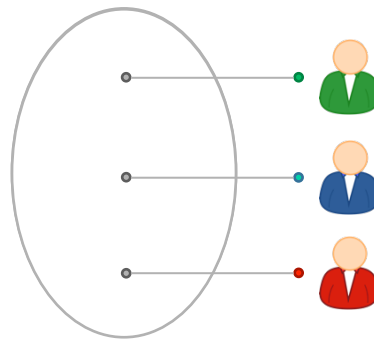
To protect Anonymity, use an Intermediary



To protect Anonymity, use an Intermediary

Online wallets
do this

Do they provide
anonymity?!



Dedicated Mixing Services

- Promise not to keep records
 - Don't ask for your identity
-

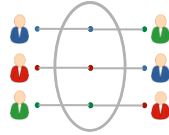
Back to Online Wallets

- 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
-

For the Rest of this Topic . . .

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

Principles for Mixing Services



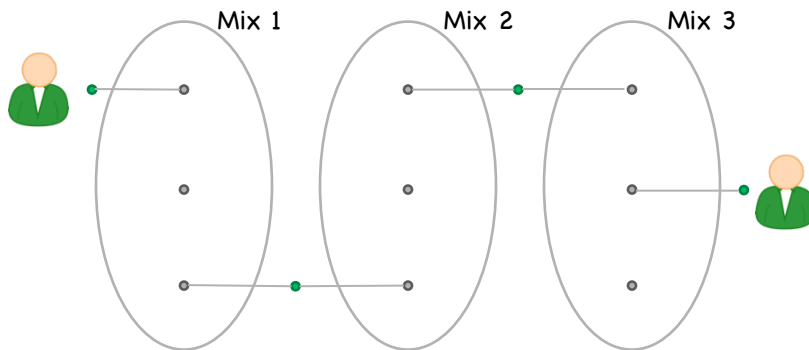
1. Use a **series** of mixes

Mixes should implement a standard API to make this easy

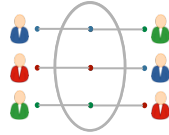
Mixcoin: Anonymity for Bitcoin with accountable mixes

J. Bonneau et al.
Financial Cryptography
2014

Series of Mixes



Principles for Mixing Services



2. Uniform transactions

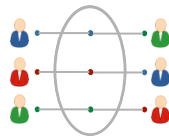
In particular: all mix transactions must have the same value!

“Chunk size”

Mixcoin: Anonymity for Bitcoin with accountable mixes

J. Bonneau et al.
Financial Cryptography
2014

Principles for Mixing Services



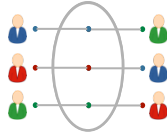
3. Client side must be automated

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

Currently no 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

Bitcoin and Anonymity

- Anonymity Basics
 - How to de-anonymize Bitcoin
 - Mixing
 - **Decentralized Mixing**
 - Zerocoin and Zerocash
 - Tor and the Silk Road
-

Decentralized Mixing

- **Eliminate** mixing services
- Replace them with **peer-to-peer** mixing protocol

Advantages

- No **bootstrapping** problem
 - **Theft** impossible
 - Possibly better **anonymity**
 - More **philosophically aligned** with Bitcoin
-

CoinJoin

Users jointly create a single transaction that combines all inputs.

Single transaction

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

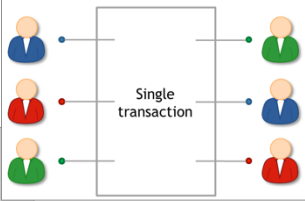
Algorithm:

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

CoinJoin: Problems

Problems:

1. How to **find peers**
2. Peers know your **input-output mapping**
(This is a worse problem than for centralized mixes)
3. **Denial of Service**



CoinJoin: Problems

Problems:

1. How to **find peers**
2. Peers know your input-output mapping
(This is a worse problem than for centralized mixes)
3. **Denial of Service**

Solution

- Use **untrusted server**
- **Q:** Why does this work?

CoinJoin: Problems

Problems:

1. How to find peers
2. Peers know your **input-output mapping**
(This is a worse problem than for centralized mixes)
3. Denial of Service

Strawman Solution:

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

CoinJoin: Problems

Problems:

1. How to find peers
2. Peers know your input-output mapping
(This is a worse problem than for centralized mixes)
3. 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:

Avoid single-payment transactions

Instead:

- Receiver provides multiple output addresses
- Sender avoids combining different inputs

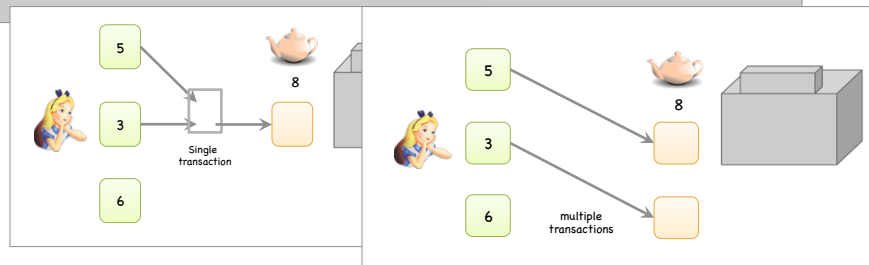
Merge Avoidance

Heuristic: Merge Avoidance:

Avoid single-payment transactions

Instead:

- Receiver provides multiple output addresses
- Sender avoids combining different inputs



Bitcoin and Anonymity

- Anonymity Basics
 - How to de-anonymize Bitcoin
 - Mixing
 - Decentralized Mixing
 - Zerocoin and Zerocash
 - Tor and the Silk Road
-

Zerocoin: Protocol-level Mixing

Mixing capability **baked into protocol**

Zerocoin: Anonymous Distributed E-Cash from Bitcoin

Advantage: **cryptographic guarantee** of mixing

I. Miers et al.
IEEE S&P 2013

Disadvantage: **not currently compatible with Bitcoin**

Basecoin and Zerocoin

Basecoin: Bitcoin-like Altcoin

Zerocoin: Extension to Bascoin

Basecoins can be **converted** into zerocoins and back.

This **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

1. How to **construct** these proofs?
2. 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

Examples:

- “**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 **acquire 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 $H(S, r)$

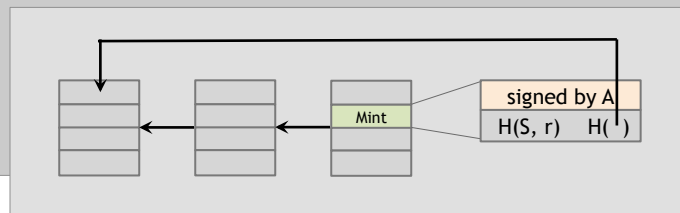


Note: This is a simplification

Minting a Zerocoin

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

Create **Mint** transaction 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



h_2

...



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

1. Different crypto for proofs (More efficient)
2. Proposal to run system without Basecoin

*Zerocash:
Decentralized
Anonymous Payments
from Bitcoin*

E. Ben-Sasson et al.
Usenix Security 2014

Zerocash: untraceable e-cash

All transactions are zerocoins

Splitting and merging supported

Put transaction value inside the envelope

Ledger merely records existence of transactions

Sender and recipients know amounts, but nobody else

Prove to miners in zero knowledge that

input amount \geq output amount

Avoids side-channel problems associated with mixing

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)

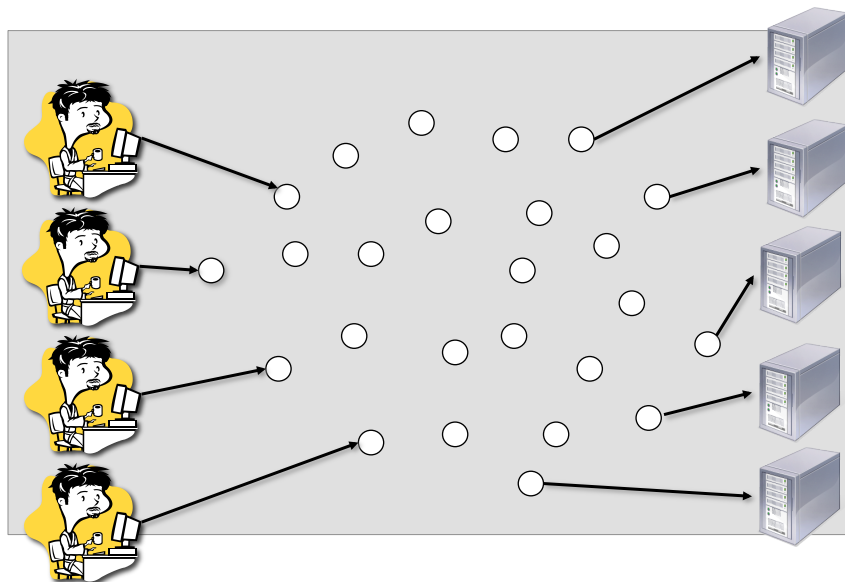
The 5 Levels of Anonymity

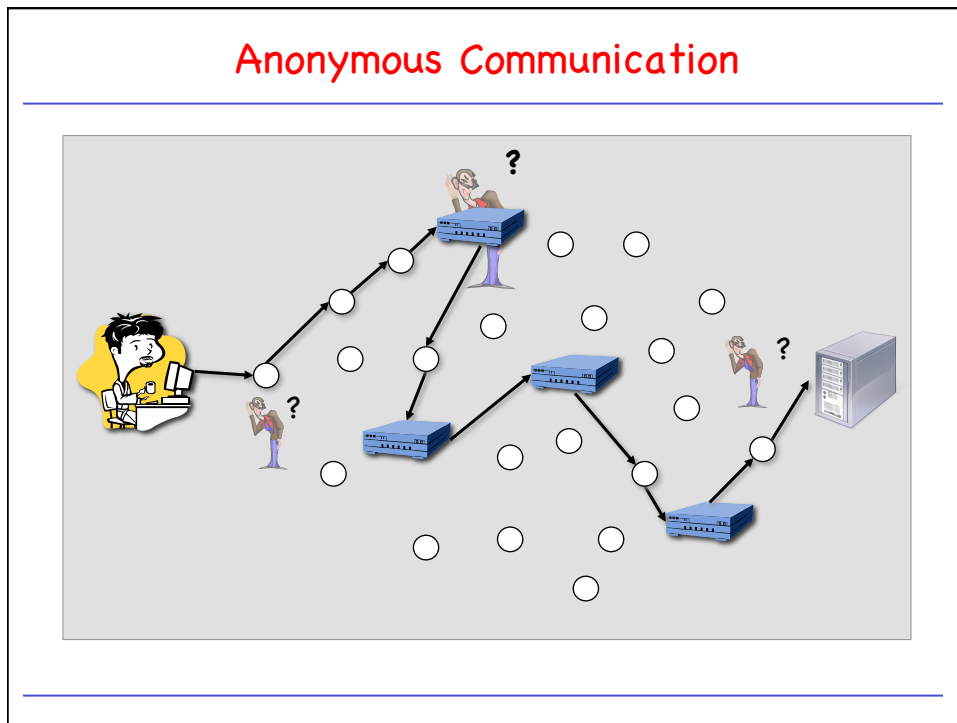
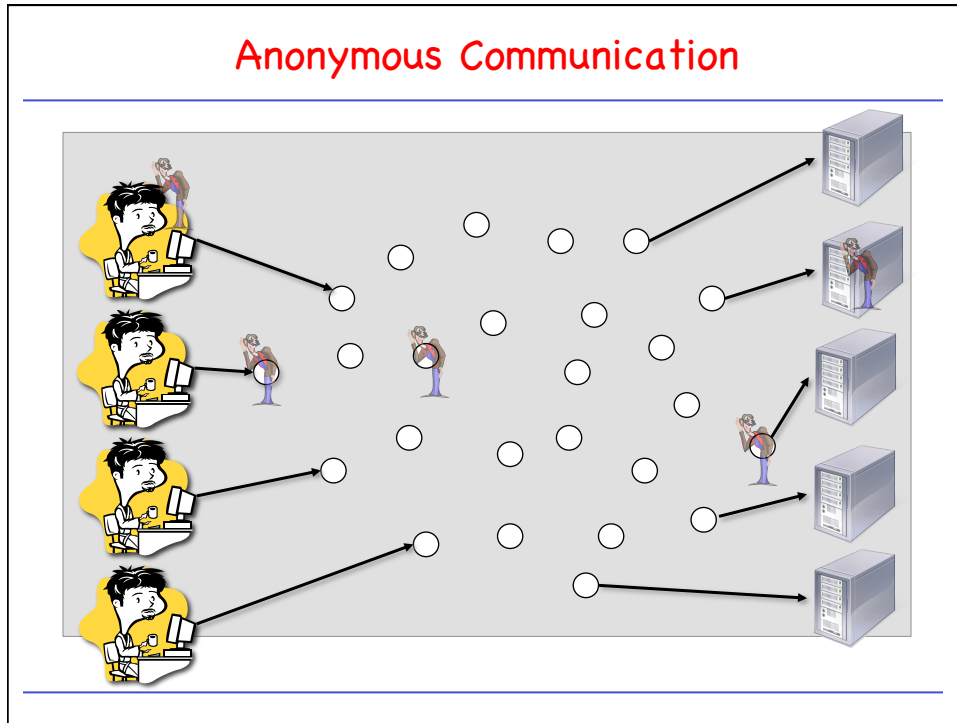
System	Type	Anonymity attacks	Deployability
Bitcoin	Pseudonymous	Tx graph analysis	Default
Single mix	Mix	Tx graph analysis, bad mix	Usable today
Mix chain	Mix	Side channels, bad mixes/peers	Bitcoin-compatible
Zerocoin	Cryptographic mix	Side channels (possibly)	Altcoin
Zerocash	Untraceable	None	Altcoin,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

Bitcoin and Anonymity

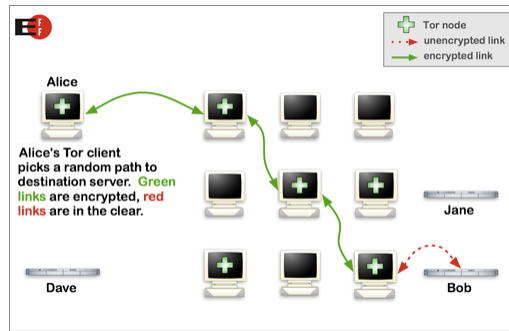
- Anonymity Basics
- How to de-anonymize Bitcoin
- Mixing
- Decentralized Mixing
- Zerocoin and Zerocash
- Tor and the Silk Road

Anonymous Communication





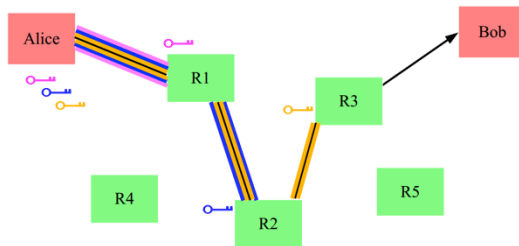
How Tor works



Safe(ish) if at least one router honest

Key challenge: hiding routing information

The "onion" in "onion routing"



Side effect: contents **encrypted** from Alice to exit node

BUT: **Unencrypted** from exit node to Bob

Hidden Services

Q: What if the **server** wants to hide its address?

Simplified:

1. Connect to "rendesvouz point" through Tor.
2. Publish name -> rendesvouz point **mapping**
3. Client connects to rendesvouz point.

Onion address looks like

`http://3g2up14pq6kufc4m.onion/`

Silk Road

- "the eBay for illegal drugs"
 - Communication: Tor hidden service
 - Payment: Bitcoin
 - Security?
 - Anonymous shipping?
-