A Blockchain-based Mapping System

IETF 97 – Seoul
November 2016

Jordi Paillissé, **Albert Cabellos,** Vina Ermagan, Fabio Maino
acabello@ac.upc.edu

OPEN OVERLAY ROUTER

http//openoverlayrouter.org

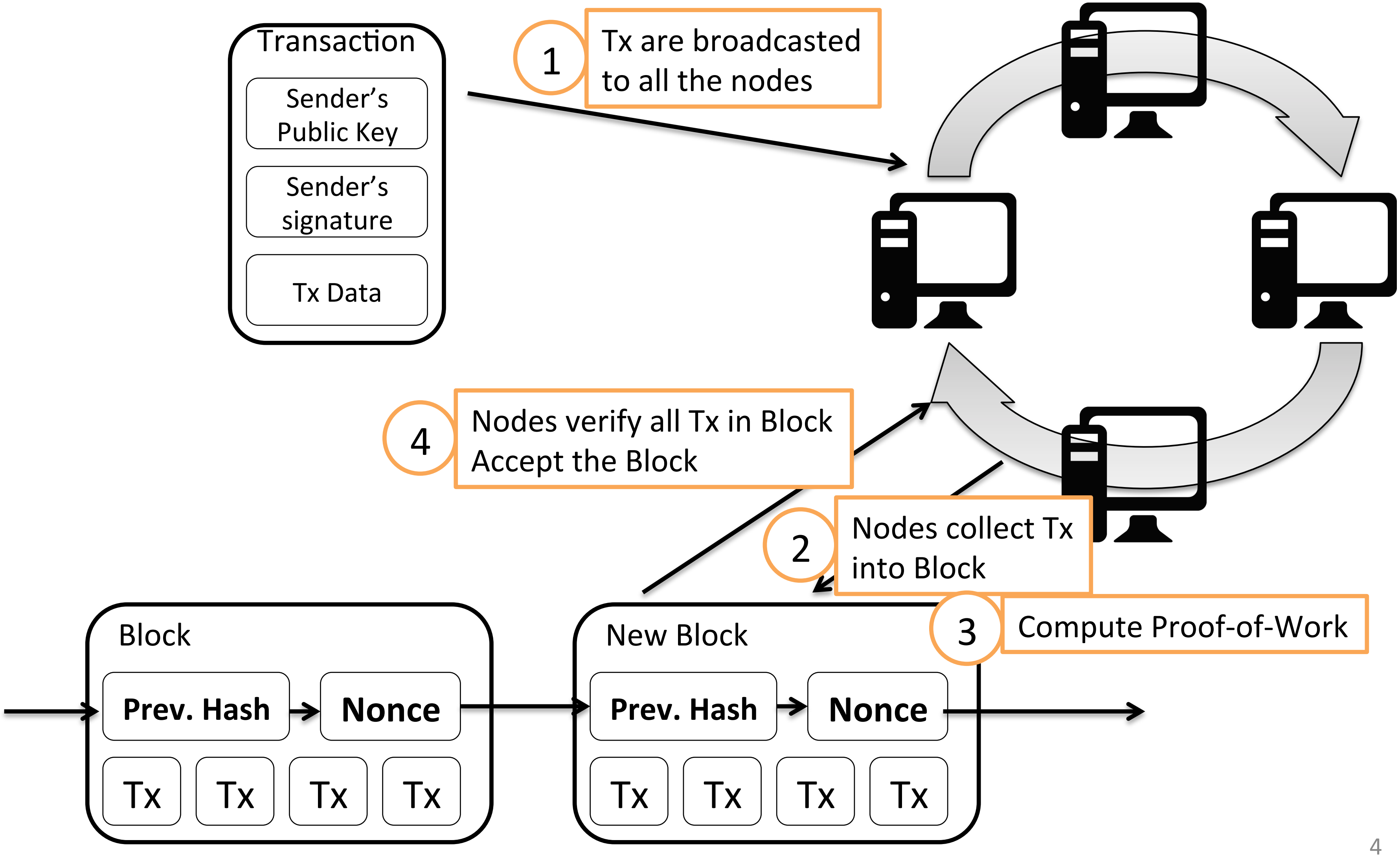
A short Blockchain tutorial

Blockchain - Basics

- Blockchain is the technology supporting Bitcoin
  - Beyond Bitcoin's controversies, blockchain is a successful technology
  - Blockchain used in many applications
- Blockchain creates a public ledger (log) with verifiable transactions
- Works based on distributed consensus
  - Does not require trust
  - Consensus is based on CPU-voting majority
  - Inherently decentralized
- Digital events are stored in an irrefutable record, participating entities can verify it
  - Append only

"Blockchain Technology", Sutardja Center (UC Berkeley)
http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf

Blockchain - Transactions



Transaction

Sender's Public Key

Sender's signature

Tx Data

1 Tx are broadcasted to all the nodes

4 Nodes verify all Tx in Block
Accept the Block

2 Nodes collect Tx into Block

3 Compute Proof-of-Work

Block

Prev. Hash

Nonce

Tx Tx Tx Tx

New Block

Prev. Hash

Nonce

Tx Tx Tx Tx

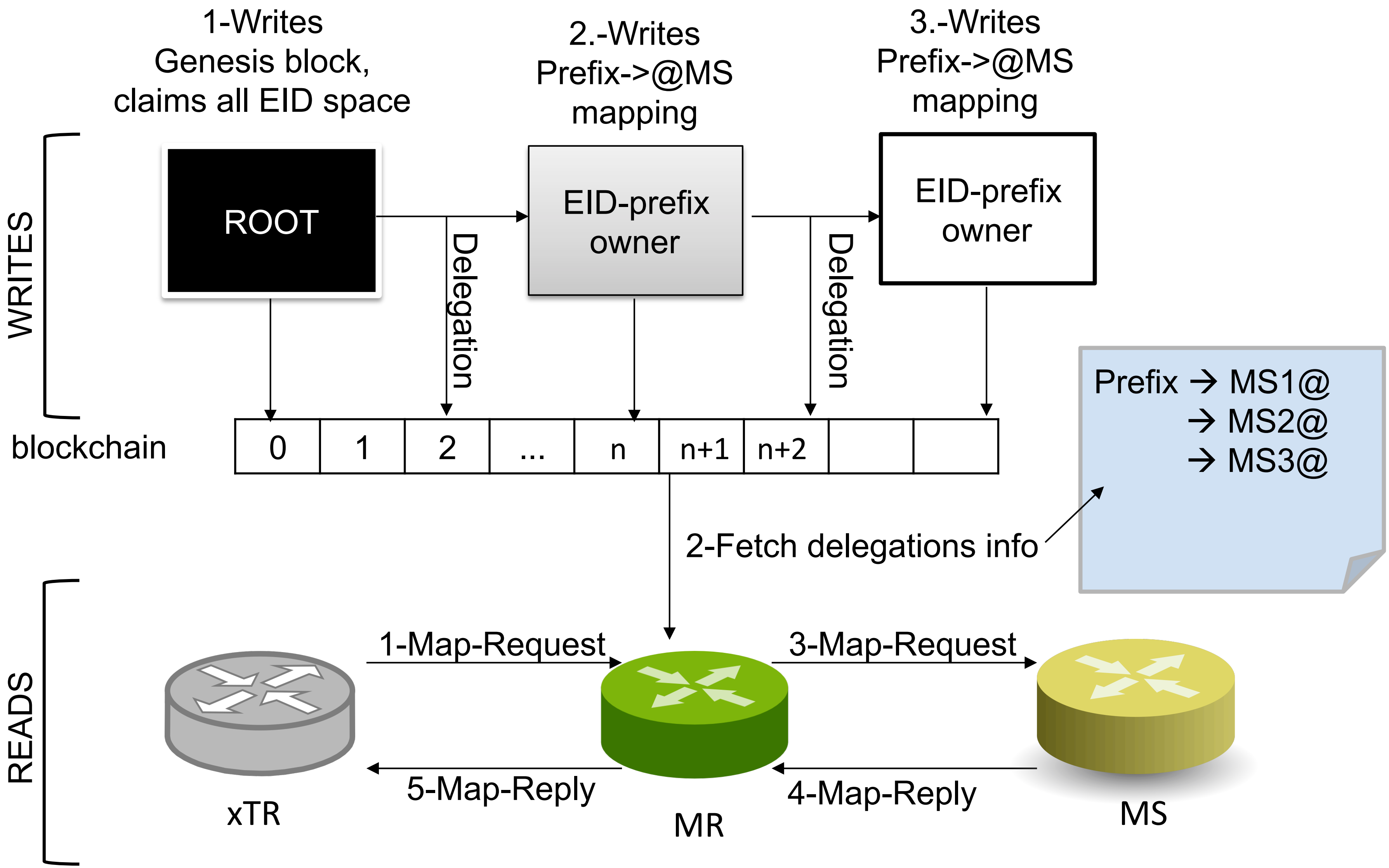
Blockchain − Mining

- Miners compute proof-of-work
  - Finding a nonce that when added to the input changes the resulting of the hash, the hash starts with N zeros.
- Miners receive incentives
  - Transaction fees
  - Mint bitcoins
- The accepted chain is the longer one
  - Has more Proof-of-Work

A Blockchain-based Mapping System **Overview**

Basic Idea

- **Objective**: Store EID-prefix delegations (LISP-DDT data) in a blockchain
  - EID to MS@
  - MRs use blockchain to locate the IP of the MS responsible of the EID-prefix
- **Idea**: An EID-prefix delegation is equivalent to a bitcoin transaction
  - Wallet: A block of EID-prefixes
  - Transaction: Delegating an EID-prefix to another entity
  - Blockchain: A public ledger of the delegations, from the current owner to the root


1-Writes
Genesis block,
claims all EID space
2.-Writes
Prefix->@MS
mapping
3.-Writes
Prefix->@MS
mapping
WRITES
ROOT
EID-prefix owner
EID-prefix owner
Delegation
Delegation
blockchain
0
1
2
...
n
n+1
n+2
Prefix → MS1@
→ MS2@
→ MS3@
2-Fetch delegations info
READS
1-Map-Request
3-Map-Request
5-Map-Reply
4-Map-Reply
xTR
MR
MS

Pros and Cons

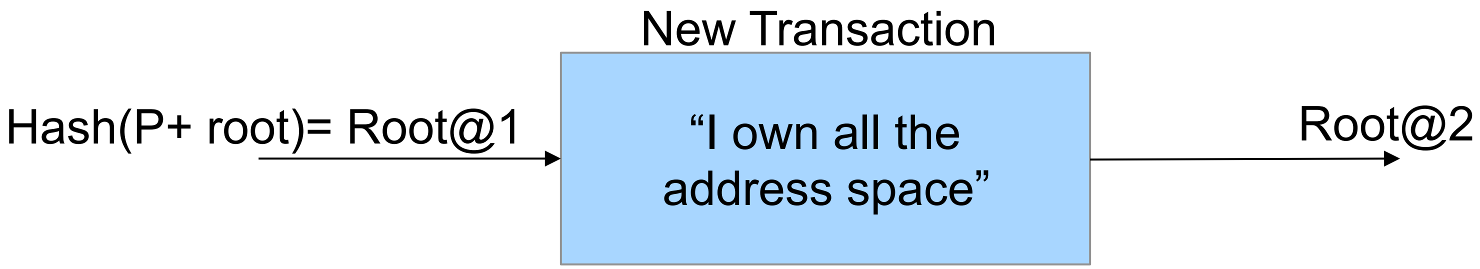
- Distributed database
  - Works on consensus
- Offers a verifiable logs of delegations
- No CAs
- Rekeying is simple
- Bootstrapping is expensive
- Consensus is based on CPU voting
  - Can be adjusted in a private chain

A Blockchain-based Mapping System

EID-Prefix Delegation

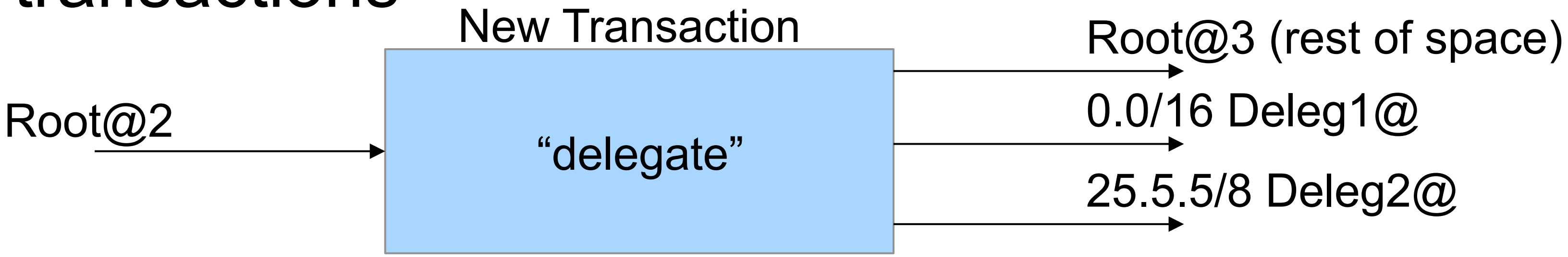
Ownership

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

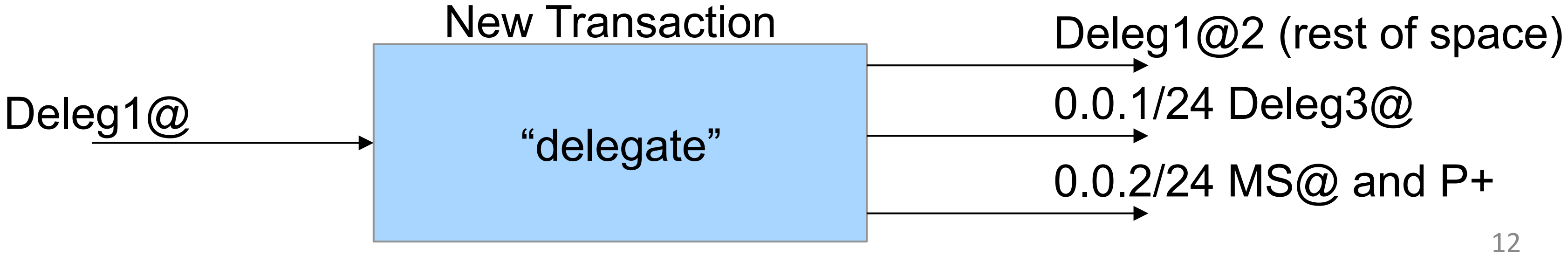


Ownership

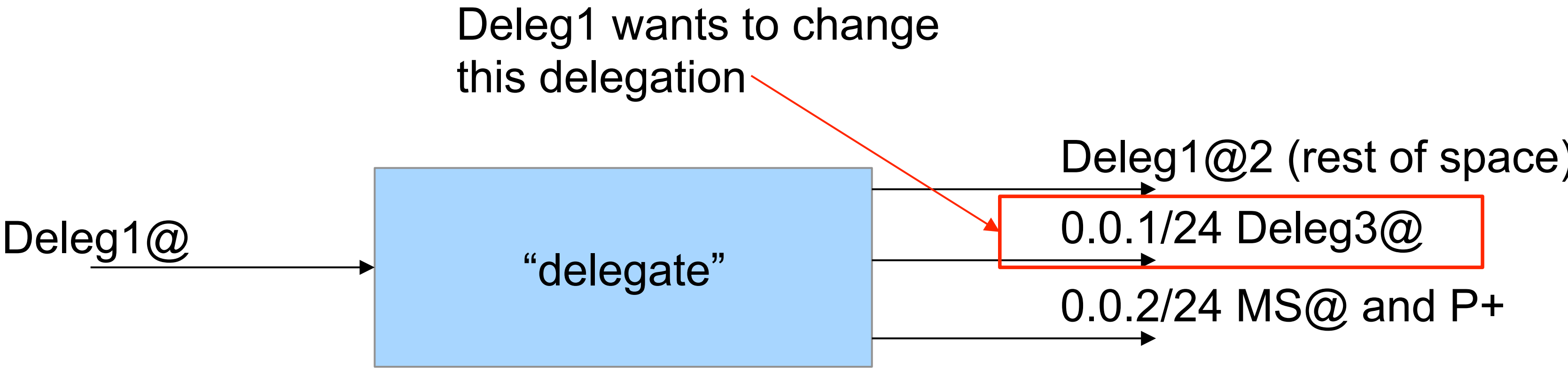
- Root delegates EID-prefixes to other entities (identified by Hash(Public Key)) by adding transactions



- Owners can further delegate address blocks to other entities or write MS addresses (and MS's Public Key)



Revocation



Deleg1 wants to change this delegation

Deleg1@

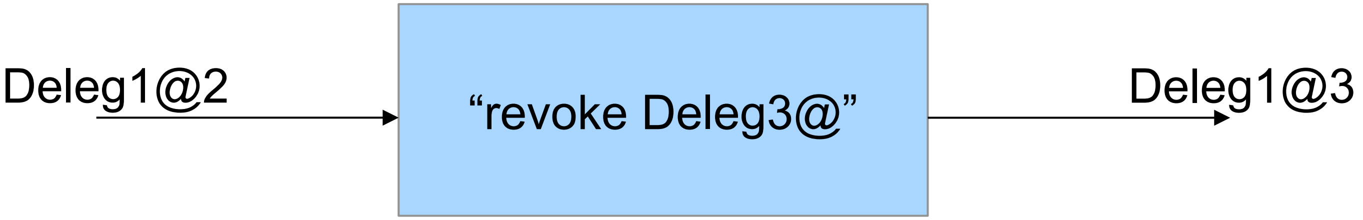
“delegate”

Deleg1@2 (rest of space

0.0.1/24 Deleg3@

0.0.2/24 MS@ and P+

Deleg1 adds a new transaction revoking the delegation



Deleg1@2

“revoke Deleg3@”

Deleg1@3

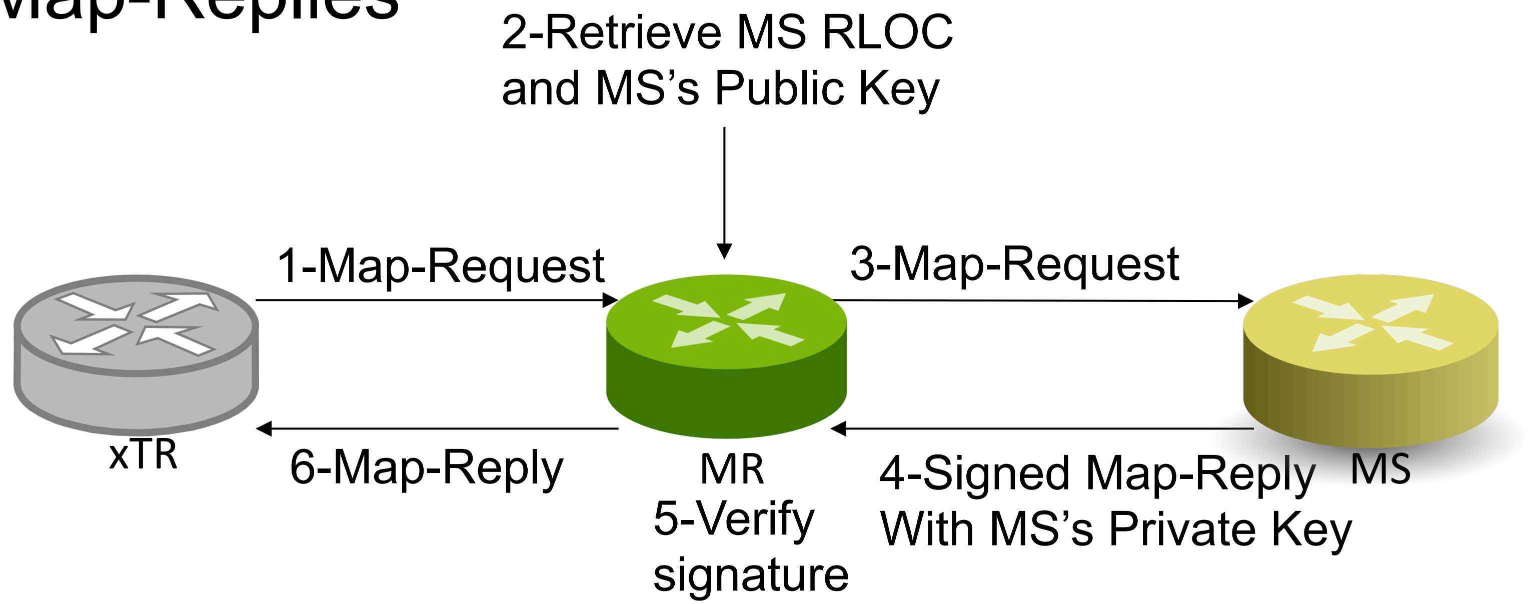
The system acknowledges Deleg1 as the immediate previous owner and changes data in the delegations DB

Rekeying

- Delegating the owned EID-prefixes to itself using a new key set.
- Simpler than traditional rekeying schemes
- Can be performed independently, i.e. each owner can do it without affecting other owners

Map-Reply Authentication

- MS public key can also be included in the delegations
- Since blockchain provides authentication and integrity for this key, MRs can use it to verify Map-Replies



2-Retrieve MS RLOC and MS's Public Key

1-Map-Request

3-Map-Request

xTR

6-Map-Reply

MR

5-Verify signature

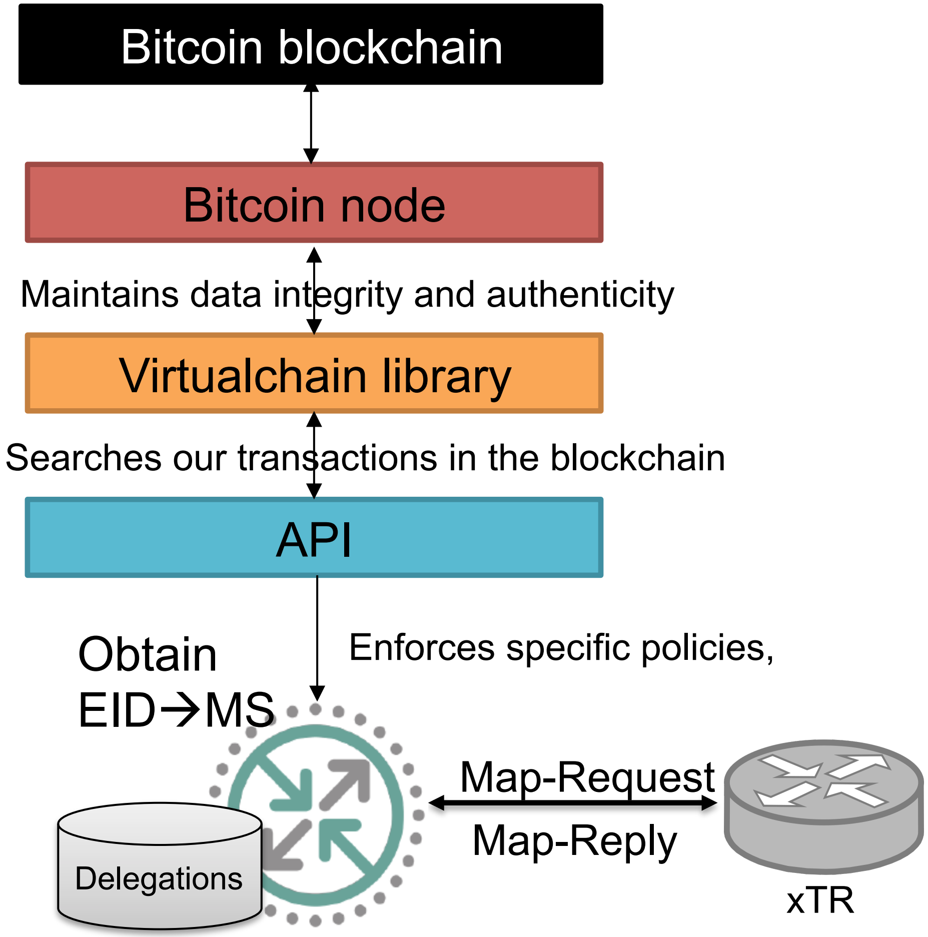
4-Signed Map-Reply With MS's Private Key

MS

A Blockchain-based Mapping System **Prototyping**

Prototype

- Currently working on an OpenOverlayRouter prototype
- On top of Bitcoin's **testing** infrastructure
- Map-Resolver that obtains and verifies all EID→MS delegations
- Scripts to write, read and verify delegations



Bitcoin blockchain
Bitcoin node
Maintains data integrity and authenticity
Virtualchain library
Searches our transactions in the blockchain
API
Obtain EID→MS
Enforces specific policies,
Delegations
Map-Request
Map-Reply
xTR

A Blockchain-based Mapping System **Summary and Future Work**

Summary and Future Work

- Represents a new approach to Mapping Systems
  - Distributed and based on consensus
  - Public ledger of delegations
  - Secure
- Work-in-progress
  - Public vs. Private chain?
  - Store information, hash of information or route to information?
  - Who should be able to revoke?
  - Extend it to include EID-to-RLOC mappings?

A Blockchain-based Mapping System

IETF 97 – Seoul
November 2016

Jordi Paillissé, **Albert Cabellos,** Vina Ermagan, Fabio Maino
acabello@ac.upc.edu

OPEN OVERLAY ROUTER

http//openoverlayrouter.org