An analysis of the applicability of blockchain to secure IP addresses allocation, delegation and bindings

draft-paillisse-sidrops-blockchain-01

OPSEC - IETF 101 - London
March 2018

Jordi Paillissé, Albert Cabellos, Vina Ermagan, Alberto Rodríguez, Fabio Maino
jordip@ac.upc.edu

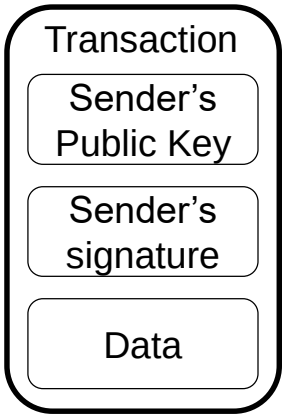
http://openoverlayrouter.org

A short Blockchain tutorial

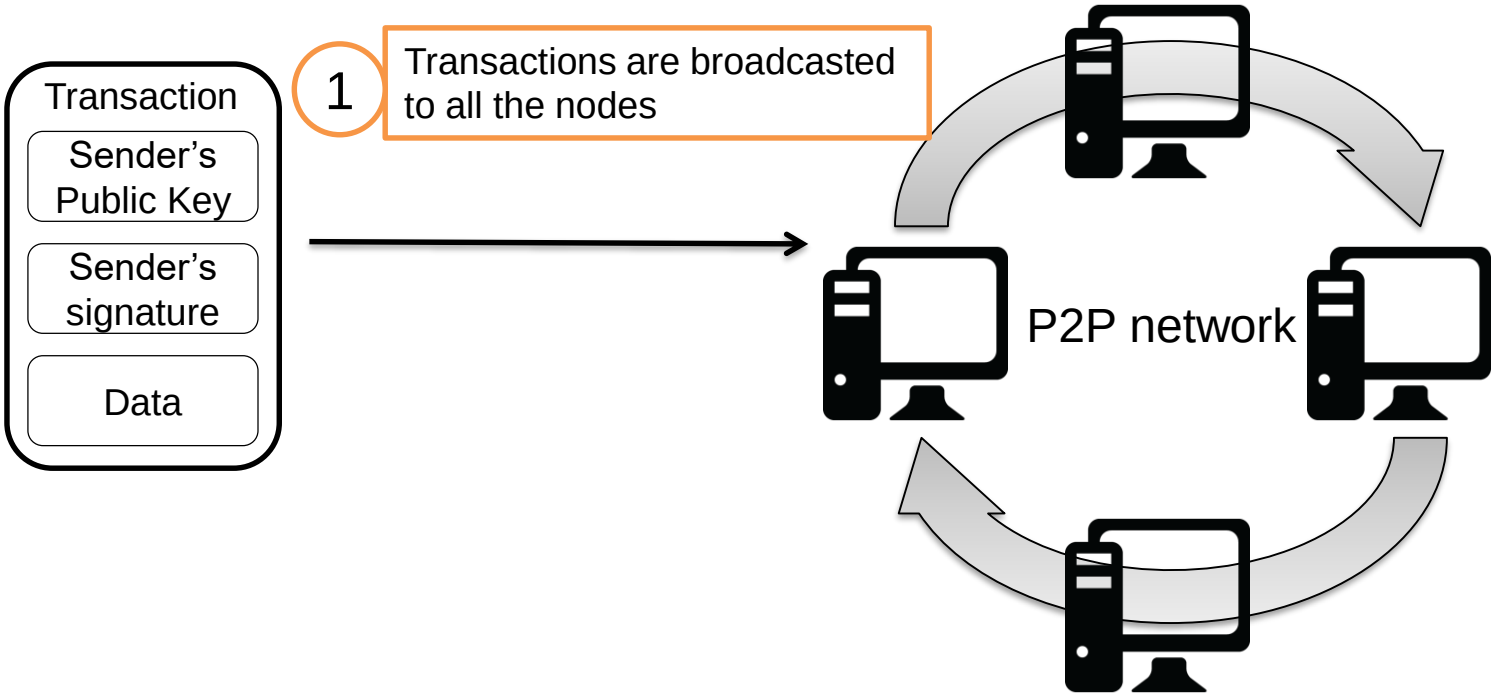
Blockchain - Introduction

- Blockchain:
  - Decentralized, secure and trustless database
  - Token tracking system (who has what)
- Add blocks of data one after another
- Protected by two mechanisms:
  - Chain of signatures
  - Consensus algorithm
- First appeared: Bitcoin, to exchange money
- Other applications are possible

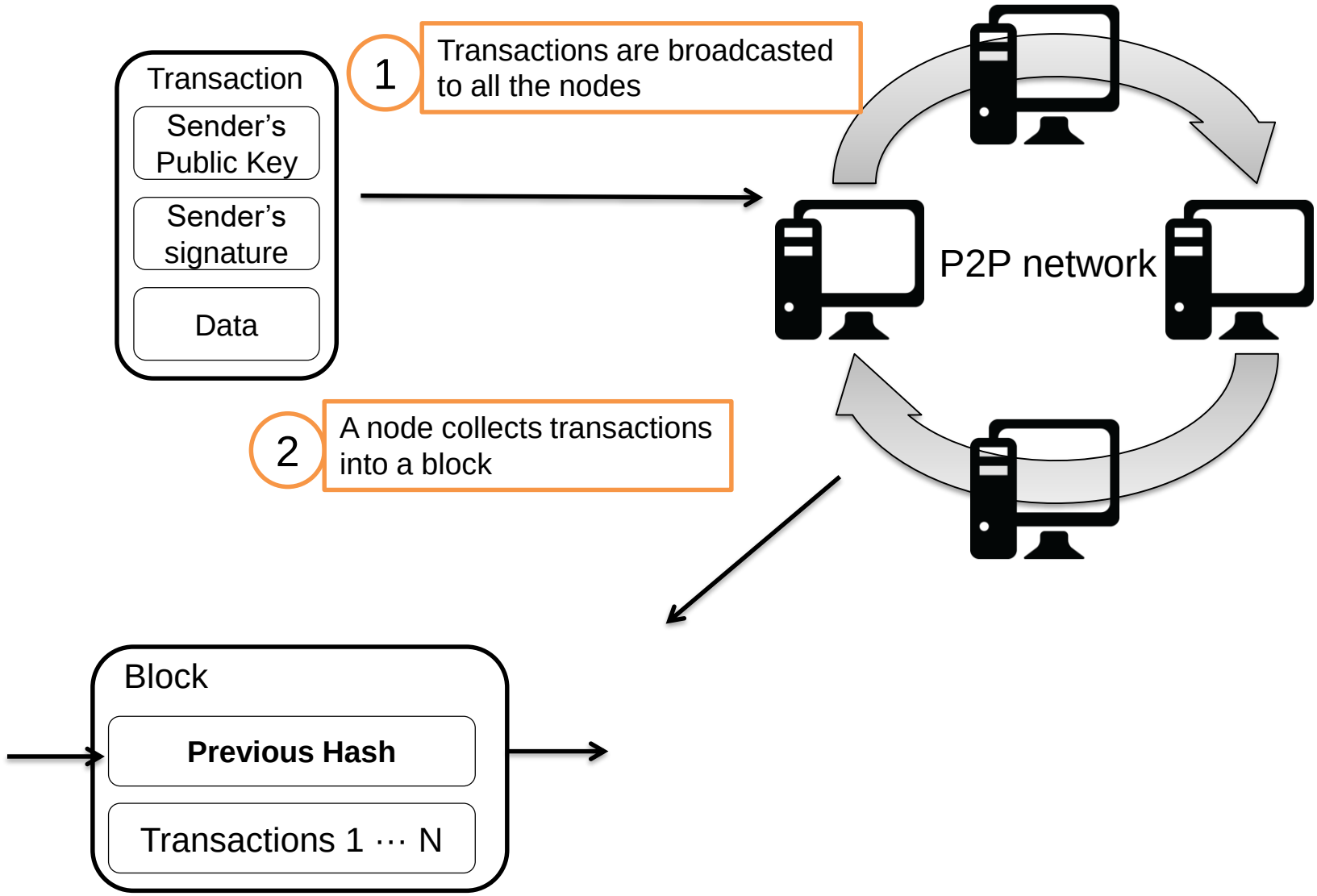
Blockchain - Transactions



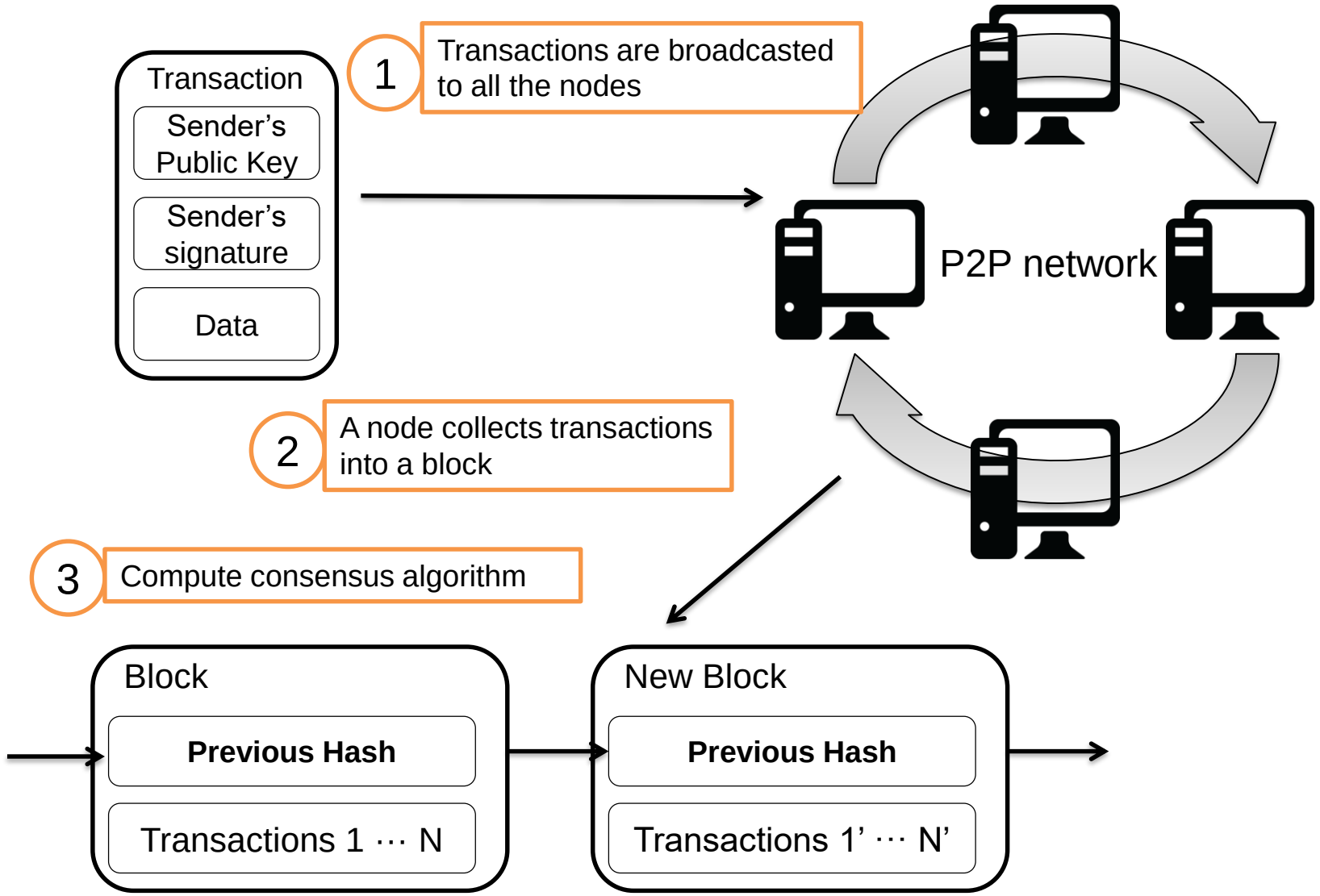
Blockchain - Transactions



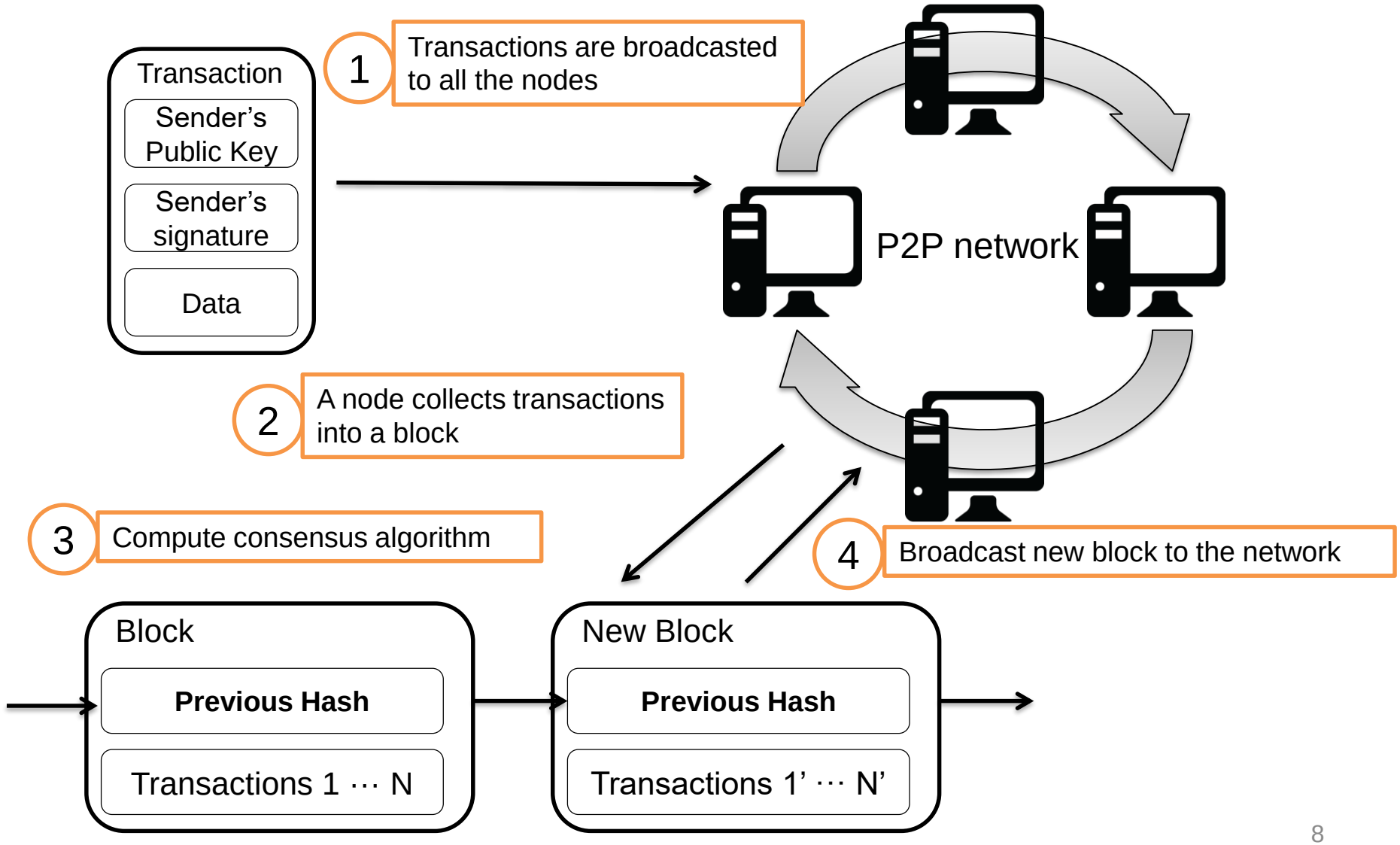
Blockchain - Transactions



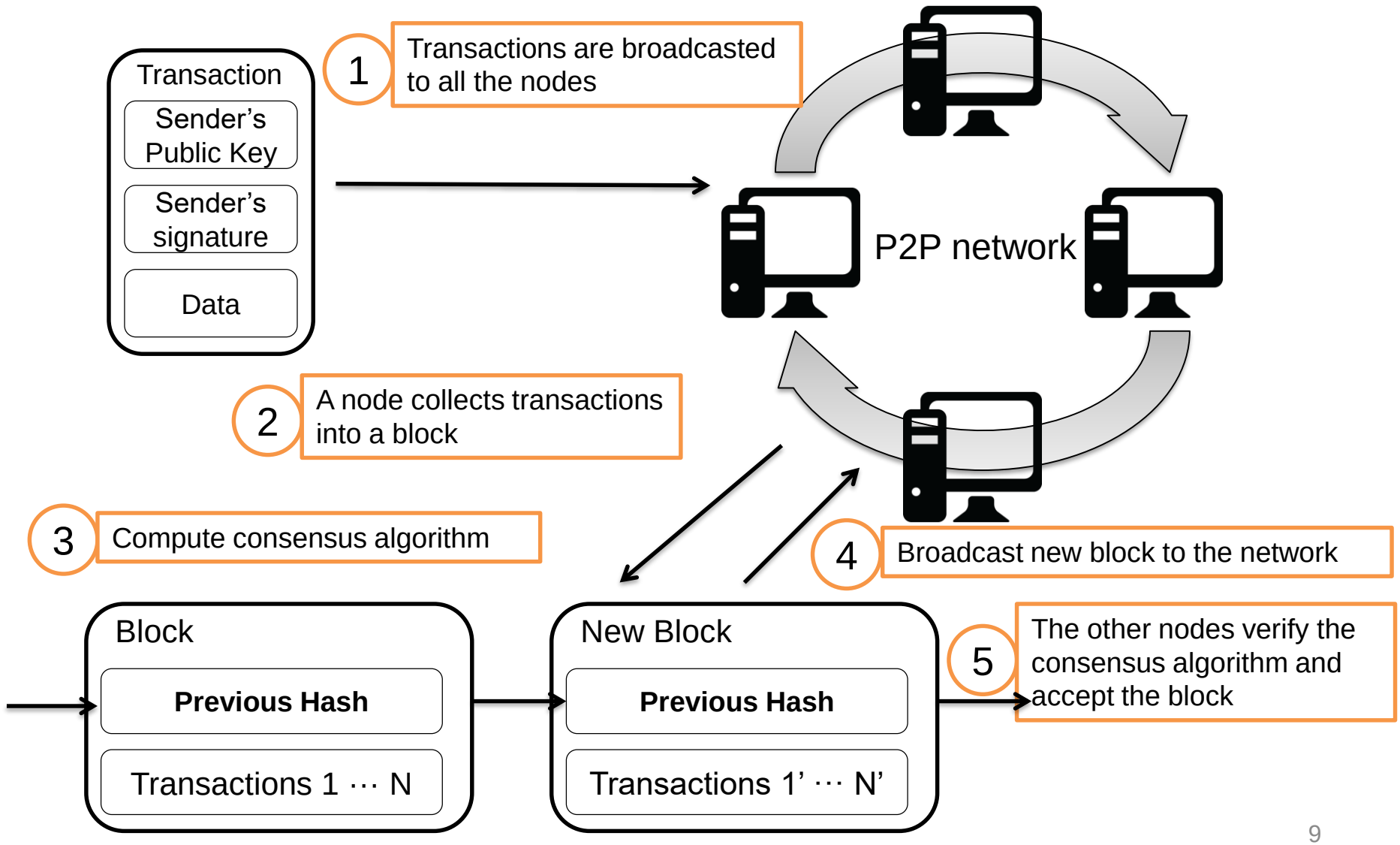
Blockchain - Transactions



Blockchain - Transactions



Blockchain - Transactions



Summary of features

vs. traditional PKI systems

Advantages

- Decentralized
- No CAs
- Simplified management
- Simple rekeying
- Limited prior trust
- Auditable
- Censorship-resistant

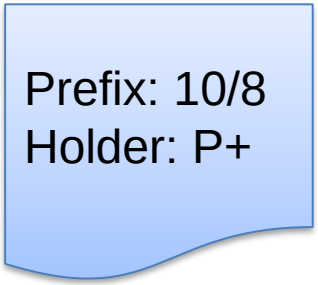
Drawbacks

- No crypto guarantees
- Large storage
- Costly bootstrapping

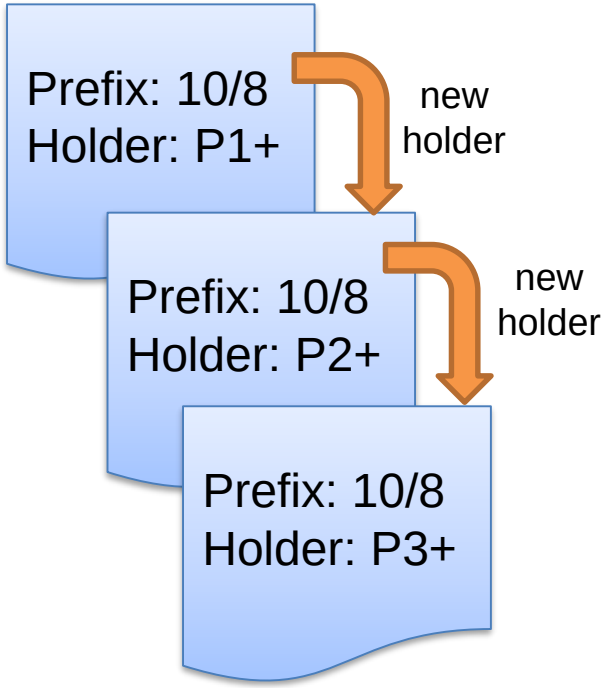
Blockchain for IP addresses

Data in the blockcahin

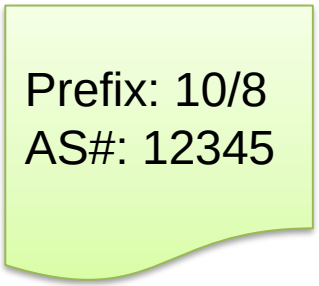
We want to store:



IP address block
+
Holder



Chain of allocations
and delegations

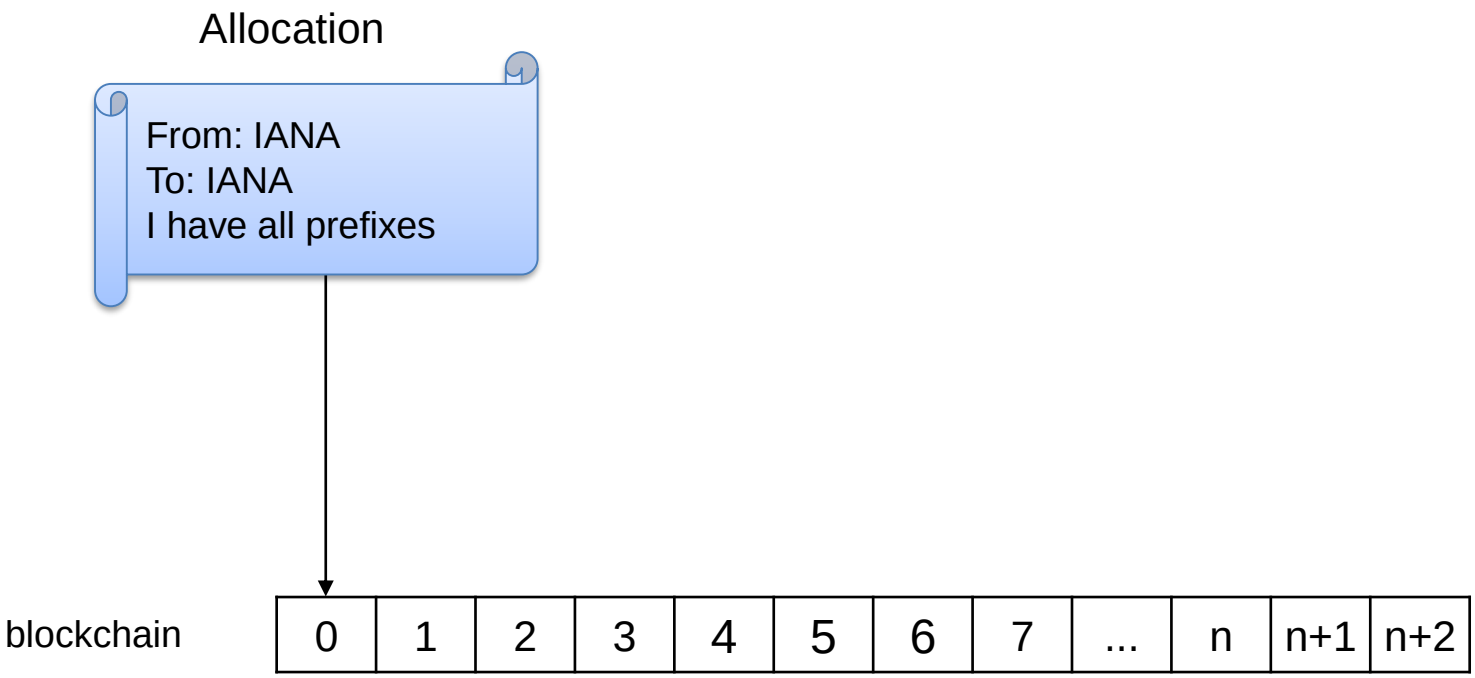


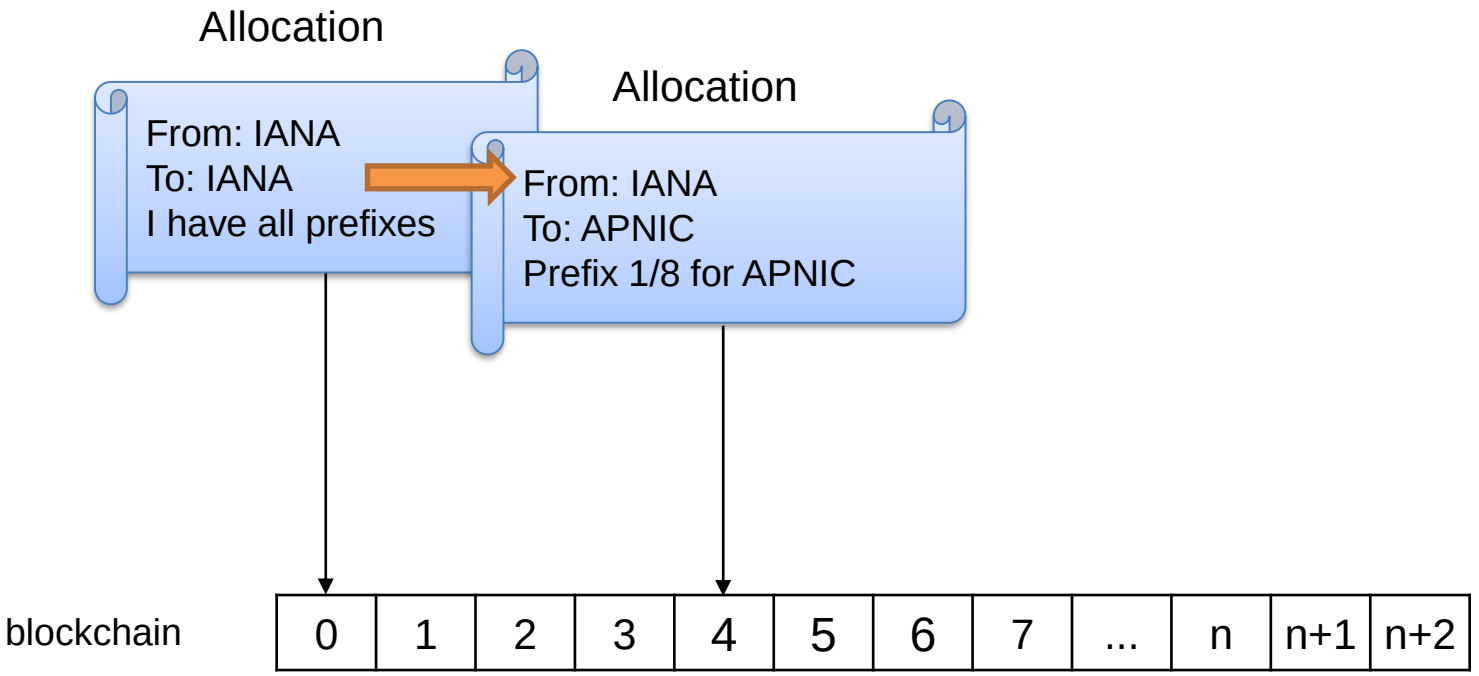
IP address block
+
AS number

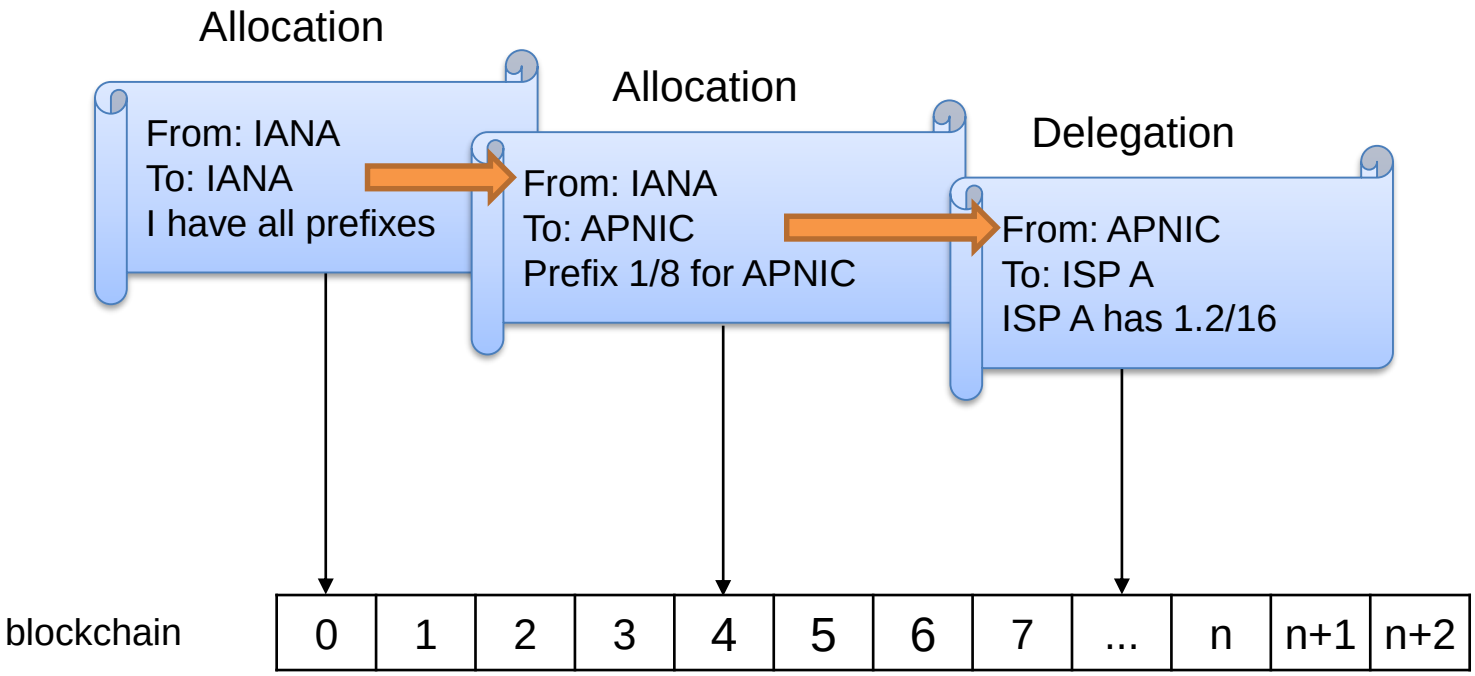
IP addresses vs. coins

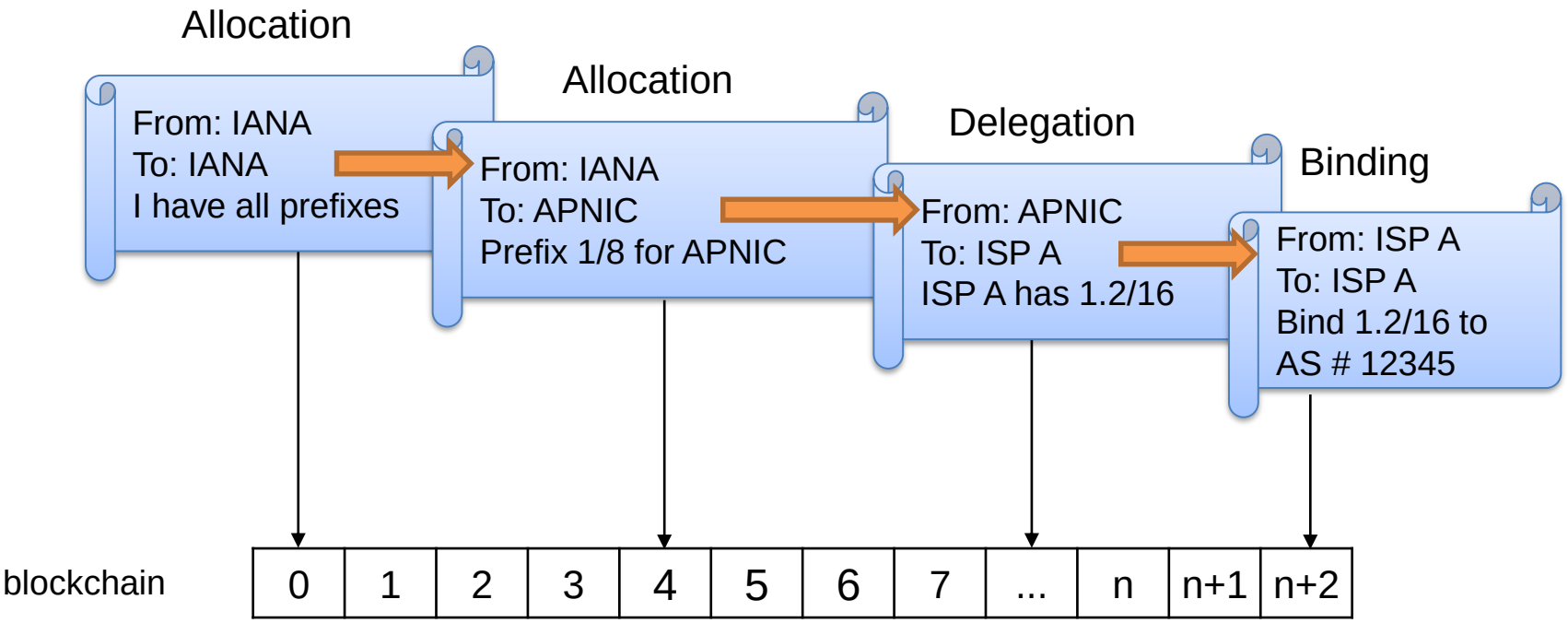
- IP addresses = coins
- Similar properties:
  - Unique
  - Transferrable
  - Divisible
- Exchange blocks of IP addresses just like coins

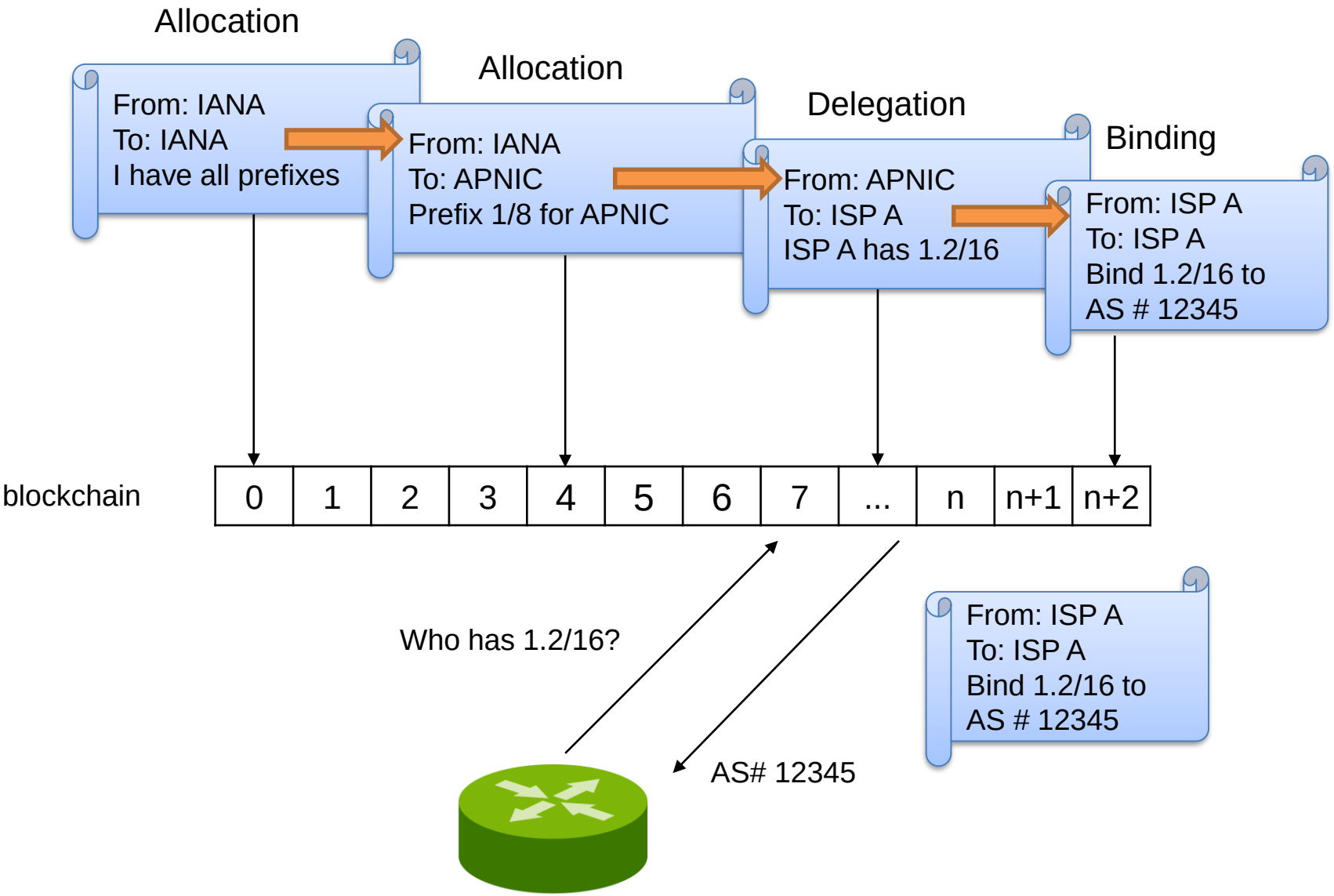
Example

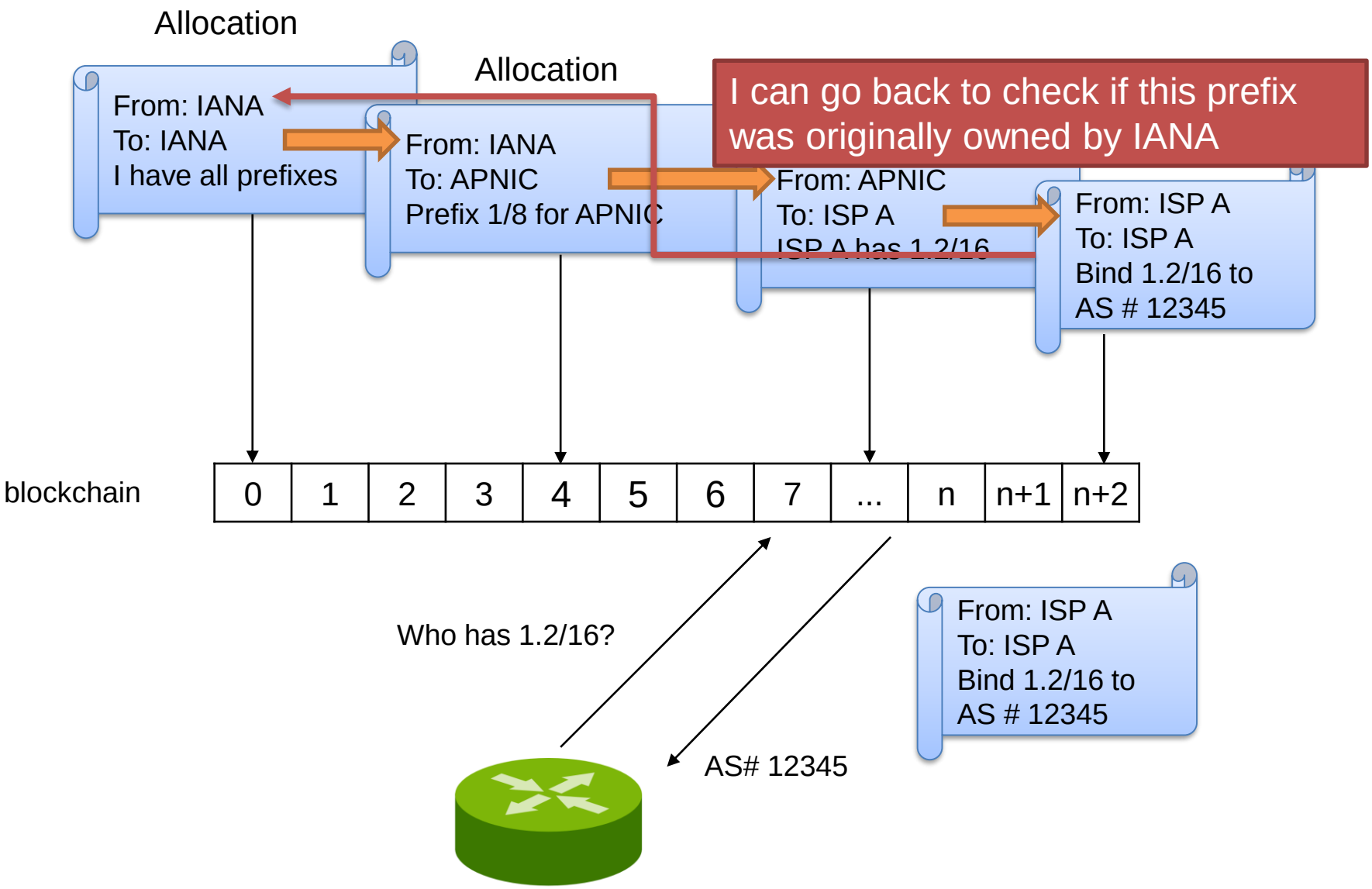

Allocation
From: IANA
To: IANA
I have all prefixes
blockchain
0
1
2
3
4
5
6
7
...
n
n+1
n+2


Allocation
From: IANA
To: IANA
I have all prefixes
Allocation
From: IANA
To: APNIC
Prefix 1/8 for APNIC
blockchain
0
1
2
3
4
5
6
7
...
n
n+1
n+2


Allocation
From: IANA
To: IANA
I have all prefixes
Allocation
From: IANA
To: APNIC
Prefix 1/8 for APNIC
Delegation
From: APNIC
To: ISP A
ISP A has 1.2/16
blockchain
0
1
2
3
4
5
6
7
...
n
n+1
n+2


Allocation
From: IANA
To: IANA
I have all prefixes
Allocation
From: IANA
To: APNIC
Prefix 1/8 for APNIC
Delegation
From: APNIC
To: ISP A
ISP A has 1.2/16
Binding
From: ISP A
To: ISP A
Bind 1.2/16 to
AS # 12345
blockchain
0
1
2
3
4
5
6
7
...
n
n+1
n+2


Allocation
From: IANA
To: IANA
I have all prefixes
Allocation
From: IANA
To: APNIC
Prefix 1/8 for APNIC
Delegation
From: APNIC
To: ISP A
ISP A has 1.2/16
Binding
From: ISP A
To: ISP A
Bind 1.2/16 to
AS # 12345
blockchain
0
1
2
3
4
5
6
7
...
n
n+1
n+2
Who has 1.2/16?
AS# 12345
From: ISP A
To: ISP A
Bind 1.2/16 to
AS # 12345


Allocation
From: IANA
To: IANA
I have all prefixes
Allocation
From: IANA
To: APNIC
Prefix 1/8 for APNIC
From: APNIC
To: ISP A
ISP A has 1.2/16
From: ISP A
To: ISP A
Bind 1.2/16 to
AS # 12345
I can go back to check if this prefix was originally owned by IANA
blockchain
0
1
2
3
4
5
6
7
...
n
n+1
n+2
Who has 1.2/16?
AS# 12345
From: ISP A
To: ISP A
Bind 1.2/16 to
AS # 12345

Operational Considerations

Revocation

Centralized control

Decentralized control

- Lost keys
- Compromised keys
- Improper use

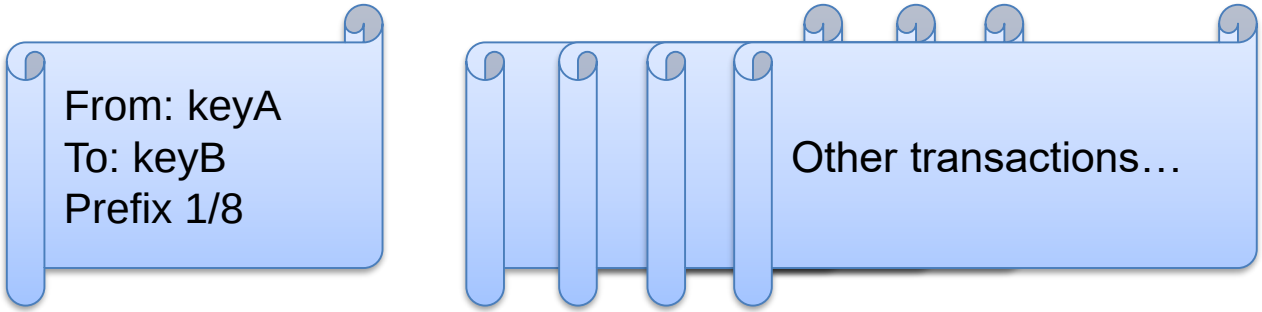
Revocation

Middle ground:

- Timeout → transfer to previous owner
- Multi-signature → more than one key
- Revocation tx. → by a third party

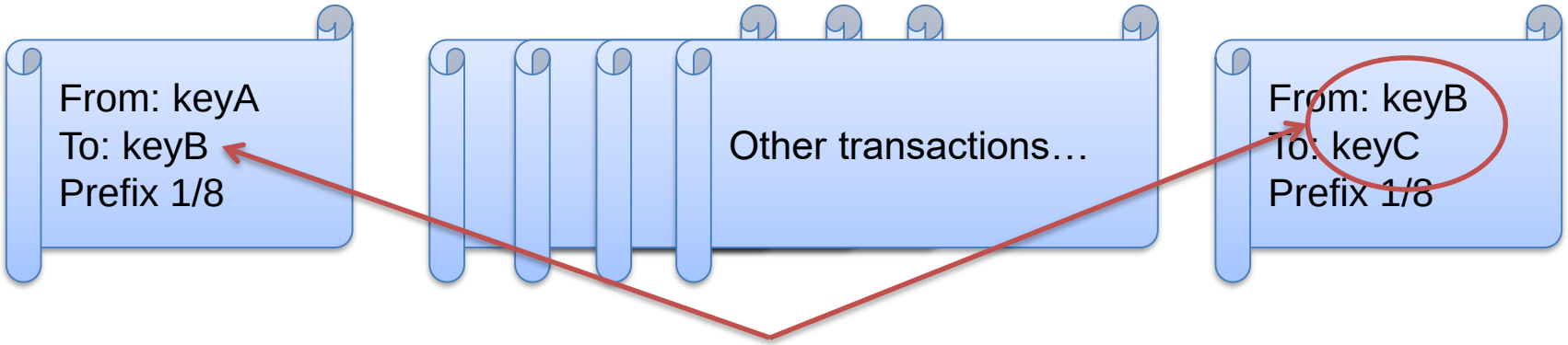
Rekeying

- Delegating the block of addresses to itself using a new key pair.
- Simpler than traditional rekeying schemes
- Can be performed independently (each holder can do it without affecting other holders)



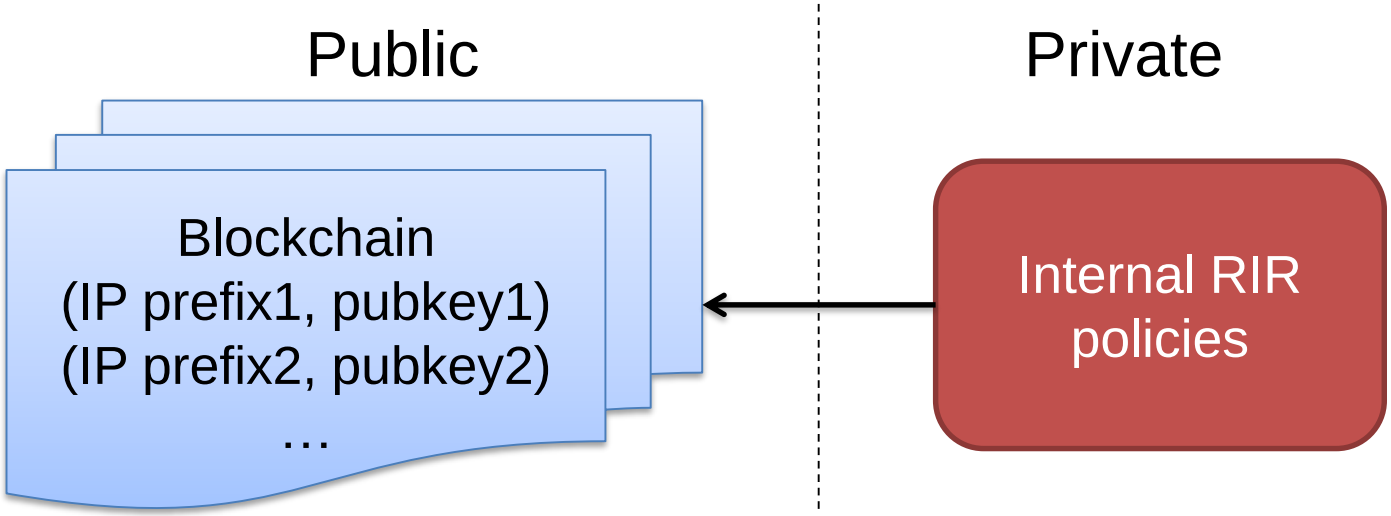
Rekeying

- Delegating the block of addresses to itself using a new key pair.
- Simpler than traditional rekeying schemes
- Can be performed independently (each holder can do it without affecting other holders)



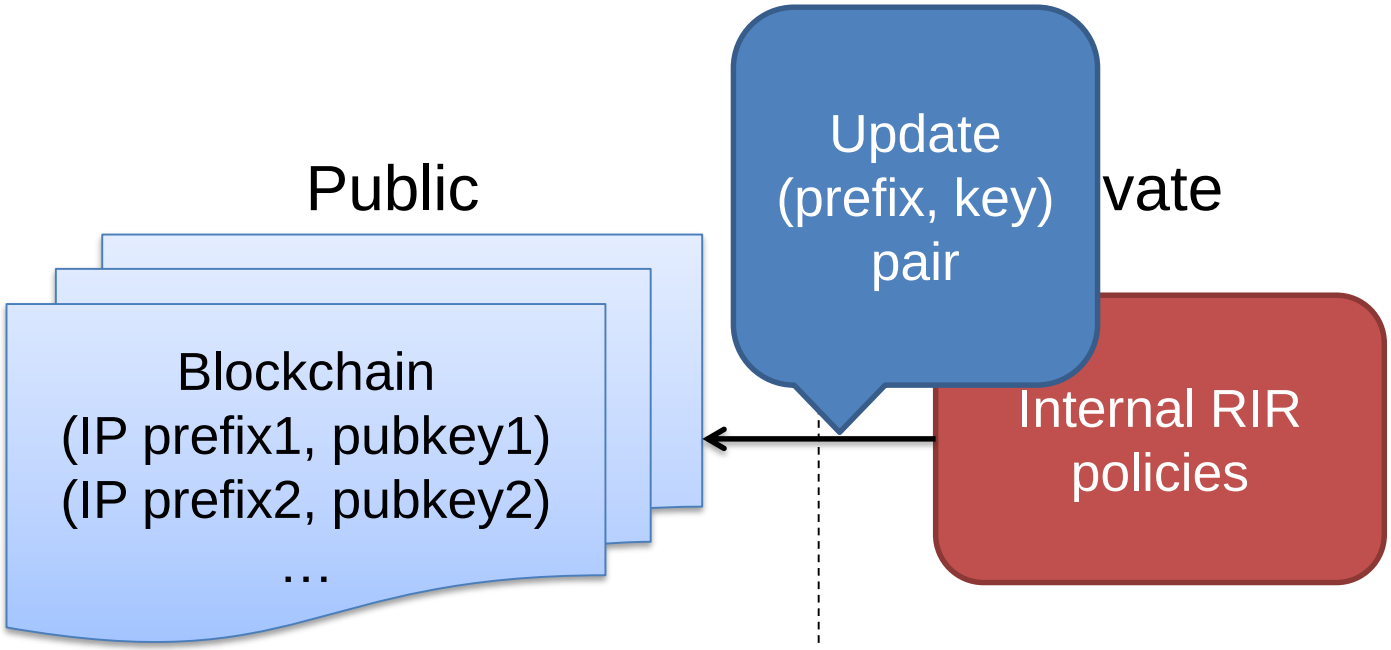
Privacy

- Lawful interception
- RIR policies
- Business relationships



Privacy

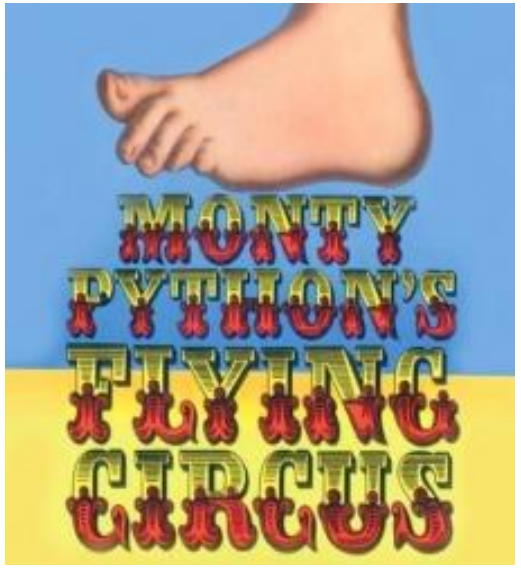
- Lawful interception
- RIR policies
- Business relationships



Prototype

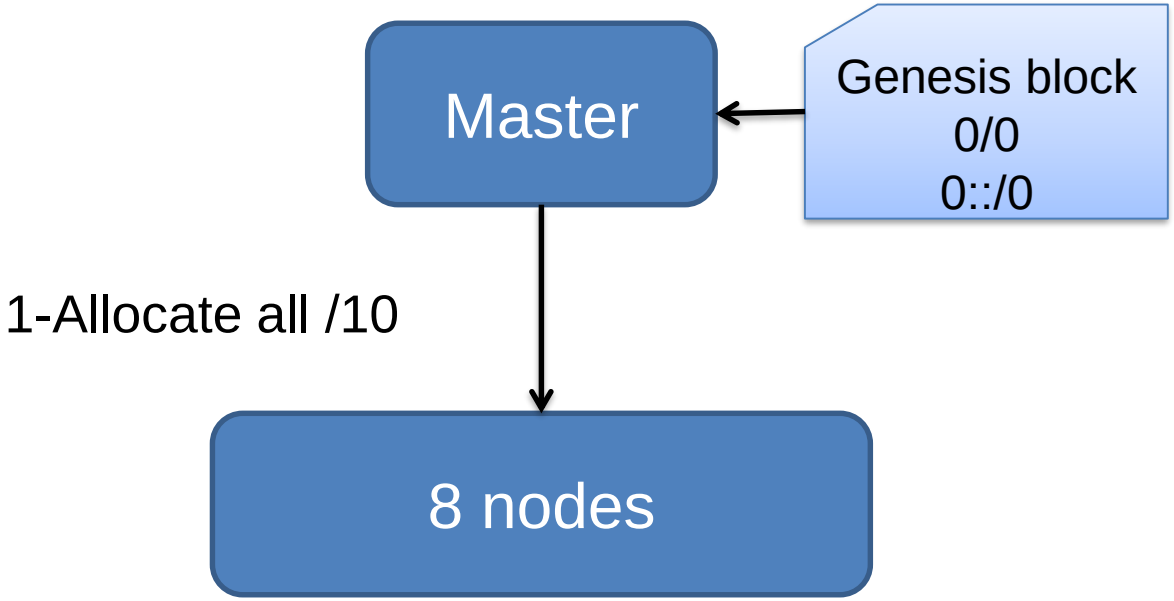
Prototype

- Python
- Features:
  - Simple Proof of Stake
  - Block time 60s
  - 2 MB blocks
  - IPv4 and IPv6
- Open-sourced: https://github.com/OpenOverlayRouter/blockchain-mapping-system

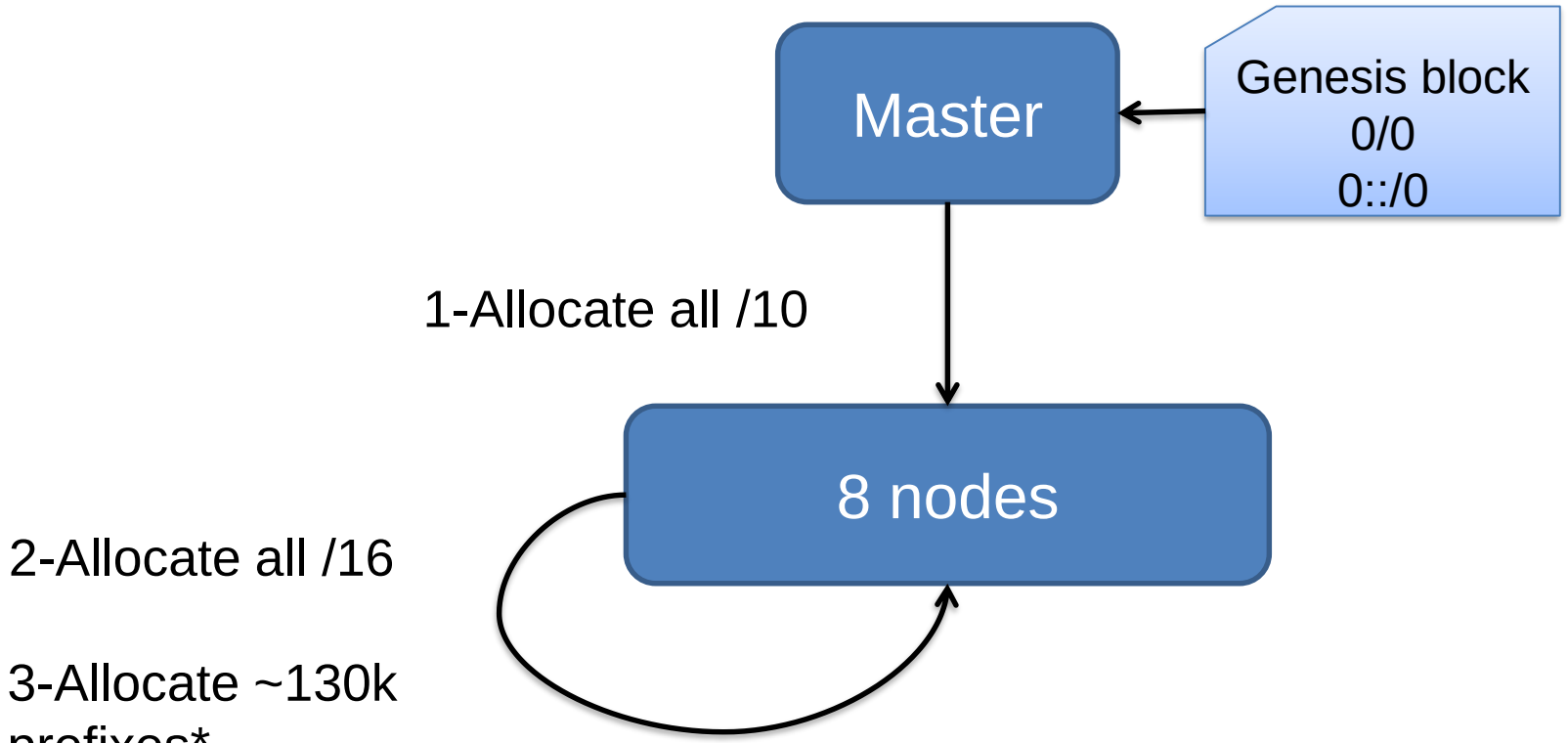


http://sharetv.com/shows/monty_pythons_flying_circus_uk

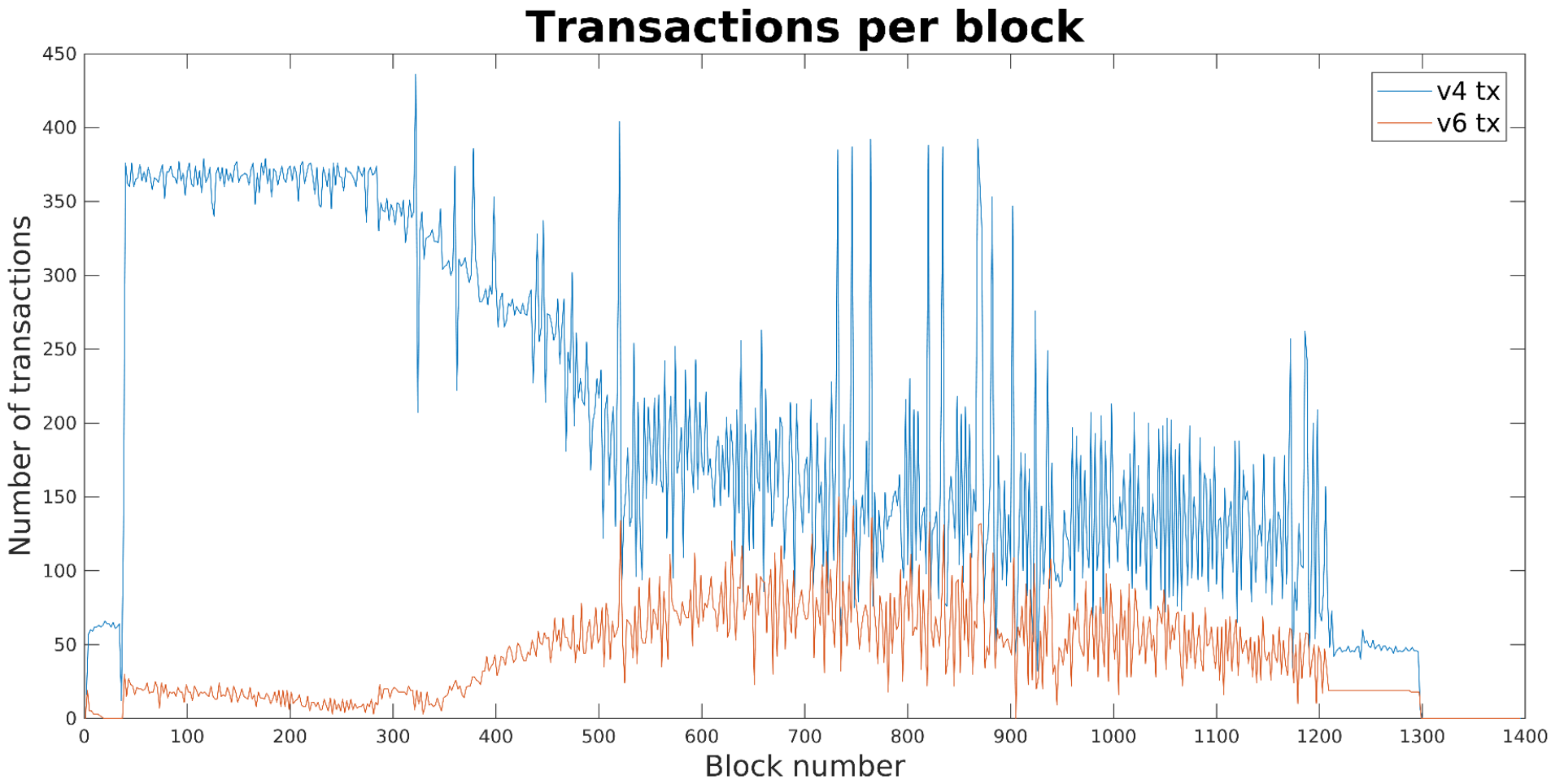
Experiment



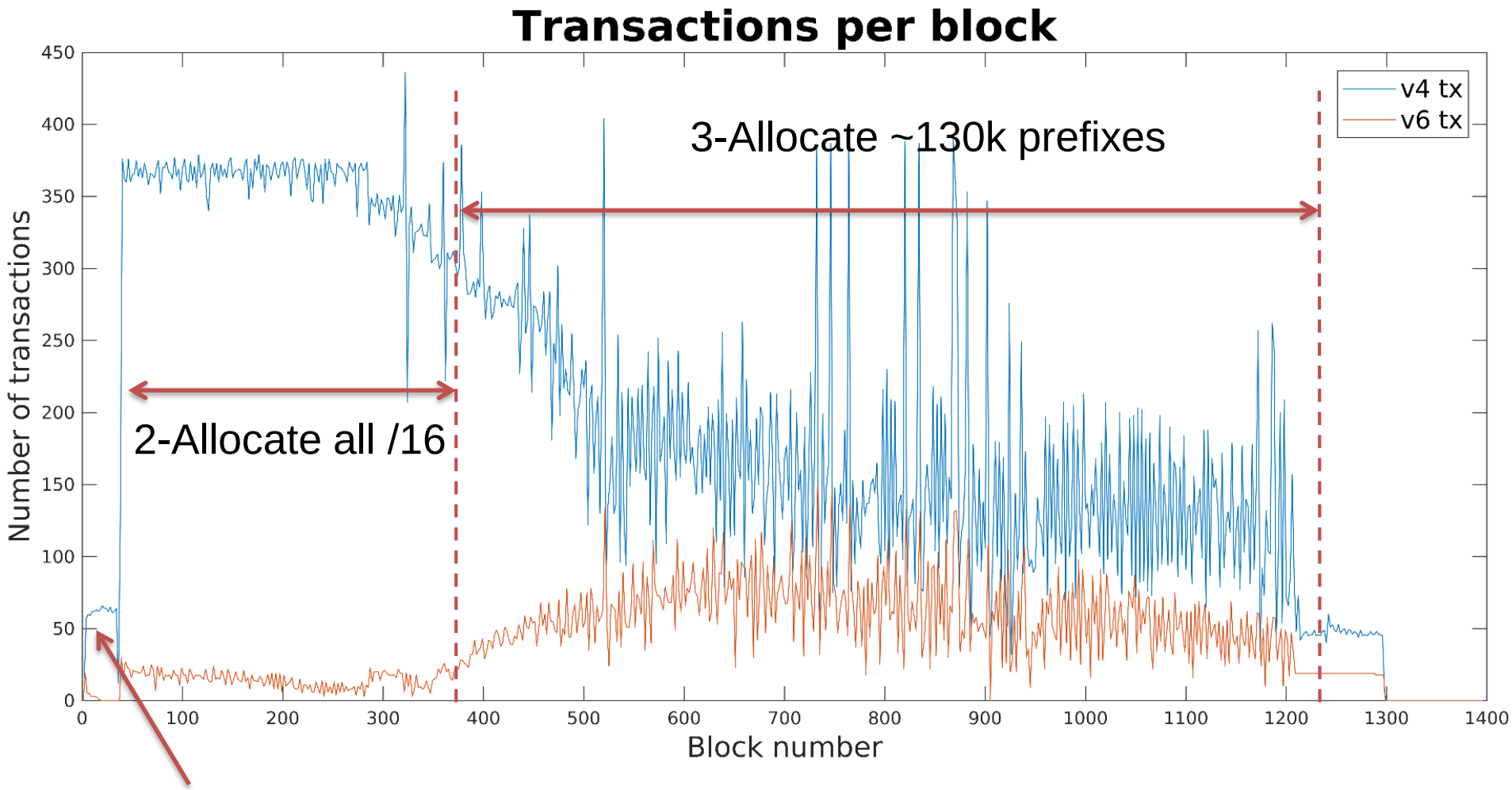
Experiment



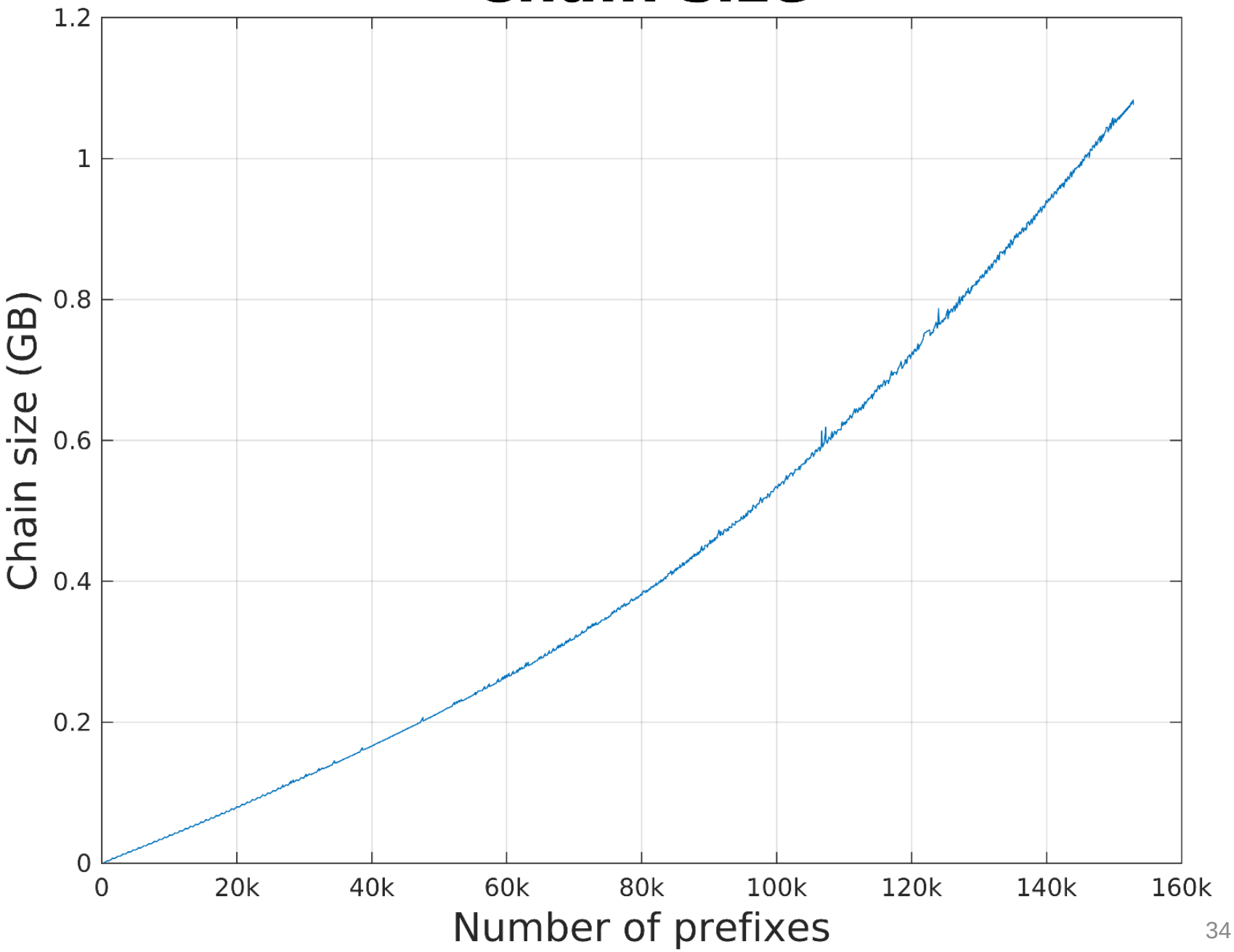
*Extracted from RIR statistics exchange files, eg.
ftp://ftp.apnic.net/pub/stats/apnic/delegated-apnic-extended-latest

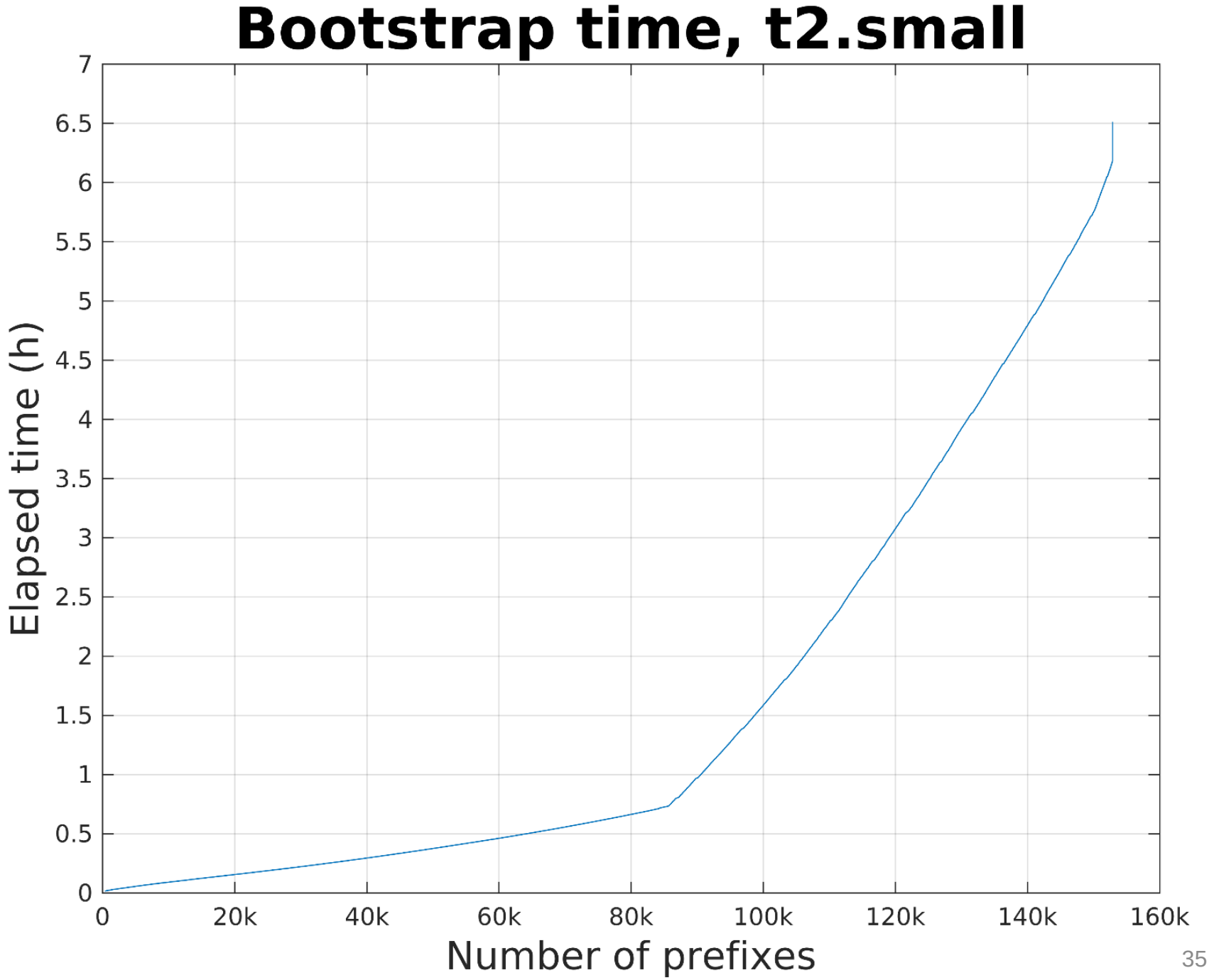


Processed ~160k transactions



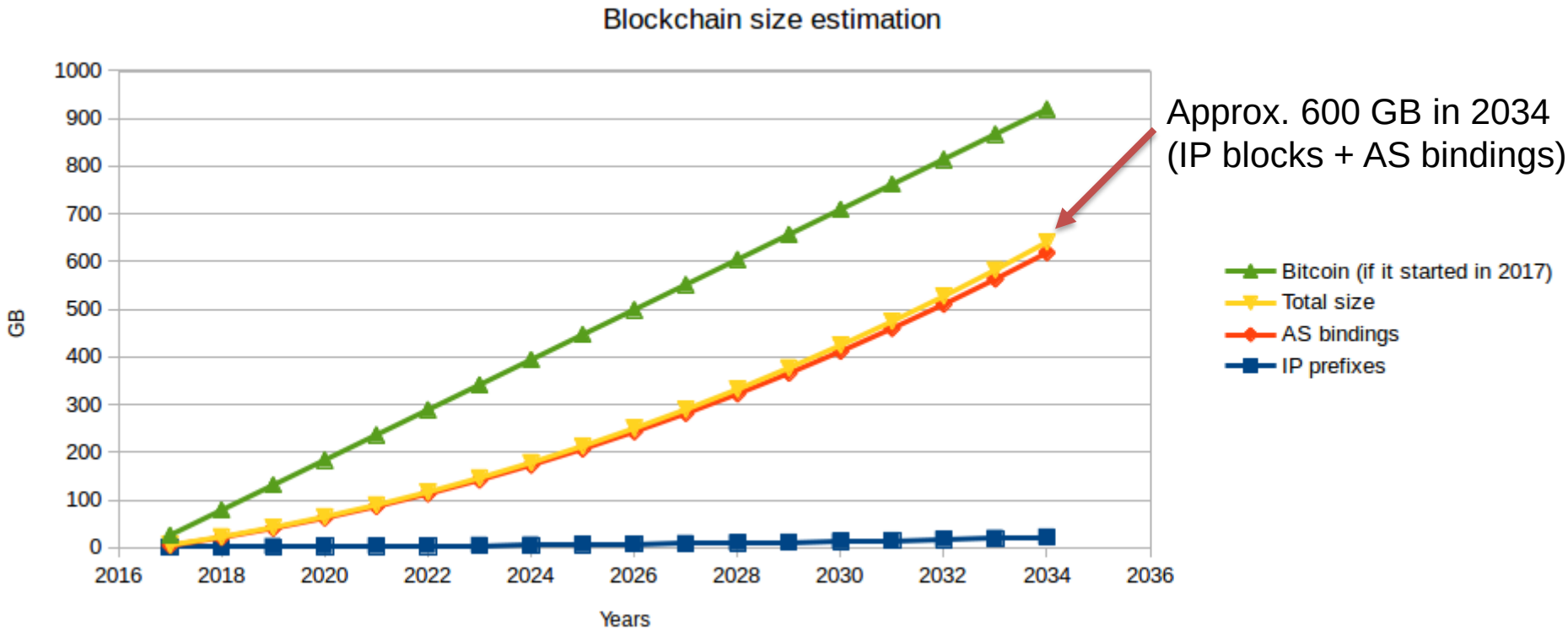
Processed ~160k transactions


Chain size
Chain size (GB)
Number of prefixes
0
0.2
0.4
0.6
0.8
1
1.2
0
20k
40k
60k
80k
100k
120k
140k
160k


Bootstrap time, t2.small
Elapsed time (h)
Number of prefixes
0
0.5
1
1.5
2
2.5
3
3.5
4
4.5
5
5.5
6
6.5
7
0
20k
40k
60k
80k
100k
120k
140k
160k

Thanks for listening!

Scalability



- One AS <> prefix binding for each block of /24 IPv4 address space
- Growth similar to BGP churn*
- Each transaction approx. 400 bytes
- Only IP Prefixes: worst case + BGP table growth*: approx. 40 GB in 20 years
- With PoS, storage can be reduced

*Source: http://www.potaroo.net/ispcol/2017-01/bgp2016.html

Storage

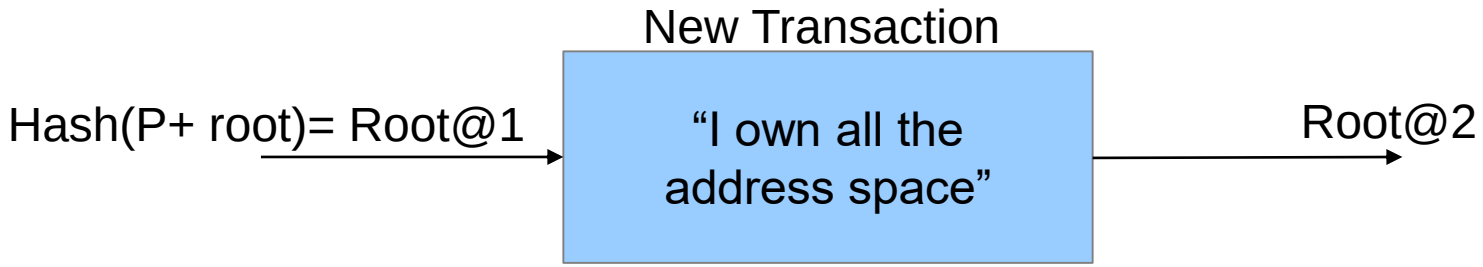
- Several mechanisms can help reducing storage, eg:
  - Prune old transactions
  - Download only headers (Bitcoin SPV*)
  - Discard old blocks
- These techniques depend on the consensus algorithm

*Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Sec. 8

Transaction examples

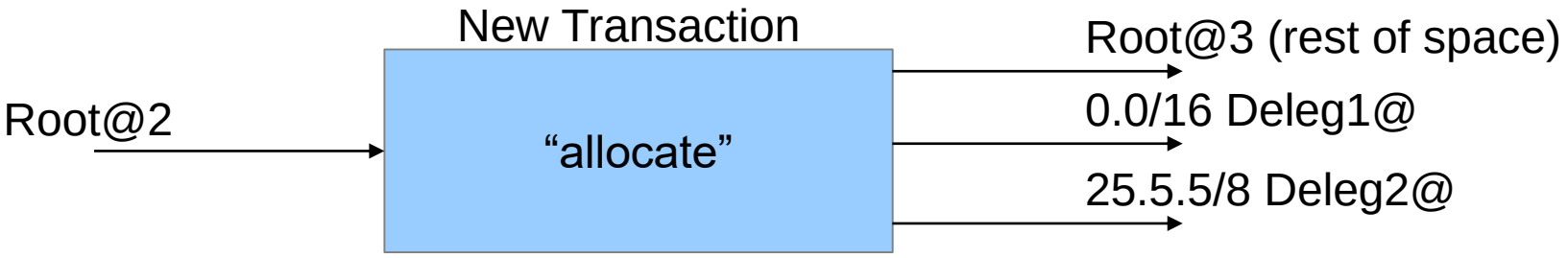
First transaction

- Users trust the Public Key of the Root, that initially claims all address space by writing the genesis block
- Root can delegate all address space to itself and use a different keypair

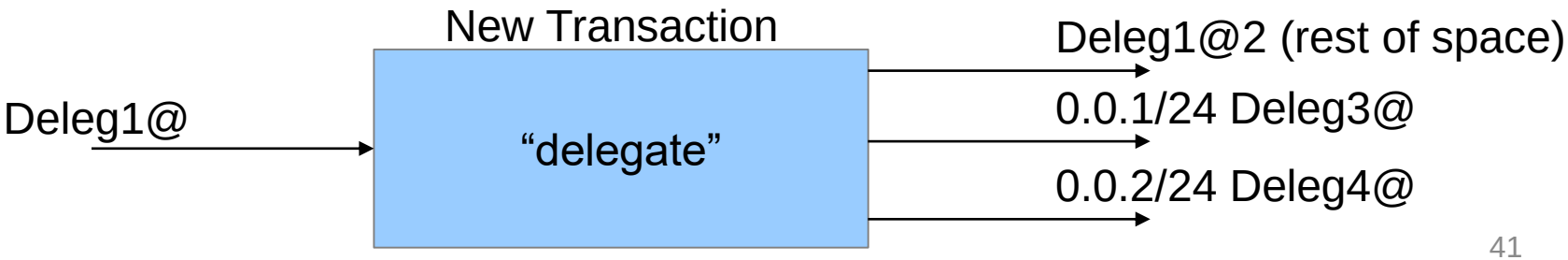


Prefix allocation and delegation

- Root allocates blocks of addresses to other entities (identified by Hash(Public Key)) by adding transactions

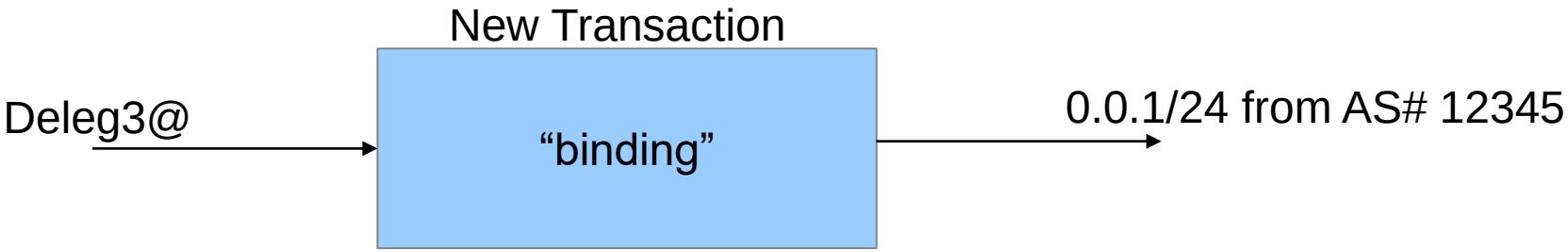


- Holders can further delegate address blocks to other entities



Writing AS bindings

- Just like delegating a prefix, but instead of the new holder, we write the binding



External server authentication

- Some information may not be suitable for the blockchain, or changes so fast it is already outdated when added into a block
- A public key from an external server can also be included in the delegations
- Since blockchain provides authentication and integrity for this key, parties can use it to authenticate responses from the external server

FAQ

- Does it grow indefinitely?
  - Yes
- Do all nodes have the same information?
  - Yes
- When answering a query, do you have to search the entire blockchain?
  - No, you can create a separate data structure only with the current data
- If I lose my private key, do I lose my prefixes also?
  - Yes, watch out!