

# Could Blockchain Help in Inter-domain Security?

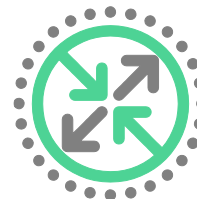
<https://datatracker.ietf.org/doc/draft-paillisse-sidrops-blockchain/>  
<http://arxiv.org/abs/1805.04439>

RIPE 76 - Marseille  
May 2018

Jordi Paillissé, Albert Cabellos, Vina Ermagan, Alberto Rodríguez,  
Fabio Maino  
[jordip@ac.upc.edu](mailto:jordip@ac.upc.edu)



UNIVERSITAT POLITÈCNICA DE CATALUNYA  
BARCELONATECH  
Departament d'Arquitectura de Computadors



OPEN  
OVERLAY  
ROUTER

<http://openoverlayrouter.org>

# It's cheap!



<https://hodl.eu/wp-content/uploads/2017/11/bitcoin-mining-farm.jpg>

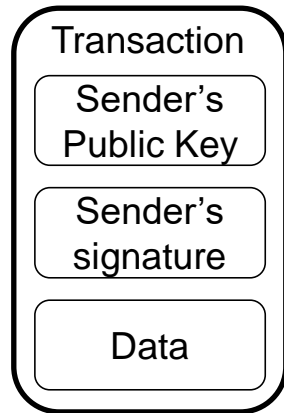
- Proof of Stake
- No power waste
- Runs on a normal PC

# **A short Blockchain tutorial**

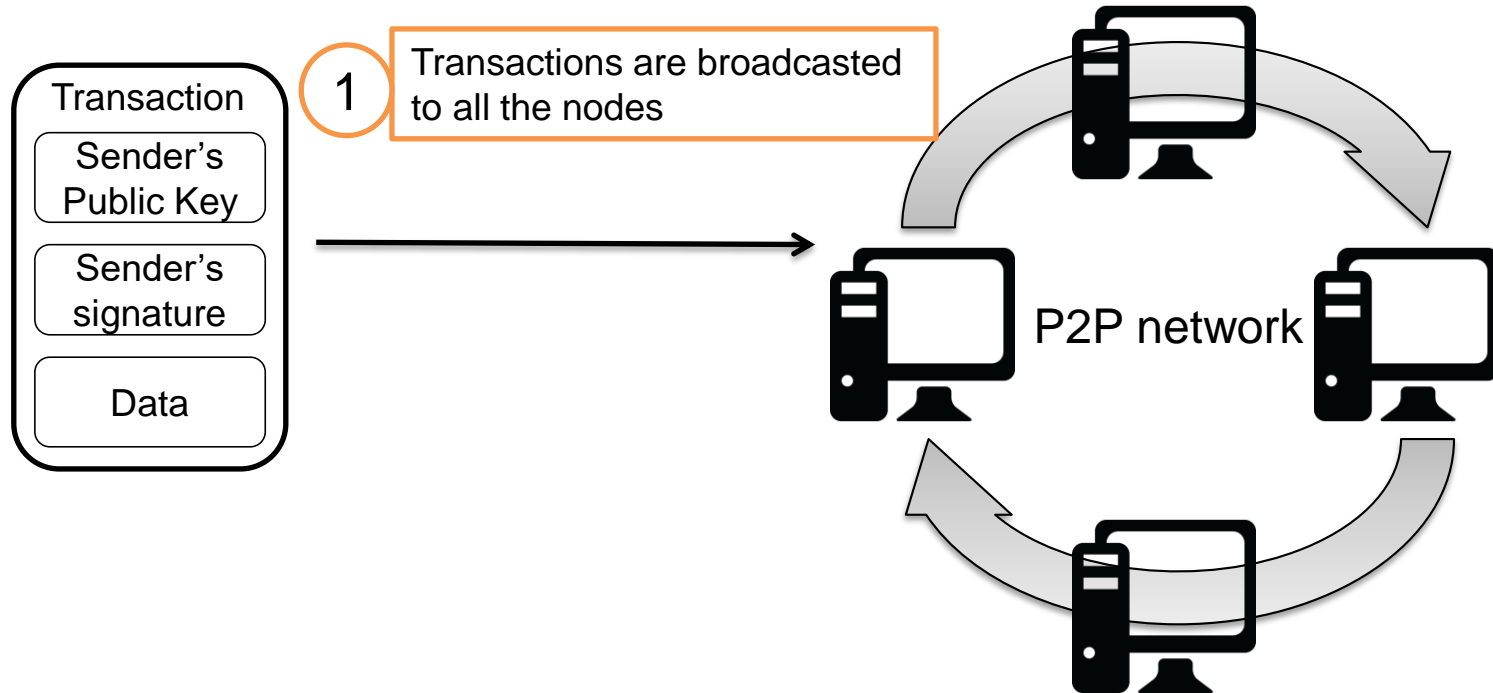
# Blockchain - Introduction

- 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

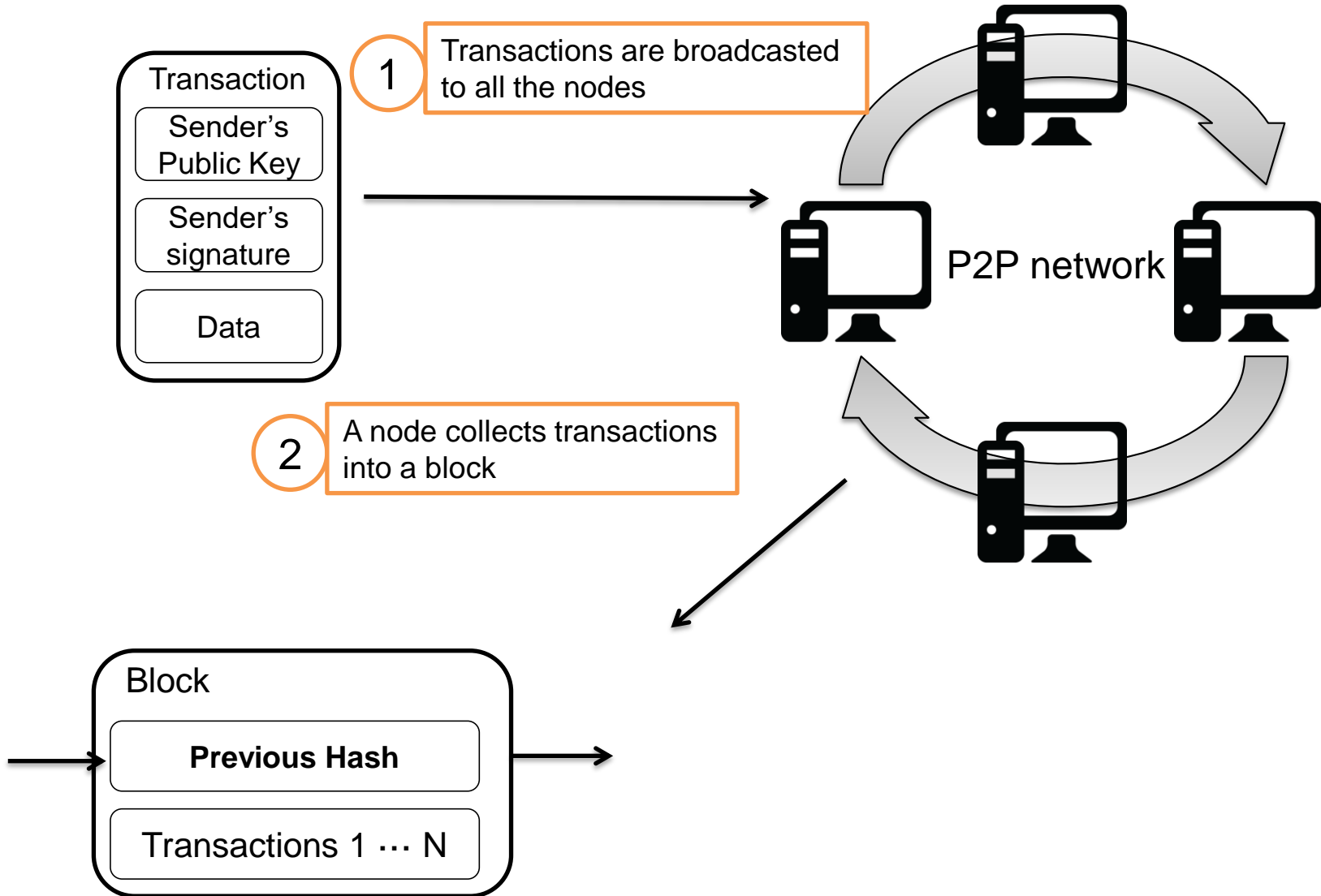
# Blockchain - Transactions



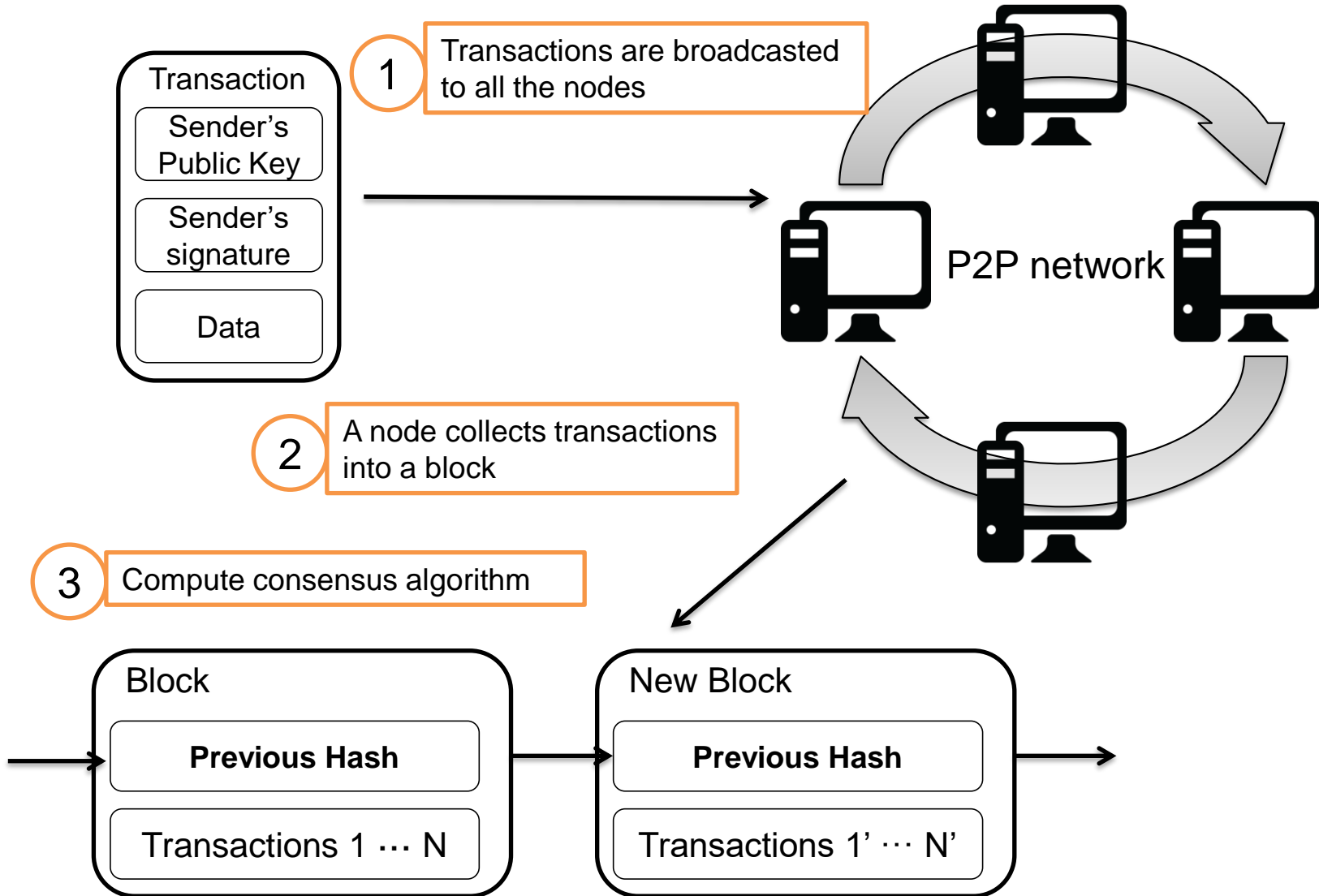
# Blockchain - Transactions



# Blockchain - Transactions

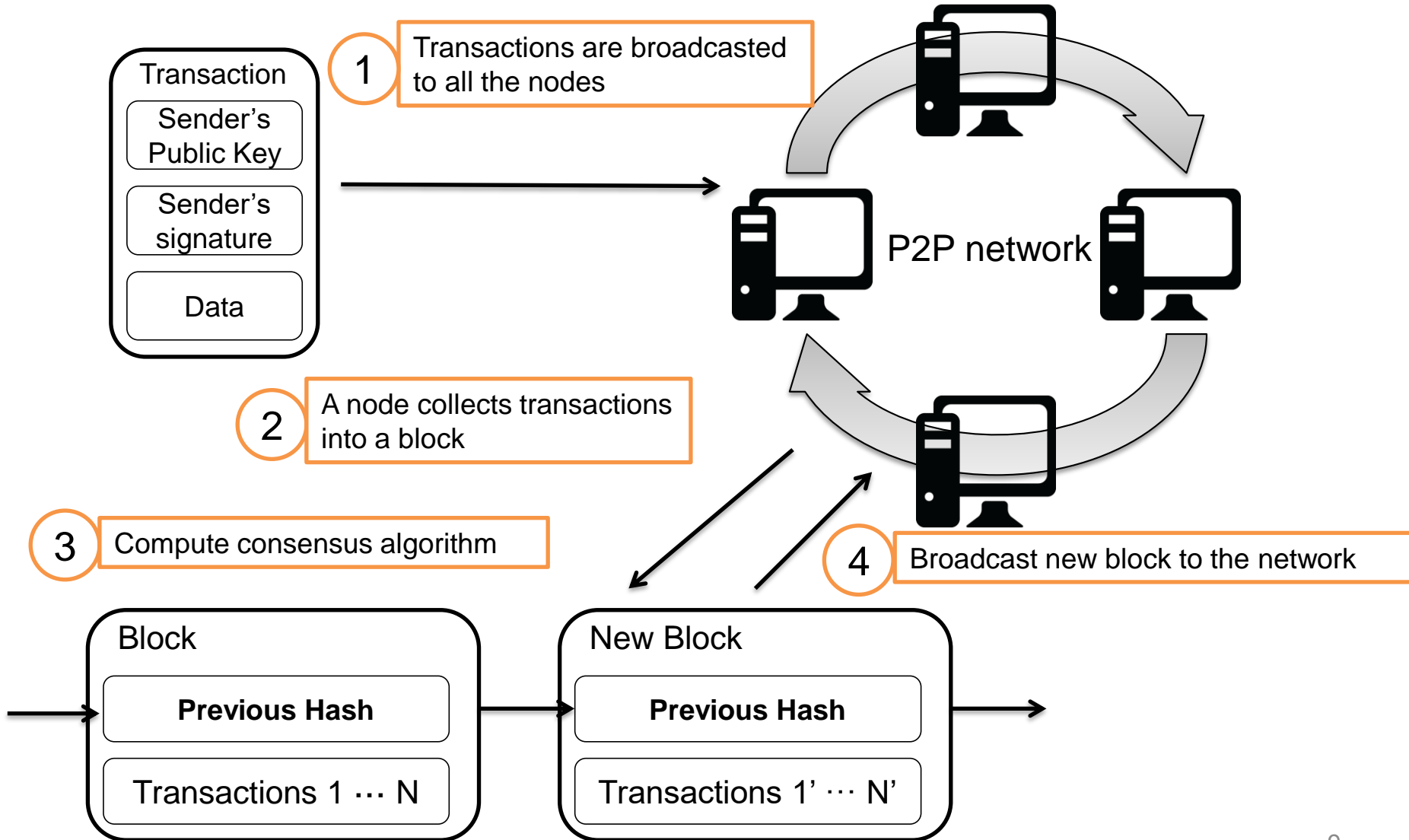


# Blockchain - Transactions

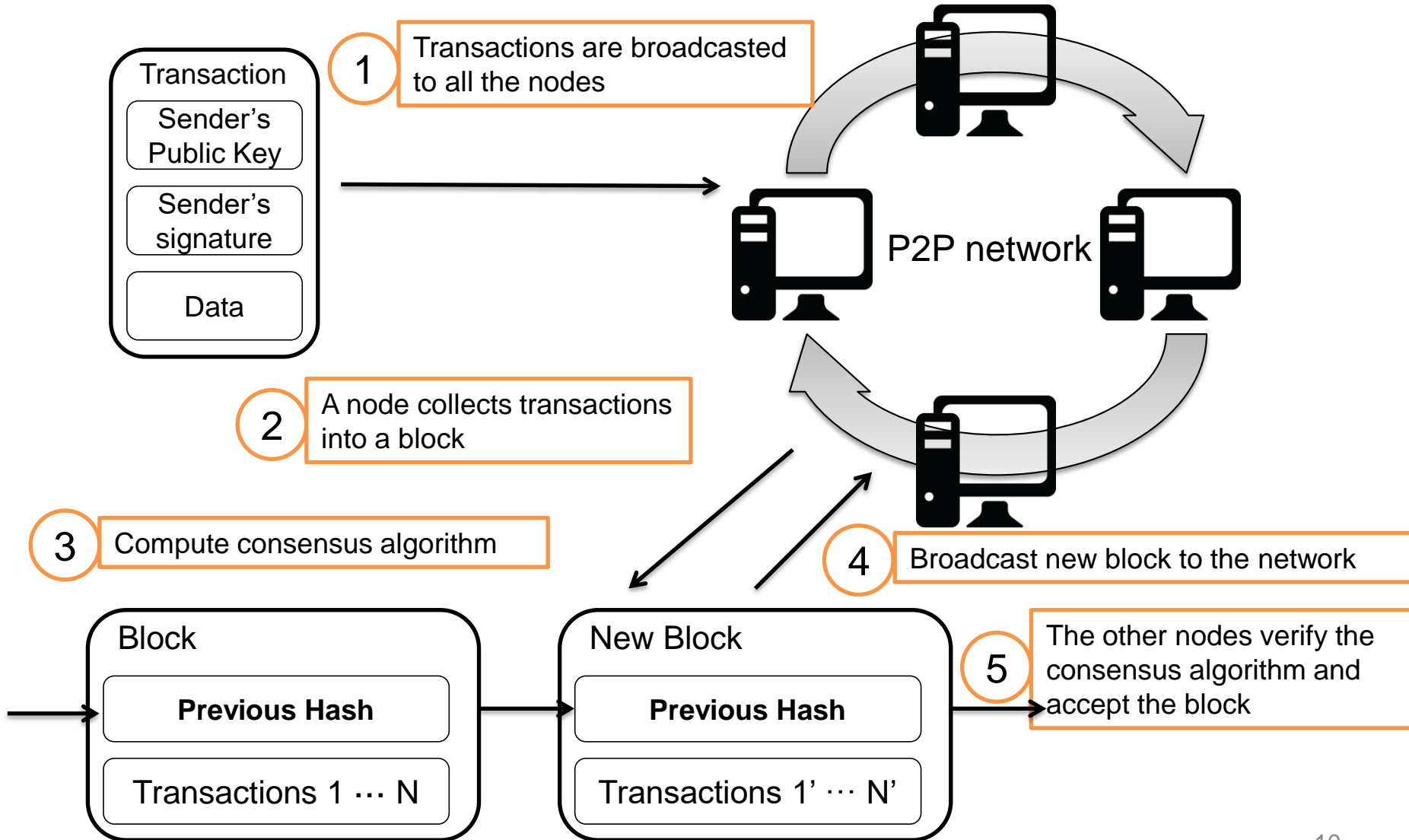




# Blockchain - Transactions



# Blockchain - Transactions



# Summary of features

## vs. traditional PKI systems

### Advantages

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

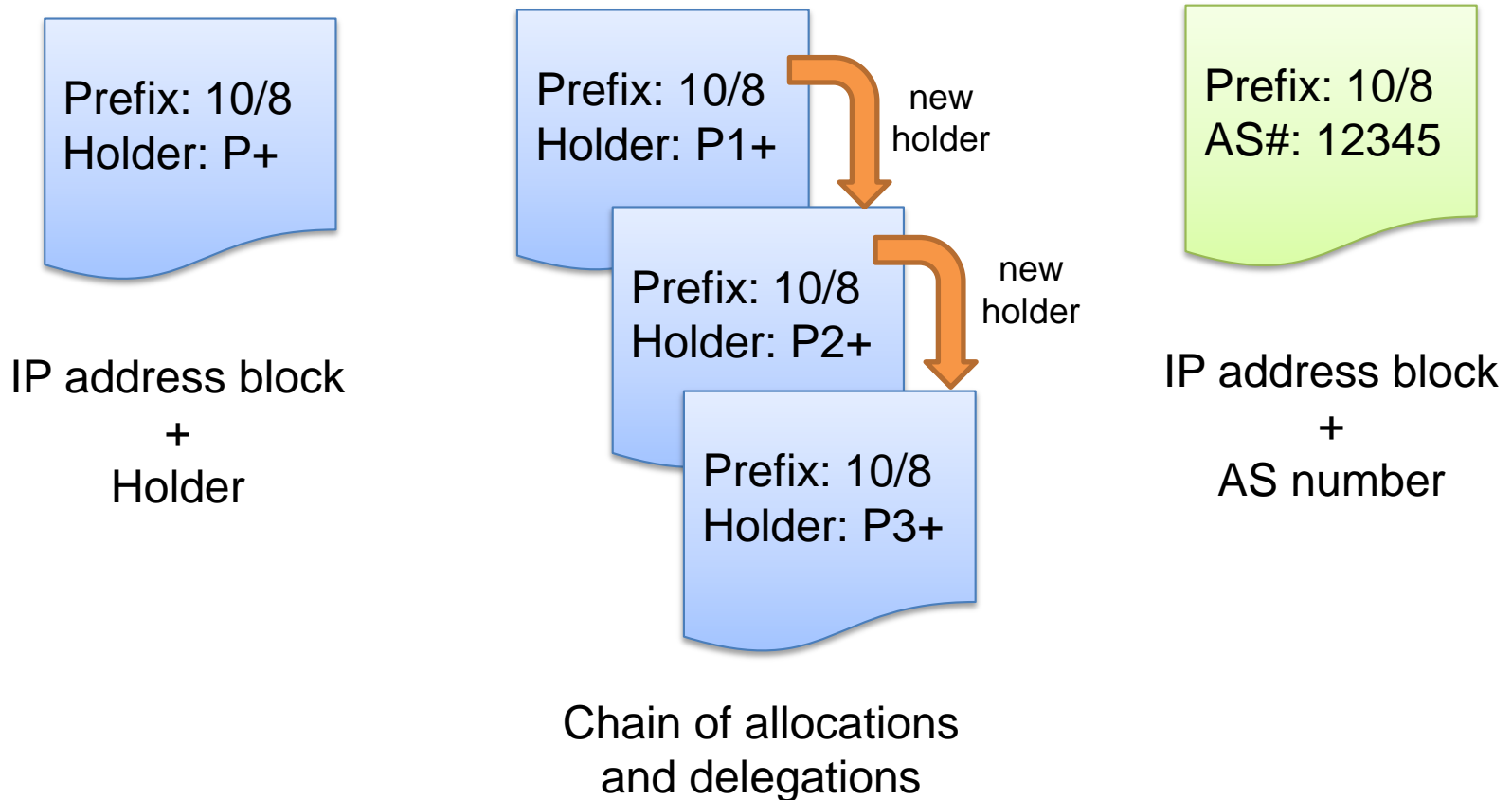
### Drawbacks

- No crypto guarantees
- Large storage
- Costly bootstrapping

# **Blockchain for IP addresses**

# Data in the blockchain

We want to store:



# IP addresses vs. coins

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

# Example

# Allocation

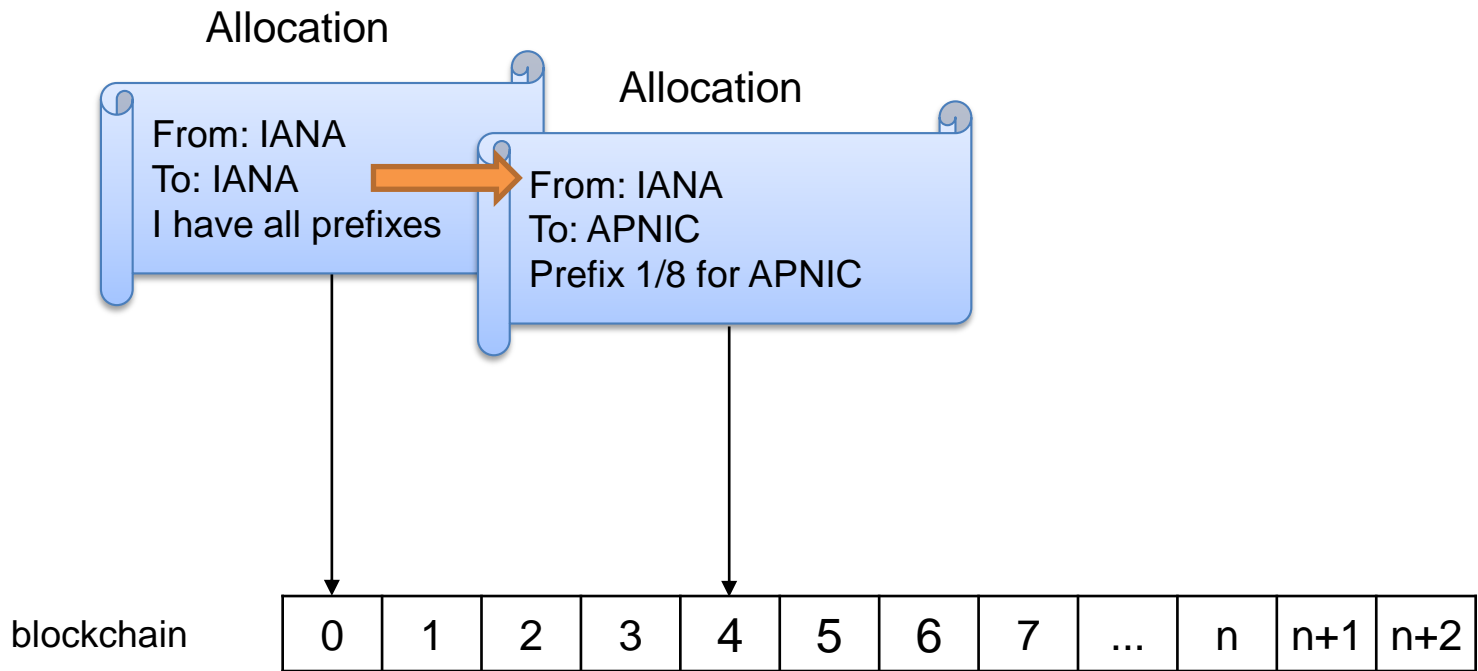
From: IANA  
To: IANA  
I have all prefixes

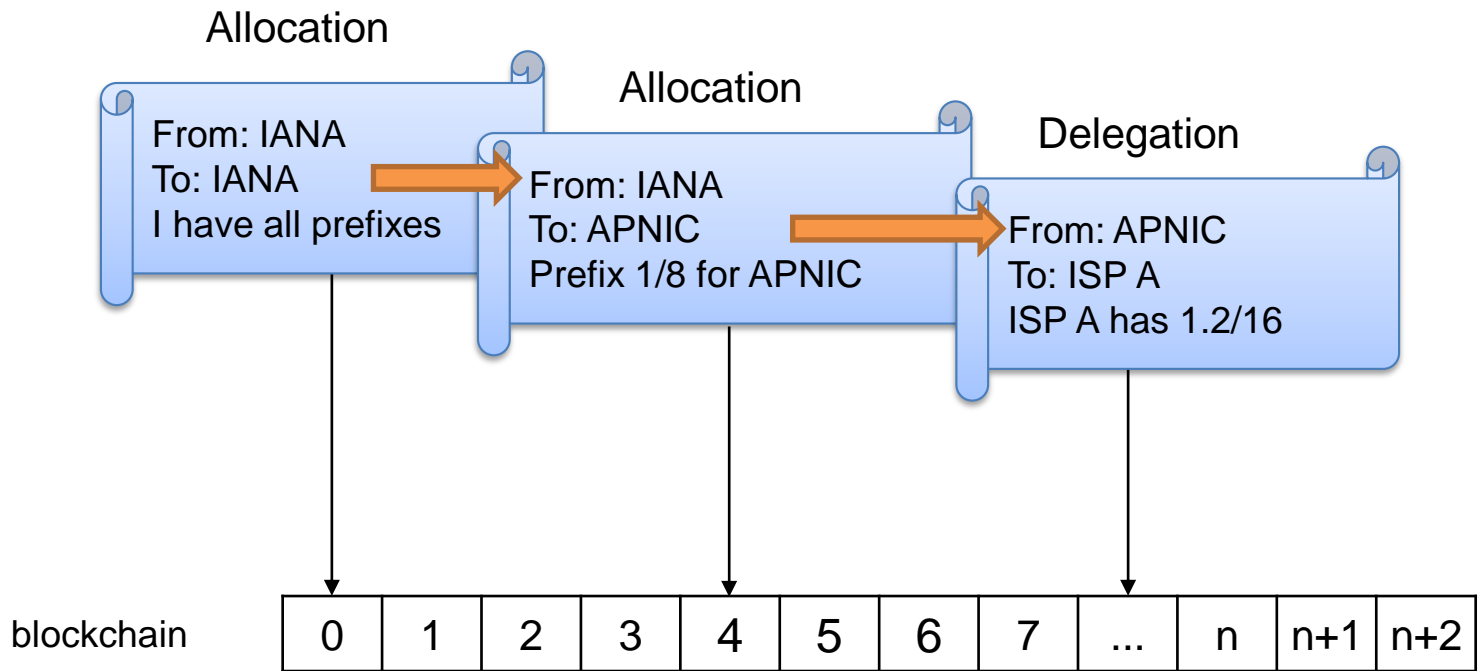


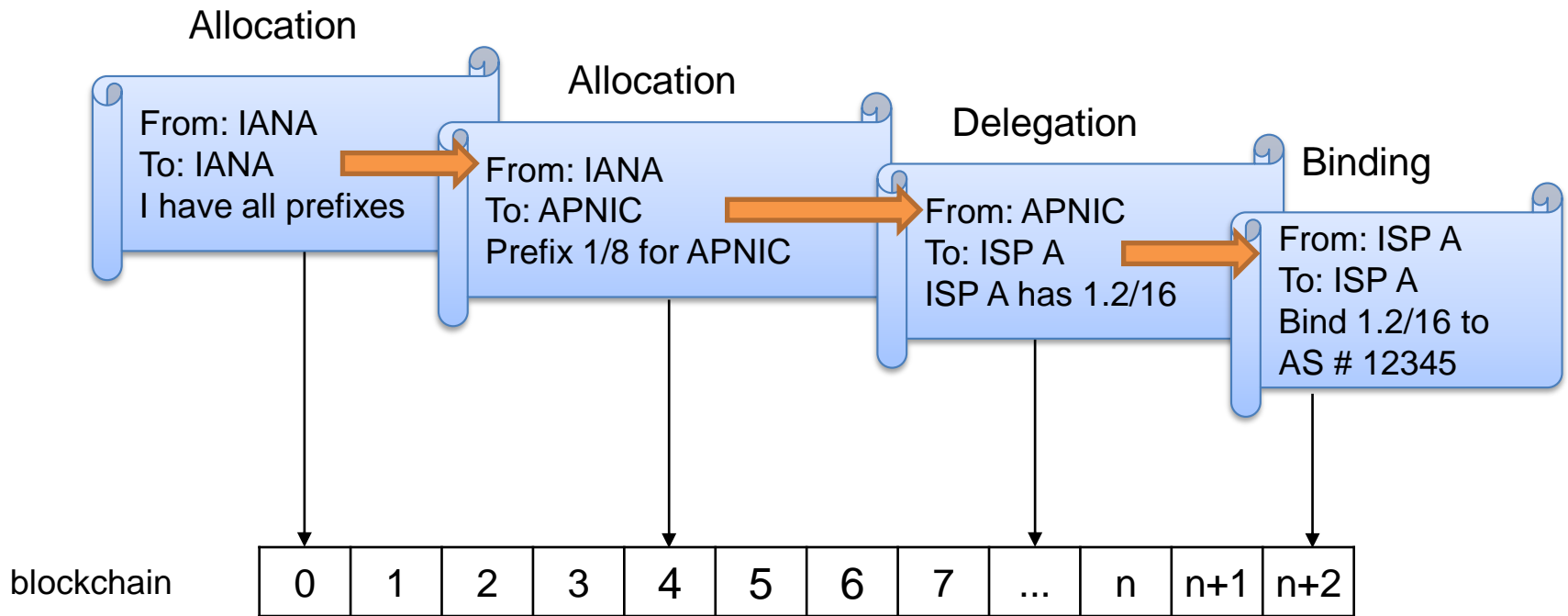
blockchain

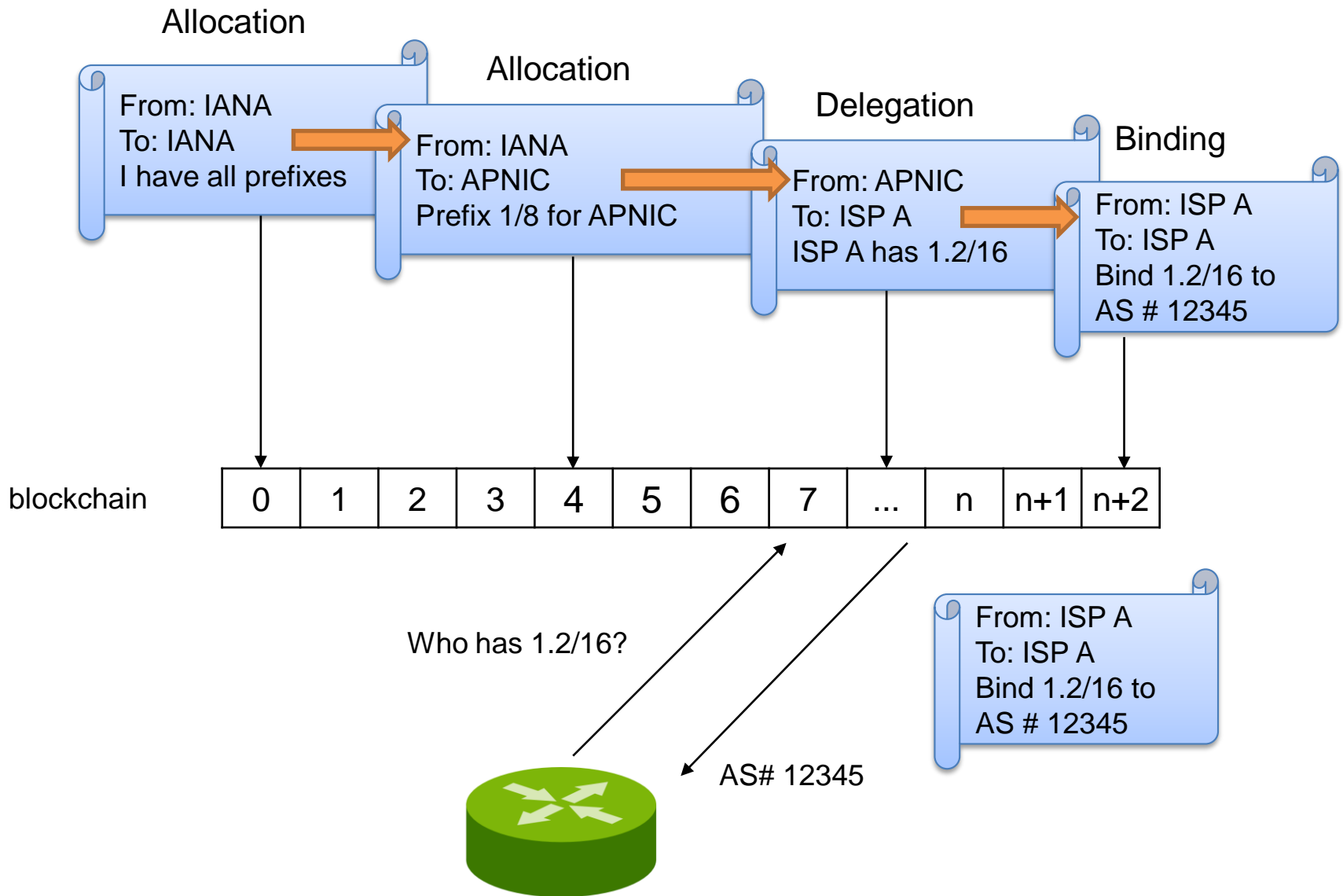
0	1	2	3	4	5	6	7	...	n	n+1	n+2
---	---	---	---	---	---	---	---	-----	---	-----	-----







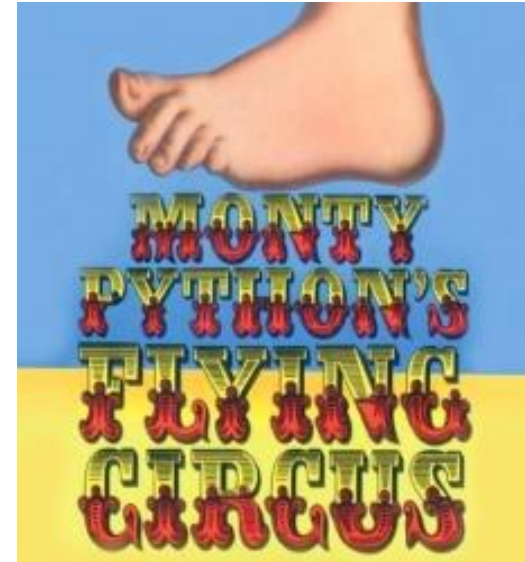




# Prototype

# Prototype

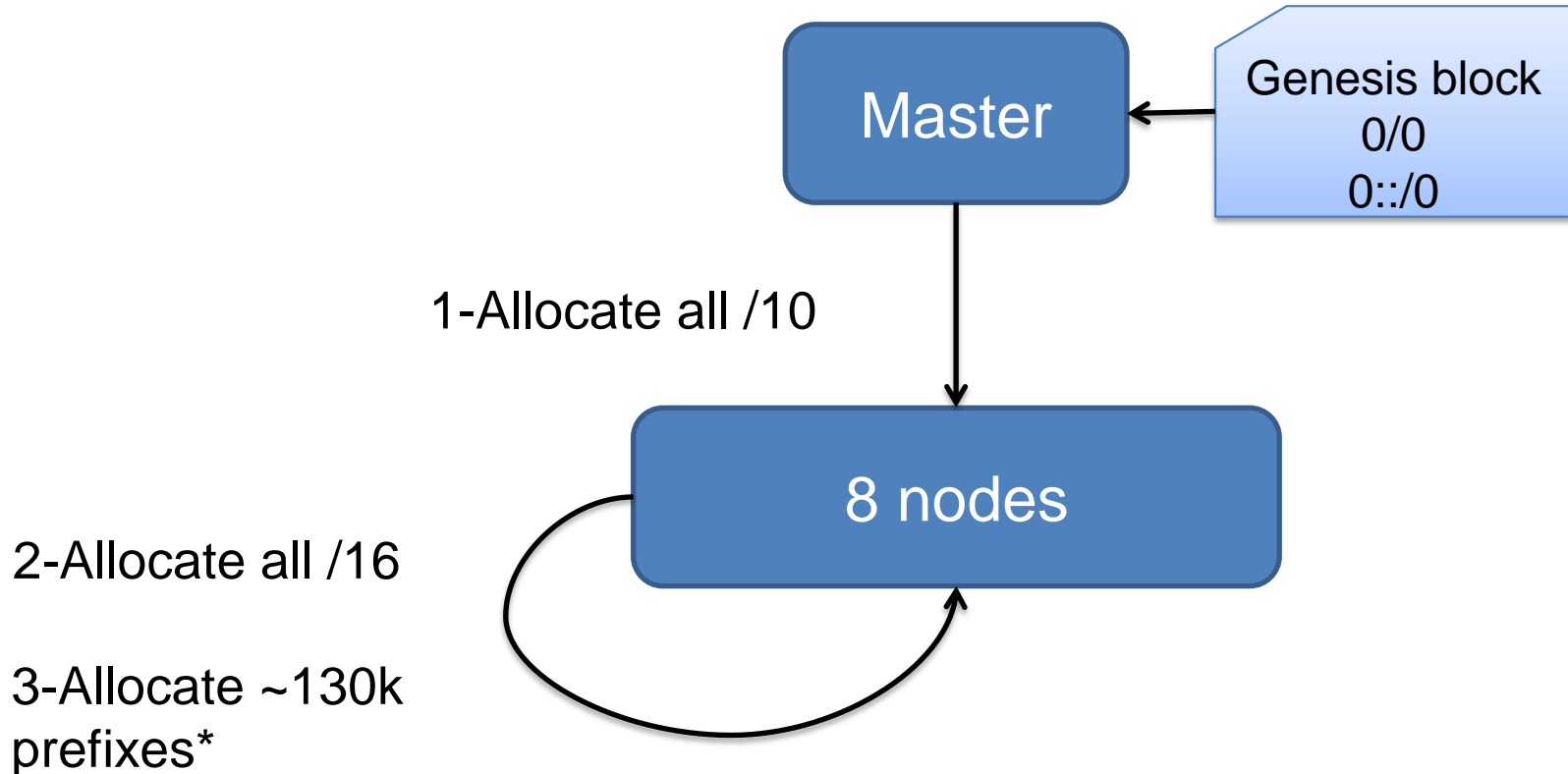
- Python
- Features:
  - Simple Proof of Stake
  - Block time 60s
  - 2 MB blocks
  - IPv4 and IPv6



[http://sharetv.com/shows/monty\\_python's\\_flying\\_circus\\_uk](http://sharetv.com/shows/monty_python's_flying_circus_uk)

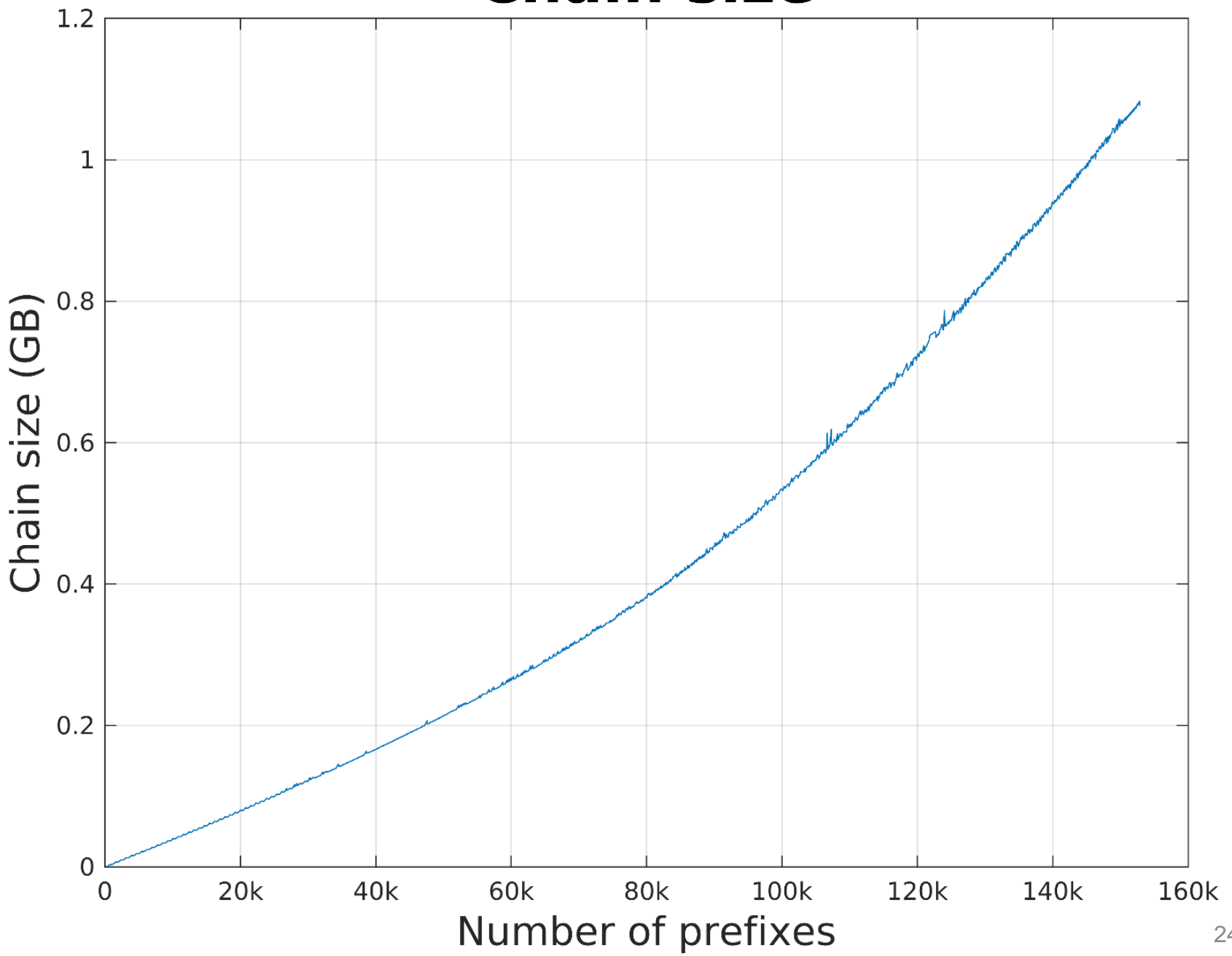
- Open-sourced:  
<https://github.com/OpenOverlayRouter/blockchain-mapping-system>

# Experiment



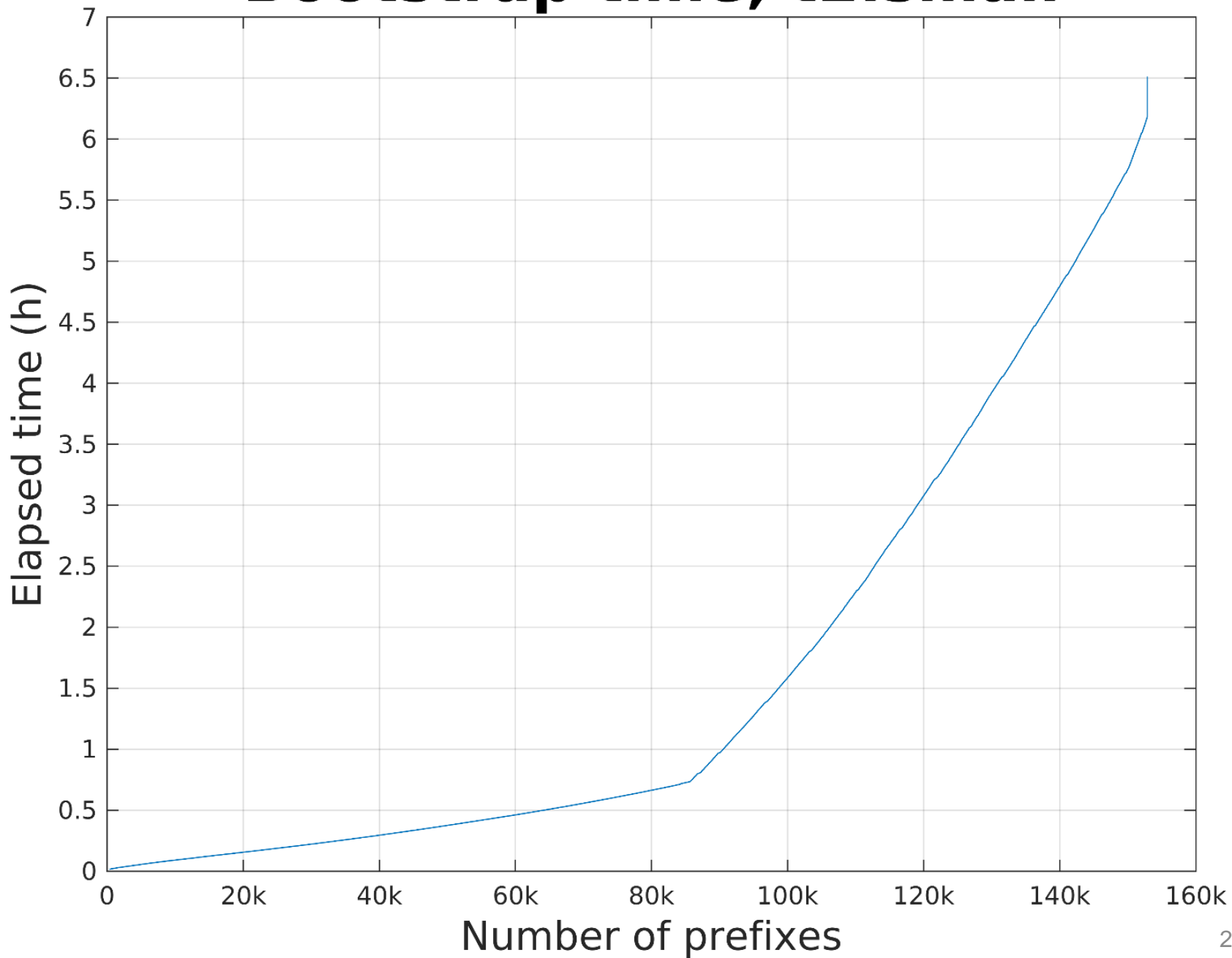
\*Extracted from RIR statistics exchange files, eg.  
<ftp://ftp.apnic.net/pub/stats/apnic/delegated-apnic-extended-latest>

# Chain size





# Bootstrap time, t2.small



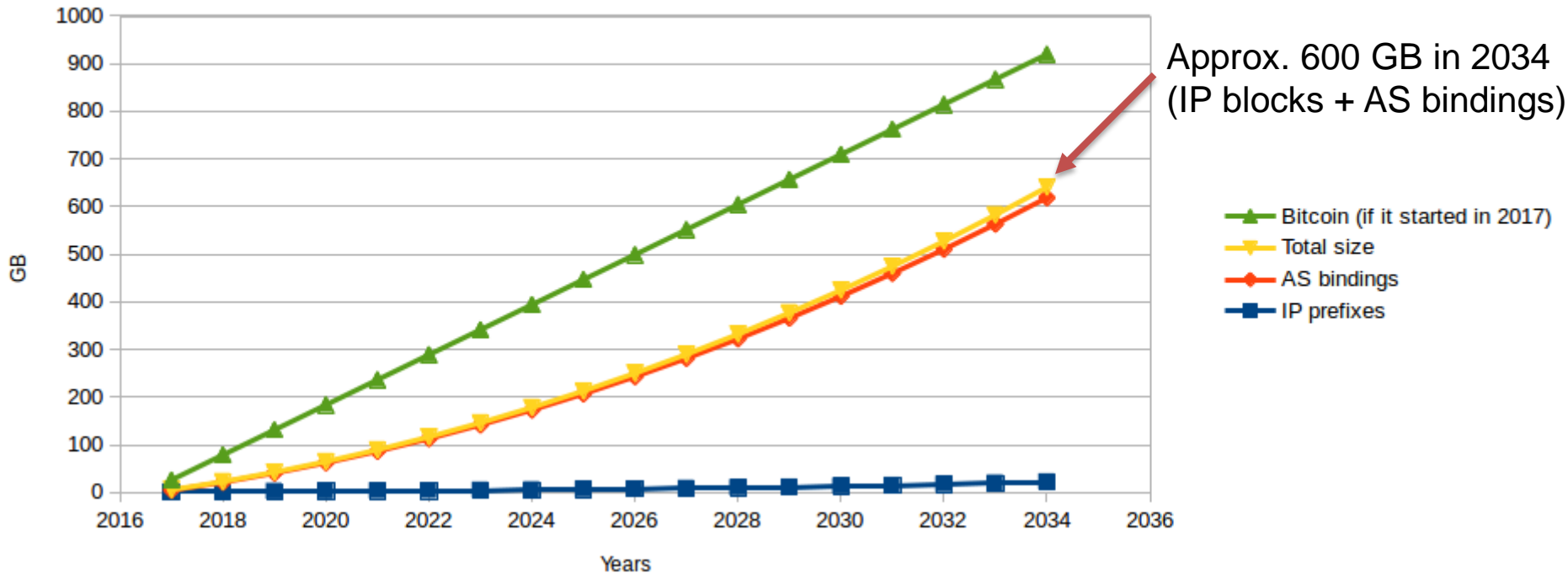
# Thanks for listening!

More info:

<http://arxiv.org/abs/1805.04439>

# Scalability

Blockchain size estimation



- 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>

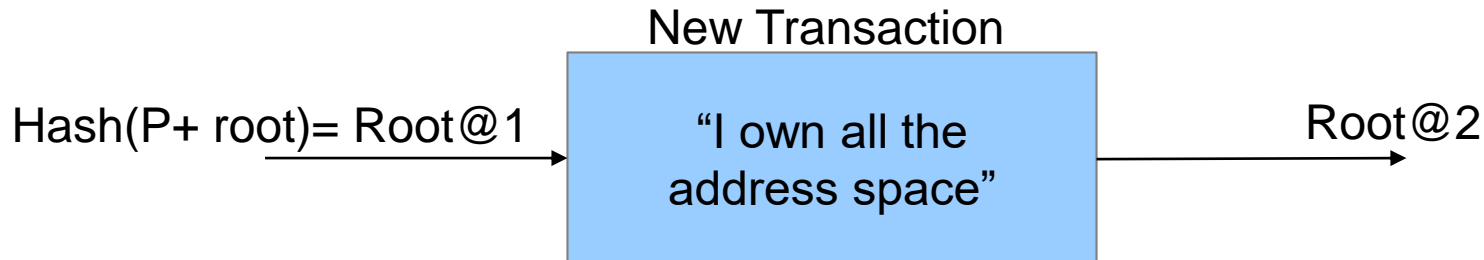
# Storage

- 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

# Transaction examples

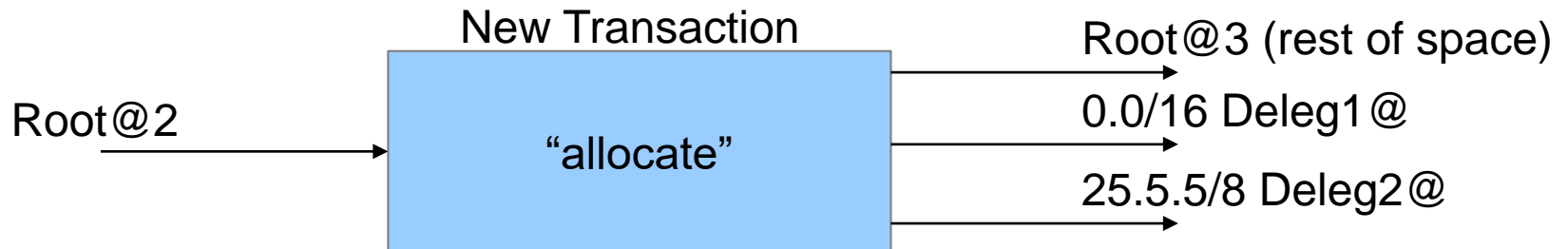
# First transaction

- 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

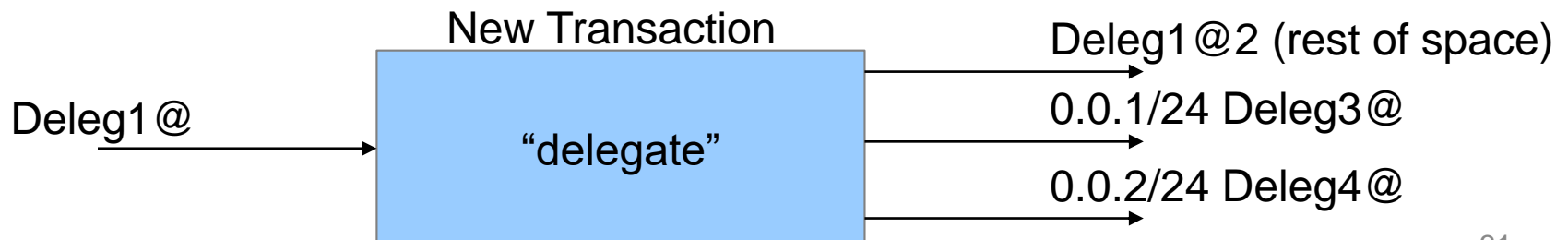


# Prefix allocation and delegation

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

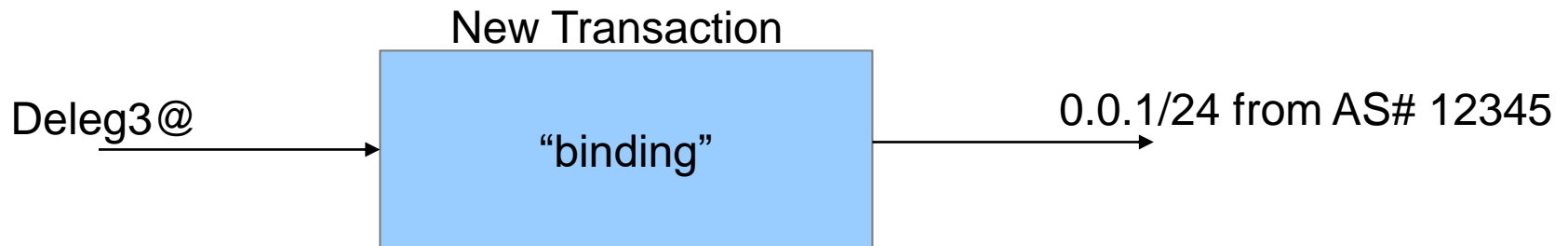


- Holders can further delegate address blocks to other entities



# 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!