BIT COIN - 3

Reference

Bitcoin and Cryptocurrency Technologies

By Arvind Narayanan, Joseph Bonneau, Edward Felten,

Andrew Miller, Steven Goldfeder

Main reference: *Bitcoin and Cryptocurrency Technologies*,

By Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder

Slides are mainly taken (or adapted) from slides of the authors of the text

Anonymity basics

What do we mean by anonymity?

- Literally: ***anonymous*** = `*without a name*'
  - Two interpretations:
    1 – without using your real name
    2 – without using any name at all

- Bitcoins: Addresses are public key hashes rather than real identities
  - By first interpretation, Bitcoin is anonymous
  - By second interpretation, it is not anonymous! Bitcoin addresses → pseudo-identity
  - Computer scientists call this ***pseudonymity***

Bitcoin provides anonymity?

" *Bitcoin is a secure and anonymous digital currency* "

— WikiLeaks donations page

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

— Wired UK

Risk that transactions can be linked back to the people that made them

What do we mean by anonymity?

Literally: ***anonymous*** = `*without a name'*

- Two interpretations:
  1 – without using your real name
  2 – without using any name at all

Bitcoins: Addresses are public key hashes rather than real identities

- By first interpretation, Bitcoin is anonymous
- By second interpretation, it is not anonymous!
  Bitcoin addresses → pseudo-identity
- Computer scientists call this ***pseudonymity***

Anonymity vs. Privacy

Anonymity is insufficient for privacy

Anonymity is necessary for privacy

Anonymity is unachievable in practice

Re-identification attack → anonymity breach → privacy breach

Just ask Justice Scalia (US Supreme Court)
"It is silly to think that every single datum about my life is private"

What do we mean by anonymity?

Literally: anonymous = without a name

Bitcoin addresses are public key hashes rather than real identities
Bitcoin addresses → pseudo-identity

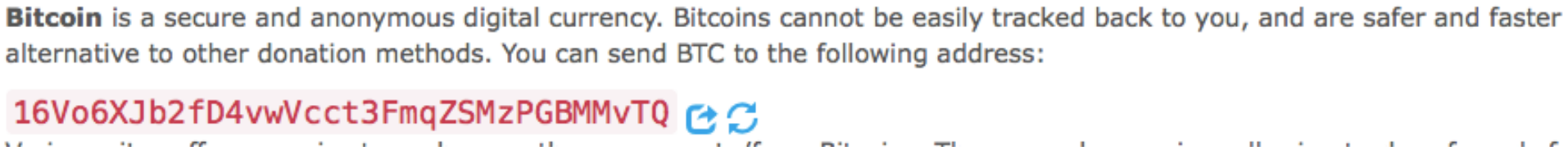
Unlikability:
Different interactions of the same user with the system should not be linkable to each other

Anonymity = pseudonymity + **unlinkability**

Wikileaks

WikiLeaks, an international organization for anonymous whistleblowers, accepts *anonymous* donations via Bitcoin claiming that

- *"Bitcoin is a secure and anonymous digital currency. Bitcoins cannot be easily tracked back to you, and are a [sic] safer and faster alternative to other donation methods."*
- Note the refresh button that every time you refresh you use a different address



Wikileaks

- Note the refresh button that every time you refresh you use a different address
- It is trivail to create a new address every time

So, unlinkable?

Pseudonymity vs anonymity in forums

Reddit: pick a long-term pseudonym

- American social news aggrgation, web content rating discussion website

4Chan: make posts with no attribution at all

- anyone can post comments and share images. Users do not need to register an account before participating in the community

Defining unlinkability in Bitcoin

Unlinkability

- 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

Anonymity = pseudonymity + unlinkability

Question: Why is unlinkability needed?
Because pseudonymity ***is not enough*** *for "privacy" in Bitcoins!*

- Bitcoin Block chain (and transactions) is public
- Linking Bitcoin addresses to real identities is possible
- This might allow to find identities
  - Easy: Many Bitcoin services require real identity
  - More complicated: Linked profiles can be deanonymized by a variety of side channels

Unlinkability

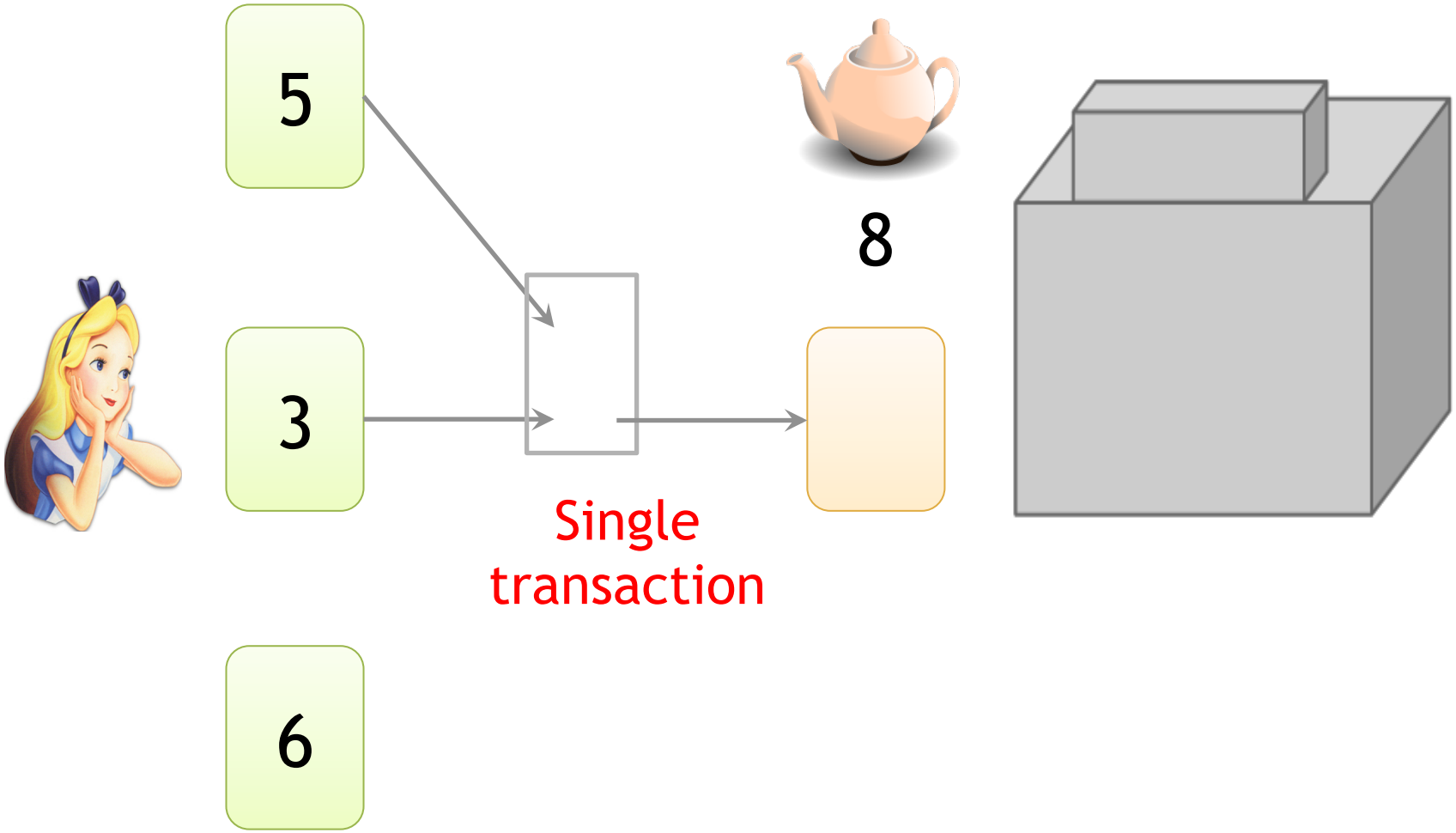
key properties that are required for Bitcoin activity to be unlinkable:

1. It should be hard to link together different addresses of the same user.
2. It should be hard to link together different transactions made by the same user.
3. It should be hard to link the sender of a payment to its recipient (this means the ultimate recipient if some trick has been used by including fake transitions)

Best practice: always receive at fresh address
So, unlinkable?

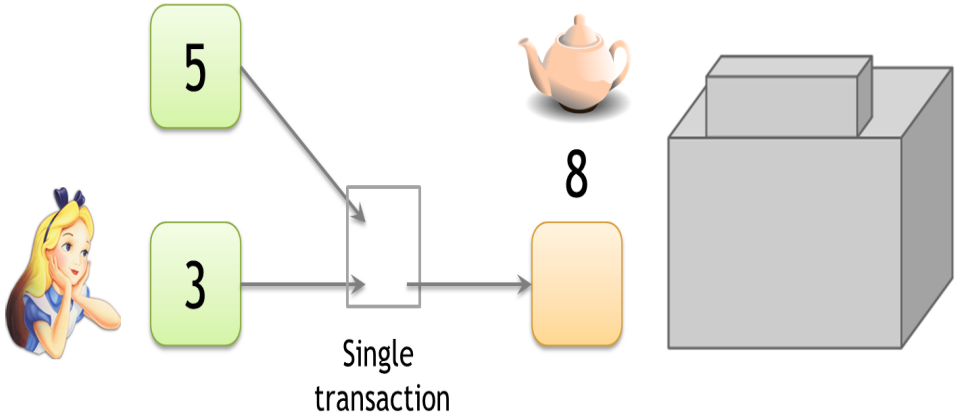
How to de-anonymize Bitcoin?

Alice buys a teapot at Big box store



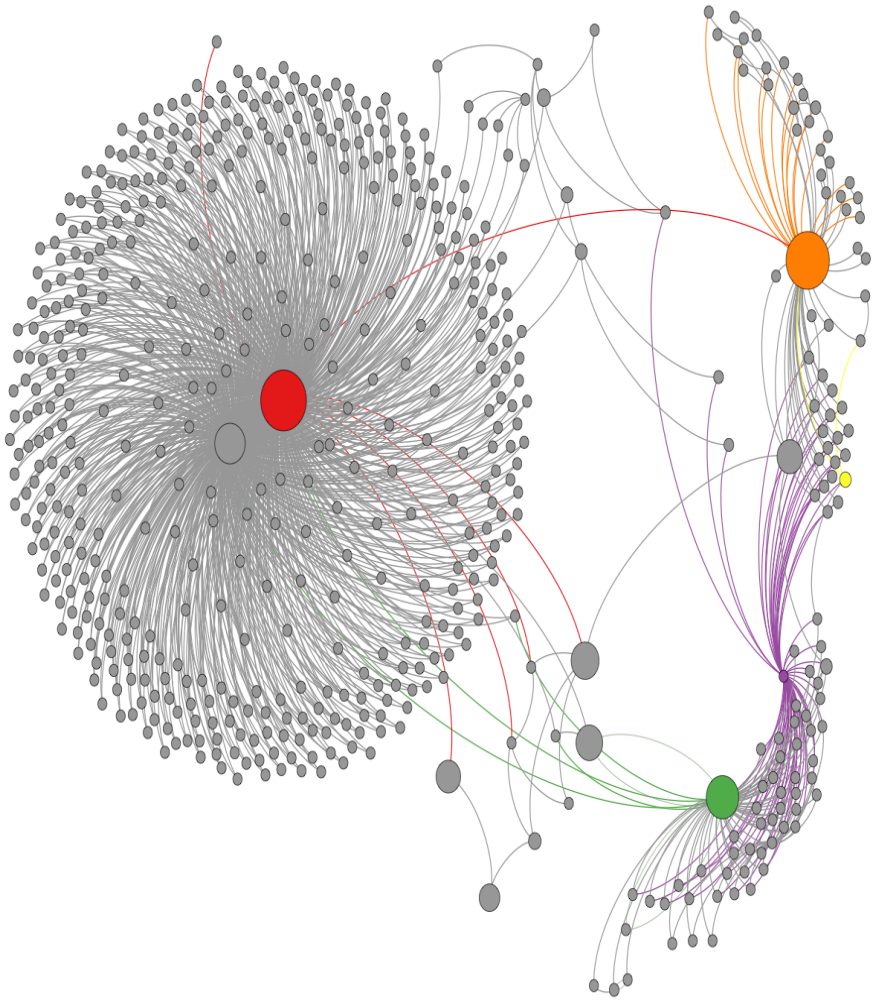
Linking addresses

Shared spending is evidence of joint control



Addresses can be linked transitively

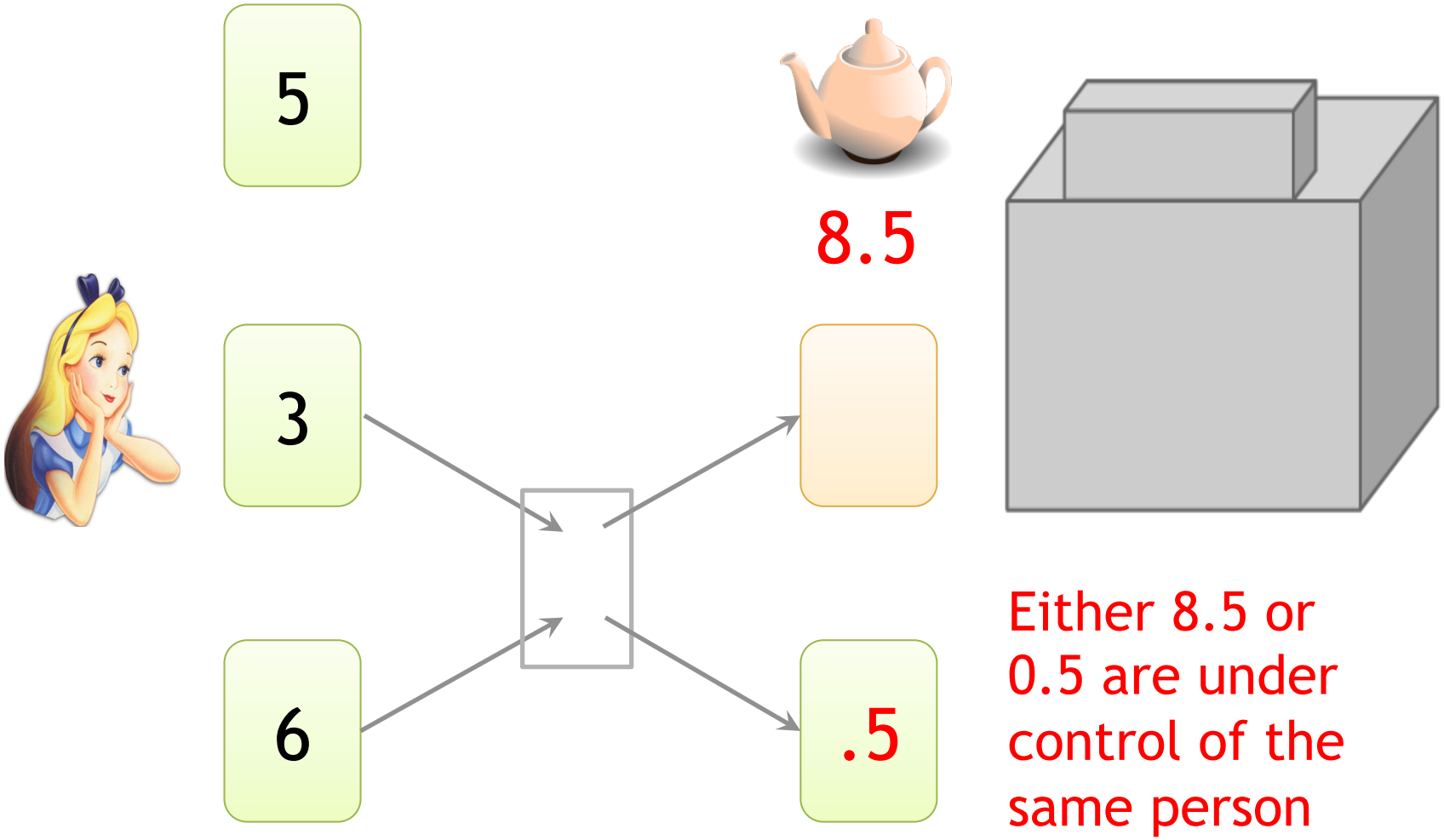
Clustering of addresses



An Analysis of Anonymity in the Bitcoin System

F. Reid and M. Harrigan
PASSAT 2011

Change addresses



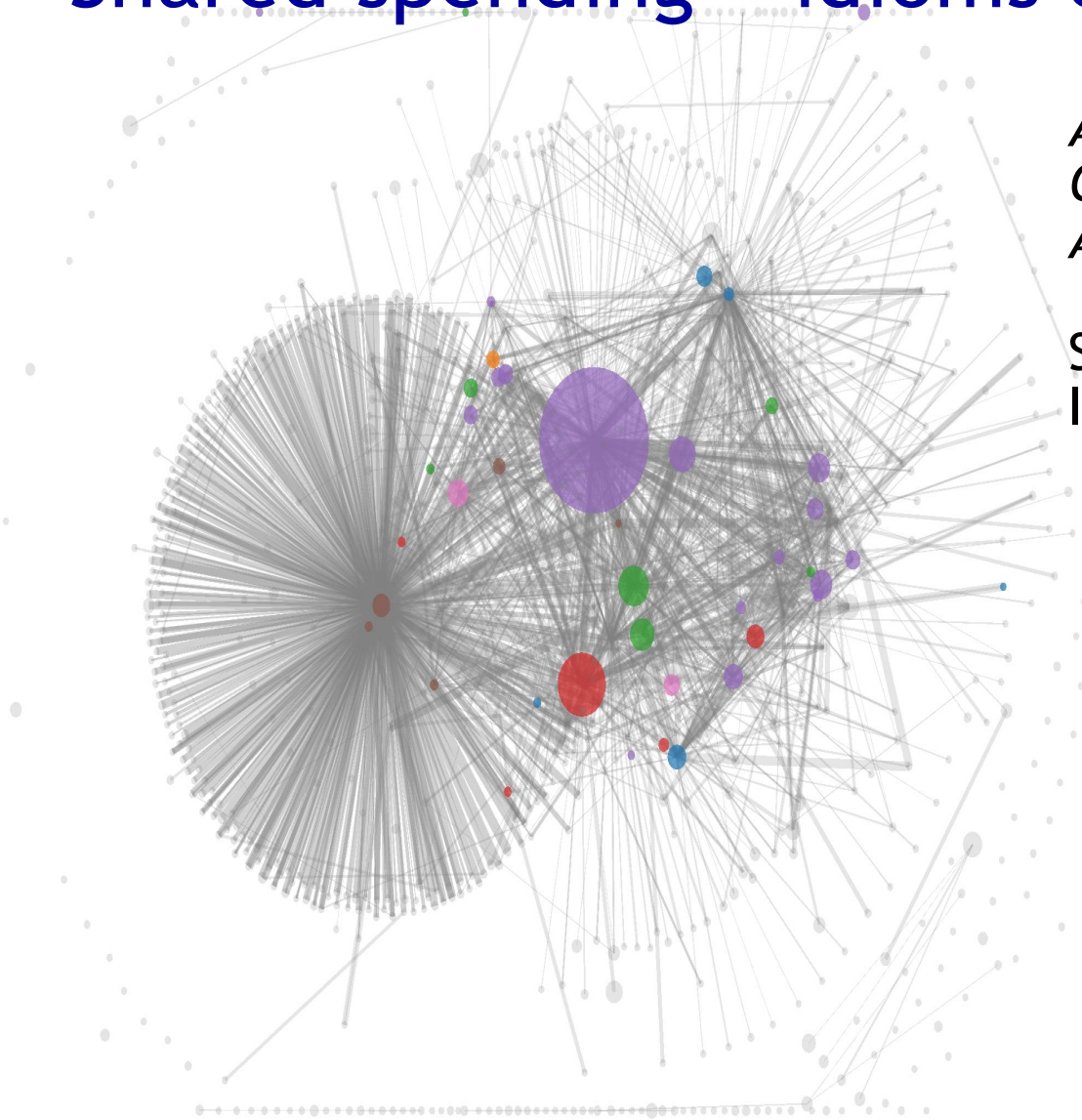
“Idioms of use”

Idiosyncratic features of wallet software

An old version put the change address always as the first address! *Solution: random choice*

In 2013 it has been found that many wallets were using a new address as change address

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

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

From links to users

Can we connect little clusters corresponding to individuals to their real-life identities?

- Directly transacting with individuals
- Via service providers: eventually a bitcoin user will interact witha service provider that must ask your identity (by the law)
- Carelessness: people are not always concerned
- Use of network layer characteristic: often "*the first node to inform you of a transaction is probably the source of it*"

Bitcoin anonymity: conclusions

- Bitcoin is **not** anonymous
- Bitcoin is pseudonymous, but pseudonymity is not enough if your goal is to achieve privacy
- Recall that the block chain is public and anyone can look up all Bitcoin transactions that involved a given address
- If anyone is ever able to link your Bitcoin address to your real world identity, then all of your transactions — past, present, and future — will have been linked back to your identity

Ethical concerns about anonymity

Legitimate "goods": may prevent learning someone's salary information or an organization's private business dealing

Legitimate "worries" : money laundering

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

Legal and Regulatory Risk

- Law-abiding user might lose their funds if an exchange is shut down for criminal activity
- Uncertain tax treatment of gains/losses due to currency fluctuations
- Let’s talk about Bitcoin’s regulatory environment

Regulating Bitcoin

- Bitcoin's original vision is in tension with regulation and government control
- Strong cyber-libertarianism streak
- The decentralized design makes it harder, but by no means impossible, to regulate

Making the case for oversight

- Untraceable digital cash defeats capital controls
- Country can't stop Bitcoin value from flowing in or out
- Government countermeasure: disconnect BTC world from financial institutions
- Example: China

Making the case for oversight

Untraceable digital cash facilitates some crimes:

- kidnapping and extortion
- tax evasion
- sale of illegal items

Welcome! | Silk Road

Silk Road

anonymous marketplace

Welcome [redacted]

messages(0) | orders(0) | account(฿0.00) | settings | log out

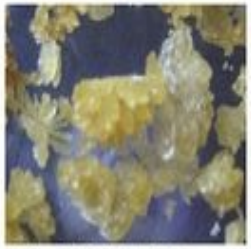
search | (0)

Shop by category:

- Drugs(1249)
  - Cannabis(410)
  - Ecstasy(86)
  - Dissociatives(47)
  - Psychedelics(142)
  - Opioids(92)
  - Stimulants(107)
  - Other(150)
  - Benzos(96)
- Lab Supplies(23)
- Digital goods(93)
- Services(107)
- Money(71)
- Weaponry(9)
- Home & Garden(4)
- Food(1)
- Electronics(11)
- Books(76)
- Drug paraphernalia(46)
- XXX(48)
- Medical(3)
- Computer equipment(19)
- Art(1)
- Apparel(8)
- Sporting goods(3)
- Tickets(1)
- Forgeries(13)
- Fireworks(2)

1g Tangerine Kush Bubble Hash

฿60.96



-NN- DMT YELLOW CLASSIC (500mg)

฿19.39

Barcode Manipulation scam keeping...

฿2.31

3.5g OG Kush

฿22.17

MDMA and MDEA mixure 1 gram

฿23.44

Guerrilla Warfare Book's

฿0.46

co-codamol 30mg codeine / 500mg...

฿4.59

CASH BLOWOUT!! Vendors, SYG is...

฿0.01

Super BOMB Jolly Rancher 1/8...

฿24.20

News:

- Site **glitches**
- Missing **deposits**
- Site **restored**
- Forum bugs **addressed**
- Pricing and hedging **improvements**
- Escrow hedging **update**
- New feature to help protect **sellers**
- Seller ranking and feedback **overhaul**

SILK Road

Largest online market for illegal drugs

- ran as a Tor hidden service
- payment in Bitcoins
- site held BTC in escrow while goods shipped
- eBay-like reputation system
- run by “Dread Pirate Roberts”

operated February 2011 to October 2013

SILK Road

- online **black market** and the first modern **darknet market** best known as a platform for selling illegal drugs.
- part of the **dark web** it was operated as a **Tor hidden service**, such that online users were able to browse it anonymously and securely without potential traffic monitoring
- Initially there were a limited number of new seller accounts available; new sellers had to purchase an account in an auction. Later, a fixed fee was charged for each new seller account.

SILK Road

- October 2013: “Dread Pirate Roberts”, Ross Ulbricht, was arrested
- Charged with money laundering, computer hacking, conspiracy to traffic narcotics, murdering
- Convicted and sentenced to life imprisonment in 2015
- He tried to cover his tracks, but they connected the dots
- Government seized 174,000 BTC
- November 2013 (after R.Ulbricht was arrested and Sik Road was closed) Silk Road 2.0 was opened
- Novemebr 2014 responsible of Sik Road 2.0 were convicted and the site was closed
- Silk Road 3.0 ….

Silk Road: Conclusions

- Hard to keep real life (Ross Ulbrucht) and virtual life (Dread Pirate Roberts) separate: a connection between the two (e.g. Ulbricht use the same computer to access his personal accounts and Dread Pirate account)

- Hard to stay anonymous for a long time

- Police can "follow the money" ⇒
  money becomes untouchable (Ulbricht owned 174K Bitcoin= 30M US$ but could not spend!)

Alternate measures of Bitcoin anonymity

- The “taint” of a Bitcoin transaction evaluates the association between an address and earlier transaction addresses. The more “‘taint” the stronger the link between the two addresses.

- Give high “taint” score (to *S*-*R* pair) if Bitcoins sent by an address *S* always end up at an address *R*

Alternate measures of Bitcoin anonymity

Give high "taint" score (to *S*-*R* pair) if Bitcoins sent by an address *S* always end up at an address *R*

Not a good measure of Bitcoin anonymity:

- Makes implicit assumptions about the adversary's calculations regarding linking pairs of addresses
- Adversary may use alternate techniques for linking address pairs – e.g., timing analysis or wallet software idiosyncrasies.

Ethical concerns about anonymity

Legitimate "goods": may prevent learning someone's salary information or an organization's private business dealing

Legitimate "worries" : money laundering

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 morally are pretty much the same technologically

Similar dilemma: Tor

Anonymous communication network

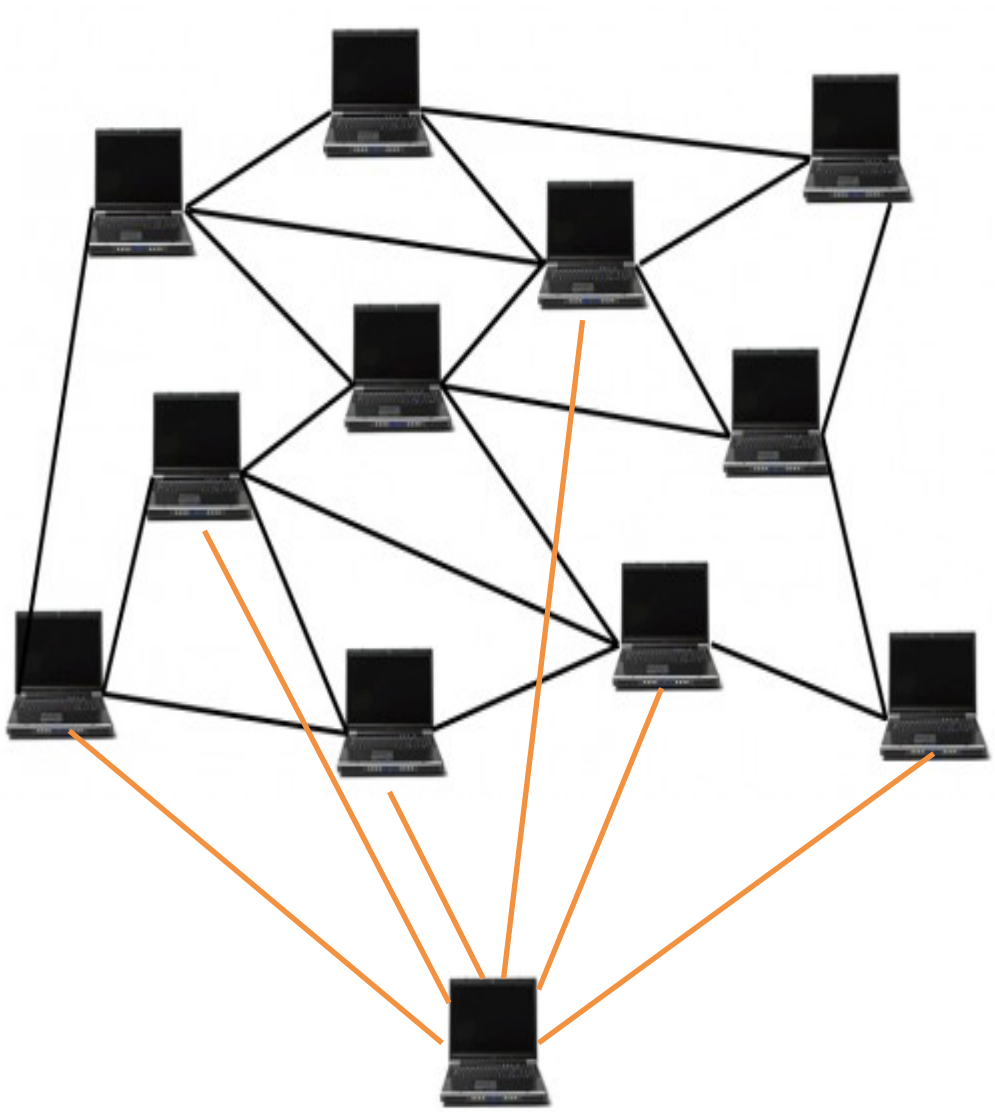
Sender and receiver of message unlinkable

Used by:

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

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

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

How to make Bitcoin anonymous

Mixing

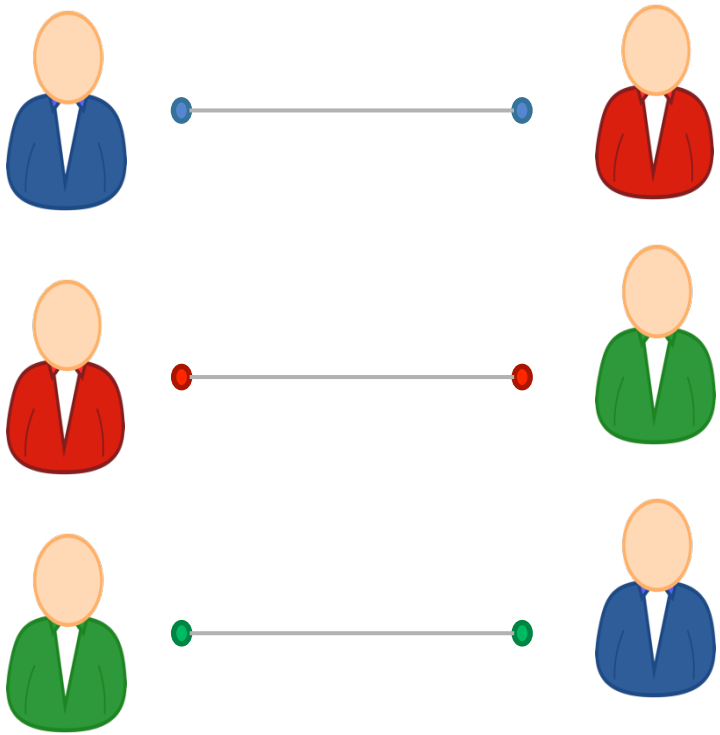
Mixing: terminology

- Bitcoin activities are recorded and available publicly via the blockchain
- when you finally use Bitcoin to pay for goods and services, you will of course need to provide your name and address to the seller for delivery purposes.
- It means that a third party can trace your transactions and find ID information.
- To avoid this, such mixing service provide the ability to exchange your bitcoins for

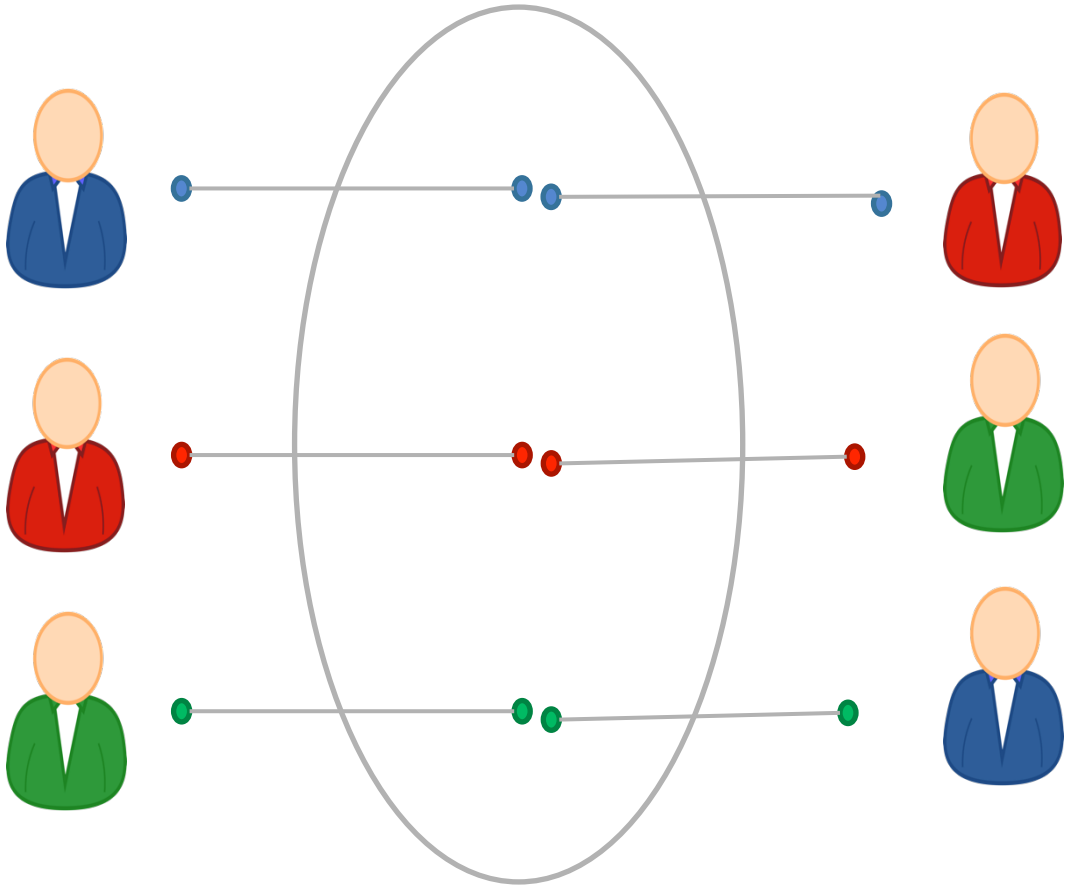
Mixing: terminology

- **mixing services** are used to mix one's funds with other people's money, intending to confuse the trail back to the funds' original source
- In traditional financial systems, the equivalent would be moving funds through banks in countries with bank secrecy laws (Cayman islands, Bahams etc.)
- When mixing bitcoins, you send your money to an anonymous service and they will send you someone else's coins.
- So, now, whatever those coins were used for may now be traceable back to you. Additionally, mixing large amounts of money may be illegal,

Mixing mix one's funds with other people's money,



To protect anonymity, use an intermediary



Bits

Study Suggests Link Between Dread Pirate Roberts and Satoshi Nakamoto

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

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
- Essentially swaps a user’s coin (address) with other users’ coins (addresses)
- Relatively small anonymity set (only comprise of those users who use the mixing service at that instant)!

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

Principles for mixing services

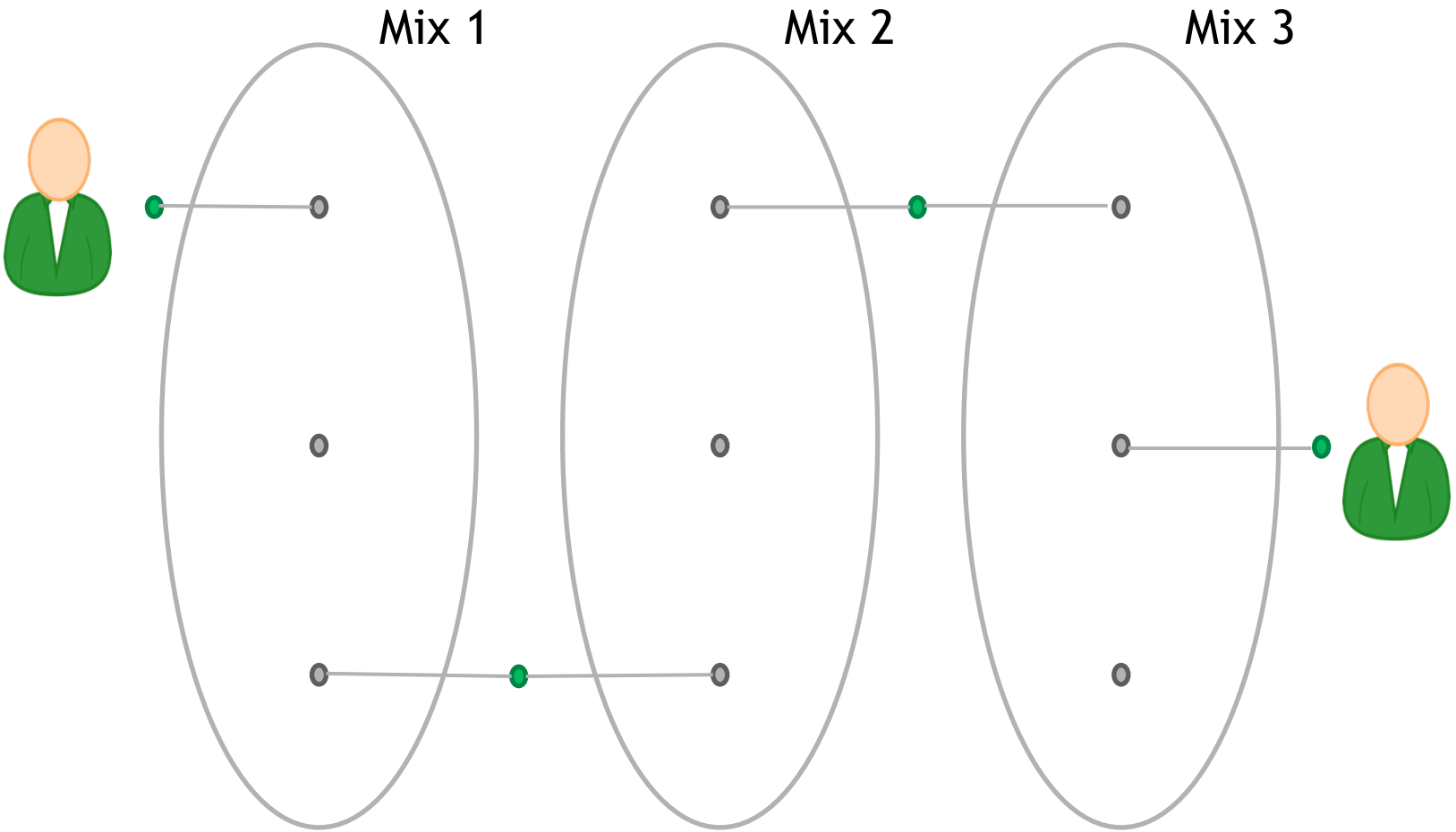
1. Use a series of mixes

   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!

3. Client side must be automated

   Desktop wallet software

Mixcoin: Anonymity for Bitcoin with accountable mixes

J. Bonneau et al.
Financial Cryptography 2014

Remaining problem: trusting mixes

1. Stay in business, build up reputation
2. Users can test for themselves
3. Cryptographic “warranties”

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.

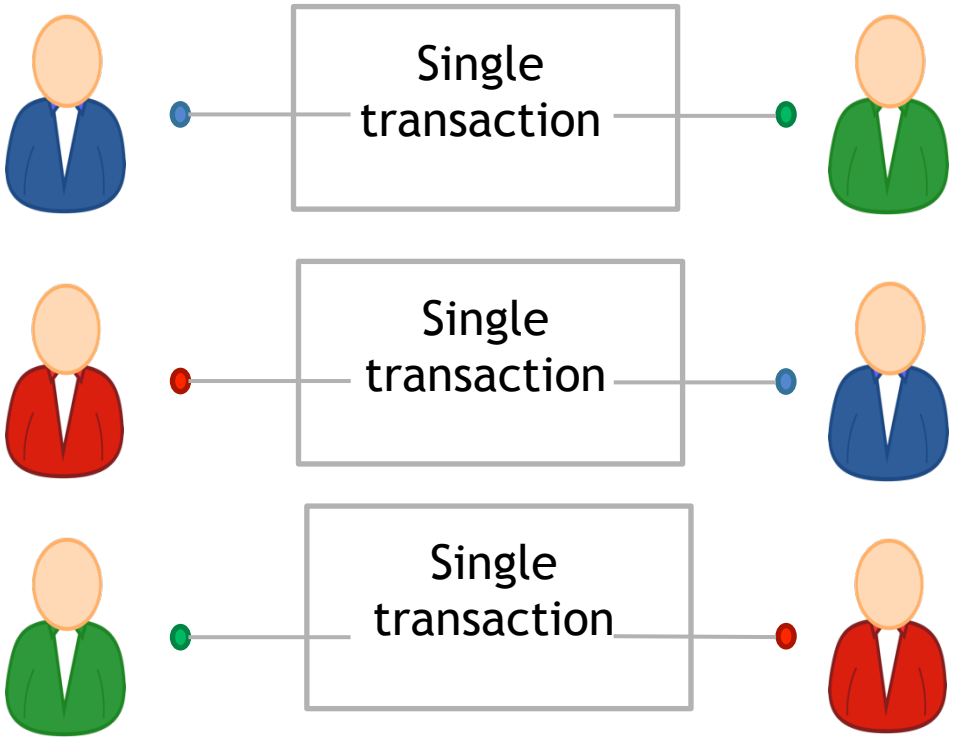
— Bitcoin Wiki

Decentralized mixing

Why decentralized mixing?

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

Coinjoin

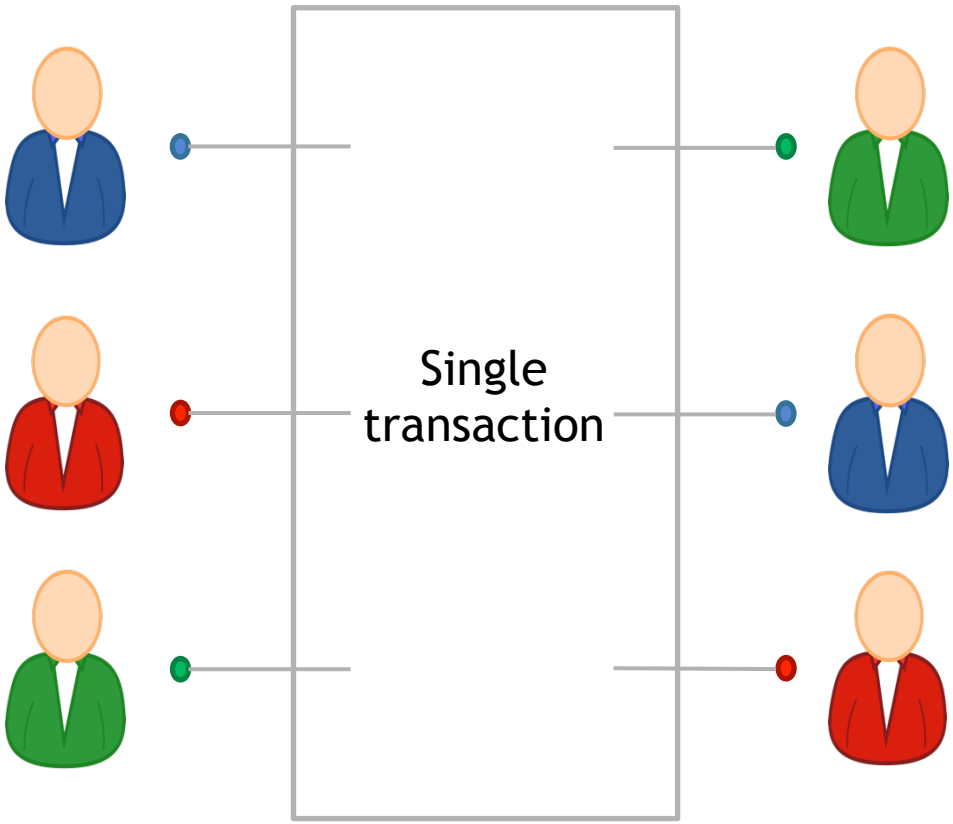


3 transactions

Each signature is entirely separate

Proposed by Greg Maxwell, Bitcoin core developer

Coinjoin



Each signature is entirely separate

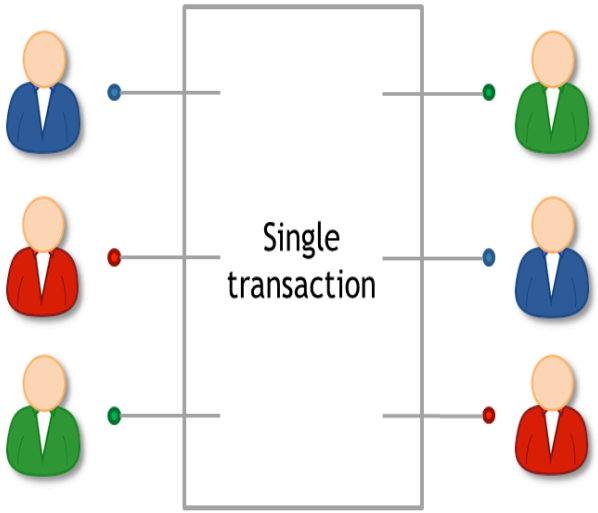
This is 1 mixing round

Mixing principles from before apply on top of basic protocol

Proposed by Greg Maxwell, Bitcoin core developer

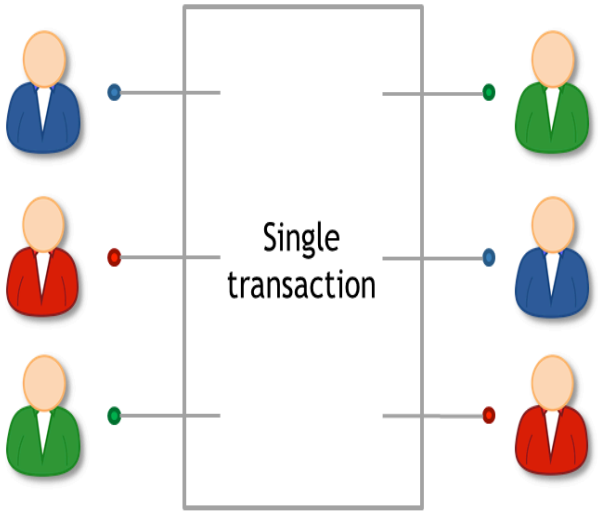
Coinjoin algorithm

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



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

Problem
Use an (un)trusted server
The server learns the mapping

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:

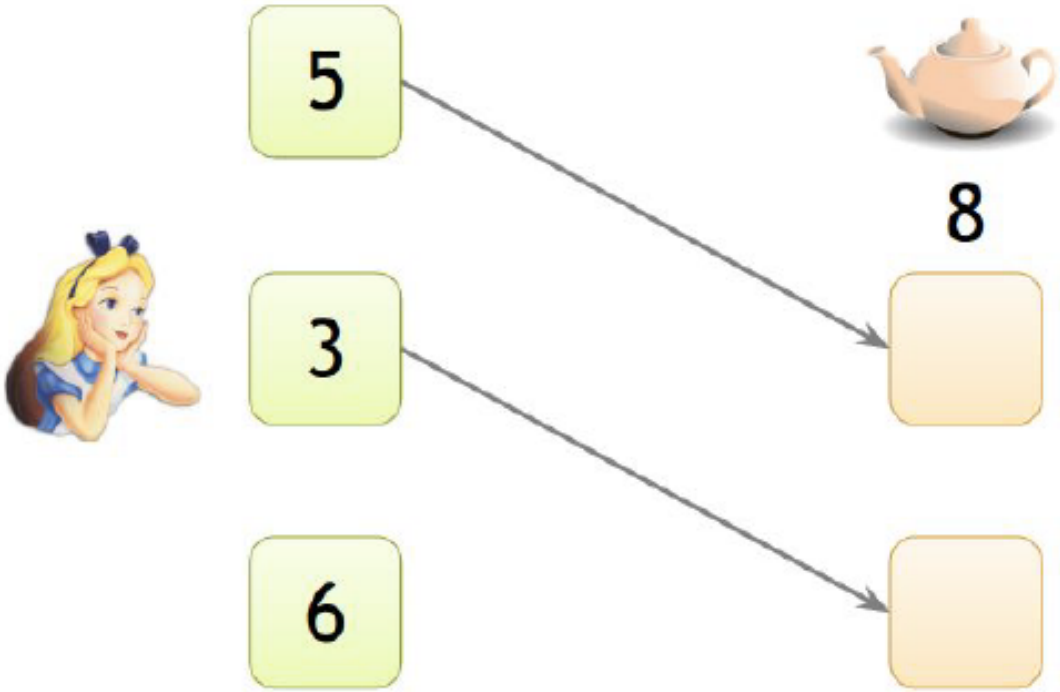
- Proof of work
- Proof of burn
- Server kicks out malicious participant
- Cryptographic “blame” protocol
  (*CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin*
  T. Ruffing et al., PETS 2014)

frequent 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



Main digital coins

		Value		Market capitalization in Billion Euro
1	Bitcoin BTC	8.550,64 €	+0,18%	154.0B €
2	Ethereum ETH	170,07 €	+2,01%	18.4B €
3	XRP XRP	0,27 €	-0,22%	11.6B €
4	Bitcoin Cash BCH	261,82 €	+6,57%	4.7B €
5	Litecoin LTC	54,54 €	+1,07%	3.5B €
6	EOS EOS	3,08 €	+0,03%	2.9B €
7	Stellar Lumens XLM	0,0606 €	+0,88%	1.2B €

Proof of Work (PoW)

- In a PoW system, network participants have to solve so-called “cryptographic puzzles” to be allowed to add new “blocks” to the blockchain. This puzzle-solving process is commonly referred to as “mining”.
- Because the input of each puzzle becomes larger over time (resulting in a more complex calculation), the PoW mechanism requires a vast amount of computing resources, which consume a significant amount of electricity. If a network participant (i.e. a node) solves a cryptographic puzzle, it proves that he has completed the work, and is rewarded with digital form of value (or in the case of a cryptocurrency, with a newly mined coin).
- This reward serves as an incentive to uphold the network. The cryptocurrency Bitcoin is based on a PoW consensus mechanism. Other examples include Litecoin, Bitcoin Cash, Monero, etc.

Proof of Stake (PoS)

- In a PoS system, a transaction validator (i.e. a network node) must prove ownership of a certain asset (or in the case of cryptocurrencies, a certain amount of coins) in order to participate in the validation of transactions.
- This act of validating transactions is called “forging” instead of “mining”. For example, in the case of cryptocurrencies, a transaction validator will have to prove his “stake” (i.e. his share) of all coins in existence to be allowed to validate a transaction.
- Depending on how many coins he holds, he will have a higher chance of being the one to validate the next block (i.e. this all has to do with the fact that he has greater seniority within the network earning him a more trusted position).
- The transaction validator is paid a transaction fee for his validation services by the transacting parties. Cryptocurrencies such as Neo and Ada (Cardano) utilize a PoS consensus mechanism.

permissionless vs permissioned blockchain

- On an *open, permissionless blockchain*, a person can join or leave the network at will, without having to be (pre-)approved by any (central) entity.
- There is no central owner of the network and software, and identical copies of the ledger are distributed to all the nodes in the network.
- The vast majority of cryptocurrencies currently in circulation is based on permissionless blockchains (e.g. Bitcoin, Bitcoin Cash, Litecoin, …).

- On a *permissioned blockchain*, transaction validators (i.e. nodes) have to be pre-selected by a network administrator (who sets the rules for the ledger) to be able to join the network.
- This allows, amongst others, to easily verify the identity of the network participants.
- However, at the same time it also requires network participants to put trust in a central coordinating entity to select reliable network nodes.

permissioned blockchains

- In general, permissioned blockchains can be further divided into two subcategories.
- On the one hand, there are open or public permissioned blockchains, which can be accessed and viewed by anyone, but where only authorised network participants can generate transactions and/or update the state of the ledger.
- On the other hand, there are closed or “enterprise” permissioned blockchains, where access is restricted and where only the network administrator can generate transactions and update the state of the ledger.
- What is important to note is that just like on an open permissionless blockchain, transactions on an open permissioned blockchain can be validated and executed without the intermediation of a trusted third-party. Some cryptocurrencies, like Ripple and NEO utilise public permissioned blockchains.

Ethereum (2015)

Ethereum is a decentralized platform that runs "smart contracts".

- Smart contracts are "self-executing" contracts or applications that run exactly as programmed without any possibility of downtime (i.e. the blockchain is always running), censorship, fraud or third-party interference.
- Ethereum has a capability that goes far beyond that of a pure P2P digital cash equivalent like Bitcoin. In simple terms, it is much like a smartphone operating system on top of which software applications can be built.
- Technically speaking, the Ethereum platform itself is not a cryptocurrency and is permissioneless blockchains. However Ethereum requires a form of on-chain value to incentivise transaction validation within the network (i.e. a form of payment for the network nodes that execute the operations).
- This is where Ethereum's native cryptocurrency "ether" (ETH) comes into play. Ether does not only allow smart contracts to be built on the Ethereum platform (i.e. it fuels them), but it also functions as a medium of exchange.

RIPPLE (public permissioned blockchain)

- Ripple is an open-source, P2P decentalized digital payment platform that allows for fast transfers of currency (e.g. US Dollar, Yen, Bitcoin, ...) launched in 2012 by the company Ripple (Labs) responsible for the further development of the Ripple protocol
- First company to have received a "BitLicense" for an institutional use case of digital assets from New York's Department of Financial Services. It is also getting support from a number of big players in the financial services industry, such as Bank of America Merill Lynch, Santander, etc.
- Ripple's uses the cryptocurrency XRP. XRP was built to become a bridge currency to allow financial institutions to settle cross-border payments a lot faster and cheaper than they can using the global payment networks that are in place today, which can be slow and involve multiple middlemen (i.e. banks).
- According to Ripple, XRP can handle more than 1,500 transactions per second. While it was initially developed and intended for enterprise use, it has been adopted by a large number of cryptocurrency users.
- Ripple (XRP) is not based on a PoW or a PoS mechanism to validate transactions, but it makes use of its own specific consensus protocol.
- The total supply of XRP has been fully "pre-mined" (or better: created upon the coin's inception) by its inventors. At present, 8 B XRP is held by Ripple (Labs),(39 B XRP has been distributed; and 52 B XRP has been placed in escrow to create certainty of XRP supply at any given time.

Stellar (public permissioneless blockchain)

- Similar to Ripple: Stellar is an open-source, distributed payments infrastructure, created in 2014 by one of Ripple's founding fathers; Stellar's development is supported by the non-profit organization Stellar.org
- Its goal is to connect people to low-cost financial services to fight poverty and develop individual potential. Stellar can also be used to build smart contracts.
- It is not based on a PoW or PoS consensus mechanism, but has its own specific consensus protocol.
- Stellar is home to the cryptocurrency Lumen (XLM) that are used to pay for transactions on the Stellar network; they contribute to the ability to move money around the world and to conduct transactions between different currencies quickly and securely.
- Similar to Ripple's cryptocurrency XRP, the total supply of Stellar Lumens is "pre-mined". It is held by Stellar.org who has been given the task to distribute Lumens for free, in the following manner213: 50% is to be given away to individuals (via a direct sign-up program); 25% is to be given away to partners (via a specific partnership program); 20% is given away to Bitcoin and XRP holders; and 5% is reserved for Stellar.org's operational expenses.

Bitcoin Cash (BCH): open, permissionless blockchain

- Bitcoin Cash was created on the 1st of August 2017 and is based on Bitcoin's original SHA-256 PoW algorithm, yet with some changes to its code.
- Bitcoin Cash is what is known in the crypto-community as a "hard fork" of the Bitcoin blockchain. It is the result of two very different visions on the future of Bitcoin and the Bitcoin blockchain, whereby the Bitcoin blockchain diverged into two potential paths forward.
- In short, some Bitcoin developers wanted to raise the block size limit from 1MB to 8MB, to reduce transaction fees and improve confirmation times, whilst others had different plans. Because the community could not reach a consensus, the new cryptocurrency Bitcoin Cash was created. Bitcoin Cash makes use of the PoW mechanism, which means that it can be mined.
- A direct result of the hard fork, is that anyone who held Bitcoin at the time Bitcoin Cash was created also became owner of the same amount of Bitcoin Cash. Any Bitcoin acquired after that specific time follows the original path and does not include Bitcoin Cash. In principle, a "hard fork" does not change the nature of a coin's blockchain. In other words, Bitcoin Cash also runs on an open permissionless blockchain, just like Bitcoin.
- Bitcoin cash is a pseudo-anonymous coin

Litecoin: open, permissionless blockchain

- Like Bitcoin, Litecoin (LTC) is an open-source decentralized P2P cryptocurrencylaunched in 2011. Scrypt PoW algorithm, which utilises Bitcoin's and is based on what is known as the original SHA-256 PoW algorithm.
- Litecoin is often described as the 'silver' to Bitcoin's gold.
- Apart from the fact that it uses a different algorithm, it is different from Bitcoin in two ways.
- Firstly, and this results from the use of the Scrypt PoW algorithm, Litecoin offers a much faster transaction speed than Bitcoin. The time needed to generate a block on the Bitcoin BC is about ten minutes, while the average block creation time on the Litecoin blockchain is approximately 2.5 minutes.
- Secondly, the total supply limit of Litecoin is with 84 million coins, much higher than the 21 million supply limit of Bitcoin.
- like Bitcoin, Litecoin is a *pseudo-anonymous coin*. Everyone can verify the chain of LTC transactions on the basis of the public ledger

IOTA: permissionless distributed ledger

- IOTA (2016), is an open-source eco-system where people and machines can transfer value (i.e. money) and/or data **without any transaction fees** in a trustless, permissionless, and decentralized environment; focus on microtransastions; total supply of IOTA is 2779 B
- IOTA is not based on blockchain technology, but constitutes a different application of distributed ledger technology; they claim is more scalable than the technology behind most other coins, and promises faster transaction speeds.
- IOTA's distributed ledger does not consist of transactions grouped into (transaction) "blocks" and stored into sequential chains (i.e. it is not a "blockchain"), but of a stream of individual transactions entangled together.
- Instead of requiring miners to perform computational PoW and validate transaction blocks in exchange for newly "mined" coins, IOTA's network participants create a consensus themselves by validating two previous transactions each time they wish to make a new transactio; this produces a directed acyclic graph (DAG).
- The majority of IOTA it was sold by IOTA's inventors in a crowdsale to pay for development costs and fund the IOTA Foundation.

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

Basecoin: Bitcoin-like Altcoin

Zerocoin: Extension of Basecoin – it iis announced it will implemented in Anoncoin (other digital coin9

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)

Zerocoins

Work with fixed amount of 1$.
Imagine a huge shared board.
Unlike Zerocoins, this is a centralized version (for clarity's sake)

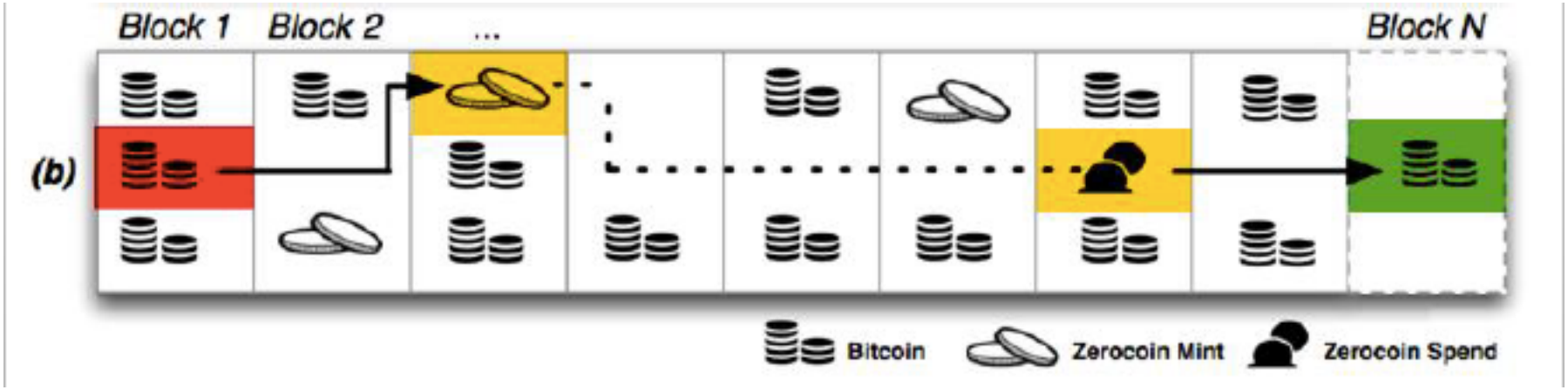
- Suppose you have 1$ on you. You want to anonymize it, in Bitcoin terms, meaning you want to change the owner, without the transaction being public. You have access to a secure board (with a trusted guardian).
- Pin 1$ on the corkboard. Receive an anonymous ticket "Certificate : 1$ pinned" from the guardian
- Give a friend your certificate.
- Send him get the 1$ back. The guardian will unpin a 1$ bill from the corkboard and give it to your friend

Zerocoins

Different from Bitcoin, not an evolution

- Uses Bitcoin as underlying money (Both are needed)
- Anonymity (without Trusted Party)

- Bitcoins X -> Mint -> Zerocoin -> Spend -> Bitcoins Y
- Public Key Y can't be linked to Public Key X (computationally infeasible)



- "Anonymized vouchers of Bitcoins", "Currency Swap"

Two challenges

Crucial observation: to mint a bitcoin transforming it in zerocoin you must have one BTC

How to construct these proofs?

1. How to make sure each proof can only be “spent” once?
2. How to be sure that these proofs do not reveal the owner of the BTC (In our example X) ?

Commitment

Generate a message S
and a random secret *r*

1. I commit on message
   By publishing *H(S, r) (H is Hash)*
2. *Then I can show my commitment*

. *on message S by revealing r*

1. 1. Commit: Equivalent to write a message S
2. and putting in an envelope and close the
3. envelope
4. 2. Show my commitment: opening the envelope

Zero-knowledge proofs

A way to prove a statement without revealing any other information

1. I know an input r such that Hash(S,r)= **da39a3ee5e** (without revealing r)

Not sufficient

2. I know an input r that hashes to some hash in the following set:
   Hash(S1,r) or Hash(S2,r) or …Hash(Sn,r)

Question: why 1. above is not enough? (unlinkability!)

Minting zerocoins

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

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)

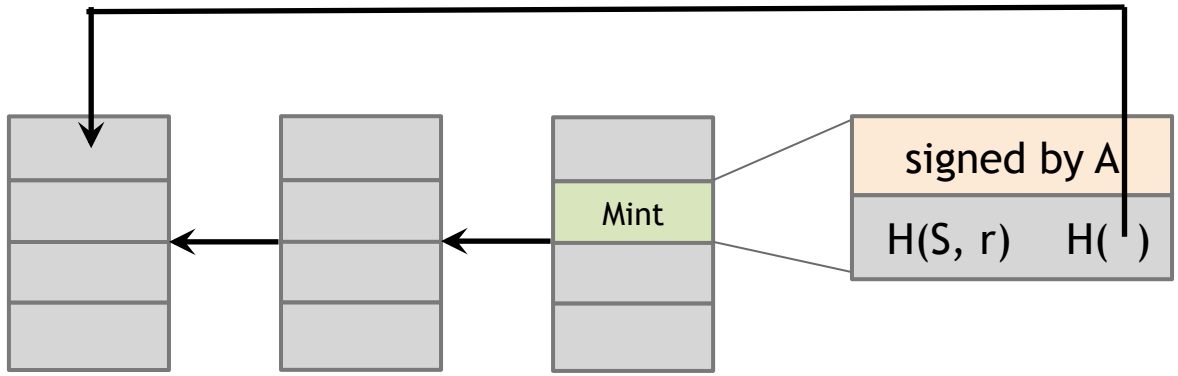
Compute *H(S, r)*

Simplification of the real protocol

Minting a zerocoin

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

Create Mint Tx with 1 bitcoin as input



To spend a zerocoin S:

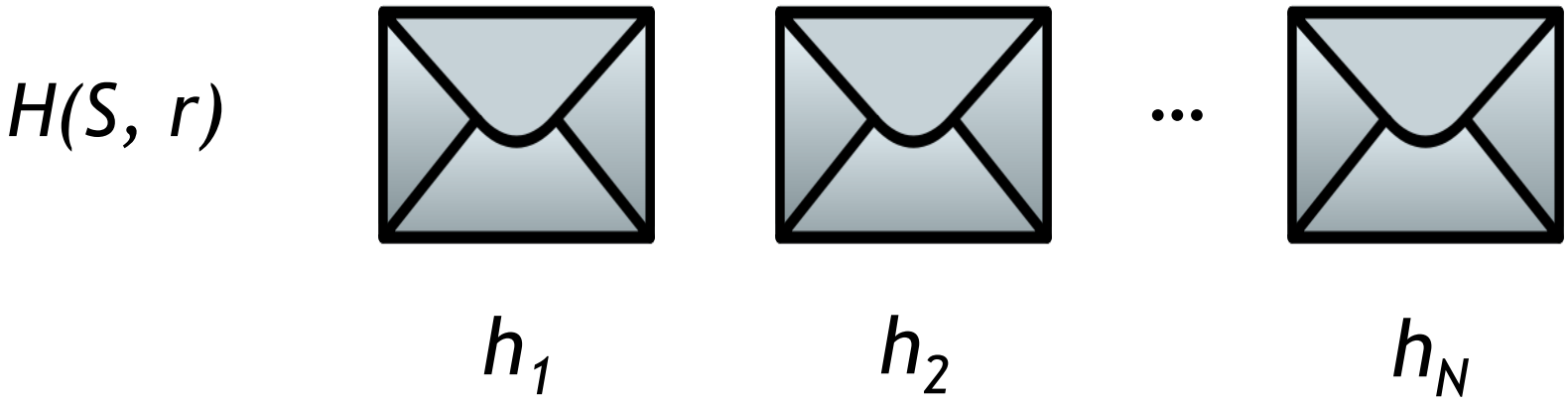
- Reveal *S*
  (miners will verify *S* hasn't been spent before)

- 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 (remember we assume all zero coins have the same value)

Zerocoin is anonymous

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



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

$H(S, r) = h_N$

Zerocoin : conclusions

- Zerocoin supports regular transactions for when you don't need unlinkability (+)

- Zerocoin includes computationally expensive transactions that are used only for mixing (-)

- Only a fixed amount (1 BTC) can be minted; we need divisible coins

- These problems might be solved in Zerocoin 2.0

Zerocash: Zerocoin without Basecoin

Two differences

- Different crypto for proofs (Much More efficient)
- More general: 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

Zerocash: the problem

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