A close-up photograph of a white boat's hull and a metal chain anchor in dark blue water. The chain is attached to a metal plate on the hull. The water is dark and reflects the light from the boat.

# Blockchain Privacy

# Fungibility

# Fungibility



?  
==



# Fungibility



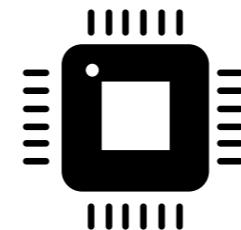
?  
==



Is 1 Bitcoin always worth 1 Bitcoin?

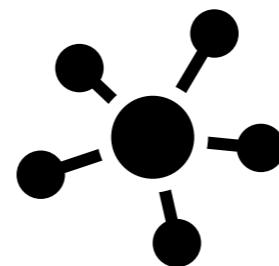
# Blockchain Privacy is a Multilayer Challenge

Hardware  
Layer

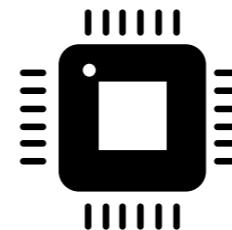


# Blockchain Privacy is a Multilayer Challenge

Network  
Layer 0

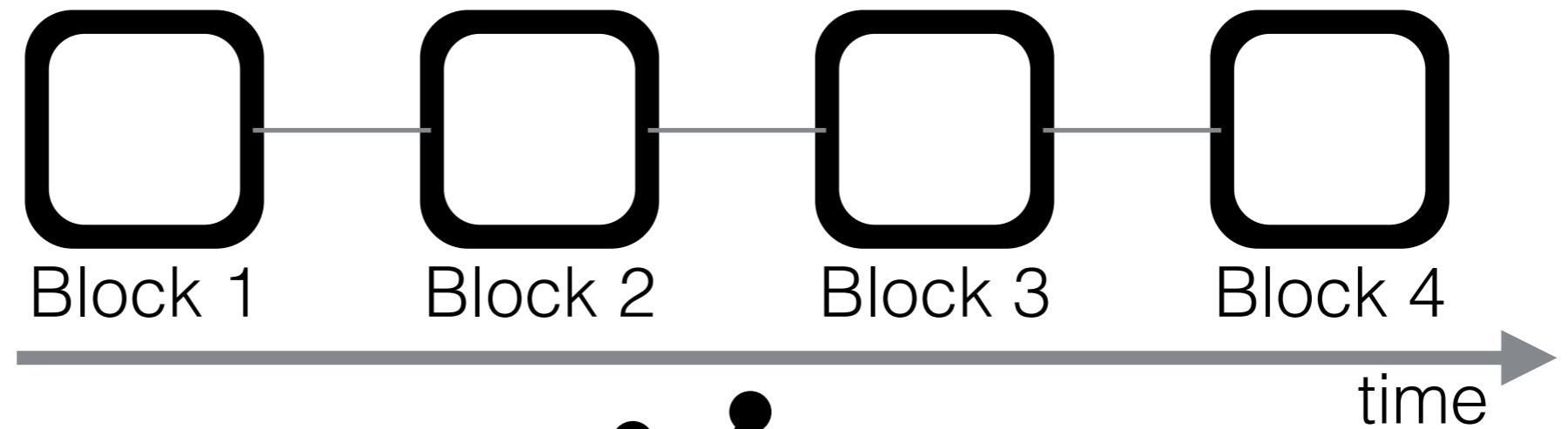


Hardware  
Layer



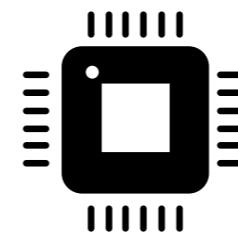
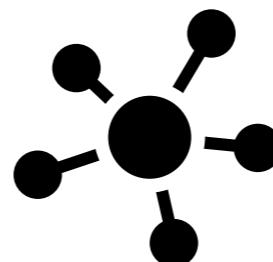
# Blockchain Privacy is a Multilayer Challenge

Blockchain  
Layer 1



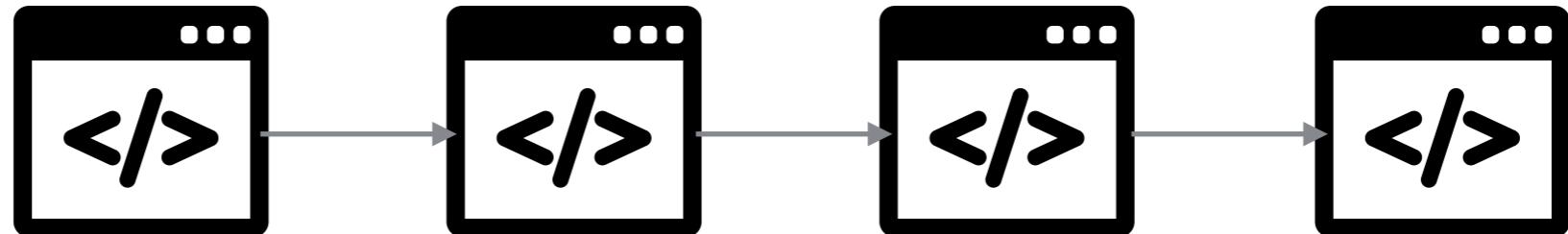
Network  
Layer 0

Hardware  
Layer

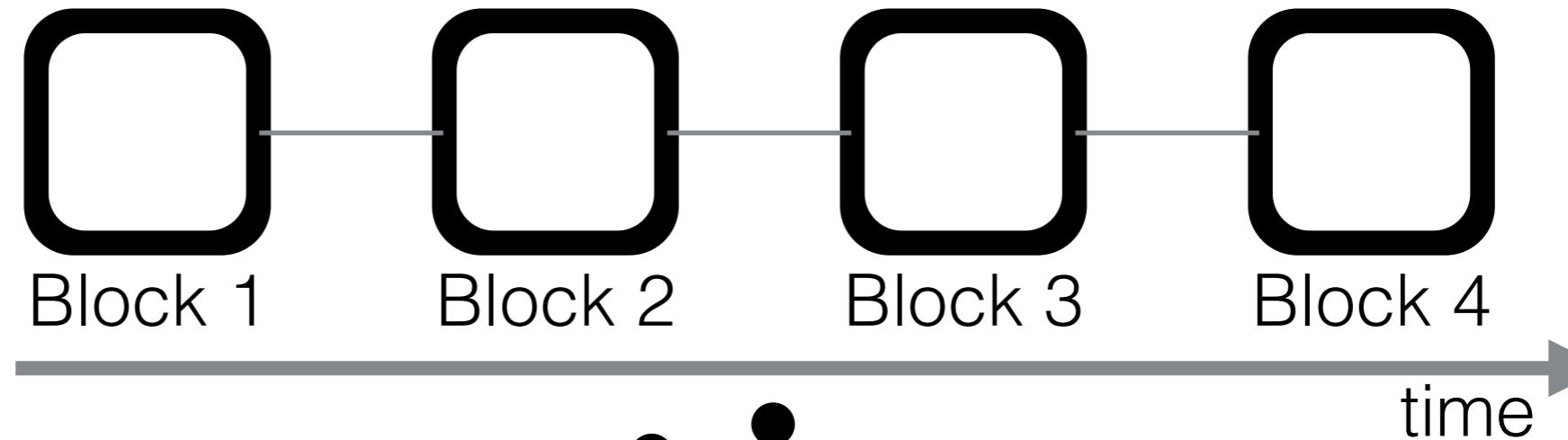


# Blockchain Privacy is a Multilayer Challenge

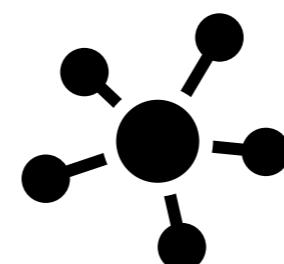
Application  
Layer 2



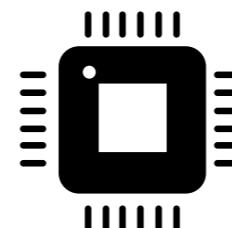
Blockchain  
Layer 1



Network  
Layer 0

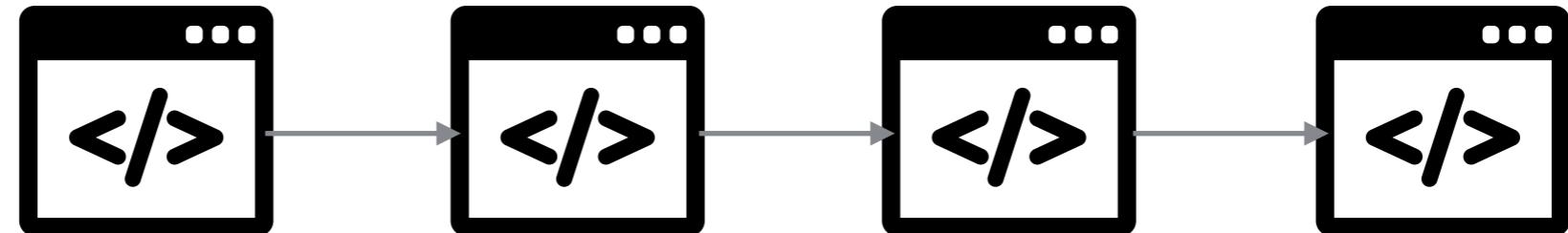


Hardware  
Layer

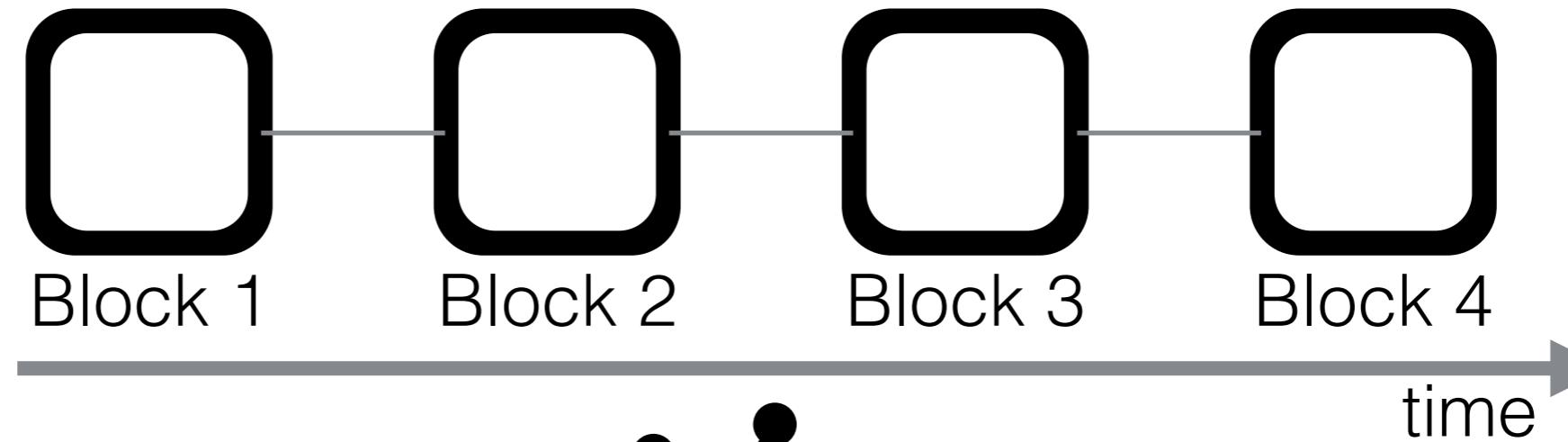


# Blockchain Privacy is a Multilayer Challenge

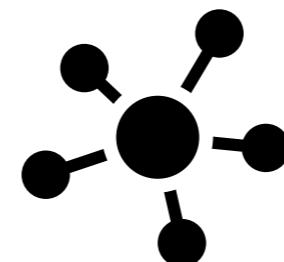
Application  
Layer 2



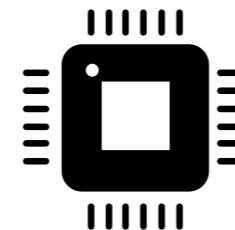
Blockchain  
Layer 1



Network  
Layer 0

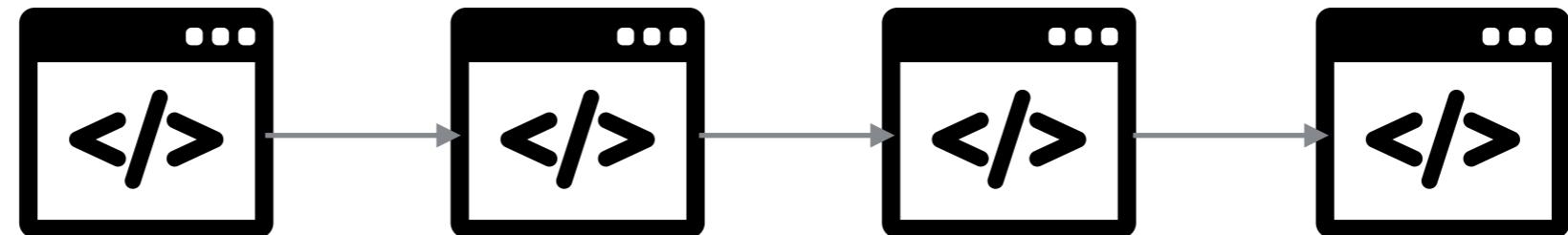


Hardware  
Layer

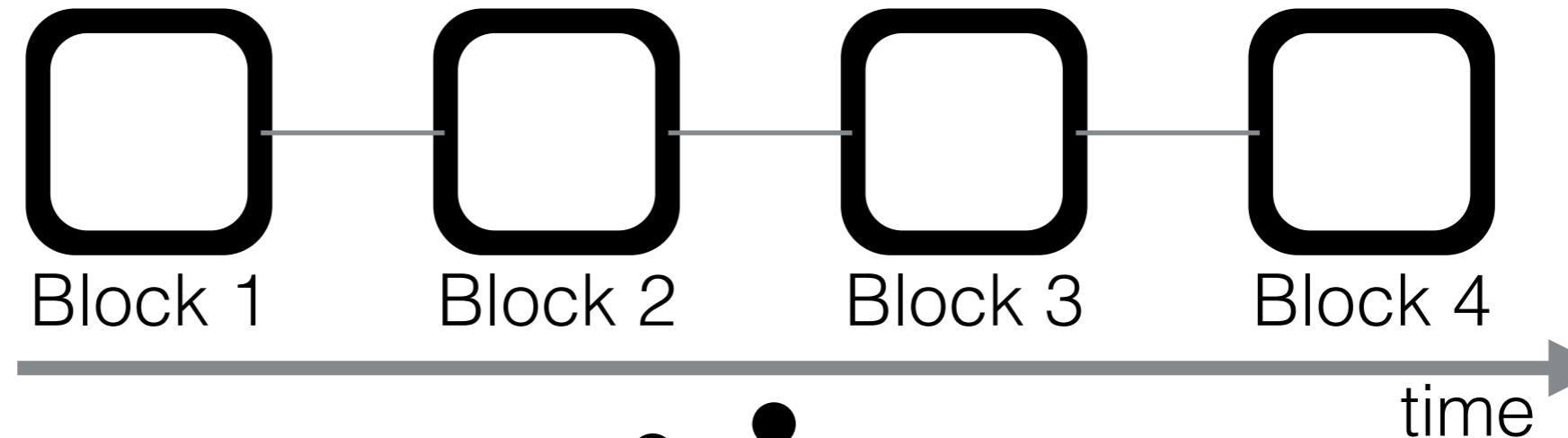


# Blockchain Privacy is a Multilayer Challenge

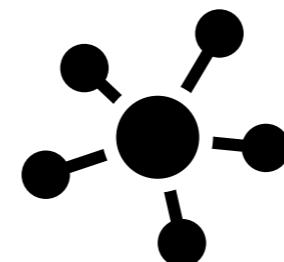
Application  
Layer 2



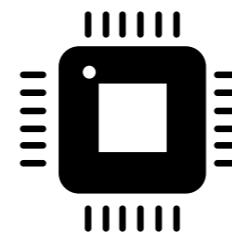
Blockchain  
Layer 1



Network  
Layer 0

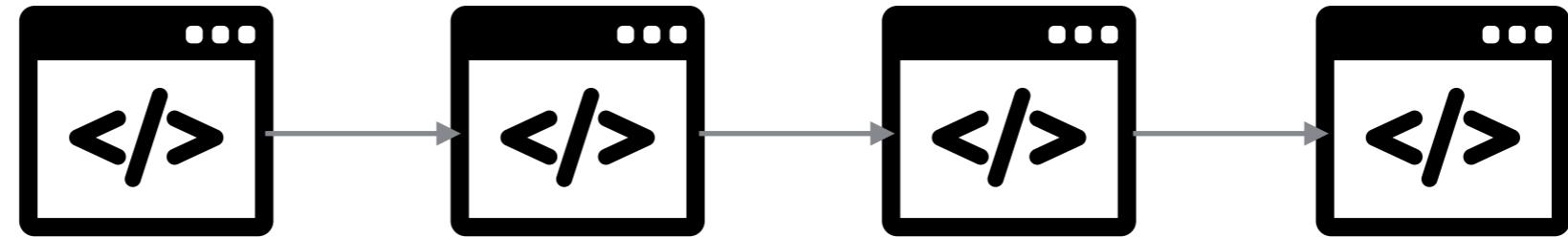


Hardware  
Layer

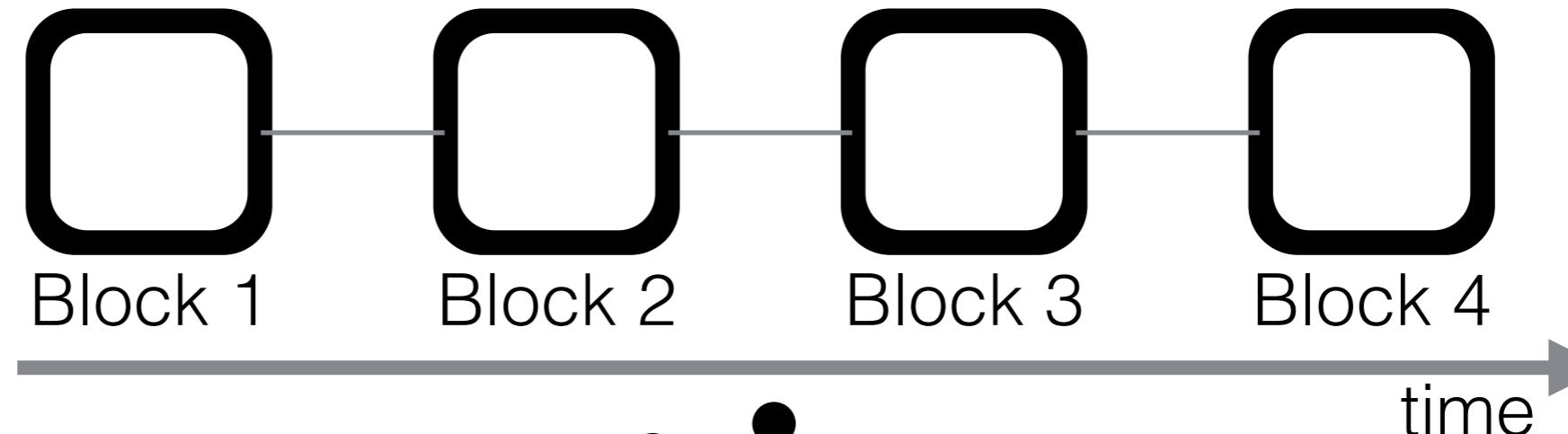


# Blockchain Privacy is a Multilayer Challenge

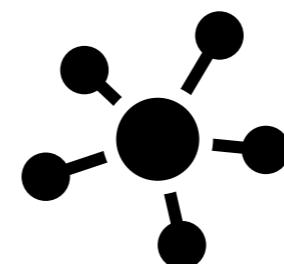
Application  
Layer 2



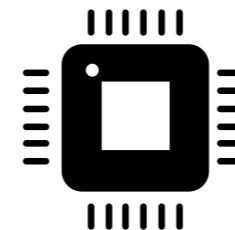
Blockchain  
Layer 1



Network  
Layer 0

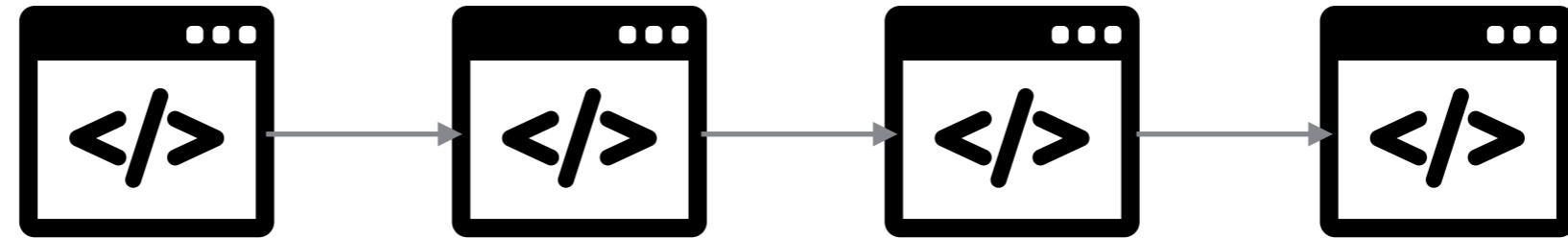


Hardware  
Layer

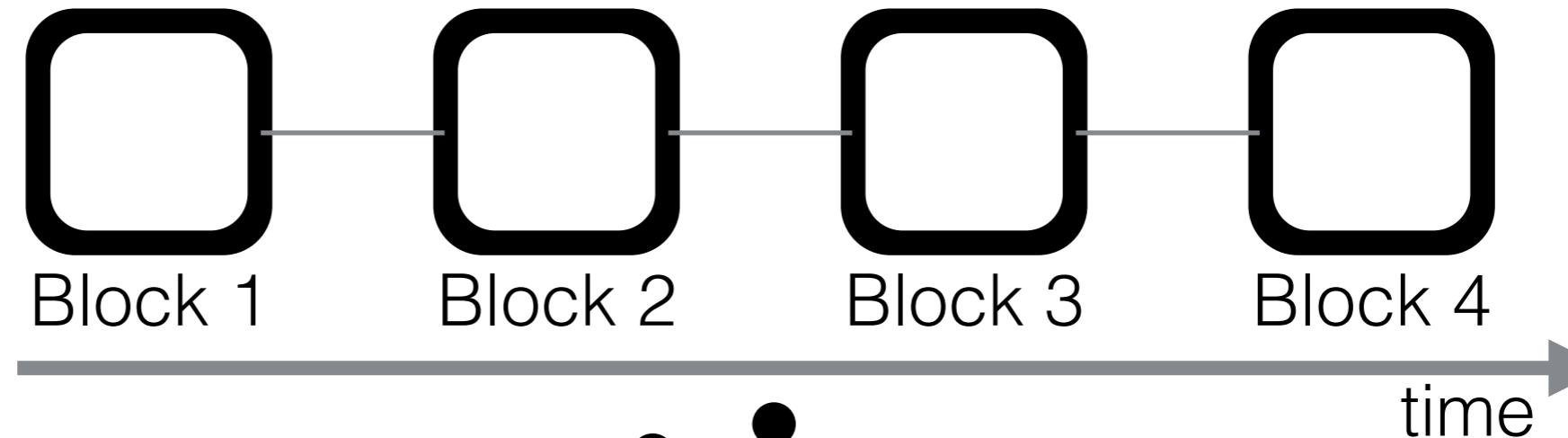


# Blockchain Privacy is a Multilayer Challenge

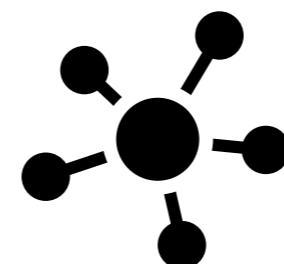
Application  
Layer 2



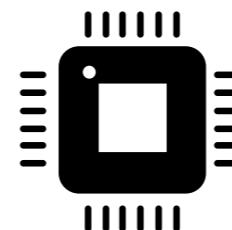
Blockchain  
Layer 1



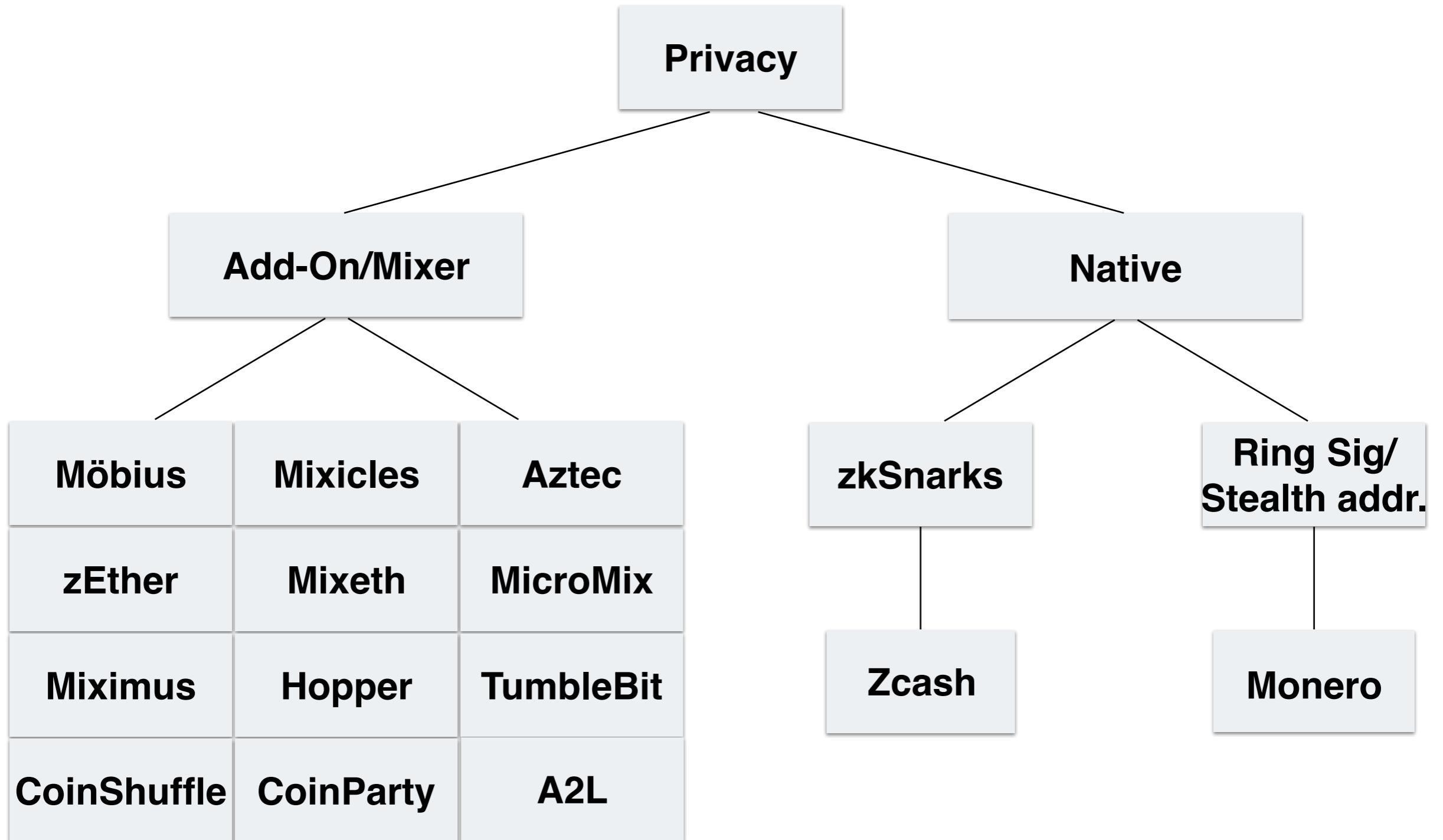
Network  
Layer 0

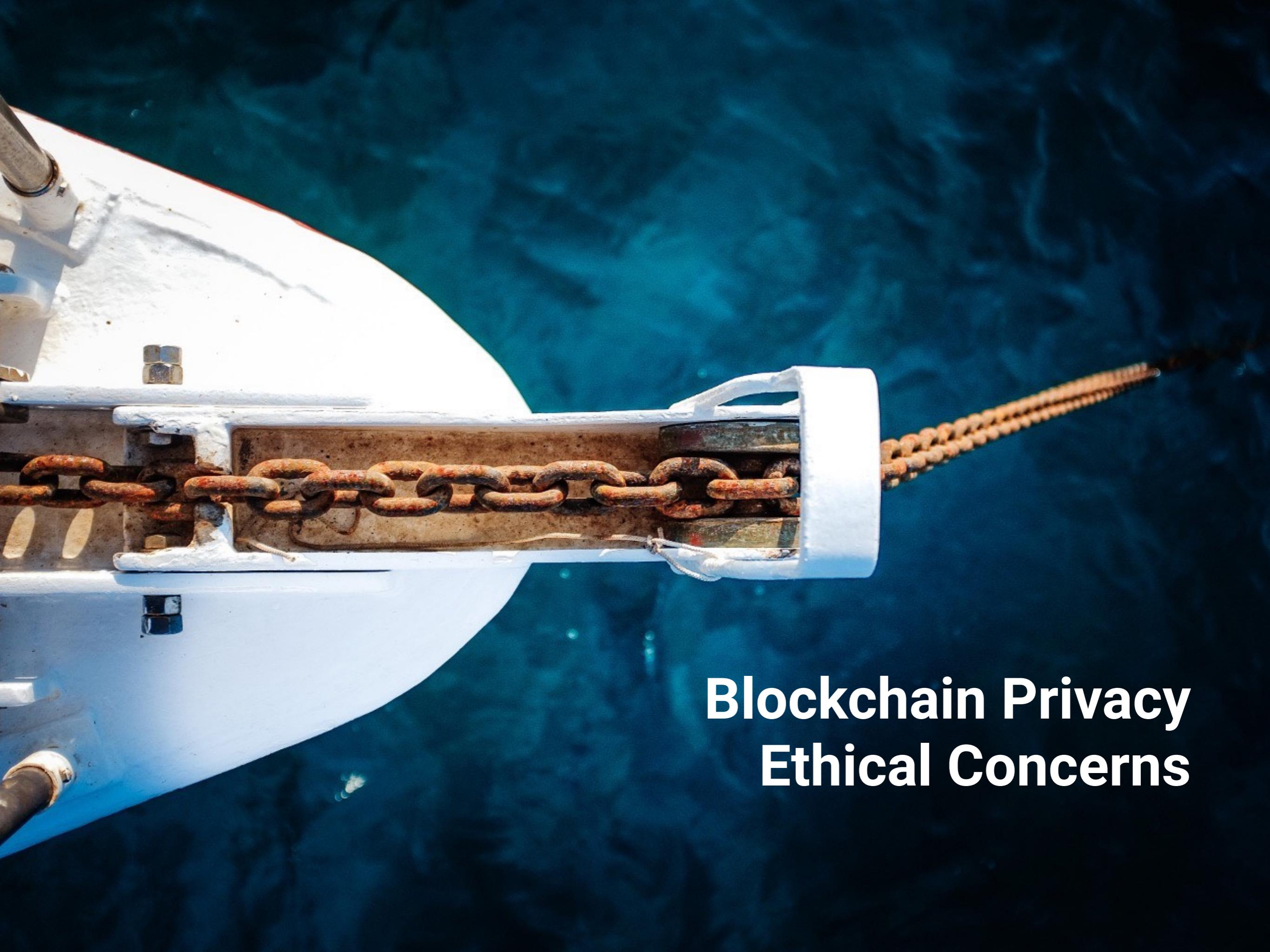


Hardware  
Layer

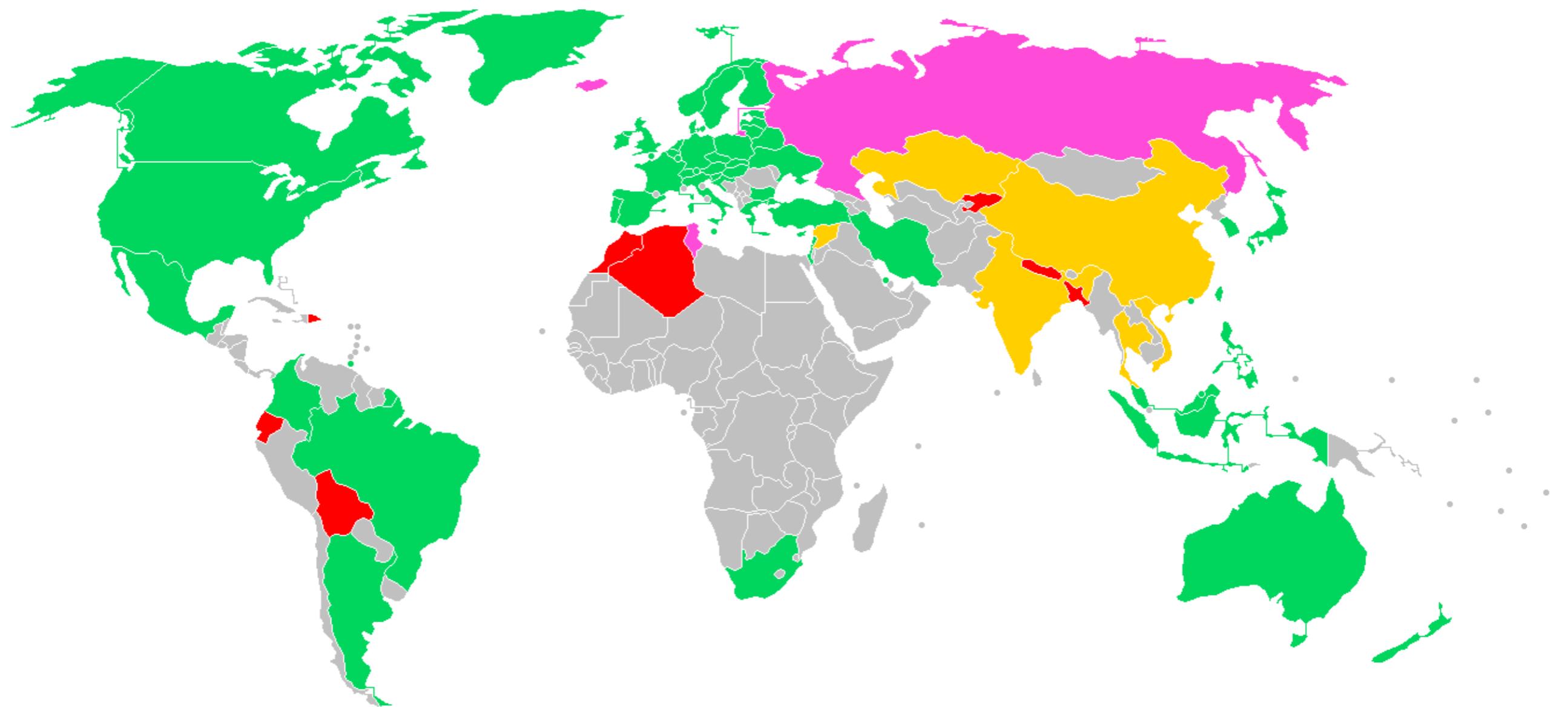


# Blockchain Privacy Solutions



A close-up photograph of a white boat's hull and a metal chain anchor in dark blue water. The chain is attached to a metal plate on the hull. The water is dark and reflects the light from the boat.

# Blockchain Privacy Ethical Concerns



## Money Laundering

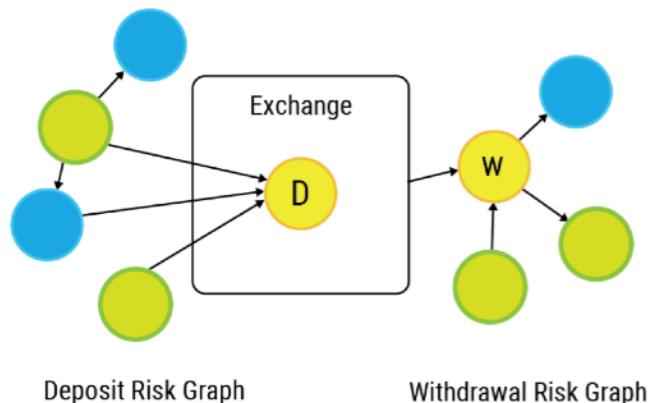
- Anonymous cash could be used for *criminal purposes*
- ZCash enables “selective disclosure”
  - > For tax and AML purposes
- Tornado Cash has a “compliance tool”

# (Breaking) Privacy is a Business

- Governments
- Secret Services
- Police

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

Walletscore Risk-Flow Graph

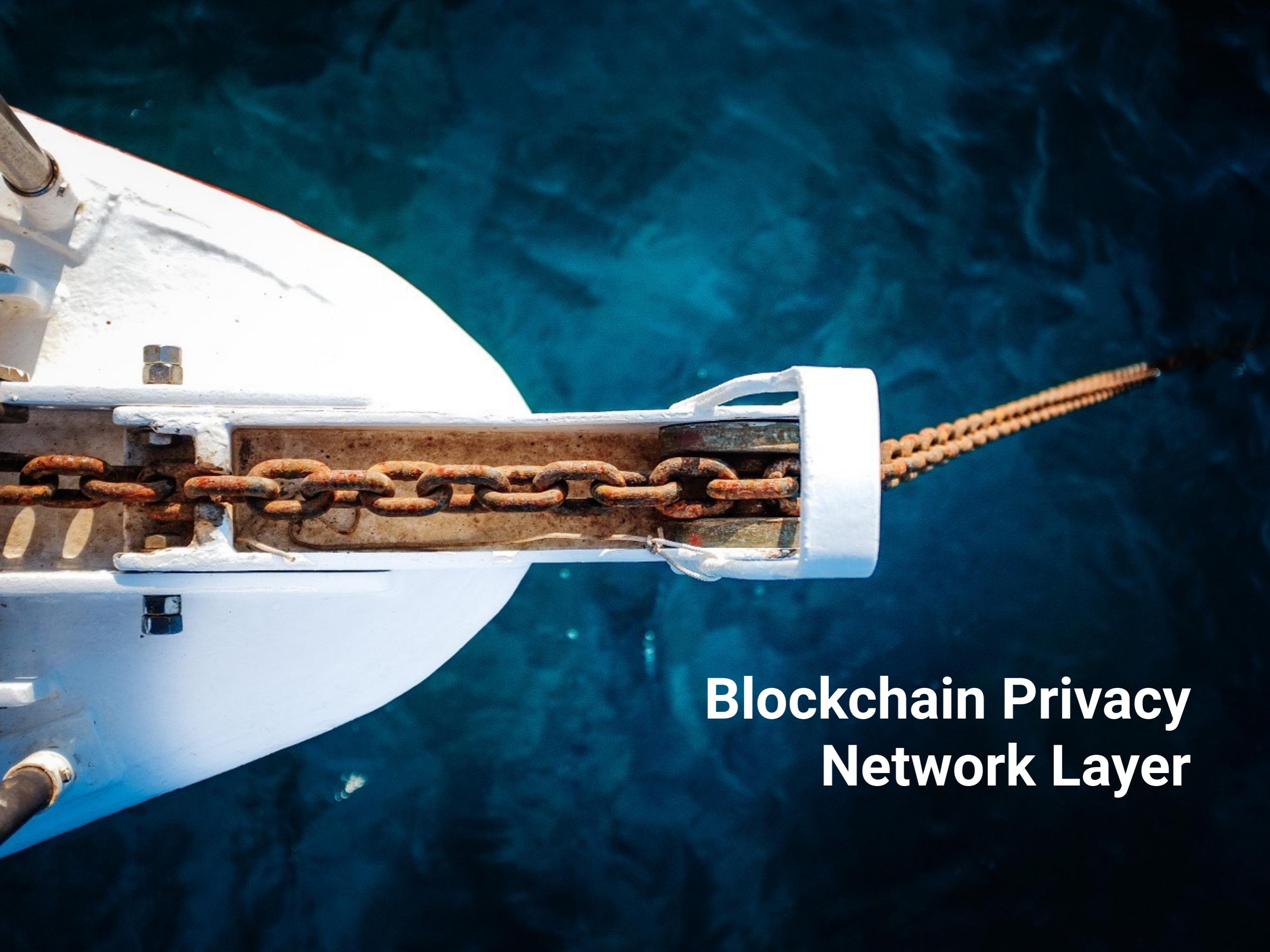


**ELLIPTIC**

WHAT WE DO WHO WE HELP ABOUT ELLIPTIC ANALYSIS

Detect And Prevent Criminal Activity In Cryptocurrency.



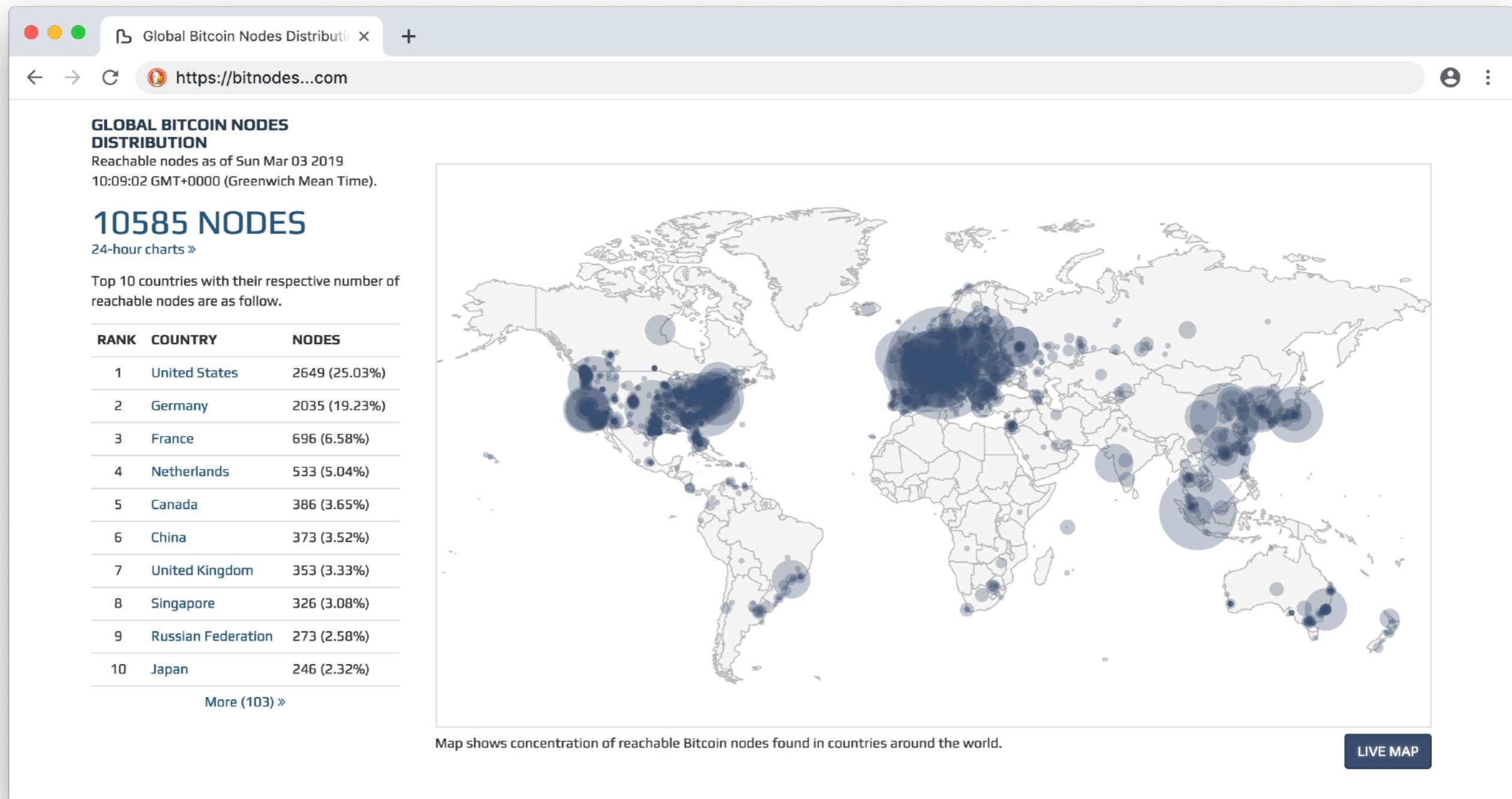
A close-up photograph of a white boat's hull and a metal chain anchor in dark blue water. The chain is attached to a metal plate on the hull. The water is dark and reflects the light from the boat.

# 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

The screenshot shows a detailed view of a Bitcoin transaction on the Blockcypher website. The transaction ID is 438c91af6d53e467a03a0a3bb48e1b6b8e5675aa64247d0375ee4b686548617a. The transaction amount is 0.02518809 BTC, with fees of 0.00000647 BTC. It was received 3 minutes ago and has 0/6 confirmations. The confidence level is 43.17%, and the miner preference is low. The transaction size is 266 bytes, lock time is 1, and it was relayed by 107.20.94.164:8333.

BTC Transaction 438c91af6d53e467a03a0a3bb48e1b6b8e5675aa64247d0375ee4b686548617a

**BLOCKCYPHER**

Bitcoin Transaction  
438c91af6d53e467a03a0a3bb48e1b6b8e5675aa64247d0375ee4b686548617a

AMOUNT TRANSACTED	FEES	RECEIVED	CONFIRMATIONS
<b>0.02518809 BTC</b>	<b>0.00000647 BTC</b>	<b>3 minutes ago</b>	<b>0/6</b>

Confidence i  
**43.17%**

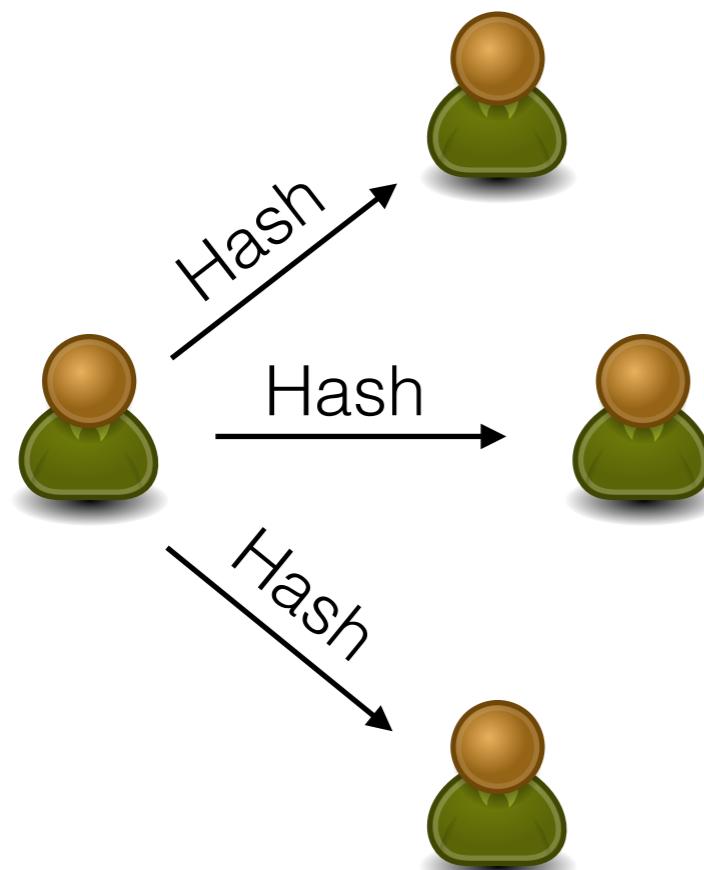
Miner Preference  
**LOW**

Size	266 bytes
Lock Time	
Version	1
Relayed By:	107.20.94.164:8333

[API Call](#) [API Docs](#)

## Remember?

1. Transaction/Block  
hash broadcast

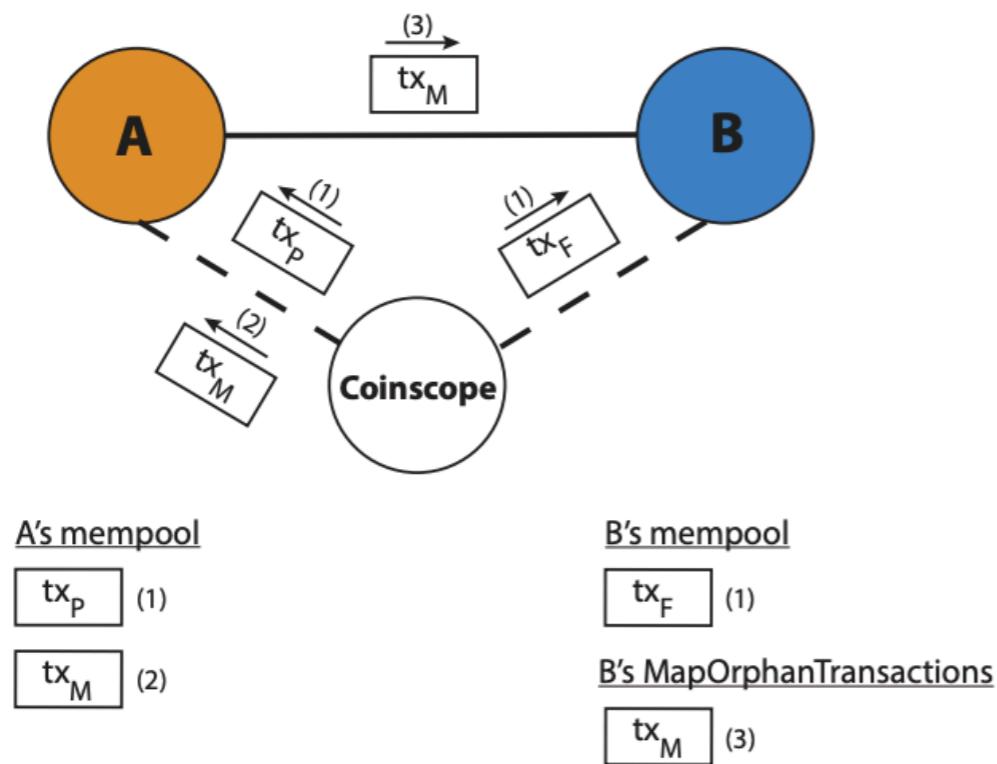


2. Transaction/Block  
request

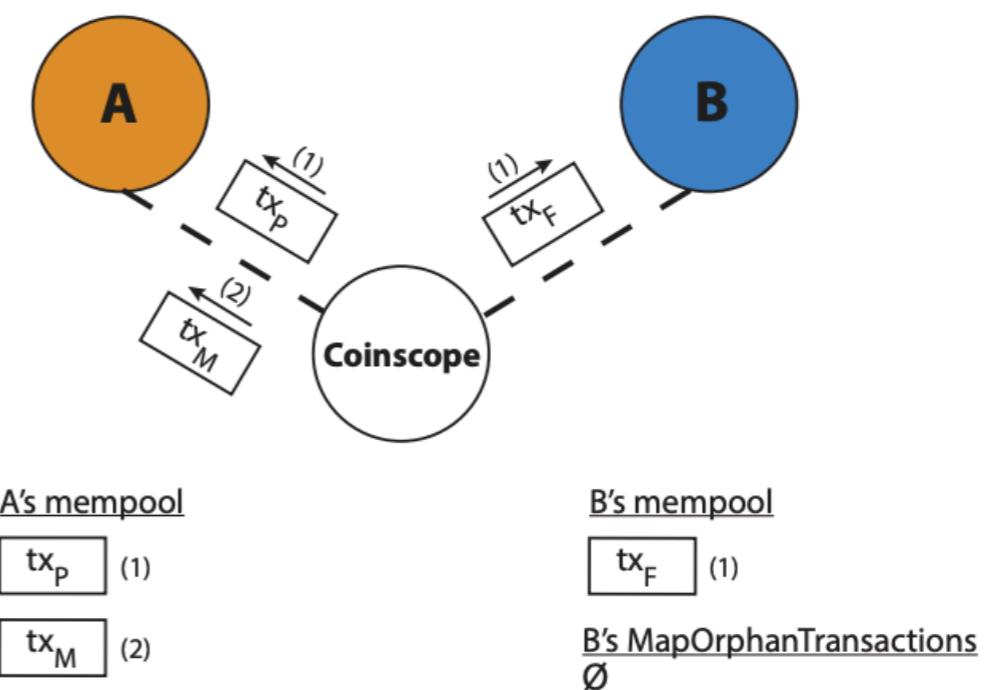


Broadcast

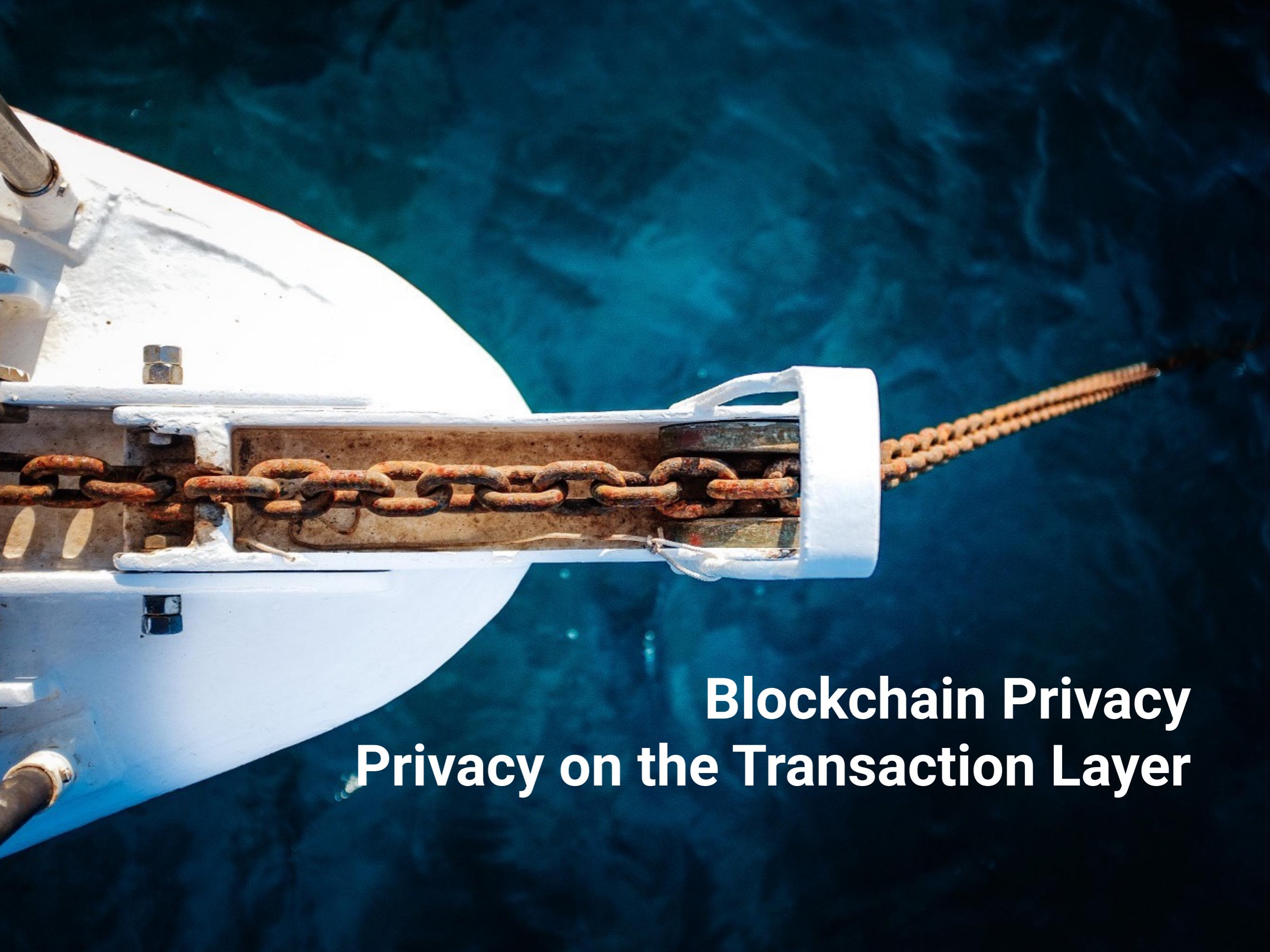
TCP/IP  
Port 8333



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



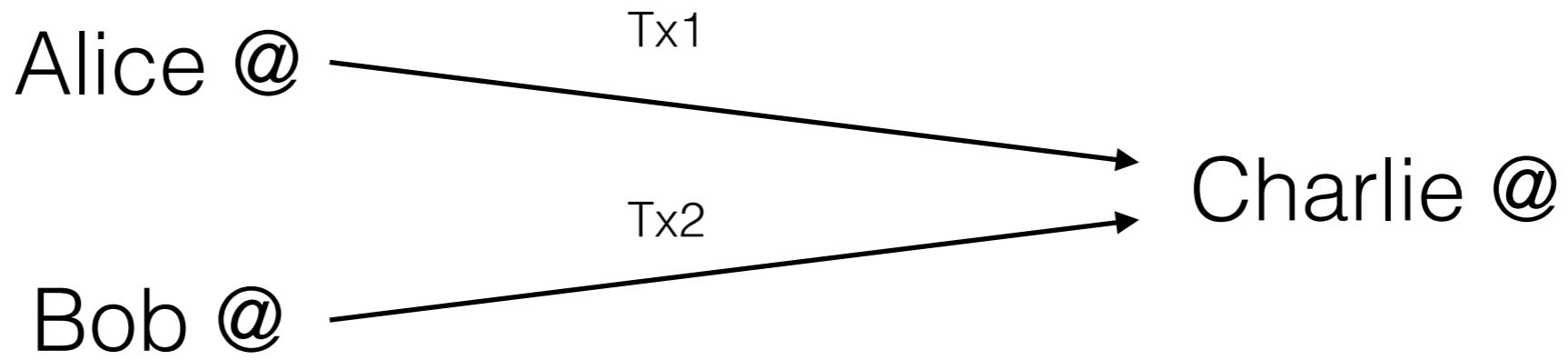
(b) Basic negative edge inferring technique between two nodes.



# Blockchain Privacy

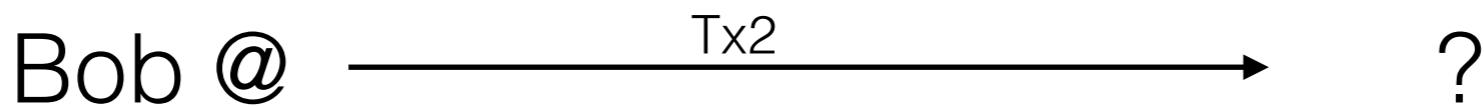
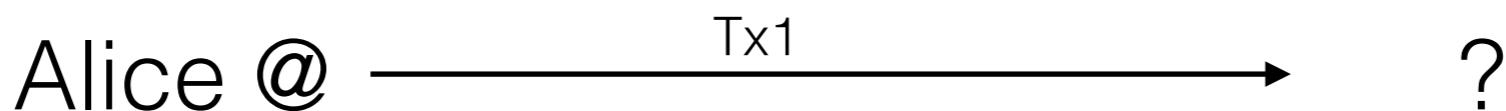
## Privacy on the Transaction Layer

## Linkability



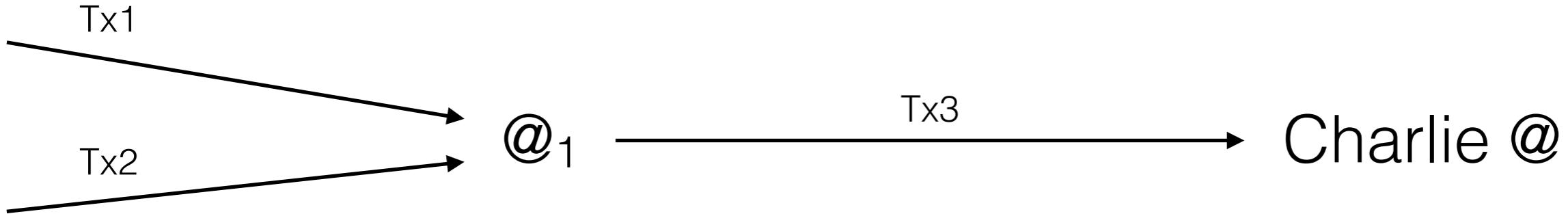
Everybody sees the transactions go to the **same** recipient.

## Unlinkability



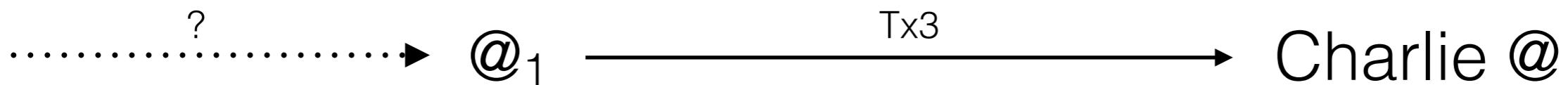
No idea where they go.

## Traceability



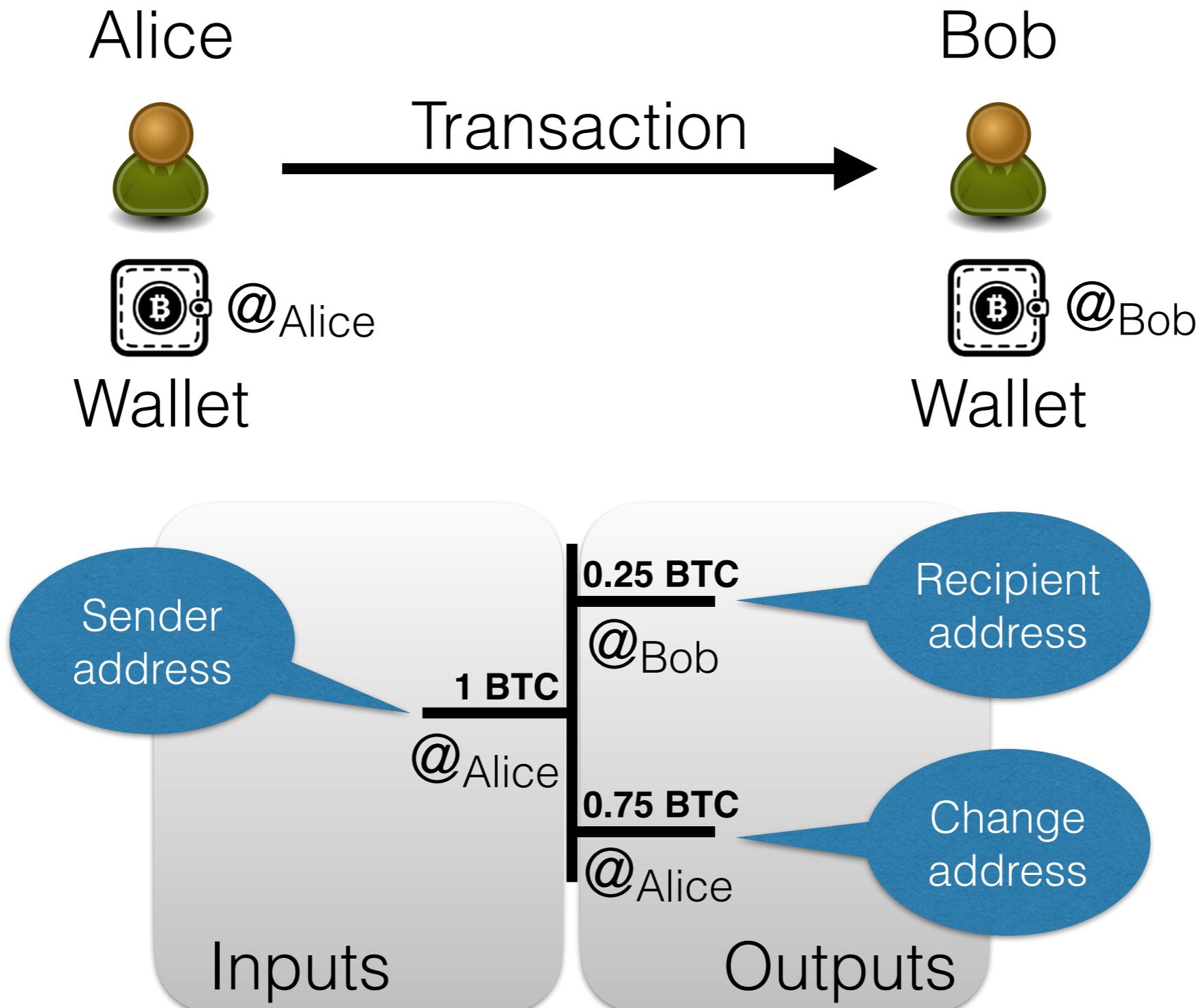
Tx3 spends funds received in Tx1 and Tx2.

## Untraceability

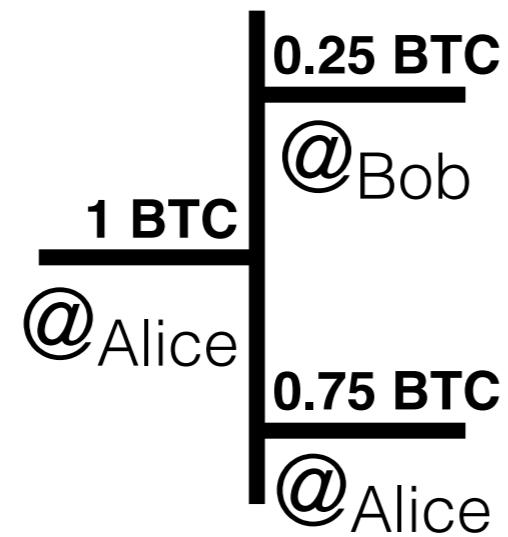


No idea where the funds from Tx3 come from.

# Transactions in Bitcoin (UTXO model)

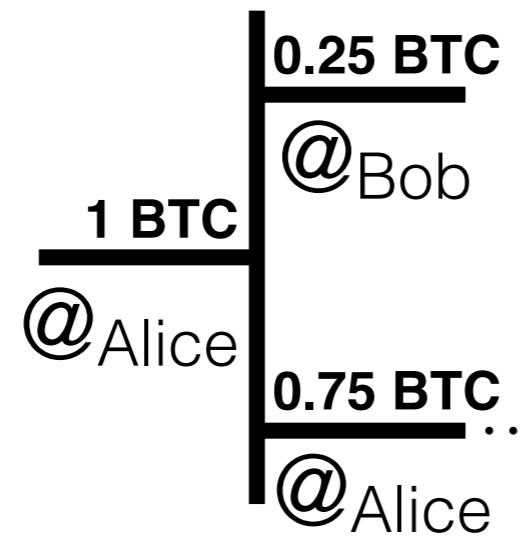


# Transactions in Bitcoin

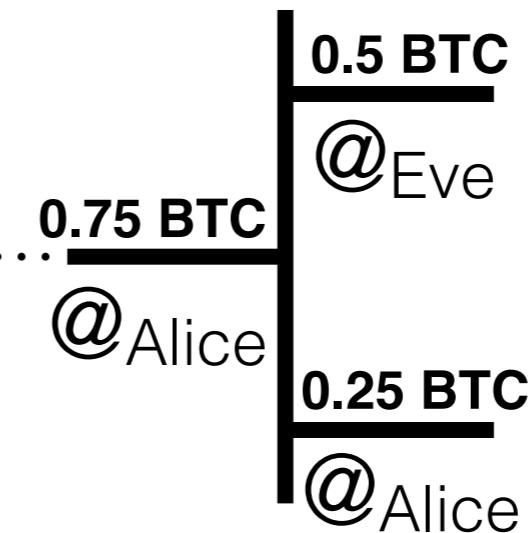


Transaction 1

# Transactions in Bitcoin



Transaction 1



Transaction 2

# Heuristics to Cluster Bitcoin Addresses

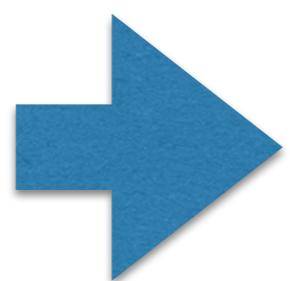
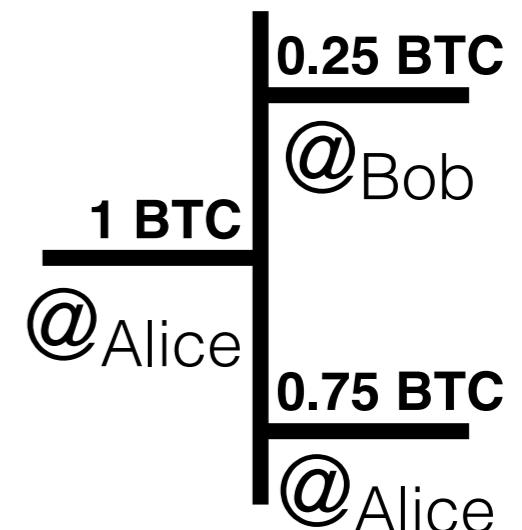


- **Change Address**

If new, then likely a change address

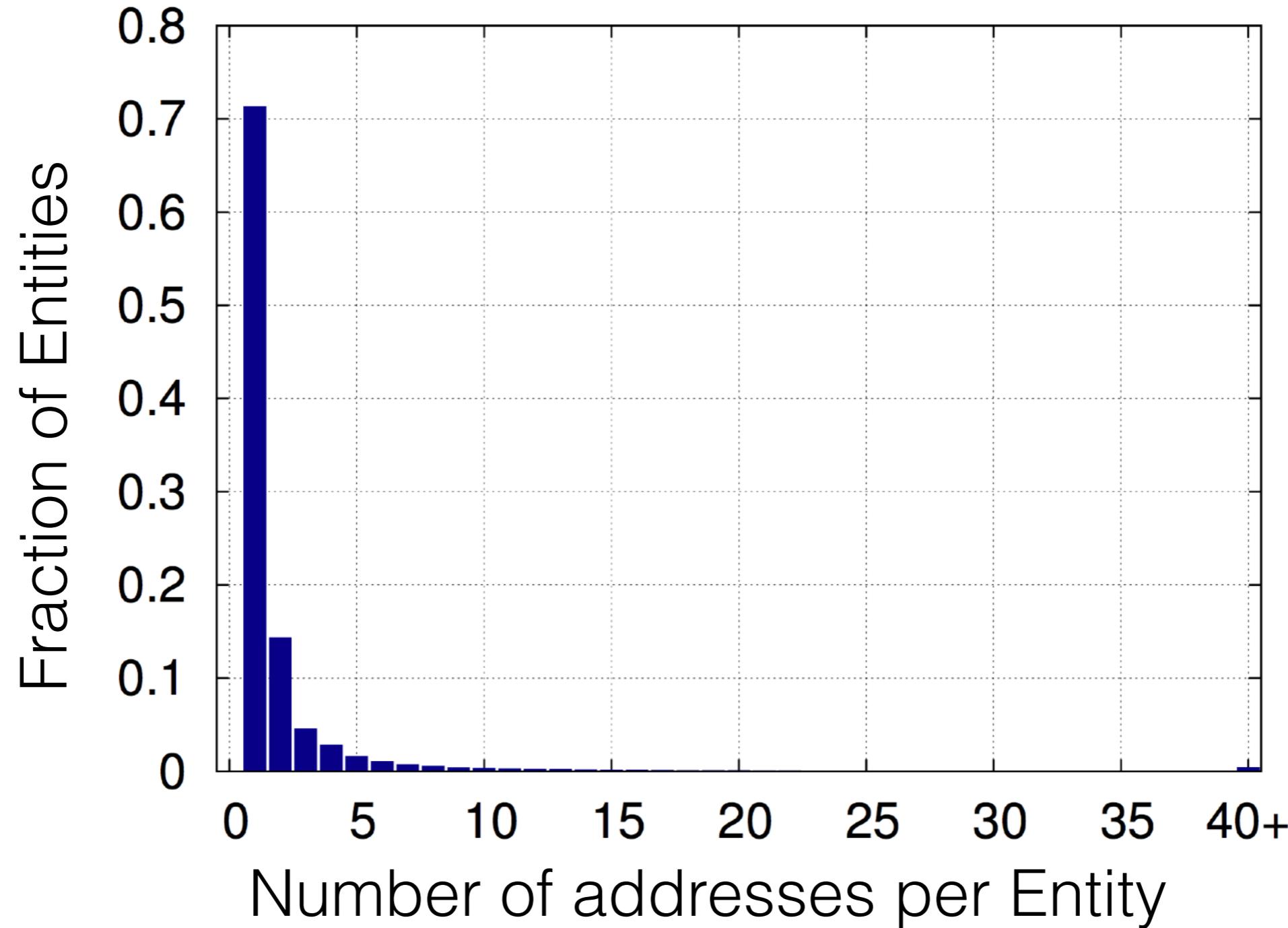
- **Multi-input Transactions**

All inputs can be signed by the same entity.



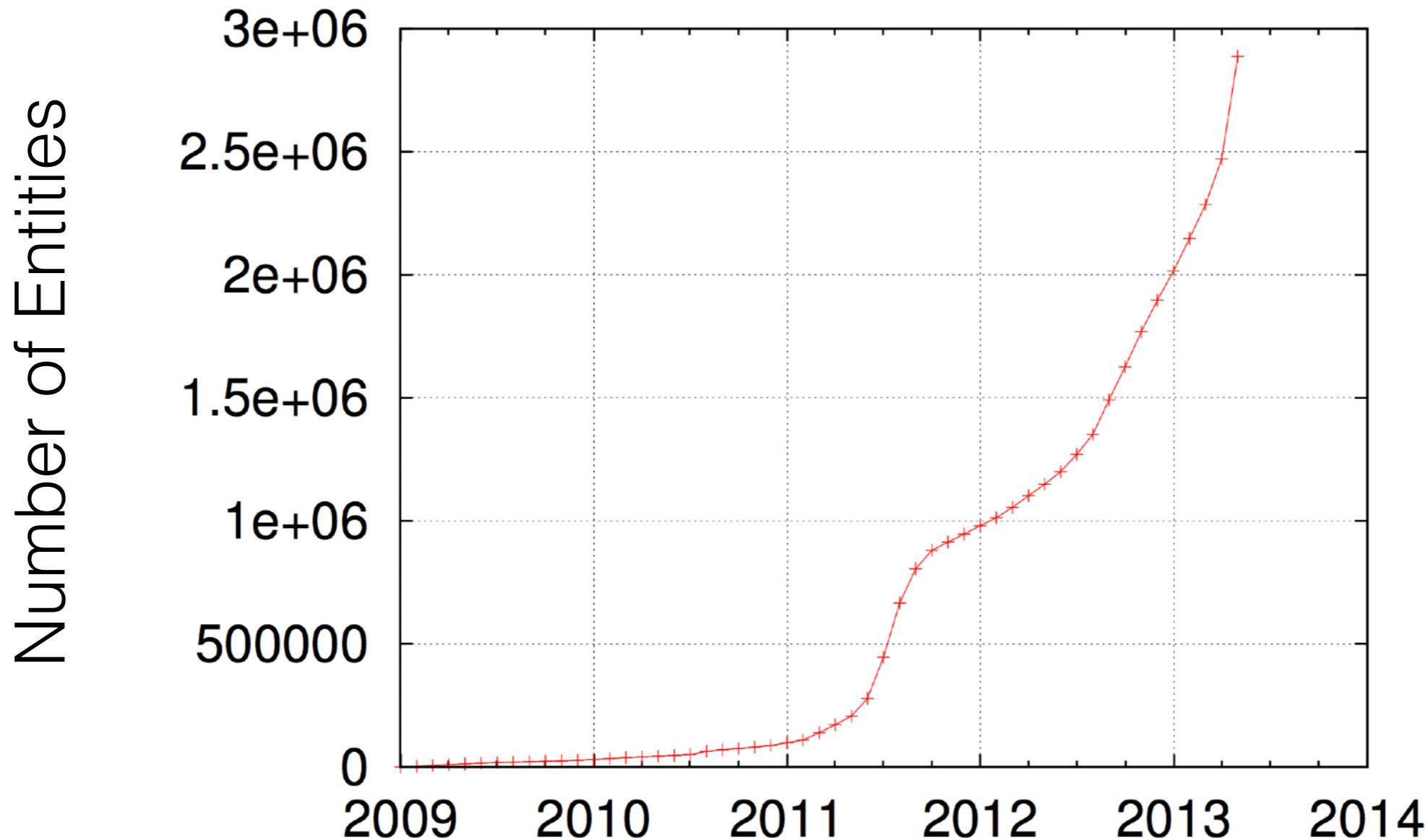
Possible to cluster addresses into cluster that might represent entities

# Entity Cluster

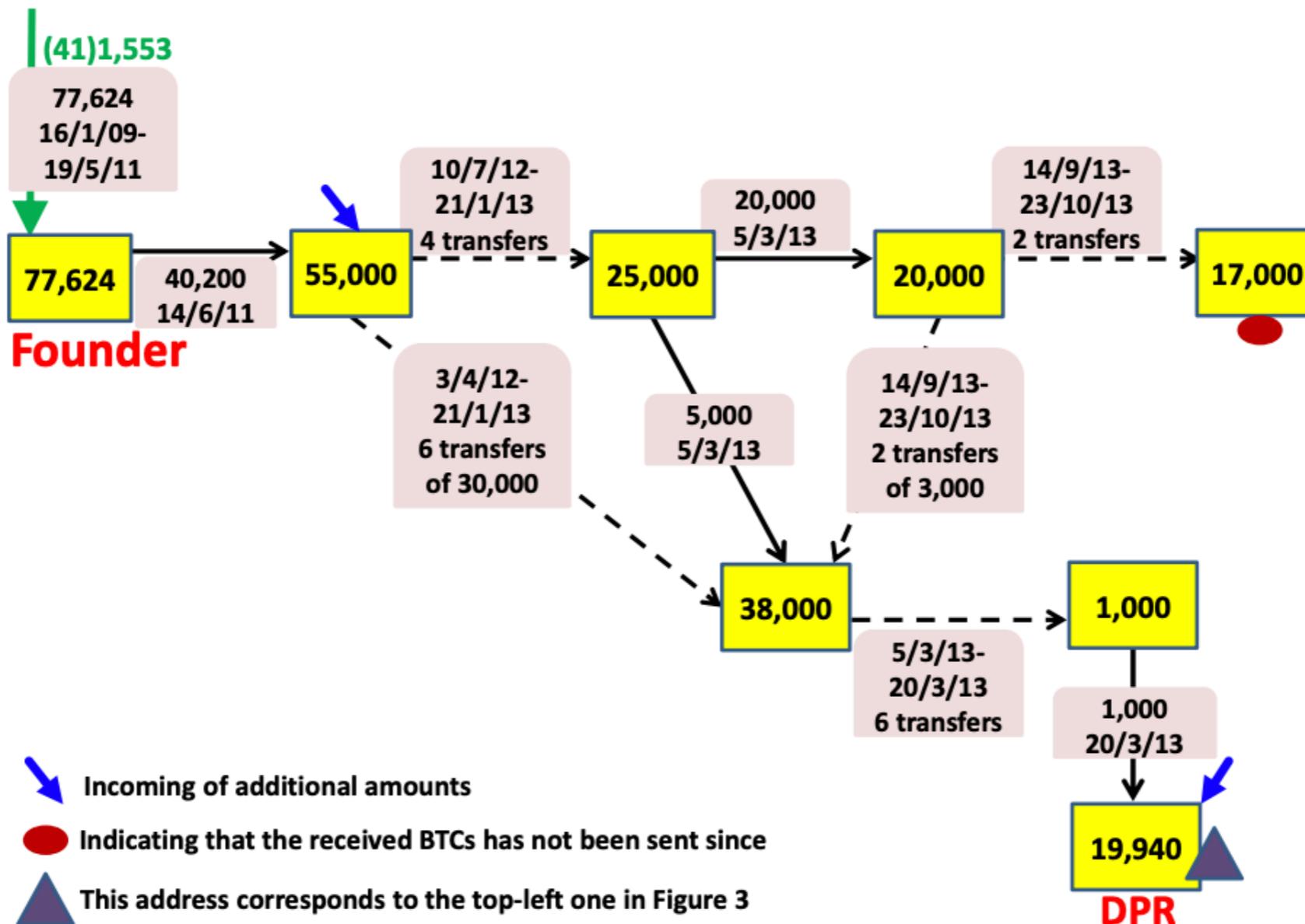


<https://github.com/znort987/blockparser>

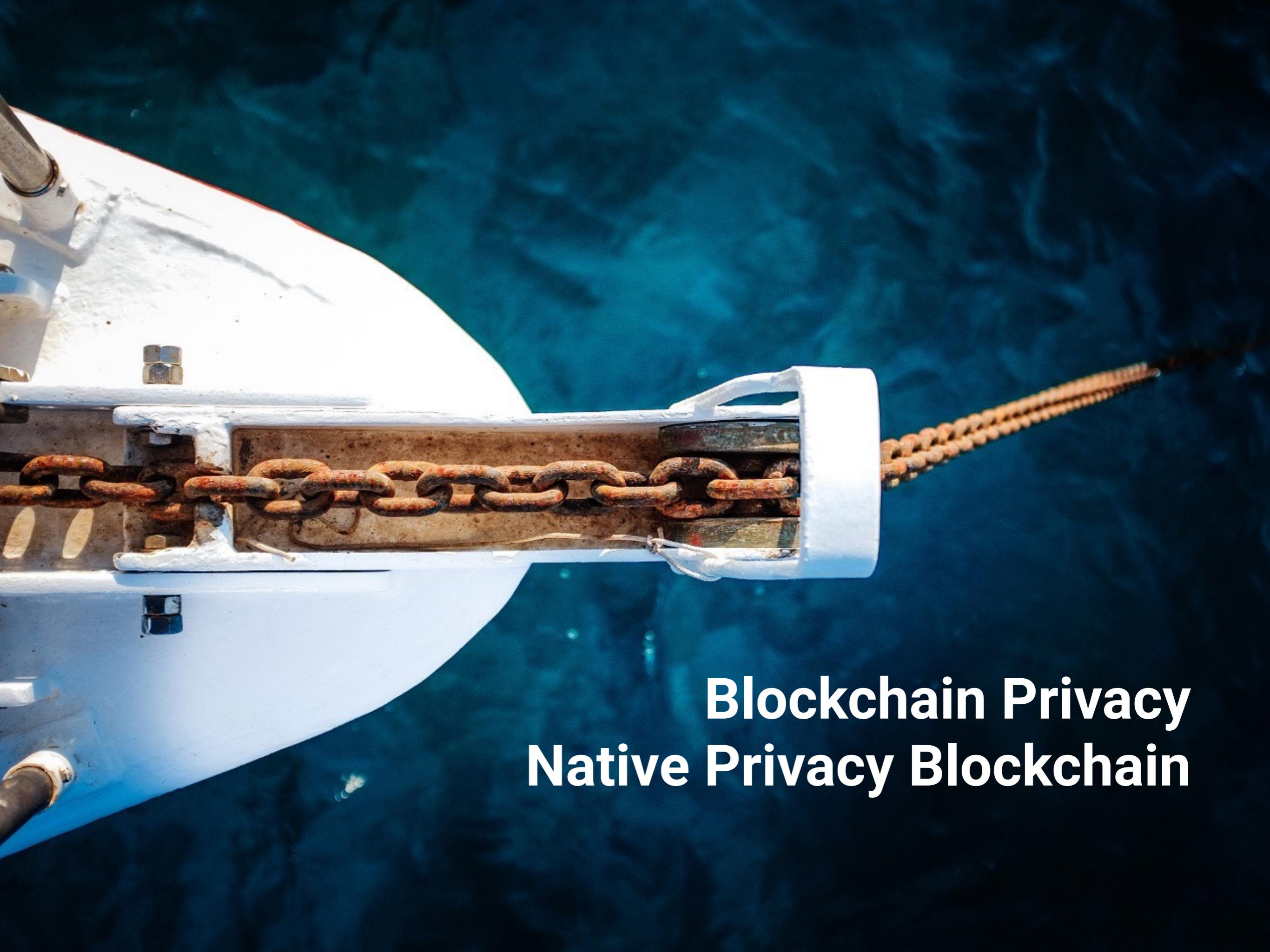
# Entity Evolution over Time



# Easy to trace?

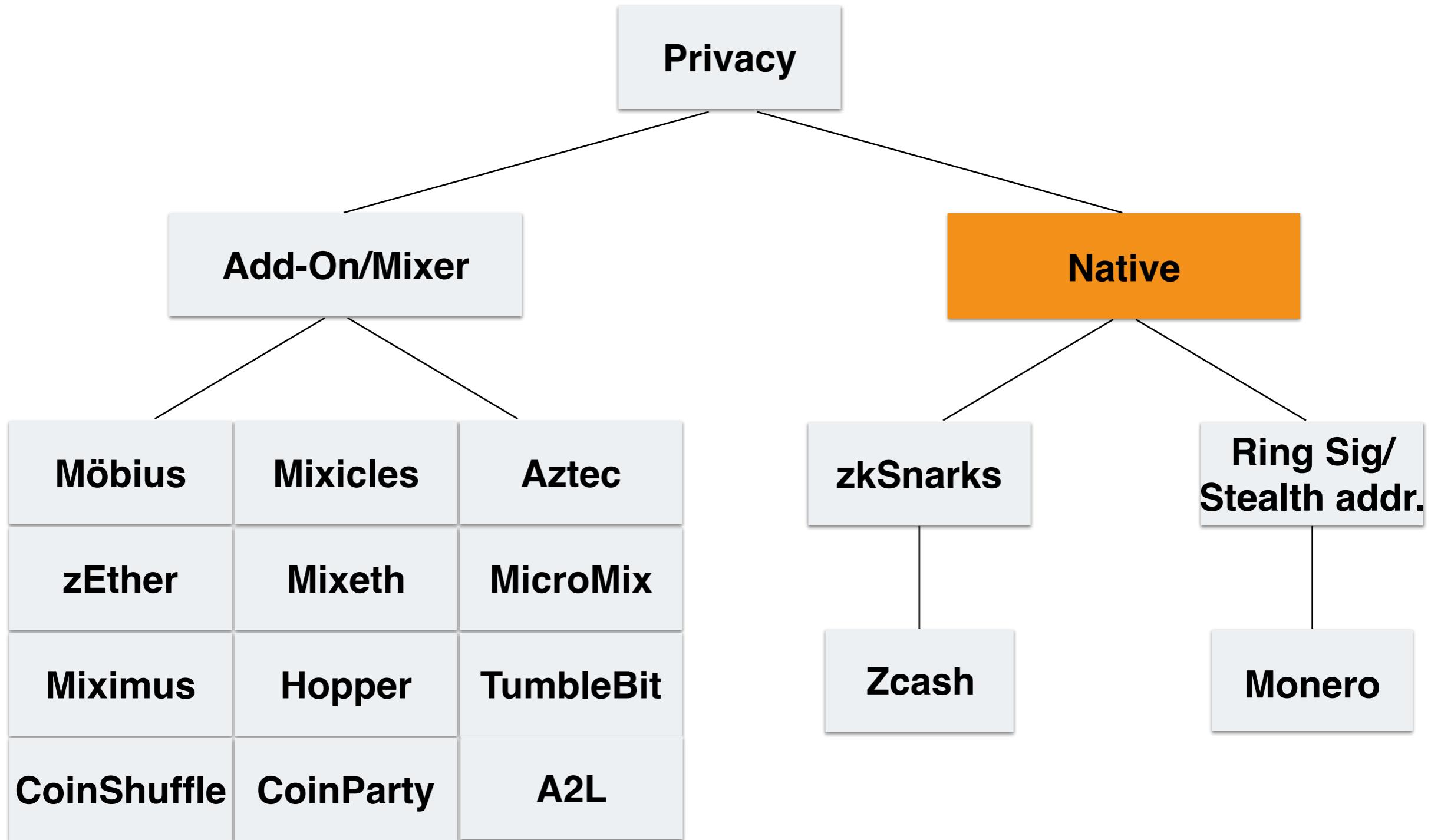


Published by FBI  
After seizing Silk Road server

A close-up photograph of a white boat's hull and a metal chain anchor in the water. The chain is rusted and attached to a metal plate on the hull. The water is dark blue.

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

	<b>Shielding</b>	<b>De-shielding</b>	<b>Shielded</b>
Source	t-addr	z-addr	z-addr
Destination	z-addr	t-addr	z-addr
Amount	Public	Public	Private

# Monero Privacy Features

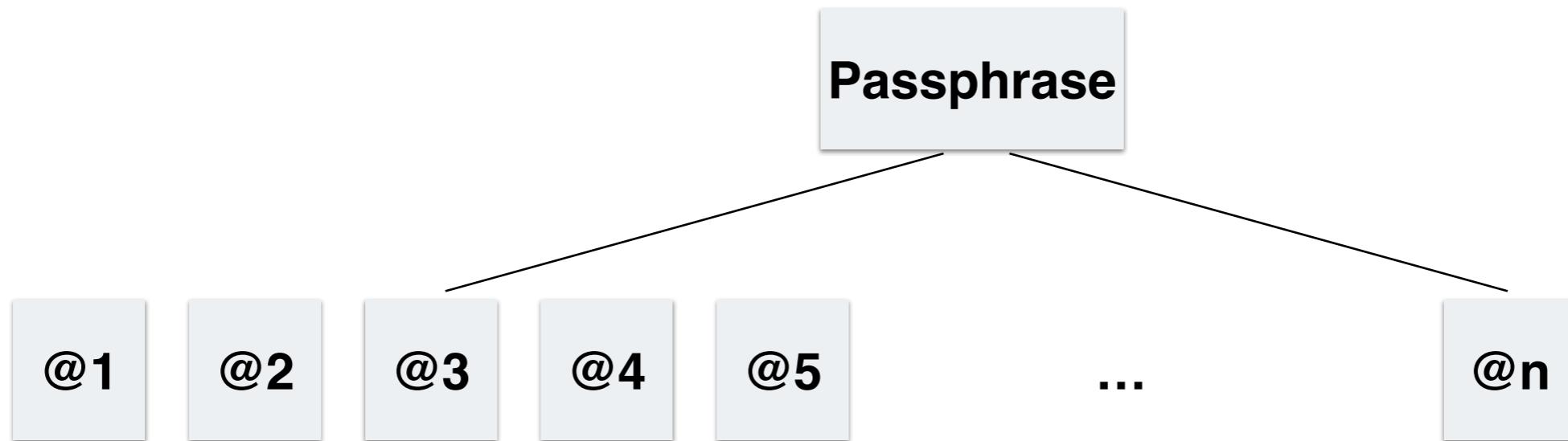


- Unlinkability (destination): Stealth Addresses
- Untraceability (source): Ring Signatures/RingCT

A close-up photograph of a white boat's hull and a metal chain anchor in the water. The chain is rusted and attached to a metal plate on the boat. The water is dark blue.

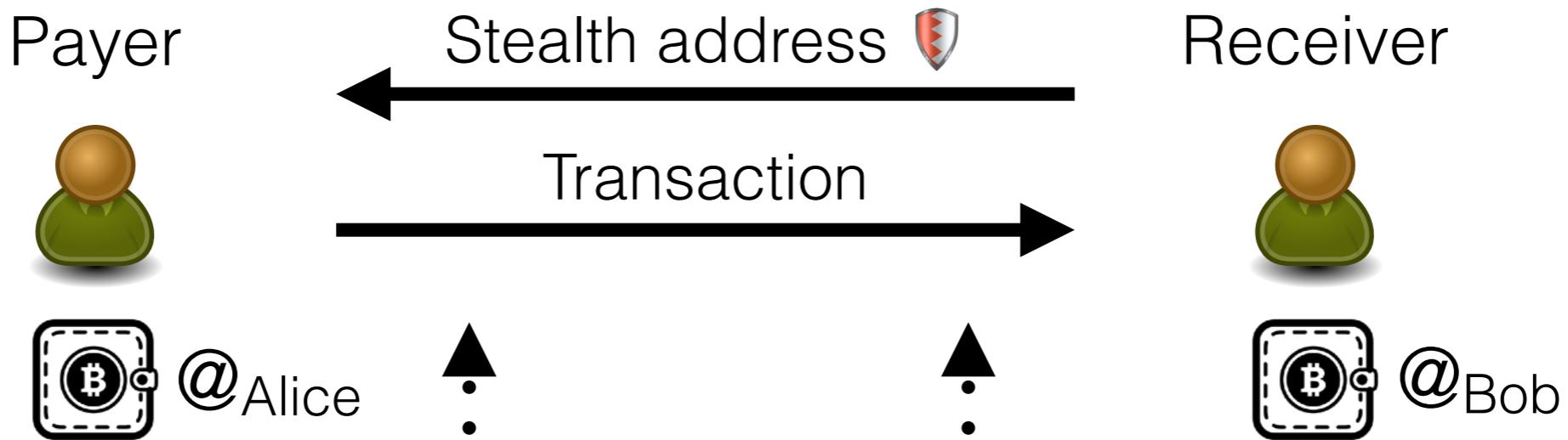
# Blockchain Privacy Stealth Addresses

# 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



## Adversary

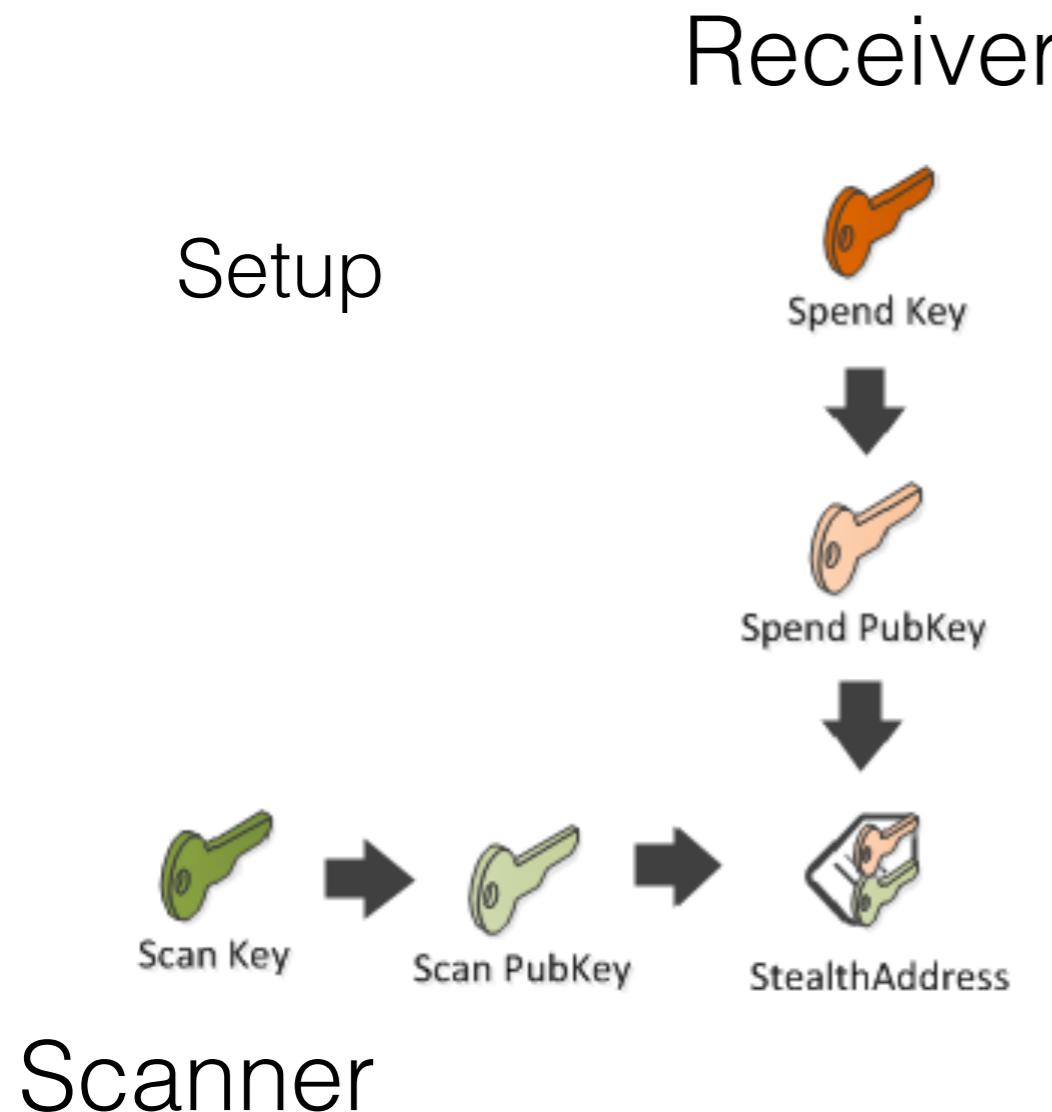
Can't see where  
this transaction  
is paid to :(



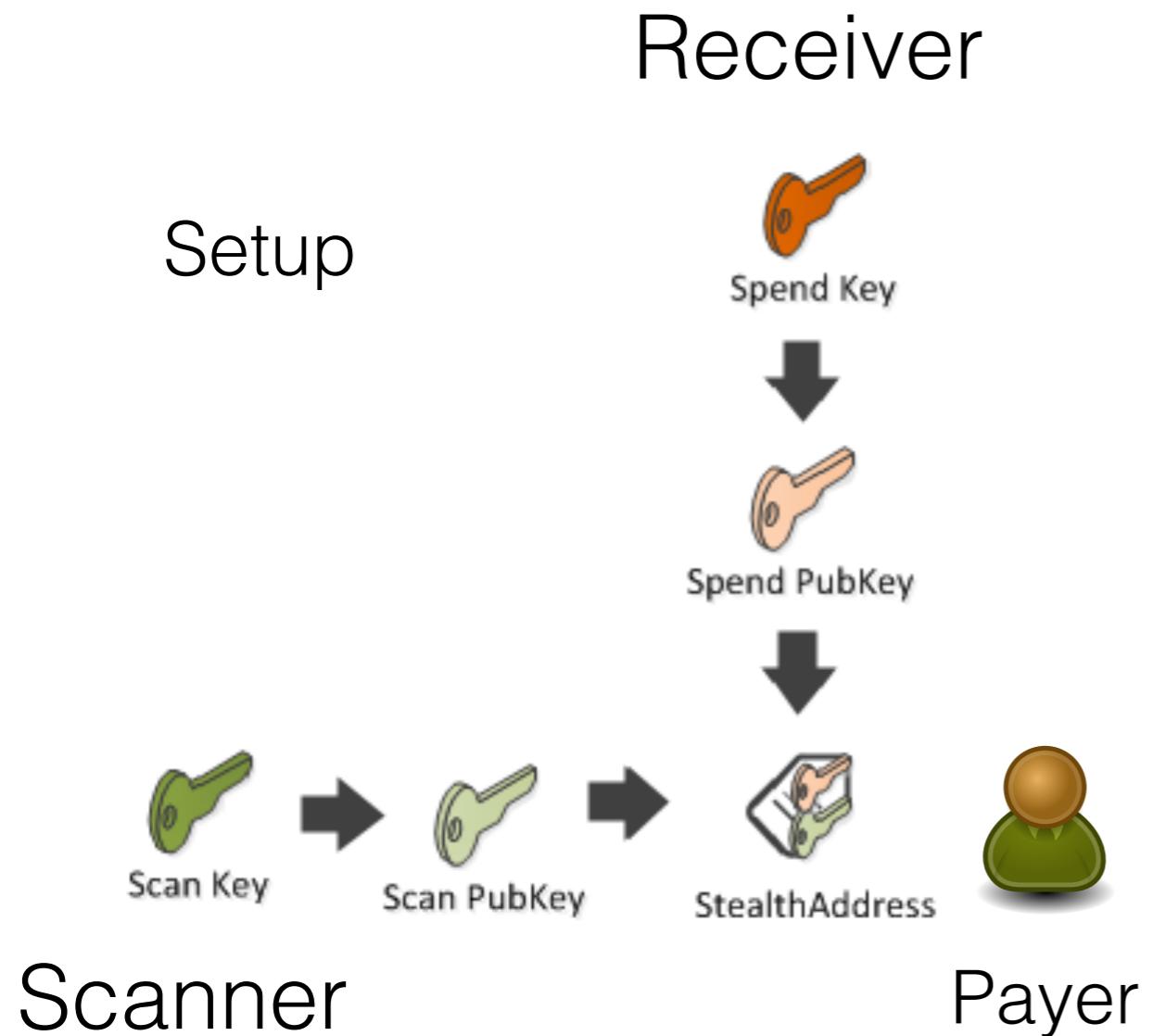
## Scanner

Hehe,  
I can see

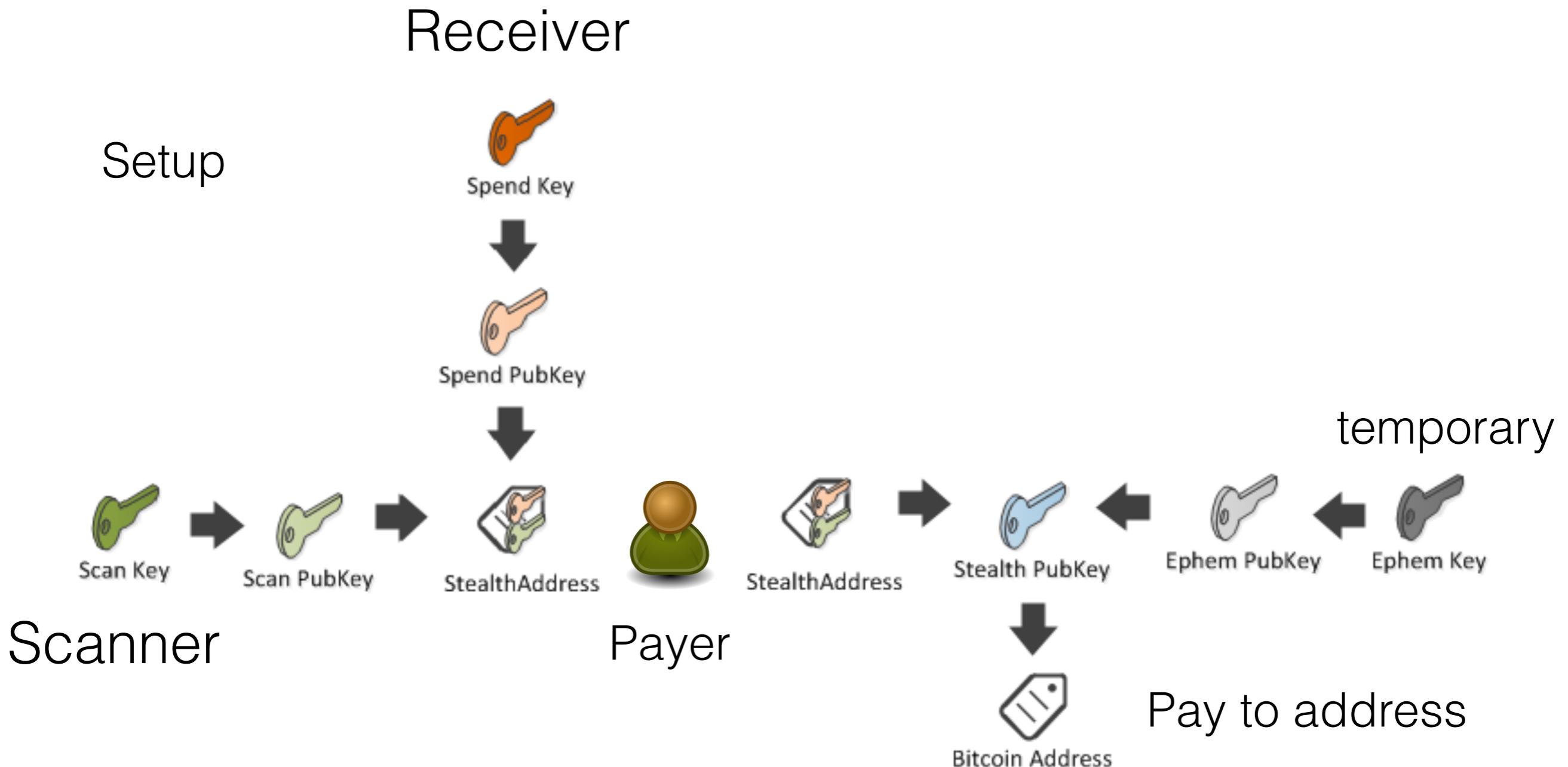
# Stealth Addresses - Paying (Dark Wallet)



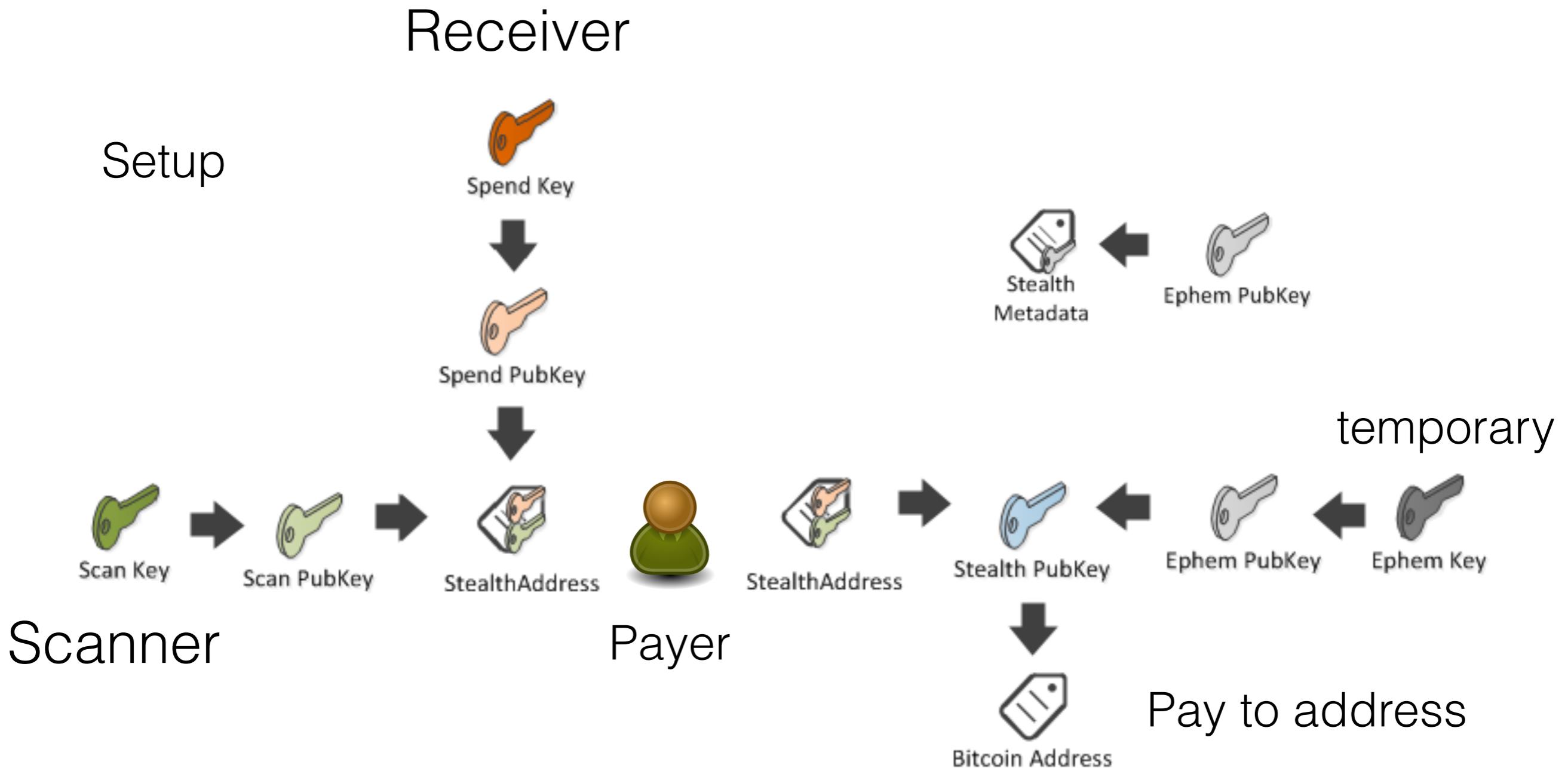
# Stealth Addresses - Paying (Dark Wallet)



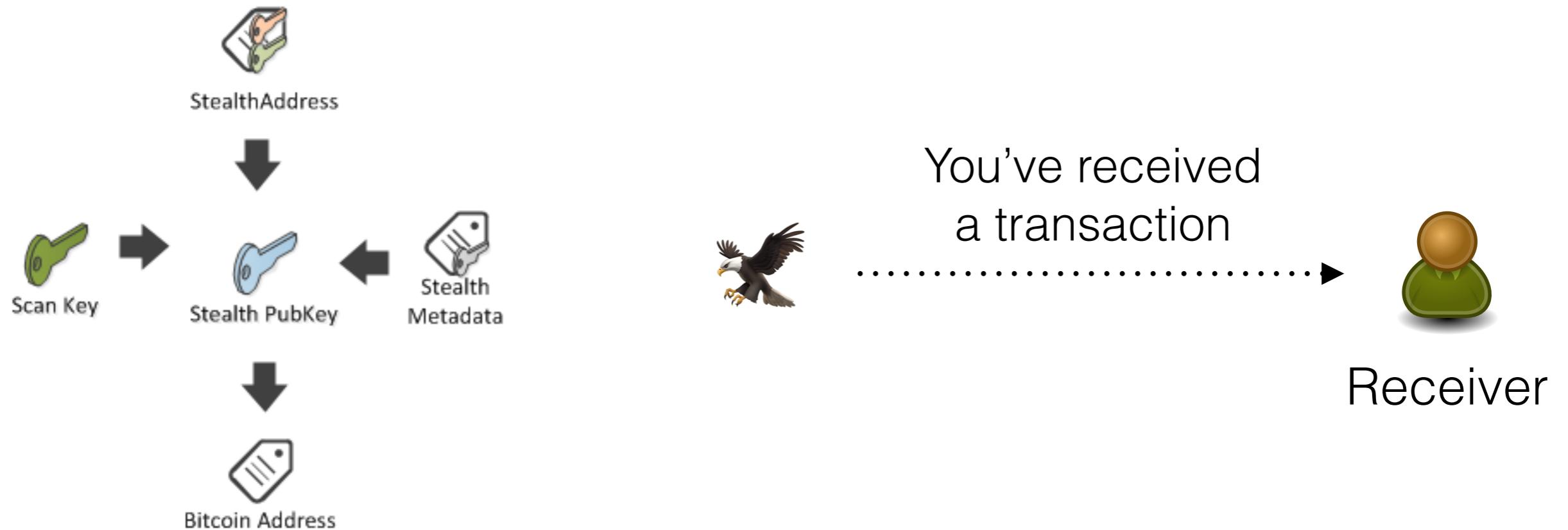
# Stealth Addresses - Paying (Dark Wallet)



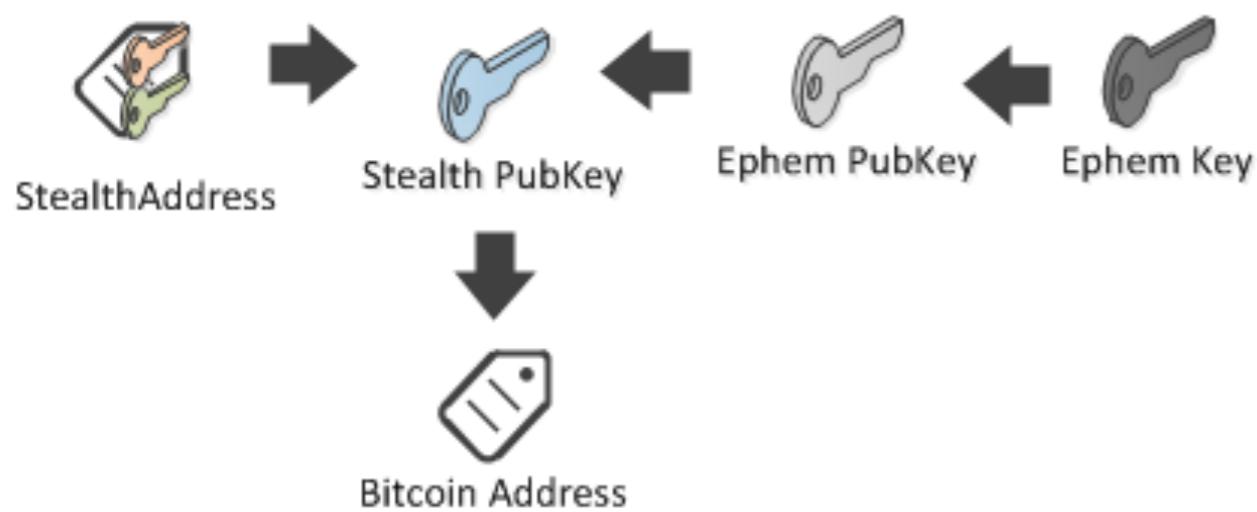
# Stealth Addresses - Paying (Dark Wallet)



# Stealth Addresses - Receiving

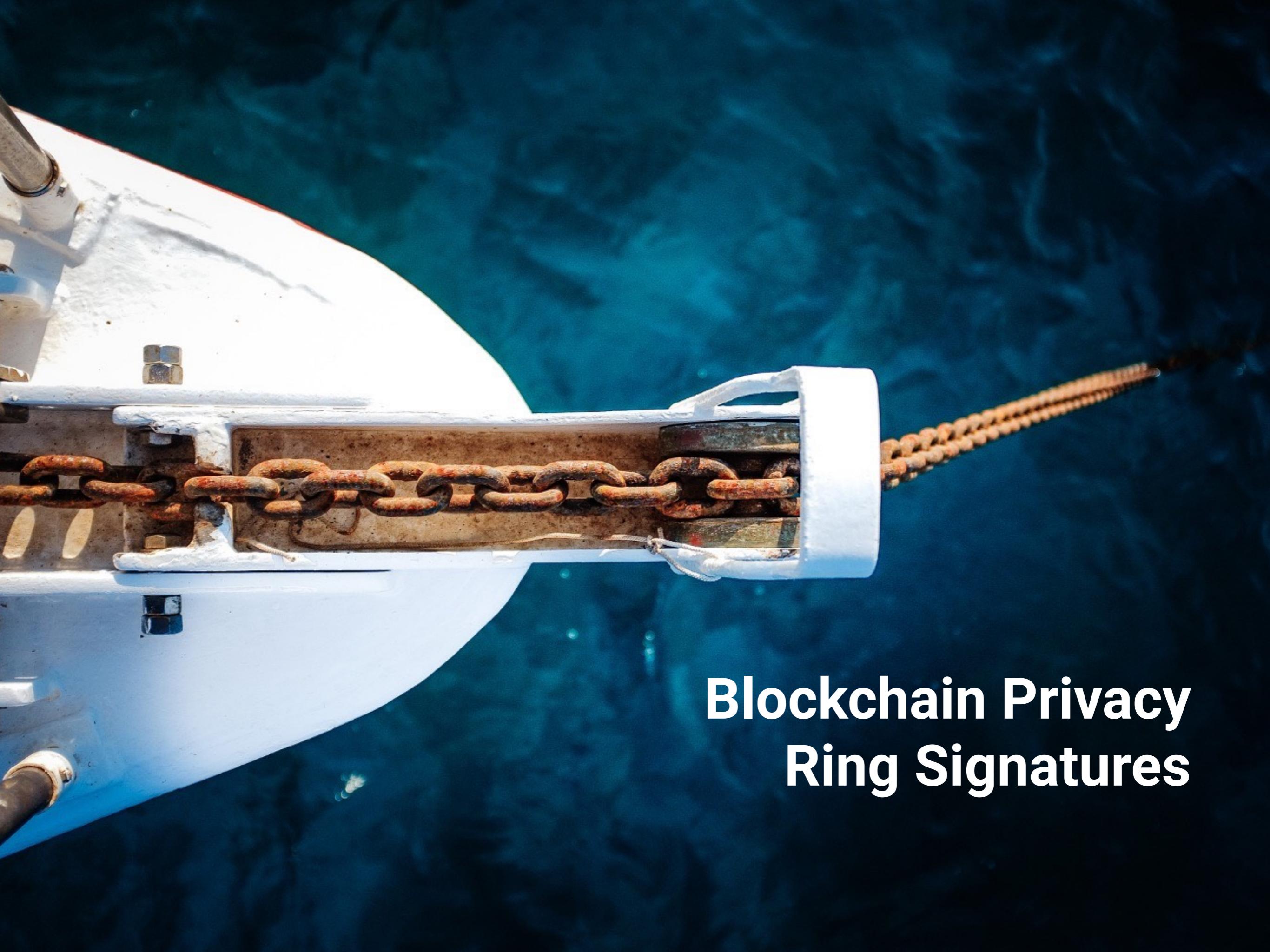


# Stealth Addresses - Spending



# Stealth Addresses - Spending





# Blockchain Privacy Ring Signatures

# Ring Signatures - Rivest, Shamir, Tauman



## Signature solutions:

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

# “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).

# “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

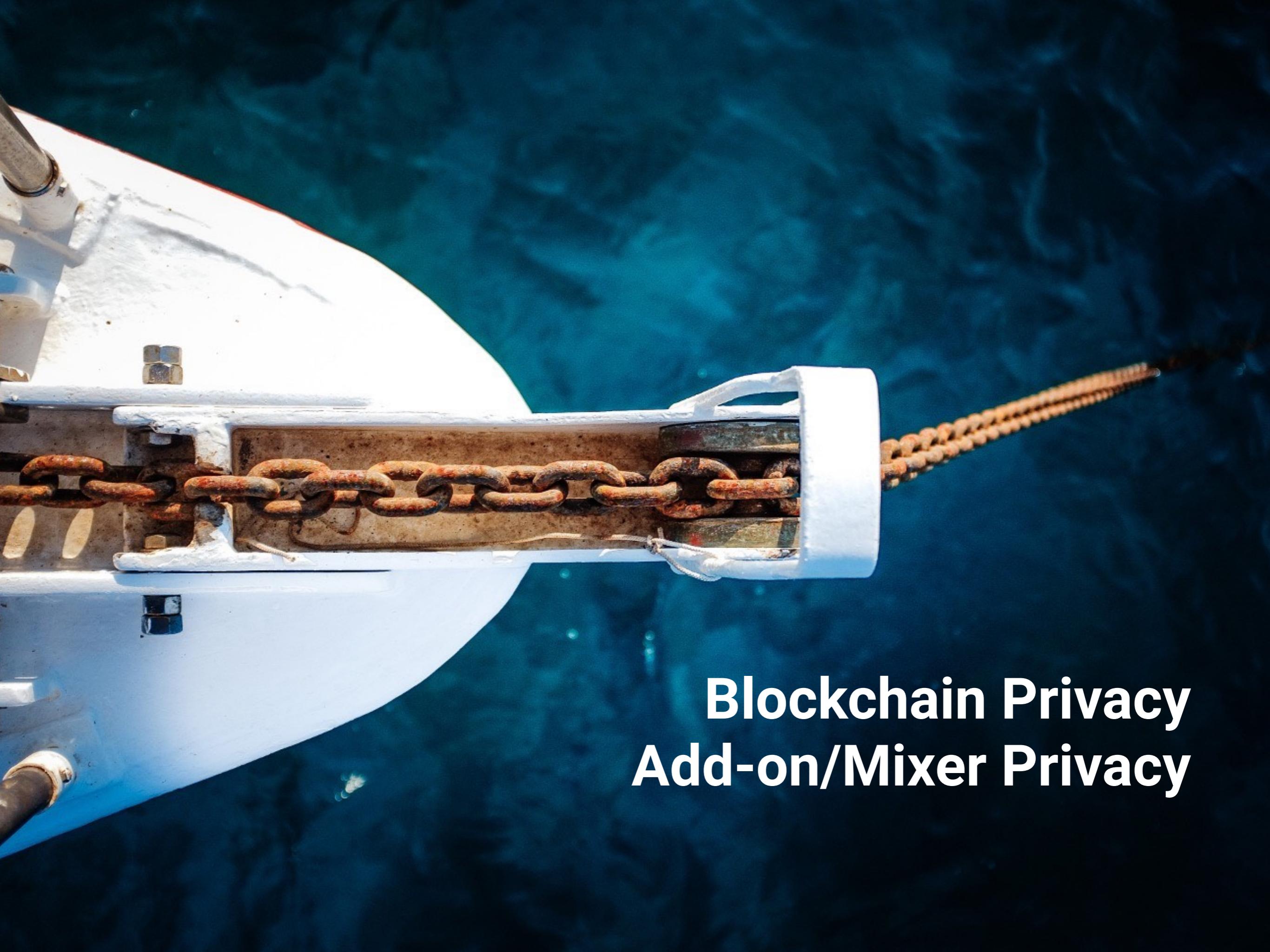
- Verify against **a set** of public keys. Computationally infeasible to determine which of the group members signed.
- Groups can be formed on an ad-hoc basis (vs. group signatures)
- $O(n)$  for the resulting signature size  
 $n$  == number of public keys
- Does not hide transaction amounts!

# 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
- Does not hide transaction amounts!

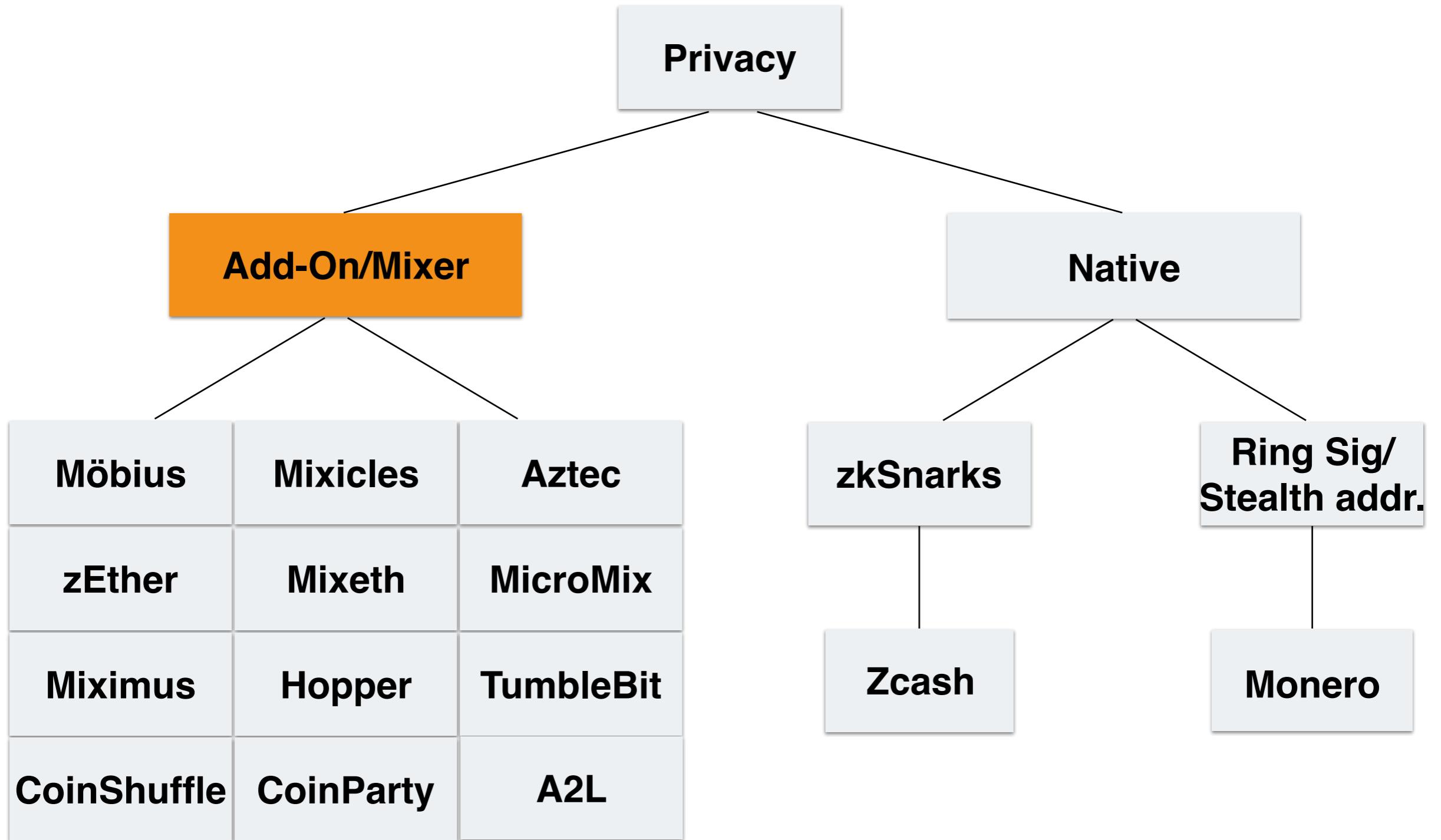


<https://www.getmonero.org/resources/research-lab/pubs/MRL-0005.pdf>

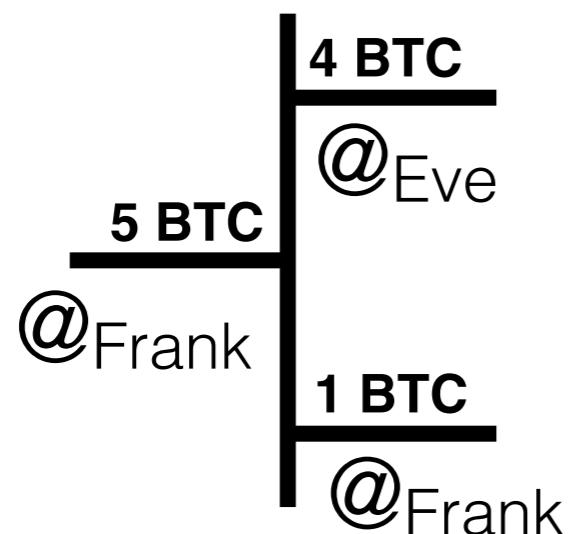
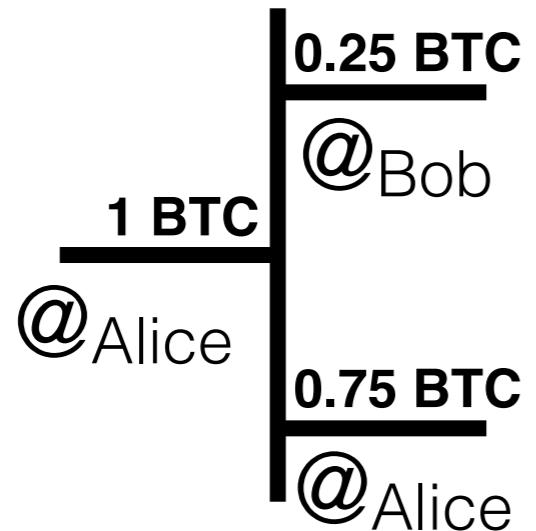


# Blockchain Privacy Add-on/Mixer Privacy

# Blockchain Privacy Solutions

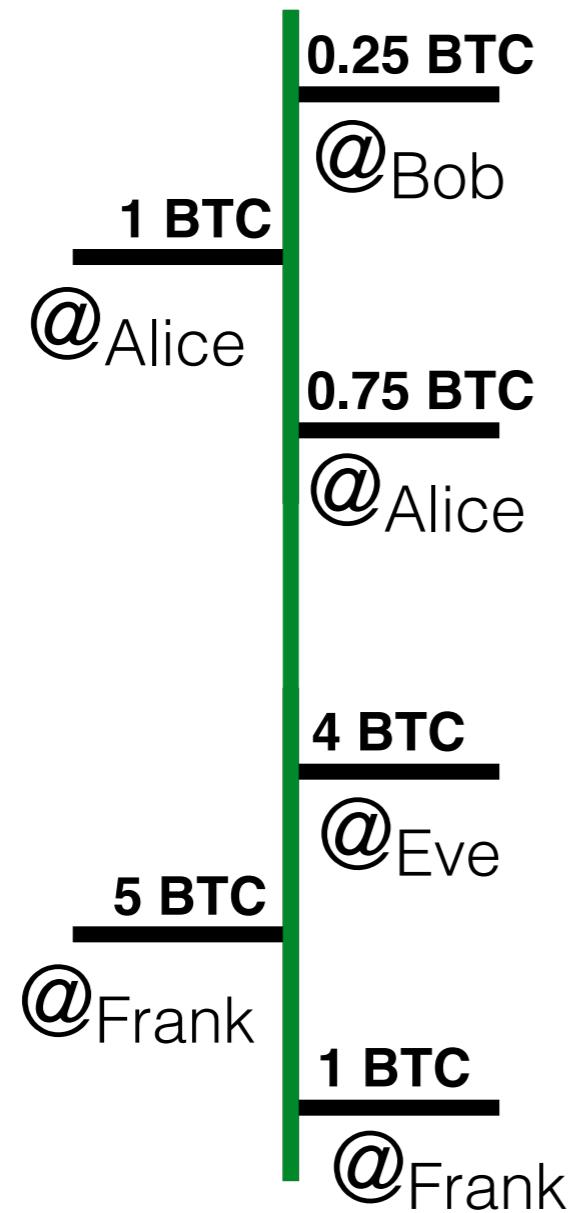


# CoinJoin



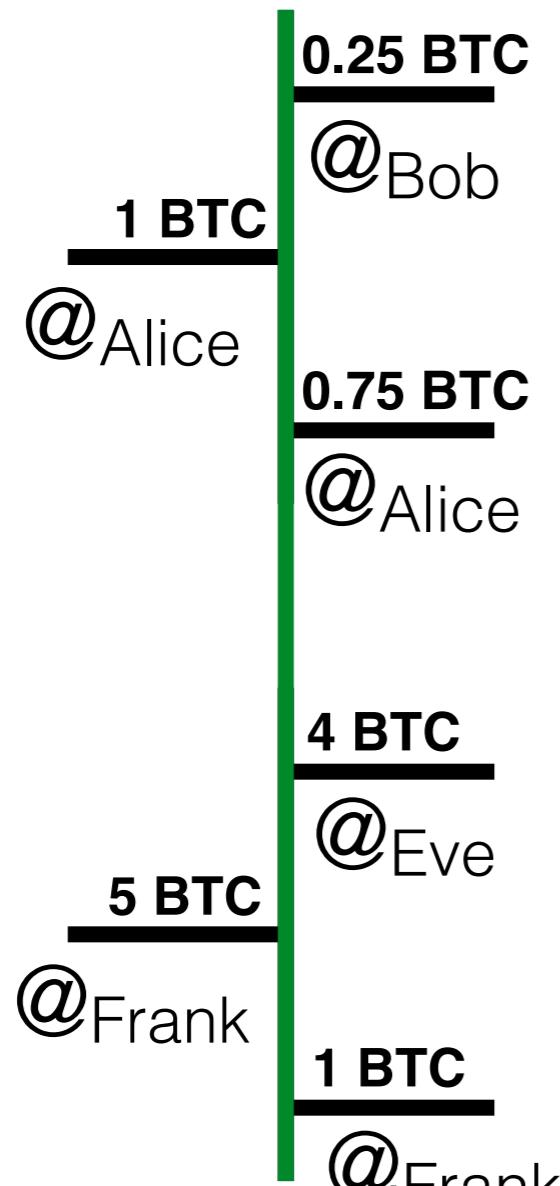
Transaction

# CoinJoin



Transaction

# CoinJoin



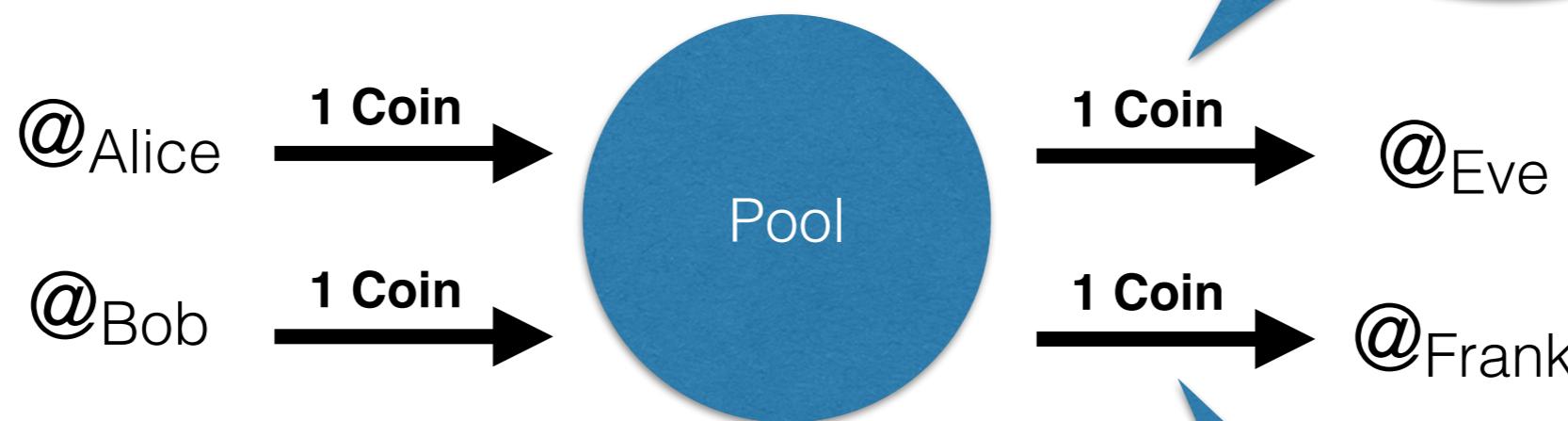
## Advantages 🤝

- Hides the originator of a transaction

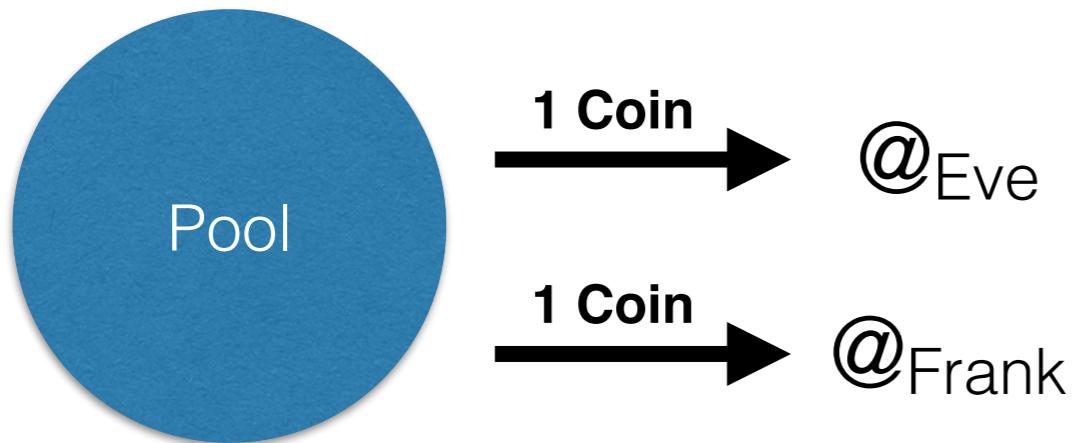
## Drawbacks 🤢

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

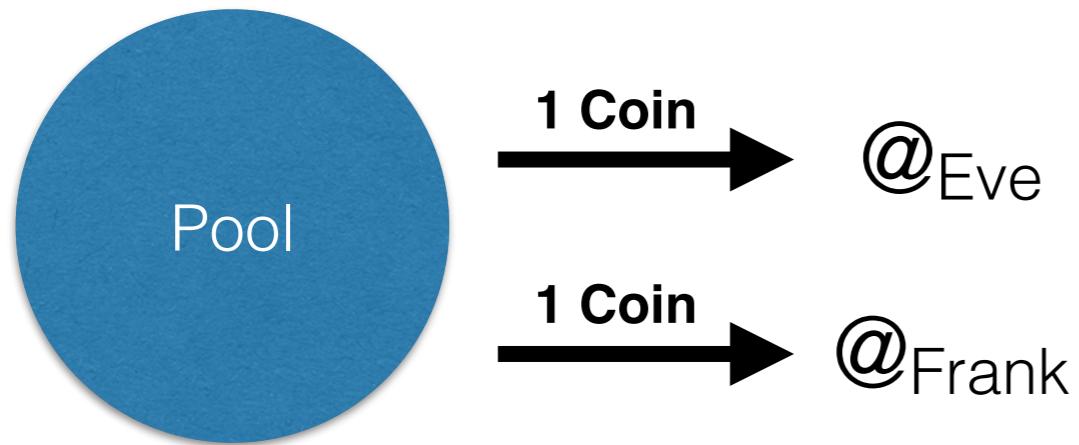
## Tornado Cash/Miximus/MicroMix



# Tornado Cash/Miximus/MicroMix



# 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

A close-up photograph of a white boat's hull and a metal chain anchor in dark blue water. The chain is attached to a metal plate on the hull. The water is dark and reflects the light from the boat.

# Blockchain Privacy Lightweight Clients

# Blockchain Broadcast Data Model

1. Log of transactions (>300 GB)



2. Mobile phones receive irrelevant transactions

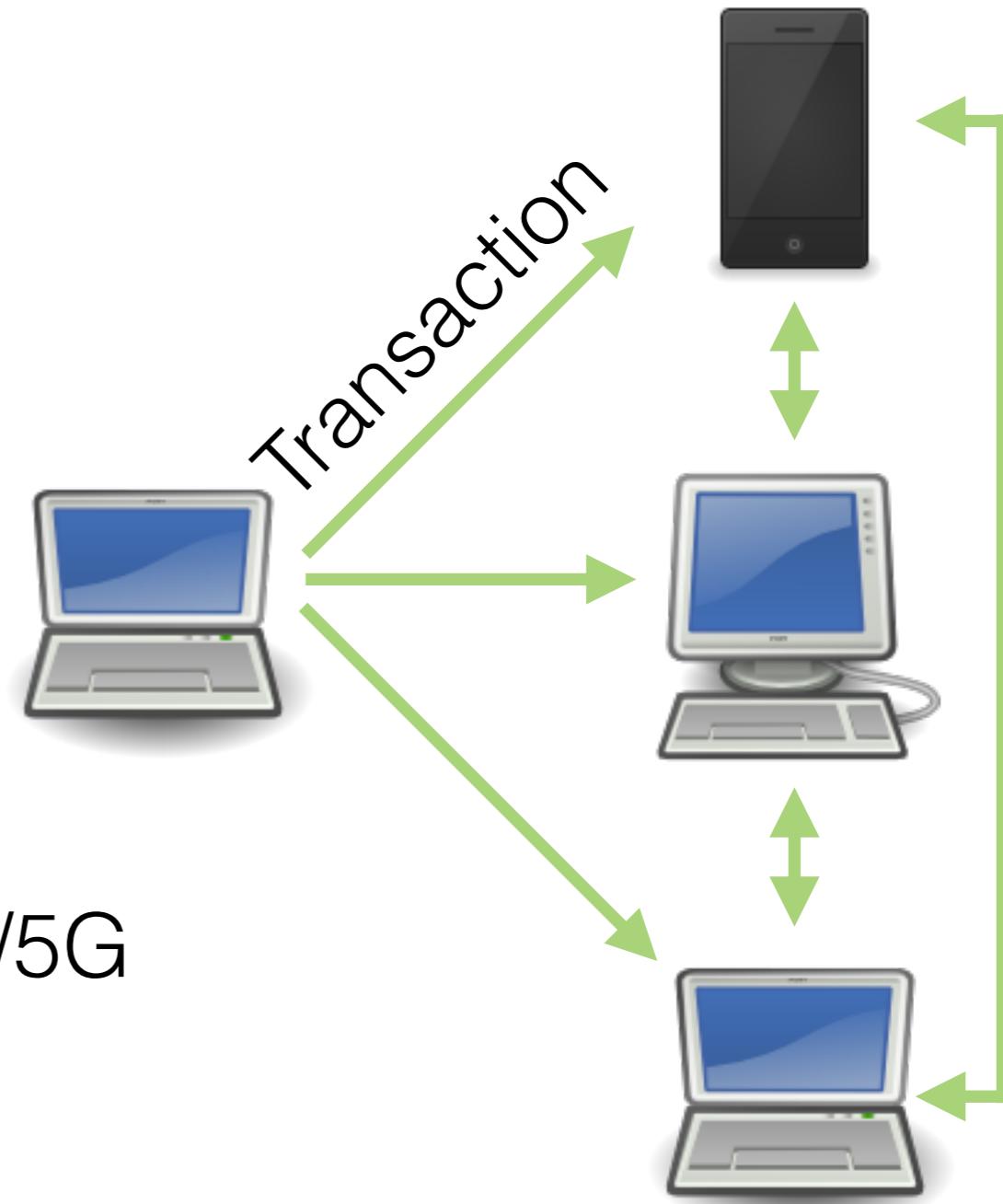


3. Limited data traffic over 3G/4G/5G



## 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

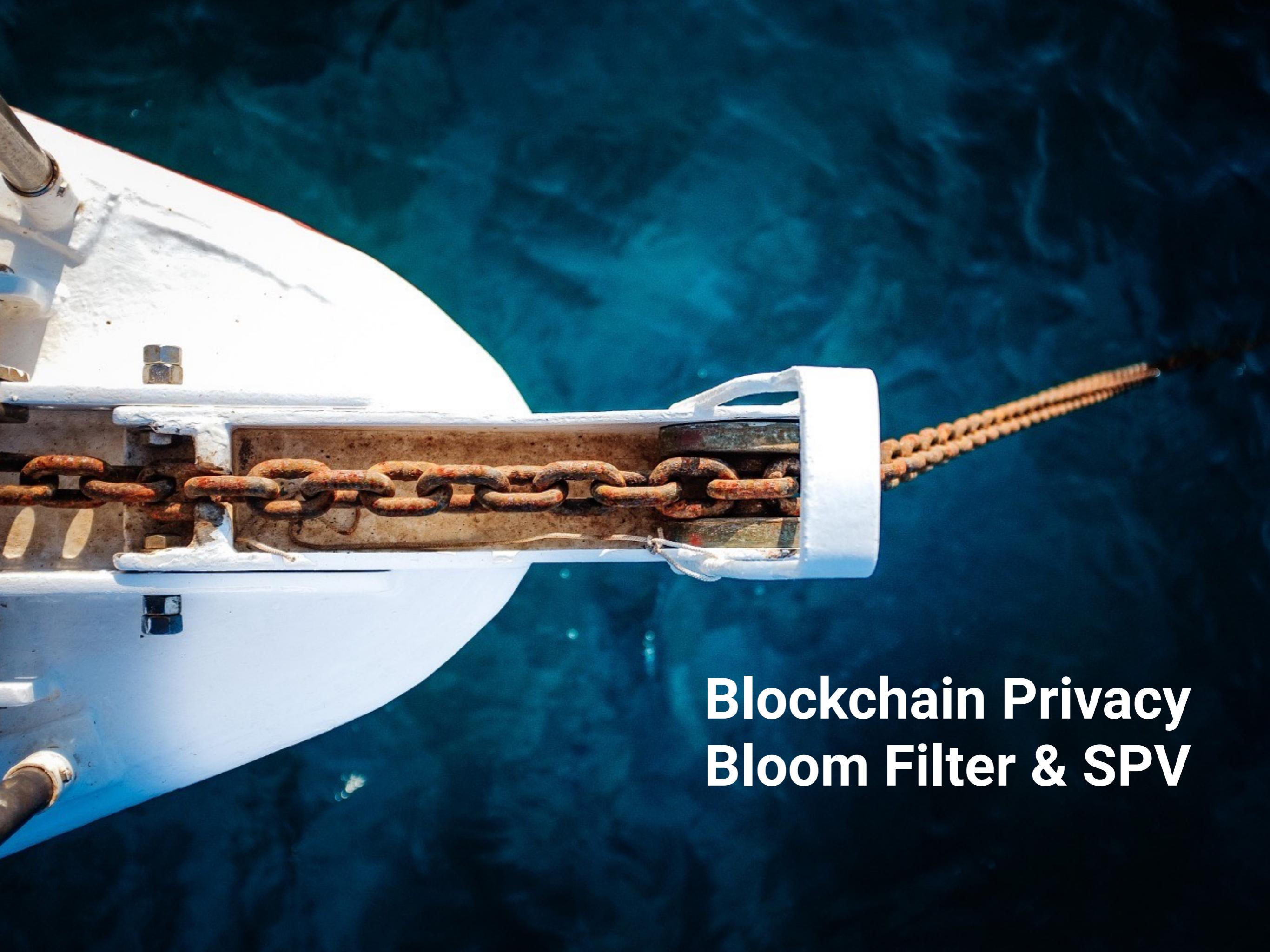


Bitcoin lightweight client implementation

3. Trusted Execution Environment



Bite or Zlite



# Blockchain Privacy Bloom Filter & SPV

# Enable mobile Bitcoin clients

Bloom filter

0	0	0	0	0	0	0
---	---	---	---	---	---	---

# Enable mobile Bitcoin clients

Insertion

{ @<sub>1</sub>, @<sub>2</sub>, @<sub>3</sub> }

Bloom filter

0	0	0	0	0	0	0
---	---	---	---	---	---	---

# Enable mobile Bitcoin clients

Insertion

Bloom filter

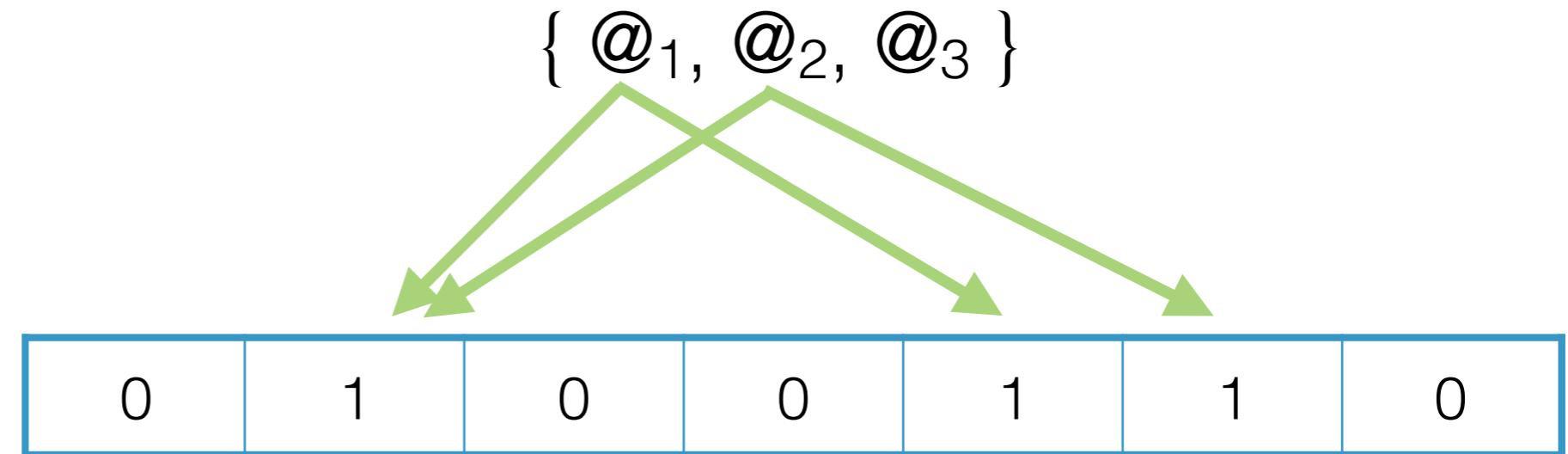
$\{ @_1, @_2, @_3 \}$



# Enable mobile Bitcoin clients

Insertion

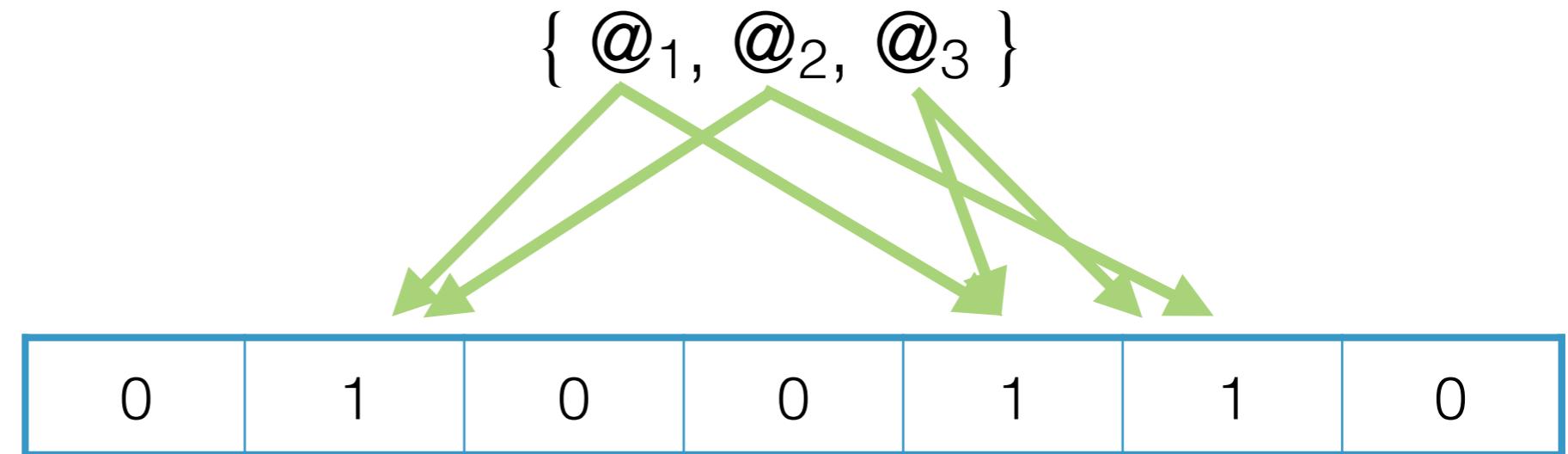
Bloom filter



# Enable mobile Bitcoin clients

Insertion

Bloom filter



# Enable mobile Bitcoin clients

Insertion

$\{ @_1, @_2, @_3 \}$



Bloom filter

0	1	0	0	1	1	0
---	---	---	---	---	---	---

Membership test

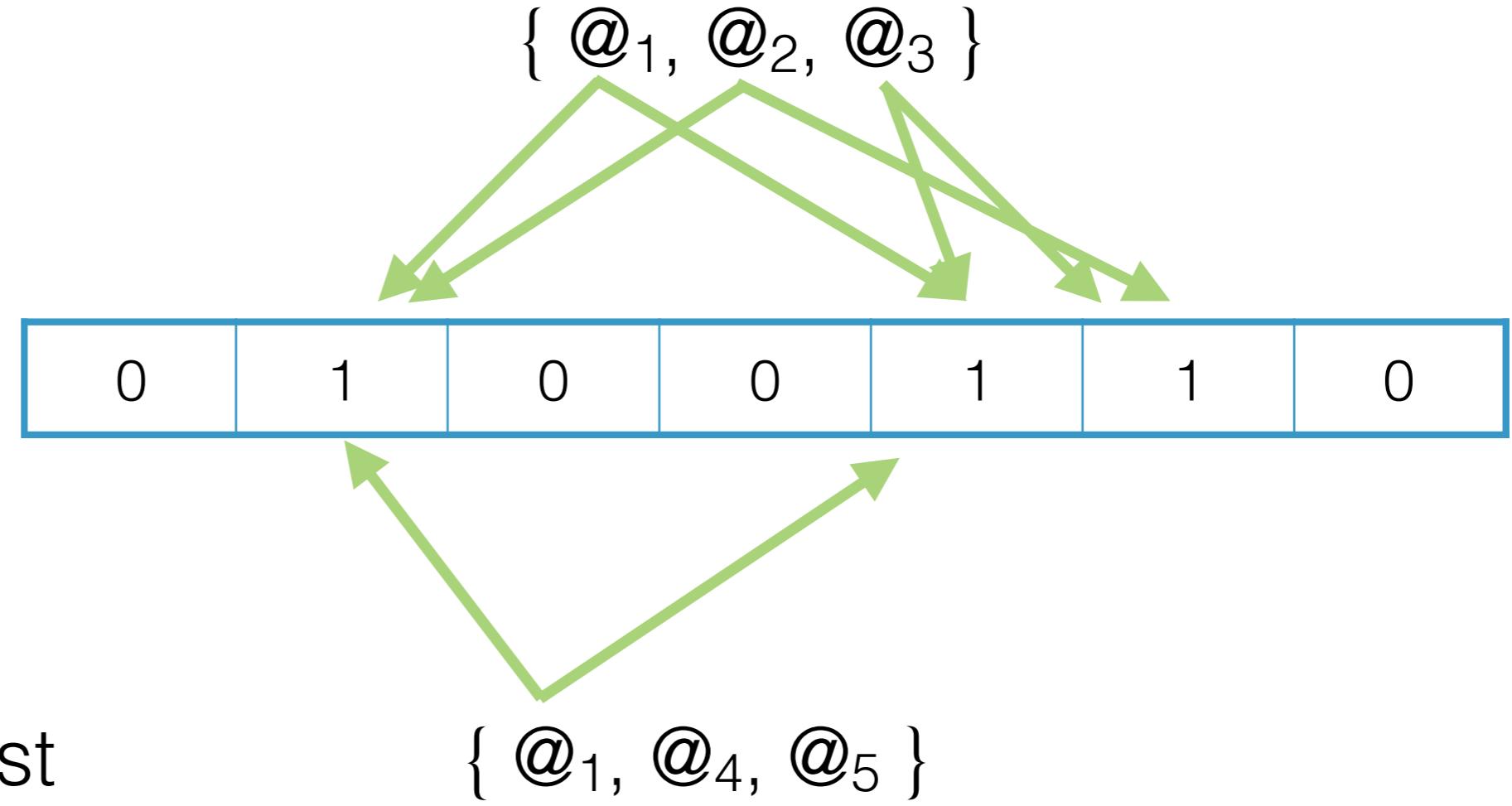
$\{ @_1, @_4, @_5 \}$

# Enable mobile Bitcoin clients

Insertion

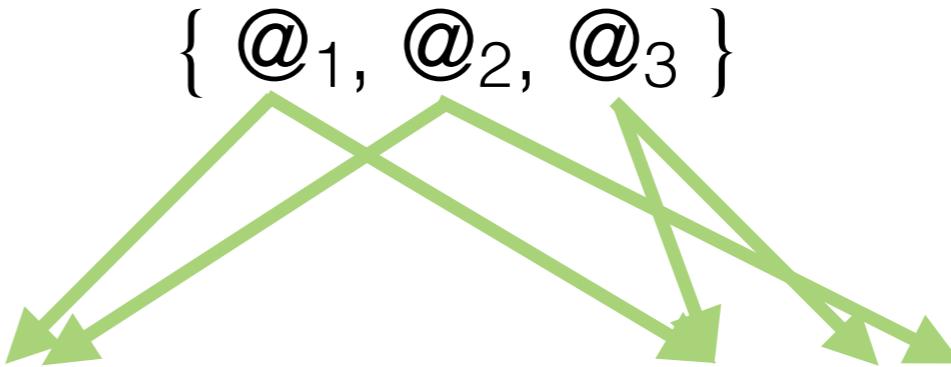
Bloom filter

Membership test



# Enable mobile Bitcoin clients

Insertion

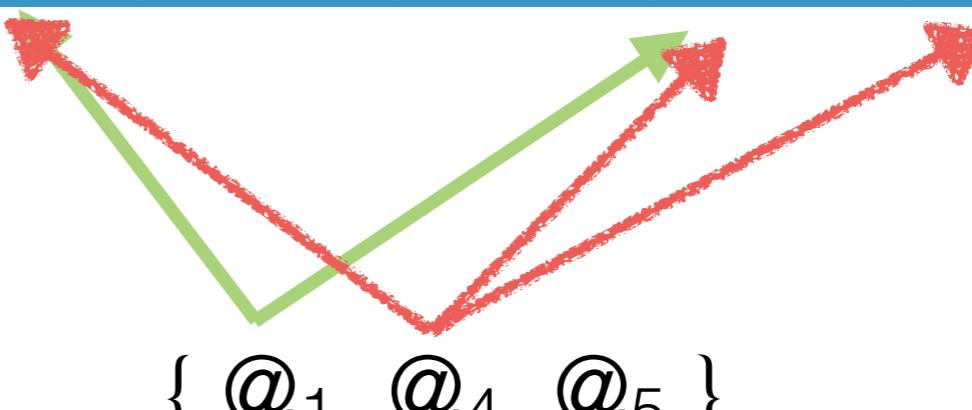


Bloom filter

0	1	0	0	0	1	1	0
---	---	---	---	---	---	---	---

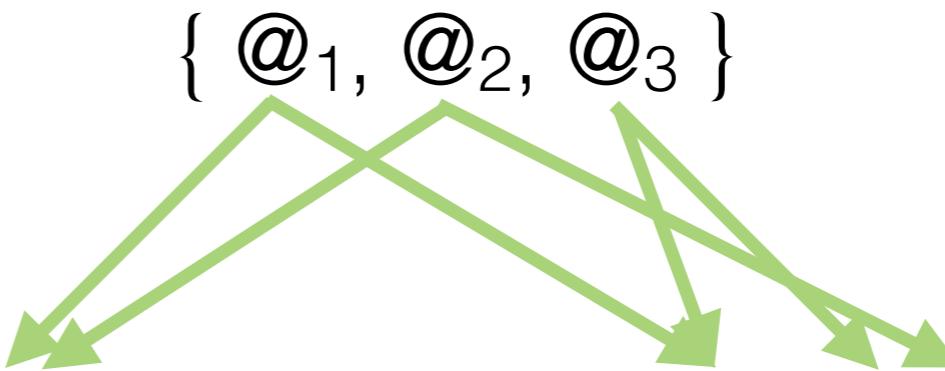
Membership test

$\{ @_1, @_4, @_5 \}$



# Enable mobile Bitcoin clients

Insertion



Bloom filter

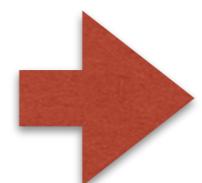
0	1	0	0	0	1	1	0
---	---	---	---	---	---	---	---

Membership test

$\{ @_1, @_4, @_5 \}$

!

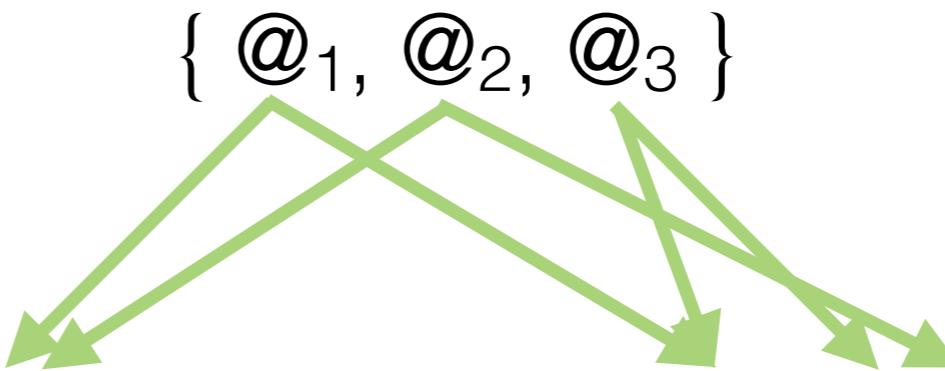
$@_4$  False positive



**target False Positive Rate (FPR)**

# Enable mobile Bitcoin clients

Insertion

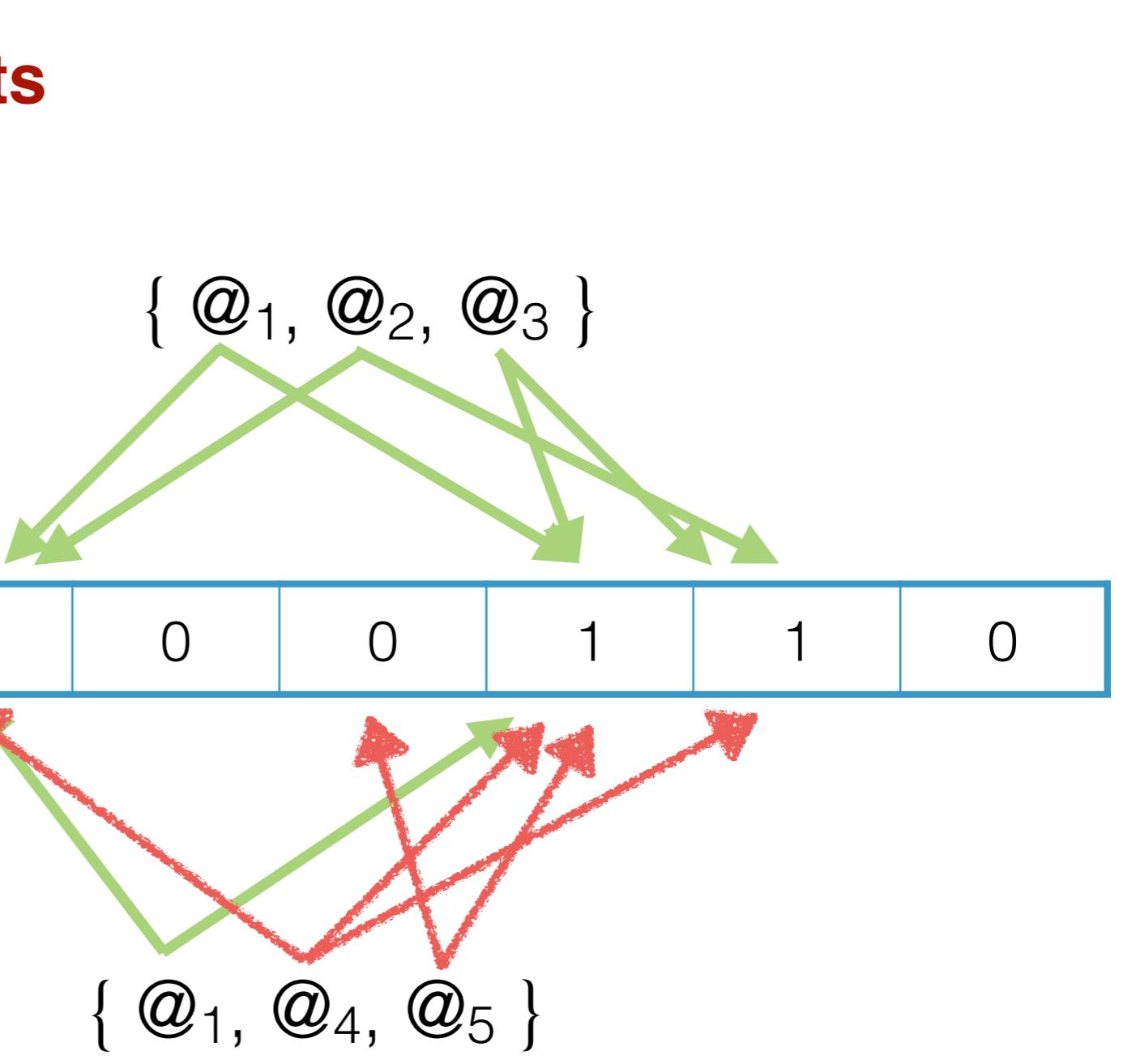


Bloom filter

0	1	0	0	0	1	1	0
---	---	---	---	---	---	---	---

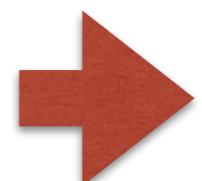
Membership test

$\{ @_1, @_4, @_5 \}$



!

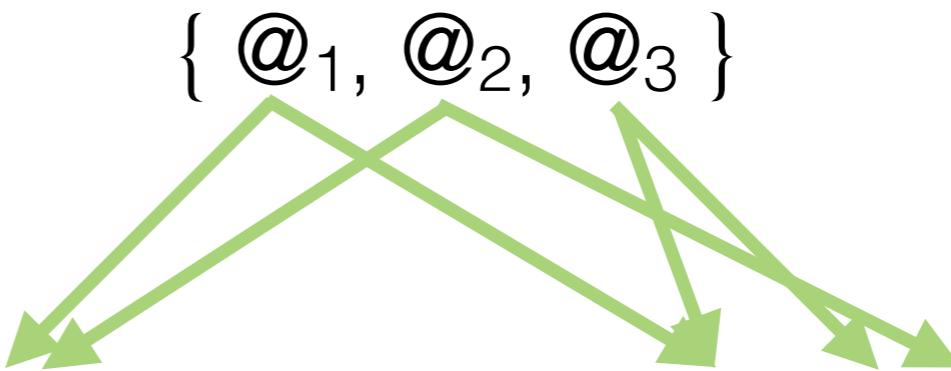
$@_4$  False positive



**target False Positive Rate (FPR)**

# Enable mobile Bitcoin clients

Insertion

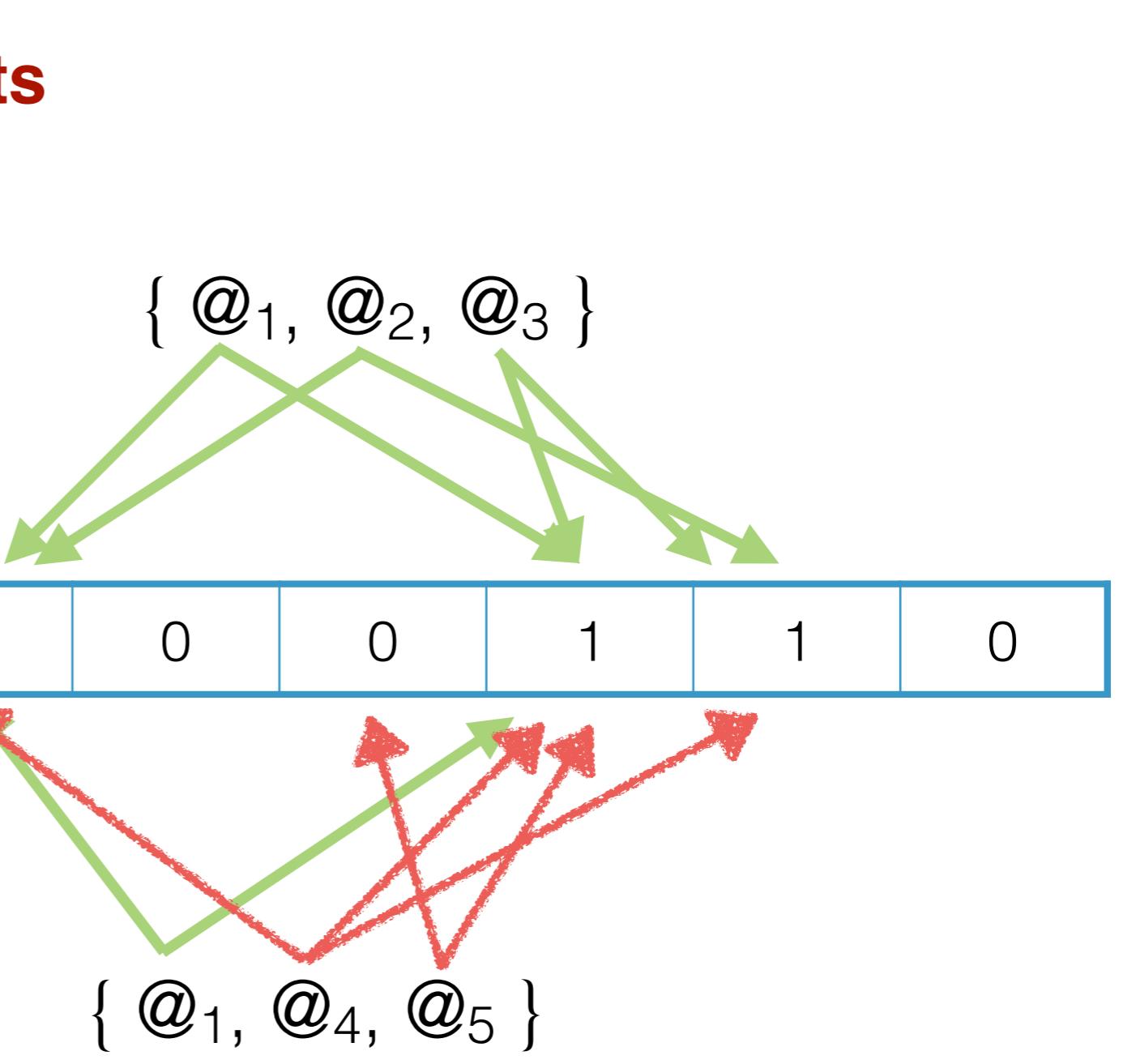


Bloom filter

0	1	0	0	0	1	1	0
---	---	---	---	---	---	---	---

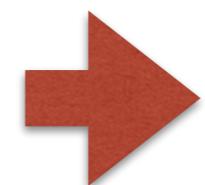
Membership test

$\{ @_1, @_4, @_5 \}$



!

$@_4$  False positive



**target False Positive Rate (FPR)**

$@_5$  True negative

# Simple Payment Verification (SPV)

**Filter** transactions not relevant for user

SPV client



Full Bitcoin node



Full Bitcoin node

# Simple Payment Verification (SPV)

**Filter** transactions not relevant for user

SPV client



$\begin{matrix} @_1 \\ @_2 \\ @_3 \end{matrix}$



Bloom filter

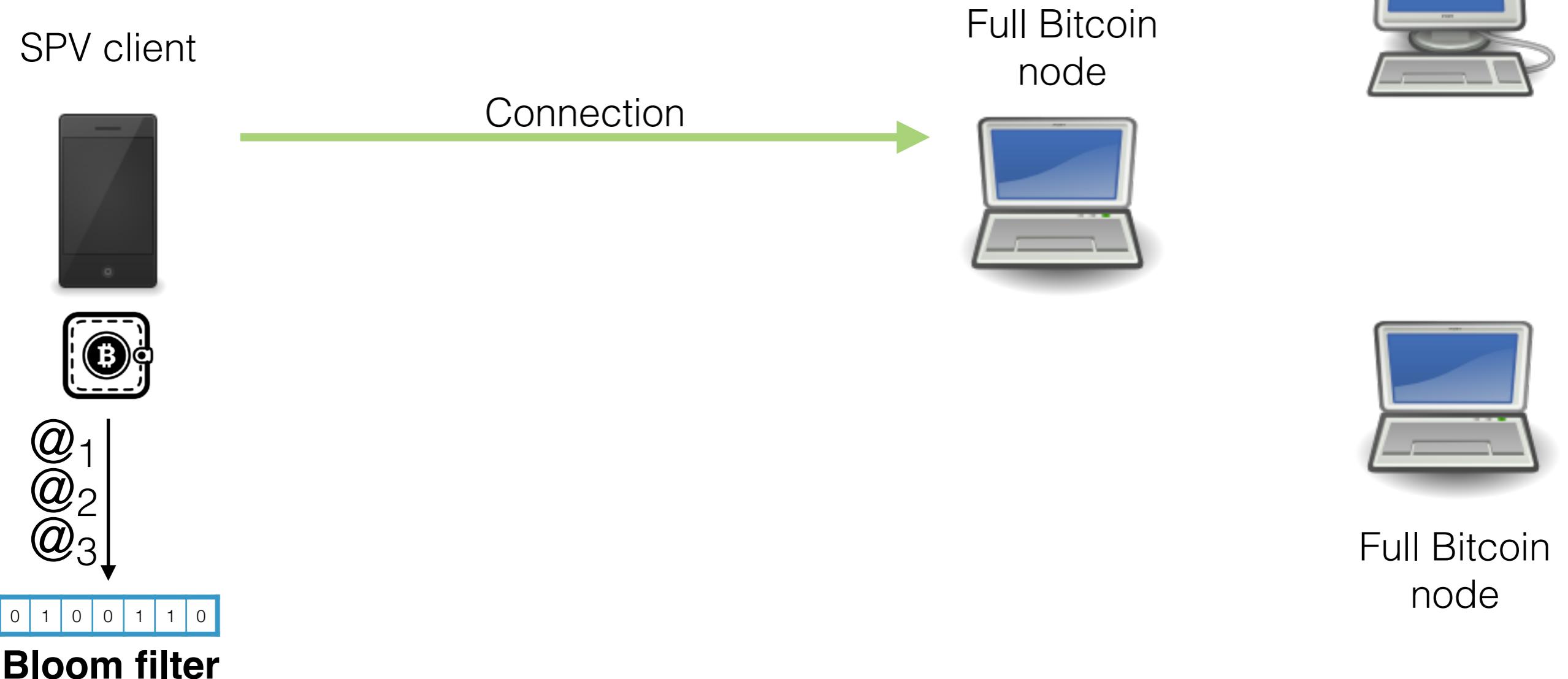
Full Bitcoin node



Full Bitcoin node

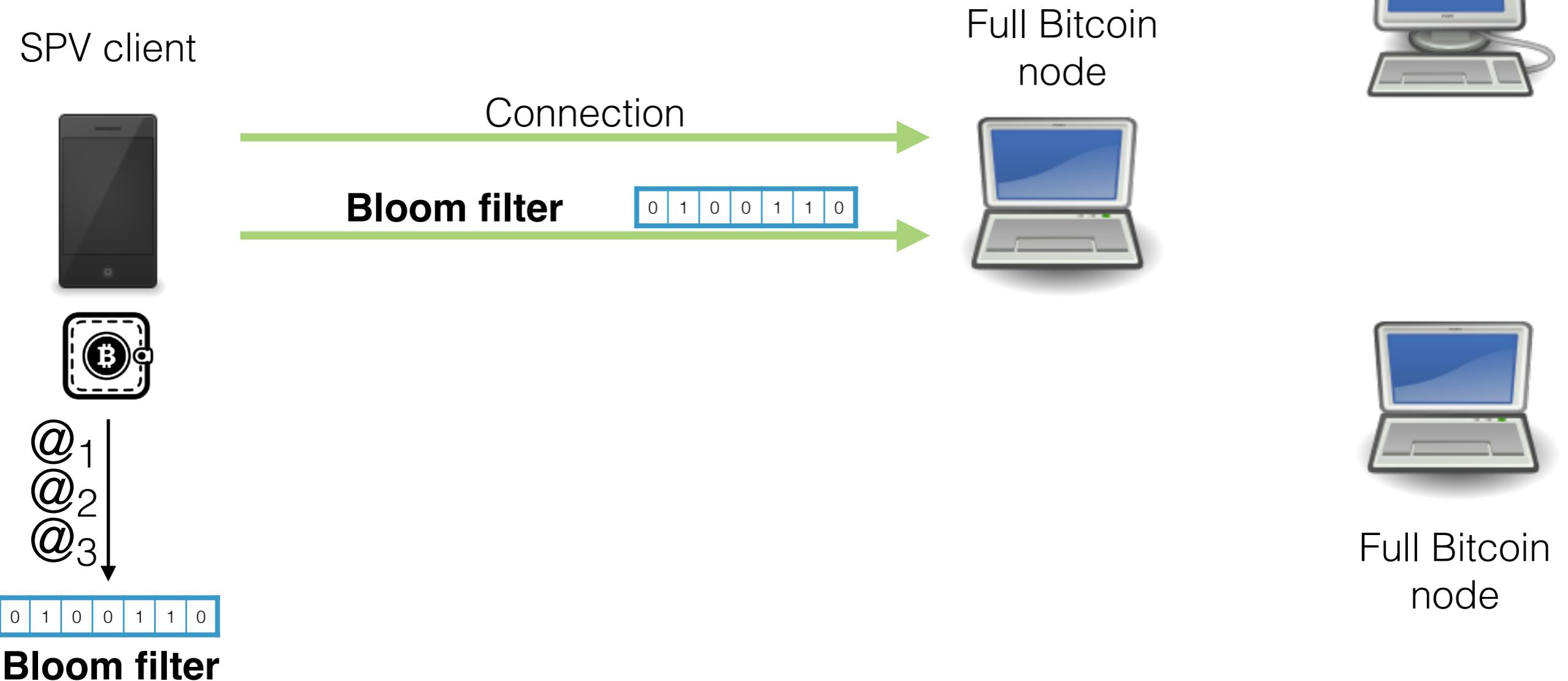
# Simple Payment Verification (SPV)

**Filter** transactions not relevant for user



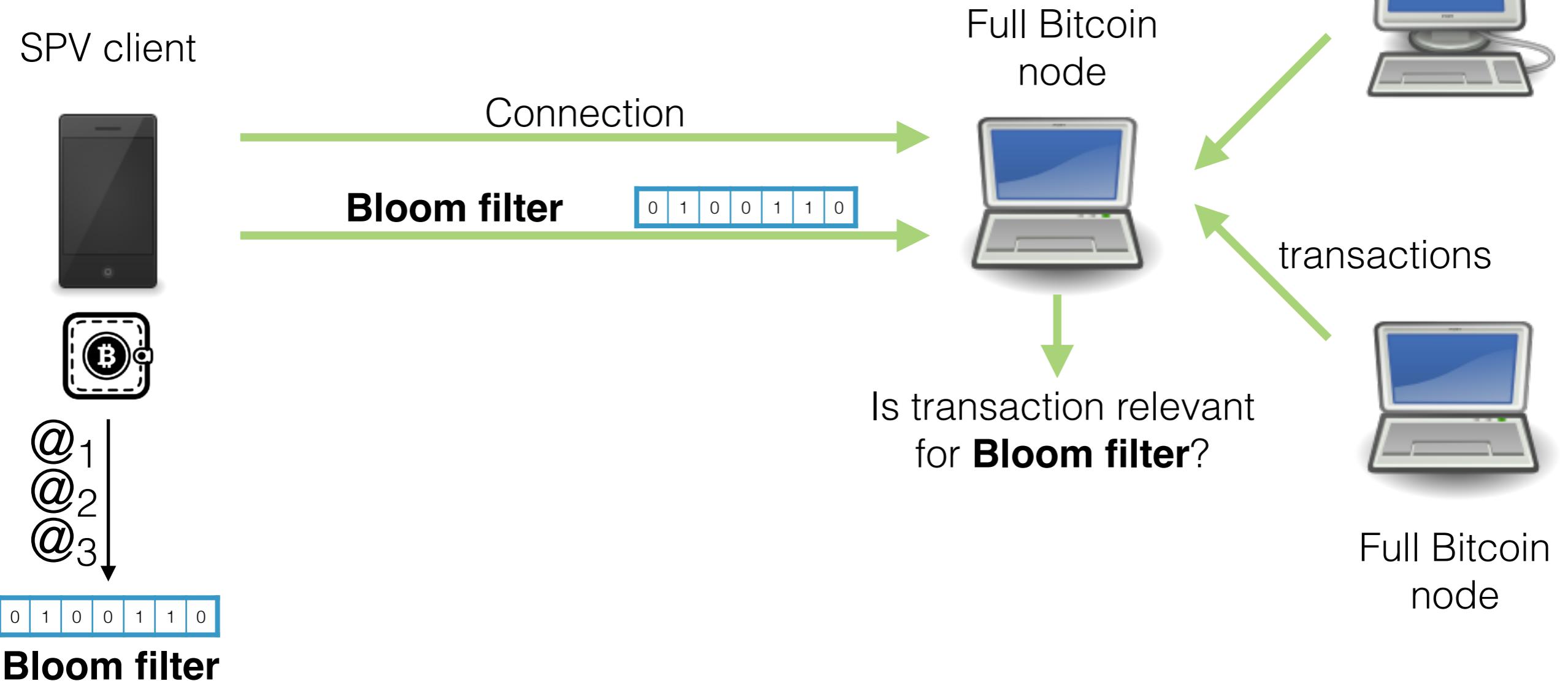
# Simple Payment Verification (SPV)

**Filter** transactions not relevant for user



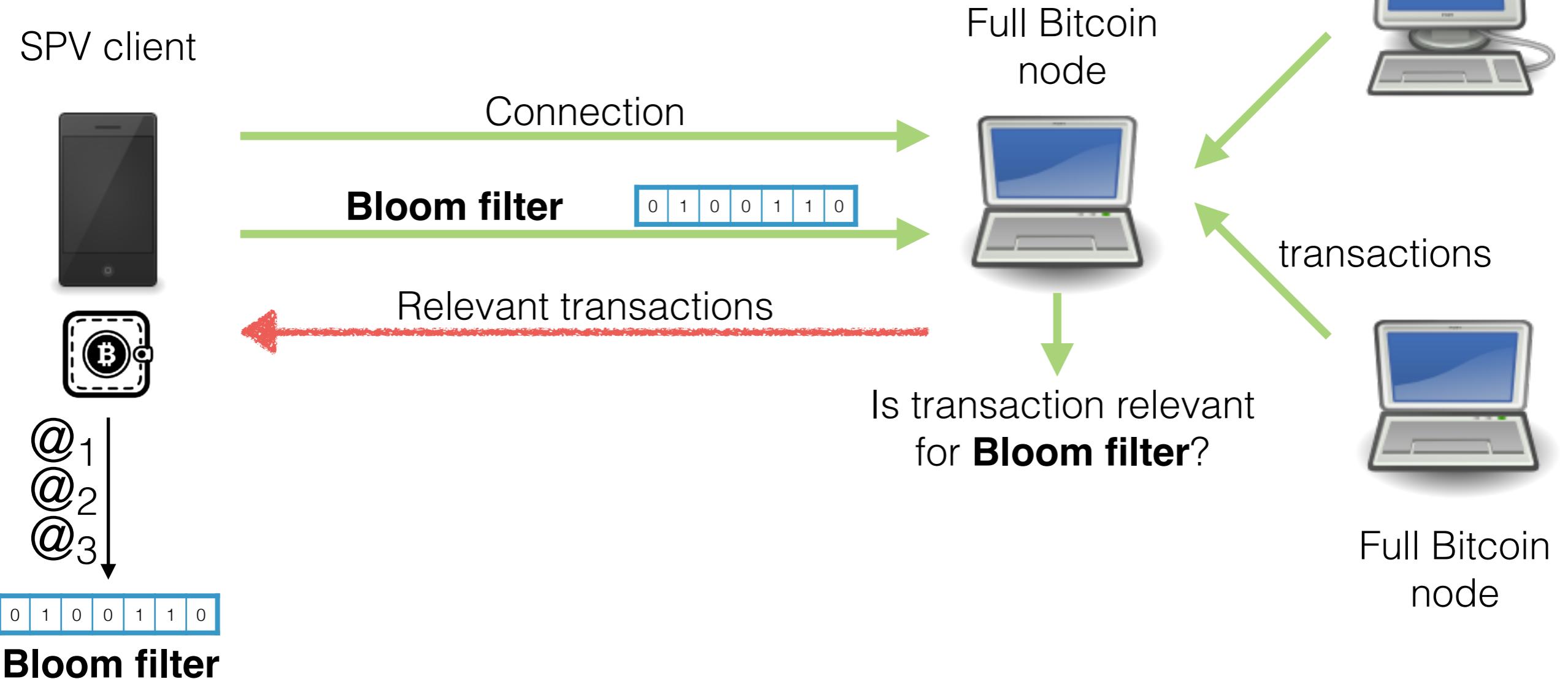
# Simple Payment Verification (SPV)

**Filter** transactions not relevant for user



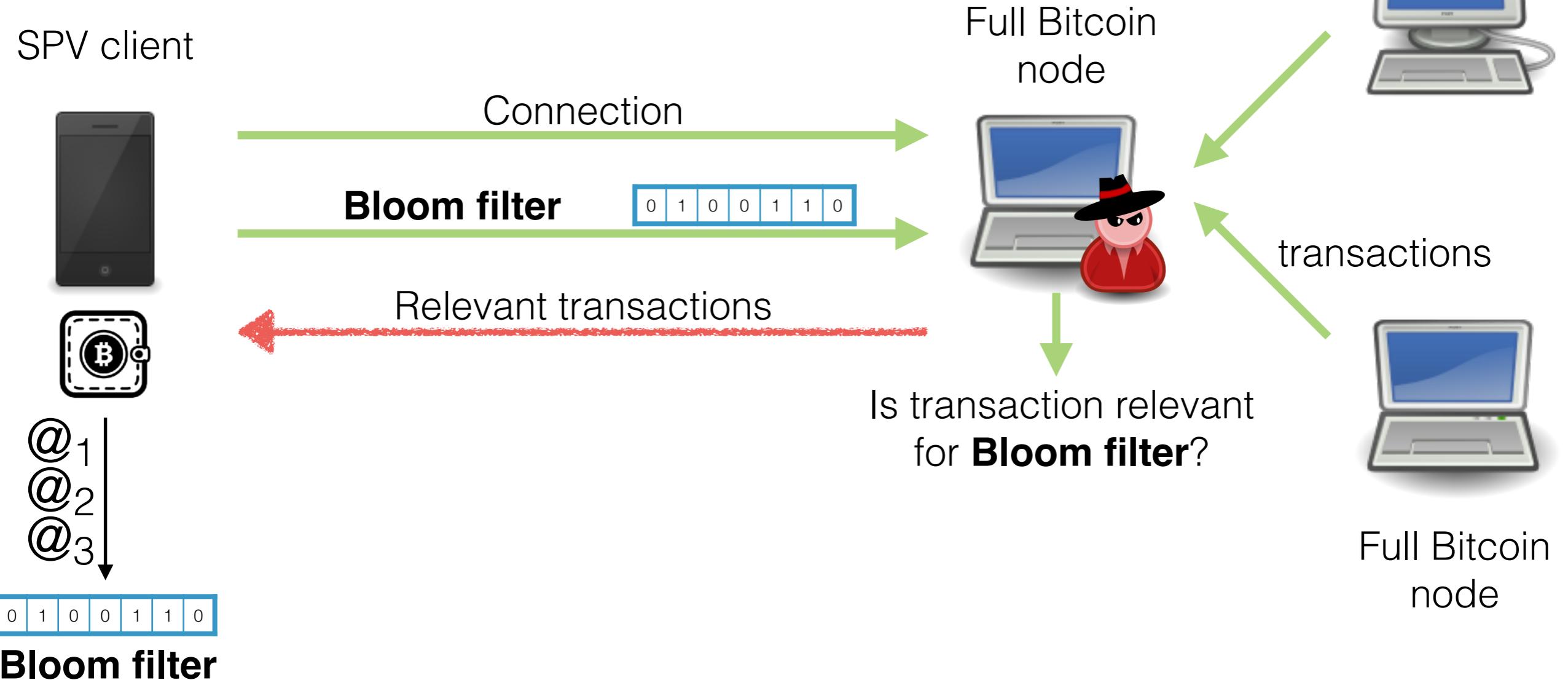
# Simple Payment Verification (SPV)

**Filter** transactions not relevant for user



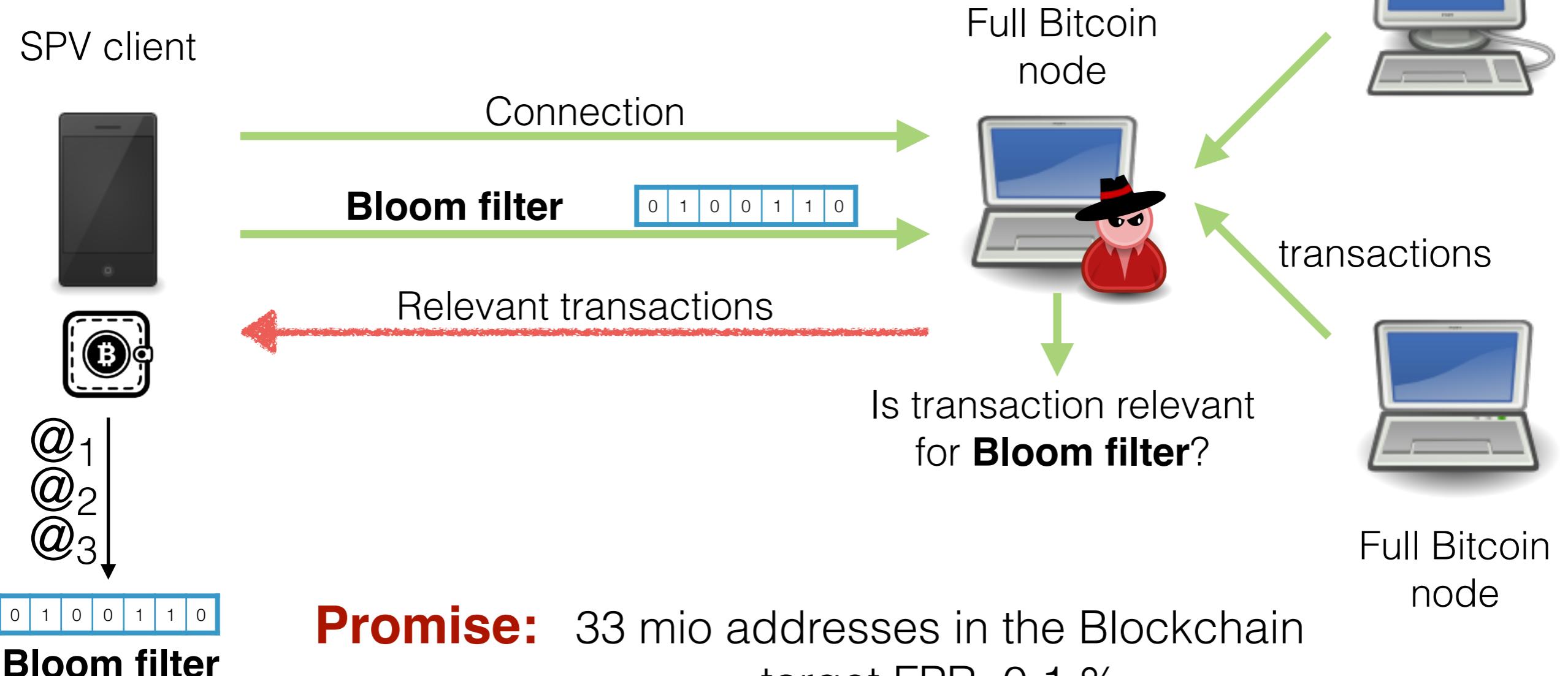
# Simple Payment Verification (SPV)

**Filter** transactions not relevant for user



# 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

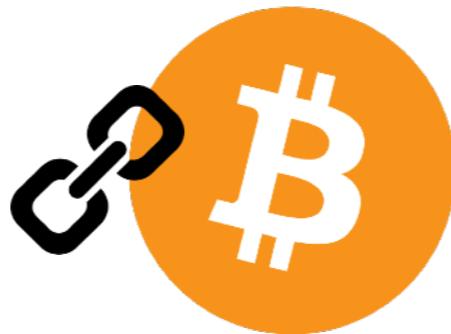


Blockchain



SPV client

# Model and Privacy measure



Blockchain

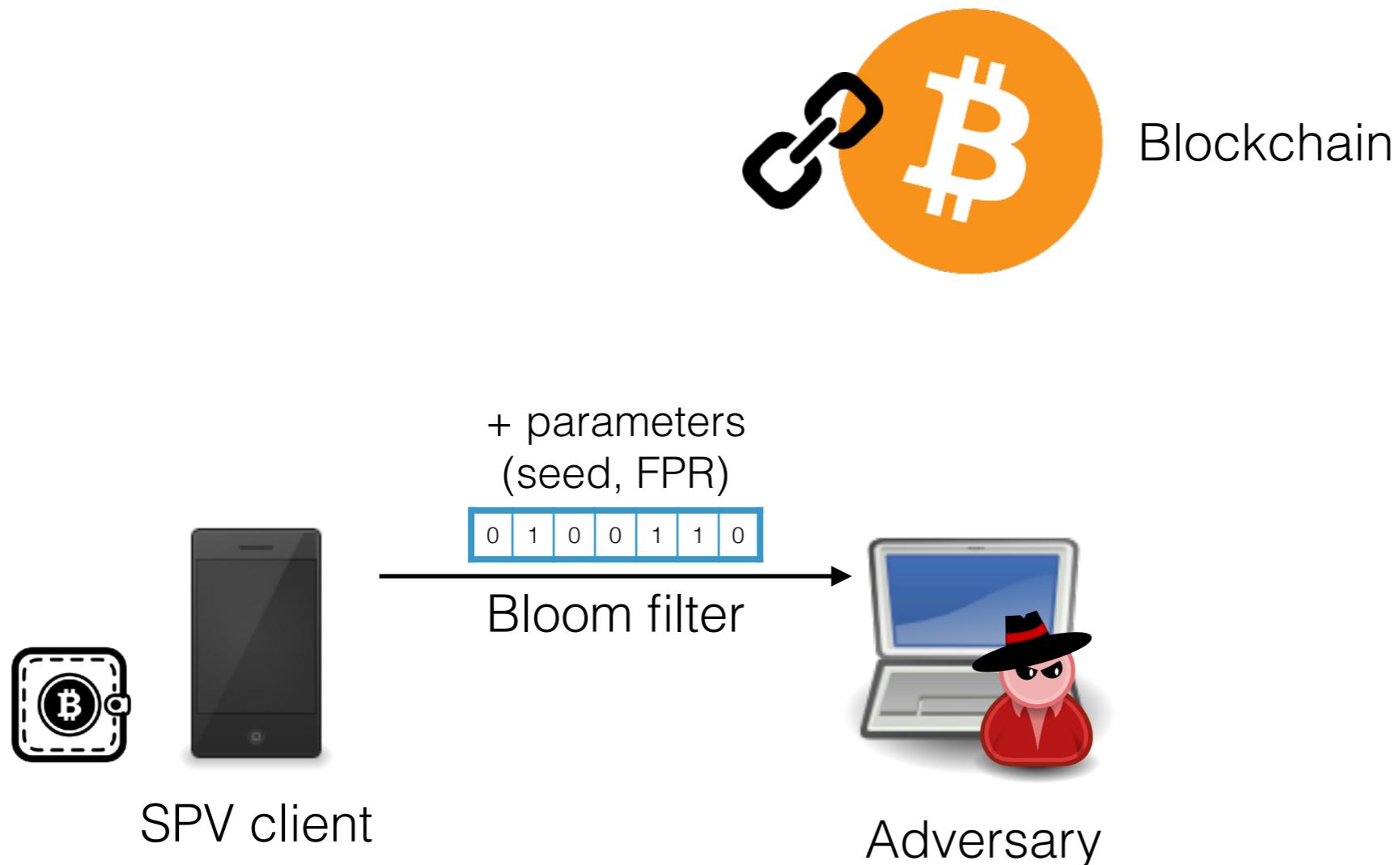


SPV client

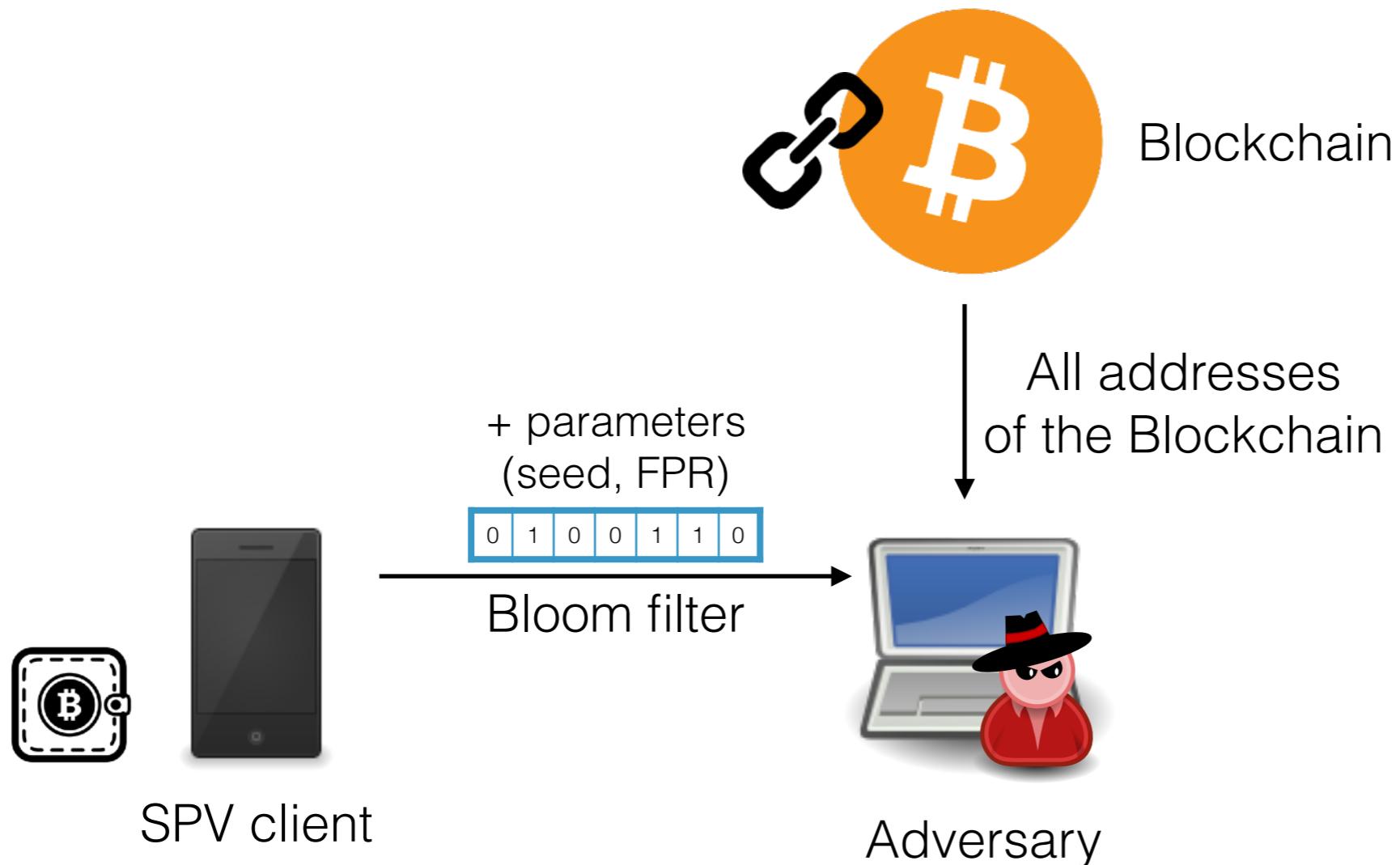


Adversary

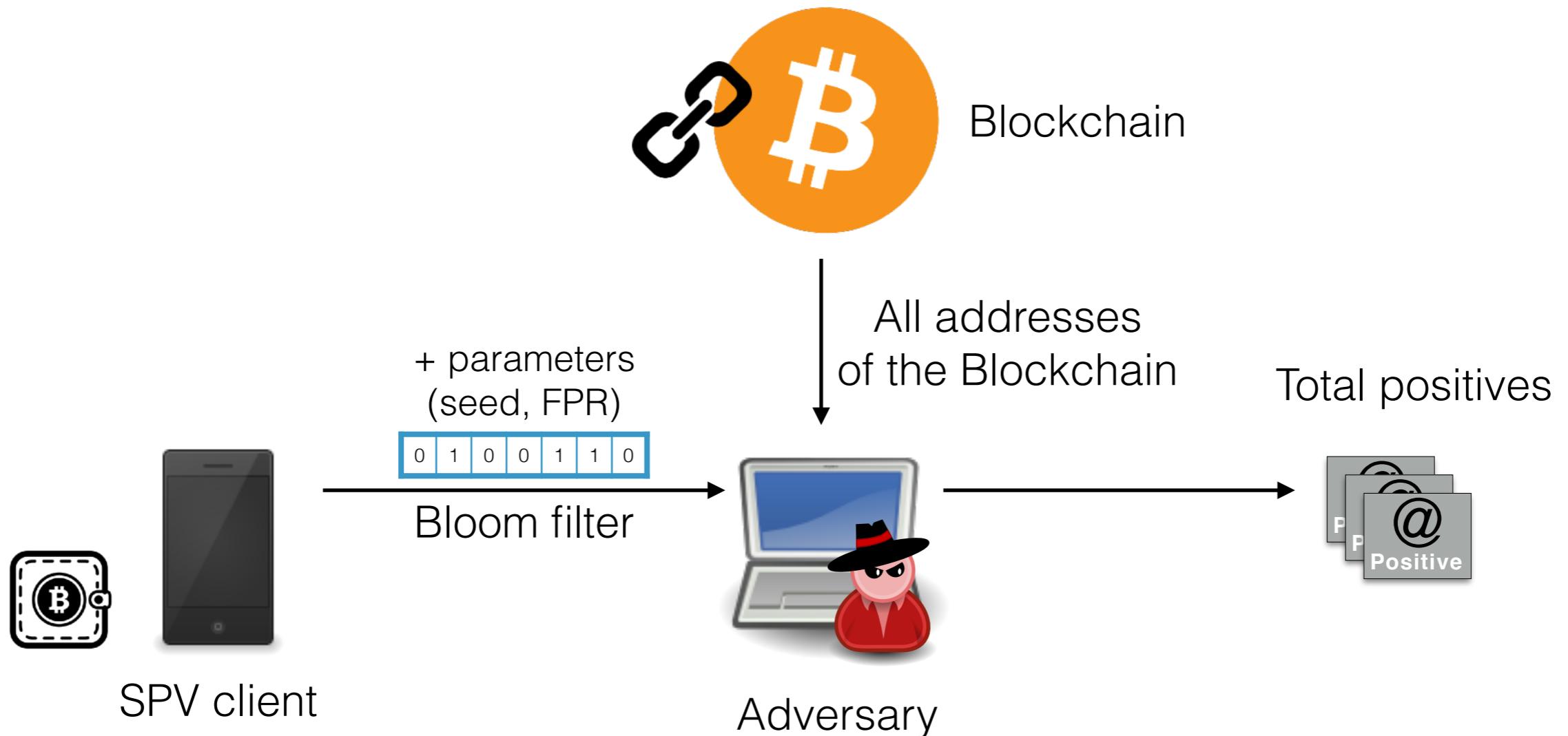
# Model and Privacy measure



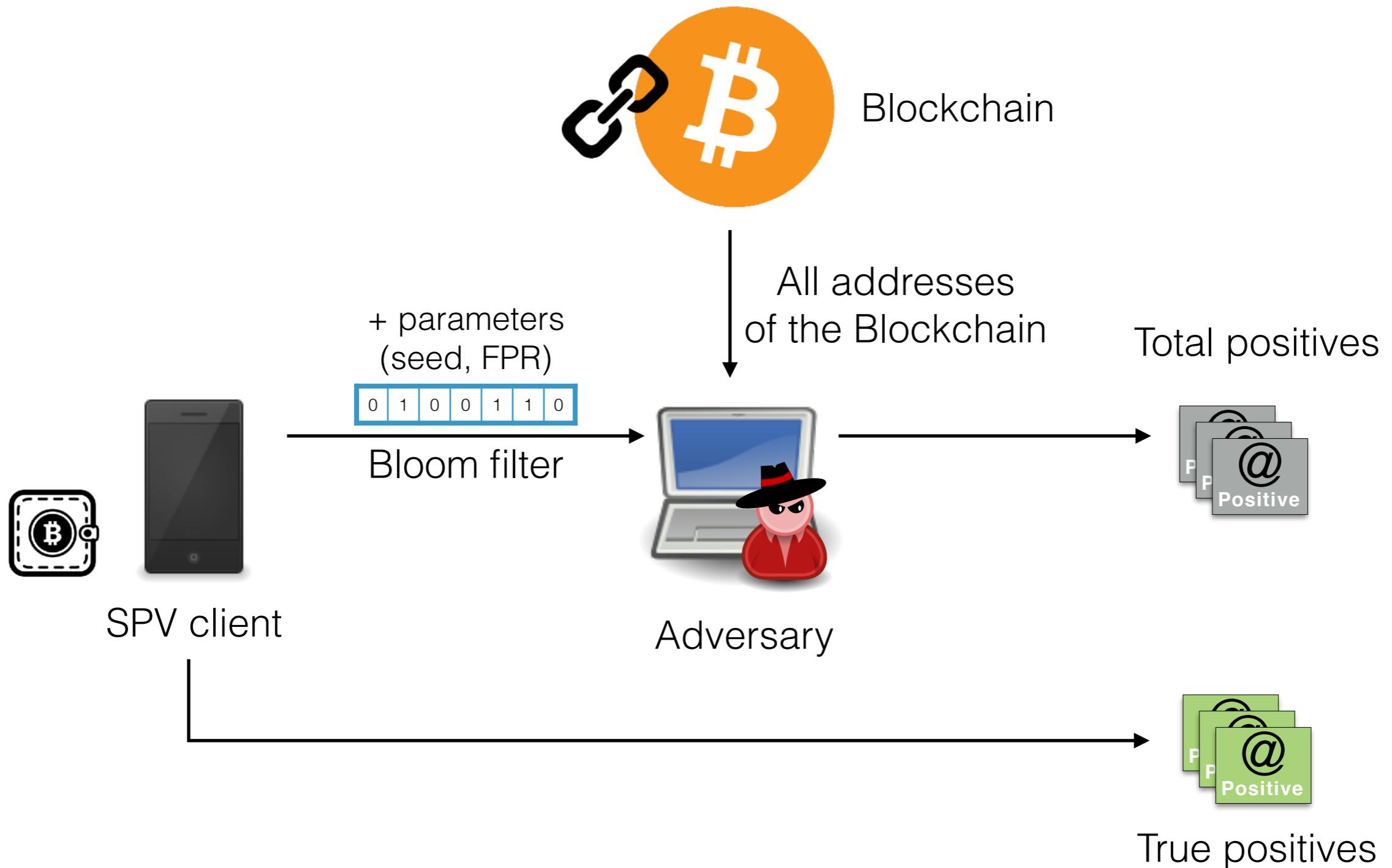
# Model and Privacy measure



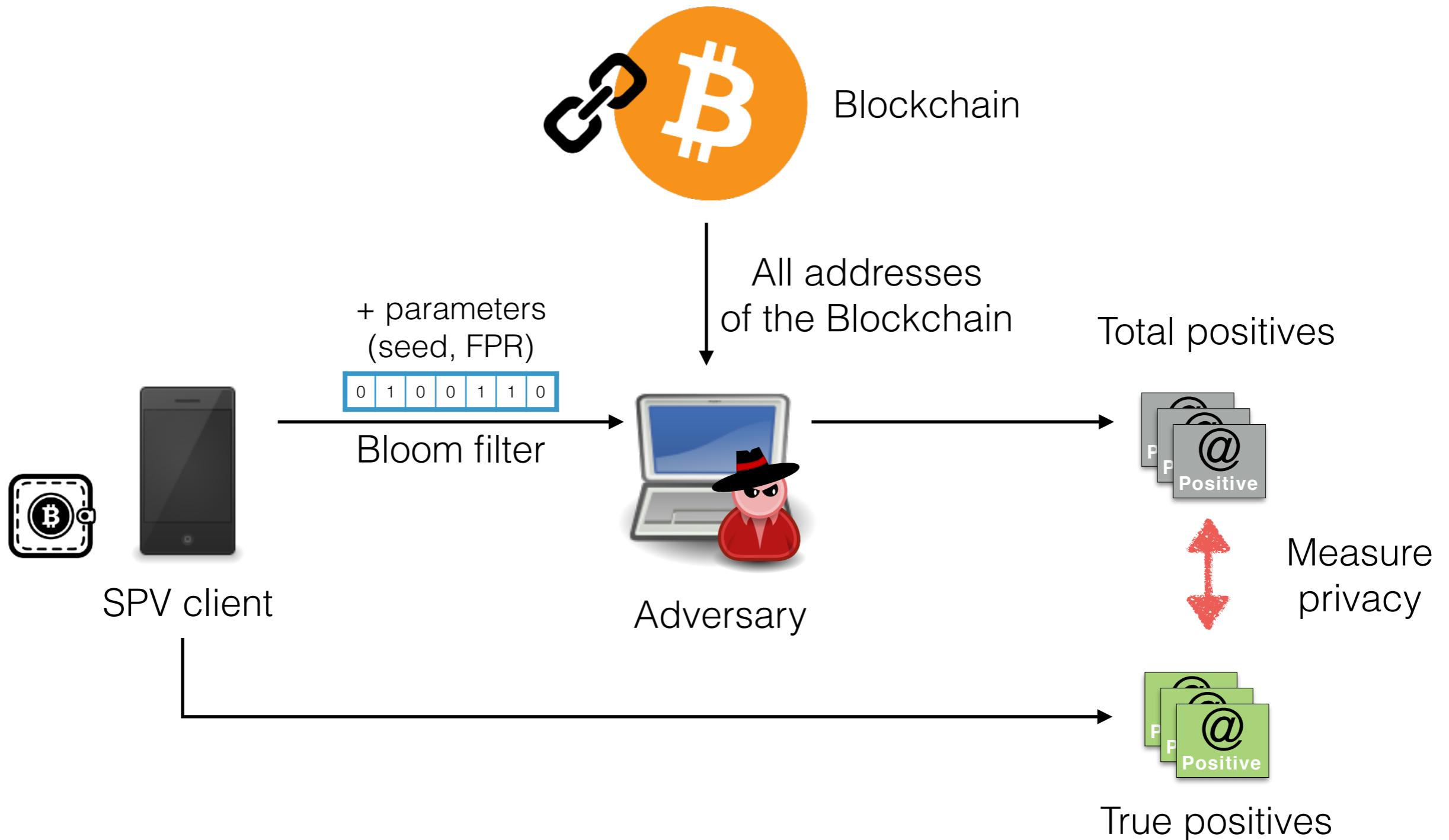
# Model and Privacy measure



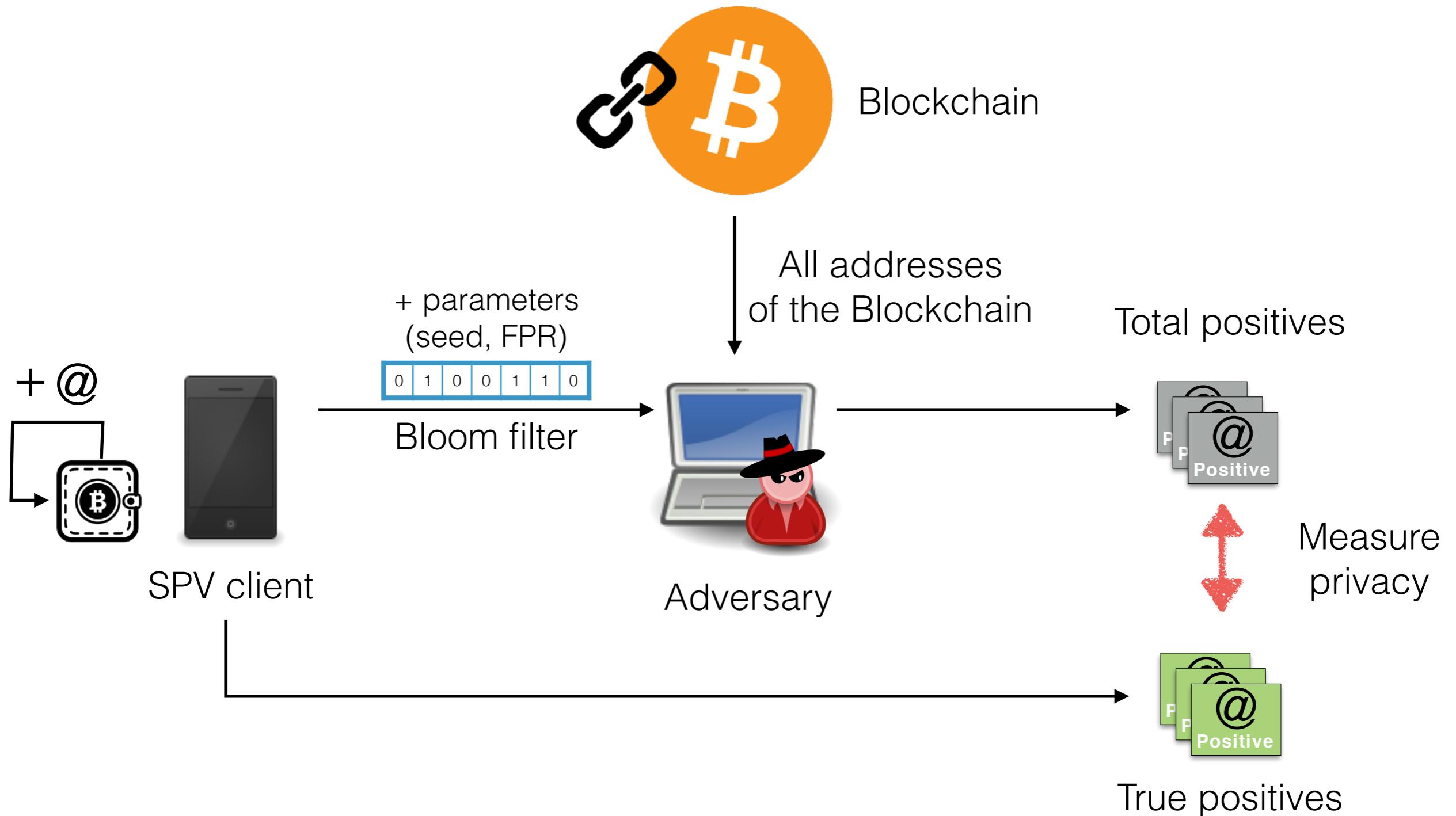
# Model and Privacy measure



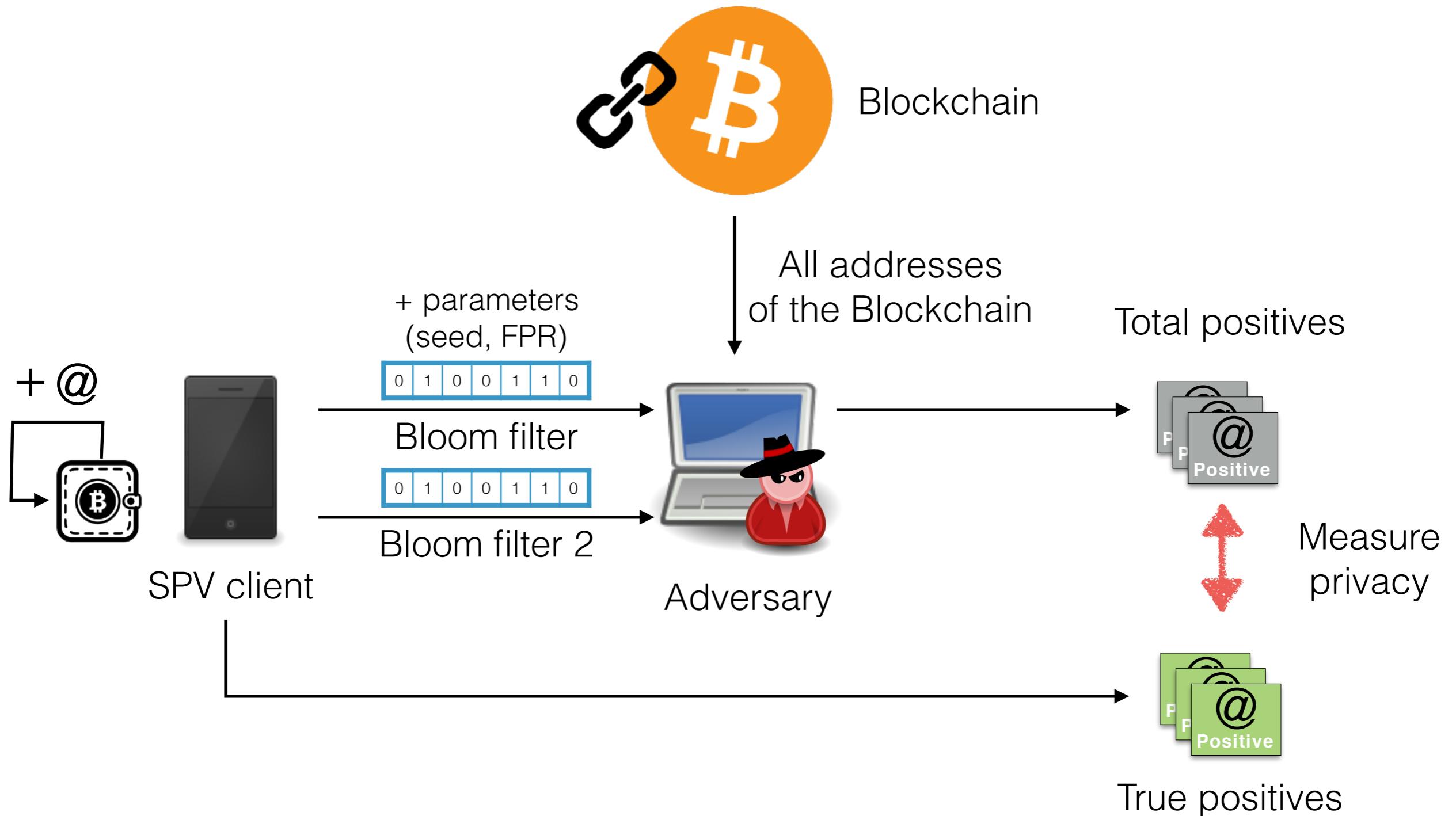
# Model and Privacy measure



# Model and Privacy measure



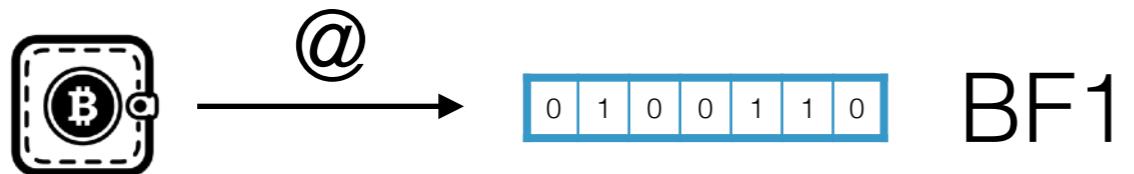
# Model and Privacy measure



## Stair stepping

Bloom filter designed for

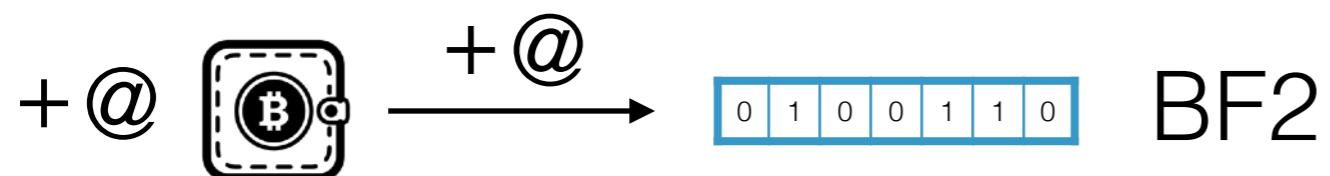
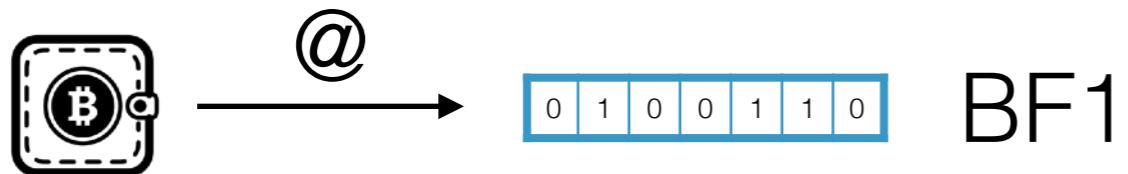
- max number of **addresses**
- **target FPR** when max addresses inserted



## Stair stepping

Bloom filter designed for

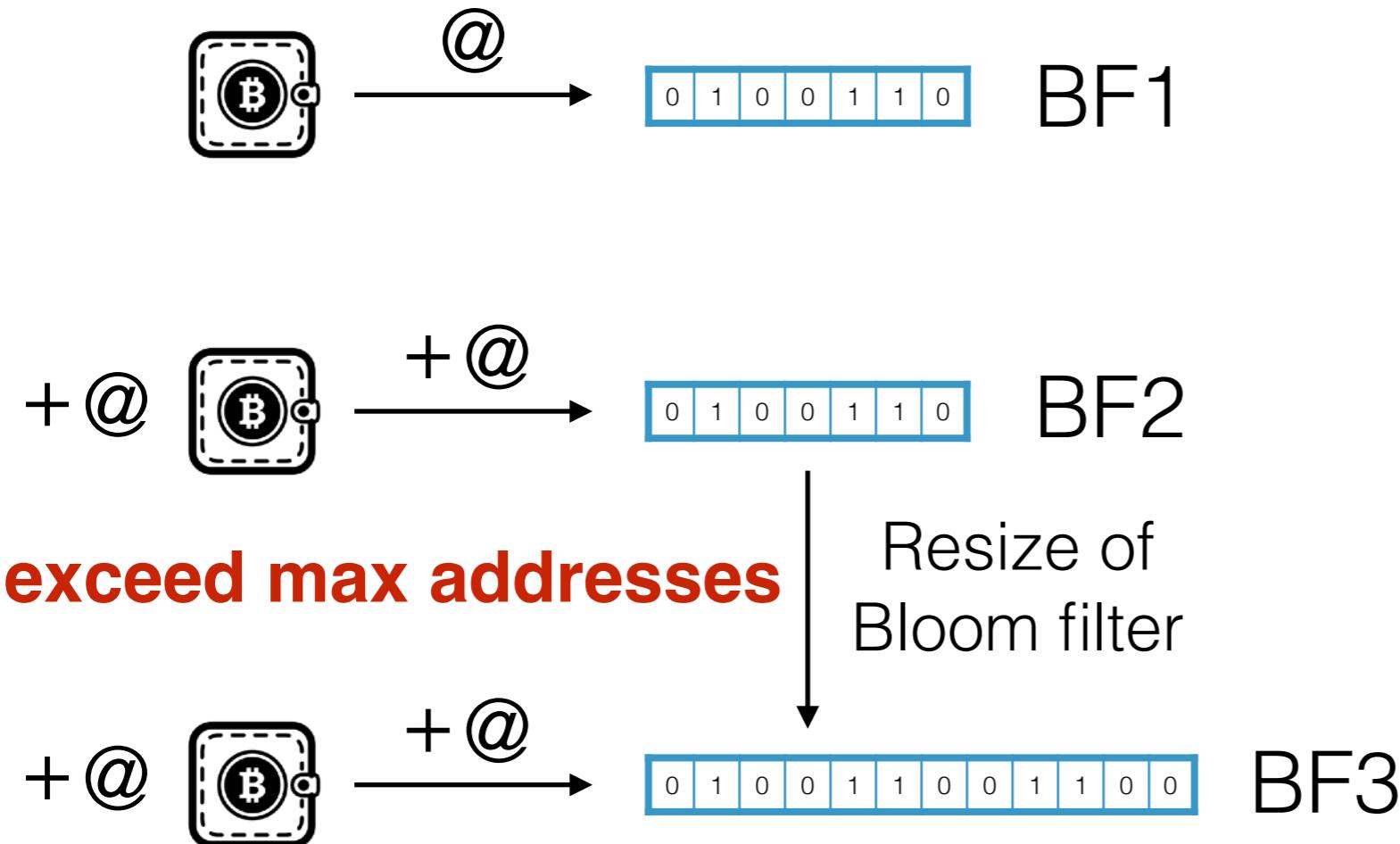
- max number of **addresses**
- **target FPR** when max addresses inserted



# Stair stepping

Bloom filter designed for

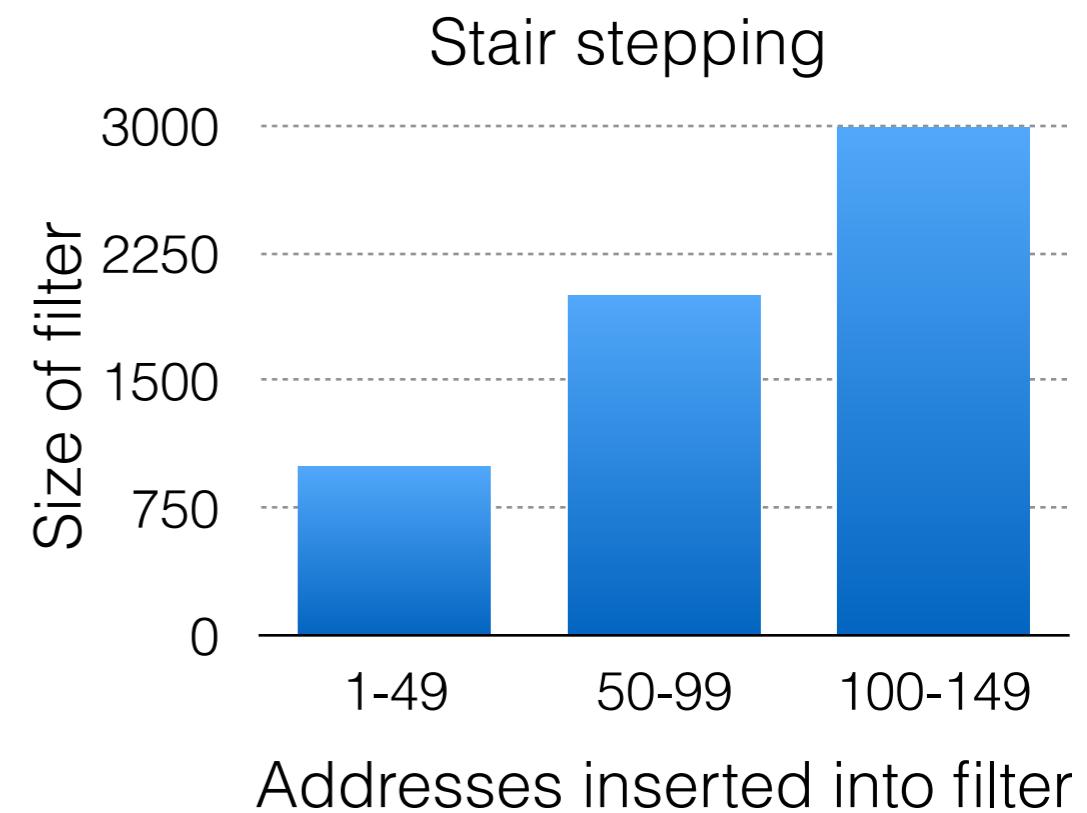
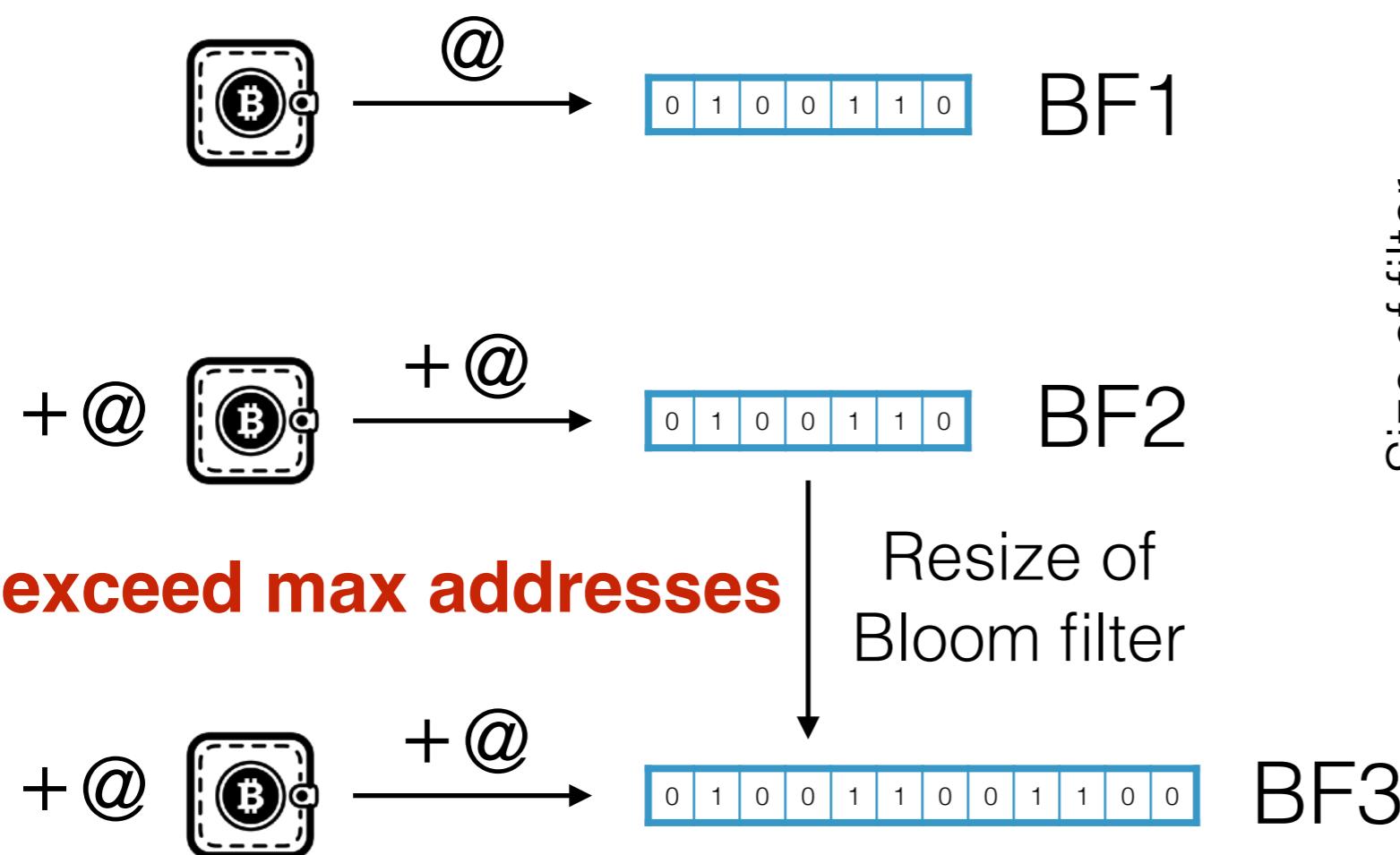
- max number of **addresses**
- **target FPR** when max addresses inserted



# Stair stepping

Bloom filter designed for

- max number of **addresses**
- **target FPR** when max addresses inserted

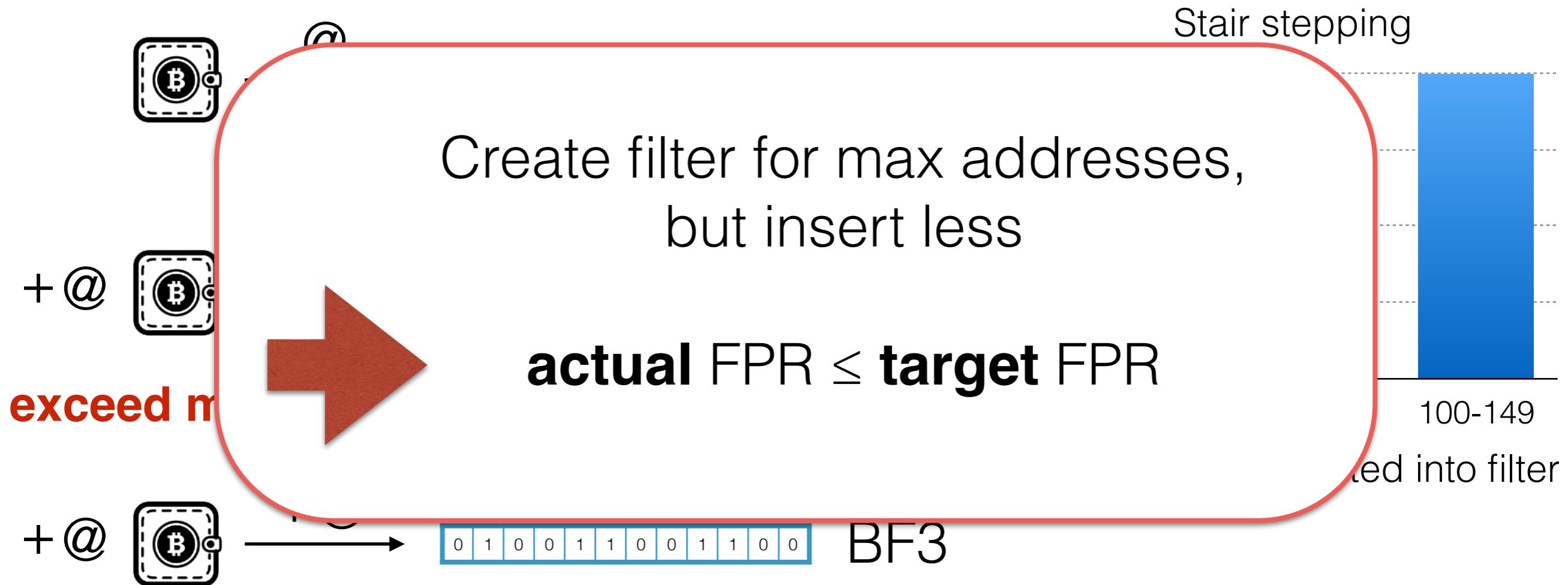


Rationale: **avoid** filters with different sizes

## Stair stepping

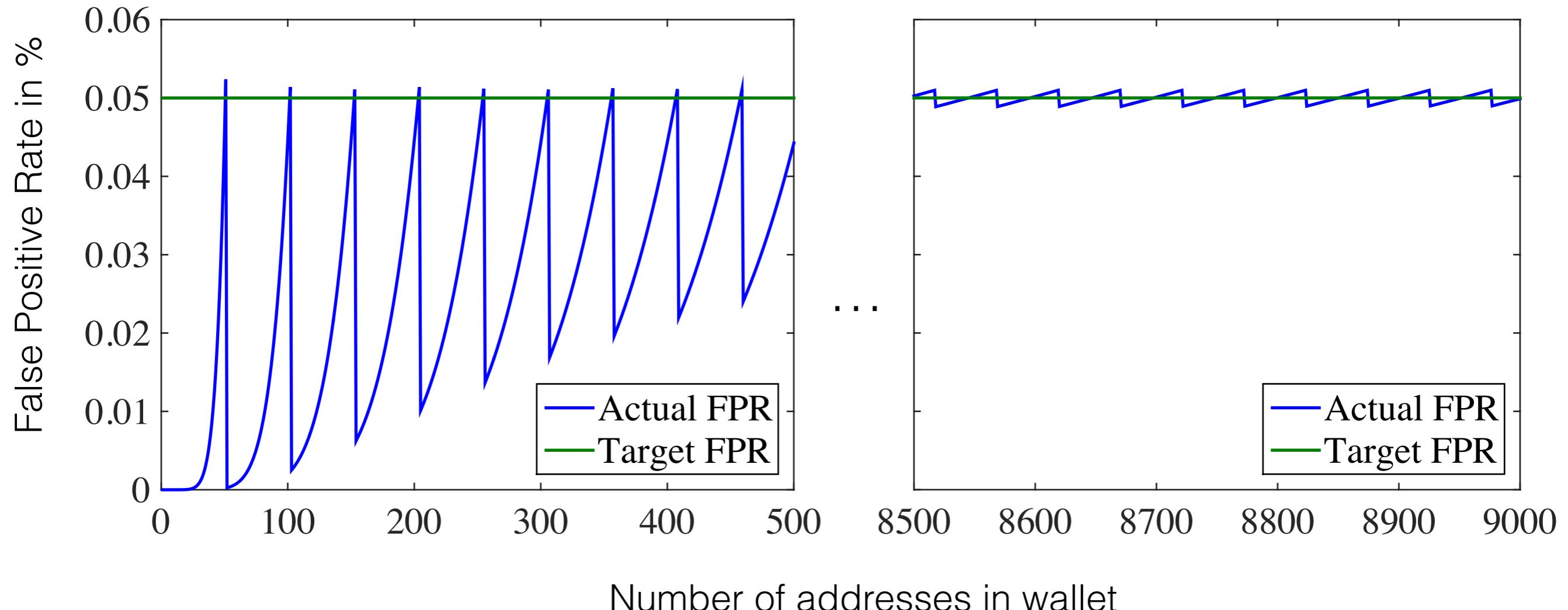
Bloom filter designed for

- max number of **addresses**
- **target FPR** when max addresses inserted

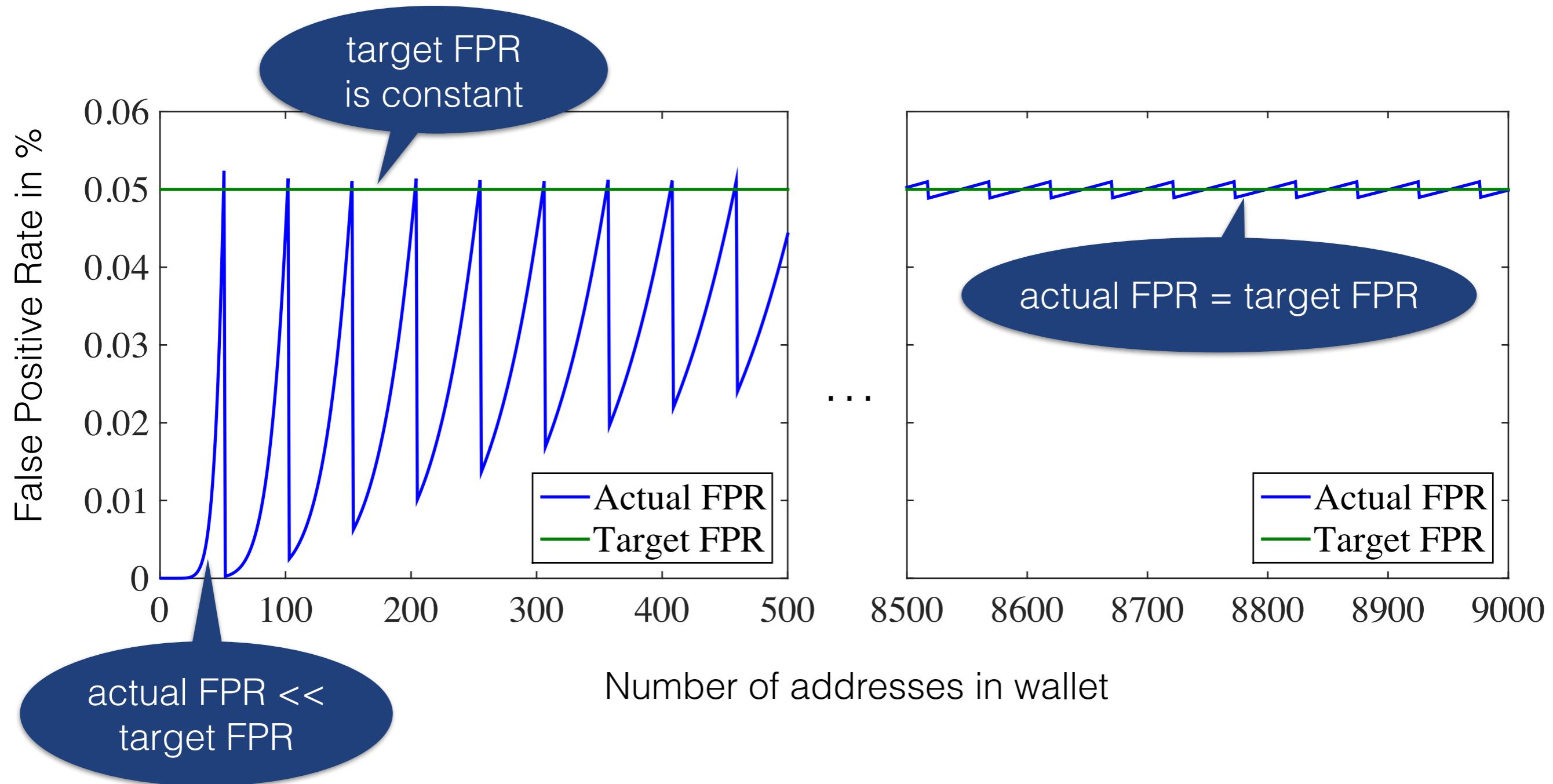


Rationale: **avoid** filters with different sizes

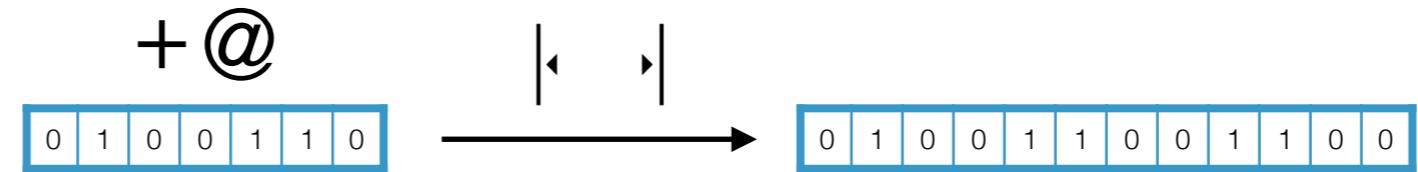
## Analytical results - Actual FPR vs. Target FPR



## Analytical results - Actual FPR vs. Target FPR



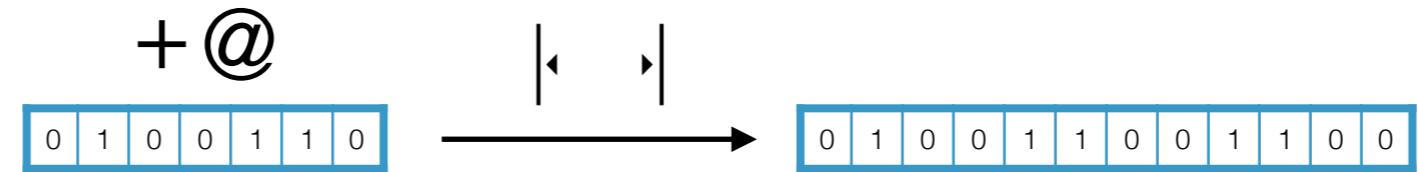
## Resizing



Once max addresses inserted —> bigger filter

- Hash functions adapted to fill space of new filter
- **Consequence:** New filter yields **different** false positives

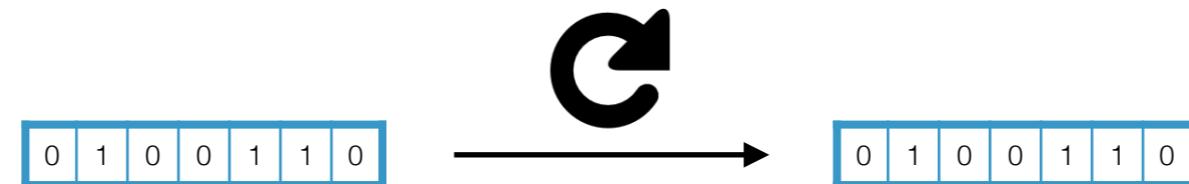
## Resizing



Once max addresses inserted → bigger filter

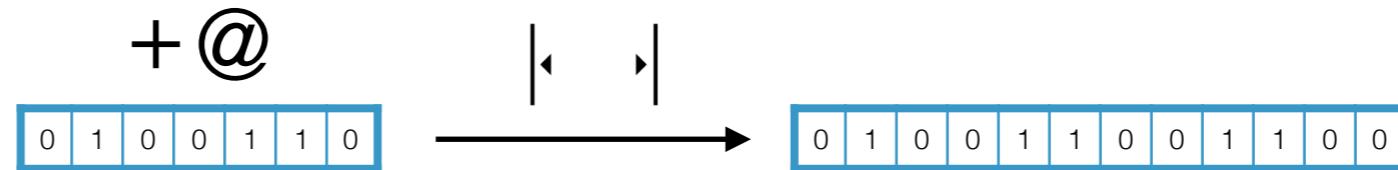
- Hash functions adapted to fill space of new filter
- **Consequence:** New filter yields **different** false positives

## Restarting



- Fresh seed value for hash functions of Bloom filter
- **Consequence:** New filter yields **different** false positives

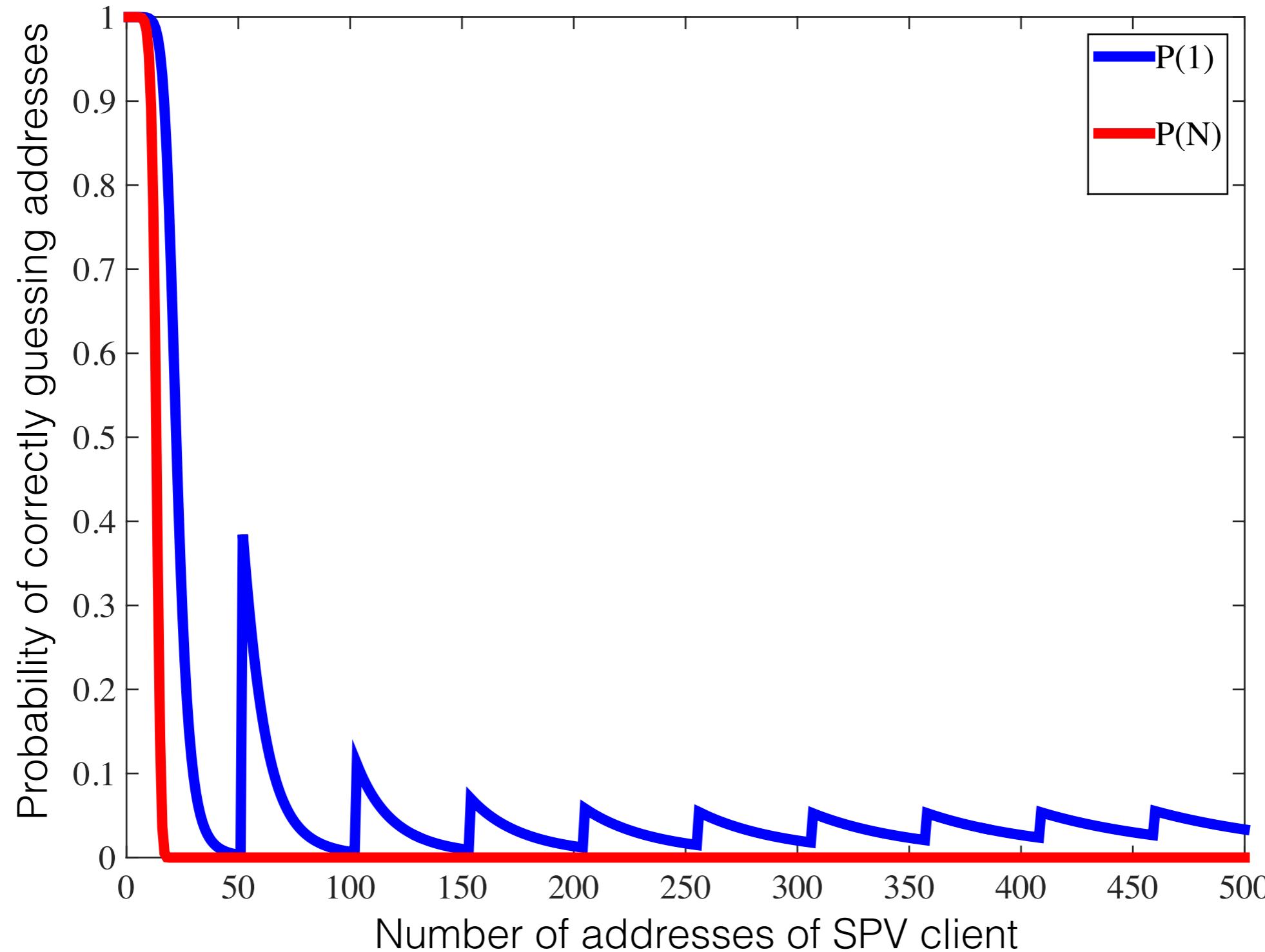
## Resizing



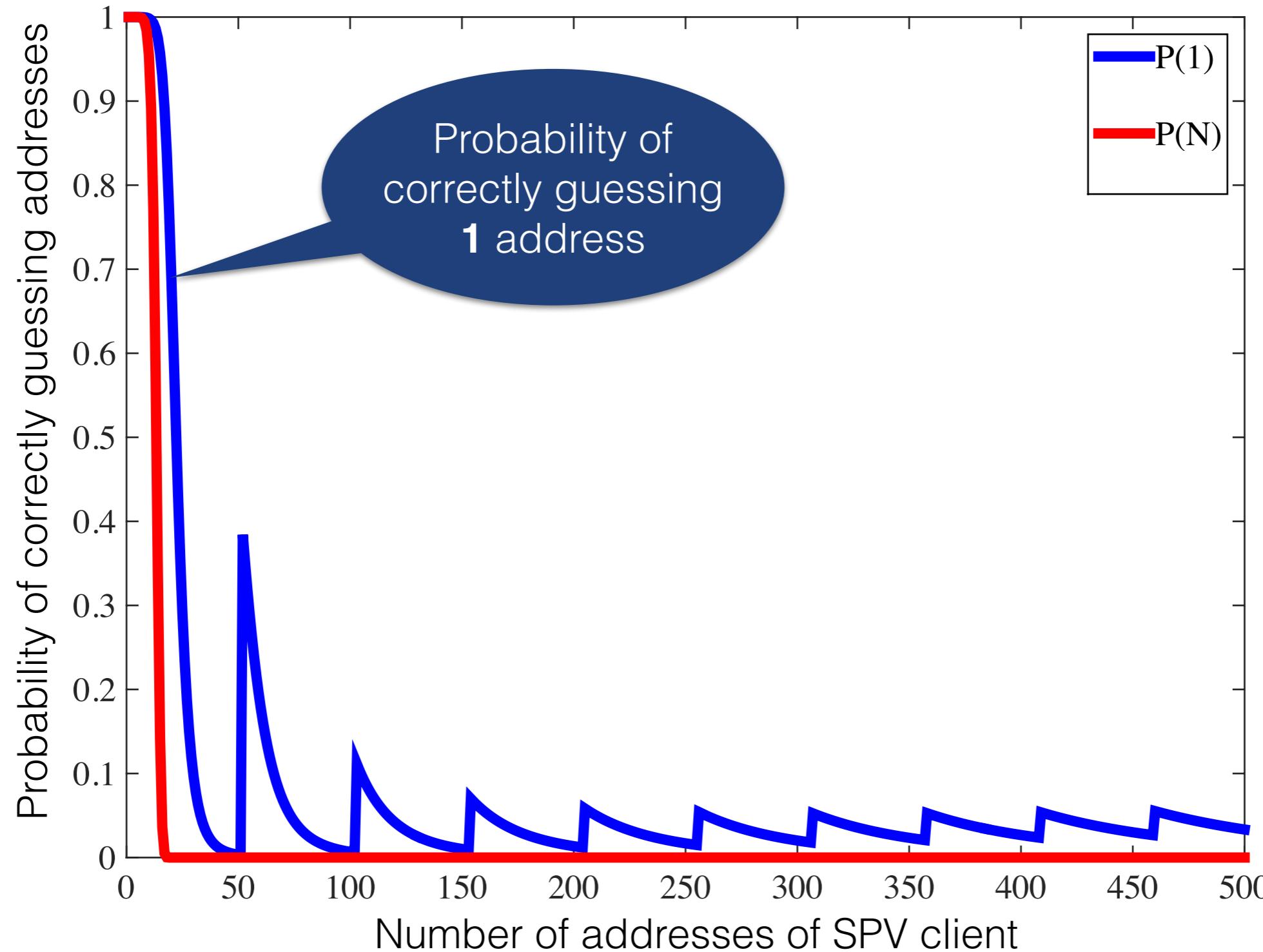
Once max addresses inserted → bigger filter

- Summary of current SPV design choices
- - 1. Stair stepping → actual FPR  $\leq$  target FPR
  - 2. Resizing → different False Positives
  - 3. Restarting → different False Positives
- **Consequence.** New filter yields **different** false positives

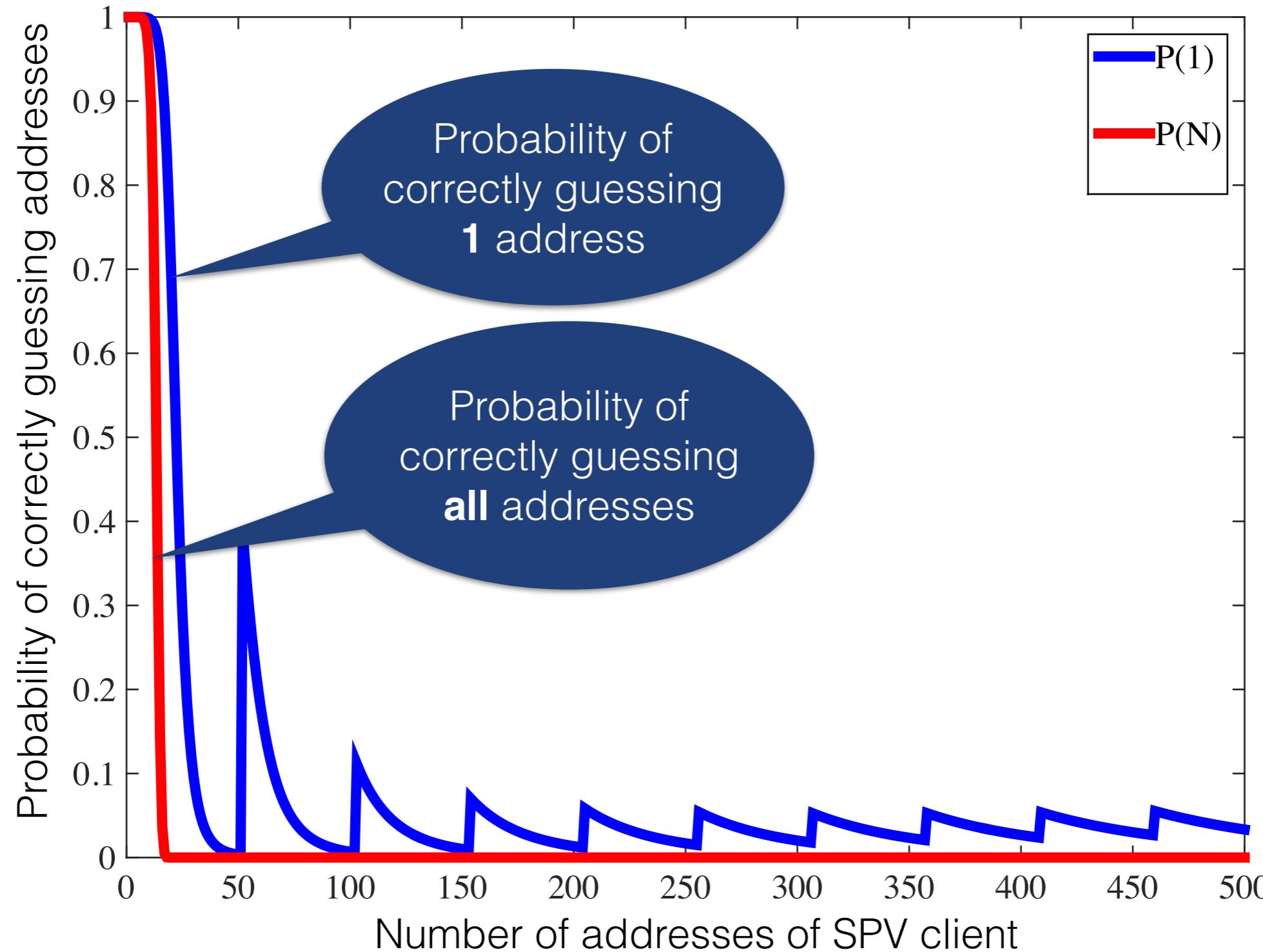
## One Bloom filter



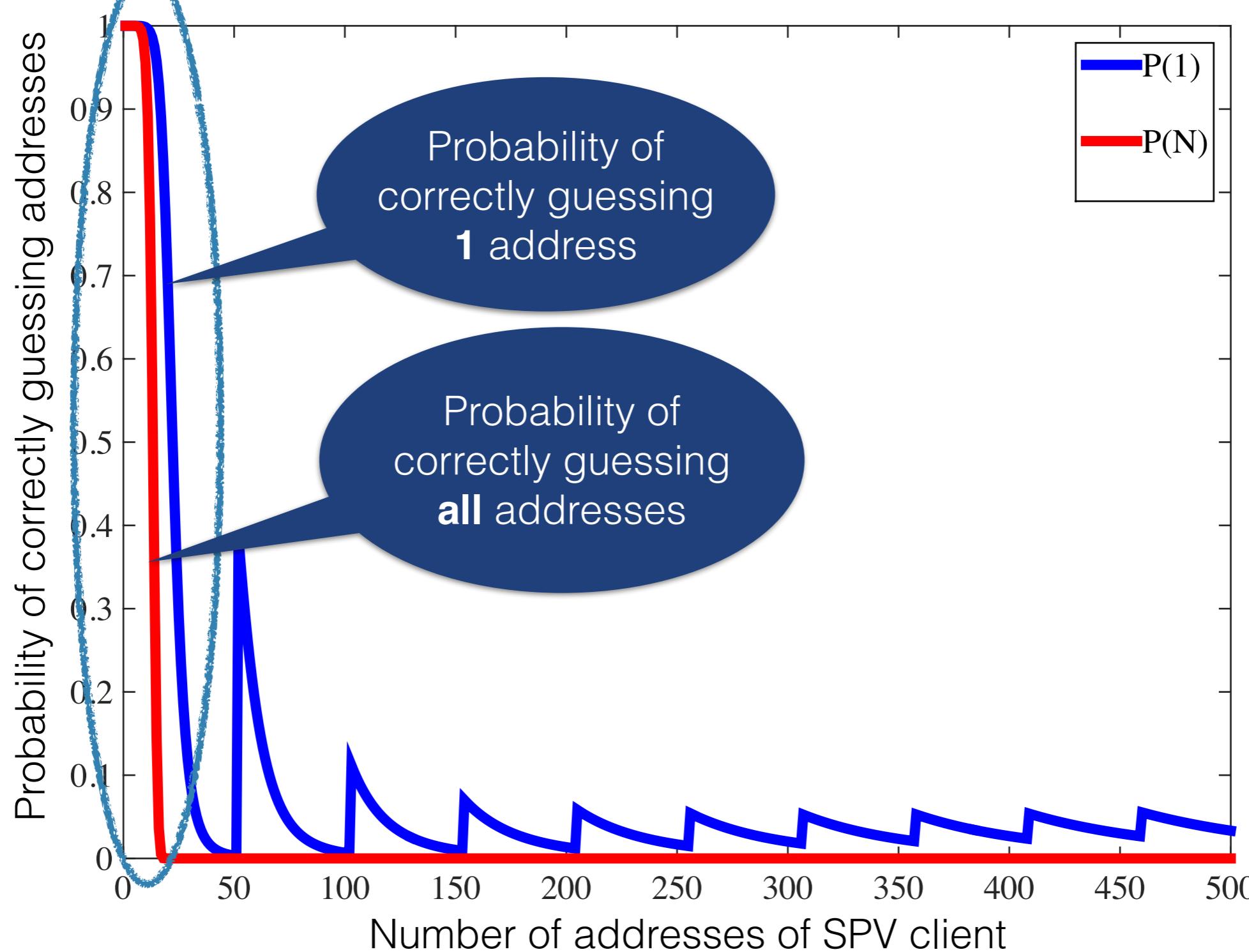
# One Bloom filter



# One Bloom filter



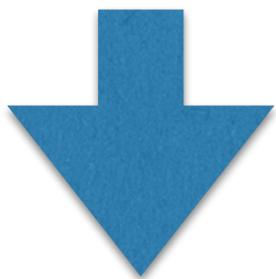
# One Bloom filter



# Multiple Bloom filters

Filter 1

0	1	0	0	1	1	0
---	---	---	---	---	---	---

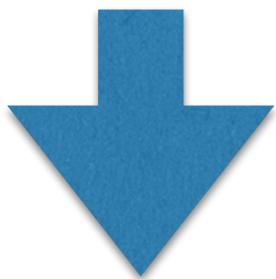


$\text{@}_1 \text{@}_2 \text{@}_3$

# Multiple Bloom filters

Filter 1

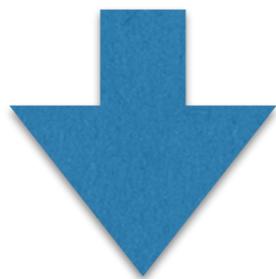
0	1	0	0	1	1	0
---	---	---	---	---	---	---



$\text{@}_1 \text{@}_2 \text{@}_3$

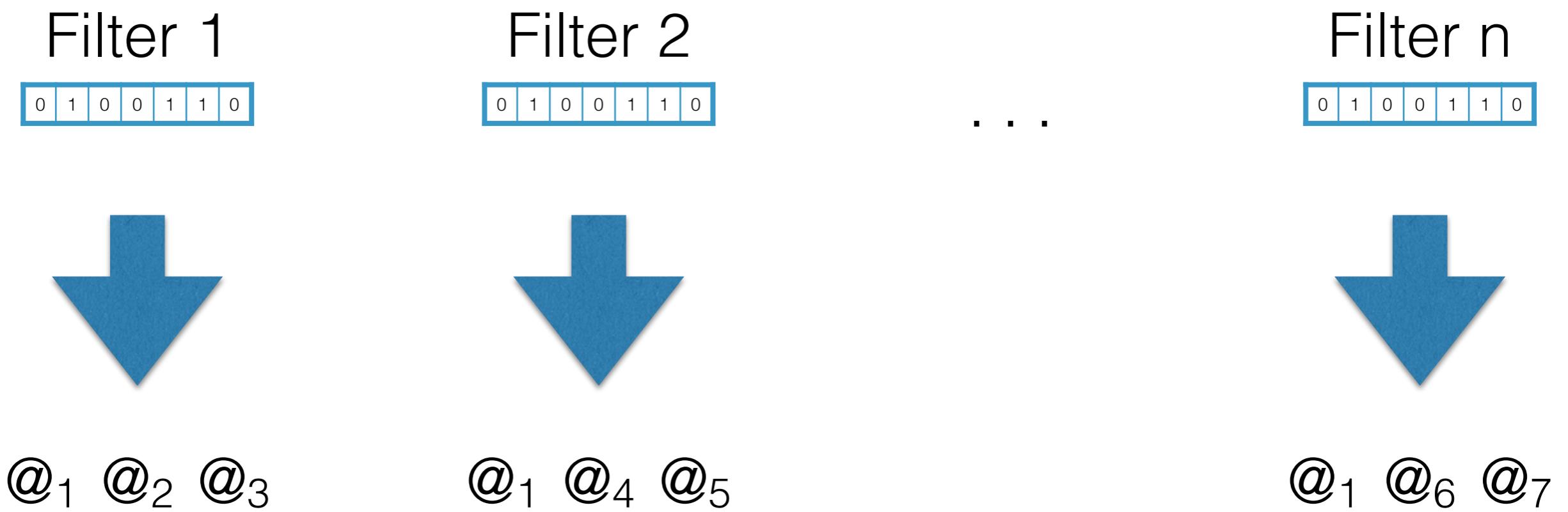
Filter 2

0	1	0	0	1	1	0
---	---	---	---	---	---	---

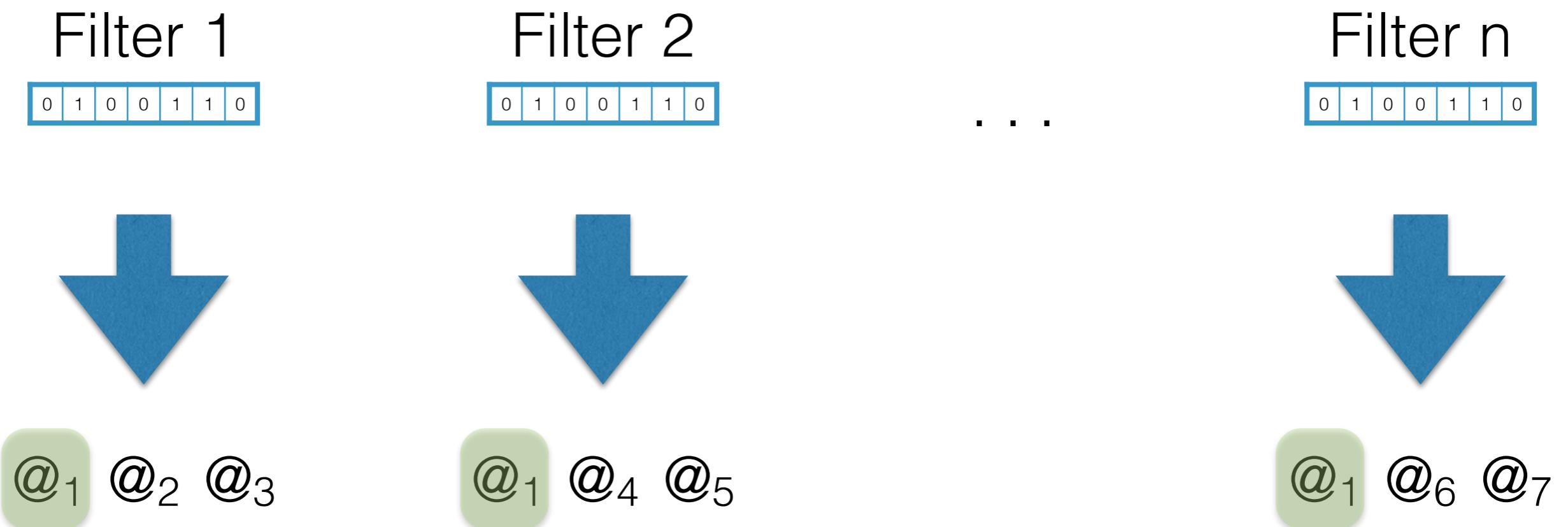


$\text{@}_1 \text{@}_4 \text{@}_5$

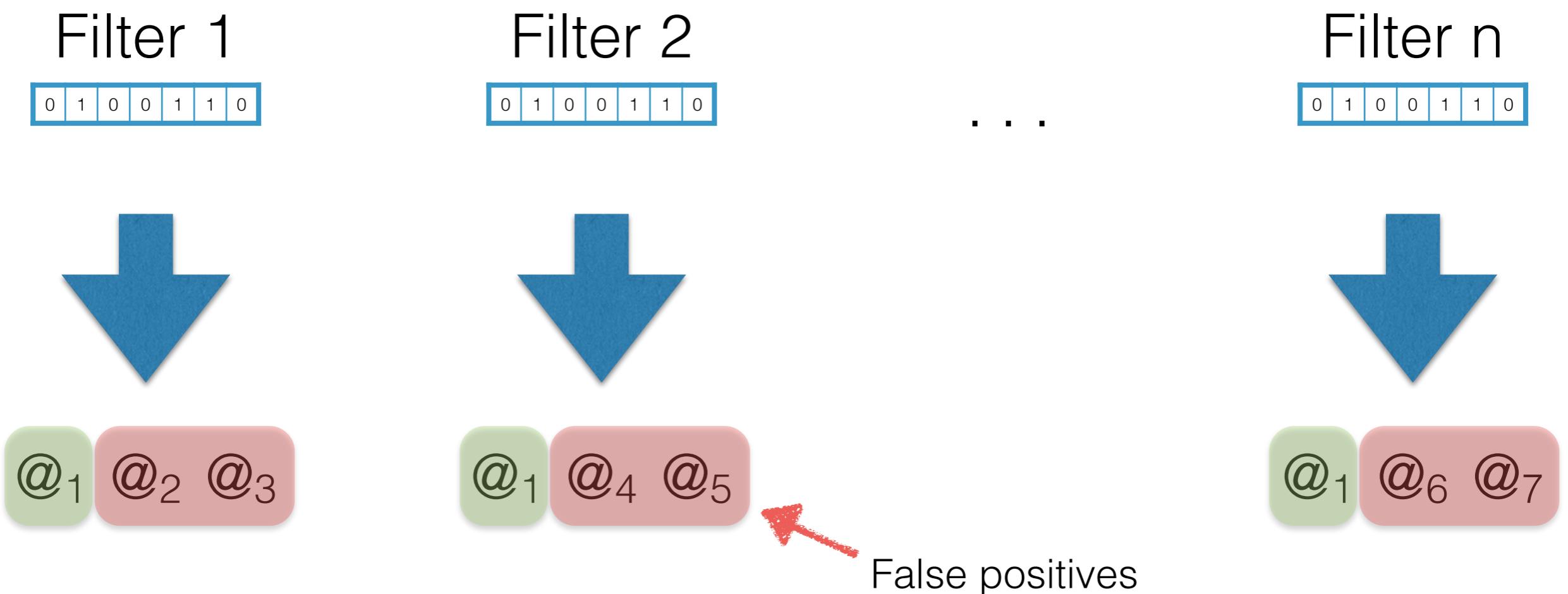
# Multiple Bloom filters



# Multiple Bloom filters



# Multiple Bloom filters



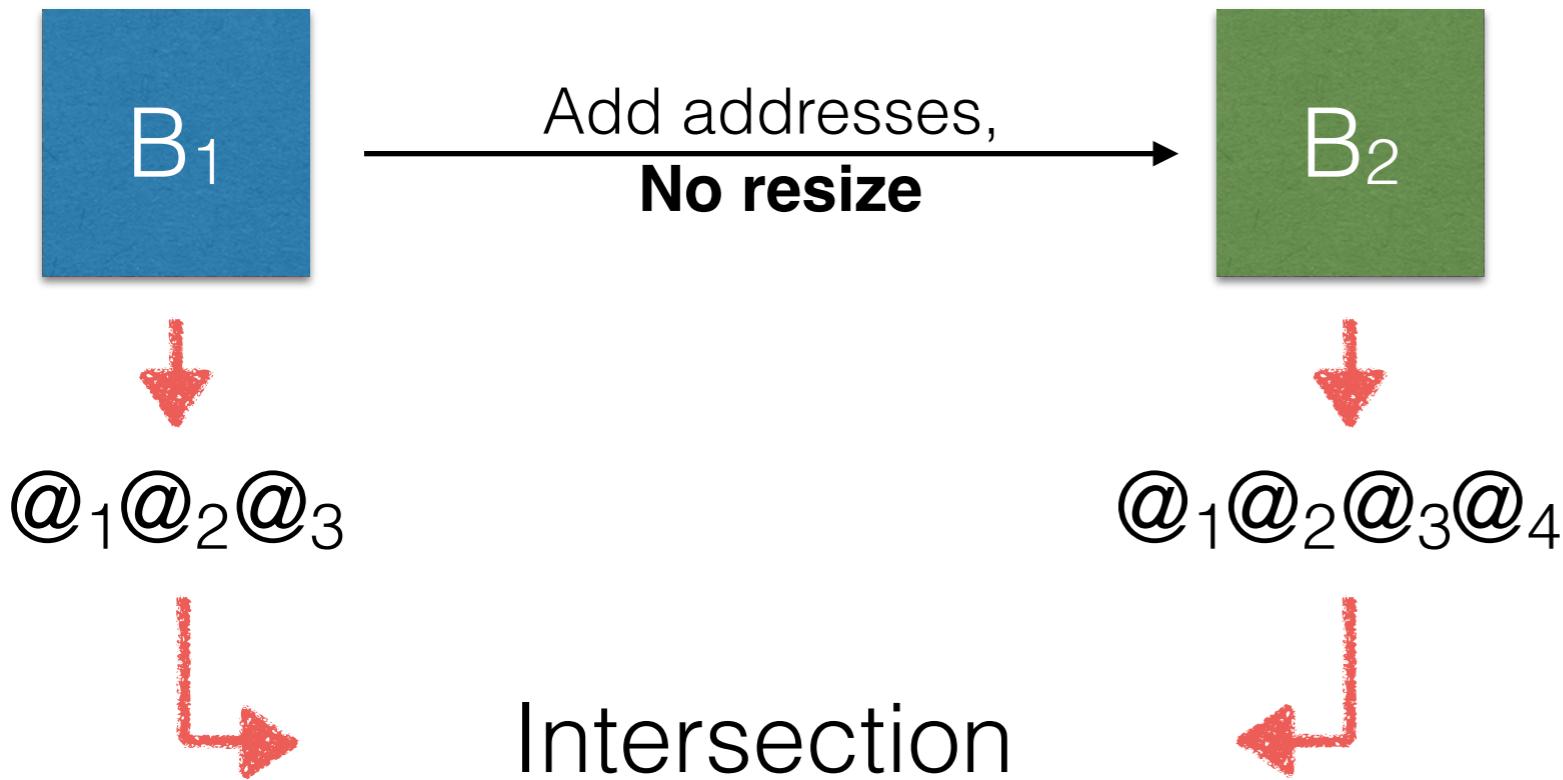
## Experiment 1 - No resize ~~1~~

Exp.	Client	Seed	Size
<b>No resize</b>	<b>Same</b>	<b>Same</b>	<b>Same</b>
<b>Resize</b>	Same	Same	Different
<b>Restart</b>	Same	Different	Same
<b>&gt; 2 filter</b>	Same	Different	Different

## Experiment 1 - No resize ~~↓↓~~

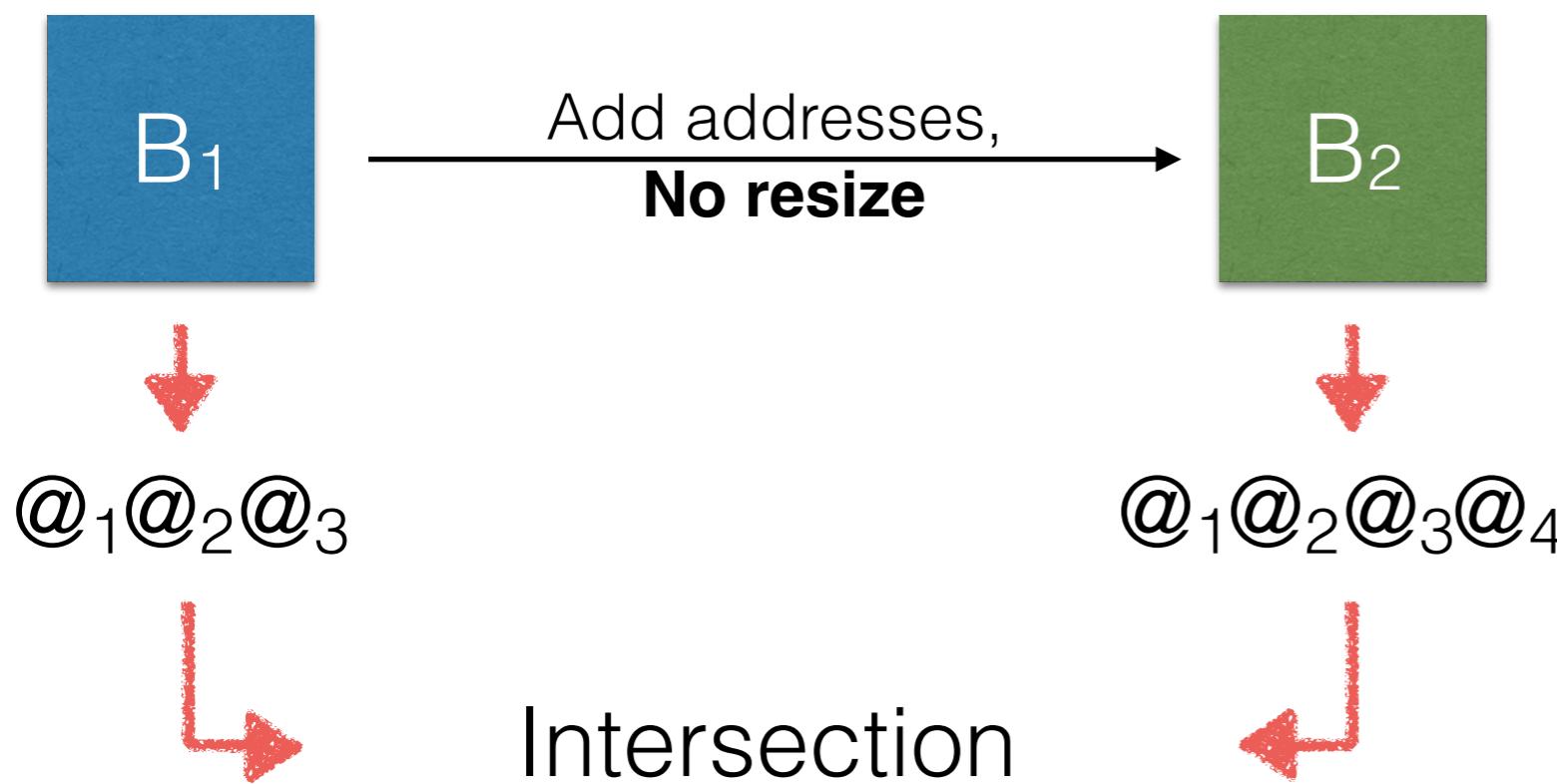
Exp.	Client	Seed	Size
No resize	Same	Same	Same
Resize	Same	Same	Different
Restart	Same	Different	Same
> 2 filter	Same	Different	Different

## Experiment 1 - No resize ~~|~~



Exp.	Client	Seed	Size
<b>No resize</b>	<b>Same</b>	<b>Same</b>	<b>Same</b>
<b>Resize</b>	Same	Same	Different
<b>Restart</b>	Same	Different	Same
<b>&gt; 2 filter</b>	Same	Different	Different

## Experiment 1 - No resize ~~1|1~~

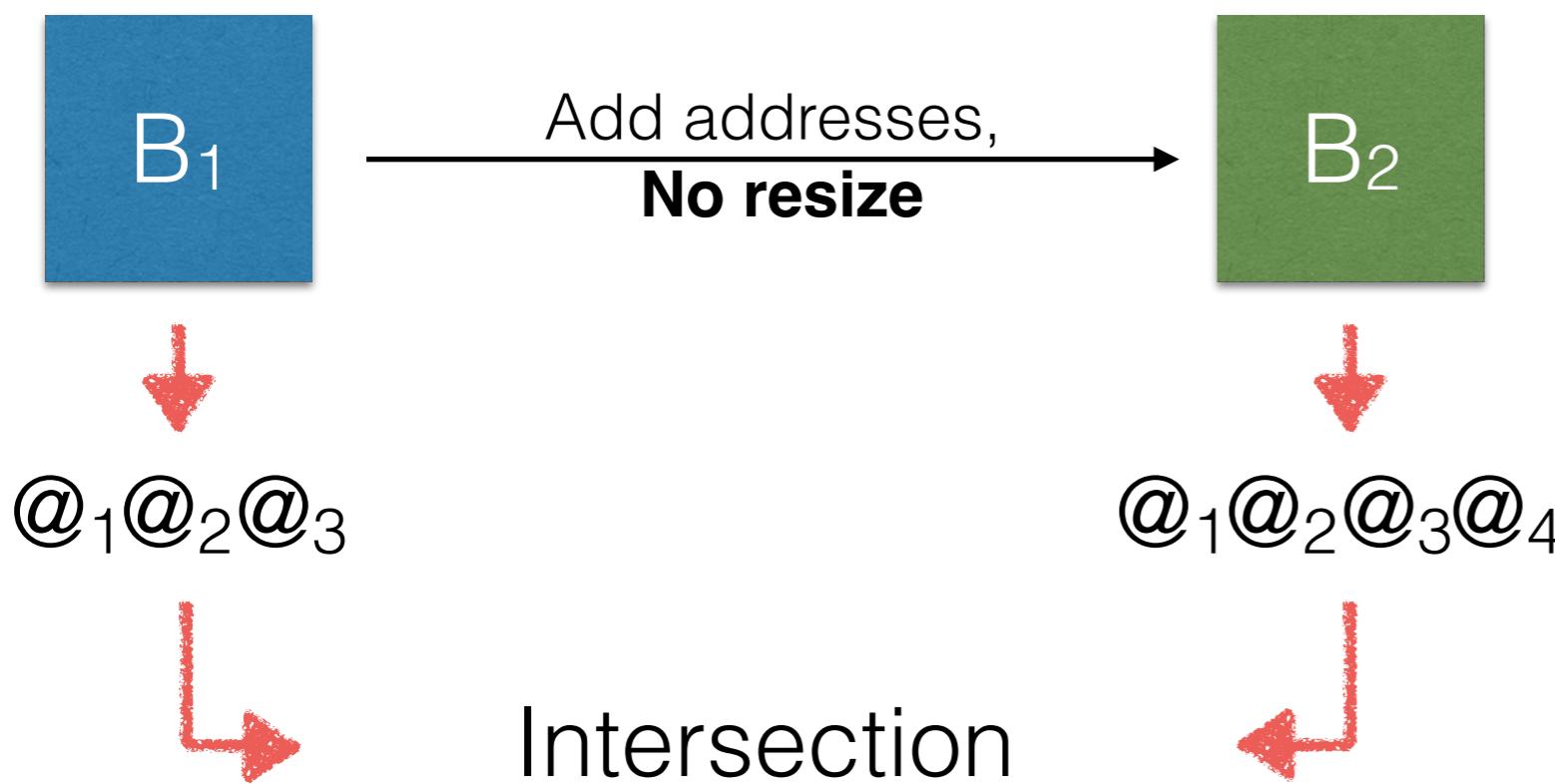


## Results

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

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

# Experiment 1 - No resize

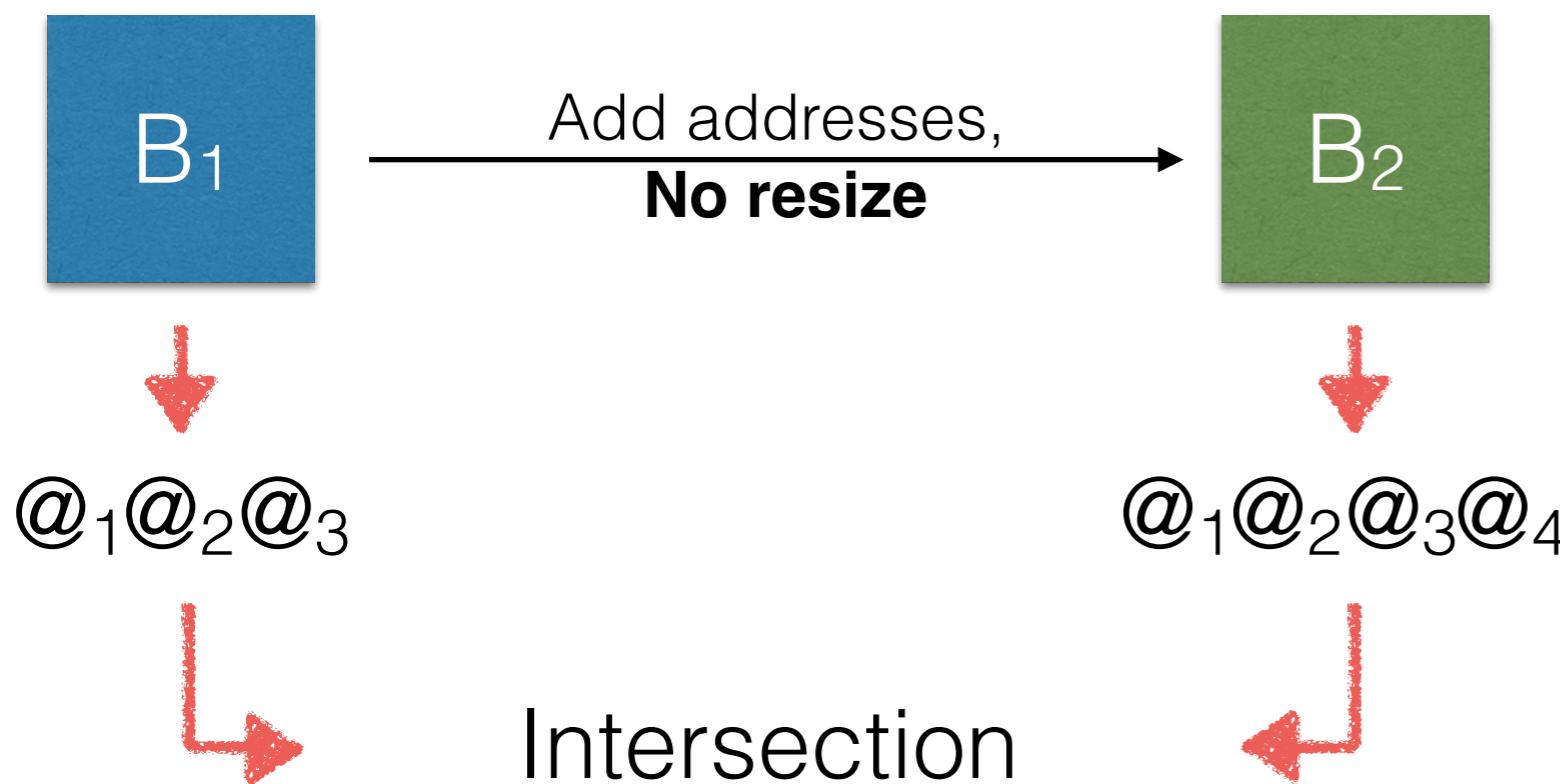


## Results

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

Exp.	Client	Seed	Size
<b>No resize</b>	<b>Same</b>	<b>Same</b>	<b>Same</b>
<b>Resize</b>	Same	Same	Different
<b>Restart</b>	Same	Different	Same
<b>&gt; 2 filter</b>	Same	Different	Different

# Experiment 1 - No resize

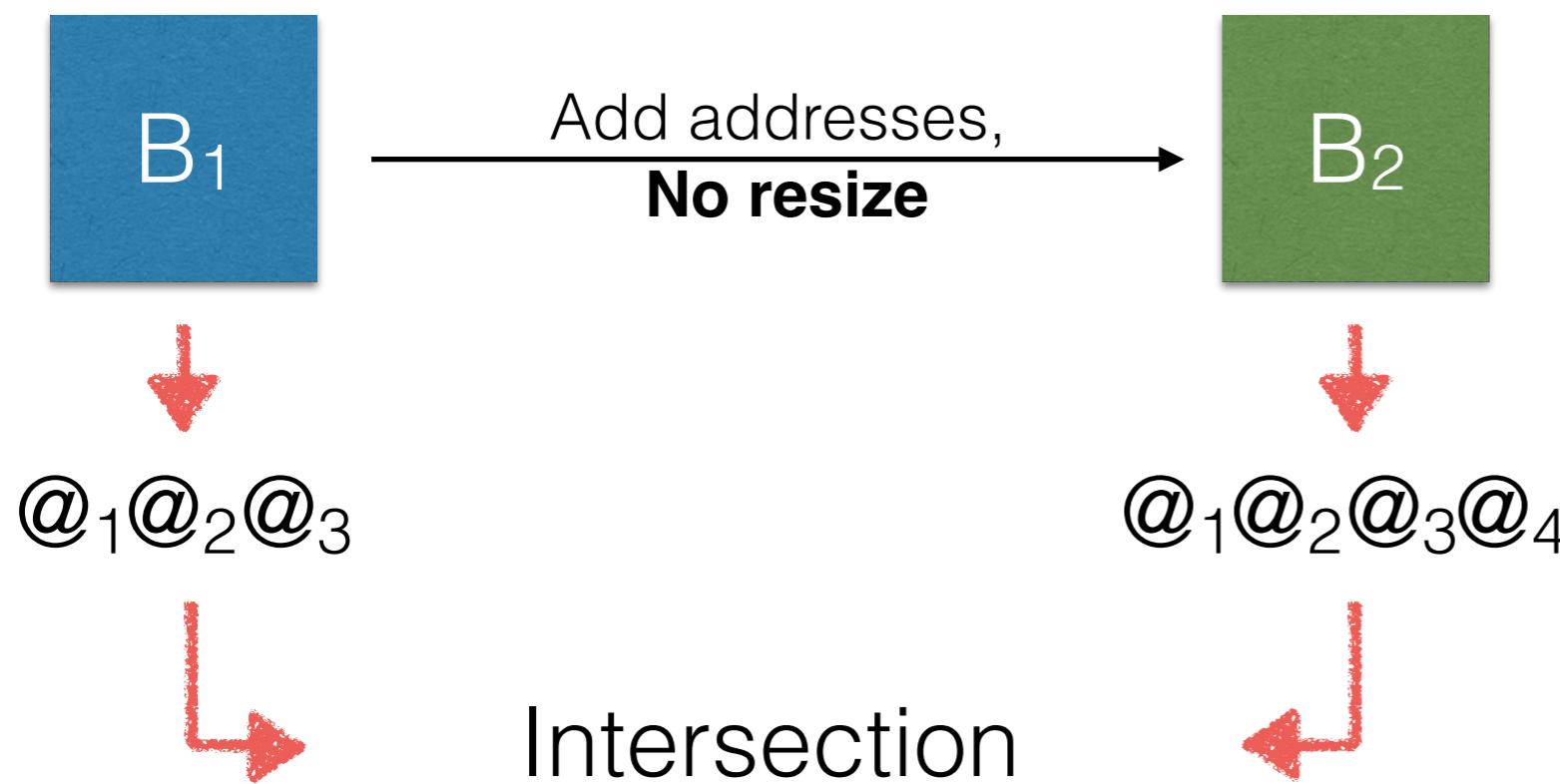


## Results

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

Exp.	Client	Seed	Size
<b>No resize</b>	<b>Same</b>	<b>Same</b>	<b>Same</b>
<b>Resize</b>	Same	Same	Different
<b>Restart</b>	Same	Different	Same
<b>&gt; 2 filter</b>	Same	Different	Different

# Experiment 1 - No resize



## Results

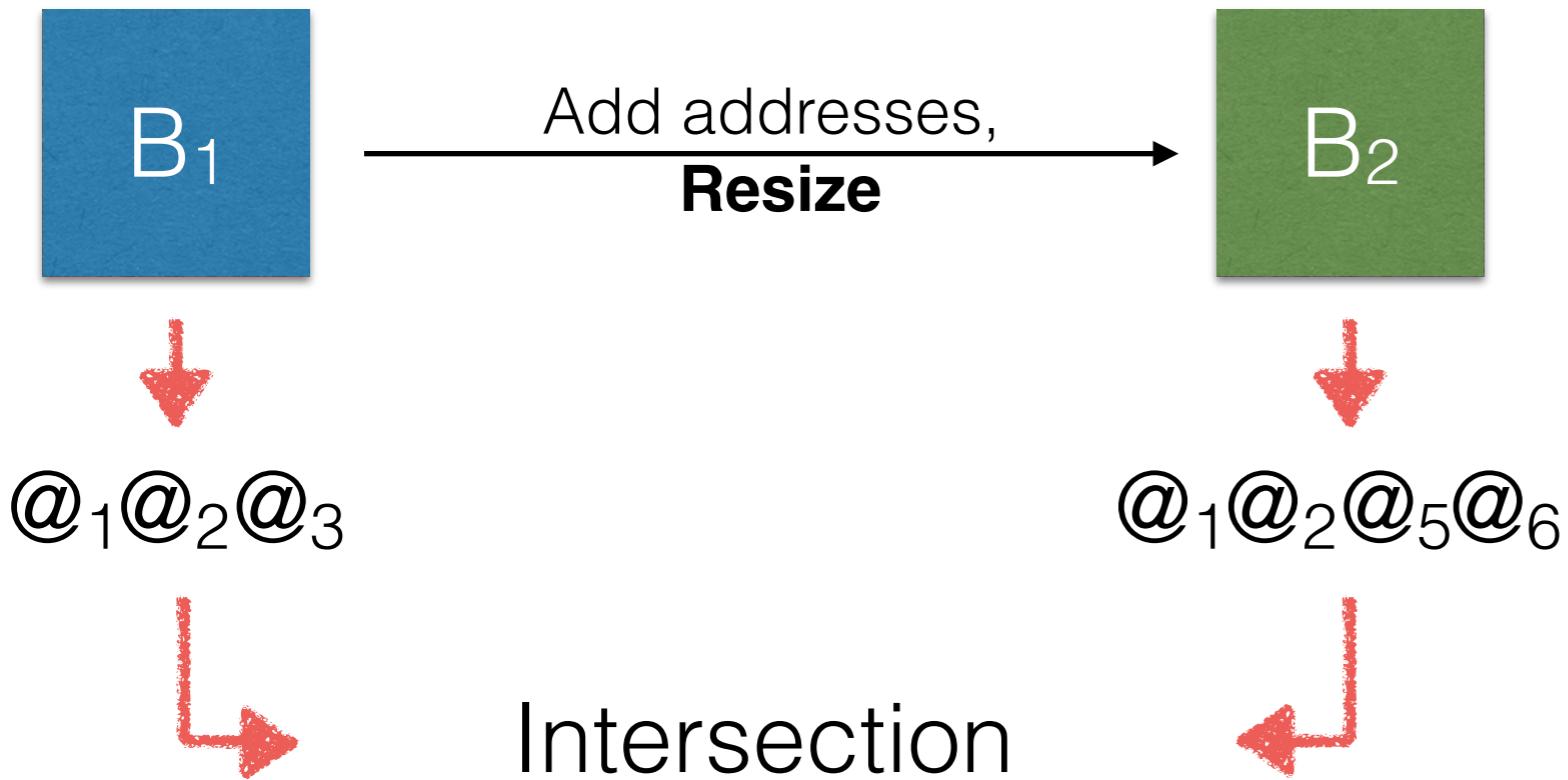
Target FPR (%)	P(1) with 2 BF	P(1) with 1 BF
0.05	0.2990	0.2910
0.1	0.1020	0.1070
0.5	0.0078	0.0075

no change of privacy

Exp.	Client	Seed	Size
<b>No resize</b>	<b>Same</b>	<b>Same</b>	<b>Same</b>
<b>Resize</b>	Same	Same	Different
<b>Restart</b>	Same	Different	Same
<b>&gt; 2 filter</b>	Same	Different	Different

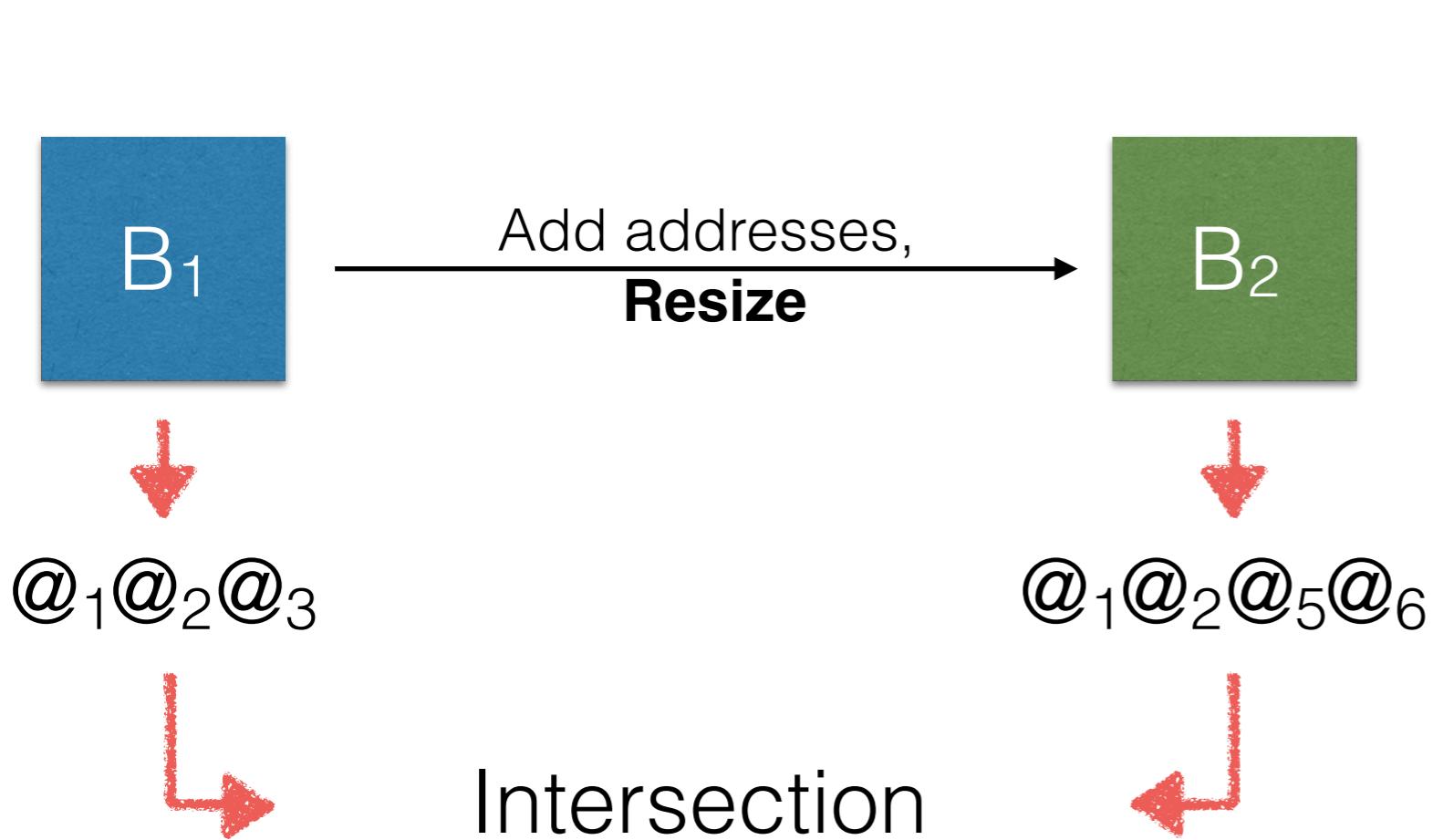
- Yield the same positives
- The adversary does not learn a lot

## Experiment 2 - Resize ↪ ↪



Exp.	Client	Seed	Size
No resize	Same	Same	Same
<b>Resize</b>	<b>Same</b>	<b>Same</b>	<b>Different</b>
Restart	Same	Different	Same
> 2 filter	Same	Different	Different

# Experiment 2 - Resize ↶ ↷

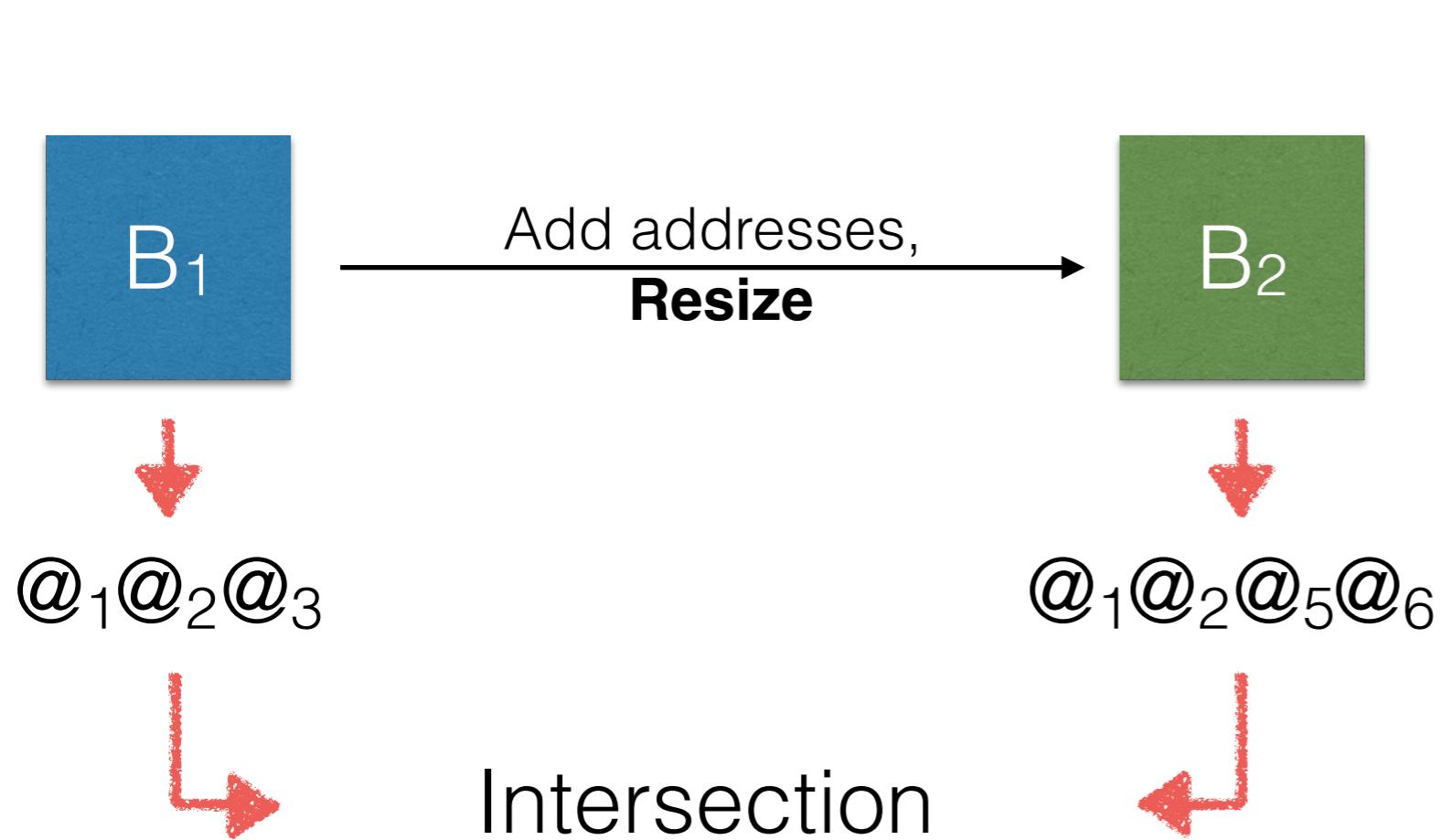


Results

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

Exp.	Client	Seed	Size
No resize	Same	Same	Same
<b><u>Resize</u></b>	<b>Same</b>	<b>Same</b>	<b>Different</b>
Restart	Same	Different	Same
> 2 filter	Same	Different	Different

# Experiment 2 - Resize | ↻ ↺

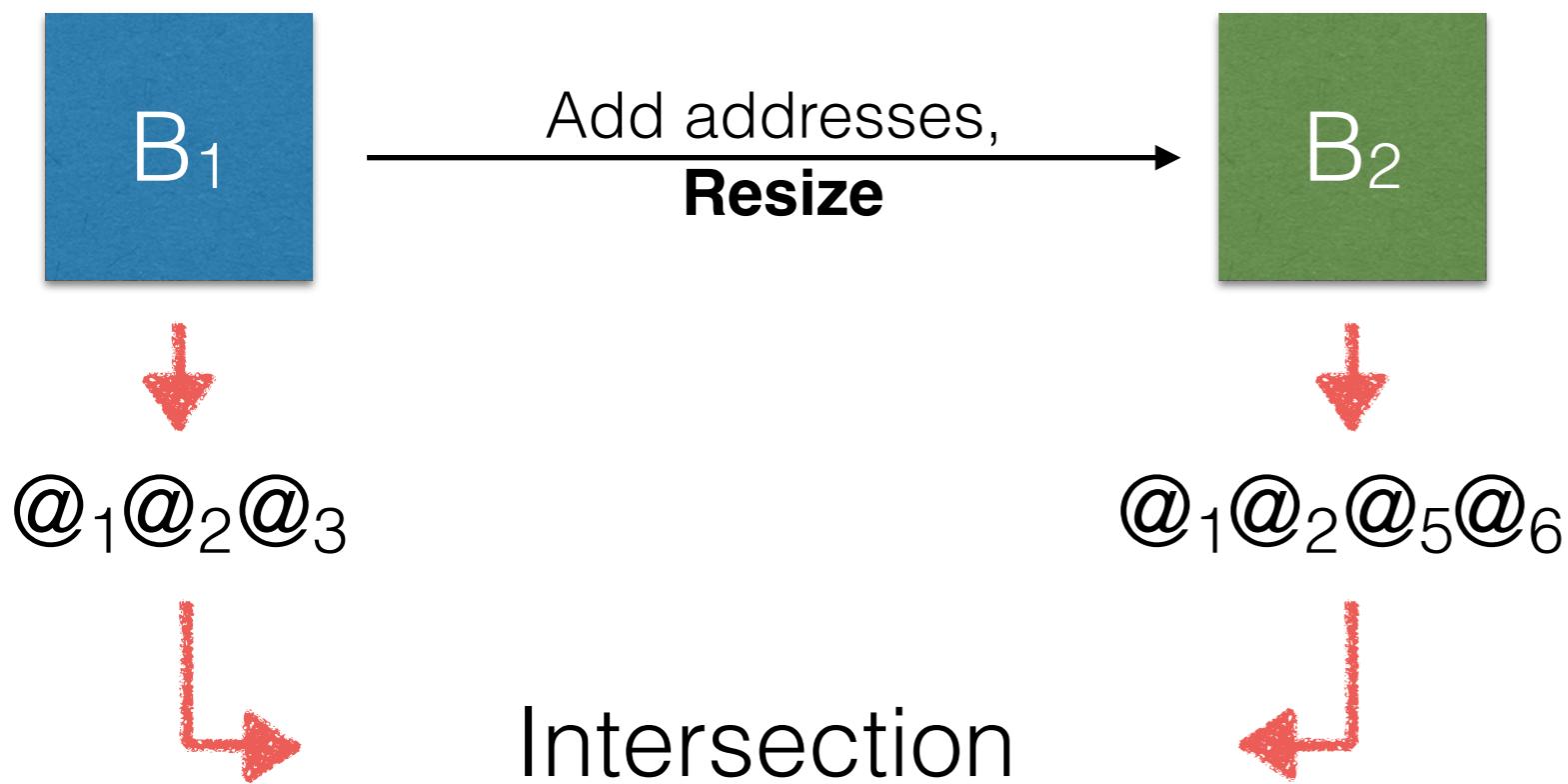


Results

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

Exp.	Client	Seed	Size
No resize	Same	Same	Same
<u>Resize</u>	<b>Same</b>	<b>Same</b>	<b>Different</b>
Restart	Same	Different	Same
> 2 filter	Same	Different	Different

# Experiment 2 - Resize ↶ ◻

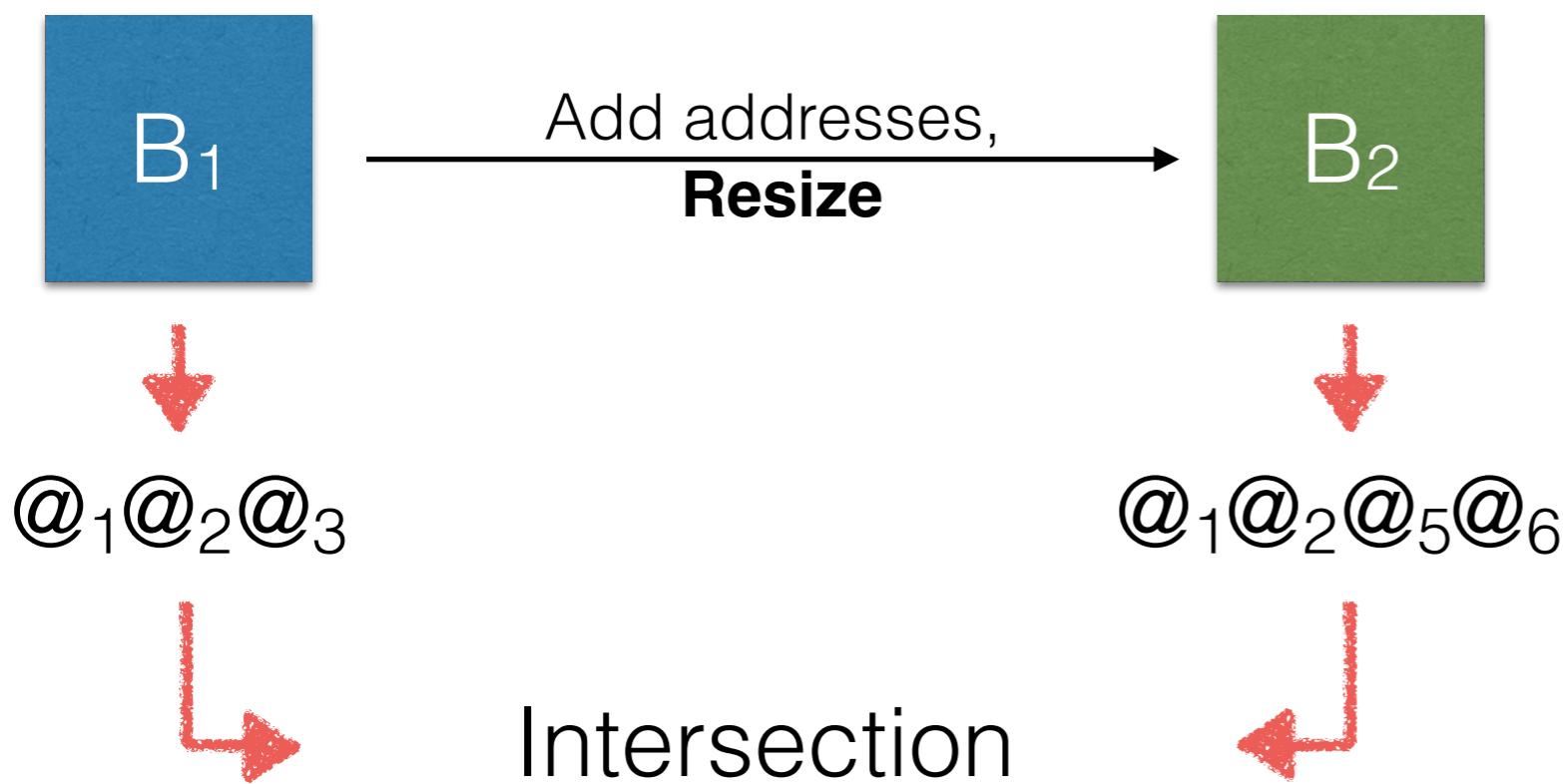


## Results

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

Exp.	Client	Seed	Size
No resize	Same	Same	Same
<u>Resize</u>	<b>Same</b>	<b>Same</b>	<b>Different</b>
Restart	Same	Different	Same
> 2 filter	Same	Different	Different

## Experiment 2 - Resize ↪ ↪



### Results

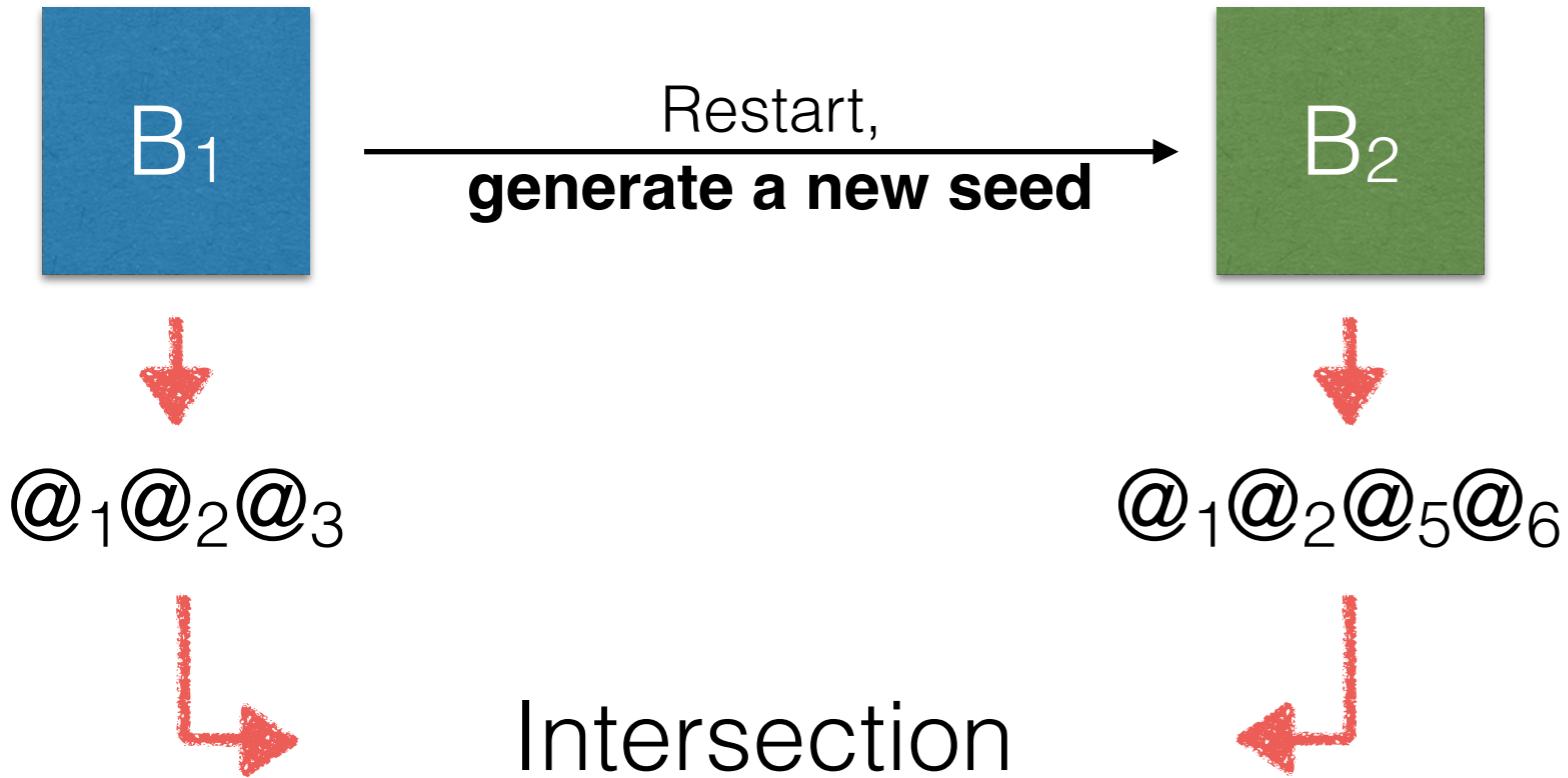
Target FPR (%)	P(1) with 2 BF	P(1) with 1 BF
0.1	0.98	0.03

significant change

Exp.	Client	Seed	Size
No resize	Same	Same	Same
<b>Resize</b>	<b>Same</b>	<b>Same</b>	<b>Different</b>
Restart	Same	Different	Same
> 2 filter	Same	Different	Different

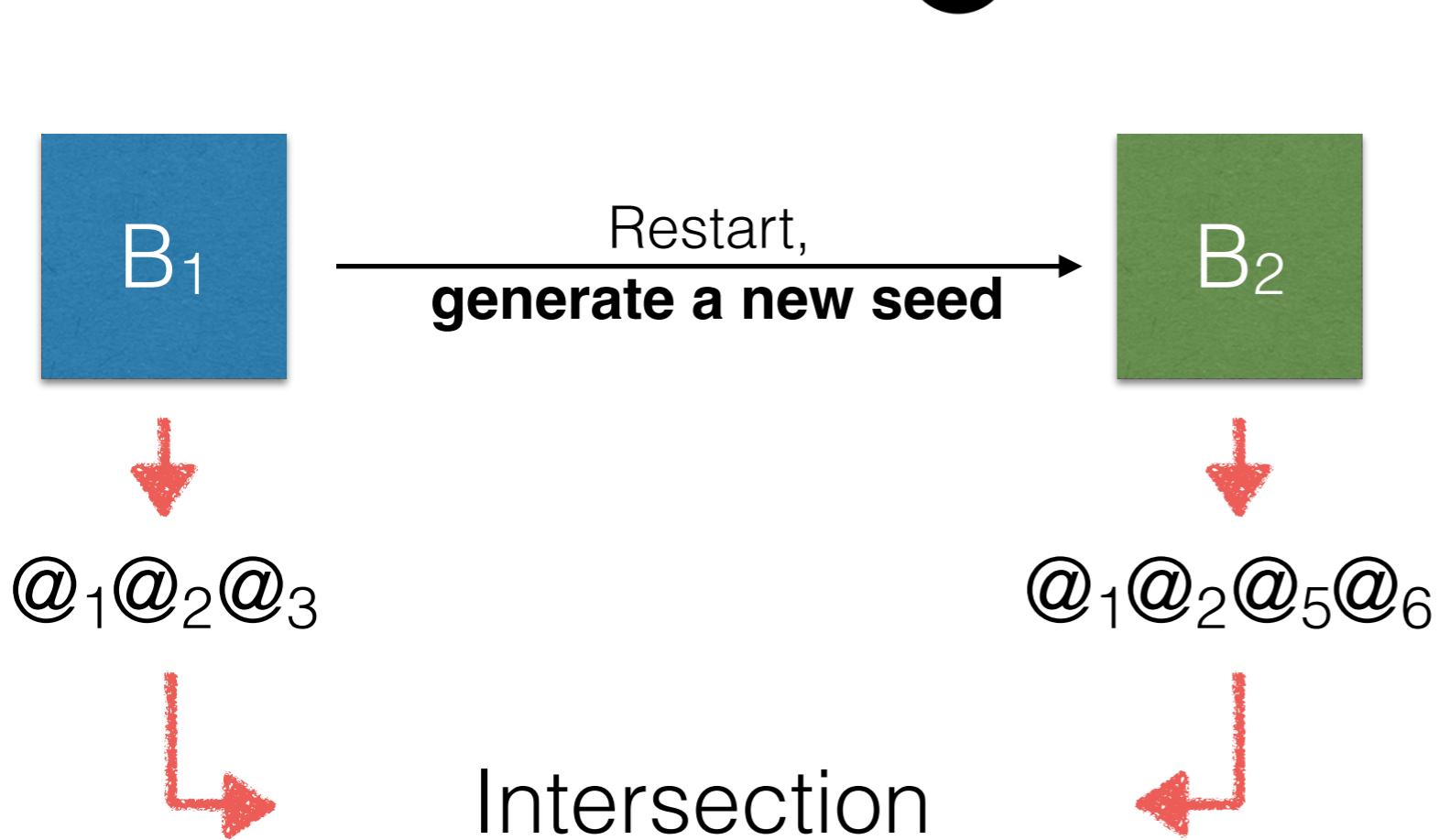
- Different BF sizes improve the attack

## Experiment 3 - restart



Exp.	Client	Seed	Size
No resize	Same	Same	Same
Resize	Same	Same	Different
<b>Restart</b>	<b>Same</b>	<b>Different</b>	<b>Same</b>
> 2 filter	Same	Different	Different

## Experiment 3 - restart

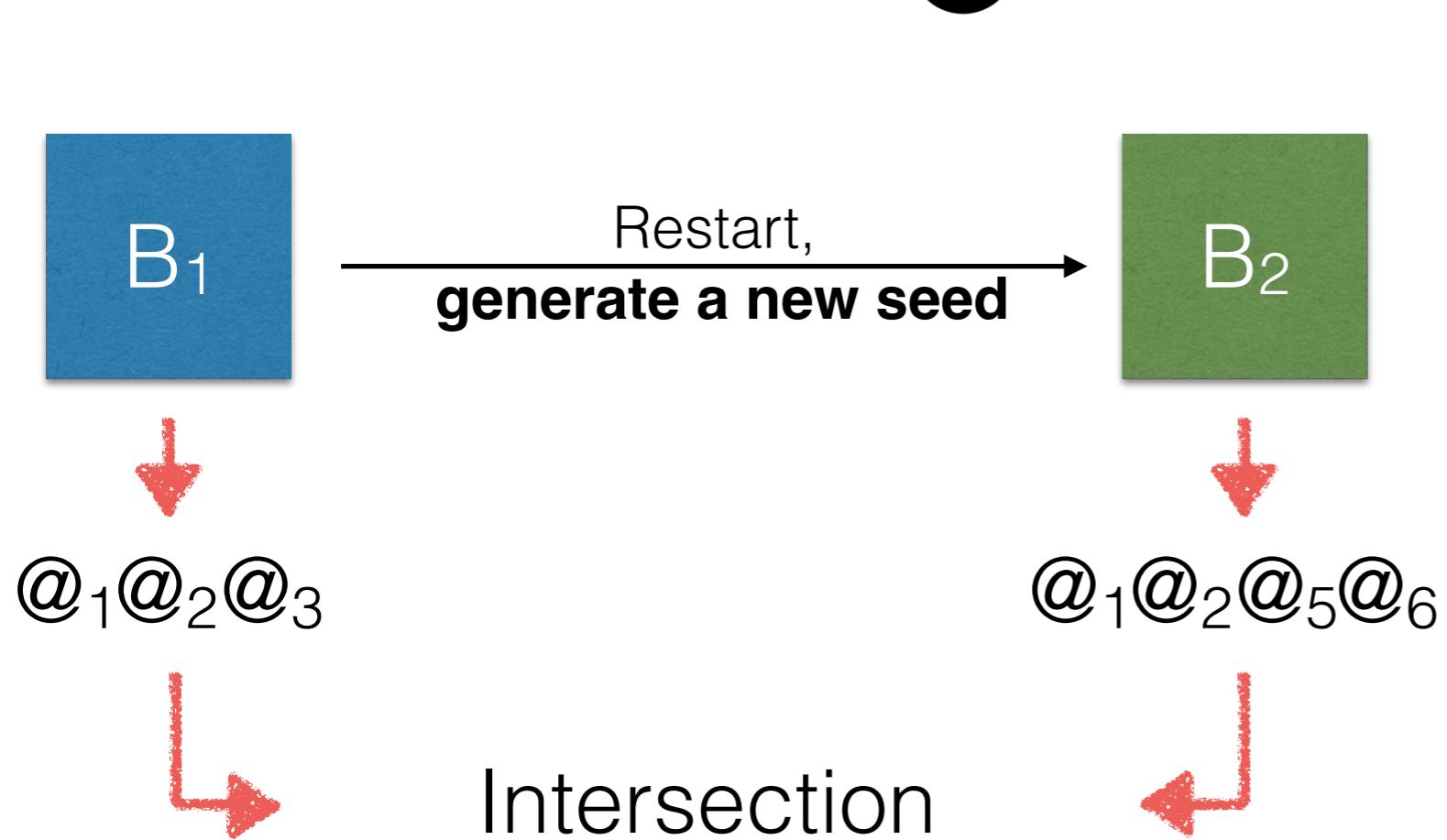


## Results

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

Exp.	Client	Seed	Size
No resize	Same	Same	Same
Resize	Same	Same	Different
<b>Restart</b>	<b>Same</b>	<b>Different</b>	<b>Same</b>
> 2 filter	Same	Different	Different

## Experiment 3 - restart



## Results

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

Exp.	Client	Seed	Size
No resize	Same	Same	Same
Resize	Same	Same	Different
<b>Restart</b>	<b>Same</b>	<b>Different</b>	<b>Same</b>
> 2 filter	Same	Different	Different

# Experiment 3 - restart

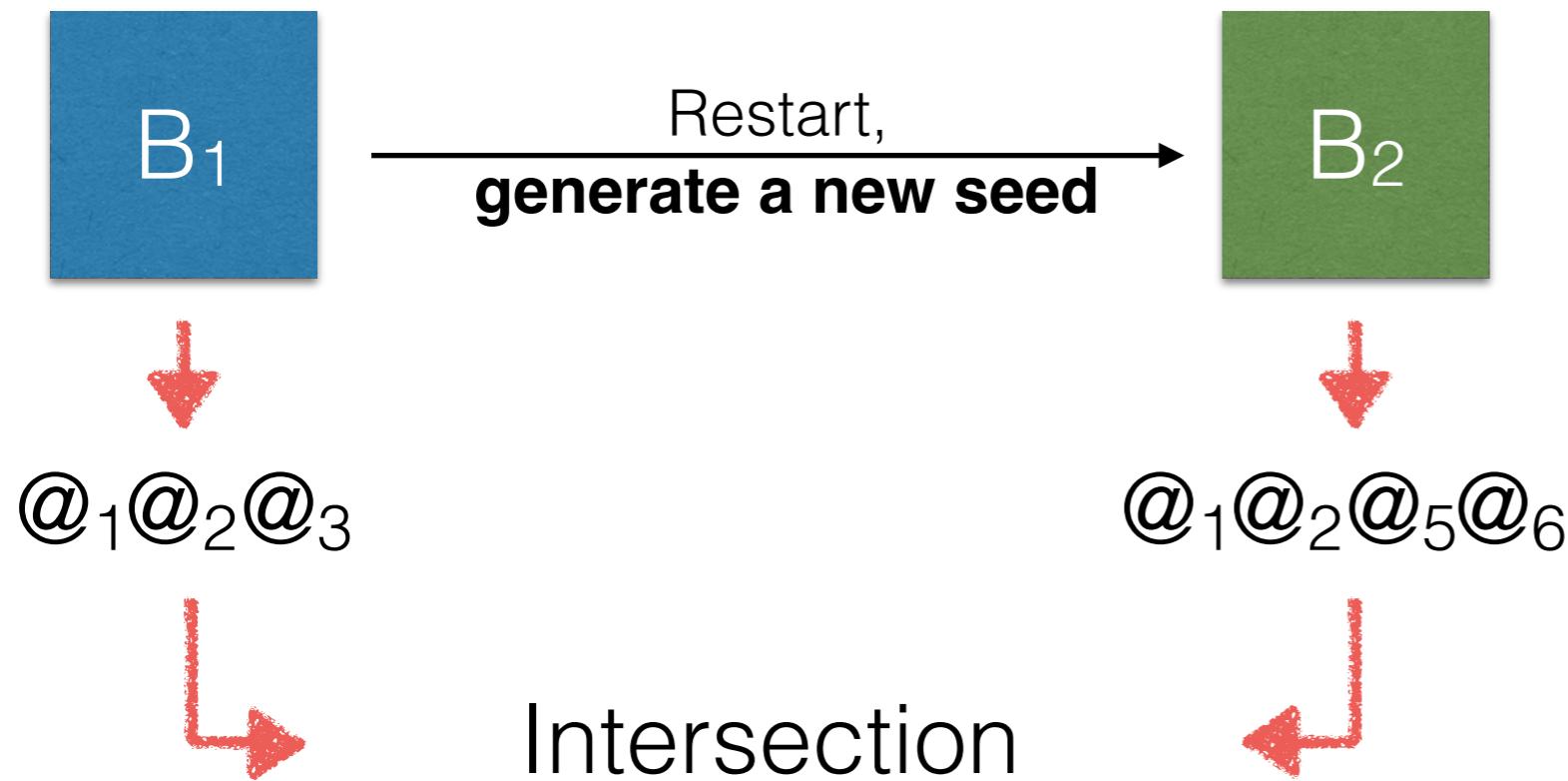
The diagram illustrates a state transition between two states,  $B_1$  and  $B_2$ . State  $B_1$  is represented by a blue square containing the text  $\text{@}_1\text{@}_2\text{@}_3$ . State  $B_2$  is represented by a green square containing the text  $\text{@}_1\text{@}_2\text{@}_5\text{@}_6$ . A horizontal arrow points from  $B_1$  to  $B_2$ , labeled "Restart,  
**generate a new seed**". Below the arrows, red hand-drawn style arrows point downwards from each state to the text below them. Red L-shaped arrows point upwards from the text back towards the respective states.

## Results

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

Exp.	Client	Seed	Size
No resize	Same	Same	Same
Resize	Same	Same	Different
<u>Restart</u>	<b>Same</b>	<b>Different</b>	<b>Same</b>
> 2 filter	Same	Different	Different

# Experiment 3 - restart



Exp.	Client	Seed	Size
No resize	Same	Same	Same
Resize	Same	Same	Different
Restart	<b>Same</b>	<b>Different</b>	<b>Same</b>
> 2 filter	Same	Different	Different

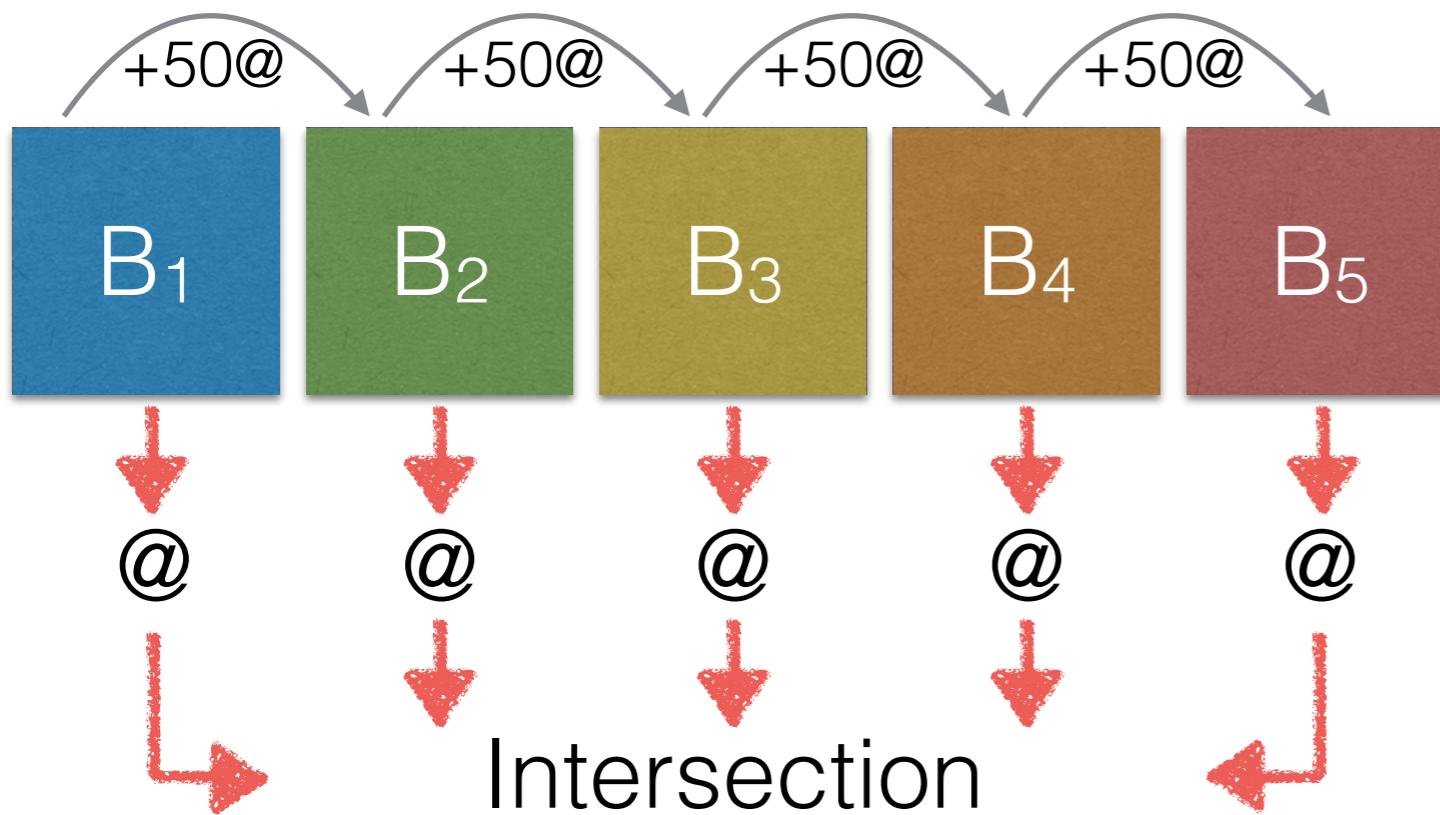
## Results

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

# significant change

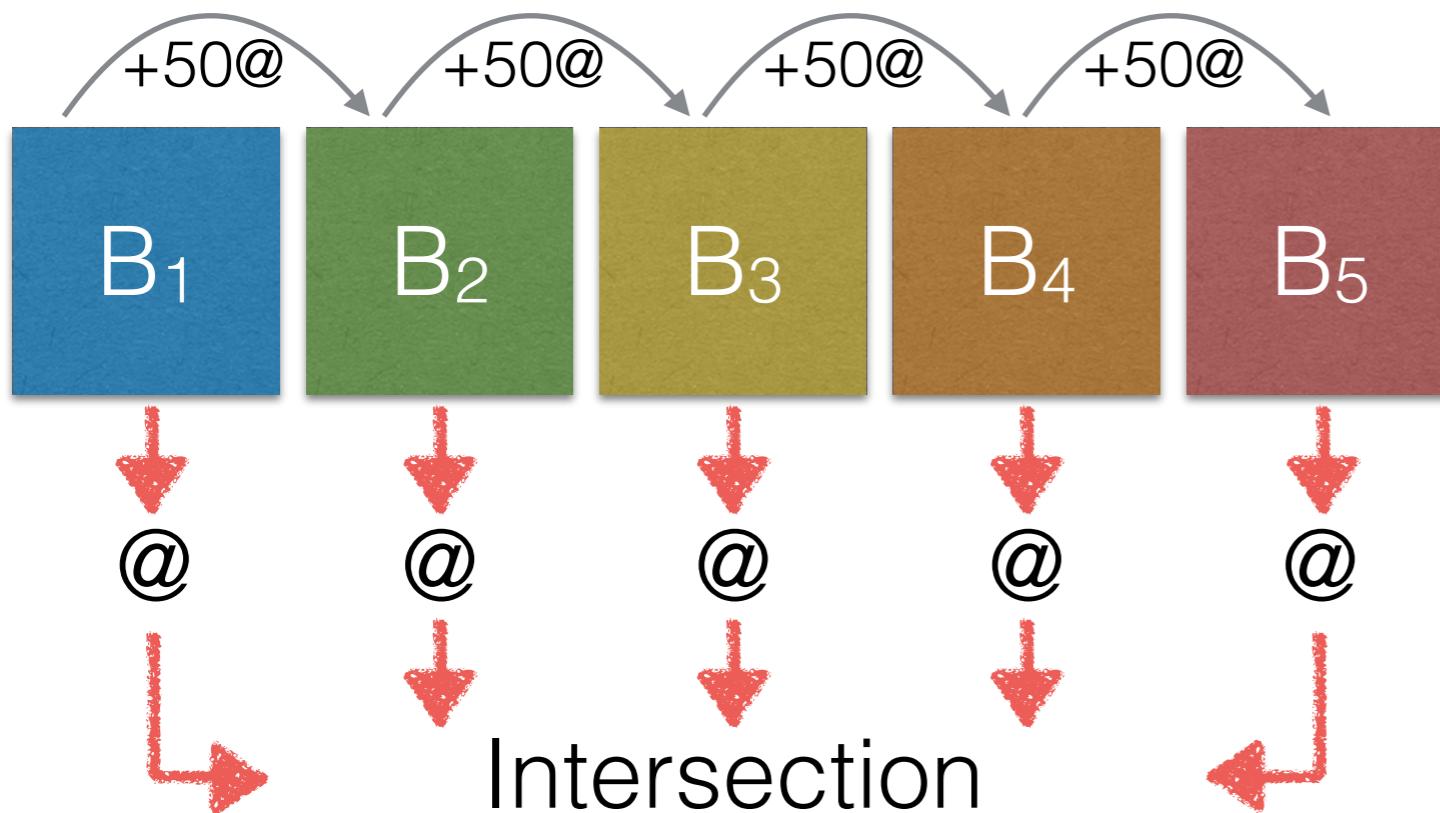
- Different BF seeds improve the attack

## Experiment 4 - More than 2 filter



Exp.	Client	Seed	Size
No resize	Same	Same	Same
Resize	Same	Same	Different
Restart	Same	Different	Same
<b>&gt; 2 filter</b>	<b>Same</b>	<b>Different</b>	<b>Different</b>

## Experiment 4 - More than 2 filter

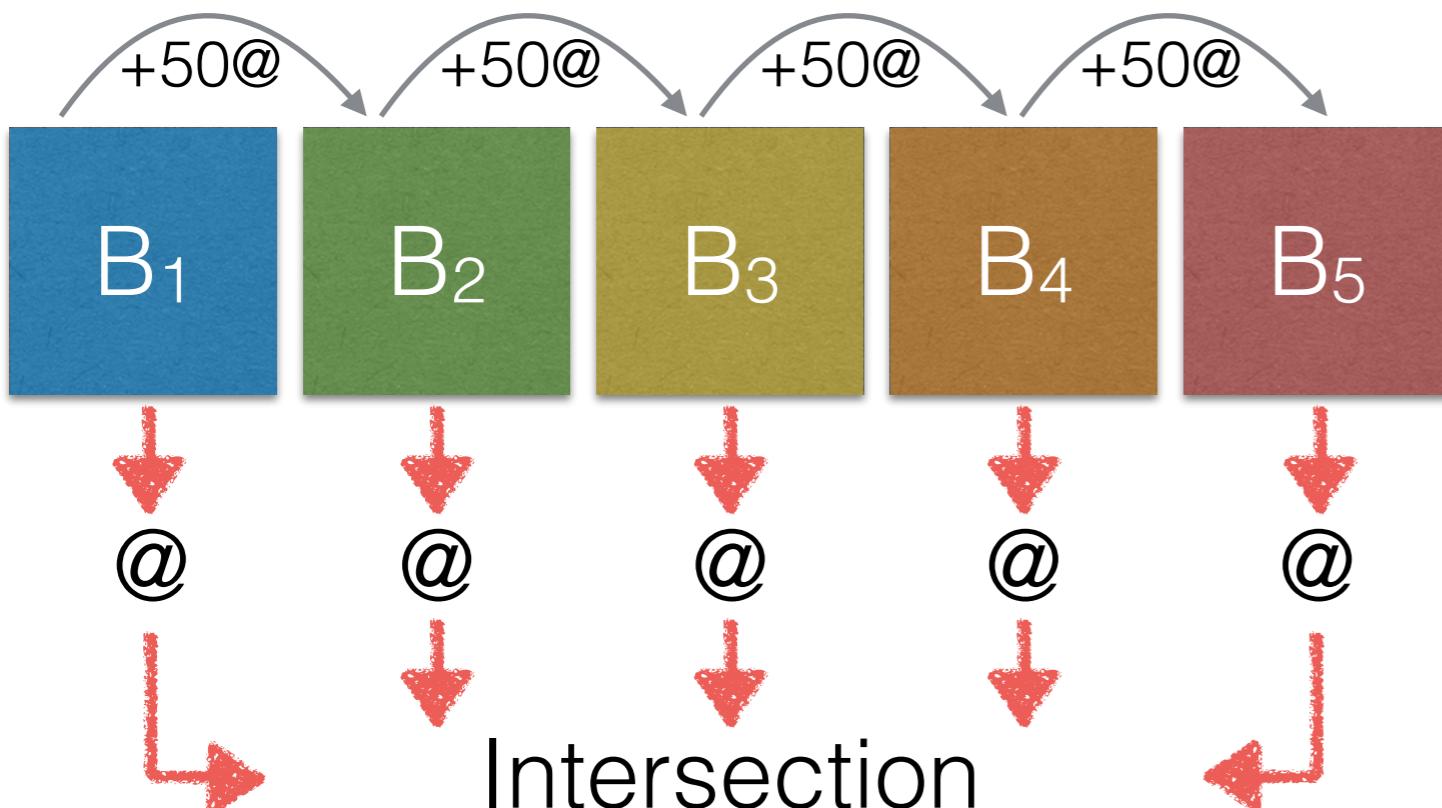


### Results

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

Exp.	Client	Seed	Size
No resize	Same	Same	Same
Resize	Same	Same	Different
Restart	Same	Different	Same
<b>&gt; 2 filter</b>	<b>Same</b>	<b>Different</b>	<b>Different</b>

## Experiment 4 - More than 2 filter



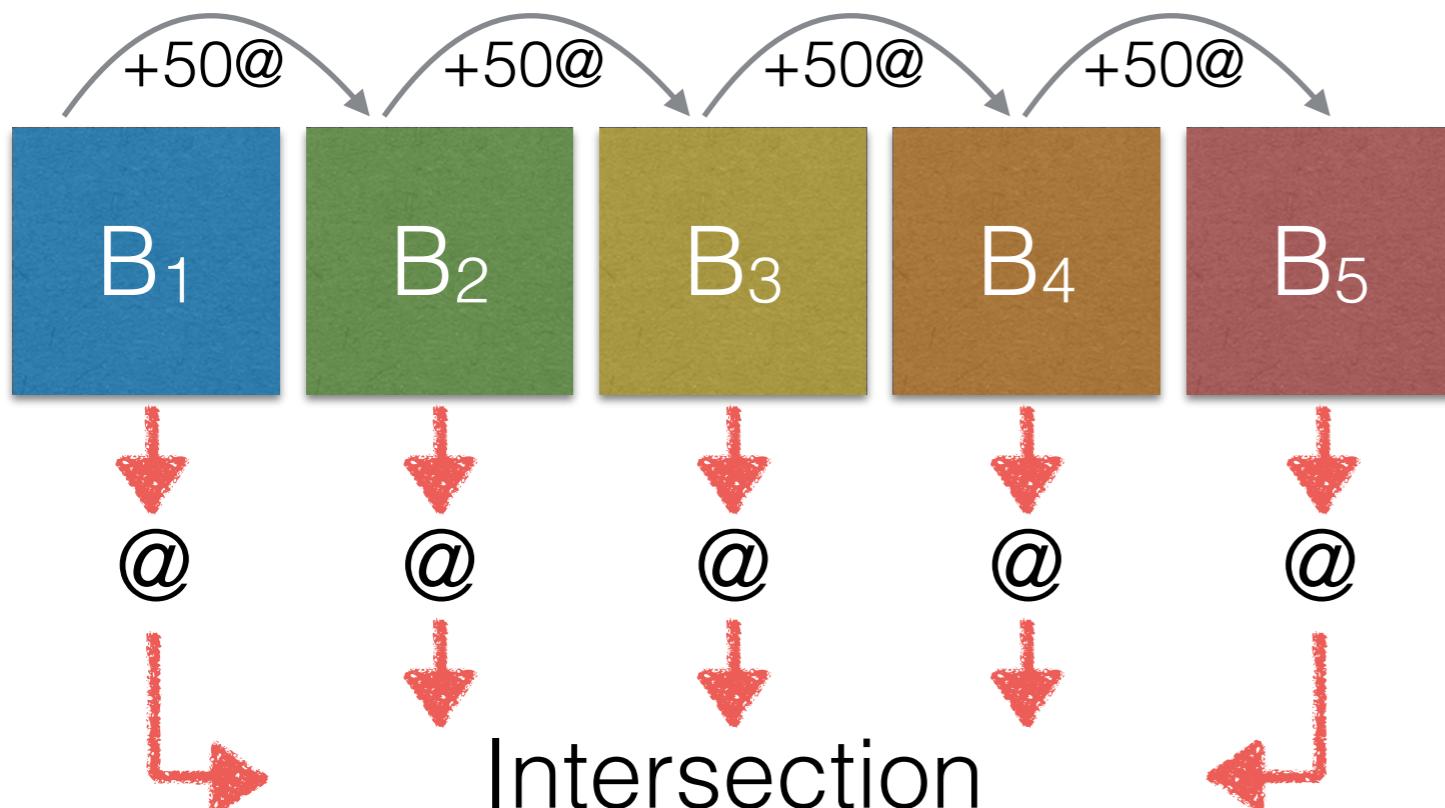
## Results

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

Guessing all addresses

Exp.	Client	Seed	Size
No resize	Same	Same	Same
Resize	Same	Same	Different
Restart	Same	Different	Same
<b>&gt; 2 filter</b>	<b>Same</b>	<b>Different</b>	<b>Different</b>

## Experiment 4 - More than 2 filter



## Results

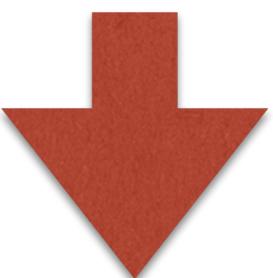
Target FPR (%)	P(N) given 3 or more BF
0.05	~1
0.1	~1

Guessing all addresses

3 Bloom filter

Exp.	Client	Seed	Size
No resize	Same	Same	Same
Resize	Same	Same	Different
Restart	Same	Different	Same
> 2 filter	<b>Same</b>	<b>Different</b>	<b>Different</b>

All addresses yielded by B<sub>1</sub> are leaked

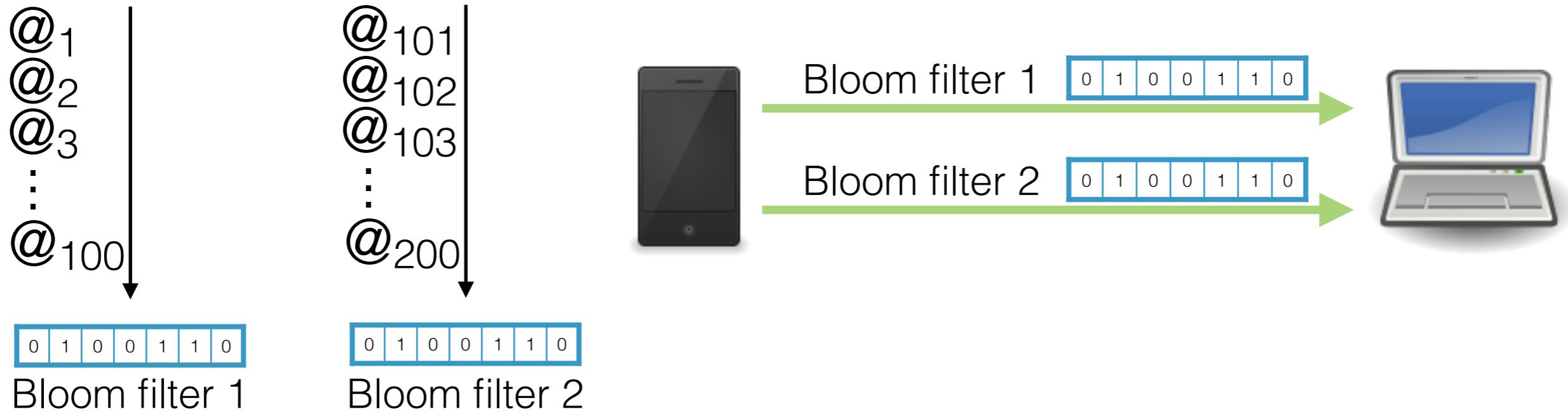


## Observations

1. Need constant FPR
2. Multiple Bloom filter with different parameters
3. SPV clients should keep state (e.g., about seed)

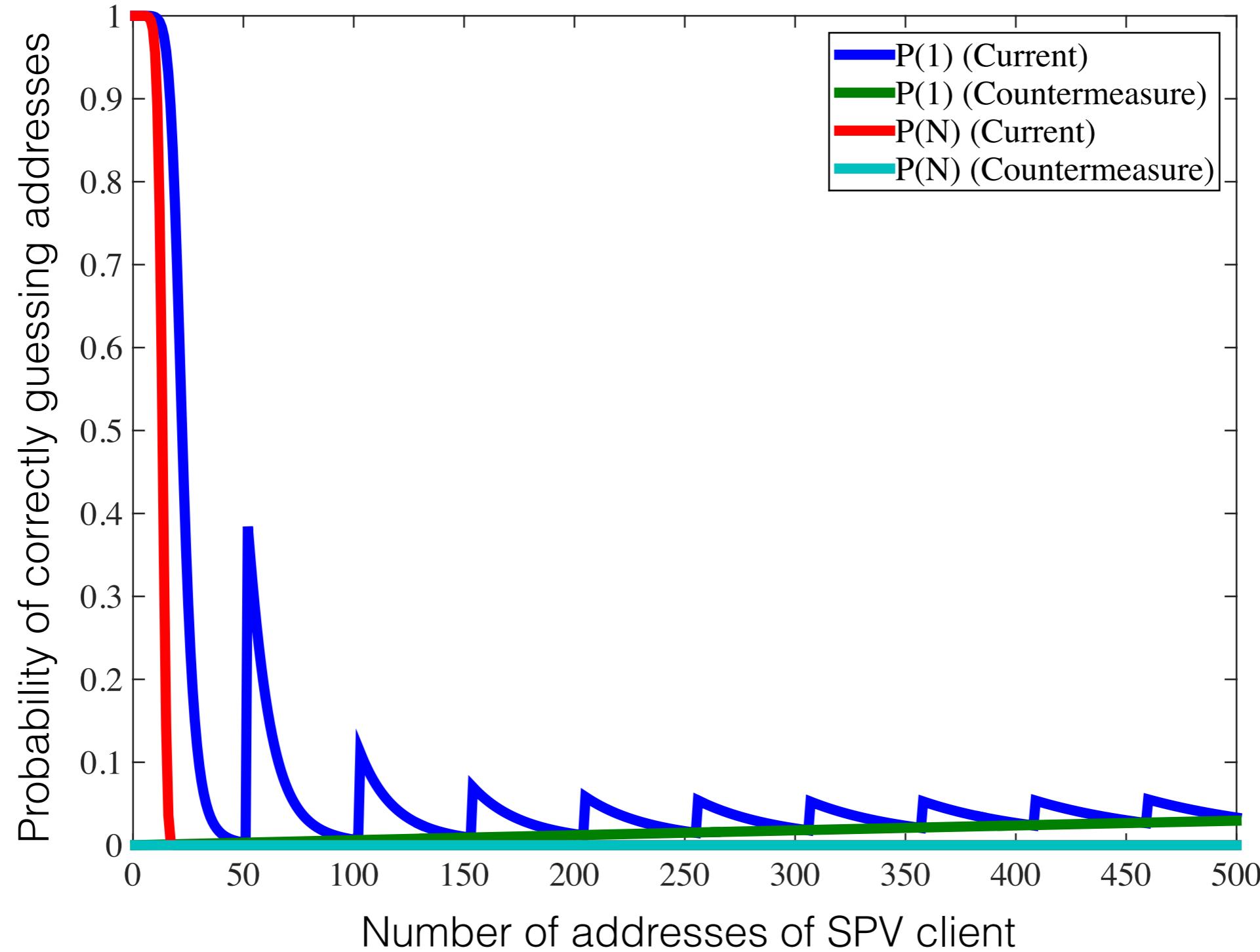


## Proposed solution

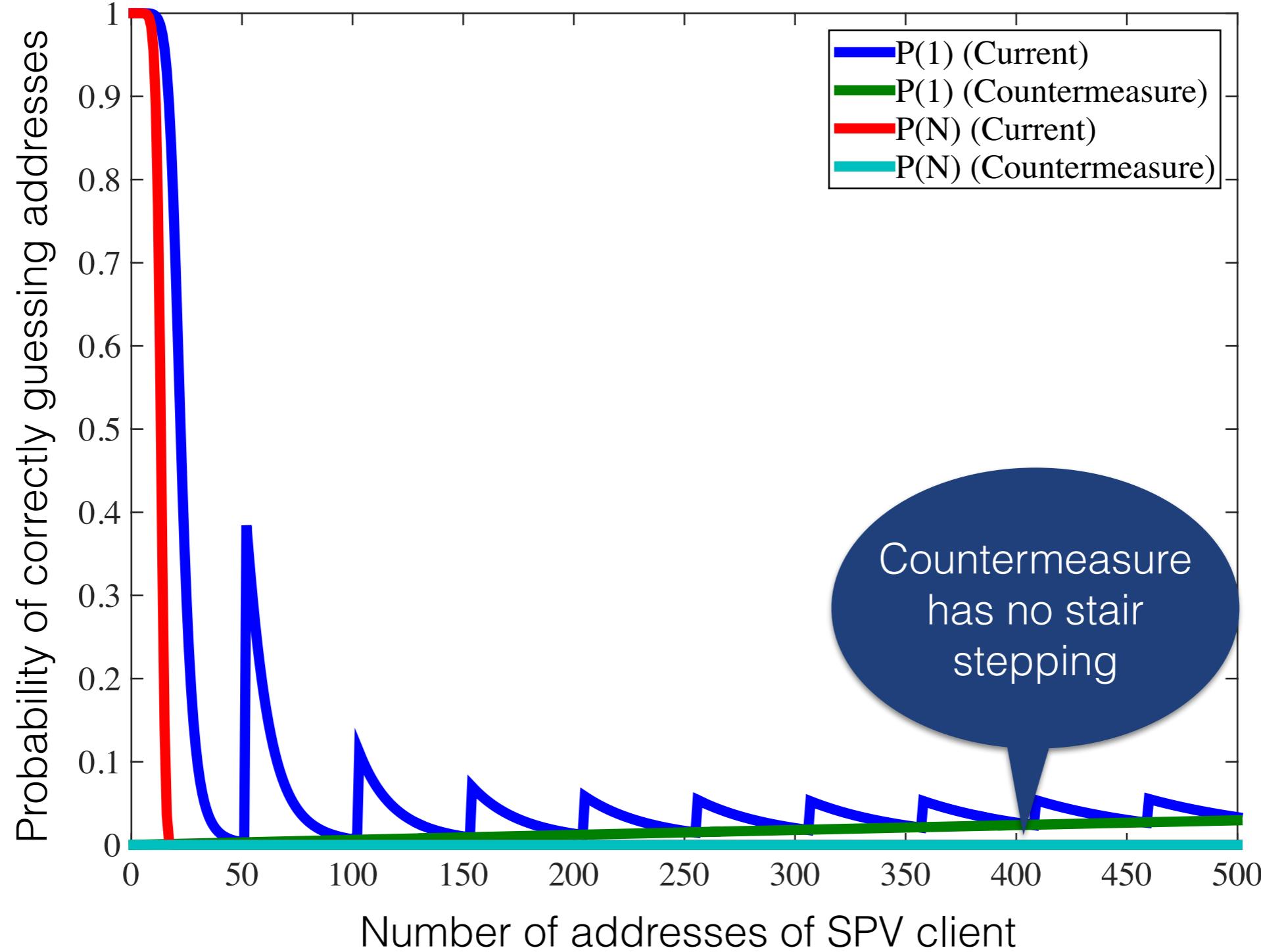


- Pre-generate Bitcoin addresses and insert into filter
- Keep state about outsourced Bloom filter 
- Overhead: For 100 addresses, < 1 kb

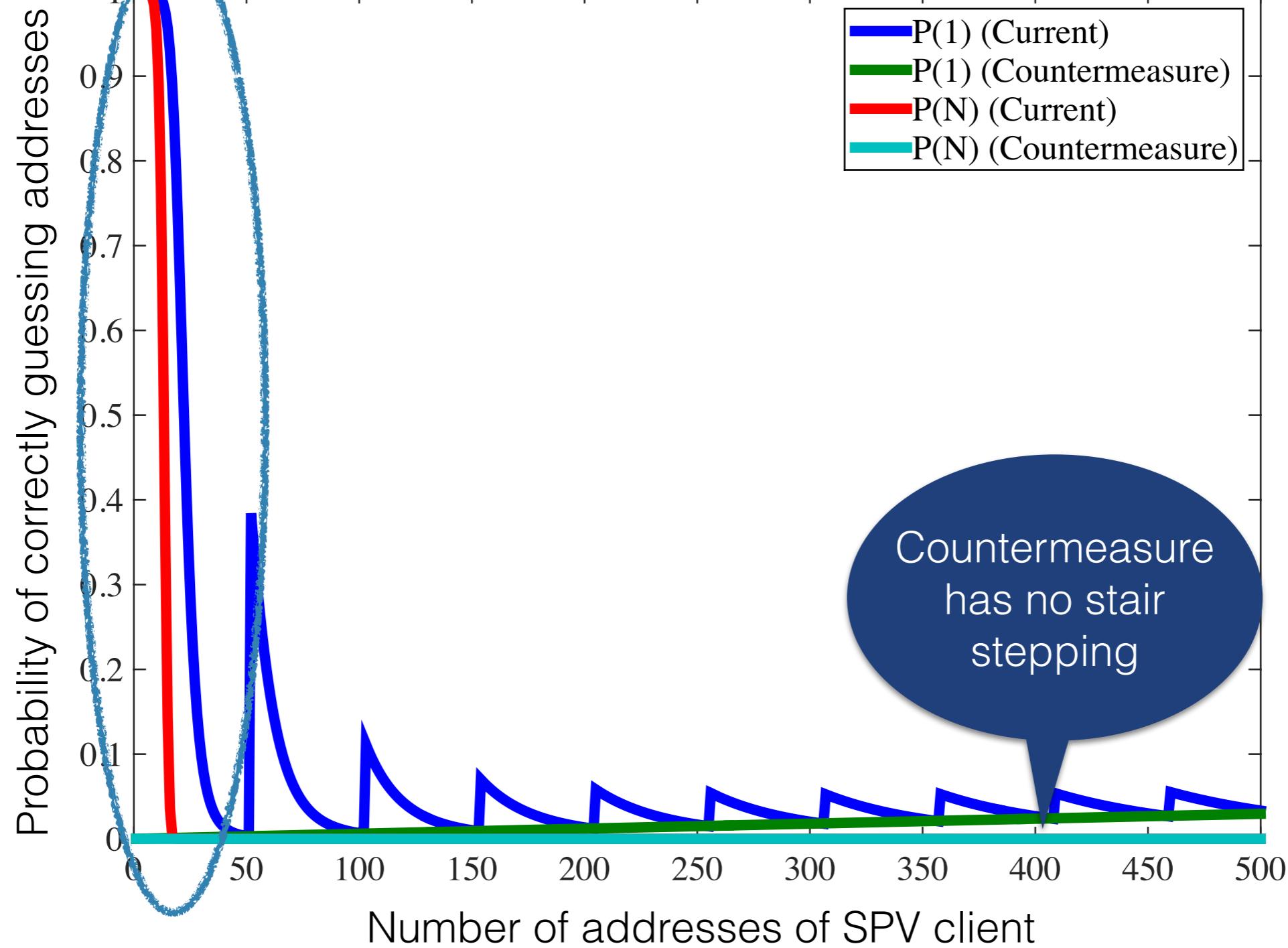
## Proposed solution



## Proposed solution



## 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 

# 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

# 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

# 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!