Blockchain Privacy

Fungibility

?
==

Fungibility

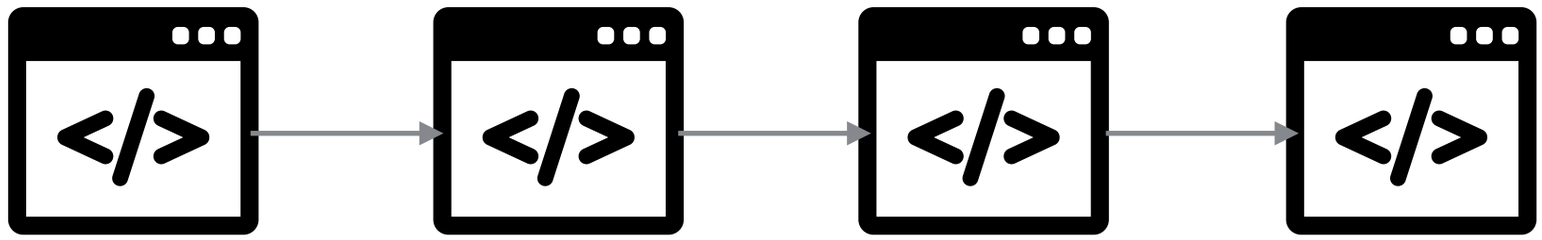
?

==

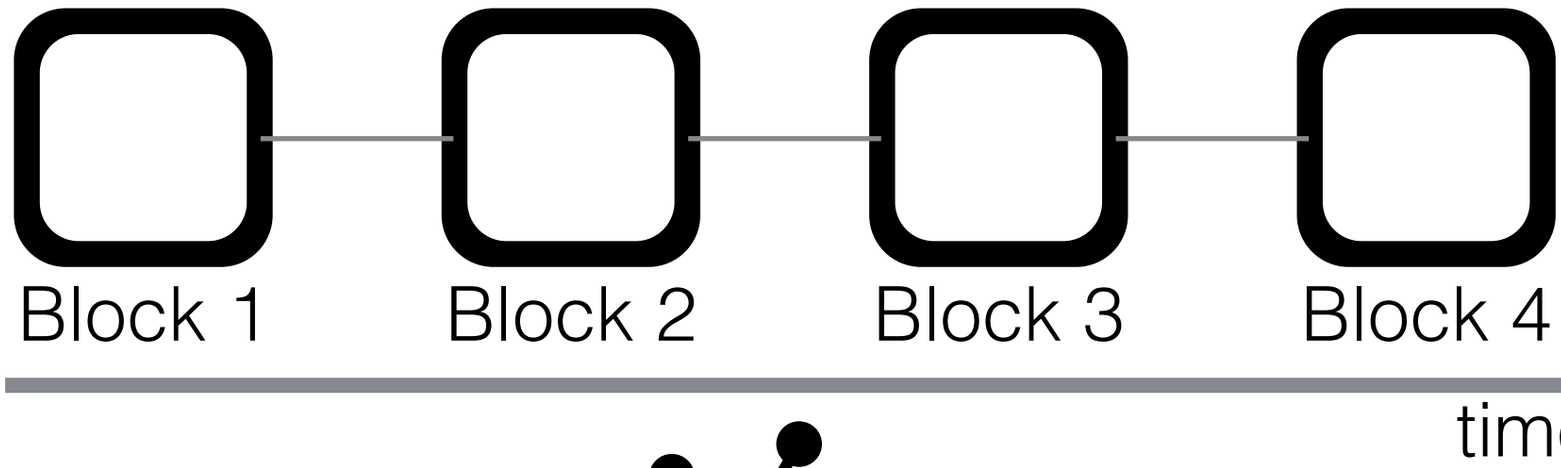
Is 1 Bitcoin always worth 1 Bitcoin?

Blockchain Privacy is a Multilayer Challenge

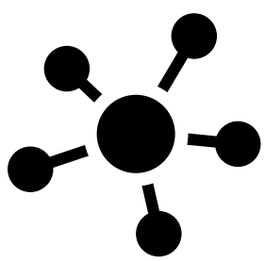
Application Layer 2



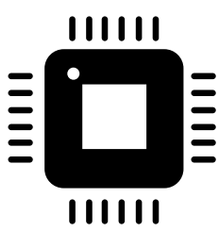
Blockchain Layer 1



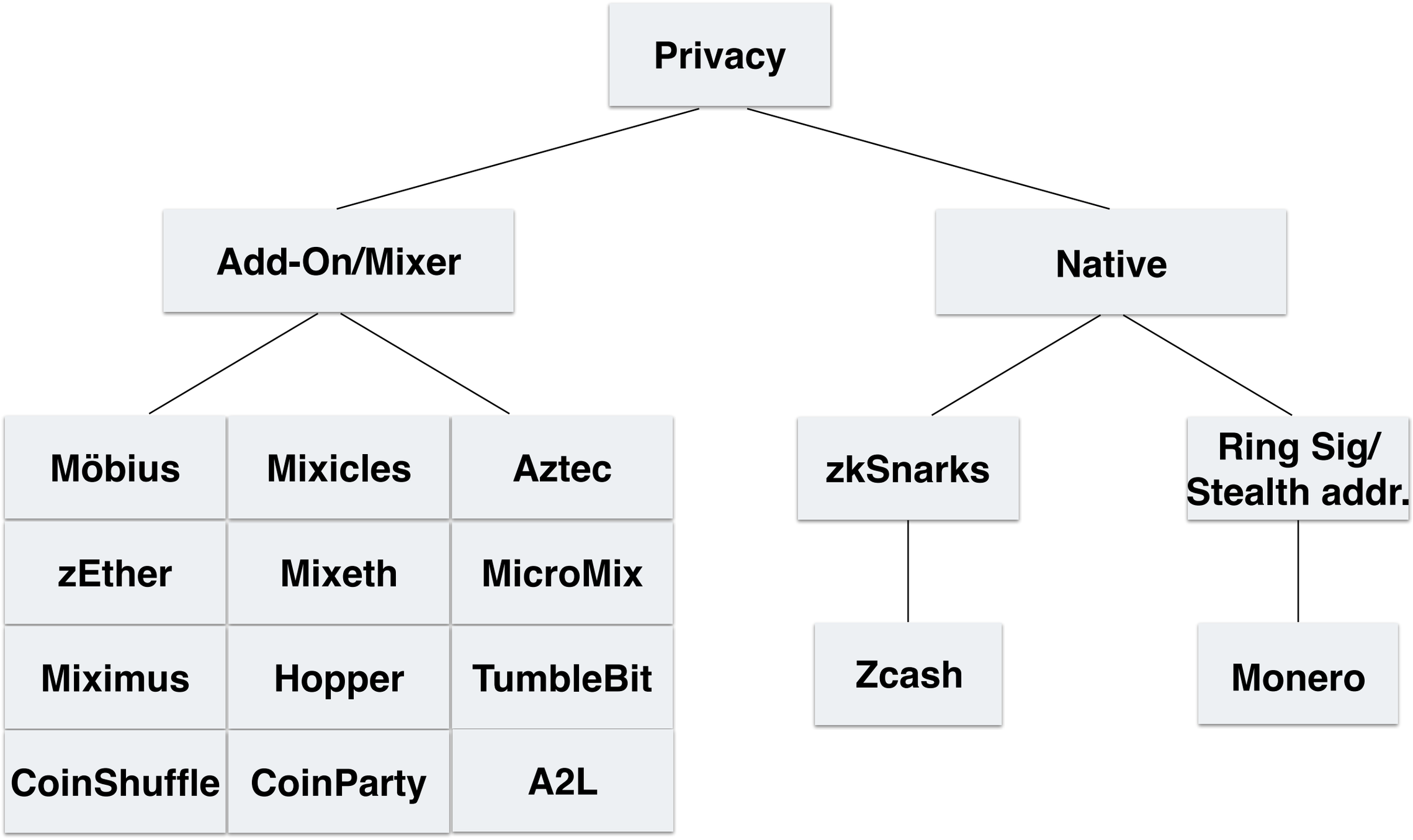
Network Layer 0



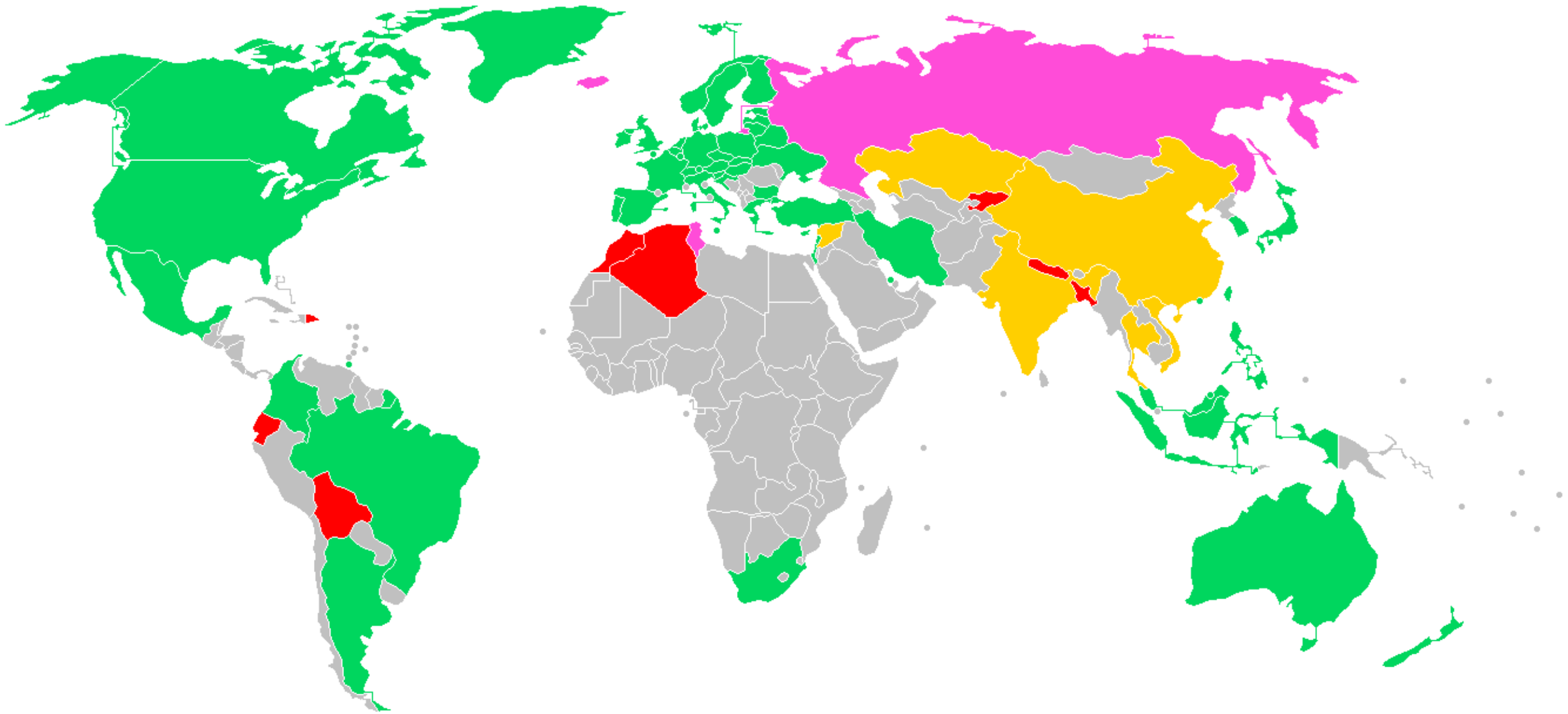
Hardware Layer



Blockchain Privacy Solutions



Blockchain Privacy Ethical Concerns



Money Laundering

- Anonymous cash could be used for *criminal purposes*

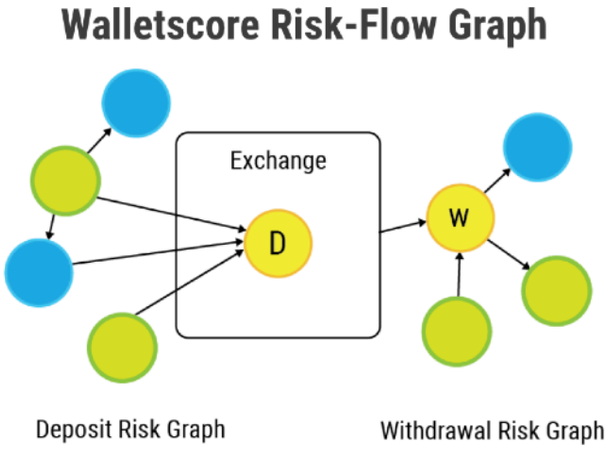
- ZCash enables “selective disclosure”
  -> For tax and AML purposes

- Tornado Cash has a “compliance tool”

(Breaking) Privacy is a Business

- Governments
- Secret Services
- Police

Want to know what the bad guys are up to..



CHAINALYSIS

ELLIPTIC

WHAT WE DO WHO WE HELP ABOUT ELLIPTIC ANALYSIS

Detect And Prevent Criminal Activity In Cryptocurrency.

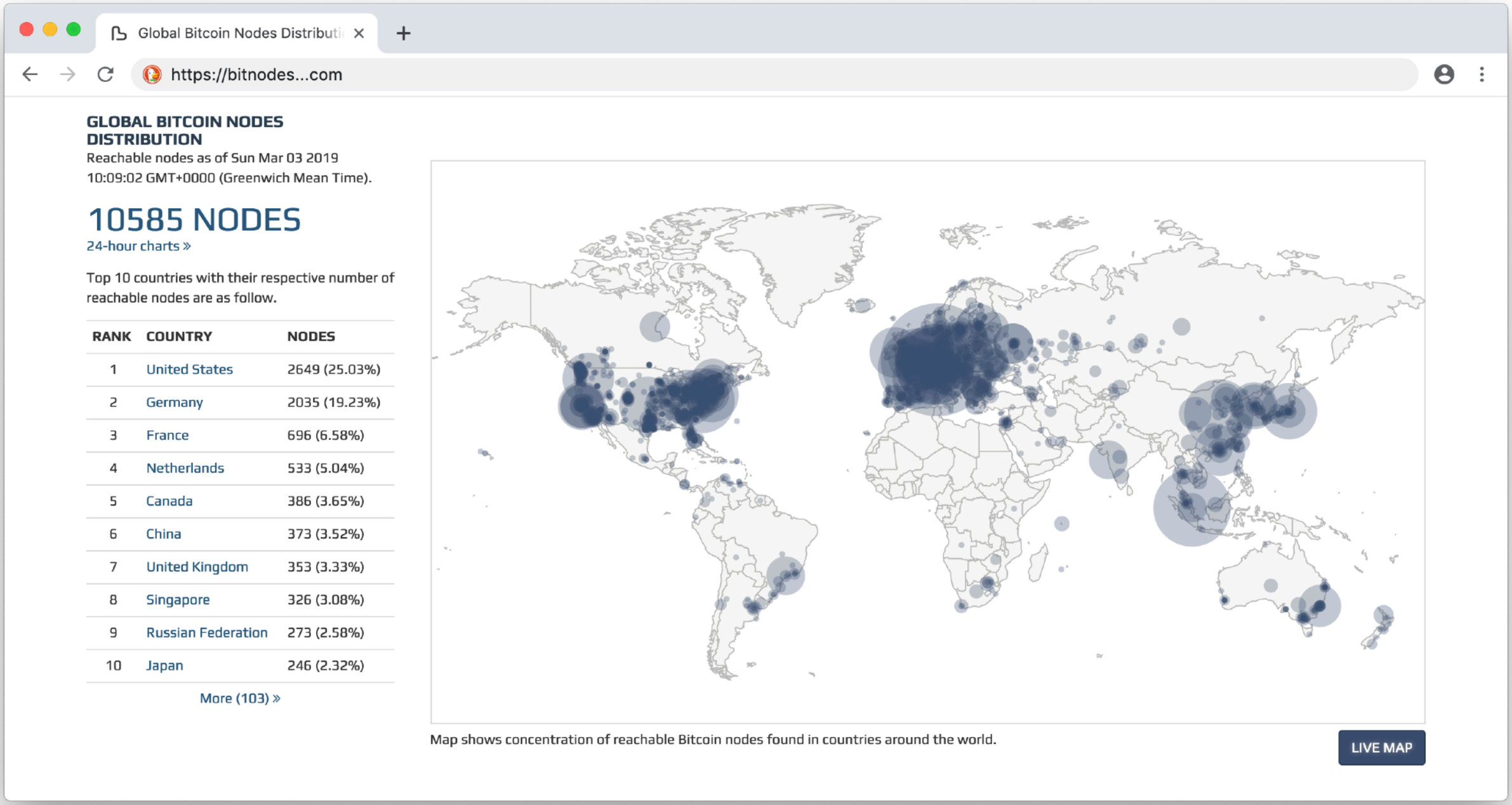
BLOCKTRACE

Blockchain Forensic and Analytical Services

Blockchain Privacy Network Layer

Peer to Peer Network

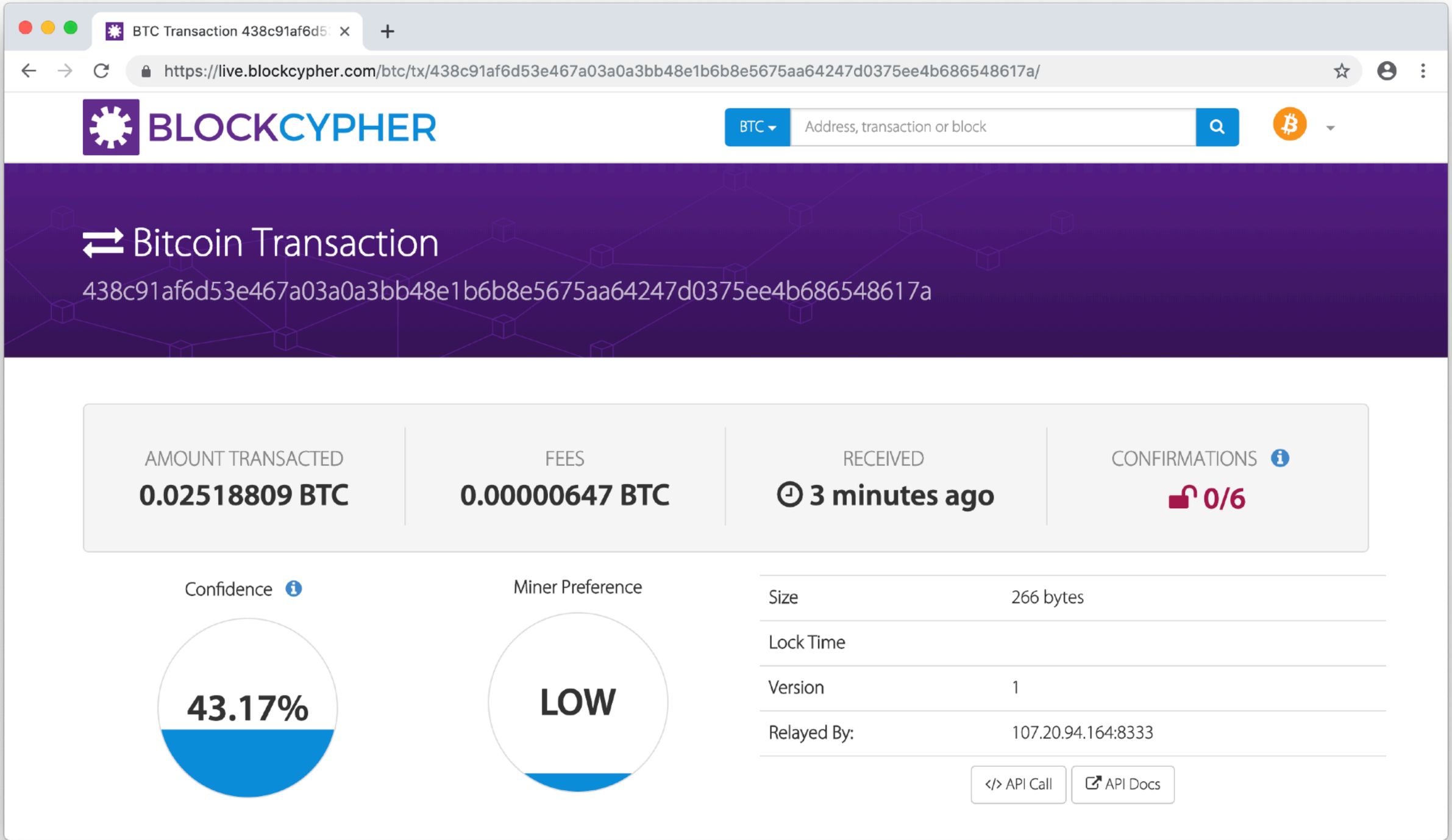
- Loosely connected network
- Validating nodes / Lightweight clients / Miner



Network Privacy Leakages

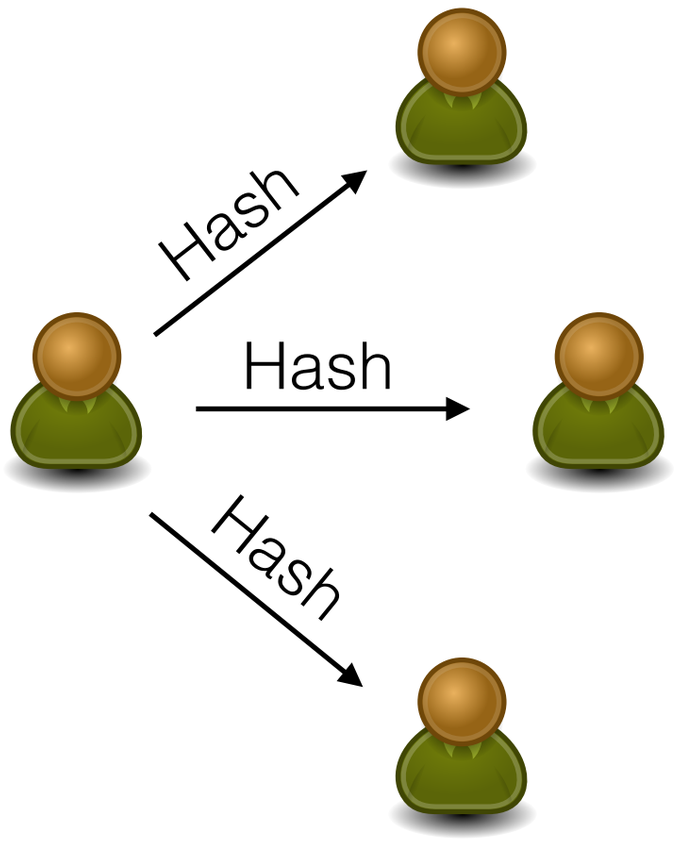
- IP addresses of other nodes
- Client version -> Fingerprinting
- Port scans can reveal operating system
- Which transactions are forwarded?
- I see a transaction first from you, are you the originator?

Network Privacy Leakages



Remember?

1. Transaction/Block hash broadcast



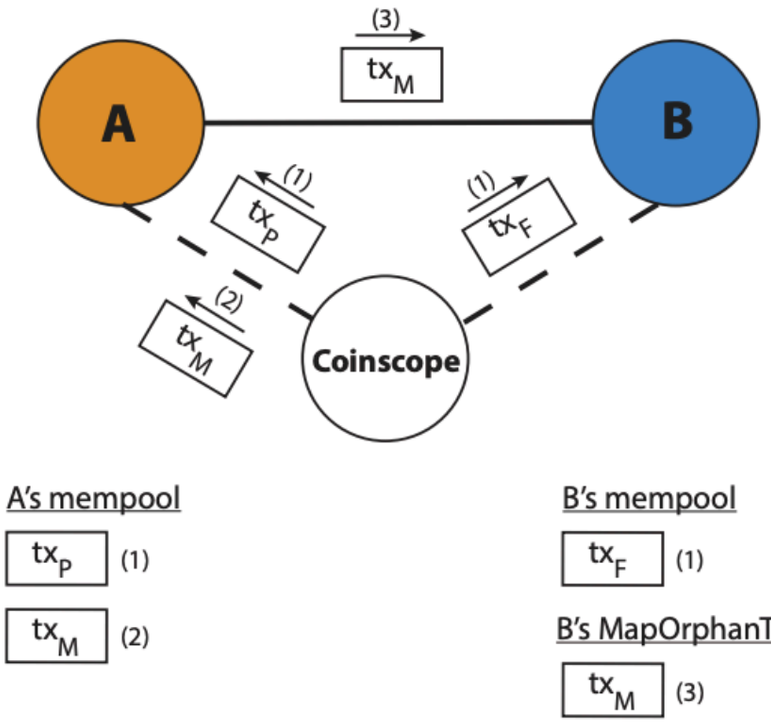
Broadcast

2. Transaction/Block request

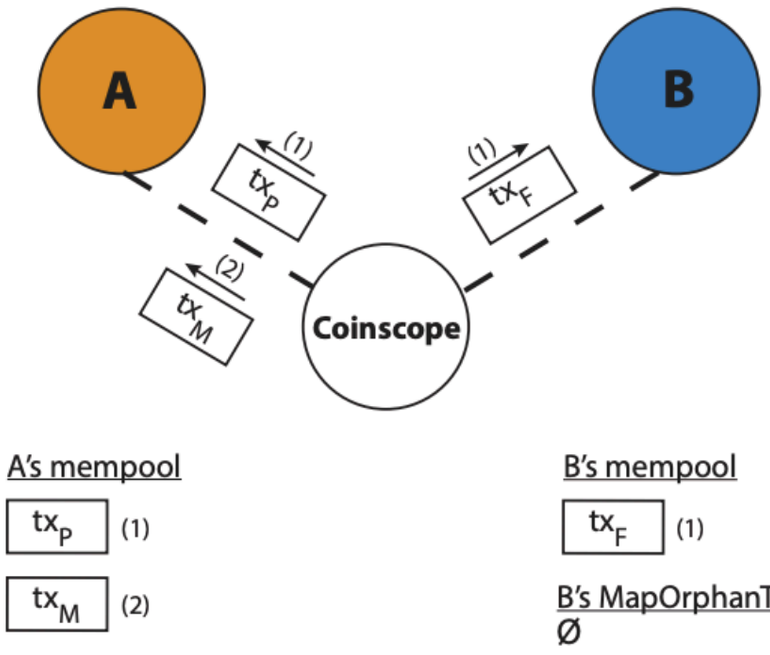
TCP/IP

Port 8333

TxProbe



(a) Basic positive edge inferring technique between two nodes.

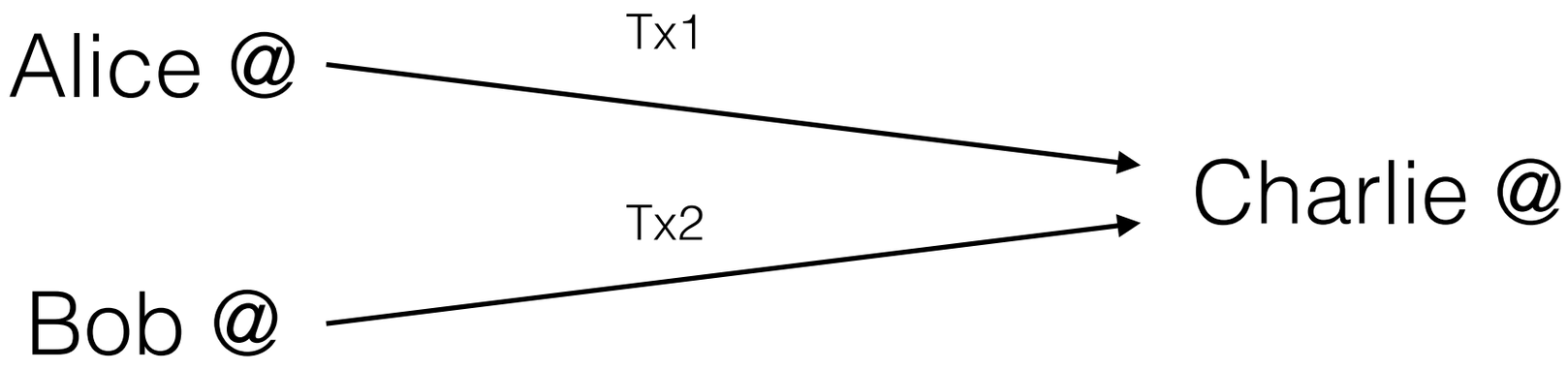


(b) Basic negative edge inferring technique between two nodes.

https://arxiv.org/pdf/1812.00942.pdf

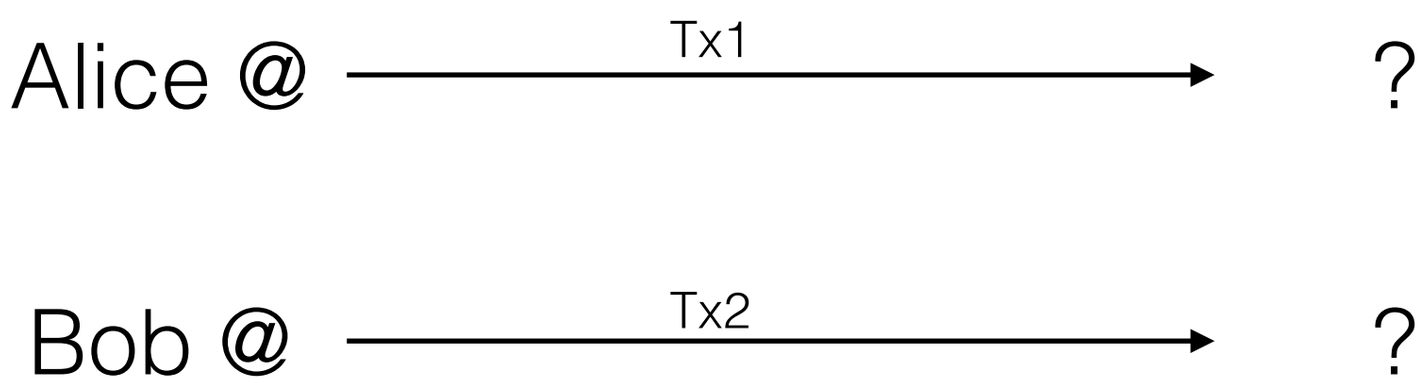
Blockchain Privacy
Privacy on the Transaction Layer

Linkability



Everybody sees the transactions go to the **same** recipient.

Unlinkability

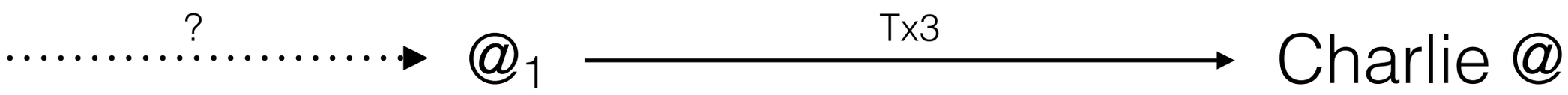


No idea where they go.

Traceability

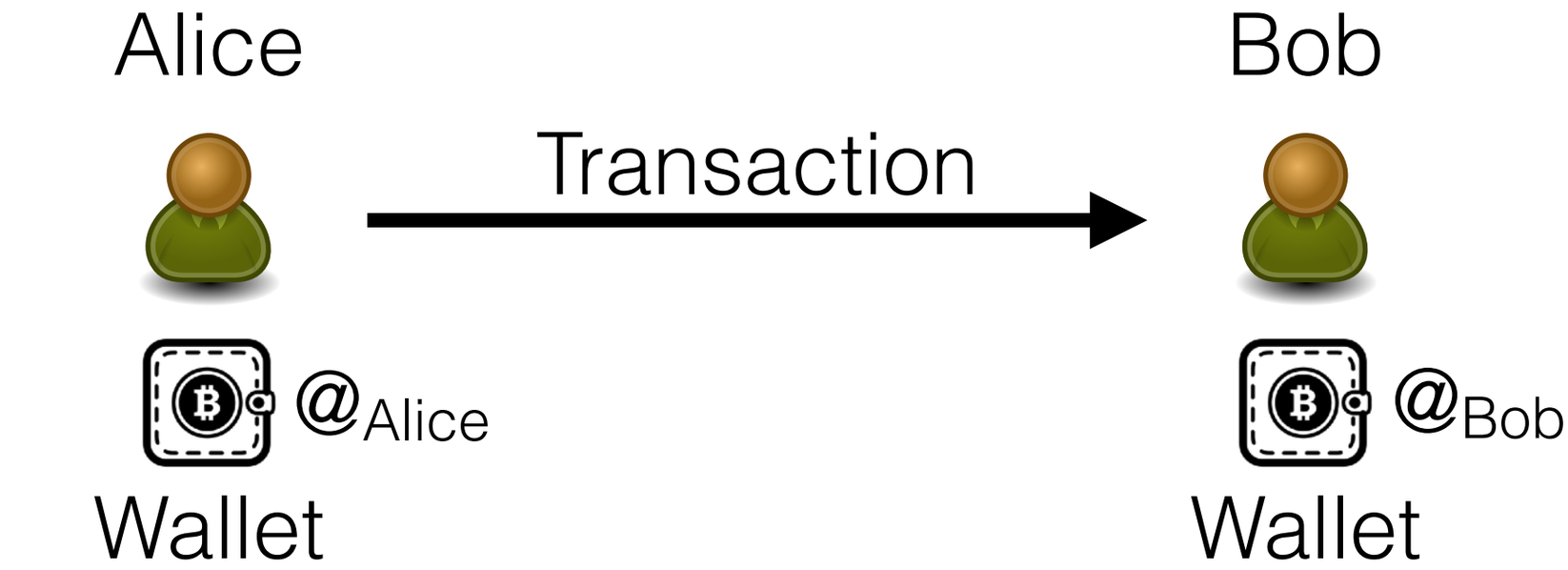
Tx3 spends funds received in Tx1 and Tx2.

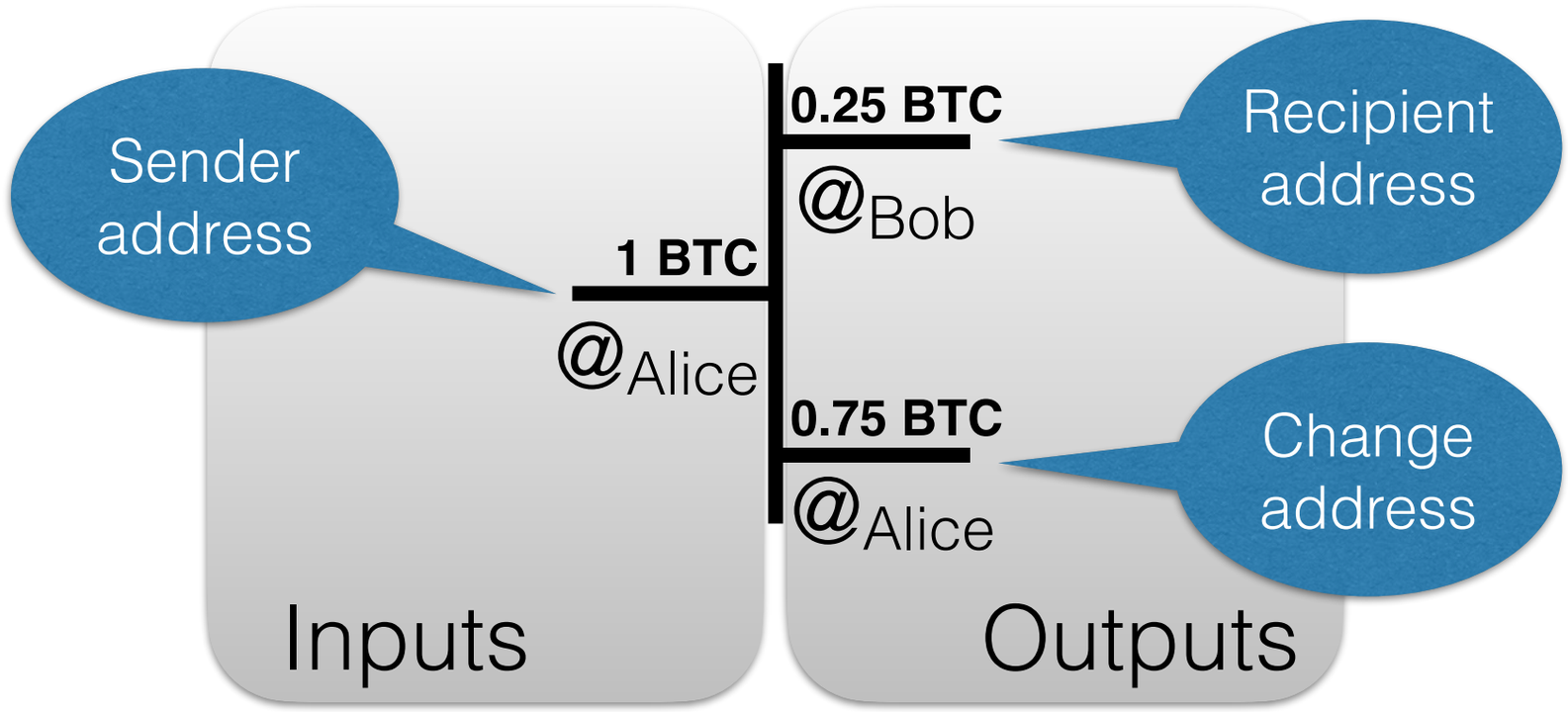
Untraceability



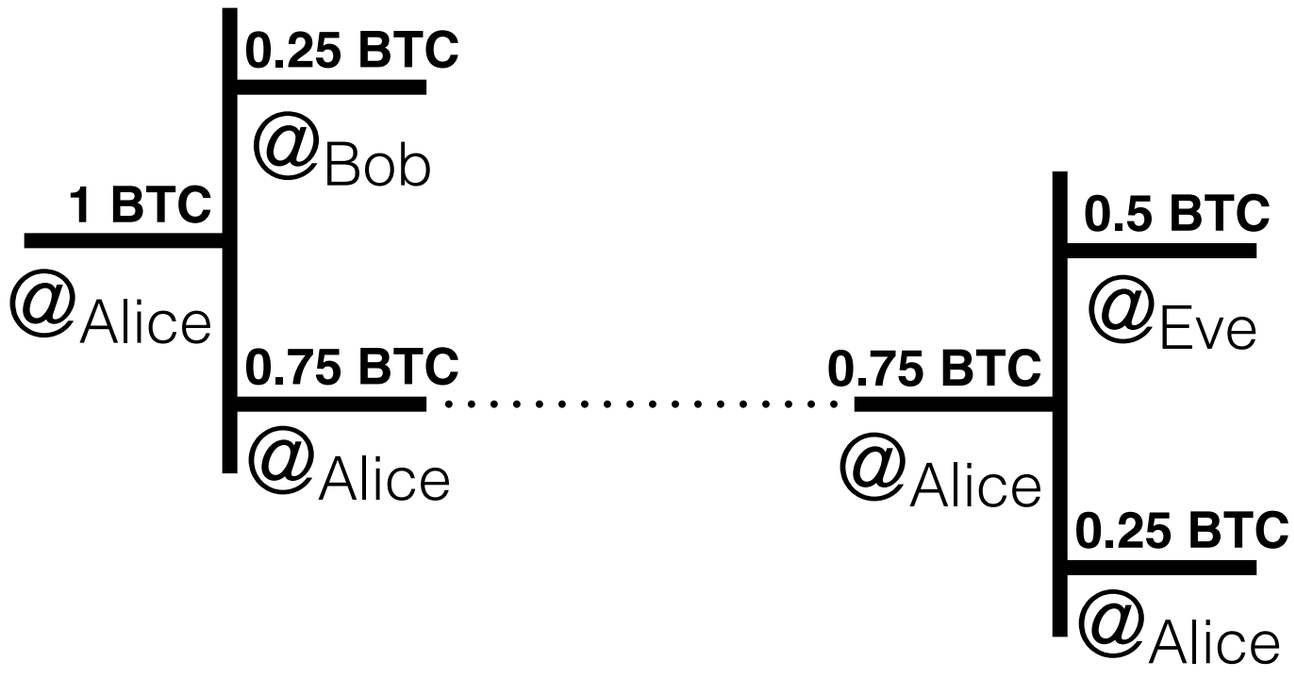
No idea where the funds from Tx3 come from.

Transactions in Bitcoin (UTXO model)





Transactions in Bitcoin

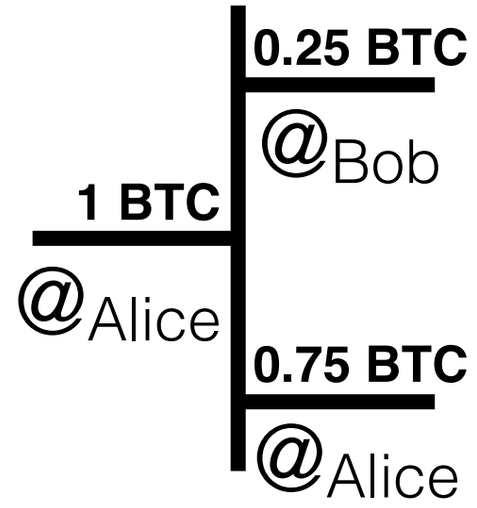


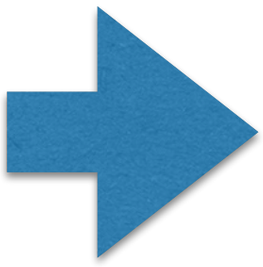
Transaction 1 Transaction 2

Heuristics to Cluster Bitcoin Addresses

- **Change Address**
  If new, then likely a change address

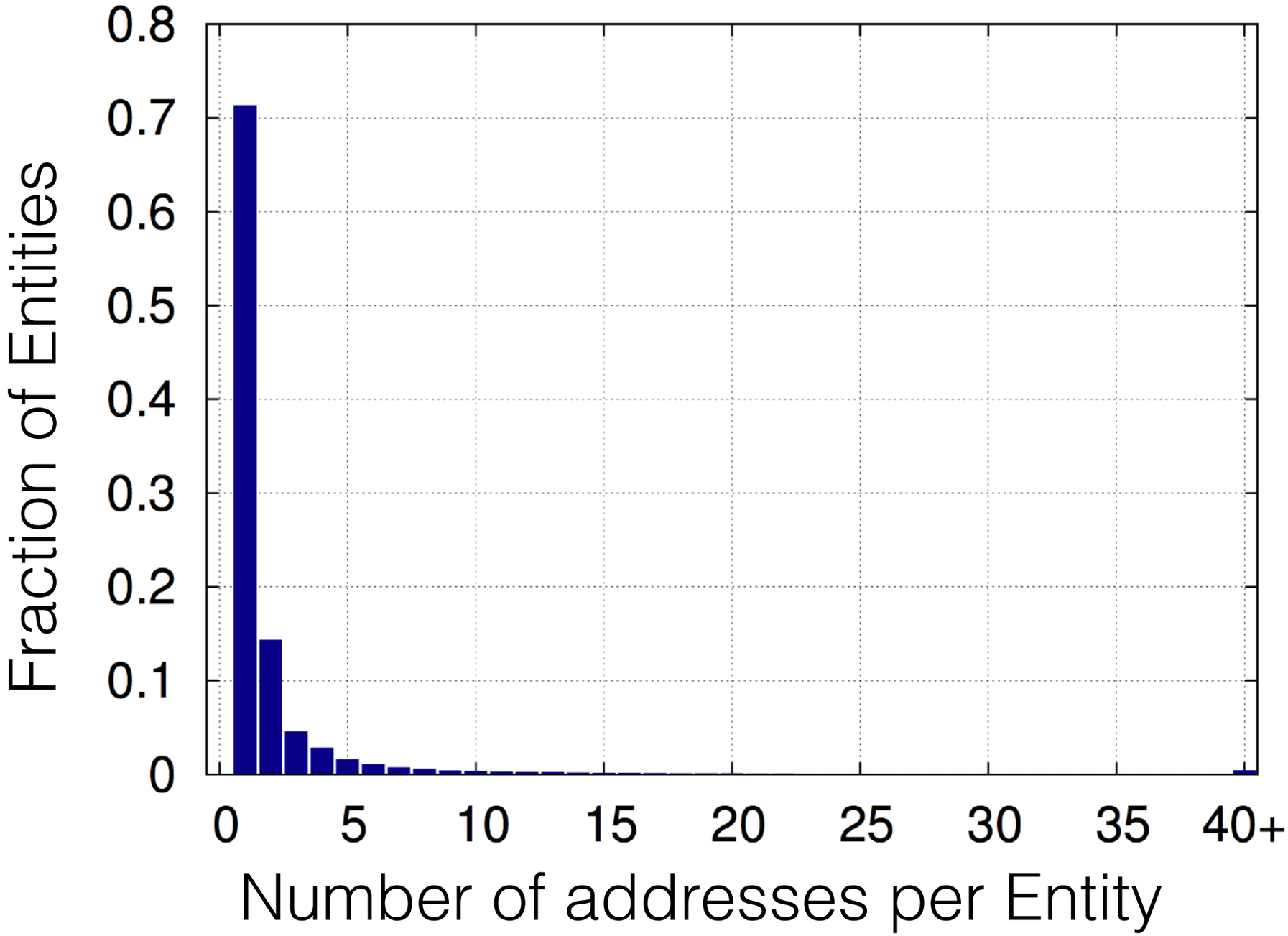
- **Multi-input Transactions**
  All inputs can be signed by the same entity.





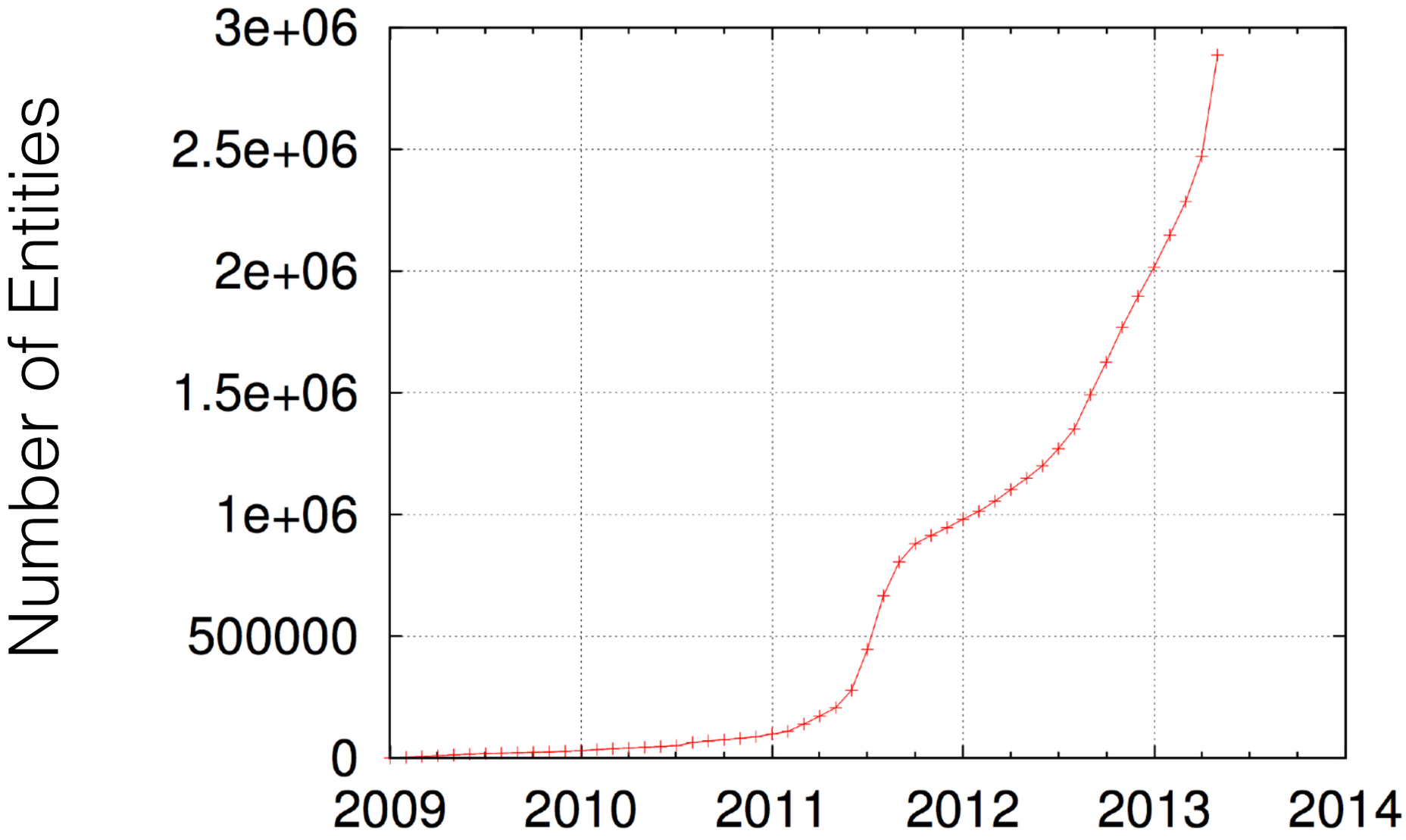
Possible to cluster addresses into cluster that might represent entities

Entity Cluster

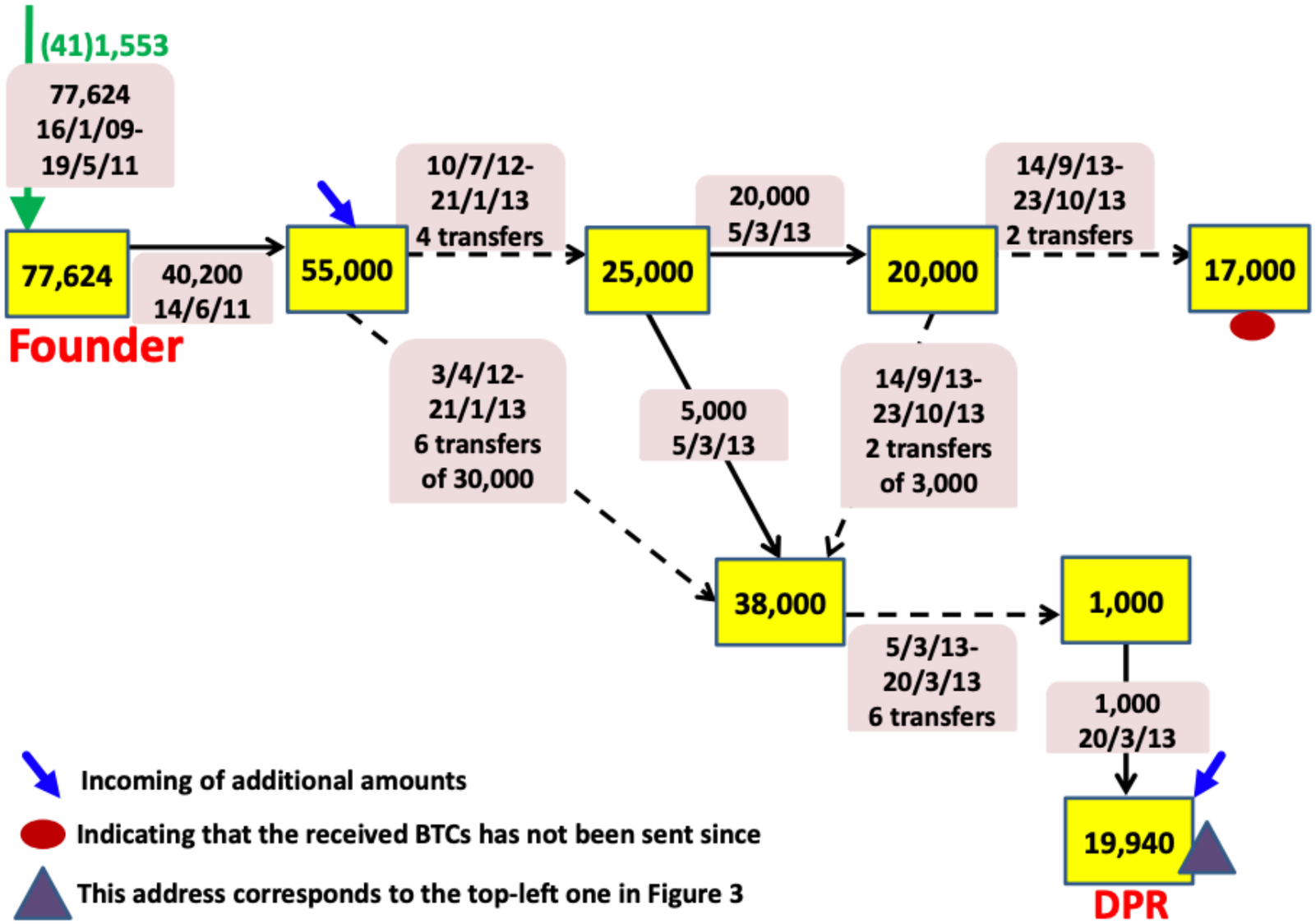


https://github.com/znort987/blockparser

Entity Evolution over Time



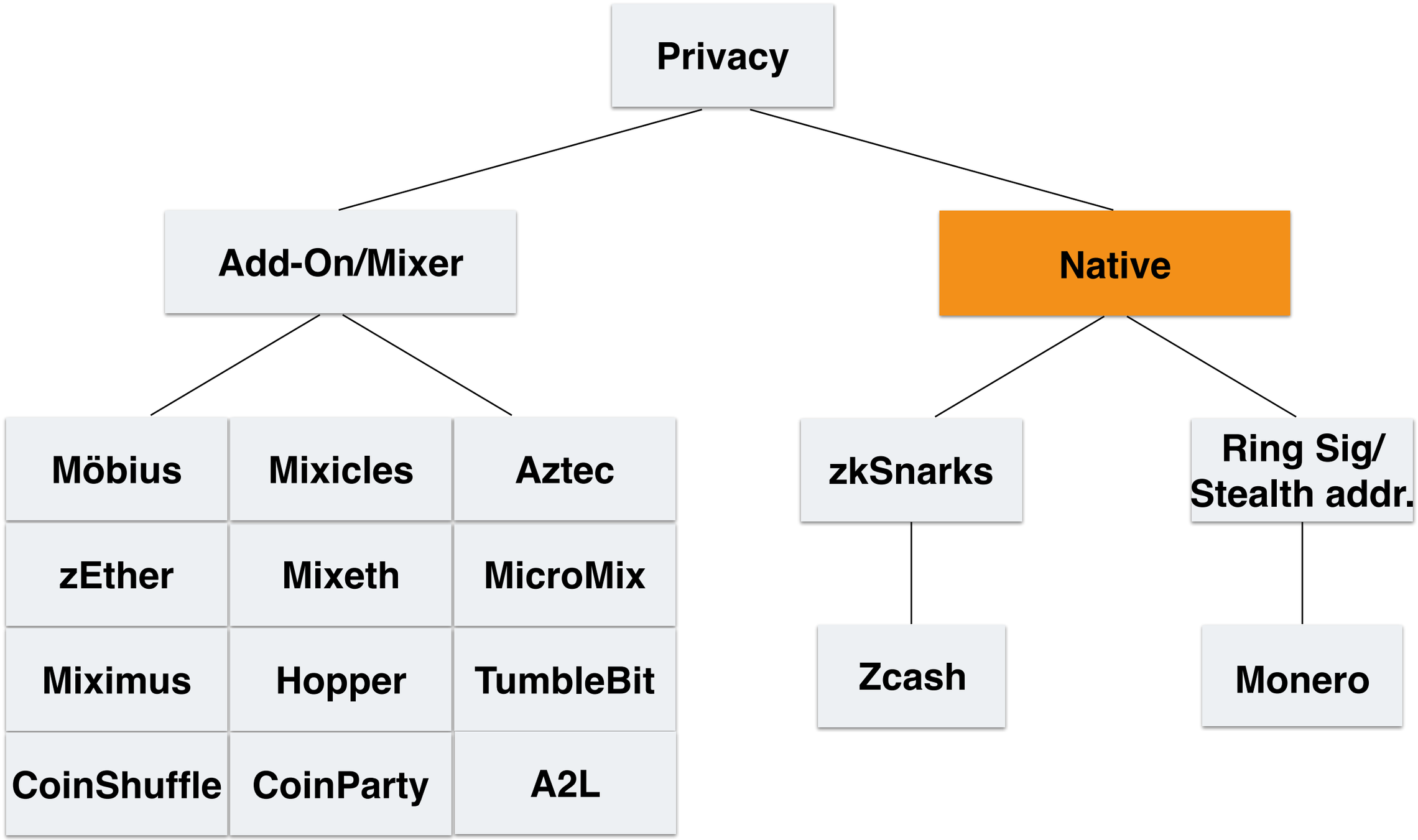
Easy to trace?



Published by FBI
After seizing Silk Road server


Blockchain Privacy
Native Privacy Blockchain

Blockchain Privacy Solutions



Privacy Preserving Blockchains - Different Approaches

Decoy of k-anonymity Privacy

- Monero, CoinJoin

N-anonymity Privacy

- ZCash

ZCash

- Bitcoin Fork

- Privacy Features:
  - Transparent Transactions (t-addr)
  - Shielded Transactions (z-addr)

- z-addr Transactions
  - # coins entering
  - # coins exiting
  - ZKP that the transaction is valid

	Shielding	**De-shielding**	**Shielded**
Source	t-addr	z-addr	z-addr
Destination	z-addr	t-addr	z-addr
Amount	Public	Public	Private

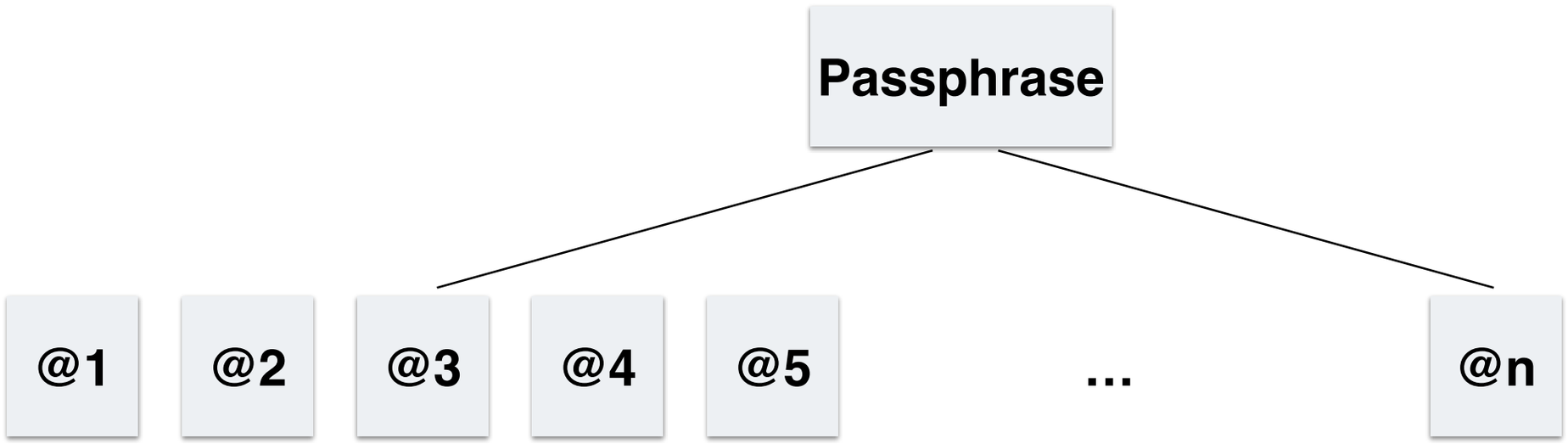
- zkSNARK
  - Non-interactive, Succinct proofs of knowledge
  - Requires trusted setup

Monero Privacy Features

- Unlinkability (destination): Stealth Addresses
- Untraceability (source): Ring Signatures/RingCT

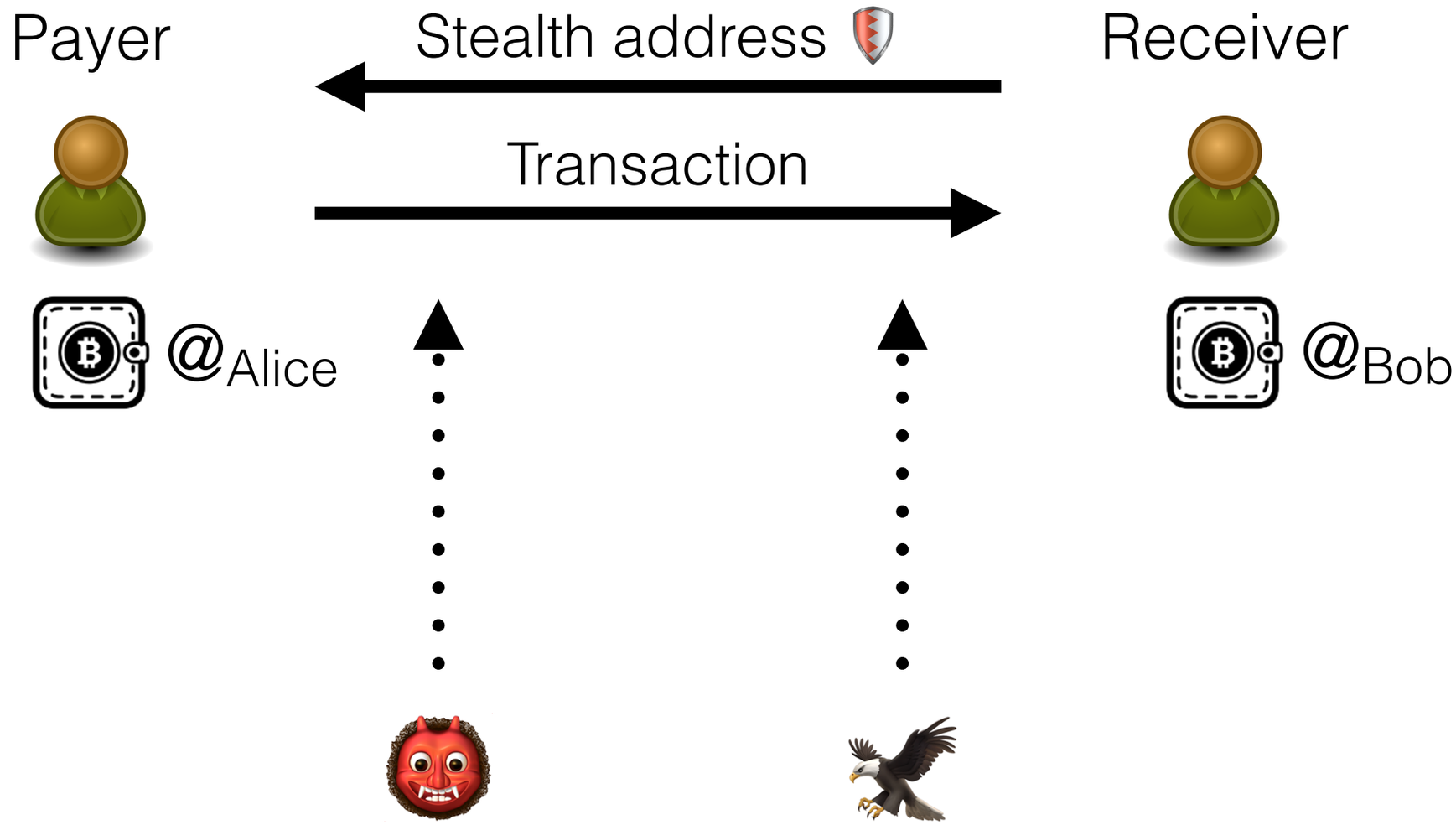
Blockchain Privacy
Stealth Addresses

Hierarchical Deterministic (HD) Wallets



- Addresses derived from the same key
- From one address cannot derive the other addresses
- Used by the majority of Bitcoin/Ethereum wallets today
- A form of stealth addresses

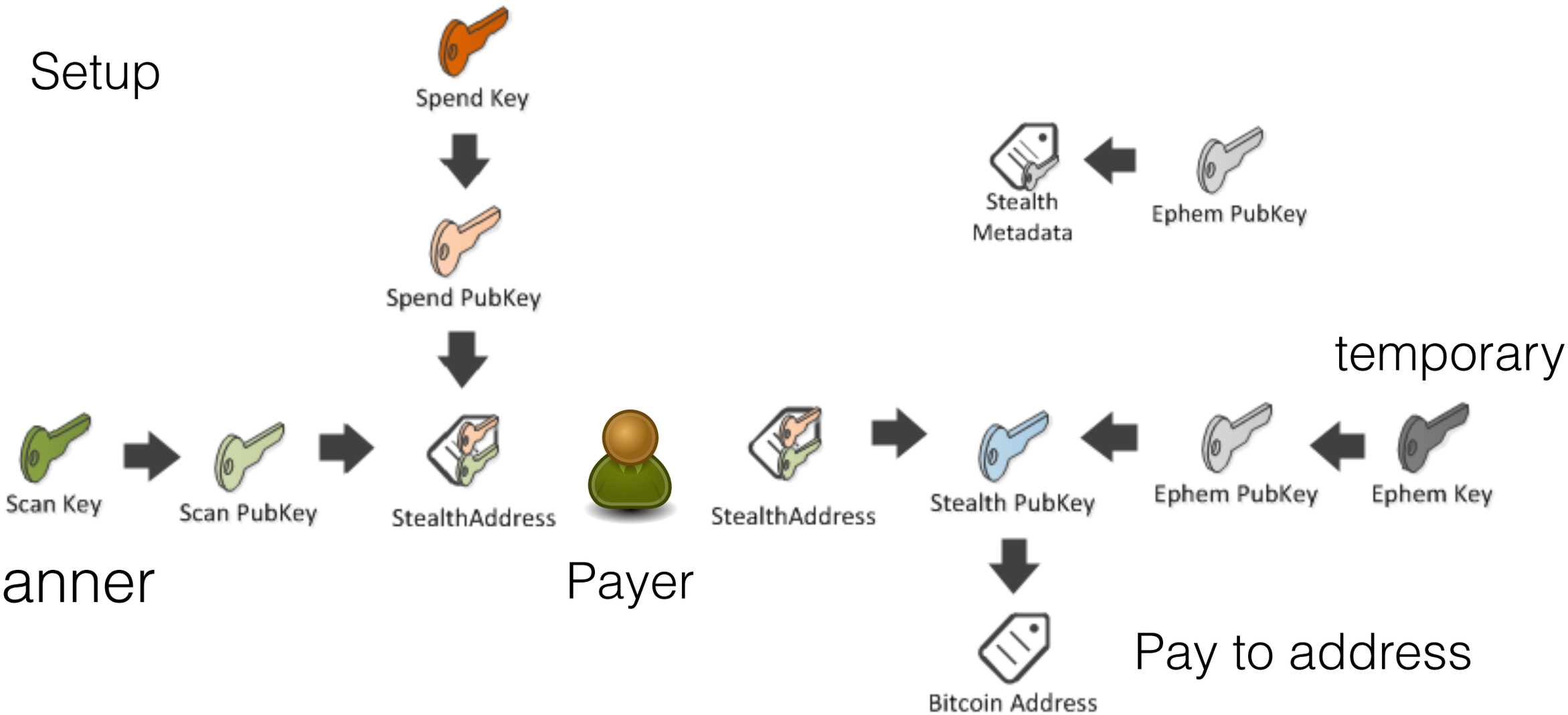
Stealth Addresses



Stealth Addresses - Paying (Dark Wallet)

Receiver

Setup

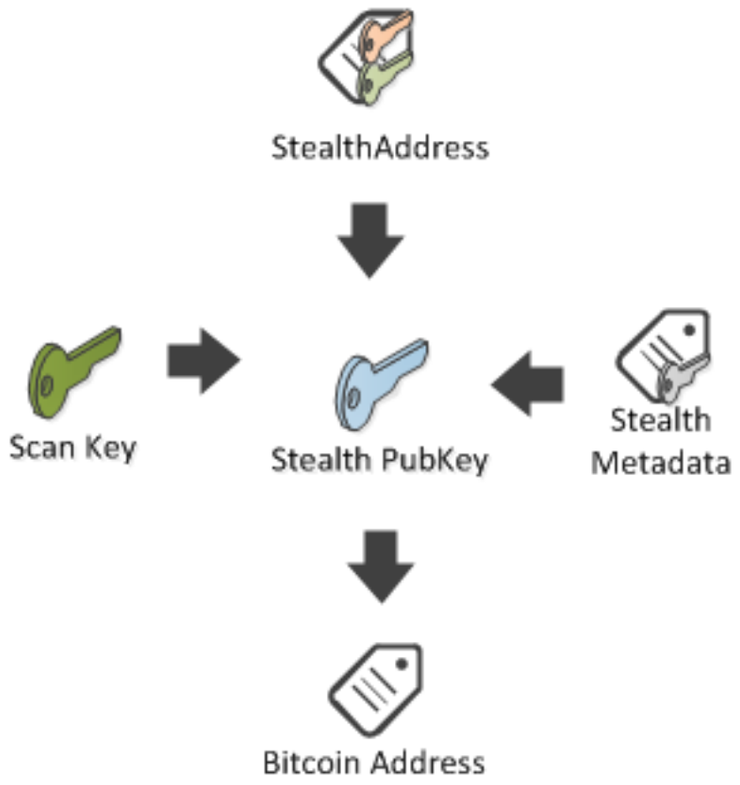


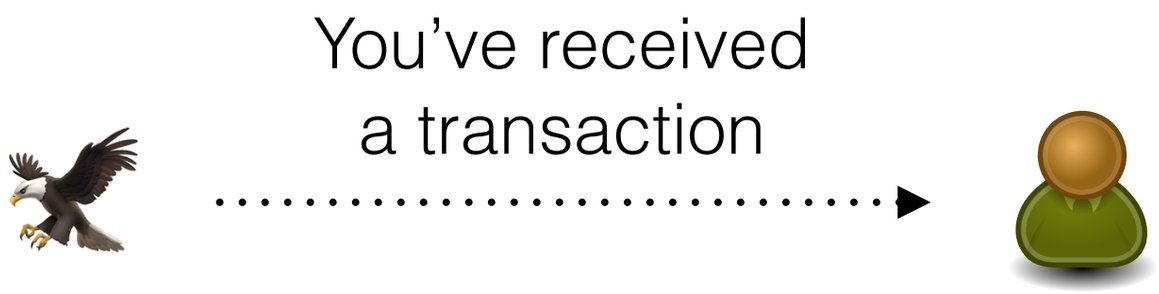
Scanner

Payer

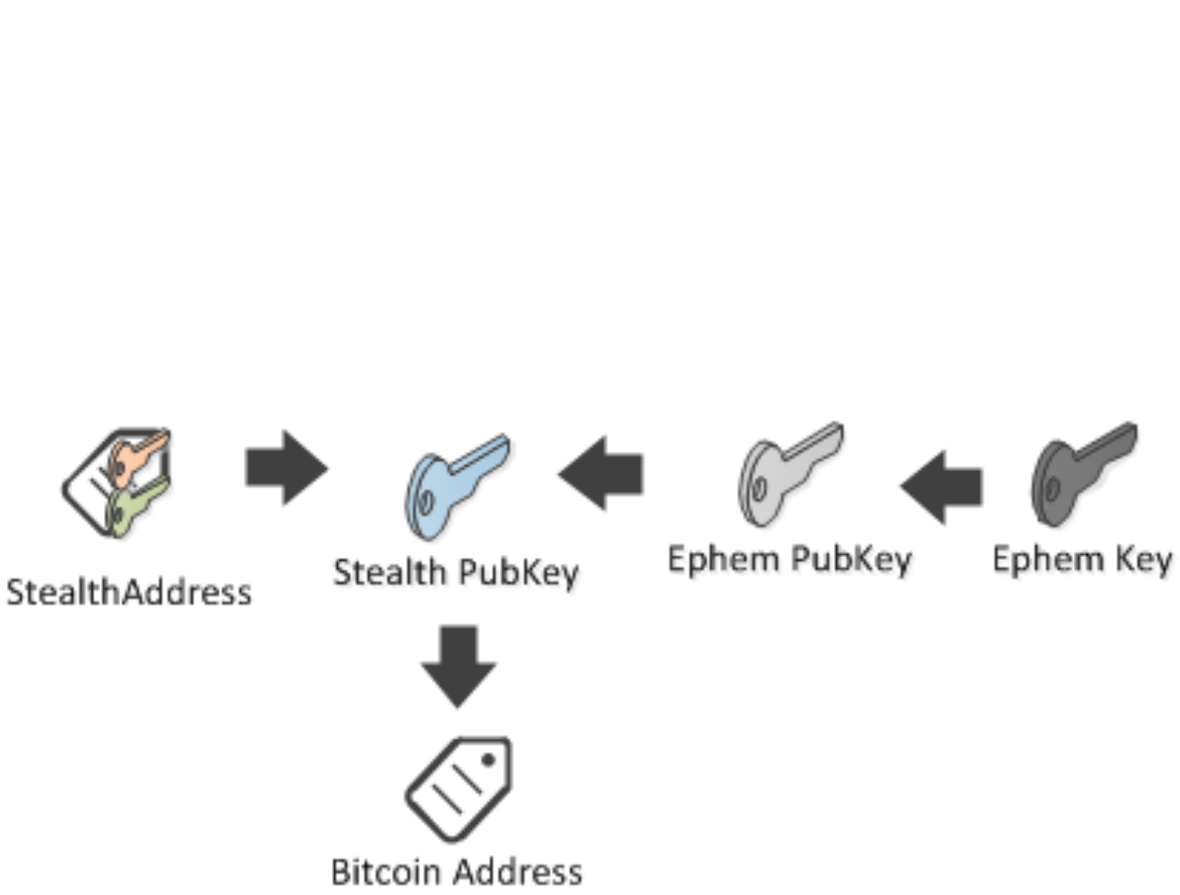
Pay to address

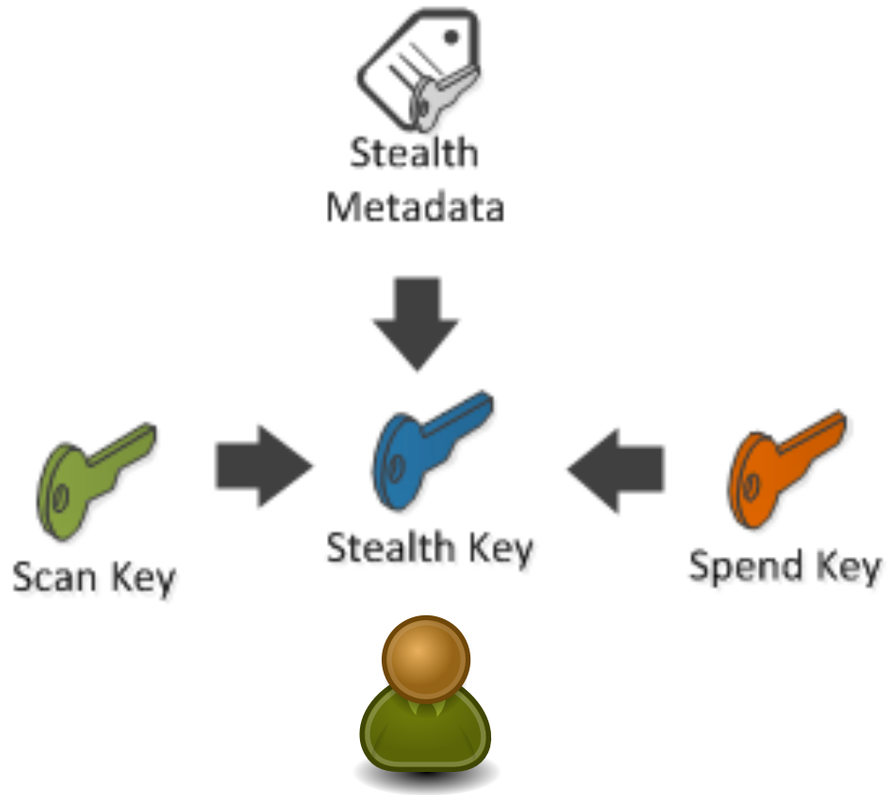
Stealth Addresses - Receiving





Stealth Addresses - Spending





Receiver

Got the private key
to spend the coins!

Thanks to https://programmingblockchain.gitbook.io/programmingblockchain/key_generation/stealth_address

Blockchain Privacy
Ring Signatures

Ring Signatures - Rivest, Shamir, Tauman

Signature solutions:

- Digital signatures ➡ verifies against a specific public key
- Group signatures
- Ring signatures ➡ verify against a set of public keys
- Linkable Ring signatures

“Set” Signatures

- Group signatures ➡️ well defined group
- Ring signatures ➡️ ad-hoc groups (great for cryptocurrencies)
- *Linkable* Ring signatures ➡️ reveal if a signer **already** produced a signature

- **Anonymity**
  An adversary cannot identify which ring signature corresponds to which of the public keys in the ring.
- **Unforgeability**
  An adversary cannot produce a valid signature, if it does not know a secret key corresponding to a public key included in the ring.
- **Exculpability**
  An adversary cannot produce a valid signature that links to the signature of another member of the ring, whose key the adversary does not control.
- **Linkability**
  Any two signatures produced by the same signer within the same ring are publicly linkable (i.e., anyone can detect that they were produced by the same signer).

Ring Signatures - Rivest, Shamir, Tauman

- Verify against **a set** of public keys. Computationally infeasible to determine which of the group members signed.

- Groups can be formed on an ad-hoc basis (vs. group signatures)

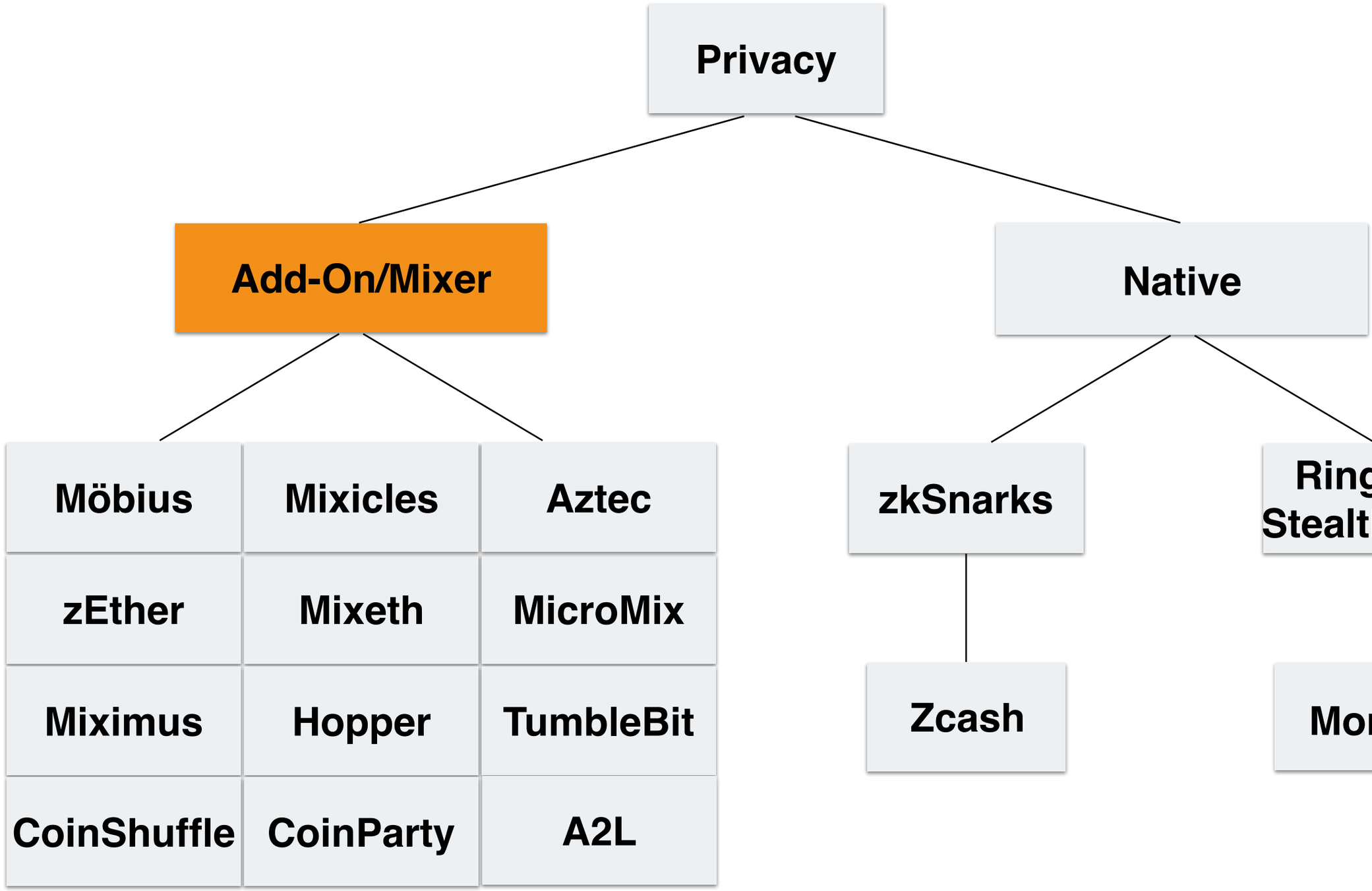
- *O(n)* for the resulting signature size
  n == number of public keys

https://ww.getmonero.org/resources/research-lab/pubs/MRL-0005.pdf

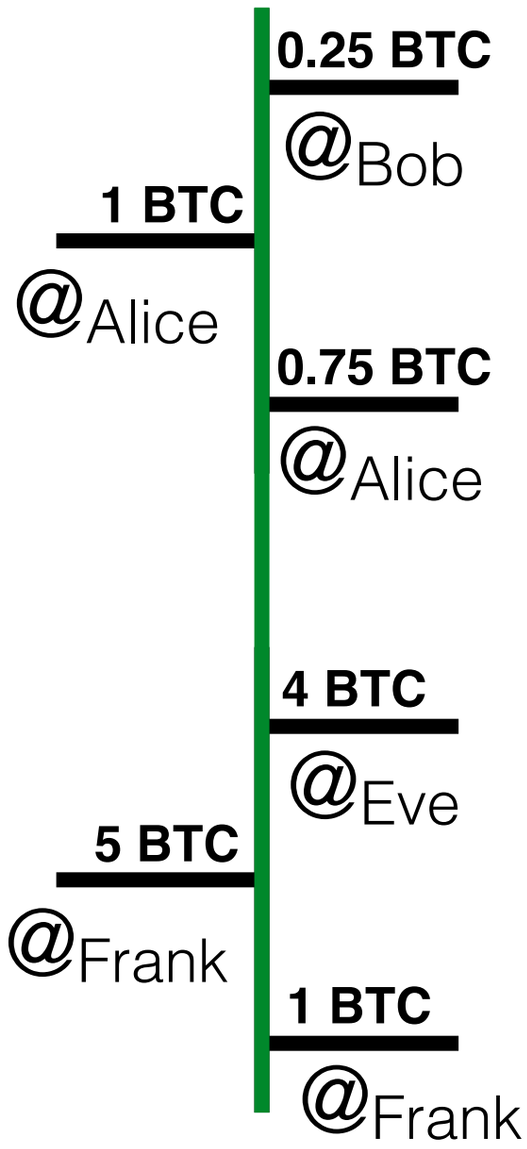
- Does not hide transaction amounts!

Blockchain Privacy
Add-on/Mixer Privacy

Blockchain Privacy Solutions



CoinJoin



Transaction

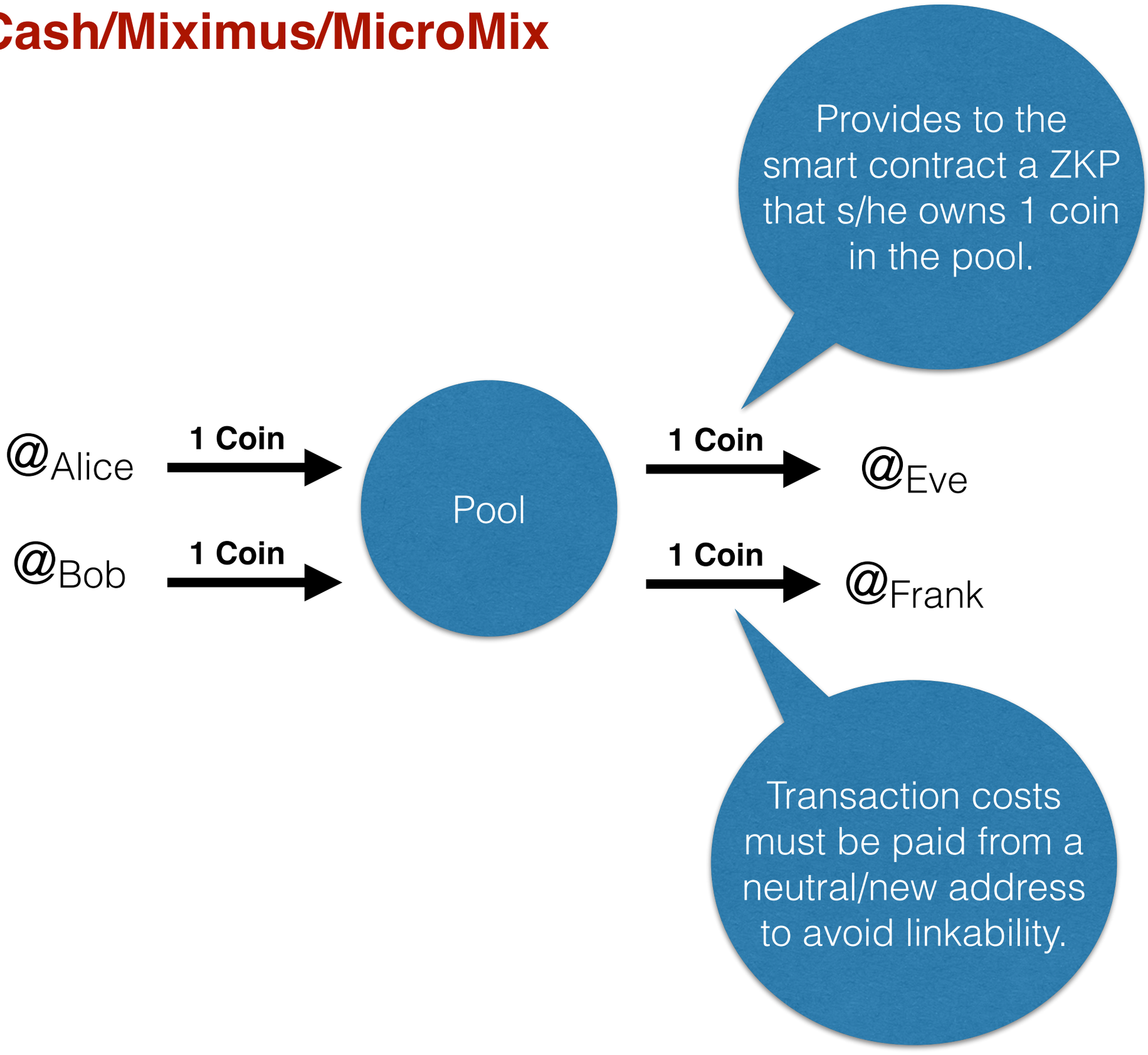
Advantages 👍

- Hides the originator of a transaction

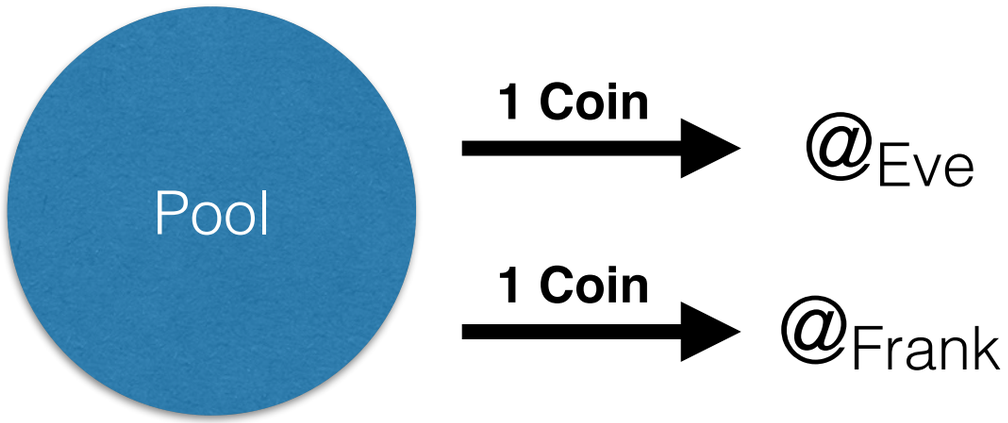
Drawbacks 👎

- Need for a *trusted third party* to merge the transactions
- No “spontaneous” mixing
- Doesn’t hide amounts
- “Small” anonymity set

Tornado Cash/Miximus/MicroMix



Tornado Cash/Miximus/MicroMix



Advantages 👍

- Hides the originator of a transaction
- Increasing anonymity set
  (as long as not everyone withdraws)
- No coordination among users

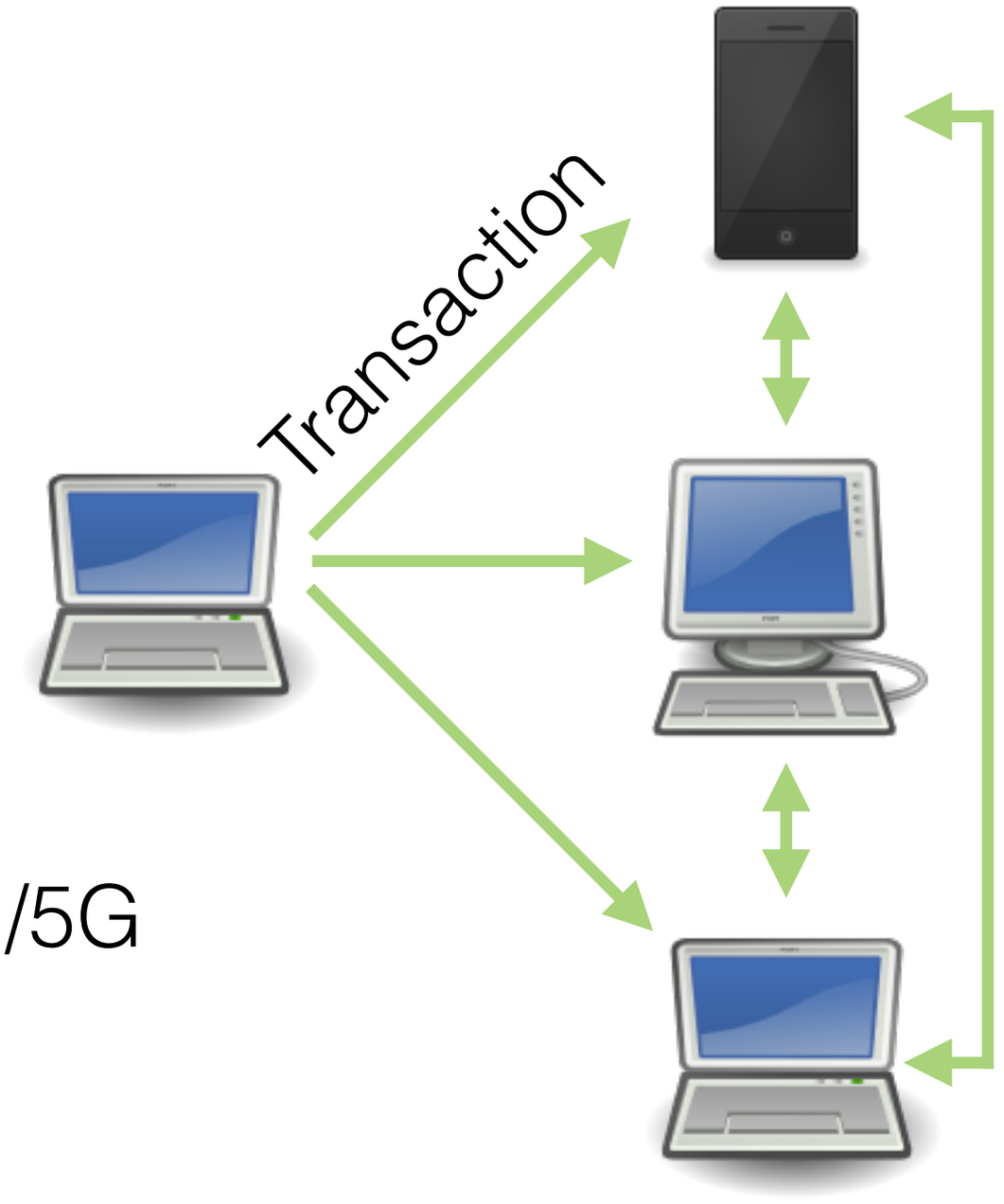
Drawbacks 👎

- Need for fresh coins to withdraw **or** a third party relayer
- Non user-friendly amounts

Blockchain Privacy Lightweight Clients

Blockchain Broadcast Data Model

1. Log of transactions (>300 GB)
2. Mobile phones receive irrelevant transactions
3. Limited data traffic over 3G/4G/5G



Private Mobile Blockchain Clients

Goal: Hide from the other nodes what the light client is interested in.

1. Private Information Retrieval
   ➡️ PIR and SPV

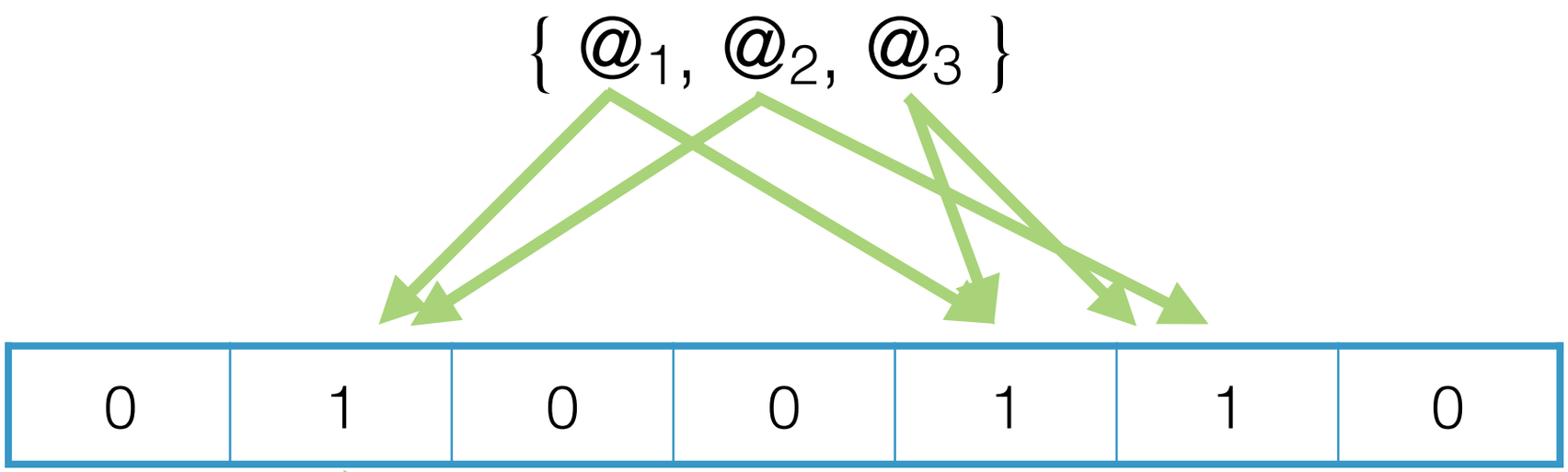
2. Bloom Filter
   ➡️ Bitcoin lightweight client implementation

3. Trusted Execution Environment
   ➡️ Bite or Zlite

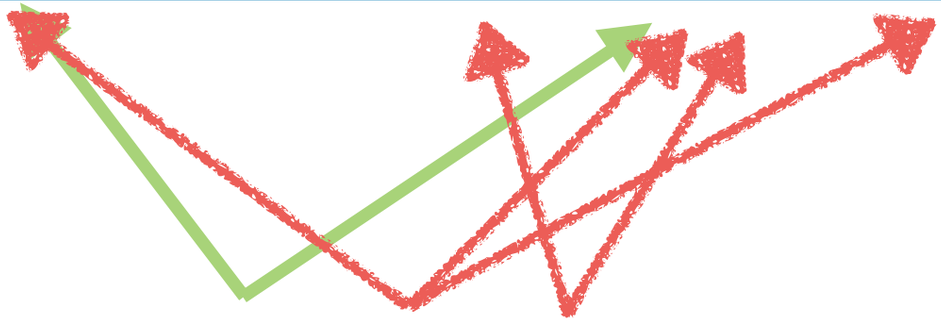
Blockchain Privacy
Bloom Filter & SPV

Enable mobile Bitcoin clients

Insertion



Bloom filter



Membership test

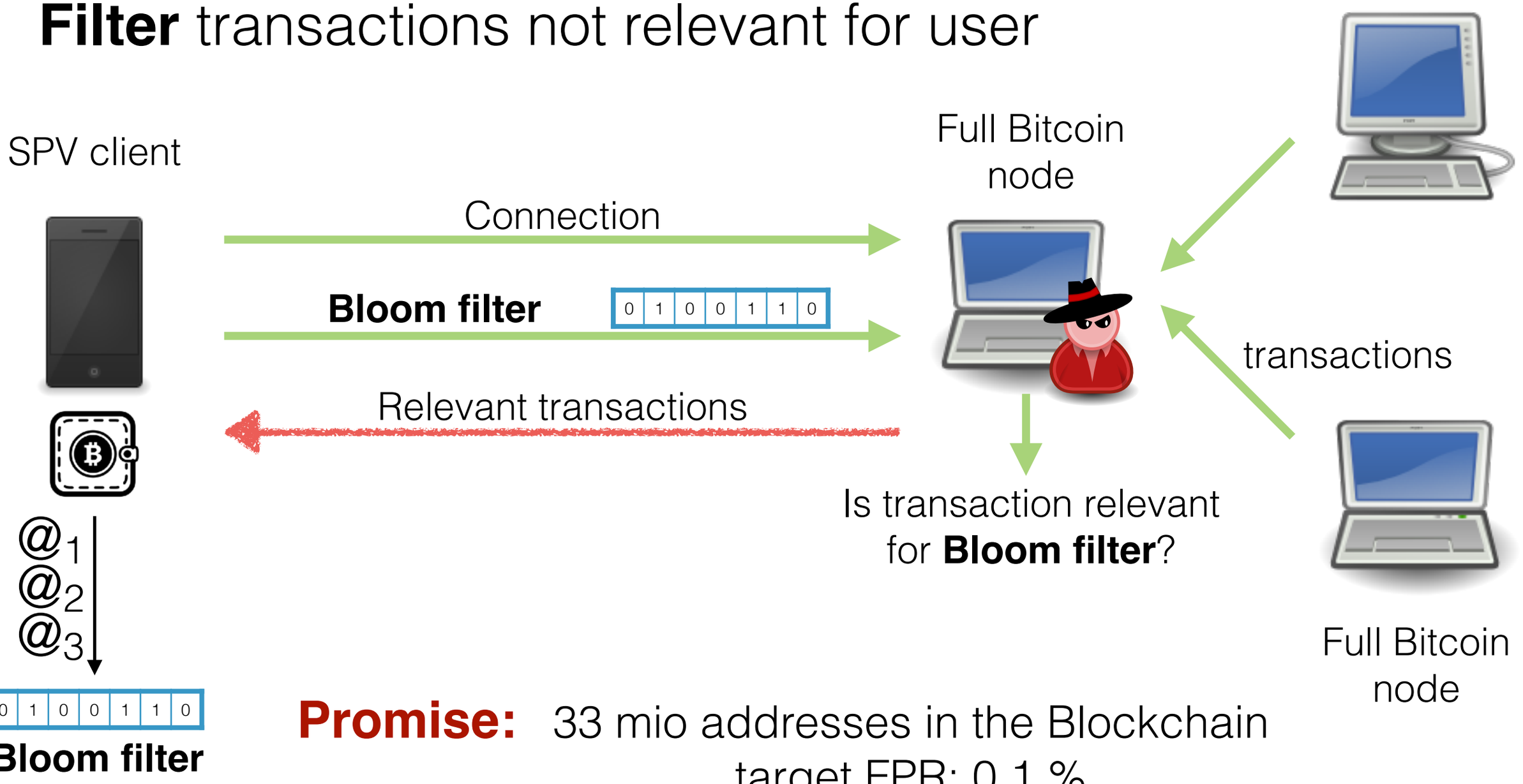
{ @1, @4, @5 }

! @4 False positive → **target False Positive Rate** (FPR)

@5 True negative

Simple Payment Verification (SPV)

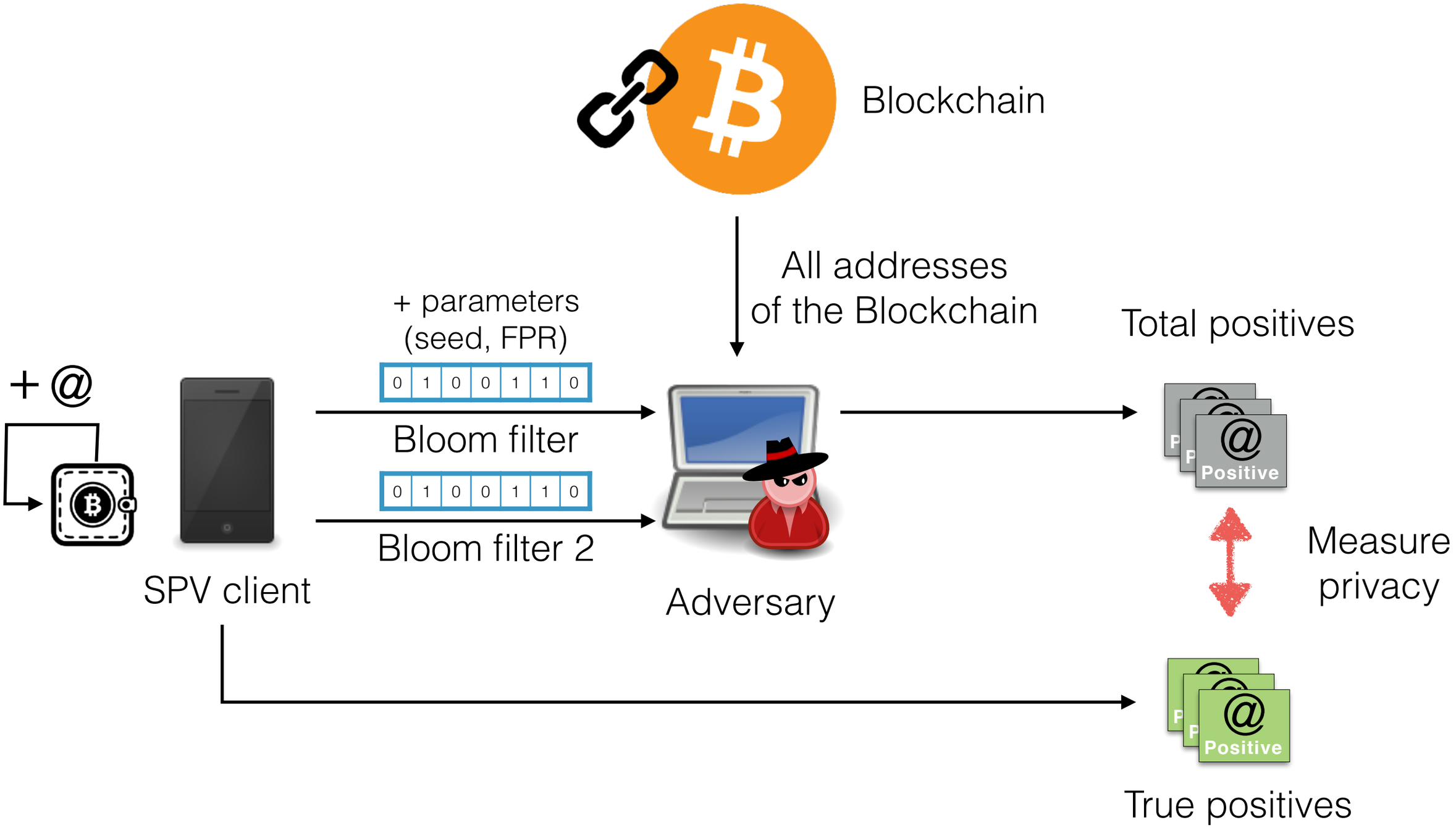
Filter transactions not relevant for user



Promise: 33 mio addresses in the Blockchain
target FPR: 0.1 %

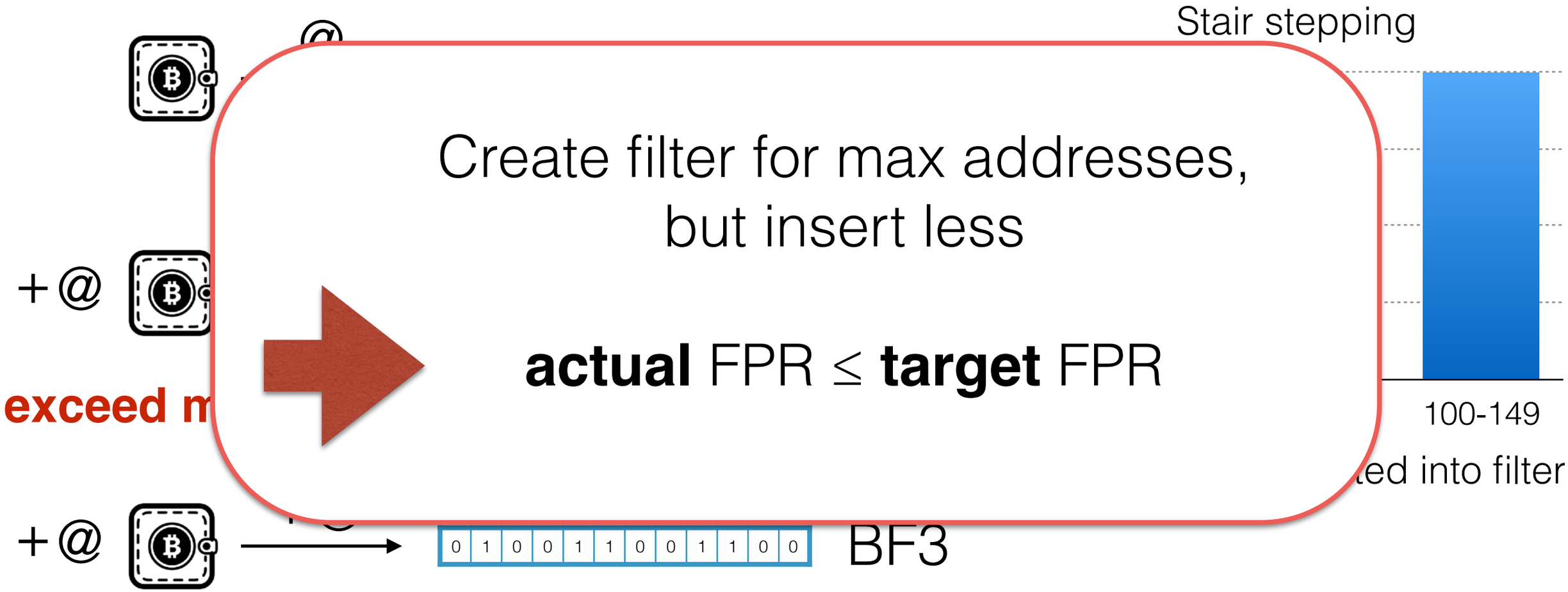
"User addresses hidden amongst 33 000" false positives

Model and Privacy measure



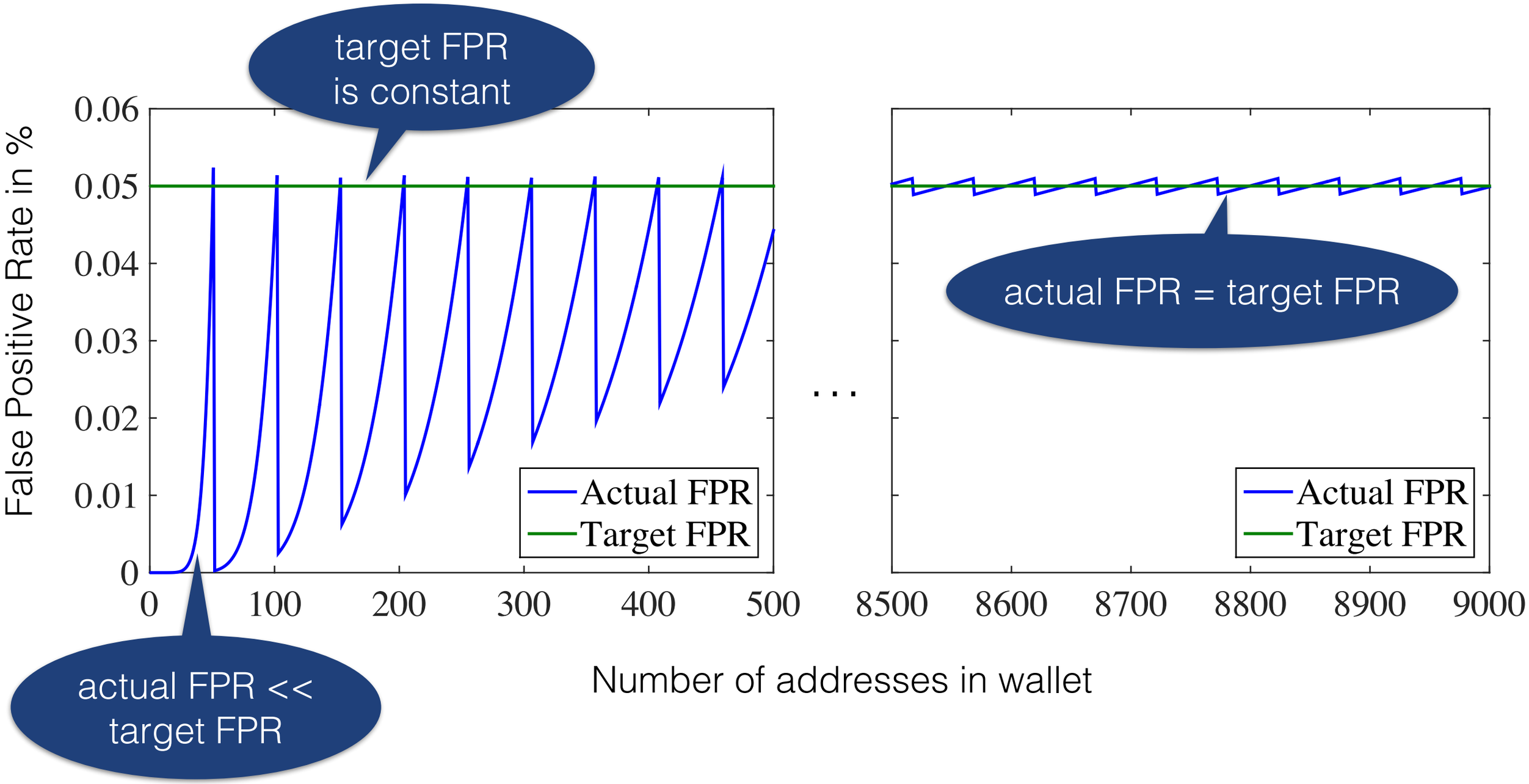
Stair stepping

Bloom filter designed for
- max number of **addresses**
- **target FPR** when max addresses inserted

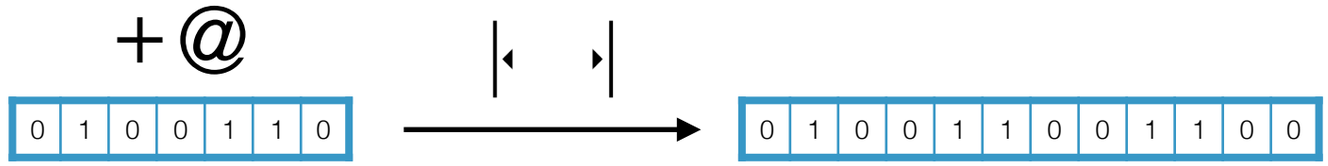


Rationale: **avoid** filters with different sizes

Analytical results - Actual FPR vs. Target FPR



Resizing



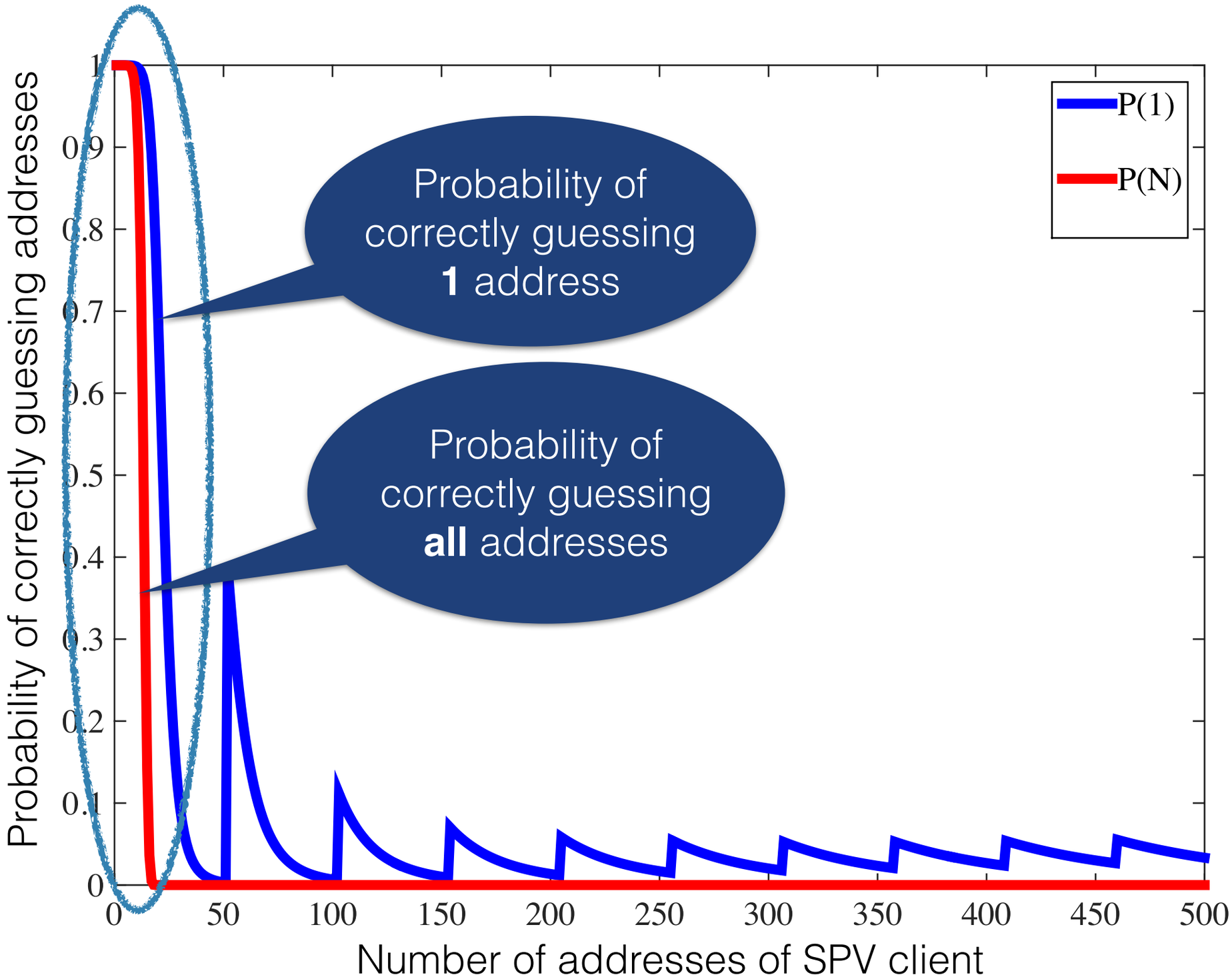
Once max addresses inserted —> bigger filter

- **Consequence**: New filter yields **different** false positives

Summary of current SPV design choices

1. Stair stepping → actual FPR ≤ target FPR
2. Resizing → different False Positives
3. Restarting → different False Positives

One Bloom filter



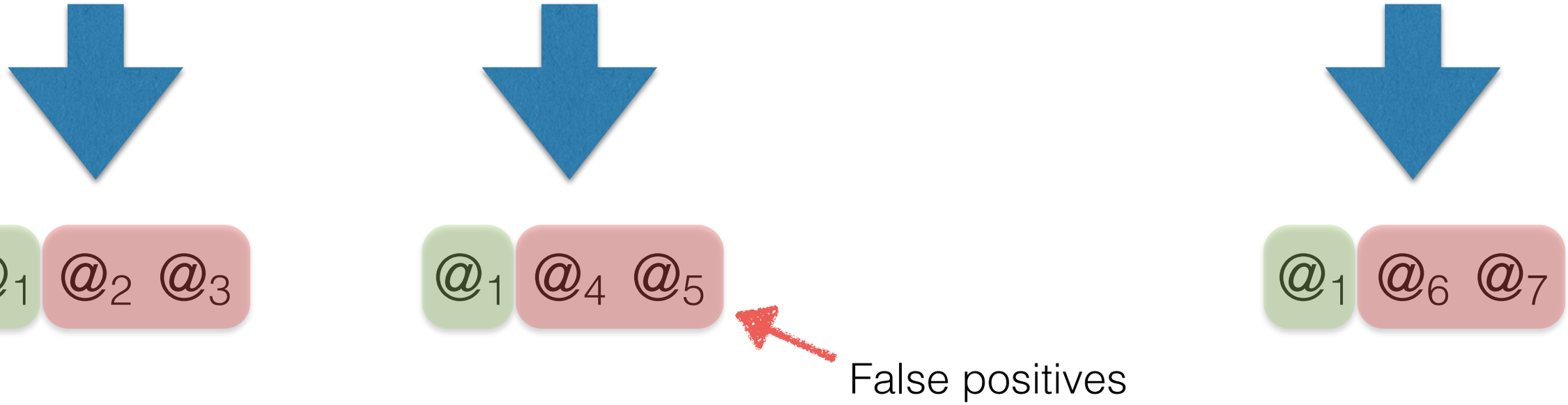
Multiple Bloom filters

Filter 1

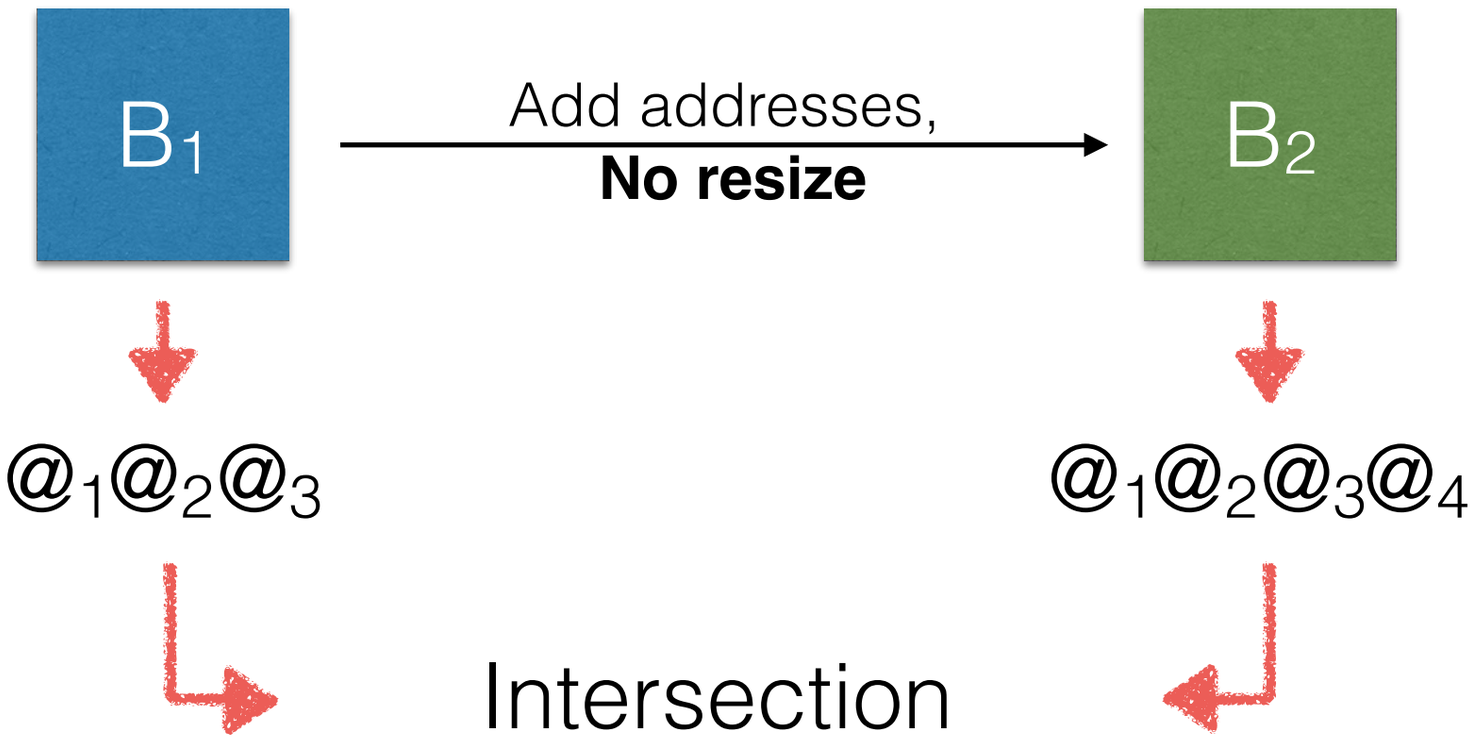
Filter 2

. . .

Filter n



Experiment 1 - No resize



Intersection

Exp.	Client	Seed	Size
No resize	**Same**	**Same**	**Same**
Resize	Same	Same	Different
Restart	Same	Different	Same
> 2 filter	Same	Different	Different

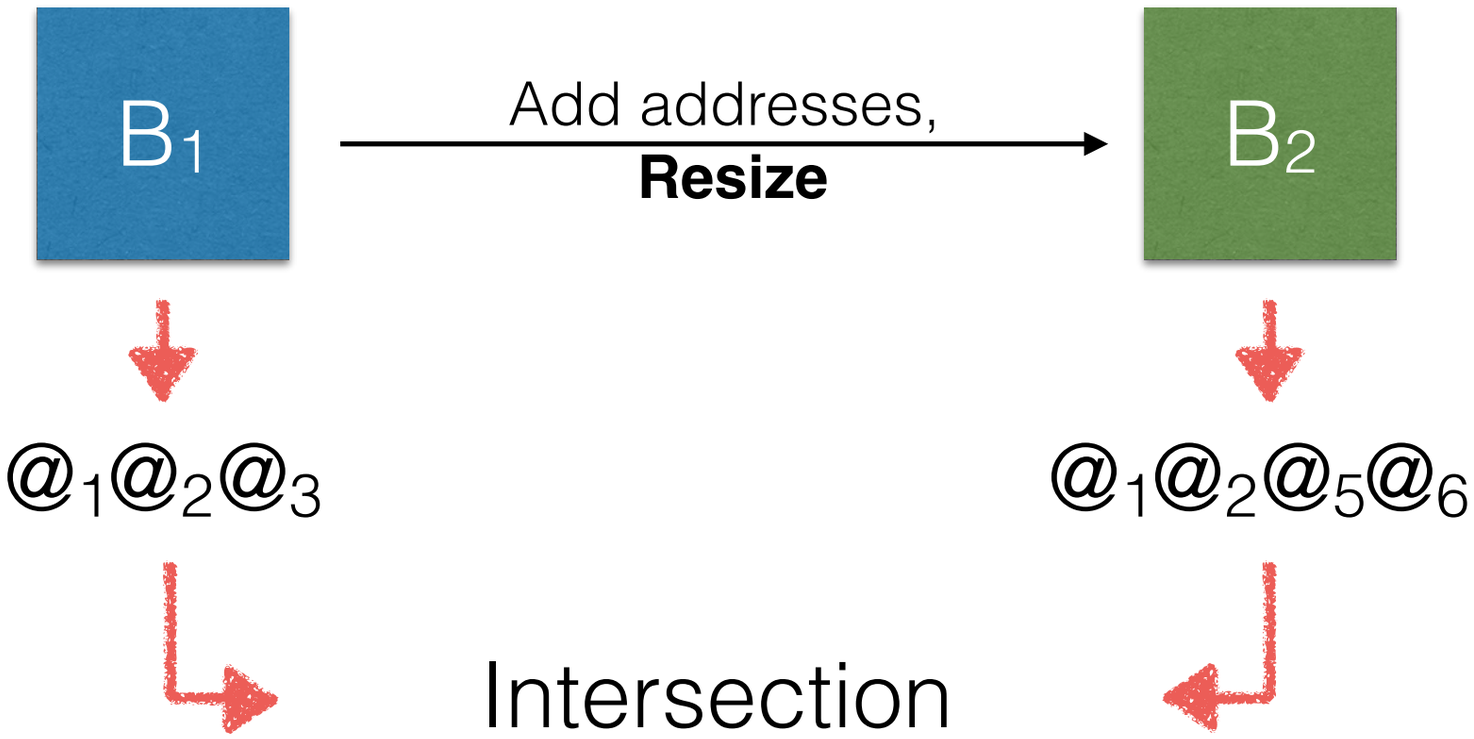
Results

Target FPR (%)	P(1) with 2 BF	P(1) with 1 BF
0.05	0.2990	0.2910
0.1	0.1020	0.1070
0.5	0.0078	0.0075

no change of privacy

- Yield the same positives
- The adversary does not learn a lot

Experiment 2 - Resize



Results

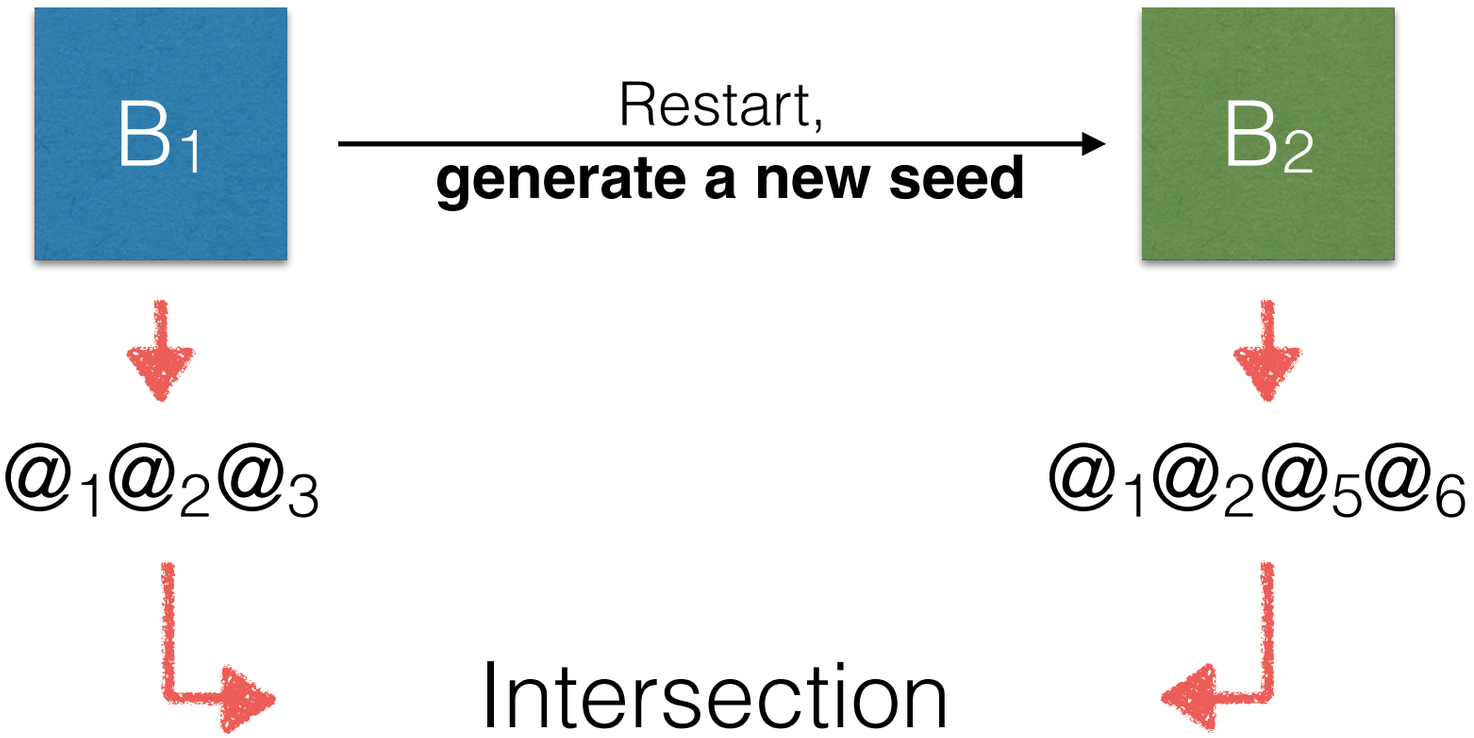
Target FPR (%)	P(1) with 2 BF	P(1) with 1 BF
0.1	0.98	0.03

significant change

Exp.	Client	Seed	Size
No resize	Same	Same	Same
Resize	**Same**	**Same**	**Different**
Restart	Same	Different	Same
> 2 filter	Same	Different	Different

- Different BF sizes improve the attack

Experiment 3 - restart



Exp.	Client	Seed	Size
No resize	Same	Same	Same
Resize	Same	Same	Different
Restart	**Same**	**Different**	**Same**
> 2 filter	Same	Different	Different

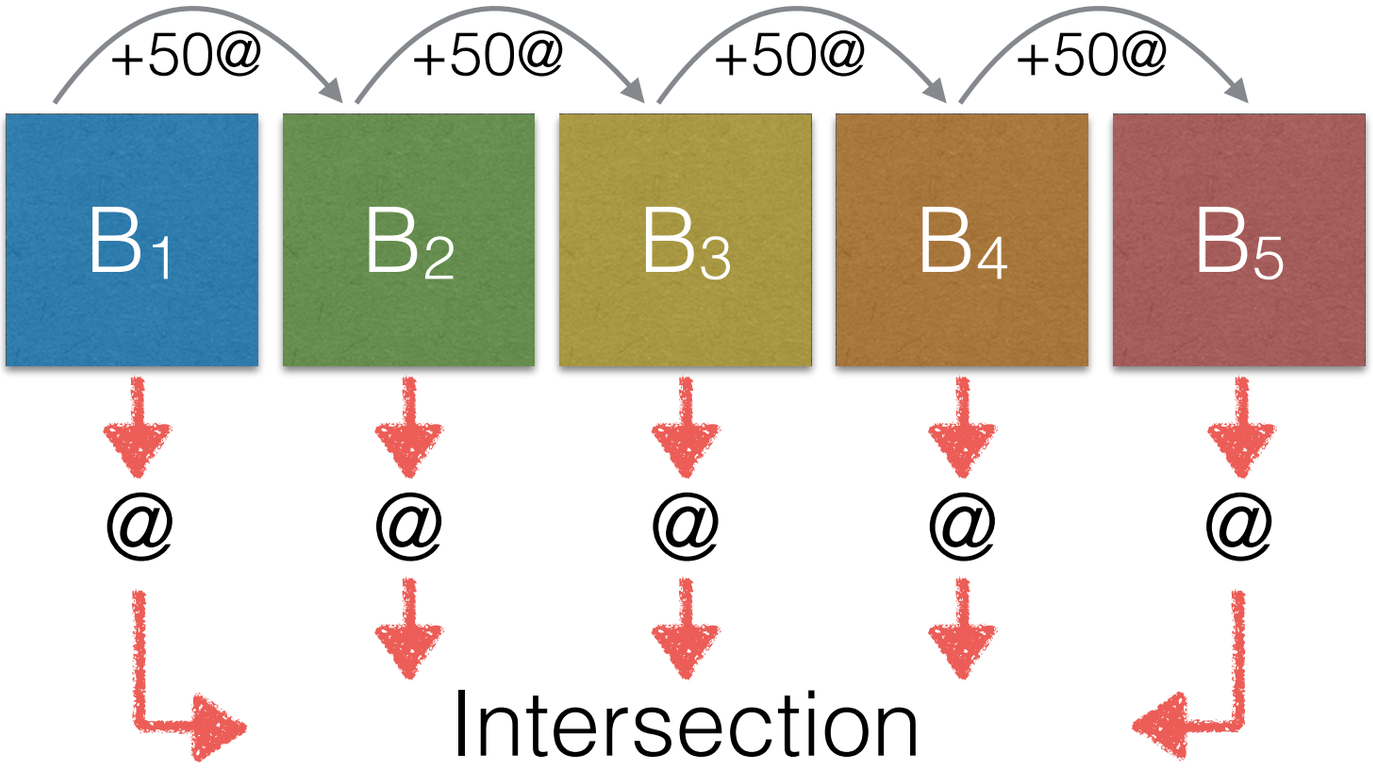
Results

Target FPR (%)	P(1) with 2 BF	P(1) with 1 BF
0.1	0.99	0.04

significant change

- Different BF seeds improve the attack

Experiment 4 - More than 2 filter



Exp.	Client	Seed	Size
No resize	Same	Same	Same
Resize	Same	Same	Different
Restart	Same	Different	Same
> 2 filter	**Same**	**Different**	**Different**

Results

Guessing all addresses

Target FPR (%)	P(N) given 3 or more BF
0.05	~1
0.1	~1

3 Bloom filter

All addresses yielded by B_1 are leaked

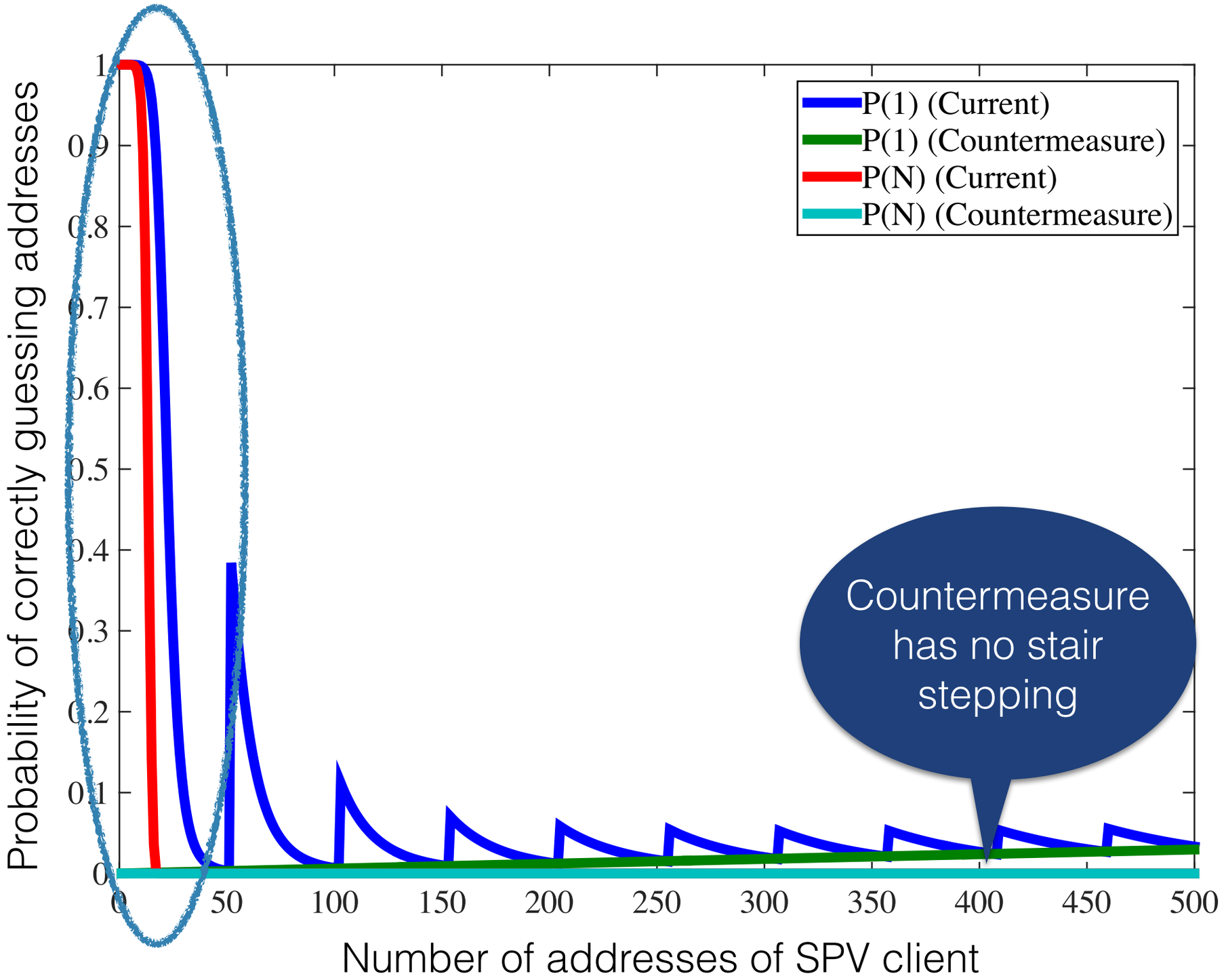
Observations

1. Need constant FPR

2. Multiple Bloom filter with different parameters 

3. SPV clients should keep state (e.g., about seed) 

Proposed solution



Information leakage through Bloom Filters in SPV clients

Analytical and Empirical evaluation

- 1 Bloom filter critical if < 20 Bitcoin addresses 
- 3+ Bloom filter intersection attack particularly strong 

Lightweight countermeasure

- **Significantly** reduces leakage
- Intersection attack **not effective**
- Requires **few** changes

Conclusion

- Bloom filter for privacy is delicate
- Designed carefully we can achieve proper privacy

Thank you!