A BlockChain based Testbed for BGP Verification

HUAWEI

<u>Shen Yan</u>
Xinpeng Wei
Fei Yang
Bingyang Liu

Telefonica

Diego Lopez

UC3M

Marcelo Bagnulo Braun

China Telecom

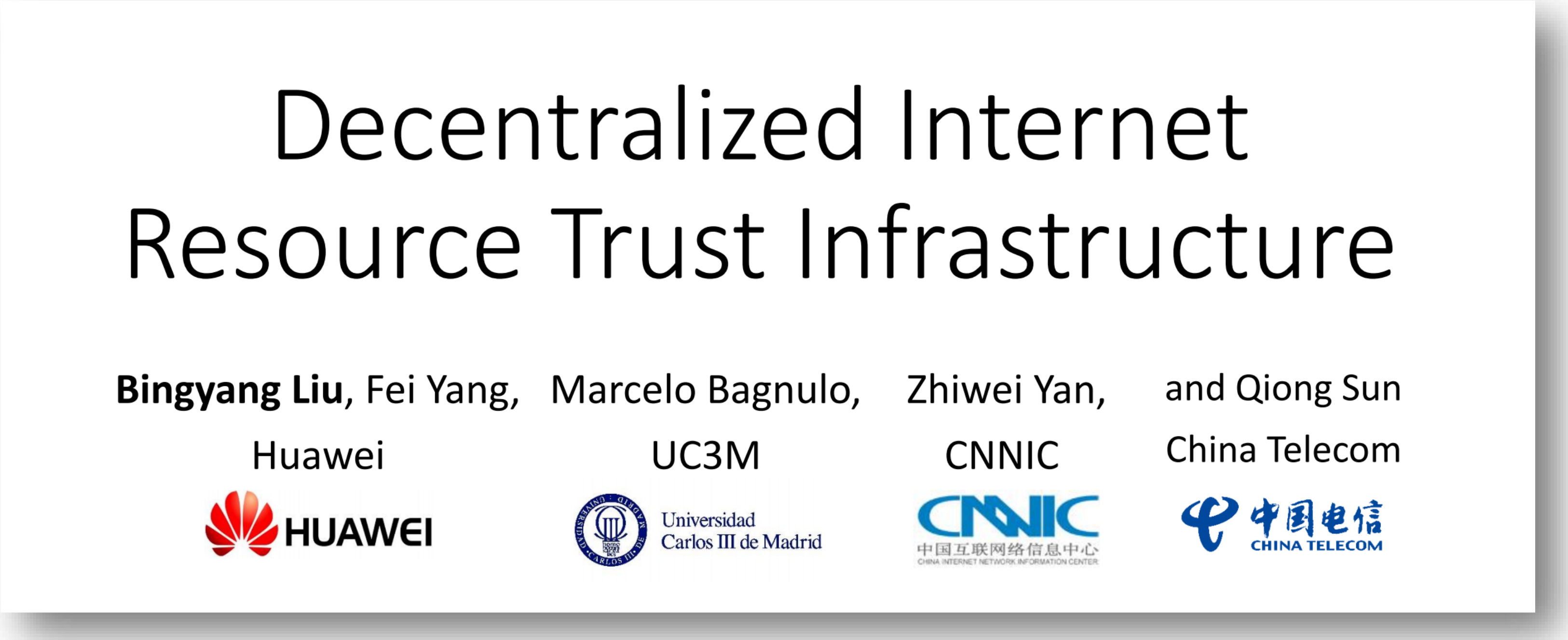
Bo Lei

CNNIC

Zhiwei Yan

DII Project

https://datatracker.ietf.org/meeting/102/materials/slides-102-dinrg-decentralized-internet-resource-trust-infrastructure-bingyang-liu-00.pdf



Decentralized Internet Resource Trust Infrastructure

Bingyang Liu, Fei Yang, Marcelo Bagnulo, Zhiwei Yan, and Qiong Sun

Huawei UC3M CNNIC China Telecom

HUAWEI
Universidad Carlos III de Madrid
CNNIC
中国互联网络信息中心
CHINA INTERNET NETWORK INFORMATION CENTER
中国电信
CHINA TELECOM

DII (Distributed Internet Infrastructure) Introduction

Application Layer

This layer is an open application layer that supports and promotes innovative, trusted, decentralized network applications.

Name Space Management Layer

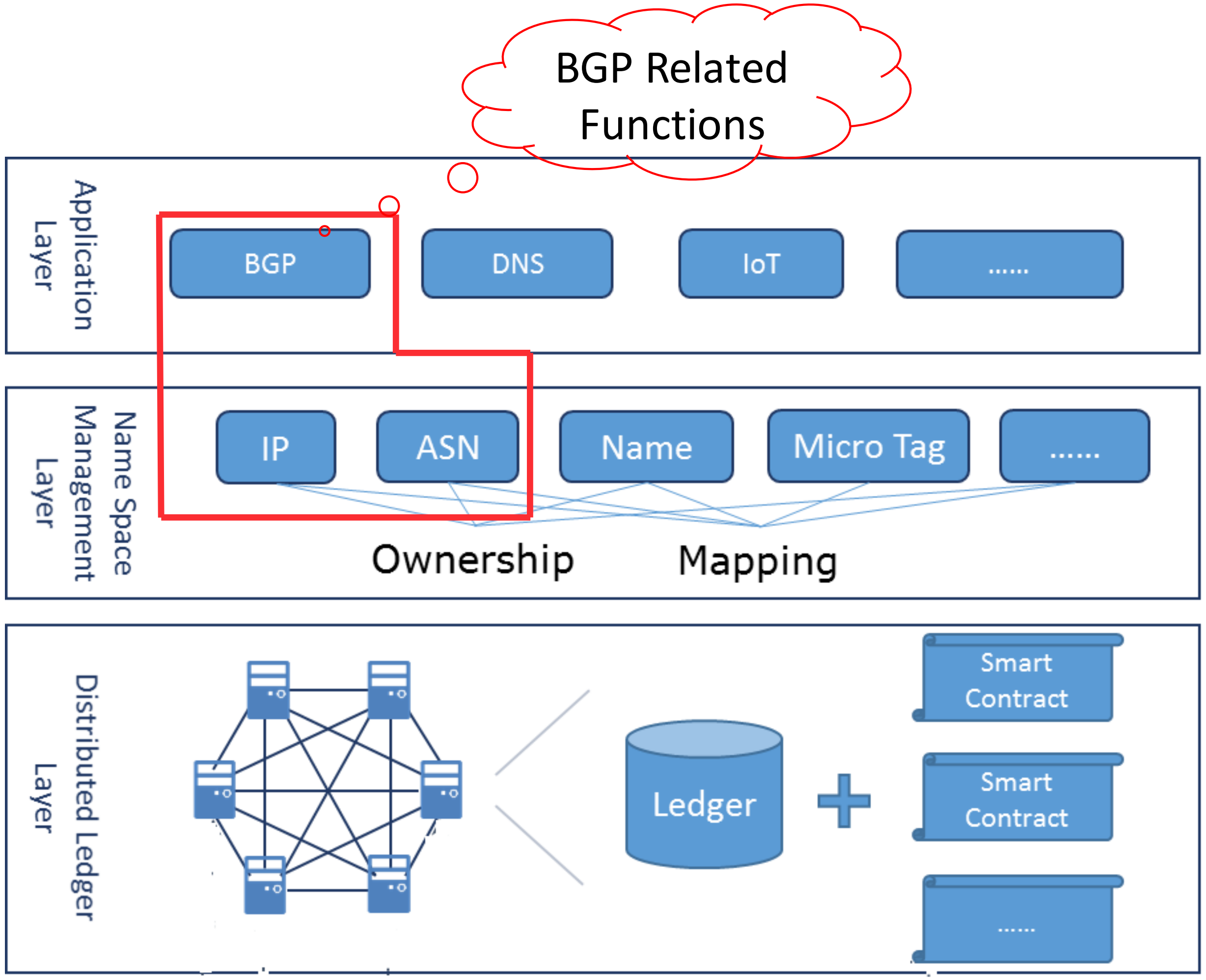
Trusted name space ownership and mapping

- IP & ASN: trusted routing system
- Domain name & IP: trusted resolution system
- Other name spaces: host identifier, content name, IoT ID, …

Distributed Ledger Layer

The Distributed Ledger Layer is the basis of decentralized network infrastructure. It is in charge of providing the following functions:

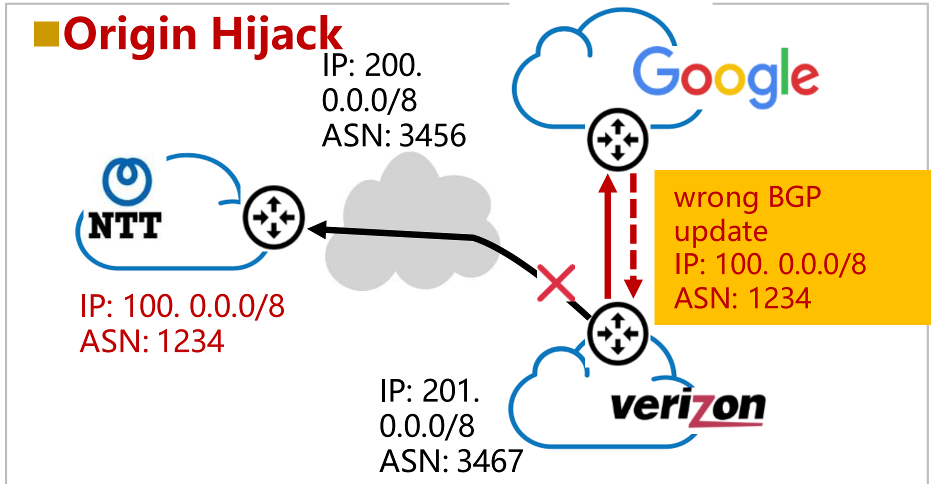
- Providing decentralized system structure
- Providing distributed consensus mechanism
- Providing smart contracts capability



BGP Issues

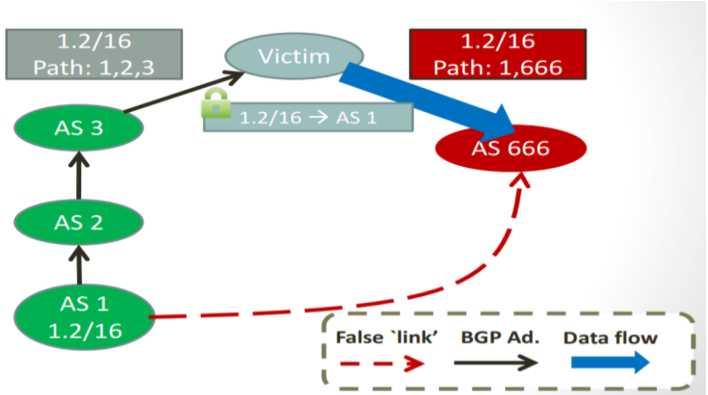
- BGP lacks the ability to verify the validity of announcement messages, which brings many risks.

Origin Hijack



- Attack traffic by publishing address prefixes that are not their own

Path Hijack



- Hijack traffic by publishing false path information

Route Leak

Google was also the victim of a routing leak. In this case Google’ s prefixes were leaked by Hathway, an Indian ISP, and accepted by their peer Bharti Airtel. Bharti then advertised routes to dozens of major ASes around the globe. In Figure 5, we can see the leak of an existing prefix 74.125.200/24 from Hathway, with traffic from Bharti (AS9498) transiting via Hathway (AS17488) to Google. This leak lasted for nearly a day, from 10:30 UTC on March 11th to 9:15 UTC on March 12th.

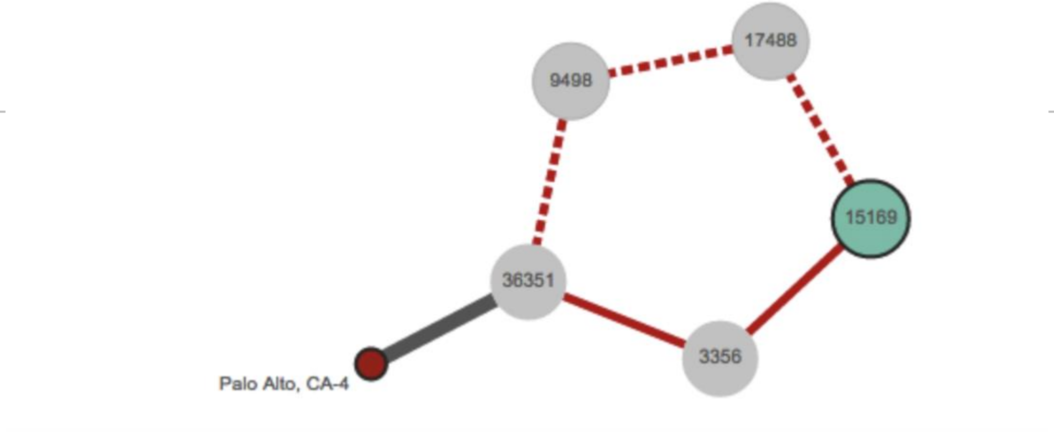
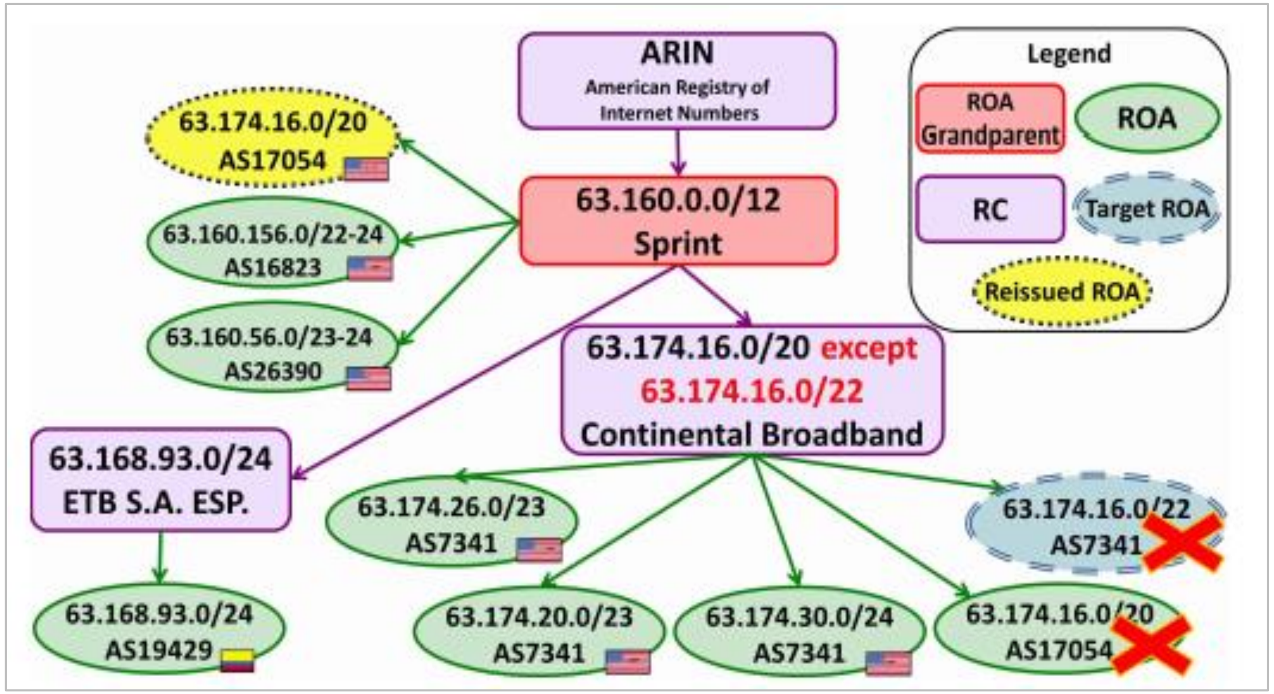


Figure 5: Route leak to Google via Hathway AS17488 that affects Bharti Airtel AS9498.

https://blog.thousandeyes.com/finding-and-diagnosing-bgp-route-leaks/

Why Not RPKI ?

- **Depending on the centralized trust model, once the Authority node is misconfigured or attacked, it raises security issues and is difficult to avoid from the mechanism.**
  - **Certificate revocation/overwrite: Unilaterally cancel the issued RC certificate, causing the BGP announcement of the lower node to be invalid; equivalent to depriving the applicant of the ownership of the IP address.**
- **Does not solve the route leakage problem**
- **Path verification requires hop-by-hop signature decryption, which affects route convergence speed.**

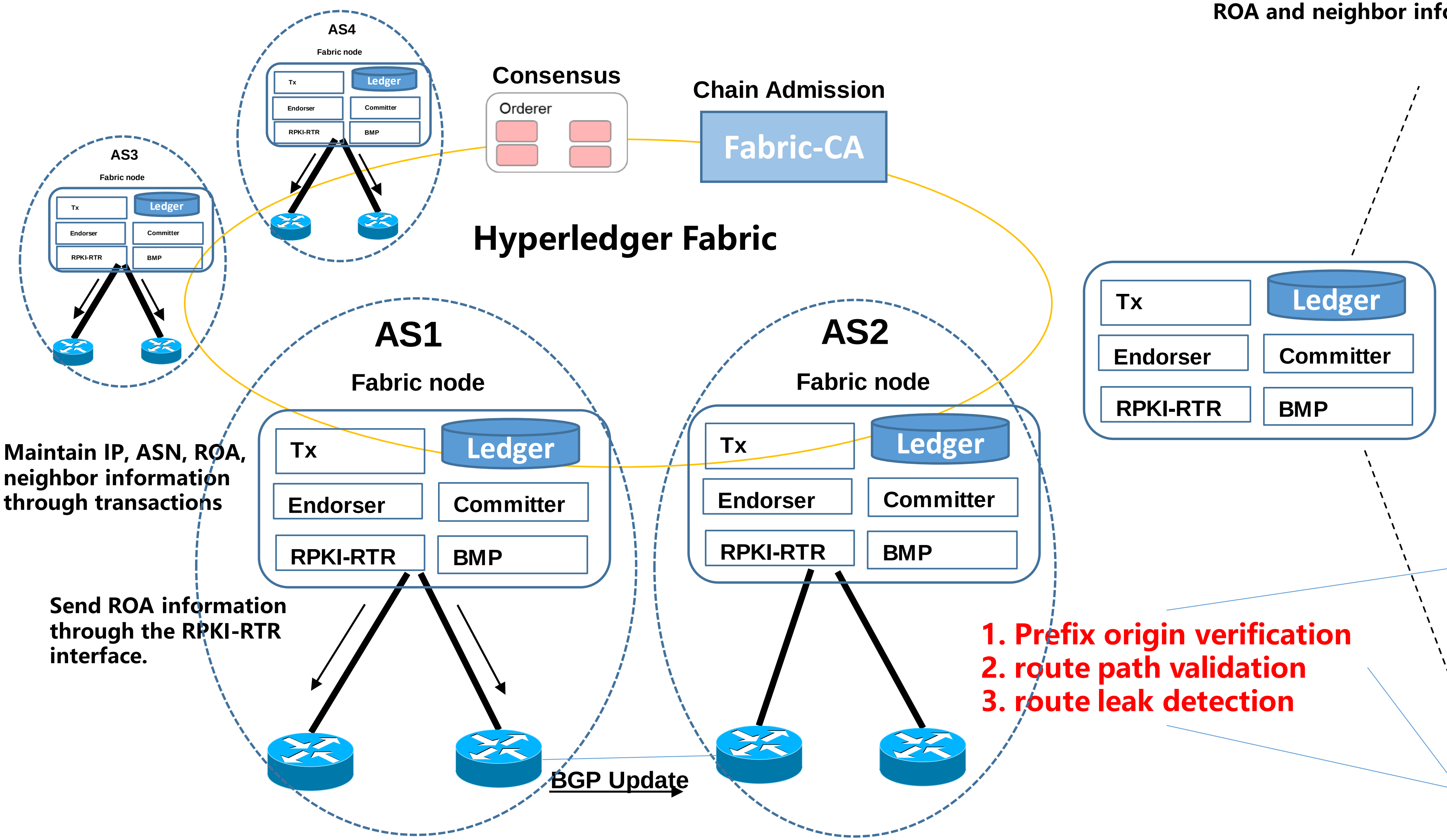


Heilman E, Cooper D, Reyzin L, et al. From the Consent of the Routed: Improving the Transparency of the RPKI[C]//ACM SIGCOMM Computer Communication Review. ACM, 2014, 44(4): 51-62.

- Real Cases
  - 2013.12, ROA (79.139.96.0/24, AS 51813) was deleted which leads network unreachability in part of Russia.
  - 2014.1, a Nigeria network’ s ROA was failed due to its parent’ s RC was overwritten.
  - 2013.12, ARIN mis-issued a ROA, allowing AS6128 to announce 173.251.0.0/17~24， lead to the legitimate announcement to be invalid.

DII-based BGP Verification System Overview

Blockchain stores Ownership, ROA and neighbor information



Maintain IP, ASN, ROA, neighbor information through transactions

Send ROA information through the RPKI-RTR interface.

1. Prefix origin verification
2. route path validation
3. route leak detection

IP Ownership

IP	Owner	Exp date
1.1.1.0/24	ISP1	19/10

ASN Ownership

ASN	Owner	Exp date
100	ISP1	19/10

ROA (IP->ASN)

IP	Maxlength	ASN
1.1.1.0/24	32	100

ASNeighbor(ASN->ASN)

Source	Target	Type
AS1	AS2	P2C
AS2	AS3	P2P

World-state

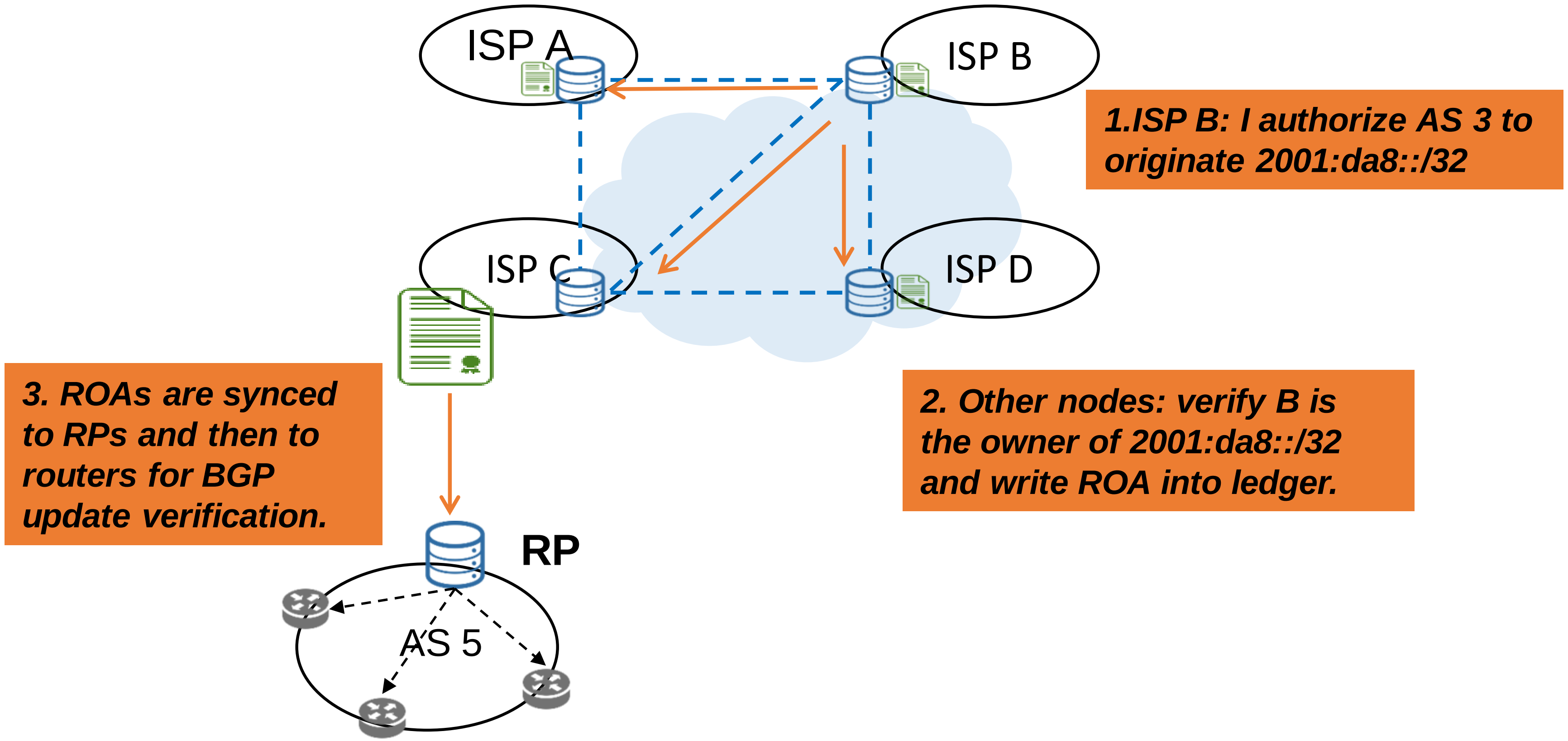
* RPKI-RTR: RPKI to Router Protocol

DII-based BGP Verification - Origin Verification

1. IP address owner initiates an ROA (IP to ASN mapping) as a transaction.

2. Smart contract verifies the address ownership, and writes the ROA into the ledger.

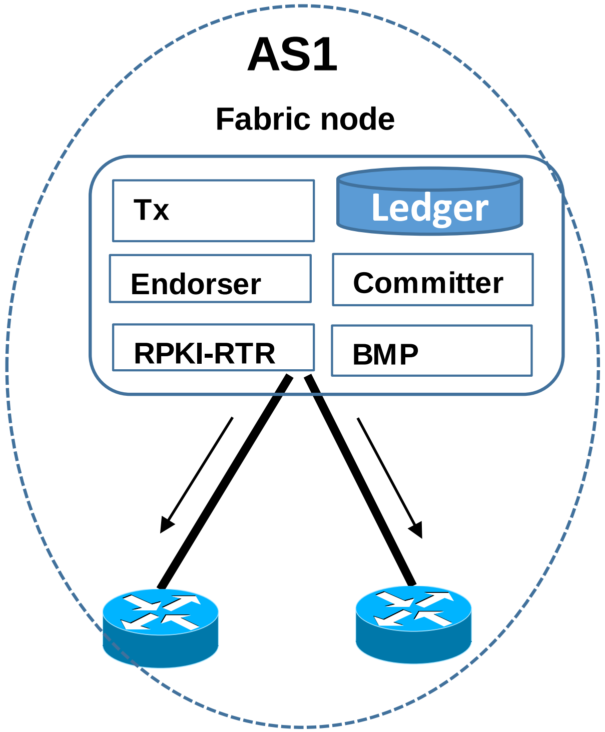
3. Relying parties (RP) get updated ROAs from the ledger, and sync to BGP routers, which then verify BGP routes.



1.ISP B: I authorize AS 3 to originate 2001:da8::/32

2. Other nodes: verify B is the owner of 2001:da8::/32 and write ROA into ledger.

3. ROAs are synced to RPs and then to routers for BGP update verification.

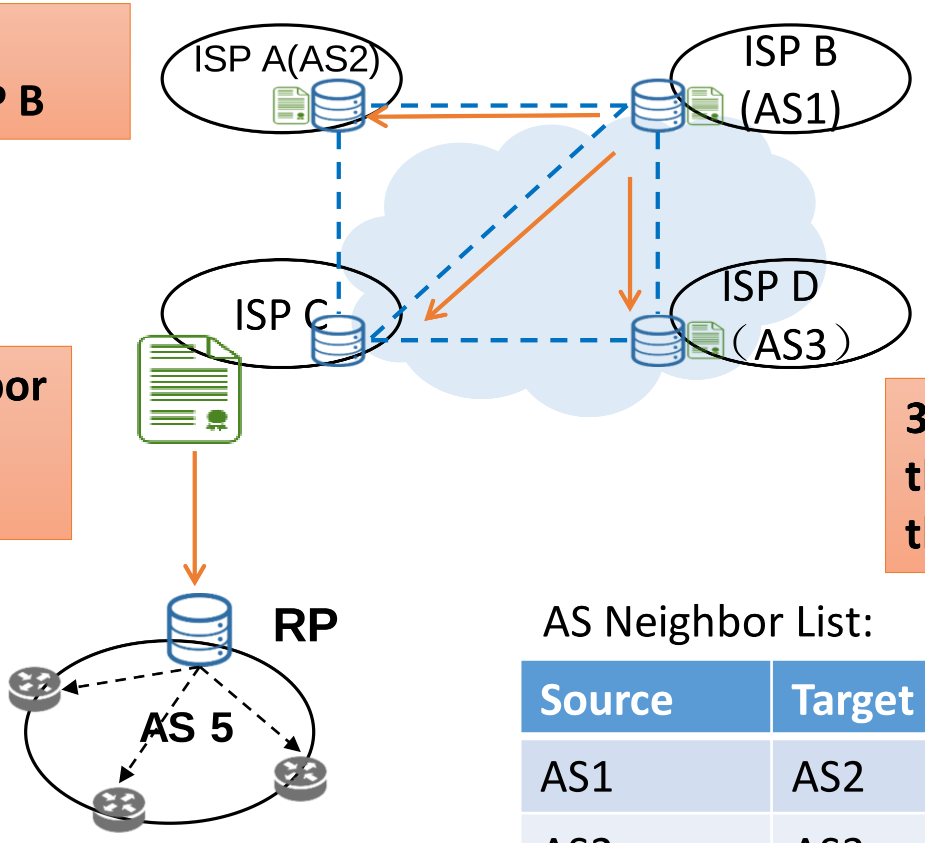


DII-based BGP Verification- AS Path Verification

- Each AS publish its neighbor information in the ledger, and the neighbor information will be used for AS path verification in BGP announcement.
- The Relaying Party (RP) get neighbor information from the ledger and synchronize the information to routers.

2. ISP A confirms its neighborhood with ISP B

1. ISP B publish its neighborhood with ISP A .



4. the RP synchronize neighbor relationship information to routers for path verification.

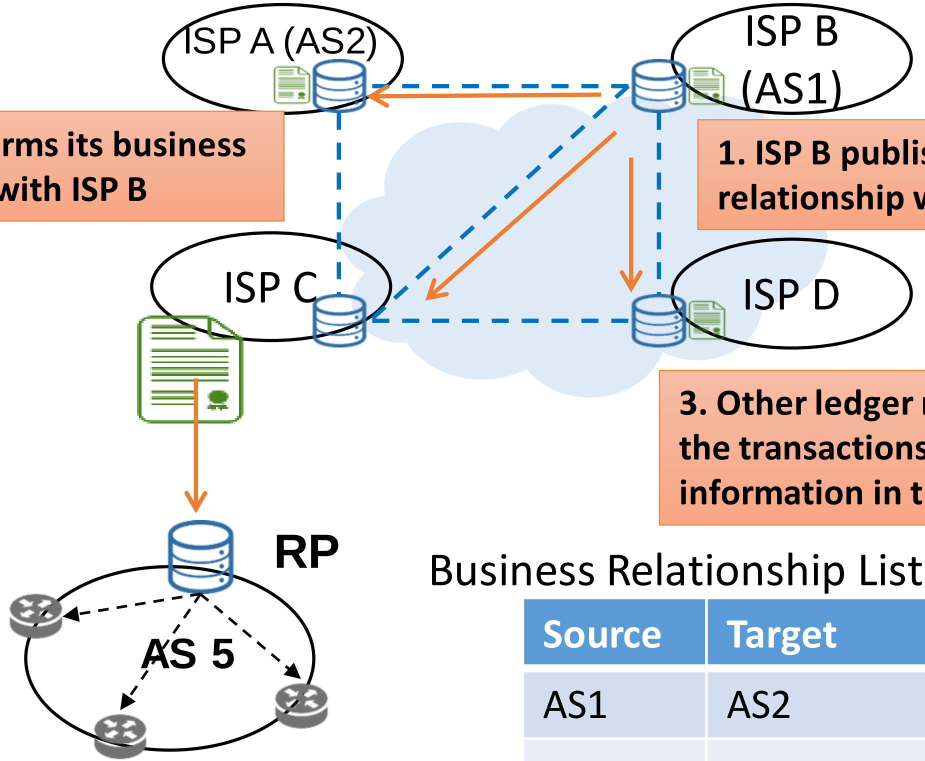
3. Other ledger nodes verify the transactions and record the information in the ledger.

AS Neighbor List:

Source	Target
AS1	AS2
AS2	AS3

DII-based BGP Verification - Route Leak Protection

- Publish of Business Relationship between ASes
  - Each AS registering their business relationship with their neighbors into the ledger.
  - The business relationship with be certified by the pair of ASes.
- Route leak detection based on ASes' business relationship information
  - The Relying Party obtains and analyzes the global neighbor business information from the ledger to generate a route filtering table.
  - The Relying Party synchronizes route filtering table to routers.
  - Router check each hop of AS Path to decide whether the route leak rule is violated or not.



1. ISP B publish its business relationship with ISP A as P2C.

2. ISP A confirms its business relationship with ISP B

3. Other ledger nodes verify the transactions and record the information in the ledger.

4. the RP synchronize business relationship information to routers for route leak detection.

Business Relationship List:

Source	Target	Type
AS1	AS2	P2C
AS2	AS3	P2P

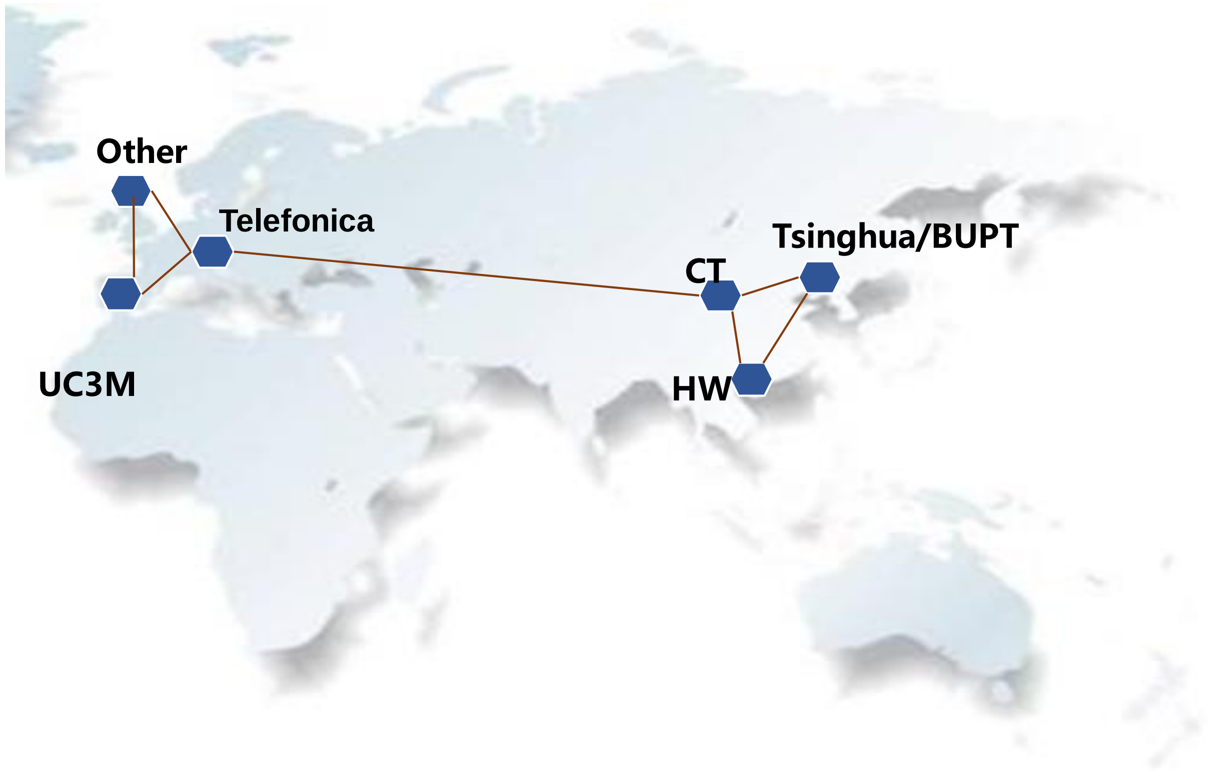
route leak rules:

Relationship for current hop	Relationship for previous hop	Result
P2P	P2C	Leak
P2P	P2P	Leak
C2P	P2C	Leak
C2P	P2P	Leek

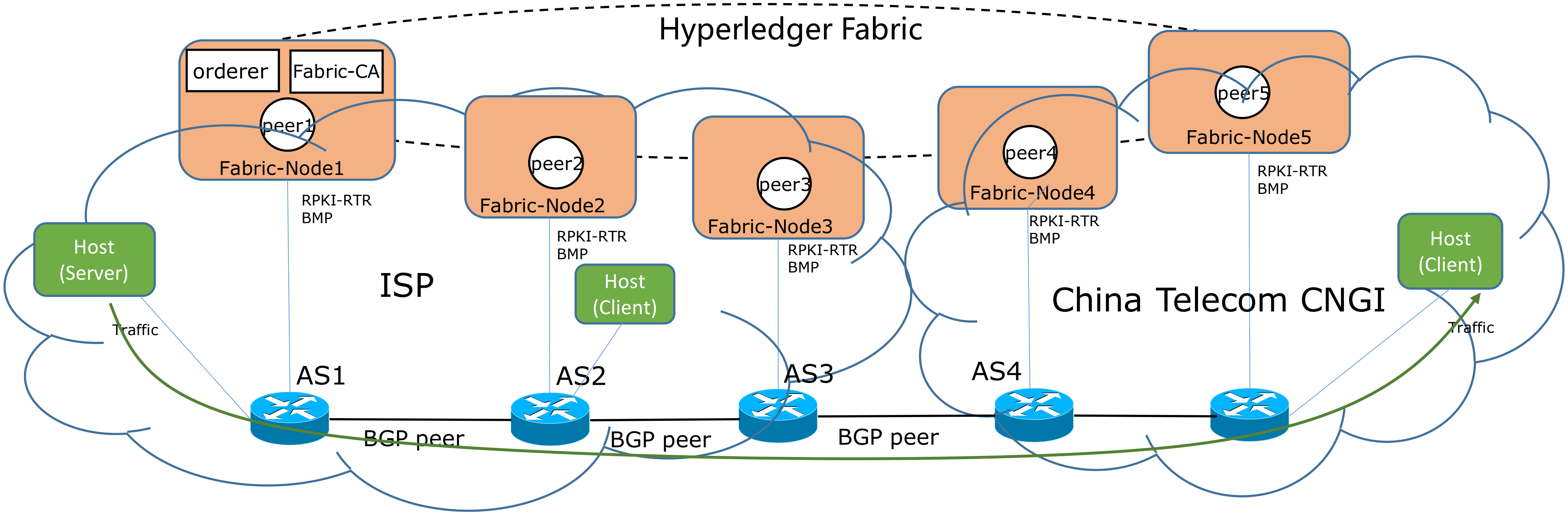
D->C->B->A

DII Testbed Overview

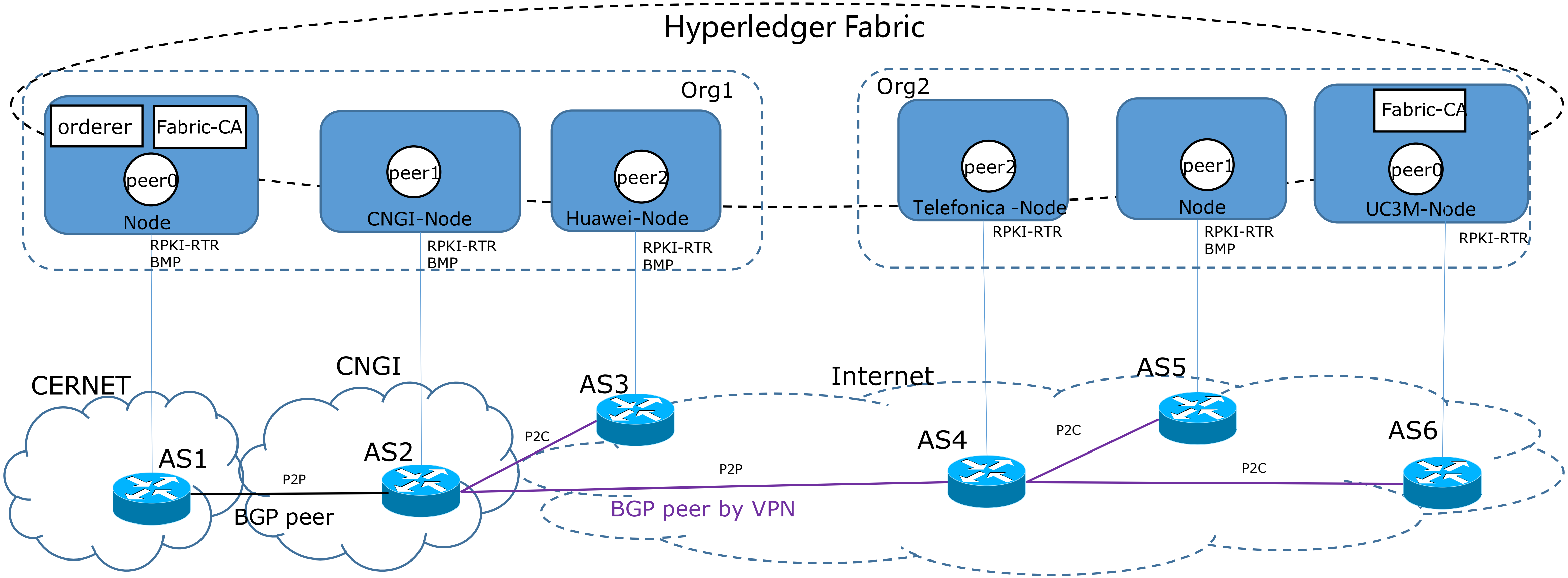
- Main goal
  - Verify DII based BGP security solution such as, ROA, BGP path verification and Route Leak Detection etc.
- The testbed is based on Hyperledger Fabric.
- Initial participants
  - China Telecom (CT)
  - Telefonica
  - Tsinghua
  - BUPT
  - Carlos III University of Madrid (UC3M)
  - Huawei (HW)
  - Others



Testbed-Stage 1 PLAN



Testbed-Stage 2 PLAN



You are welcome to join in this project.

Contact with: yanshen@huawei.com

Thank you!