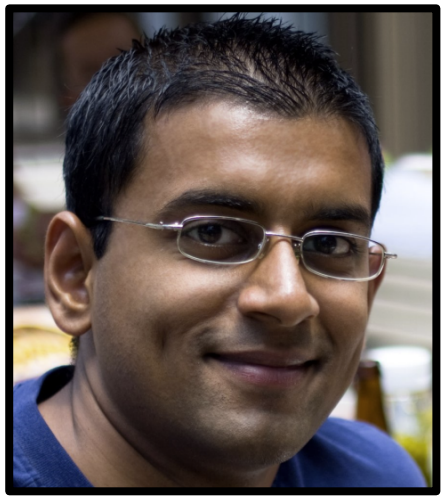
Acknowledgements

Joseph Bonneau

Ed Felten



Arvind Narayanan

Andrew Miller

Bitcoin Operations

Info from the public blockchain

+

Owner's secret signing key

So it's all about key management!

Bitcoin Operations

Simplest approach: store key in a file, on your computer or phone

Very convenient.

As available as your device.

- device lost/wiped ⇒ key lost ⇒ coins lost

As secure as your device.

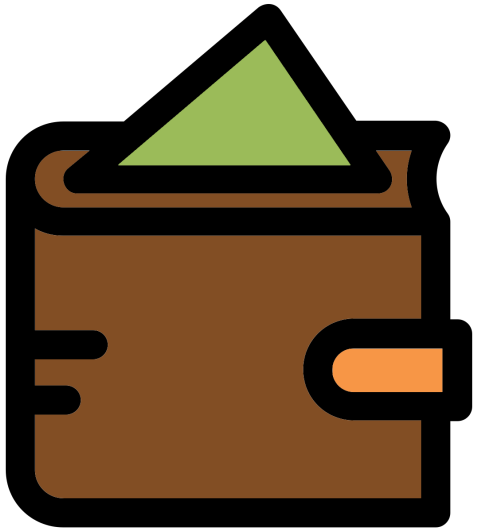
- device compromised ⇒ key leaked ⇒ coins stolen

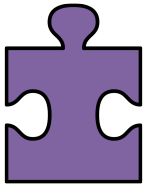
Bitcoin Wallet Quiz

What is the defining characteristic of these bitcoin wallets?

Hot storage: online

Cold storage: offline



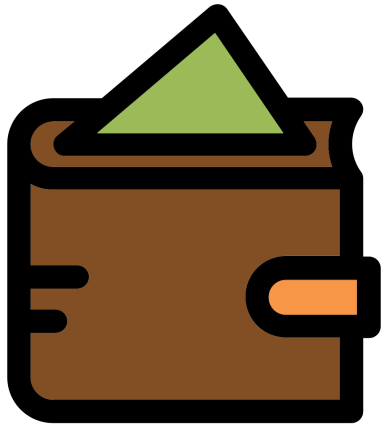


Bitcoin Wallet Quiz

	Hot Storage	Cold Storage
Location	Online	Offline
Convenient?	Yes	No
Security?	Risky	Archival but safe

Bitcoin Wallet Quiz

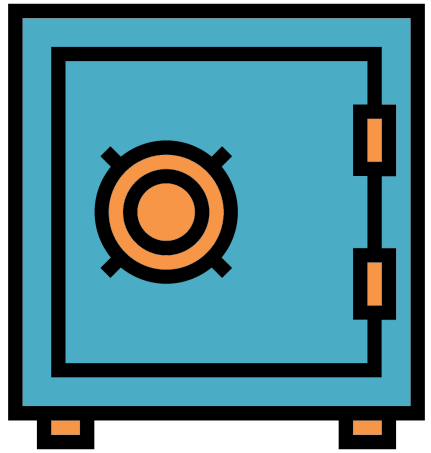
Hot storage



online

convenient but risky

Cold storage



offline

archival but safer

separate keys

Hierarchical Wallet

Problem:

- Want to use a new address (and key) for each coin sent to cold
- But how can hot wallet learn new addresses if cold wallet is offline?

Awkward solution:

- Generate a big batch of addresses/ keys, transfer to hot beforehand

Hierarchical Wallet

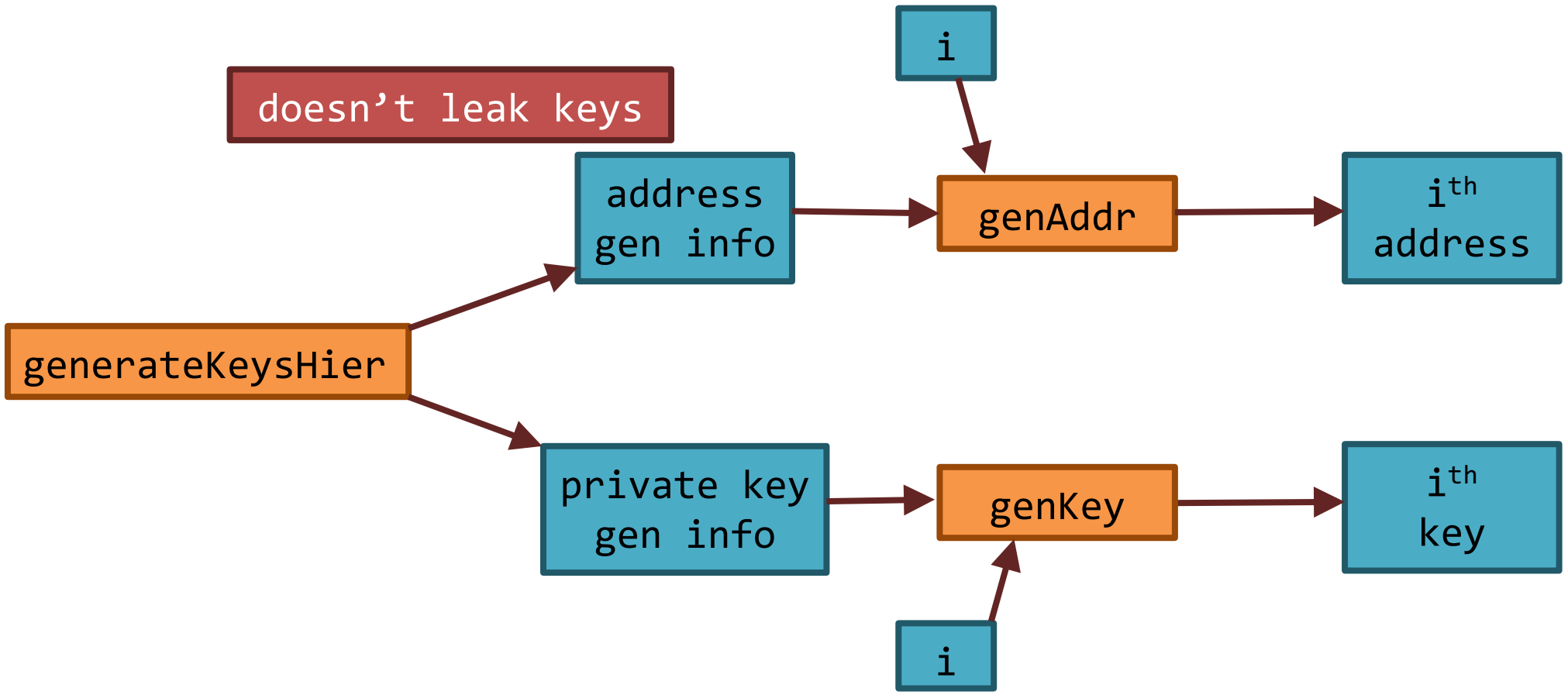
Problem:

- Want to use a new address (and key) for each coin sent to cold
- But how can hot wallet learn new addresses if cold wallet is offline?

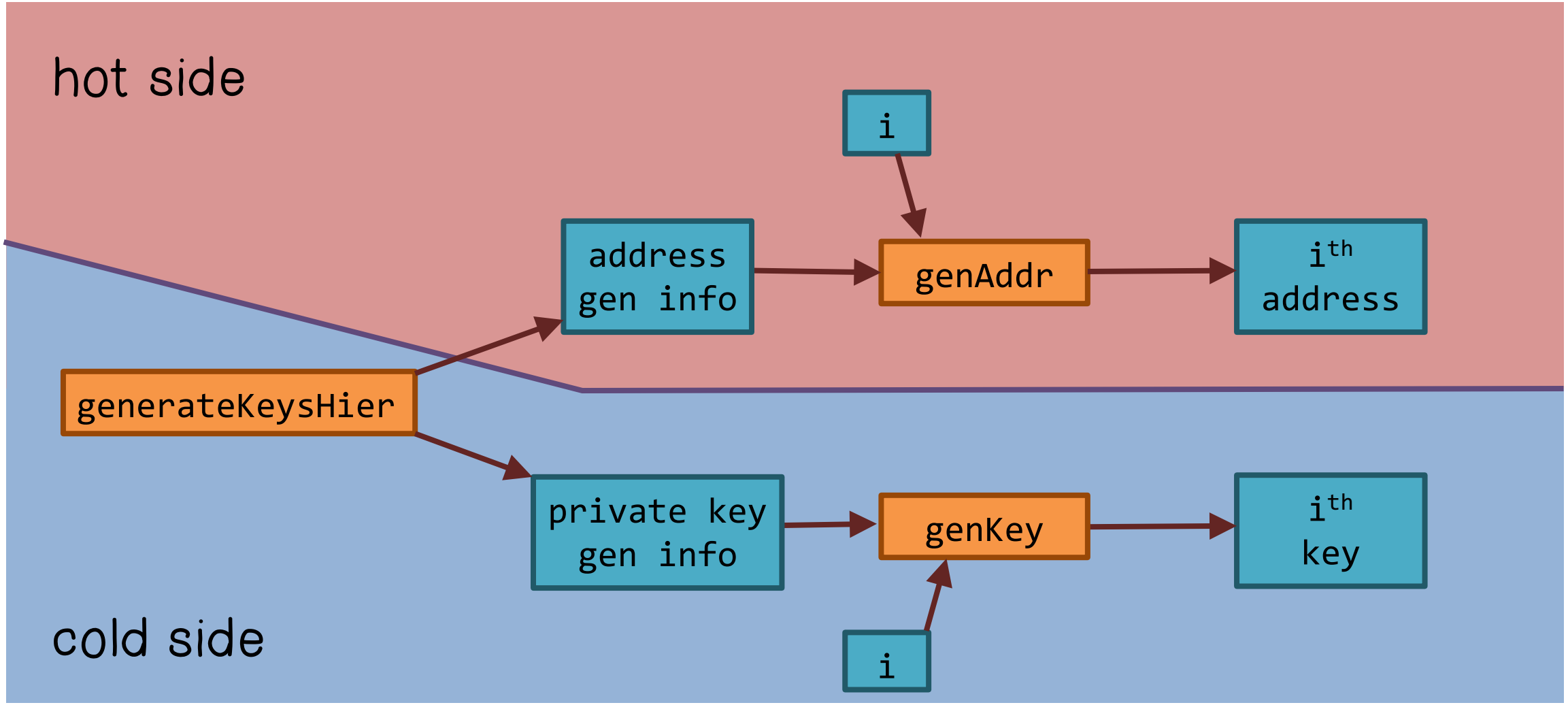
Better solution:

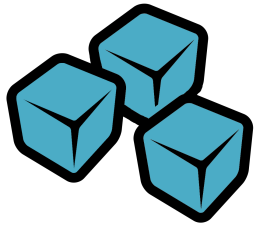
- Hierarchical wallet

Hierarchical Wallet



Hierarchical Wallet





Cold Storage

How to store cold information:

- Info stored in device, device locked in a safe
- "Brain wallet" encrypt info under passphrase that user remembers
- Paper wallet
  - print info on paper
  - lock up the paper
- In "tamperproof" device
  - device will sign things for you, but won't divulge keys

Cold Wallet Quiz

Match the cold storage to its characteristic:

- USB drive or other data storage (USB)
- Paper wallet (Paper)
- Physical bitcoin (Coin)
- Online cold storage (Online)
- Offline bitcoin wallet (Offline)

Paper	Can rot or be lost, torn, stolen
Coin	If made of magnesium, tin, lead can be destroyed by fire
Online	Multiple overwriting attempts are not enough to ensure that discarded computers cannot be hacked
USB	Data can be hard to recover if the storage device is old
Offline	Can be damaged by magnets

Online Wallets and Exchanges

Bitcoin Exchanges:

- Accept deposits of Bitcoins and fiat currency ($, €, ...)
  - Promise to pay back on demand
- Lets customers:
  - make and receive Bitcoin payments
  - buy/sell Bitcoins for fiat currency
  - typically, match up BTC buyer with BTC seller

Online Wallets and Exchanges

Bank Regulation

for traditional banks, government typically:

- imposes minimum reserve requirements
- must hold some fraction of deposits in reserve
- regulates behavior, investments
- insures depositors against losses
- acts as lender of last resort

Online Wallets and Exchanges

Proof of Reserve

Bitcoin exchange can prove it has fractional reserve.

- fraction can be 100%

Prove how much reserve you're holding:

- publish valid payment-to-self of that amount
- sign a challenge string with the same private key

Prove how many demand deposits you hold: ...

Merkle Tree Quiz

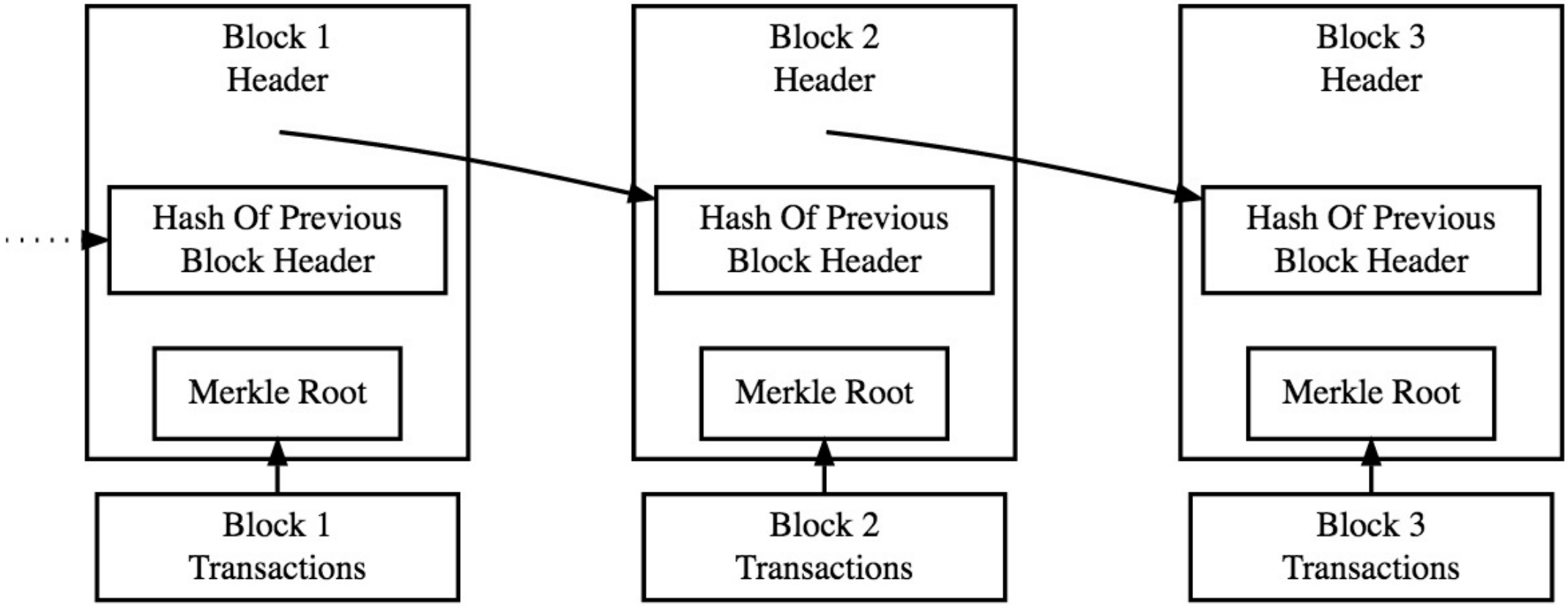
Answer the following questions with regards to Merkle Trees.

Two Merkle trees can be compared if they have the same hash depth .

If two Merkle trees have the same root hashes, then their data blocks can be considered to be the same .

In a bitcoin block, the Merkle root is stored in the block header.

Merkle Tree Quiz

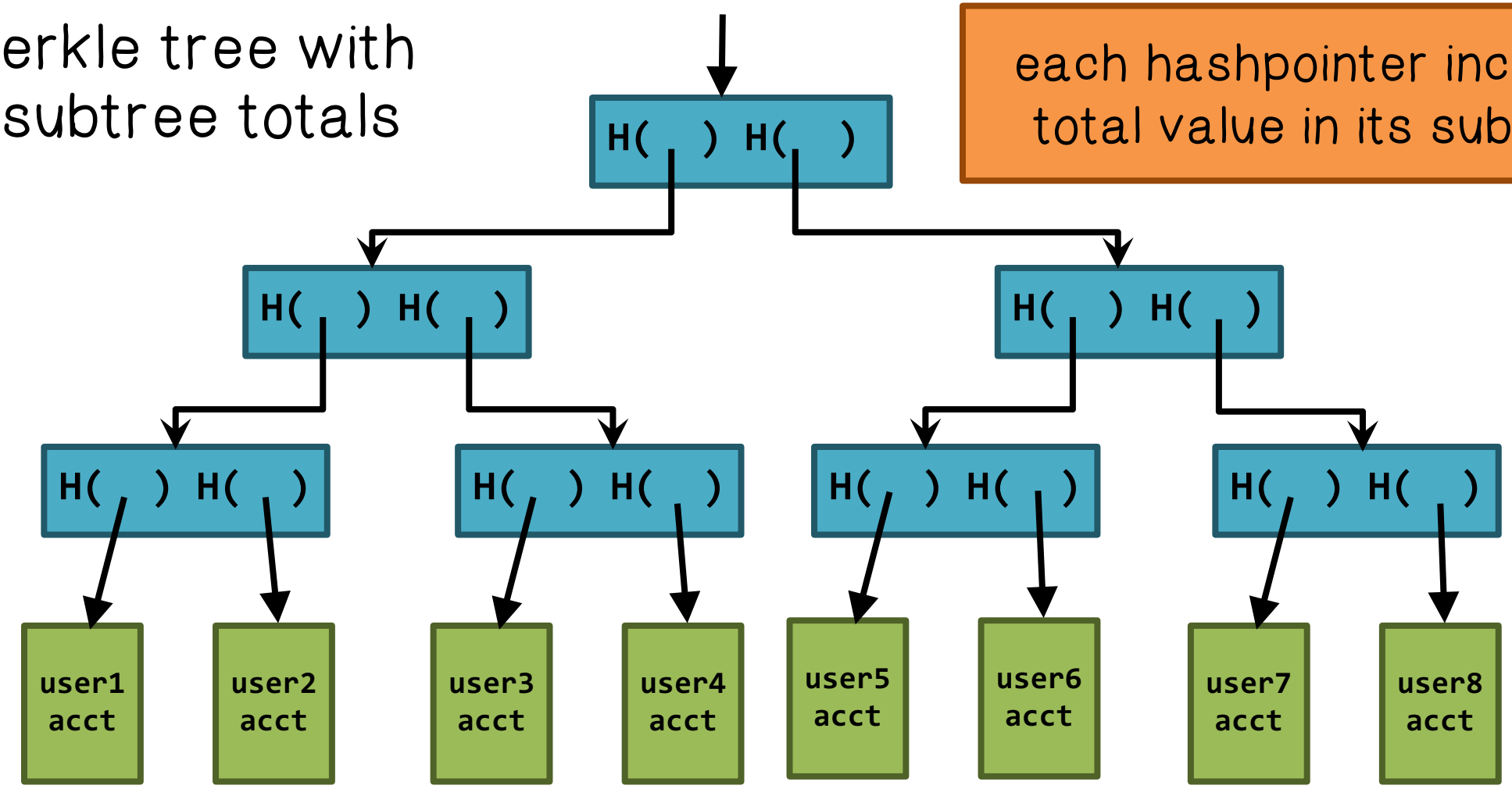


Simplified Bitcoin Block Chain

Merkle Trees

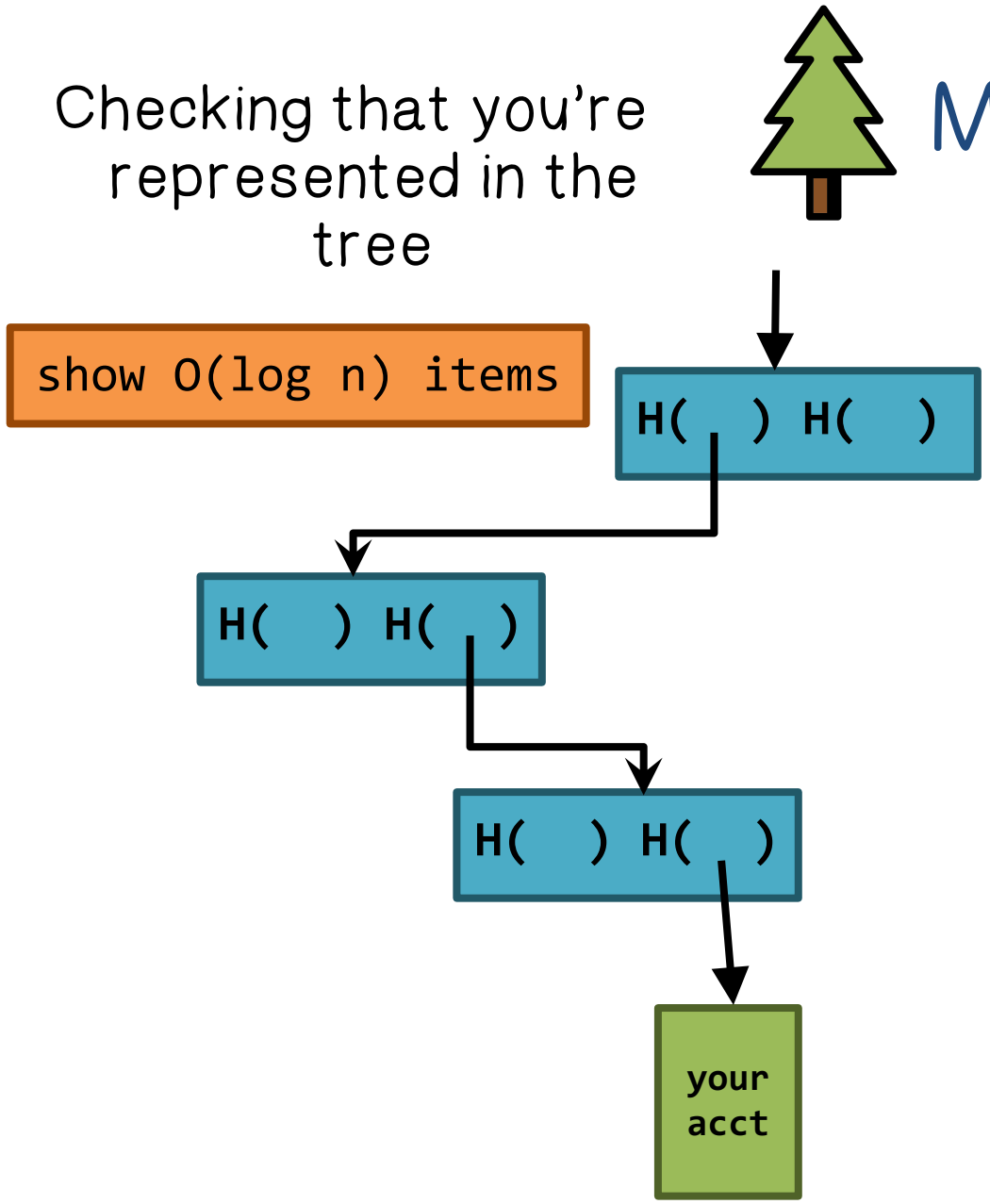
Merkle tree with subtree totals

each hashpointer includes total value in its subtree



Merkle Trees

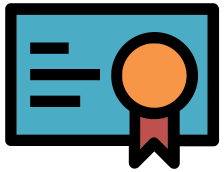
Checking that you're represented in the tree



Customer verifies:

1. Root hash pointer and root value == the signed and published root hash pointer and root value
2. Each hash value is indeed the cryptographic hash of the node it points to.
3. The leaf contains the correct user account info
4. Each value is the sum of the values of the two values beneath it.

If every customer checks …
Every branch will be explored!



Proof of Reserve

Prove that you have at least X amount of reserve currency

Prove that customers have at most Y amount deposited

So reserve fraction ≥ X / Y

No Central Regulator is Required

Anonymity

Some say Bitcoin provides anonymity

"Bitcoin is a secure and anonymous digital currency"

WikiLeaks donations page

Anonymity

Others say it doesn't

Wired UK

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

Anonymity

What do we mean by anonymity?

Literally: anonymous = without a name

Anonymity

What do we mean by anonymity?

Bitcoin addresses are public key hashes rather than real identities

Computer scientists call this pseudonymity

Anonymity in Computer Science

Anonymity = pseudonymity + unlinkability

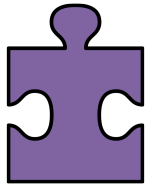
Different interactions of the same user with the system should not be linkable to each other

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



Bitcoin Anonymity Quiz

With regards to Bitcoins, check all the true statements:

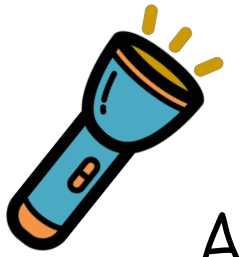
- [x] A time-stamping service prevents people from double spending Bitcoins.
- [ ] Each user has a single Bitcoin that is used in all transactions.
- [ ] The expenditure of individual coins cannot be tracked.

De-Anonymize Bitcoin

Trivial to create a new address

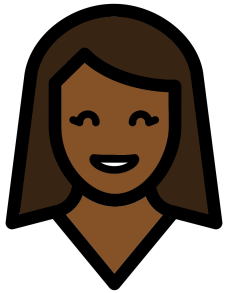
Best practice: always receive at fresh address

So, unlinkable?



De-Anonymize Bitcoin

Alice buys a teapot at Big box store



Alice

5

3

6

Single transaction

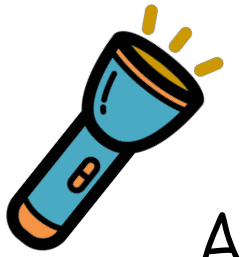
8

Two transactions... must be the same user.

De-Anonymize Bitcoin

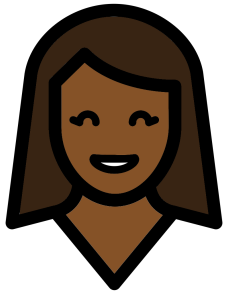
Linking addresses

- Shared spending is evidence of joint control
- Addresses can be linked transitively



De-Anonymize Bitcoin

Alice buys a teapot at Big box store



Alice

5

3

6

8.5

.5

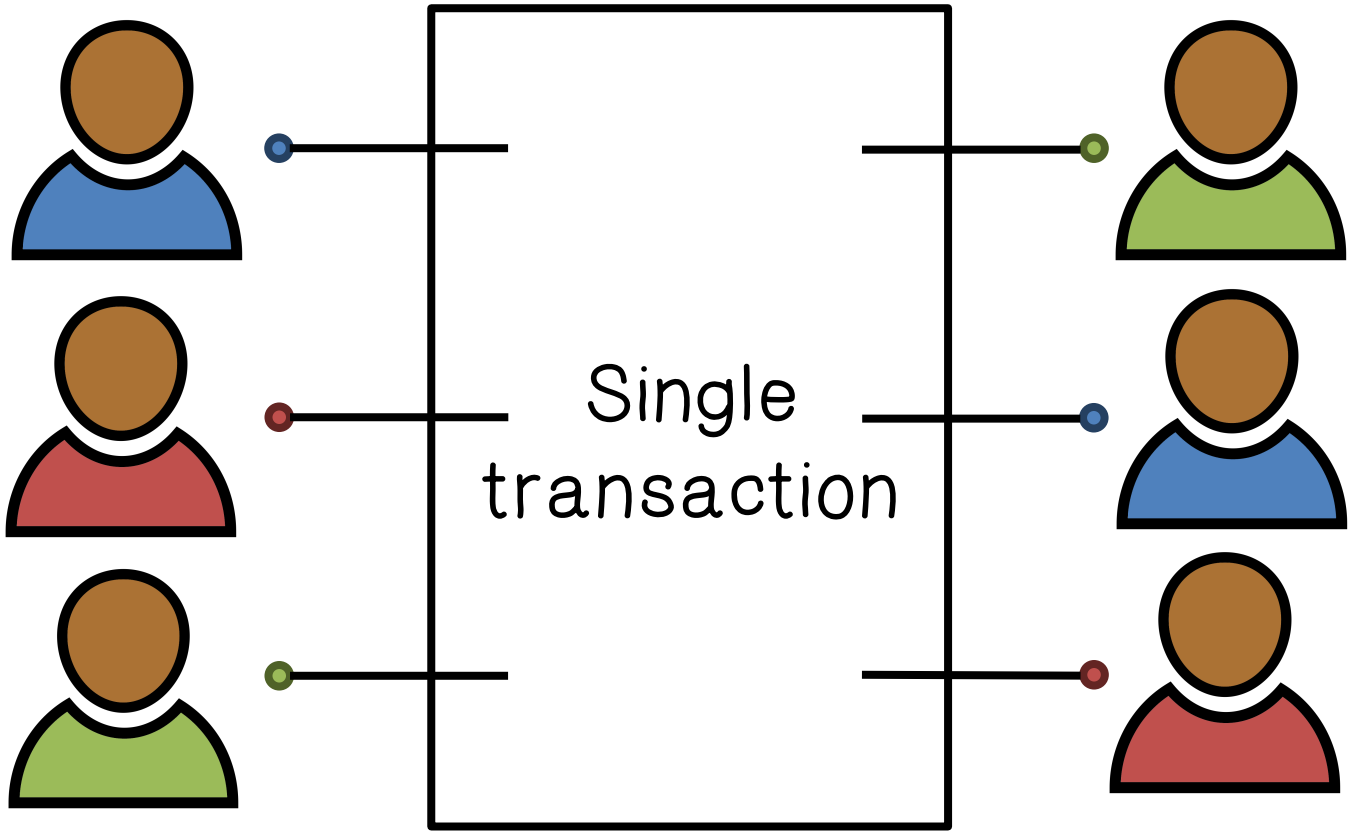
The output addresses belong to the same user!

De-Anonymize Bitcoin

Identifying Users

- High centralization in service providers
  - Most flows pass through one of these - in a traceable way
- Address - identity links in forums

Decentralized Mixing

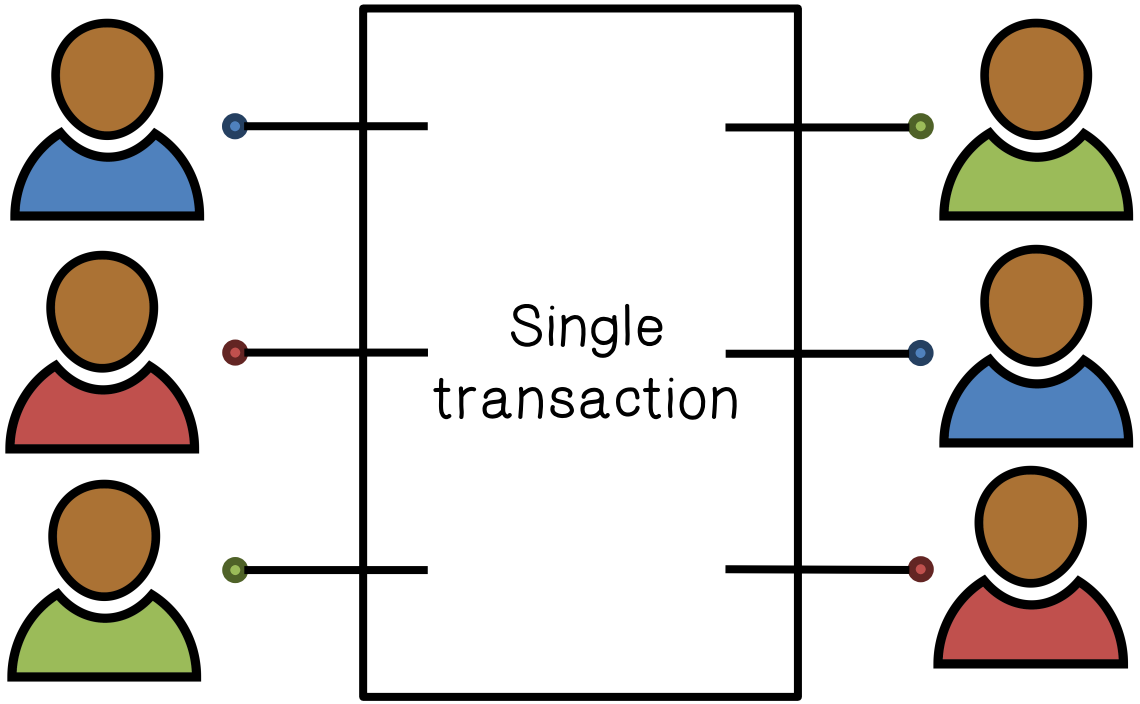


Each signature is entirely separate

Mixing principles apply on top of basic protocol

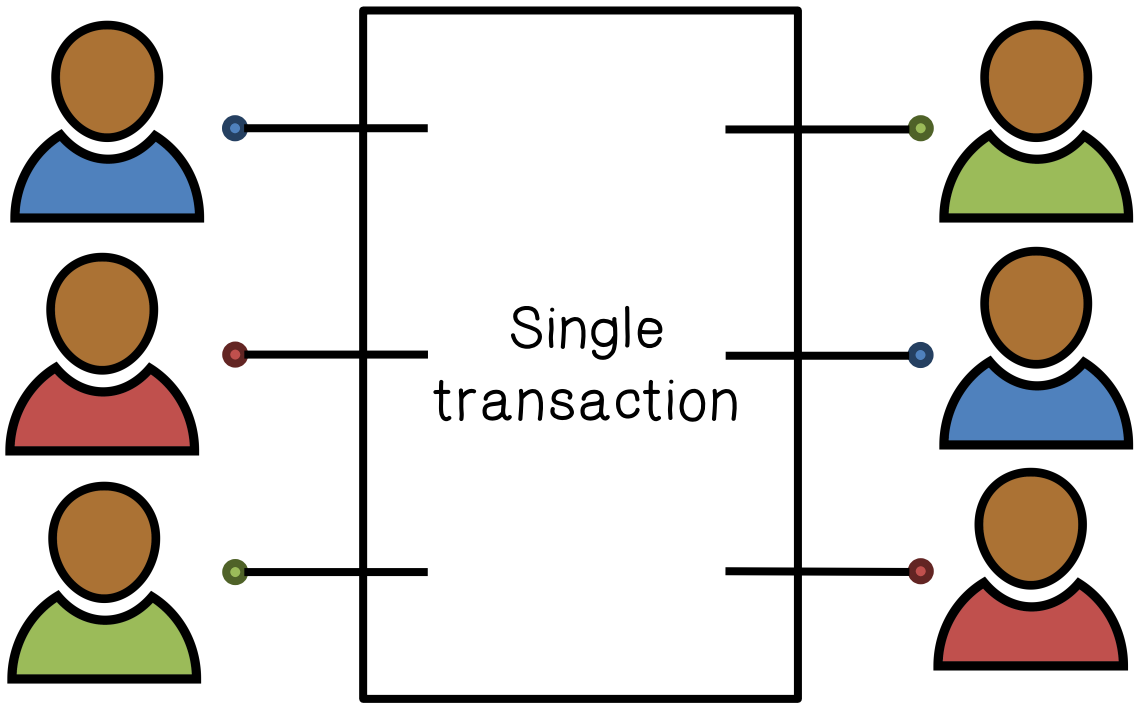
Proposed by Greg Maxwell, Bitcoin core developer

Decentralized Mixing

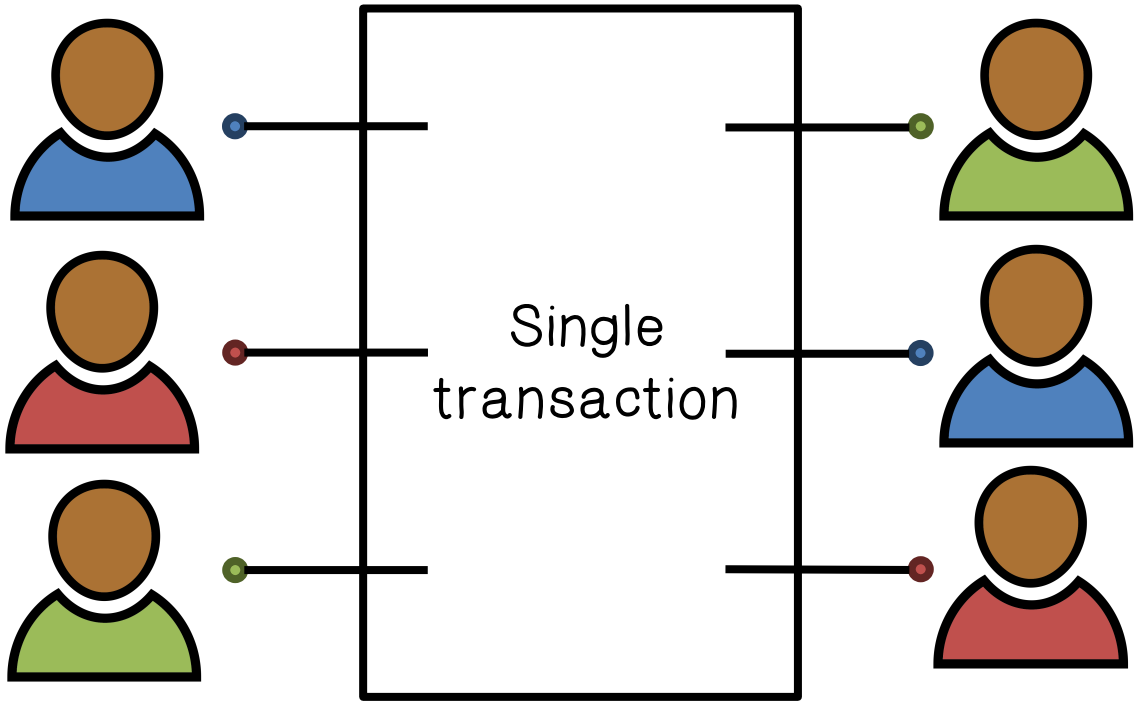


- Coins from a group of users are mixed with a single transaction.
- Each user provides an input and output address
- The order of the input and output is randomized.

Decentralized Mixing



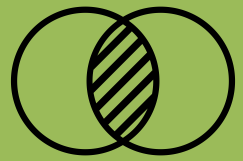
Decentralized Mixing



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

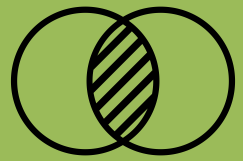
Decentralized Mixing



Coinjoin

Participants must exchange these addresses in such a way that even the other members of the peer group do not know the mapping between input and output addresses

Decentralized Mixing



Coinjoin

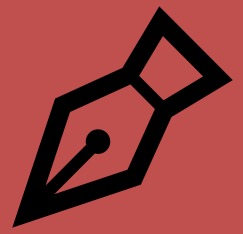
For unlinkable addresses:

- An anonymous communication protocol is necessary
- It is not necessary to communicate outputs securely

Bitcoin Append Only Log

Secure Timestamping

Goal: Prove knowledge of x at time t If desired, without revealing x at time t



Evidence should be permanent

Bitcoin Append Only Log

Hash Commitments

Recall: Publishing H(x) is a commitment to x

- Can't find an x'≠x later s.t. H(x') = H(x)
- H(x) reveal no information* about x

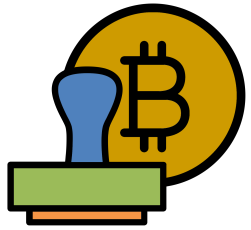
*assuming the space of possible x is big

Can publish a commitment to x, reveal later

Timestamping

Secure timestamping applications

- Proof of knowledge
- Proof of receipt
- Hash-based signature schemes
- Many, many more…



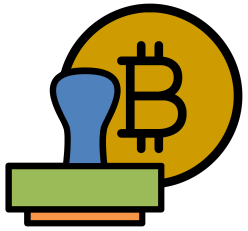
Timestamping in Bitcoin

Simplest Solution:

- Send money to the hash of your data
- Burns the coins, making them unspendable

Pros:
Compatible, easy

Cons:
creates unspendable UTXO forever

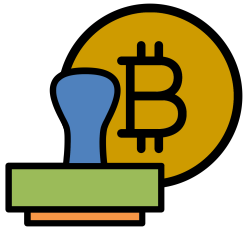


Timestamping in Bitcoin: CommitCoin

Encode data into the private key

ECDSA can leak your private key

- Good source of randomness is essential



Timestamping in Bitcoin: CommitCoin

Generate a new private key that encodes commitment

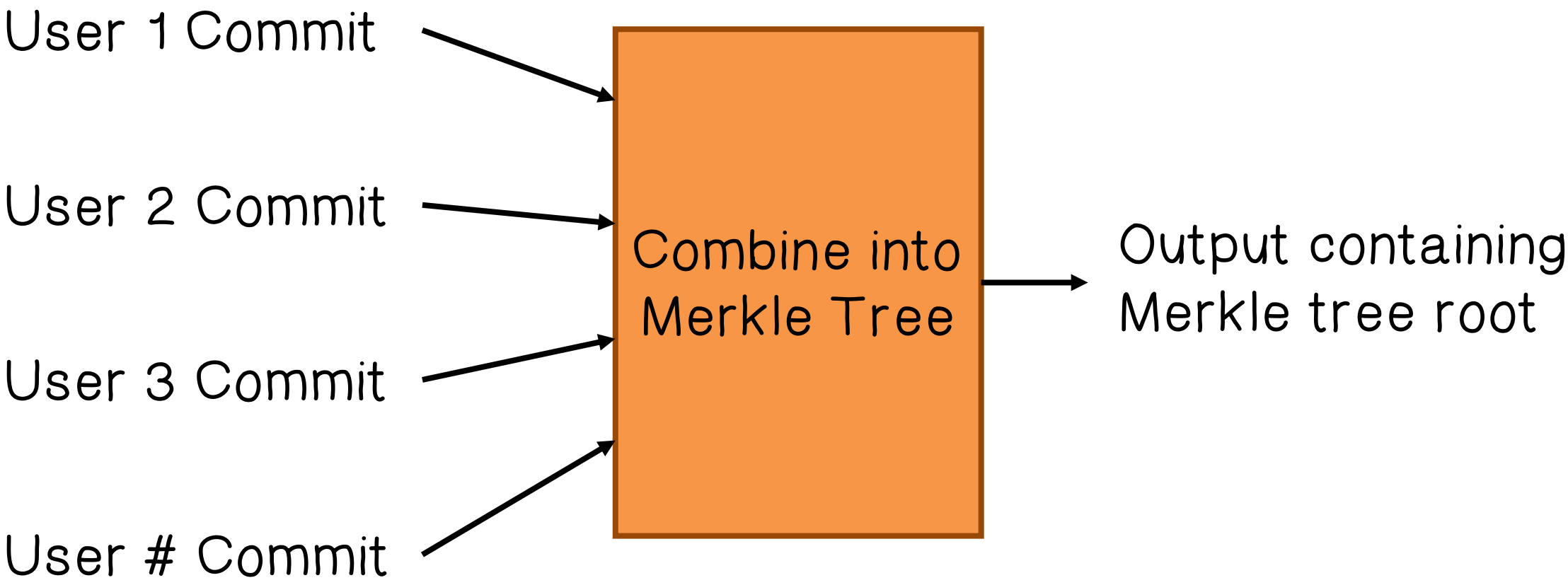
CommitCoin:

- avoids the need to burn coins
- is very complex

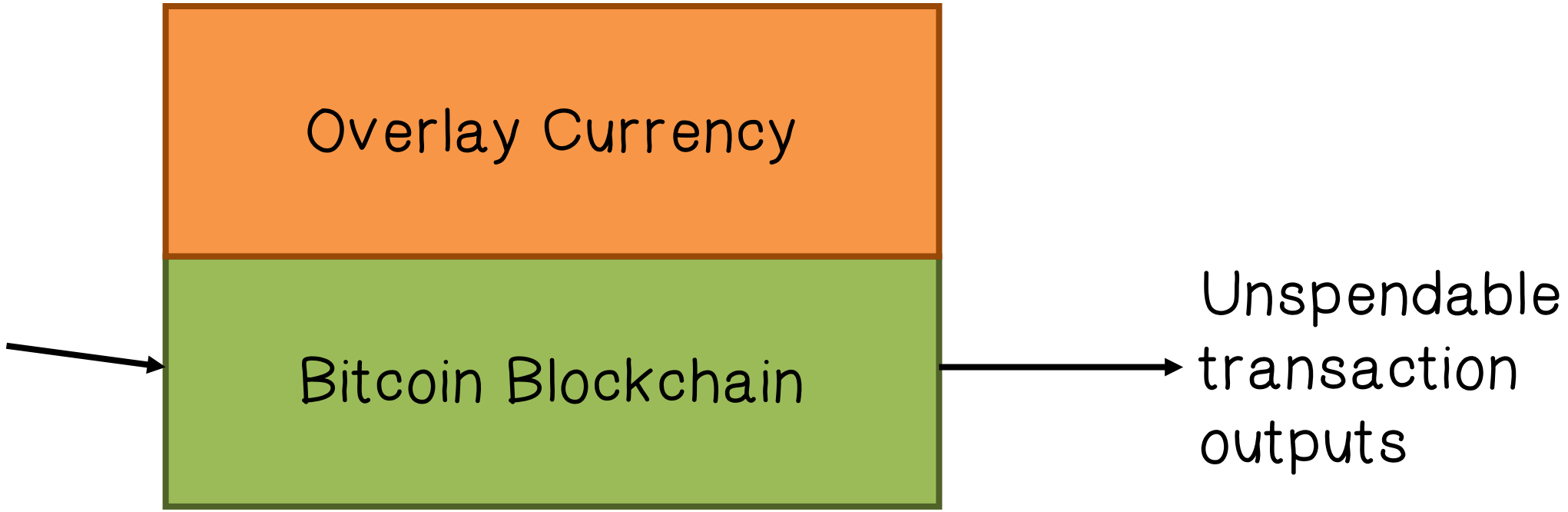
Provable Unspendable Commitments

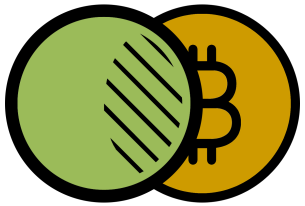
OP_RETURN
<arbitrary data>

Provable Unspendable Commitments



Overlay Currencies





Overlay Currencies

Miners don't validate what you are writing into the block chain

Anyone can write as long as the transaction fee is paid

Need more complicated logic for validating transactions

This logic must reside in each end-user client that participates in sending or receiving overlay currency

Mastercoin

Pros:

- Can develop smart contracts, user defined currencies, etc.

Cons:

- Still dependent on Bitcoin
- Inefficient, overlay currency may need to process a lot of data