Security Level:

Decentralized Network Resource Management and Trust Model

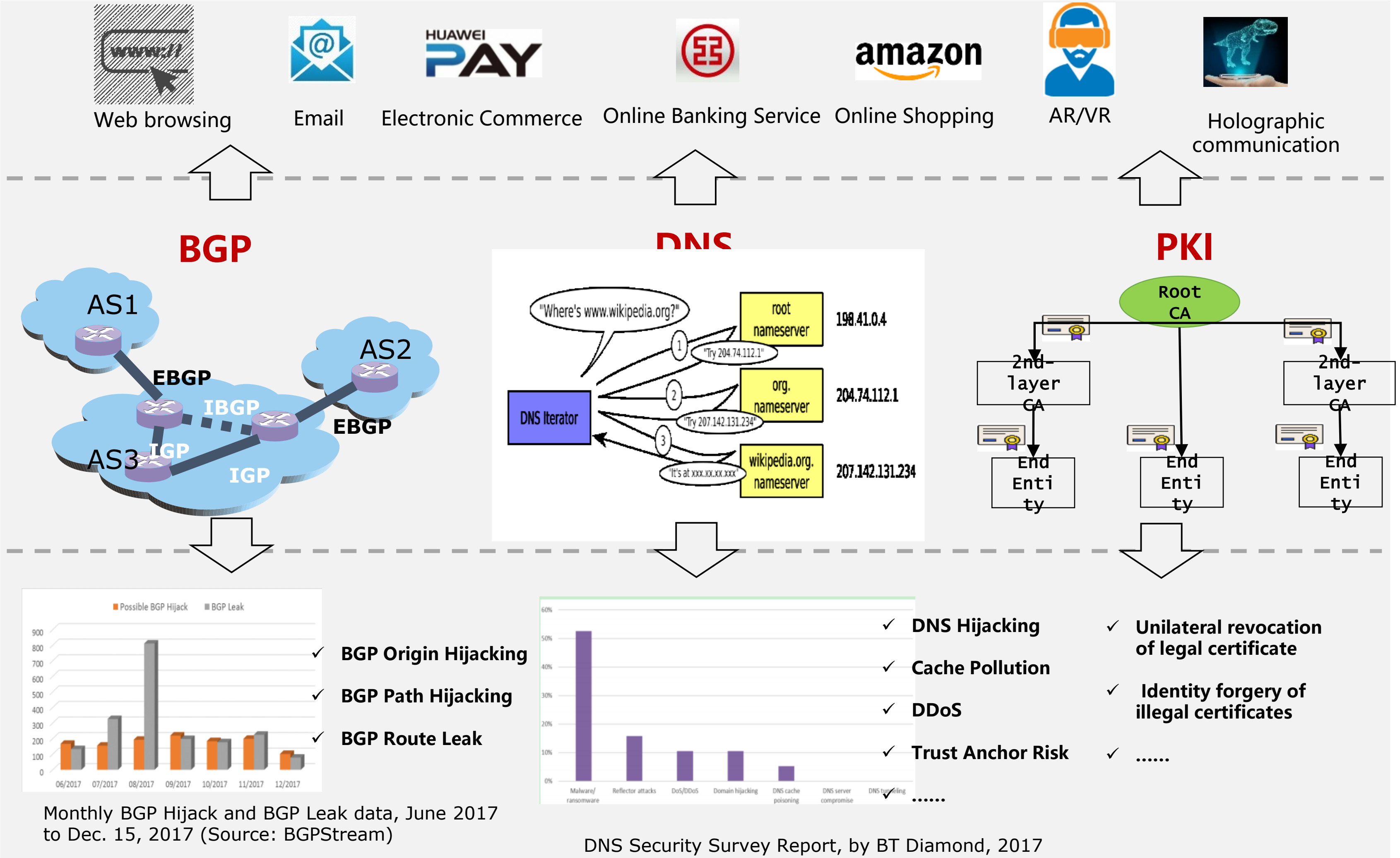
www.huawei.com

Shen Yan yanshen@huawei.com

Are we opening the Age of New Discovery......

Network Services Rely on Trust Infrastructures

- **Infrastructure:**
  - Inter-domain Routing System (BGP)
  - Name Resolution System
  - Public Key Certificate System (PKI).
- **Almost all network services rely on these infrastructure to ensure connectivity, service availability and credibility.**
- **The current infrastructure lacks a solid, secure and credible foundation.**
  - › BGP and DNS were not designed with any security and credibility at the beginning, so naturally lacked security capabilities.
  - › PKI relies on trust anchors for endorsement



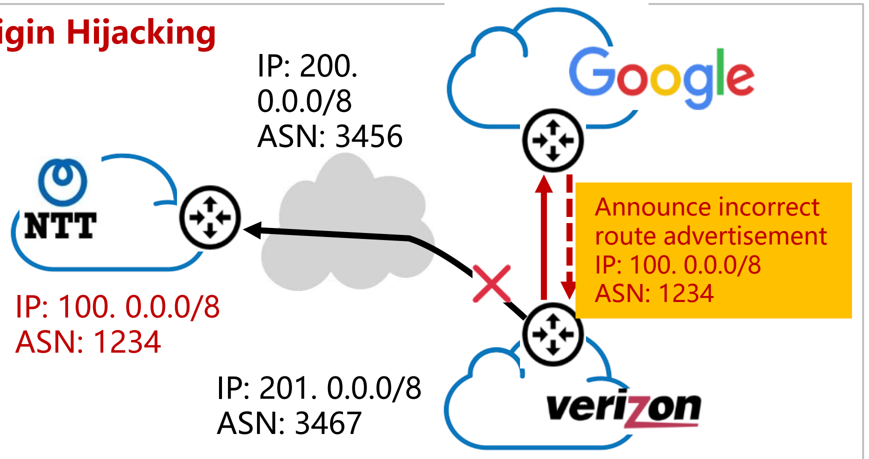
Monthly BGP Hijack and BGP Leak data, June 2017 to Dec. 15, 2017 (Source: BGPStream)

DNS Security Survey Report, by BT Diamond, 2017

BGP Issues

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

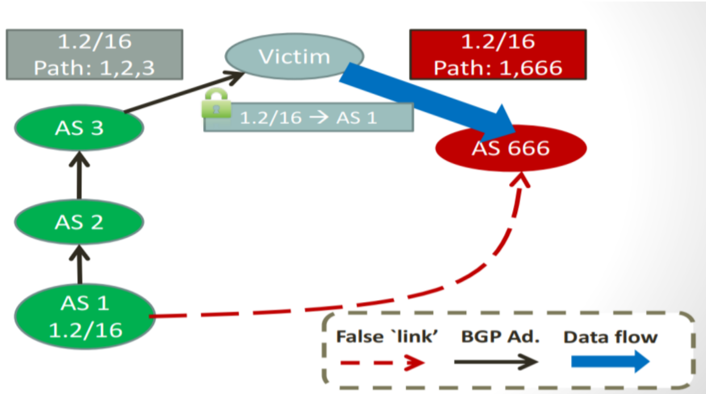
Origin Hijacking



- Drive traffic by announcing address prefixes that are not their own
- Google announced Verizon an IP address segment that was originally attributed to NTT. Verizon sent traffic to NTT to Google, causing Japan to disconnect for 1 hour.

https://www.thedrum.com/news/2017/08/28/google-hijack-made-japan-land-no-internet-more-30-minutes

Path Hijacking



- Using the characteristics of the AS_PATH attribute being easy to modify, announce incorrect path information to hijack traffic.
- AS 666 deliberately announced incorrect information, claiming that it was only one hop away from AS1, causing all traffic destined for AS1 to be hijacked to AS666.

*AS (Autonomous System)

Route Leak

"Google was also the victim of a routing leak. In this case Google' s prefixes were leaked by Hathway, 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. "

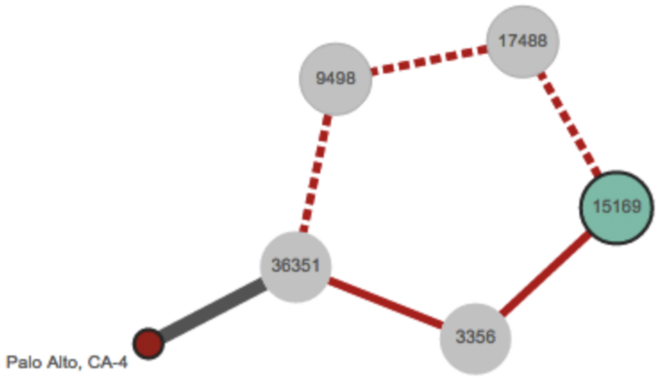


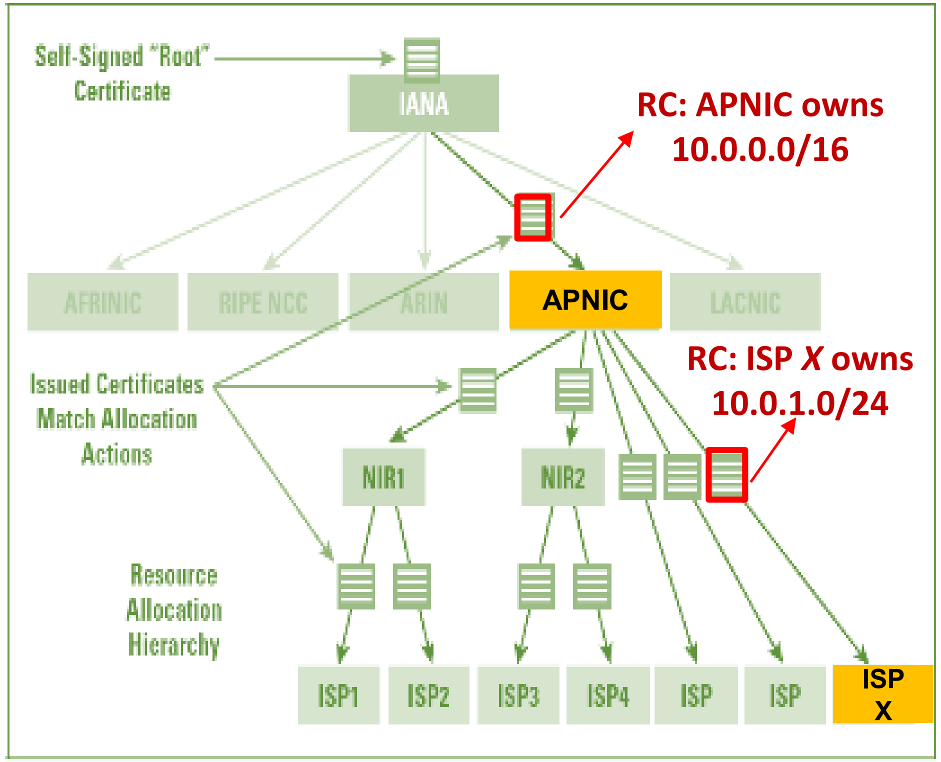
Figure 5: Route leak to Google via Hathway AS17488 that affects Bharti Airtel AS9498.

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

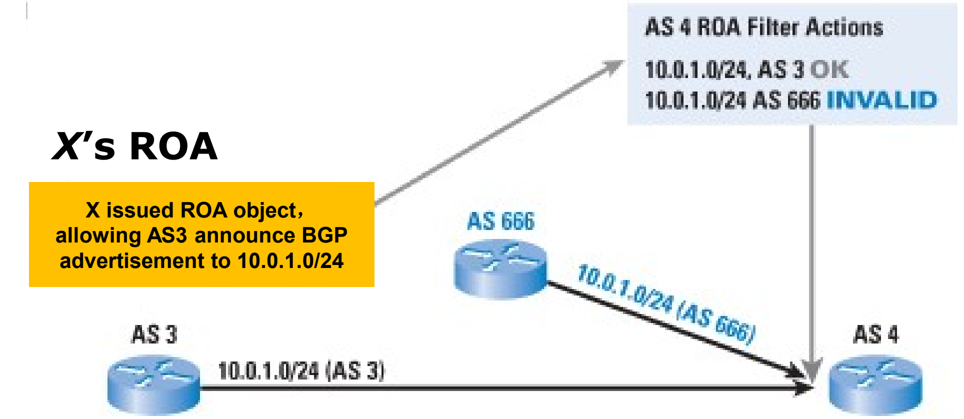
https://www.internetsociety.org/blog/2018/01/14000-incidents-2017-routing-security-year-review/

IETF proposed RPKI and BGPSEC

- **RPKI provides RC certificate-based verification capabilities**
  - Use Resource Certificate to prove address ownership
  - The issuance of RC depends on the allocation process of the address

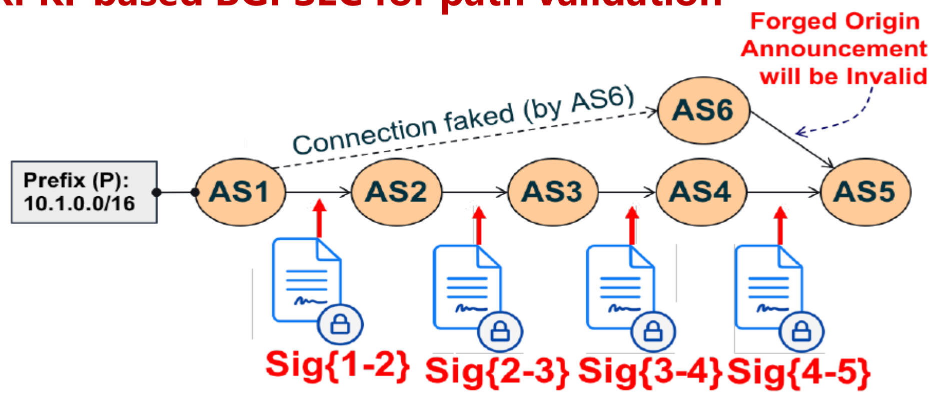


RPKI ROA for BGP source verification



- Verify ROA legality by RC certificate chain
- Verify the legality of BGP announcements by ROA

RPKI-based BGPSEC for path validation

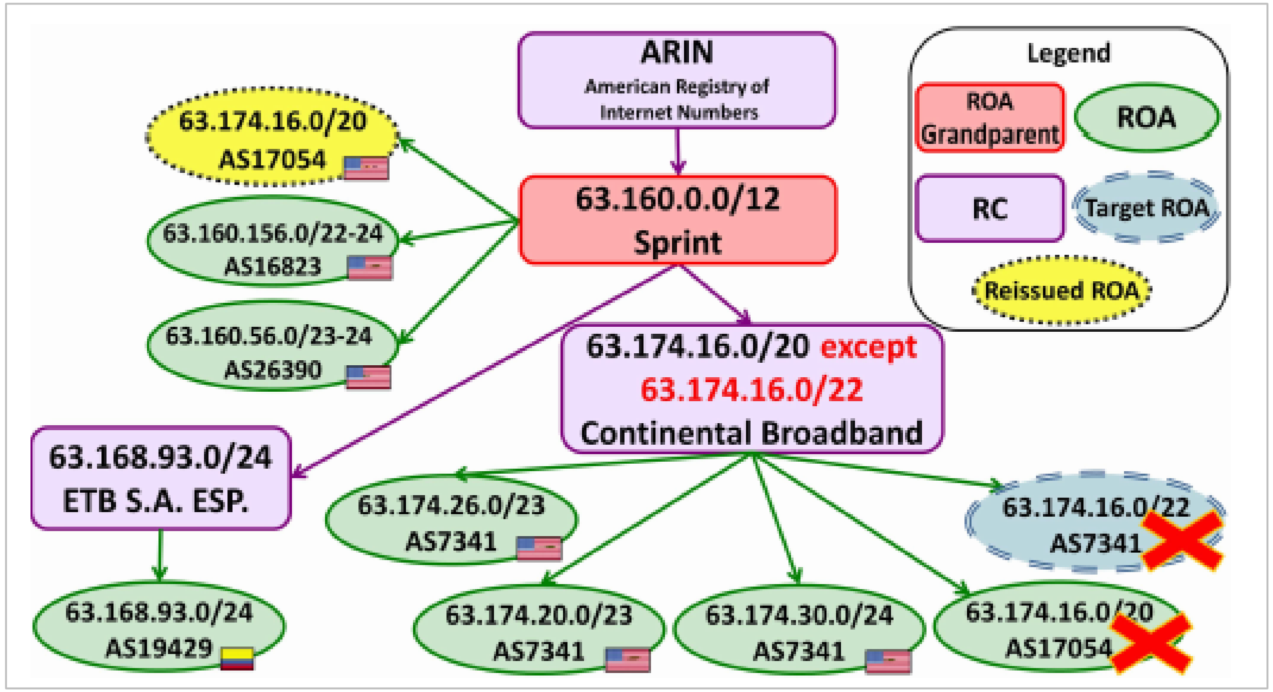


- Verify the legality of the signed public key by the RC certificate chain
- Sign the path information AS-by-AS

BUT…RPKI does not completely solve the problems and introduce centralization issues

- **Depending on the centralized trust model, once the Authority node is misconfigured or attacked, it will cause security issues**
  - 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.
  - ROA (Route Origin Authorization) coverage: The superior node issues an ROA that has been distributed to the subordinate institution prefix to attract part of the traffic.

- **Path validation requires hop-by-hop signature decryption which affects route convergence speed.**



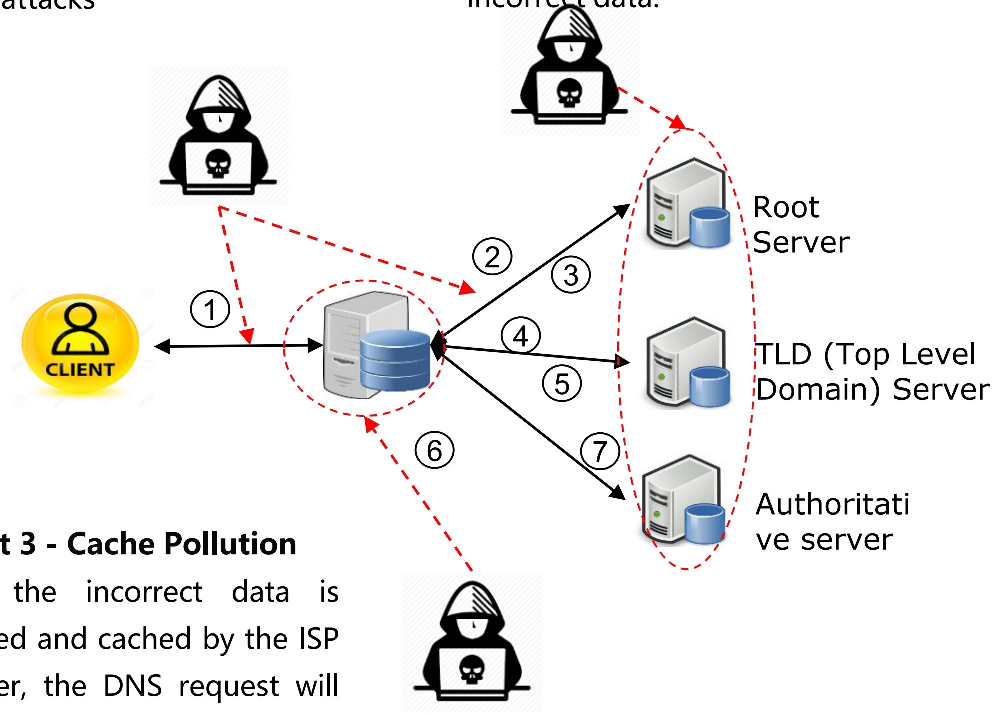
Heilman E, Cooper D, Reyzin L, et al. From the Consent of the Routed: Improving the Transparency of the RPKI[C]//ACM SIGCOMM Computer Communication Review. ACM, 2014, 44(4): 51-62.

Real Case Scenario

- In Dec,2013, A ROA (79.139.96.0/24, AS 51813) was accidentally deleted, resulting in a certain part of the network prefix in Russia became unreachable.
- In Jan,2014, the ROA of one of Nigeria' s network was “invalid” , because its parent RC was overwritten.
- In Dec,2013, ARIN mistakenly issued a ROA, allowing AS6128 to announce the prefix 173.251.0.0/17~24, causing the legal declaration of the prefix to become invalid.

DNSSEC also cannot completely solve the security threats and centralization problems of DNS

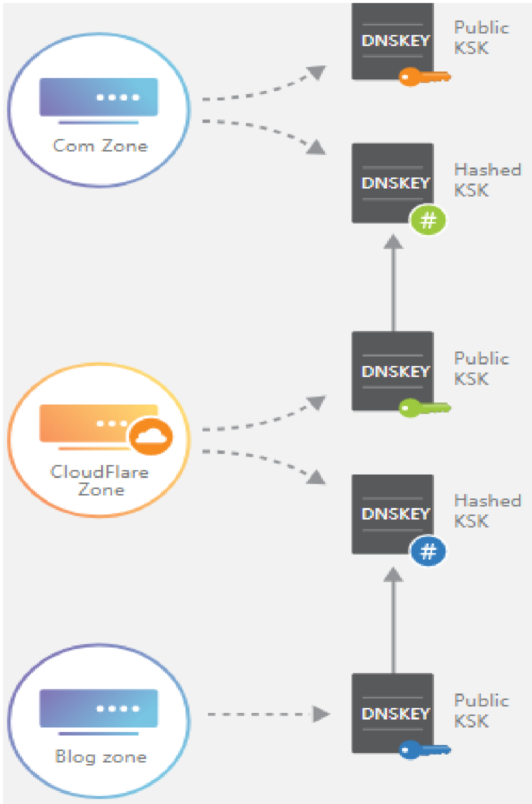
- **Threat 1 - DNS Hijacking**
  - The data of any link on the DNS resolution path may be subject to MITM attacks
- **Treat 2 - Chained threat**
  - Any device on the DNS resolution tree may be attacked and return incorrect data.



- **Threat 3 - Cache Pollution**
  - Once the incorrect data is received and cached by the ISP resolver, the DNS request will receive the incorrect data for a long time.

DNSSEC only solve DNS hijacking problems

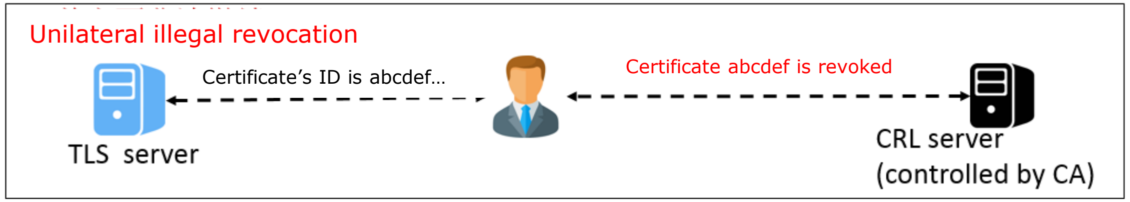
- Depends on signature information to ensure data integrity
- Based on the basic principle of PKI, it verify the DNSKEY of the subzone rely on the DNSKEY of the parent zone.



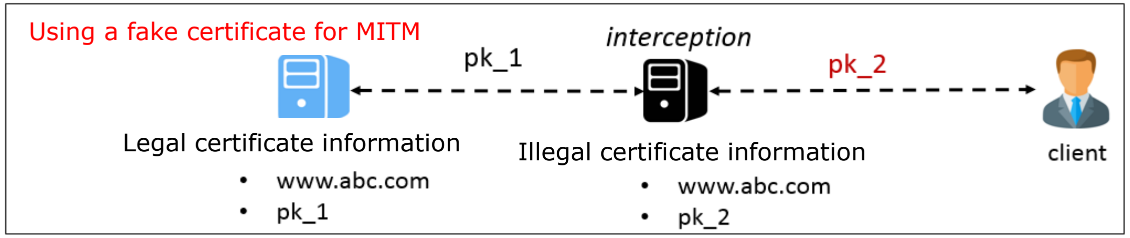
- **Centralization still exists**
  - Unilaterally delete the sub-domain DS records in its zone file, so that the subzone's KEY is not trusted.
  - Unilateral fake subzone’s DNSKEY and signed it.
- **Centralization problems still cause cache pollution**

PKI also faces security vulnerability and trust chain failure of central nodes

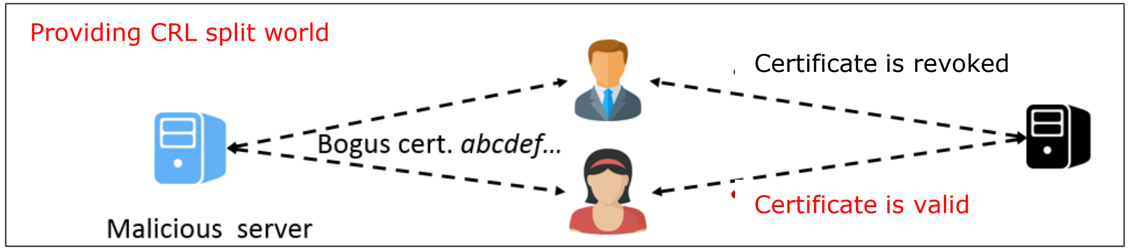
- **All the control of the certificate are owned by the CA, so if the CA is attacked, it will bring the following security threats:**
  - Illegal revocation



  - Issuing an illegal identity



  - Issue or revoke CRL



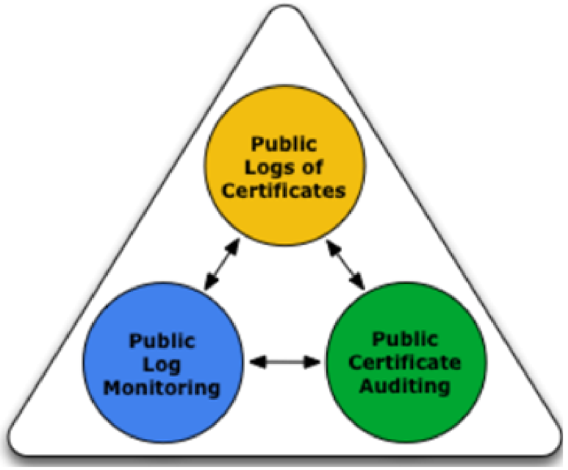
* CRL: Certificate Revocation List

Real Case Scenario

- In Jul, 2011, the Netherlands noted that 8 servers of CA DigiNotar were hacked. At least 531 false certificates were released including Yahoo!, Mozilla, WordPress, The Tor Project, etc.
- In Jul, 2011, Google service suffered from the above-mentioned illegal certificate attack, affecting the Dutch financial, technology, manufacturing and other industries.

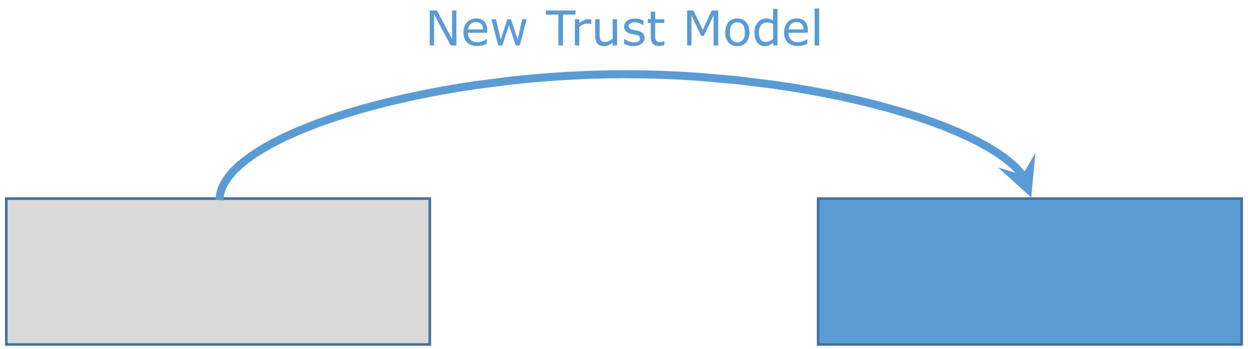
Certificate Transparency

- Use the public certificate Log t a certificate signing example
- Only be detected afterwards, p evidence of responsibility
- Unable to fundamentally solve centralization problem of PKI



Privacy Protect and Data Sharing

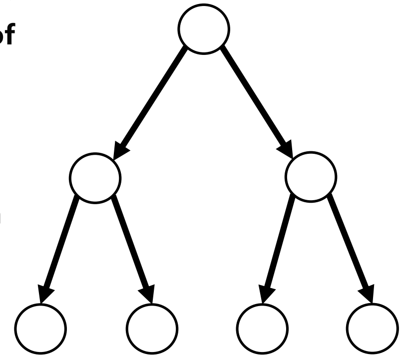
- It is very IMPORTANT now and future
- However, the current trust model can hardly work
- A novel trust model may support more upper layer applications



The root cause is the centralized trust model.

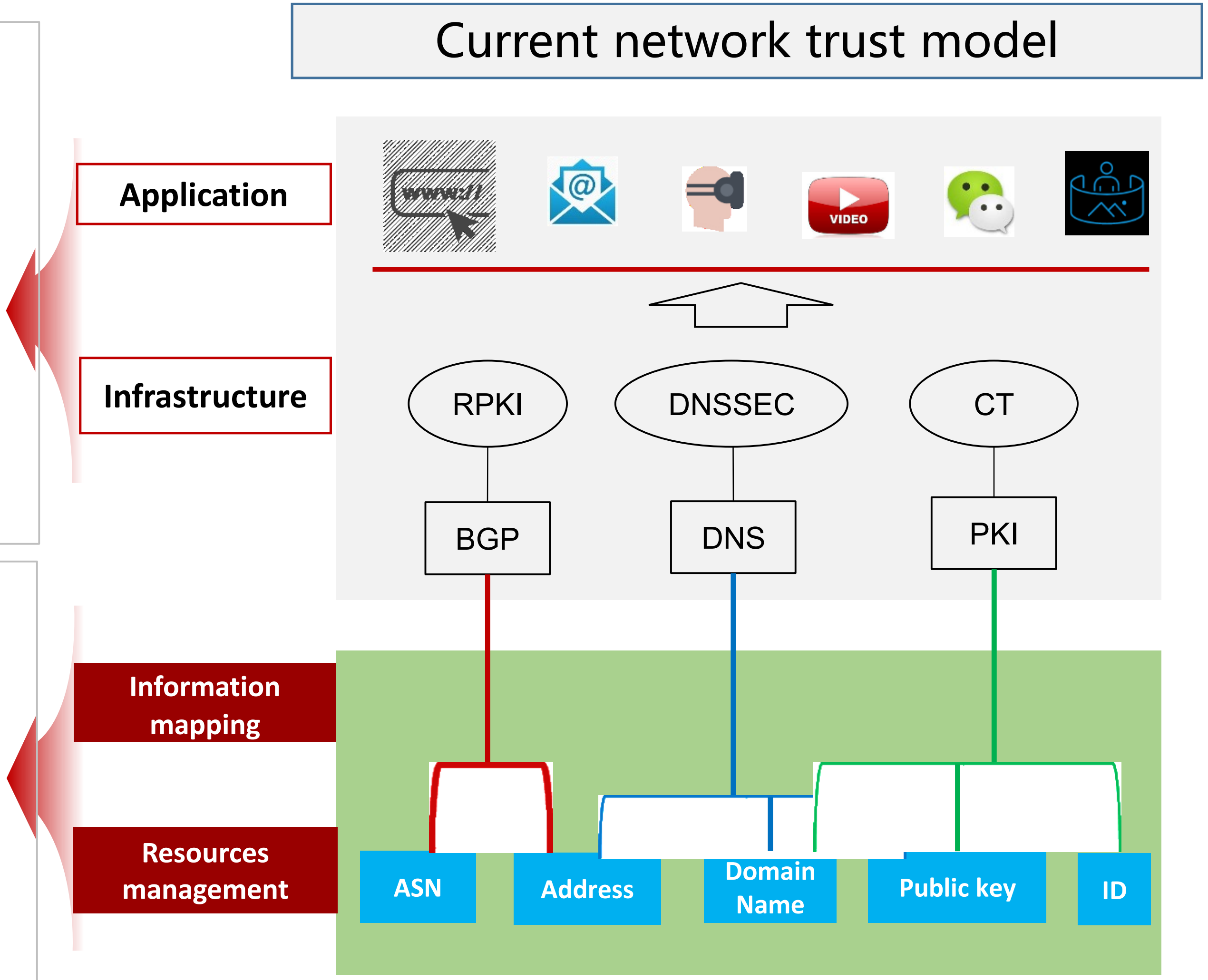
Where is the current problem?

- Reason 1: BGPSEC, DNS (SEC), and PKI all adopt a centralized trust model. There is a single point of security and credibility in the mechanism. Without changing the architecture, it is difficult to solve.
- Reason 2: At a deeper level, the current solution is a patched solution, which does not fundamentally examine where the Internet security credibility is.



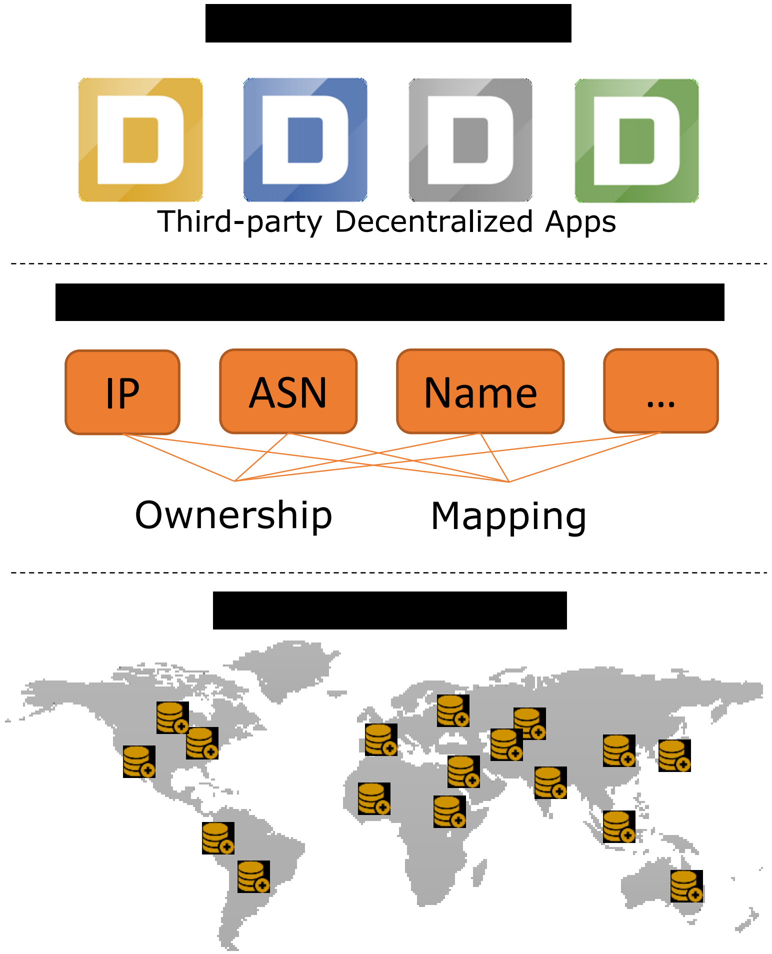
Where is the security and trustworthy foundation?

- **Decentralization technology to solve problems naturally**
  - Additional benefits: increased reliability, increased security, reduced latency...
- **Not depending on a single trust anchor is the basis of network security and trustworthiness.**
  - What is needed for the Upper Layer: Mapping between resource information
  - What is the dependency of the mapping: the mapping information authorized by the resource owner is trusted



Consider to introduce decentralized trust model for resource management and privacy protect

The overview of DNI (Decentralized Network Infrastructure)



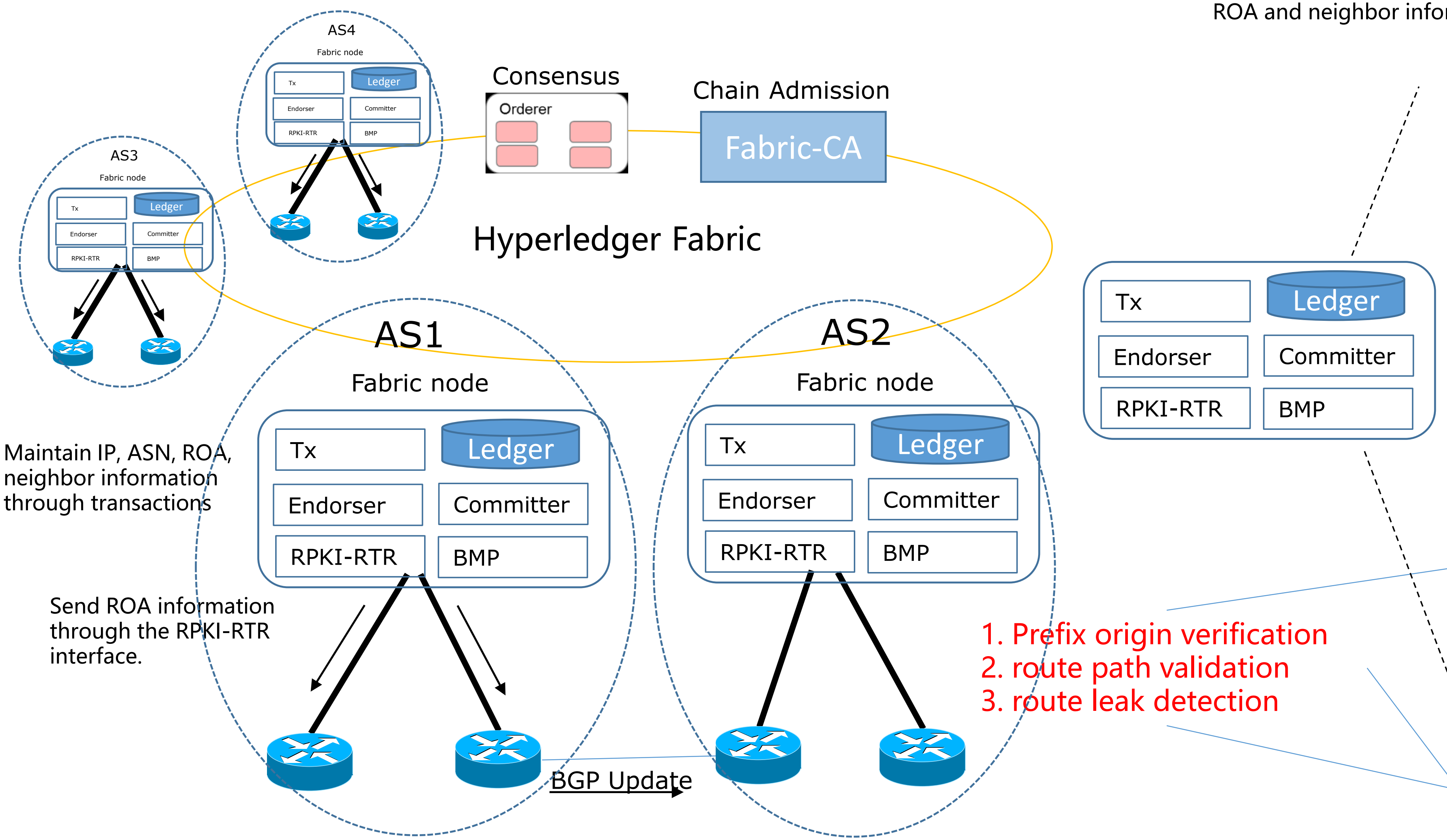
Third-party decentralized APP platform
- Decentralized PKI platform
- Pay remote DDoS defense services on demand
- Cross-domain end-to-end QoS capabilities

Trusted name space ownership and mapping system
- IP and ASN: Trusted Routing System
- IP and domain name: Trusted DNS resolution system
- Other: trusted host ID, trusted content, trusted IoT ID, etc.

Decentralized network infrastructure based on blockchain
- Decentralized (p2p) network architecture and trusted model
- Consensus mechanism
- Smart contract for computing models
- Monetization trading platform for Internet services

A consortium chain-based DNI Verification System

Blockchain stores Ownership,
ROA and neighbor information



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)

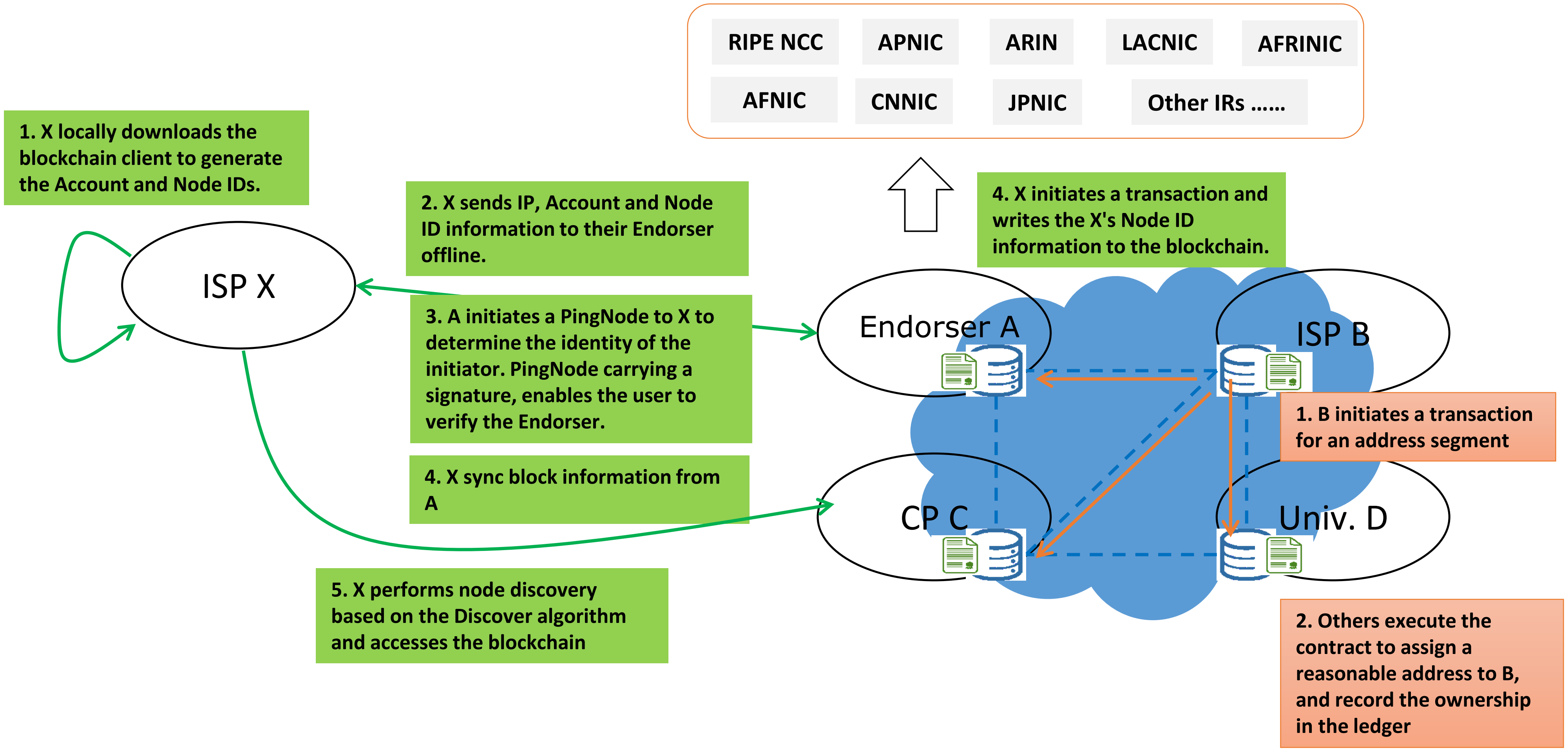
Source	Target	Type
AS1	AS2	P2C
AS2	AS3	P2P

World-state

- RPKI-RTR: RPKI to Router Protocol
- BMP: BGP Monitoring Protocol

IP address management and access control

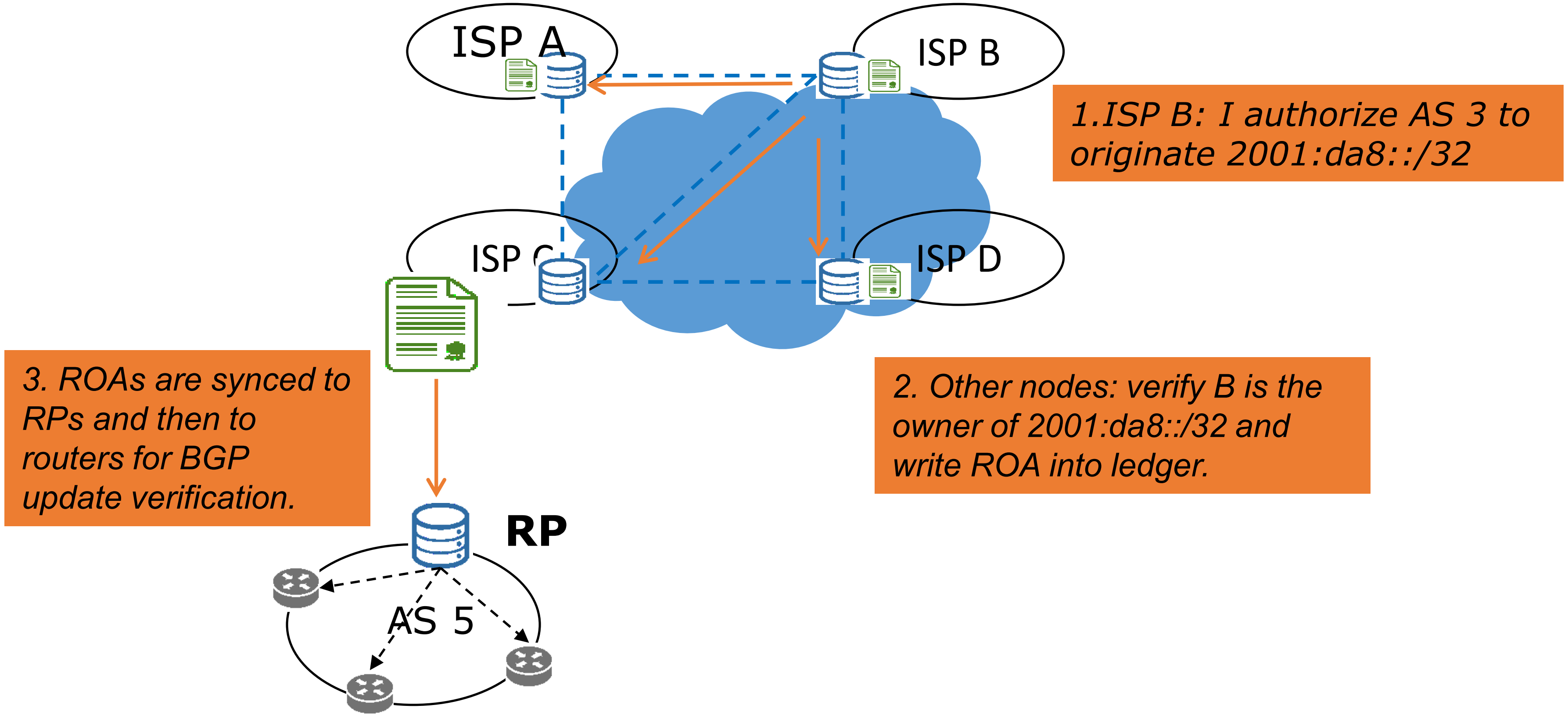
- **Simultaneous implementation of endorsement access control and dynamic node management**
- **The blockchain application layer is reversed from the underlying network layer, allowing the network layer to implement a dynamic node admission control strategy based on the consensus result of the application layer.**

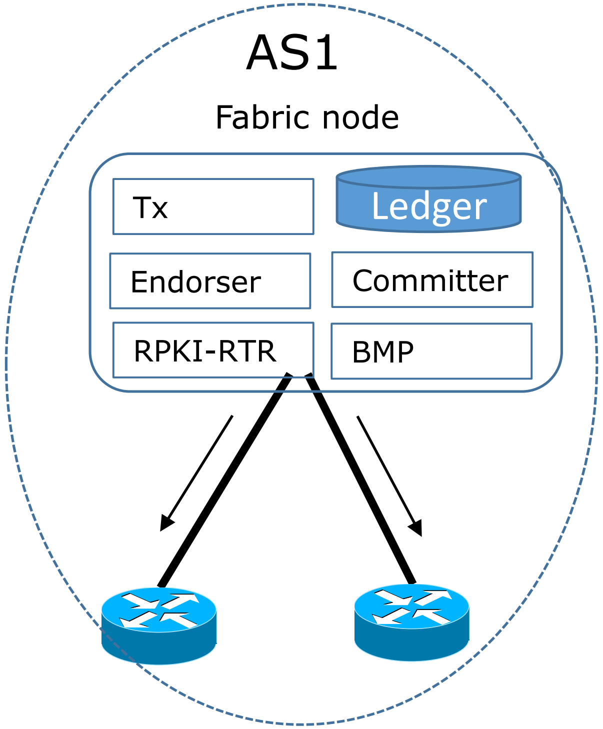


HUAWEI

DNI-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.

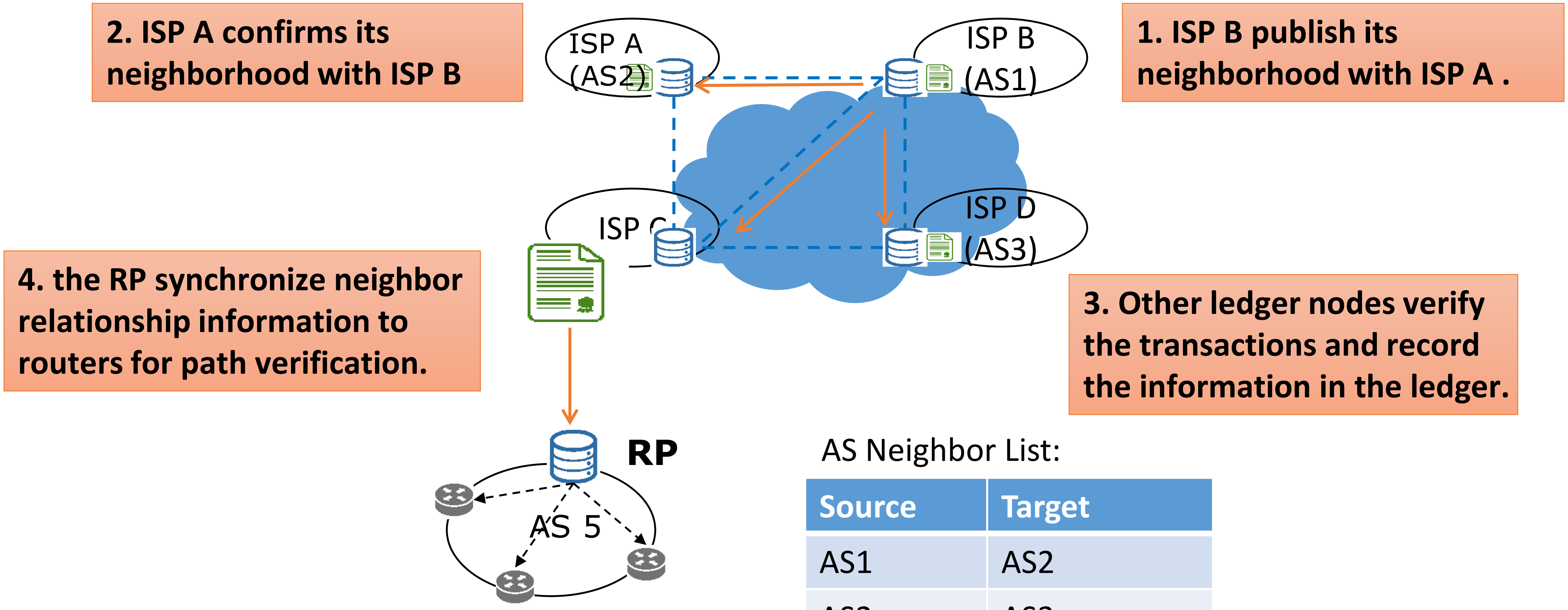




HUAWEI

DNI-based BGP Verification - AS Path Verification

1. Each AS publishes its neighbor information in the ledger for AS path verification in BGP advertisement.
2. The Relaying Party (RP) get neighbor information from the ledger and synchronize the information to routers.



AS Neighbor List:

Source	Target
AS1	AS2
AS2	AS3

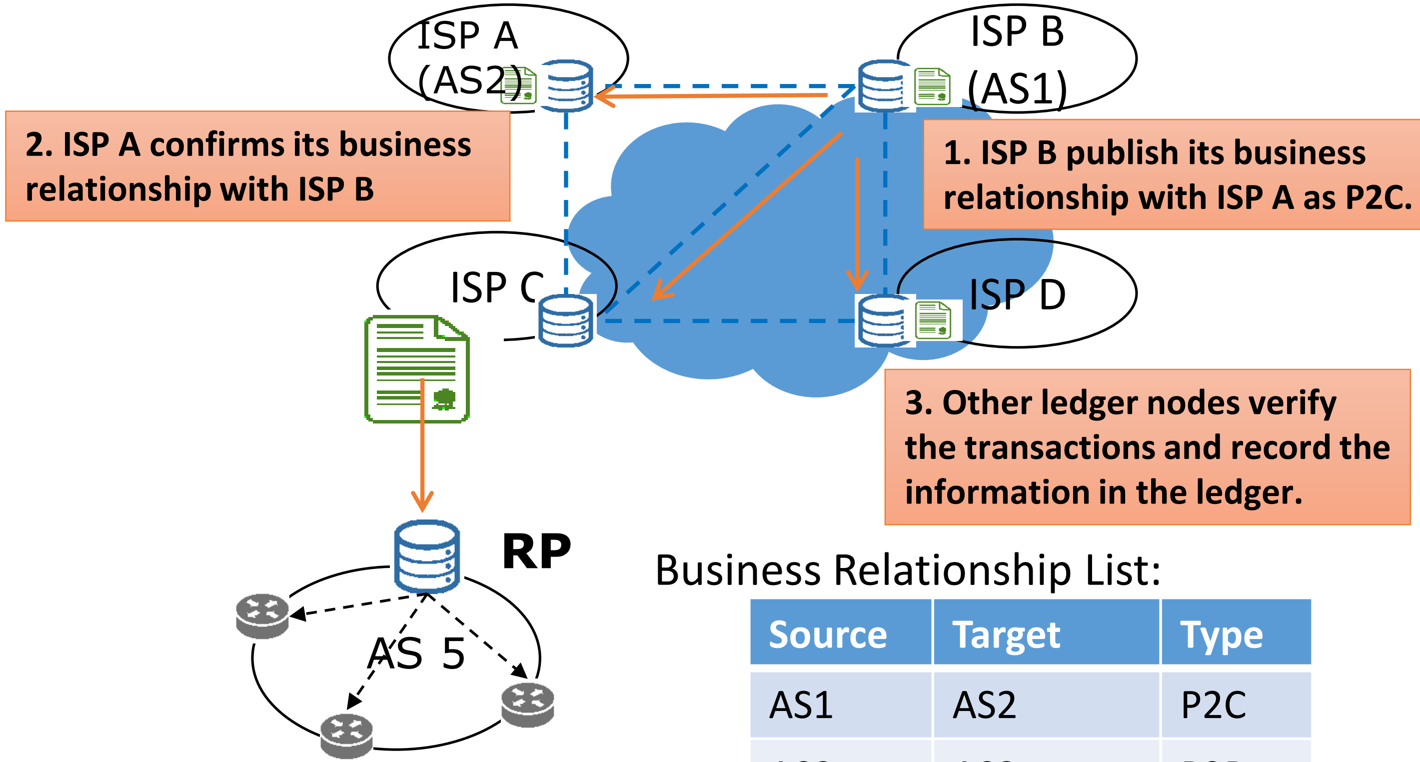
DNI-based BGP Verification - Route Leak Protection

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.



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

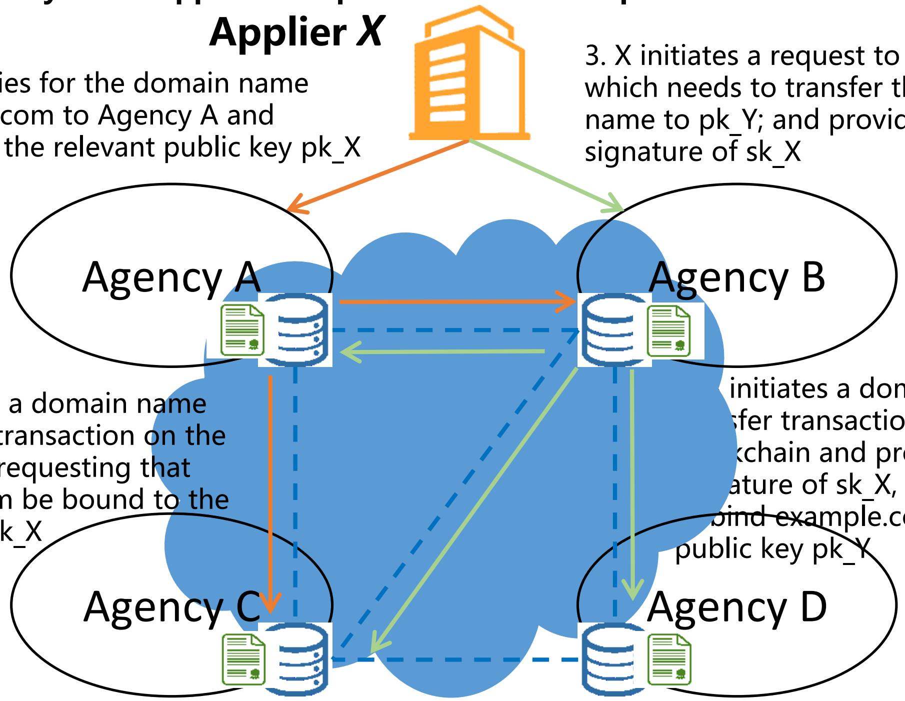
D->C->B->A

HUAWEI

Domain name management solution

Decentralized domain name management

- **The domain name is bound to the public key. As long as the private key is signed, anyone can operate the related domain name.**
- **Agency needs applicant to provide transaction proof information**



0. X applies for the domain name example.com to Agency A and provides the relevant public key pk_X

3. X initiates a request to Agency B, which needs to transfer the domain name to pk_Y; and provides the signature of sk_X

1. A initiates a domain name application transaction on the blockchain, requesting that example.com be bound to the public key pk_X

initiates a domain name ...sfer transaction on the ...kchain and provides the ...ature of sk_X, requesting ...bind example.com to the public key pk_Y

2. Others: Verify that the transaction of A is legal; if it is legal, write the information to the blockchain, and the owner public key of the domain name example.com is pk_X

5. Others: Verify that the signature in the transaction initiated by B is legal; if it is legal, the owner of the record example.com is changed to pk_Y

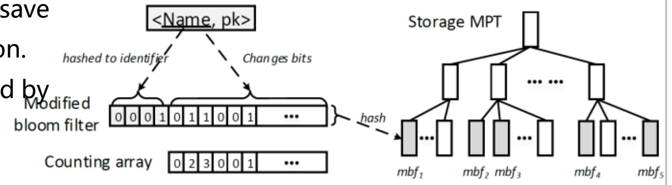
Lightweight data verification mechanism

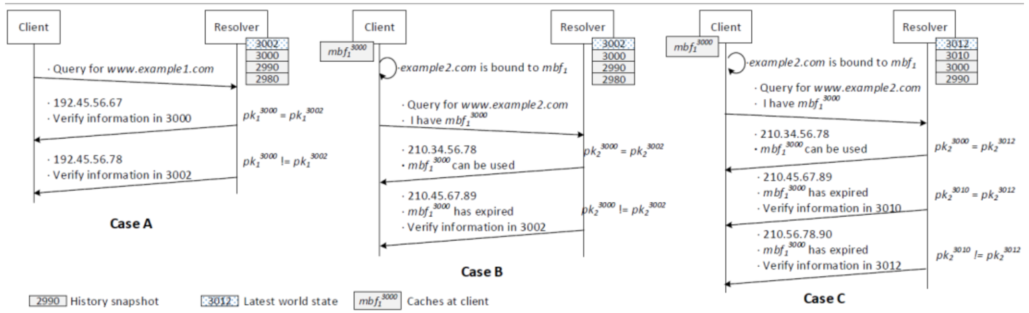
- **In the current DNS system, the client does not have any ability to verify the data authenticity, and can only trust the resolution result unconditionally.**
- **The Blockchain provides the SPV (Simplified Payment Verification) mode, but it needs to obtain the latest blockchain information to verify each time. The single overhead is at the KB level.**
- **This mechanism reduces the single verification overhead to the Bytes level.**
- **A blockchain-based DNS information verification and caching mechanism security enhancement**

› Add a bloom filter to the contract to save the existence of the owner information.

› Verification information can be reused by the cache

› A bloom filter can be used to verify multiple domain ownership information

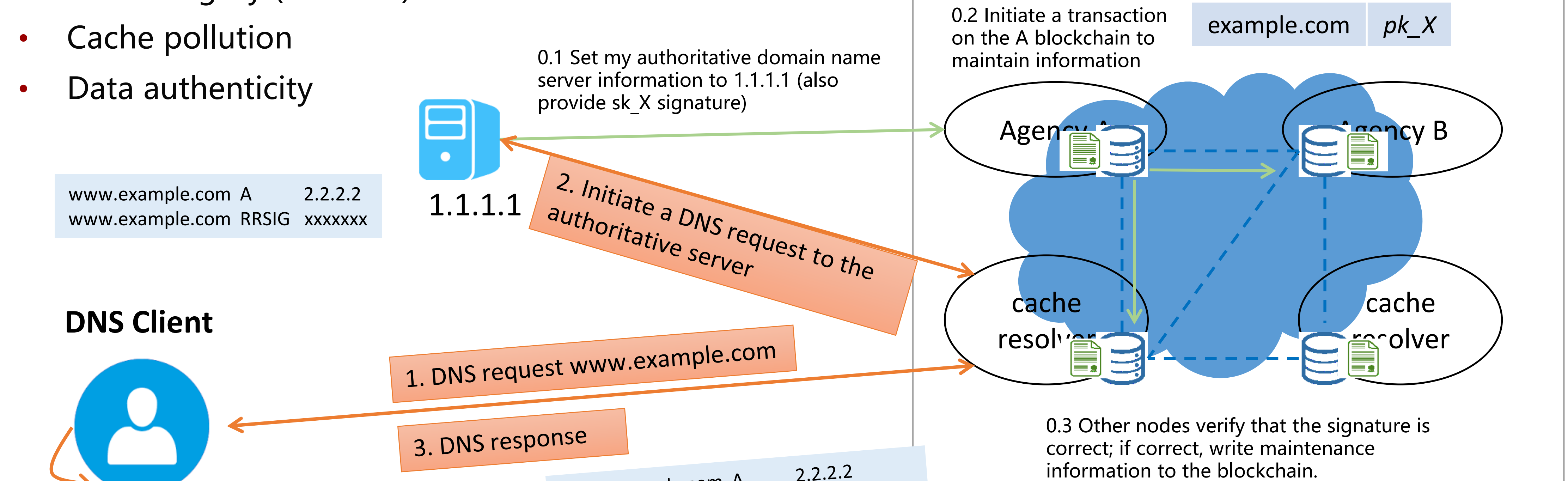




Secure verifiable domain name resolution

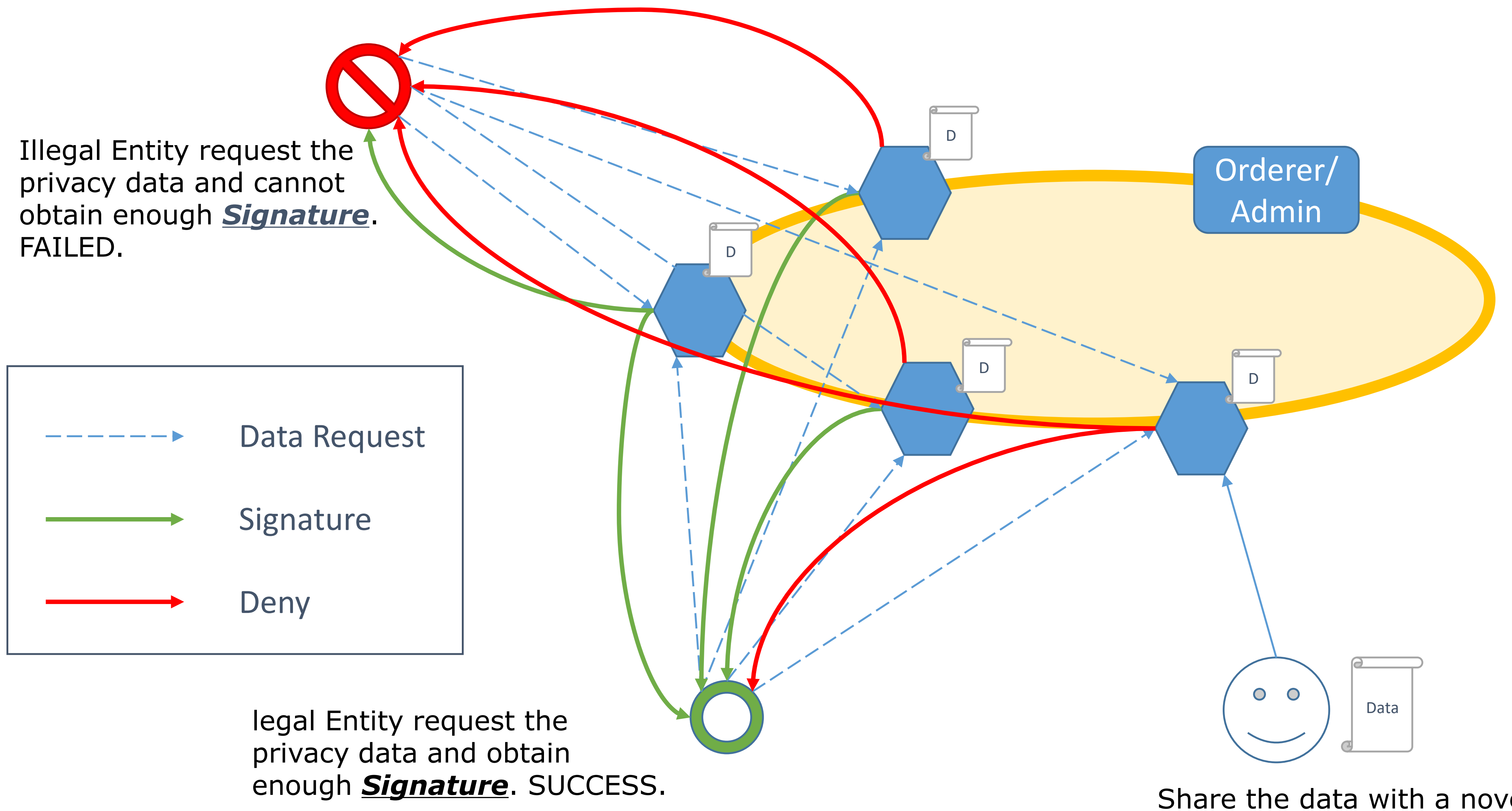
- **Enhance the security capabilities of the DNS protocol instead of DNSSEC**
  - Data integrity (DNSSEC)
  - Cache pollution
  - Data authenticity

- **The blockchain only stores the ownership information and the authoritative server information because the update frequency of ownership is very low.**



Domain name	Owner	Authoritative server
example.com	*pk_X*	1.1.1.1

Improve RPKI and Privacy Protect

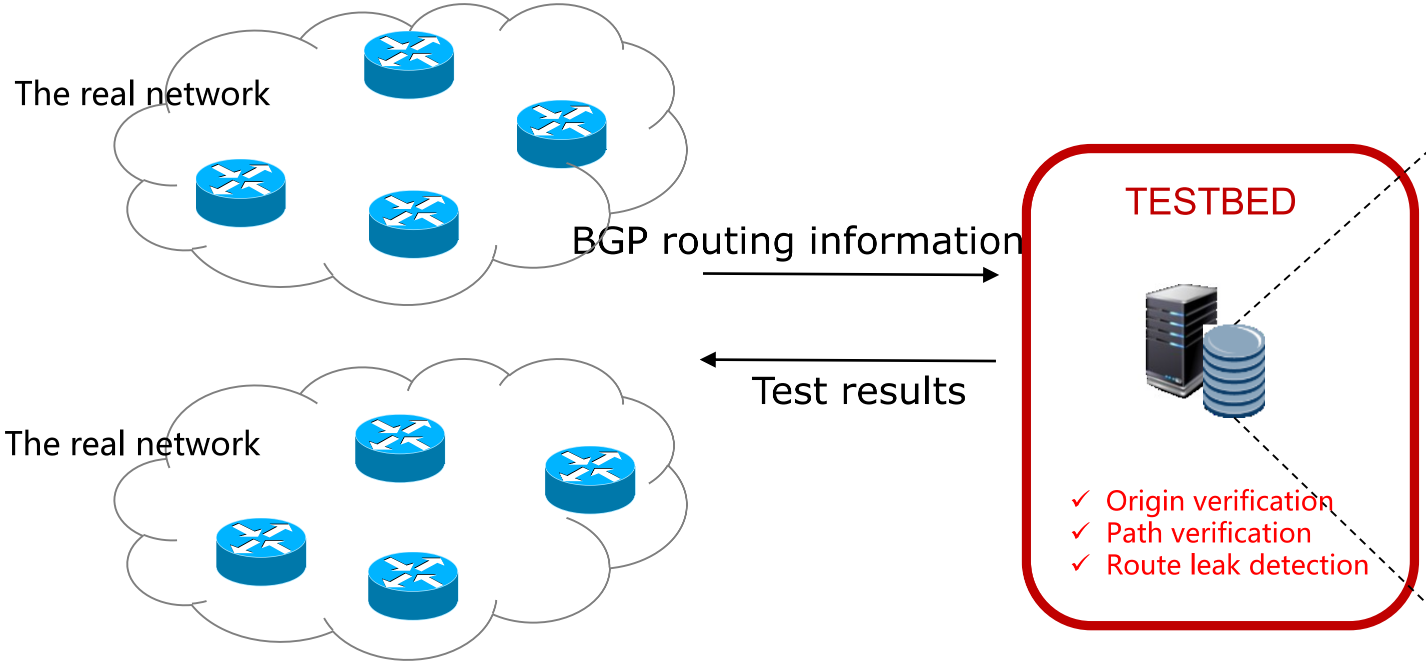


Share the data with a novel trust model.

HUAWEI

Testbed of BGP security, address management and DNS security based on blockchain

- Solve the single point problem of RPKI.
- Provides a unified solution to support origin validation, path validation, and route leak detection.



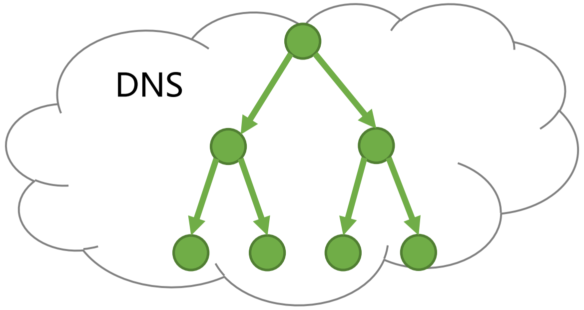
Obtain and maintain through blockchain

Source validation information

IP	Maxlength	ASN
1.1.1.1/32	32	100

Path validation and route leak detection information

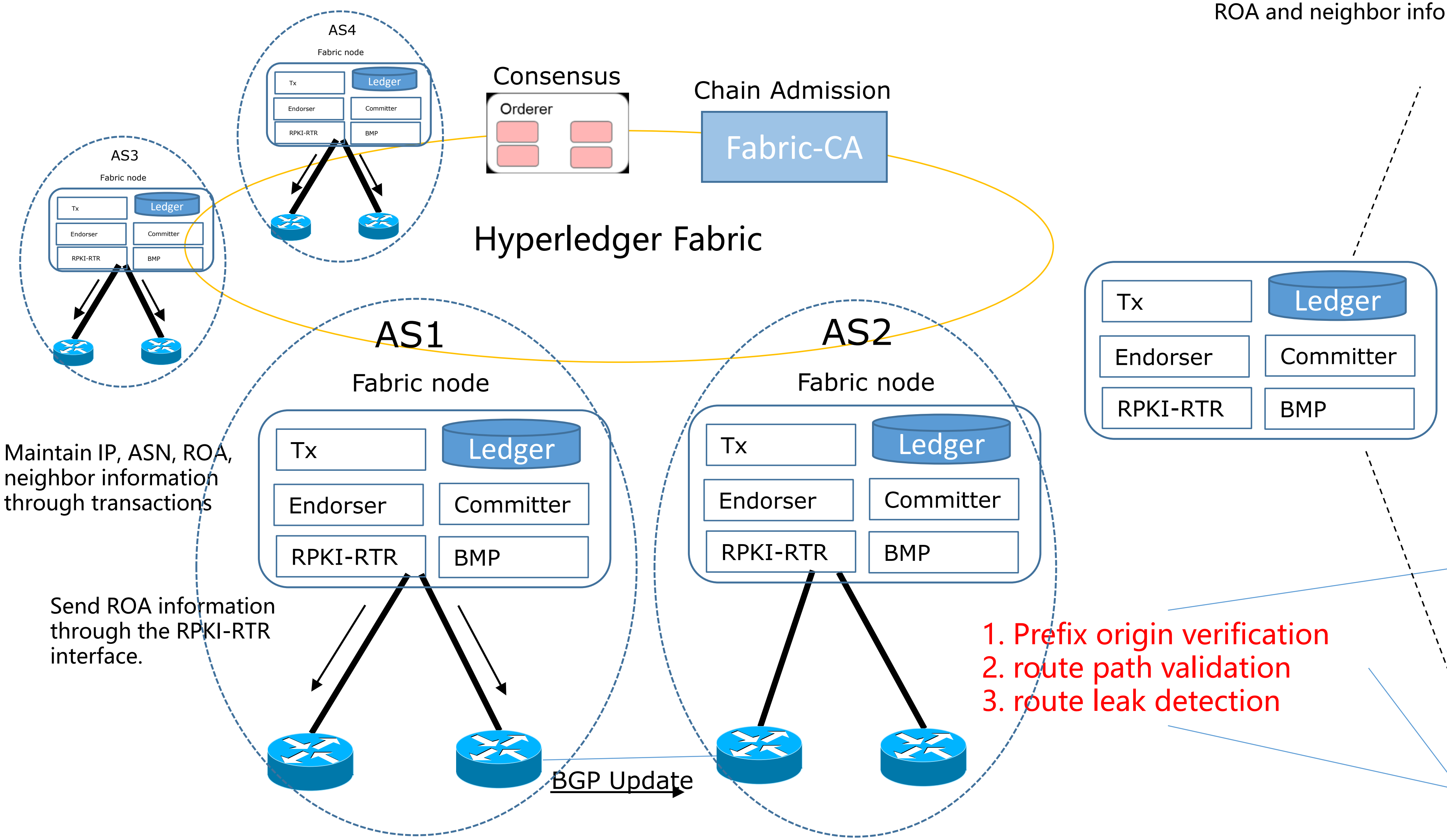
Source	Target	NeighborInfo
AS1	AS2	P2C
AS2	AS3	P2P



1. Incremental deployment
   - Provide a unified deployment plan.
2. Reference Mode
   - The routing information is obtained from the real network, and the detection result is returned to the network for reference.
3. Admin Mode
   - The router can be controlled by the DNI system.

DNI System Overview

Blockchain stores Ownership,
ROA and neighbor information



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

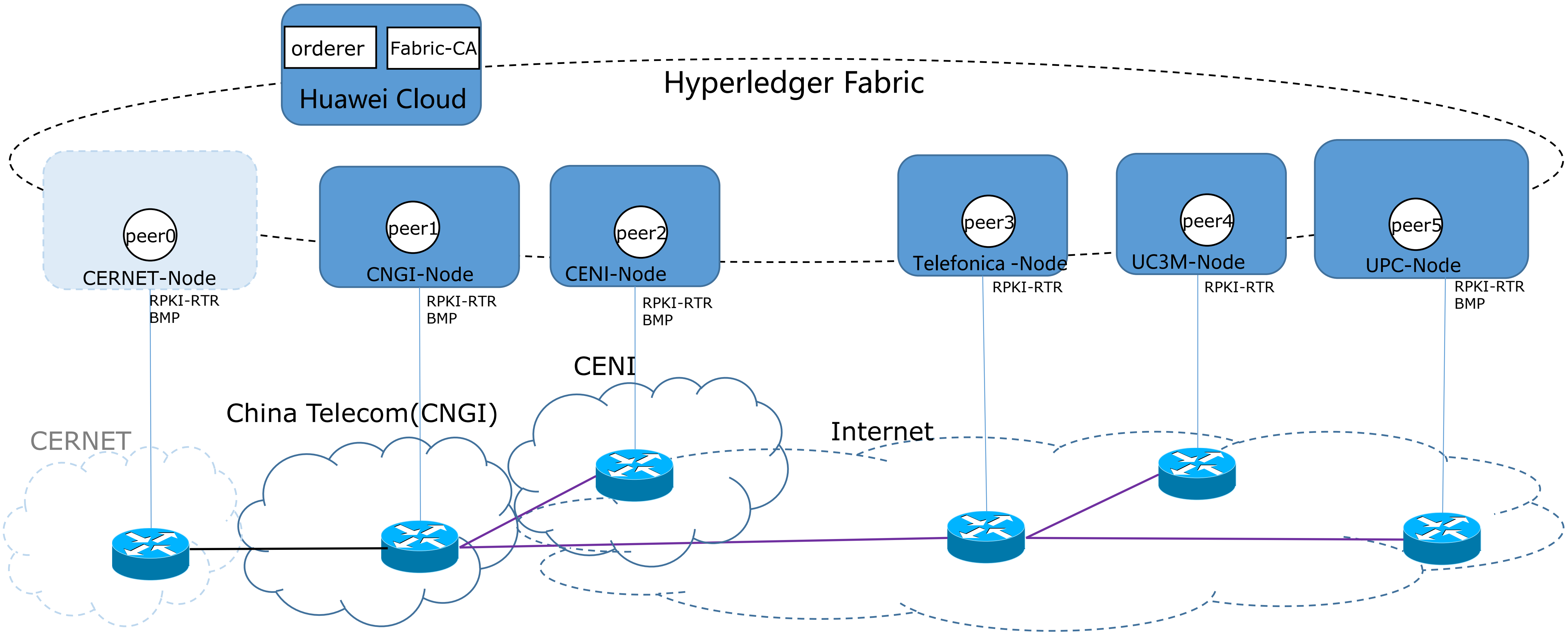
ASNeighbor(ASN->ASN)

Source	Target	Type
AS1	AS2	P2C
AS2	AS3	P2P

World-state

- RPKI-RTR: RPKI to Router Protocol
- BMP: BGP Monitoring Protocol

DNI Testbed based on Consortium Chain



- **China Telecom, Telefonica, CENI, CERNET2, UC3M, UPC, BUPT, Tsinghua, …**

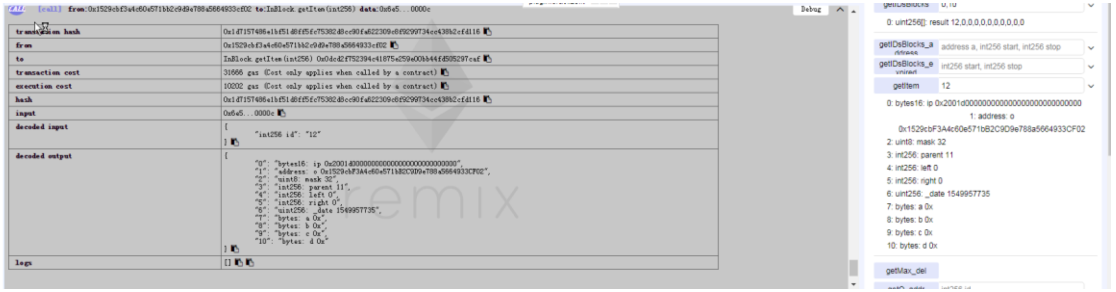
Current Testbed operation

- Based on ethereum / Hyperledger Fabric
- Smart contract development:

by Remix GUI

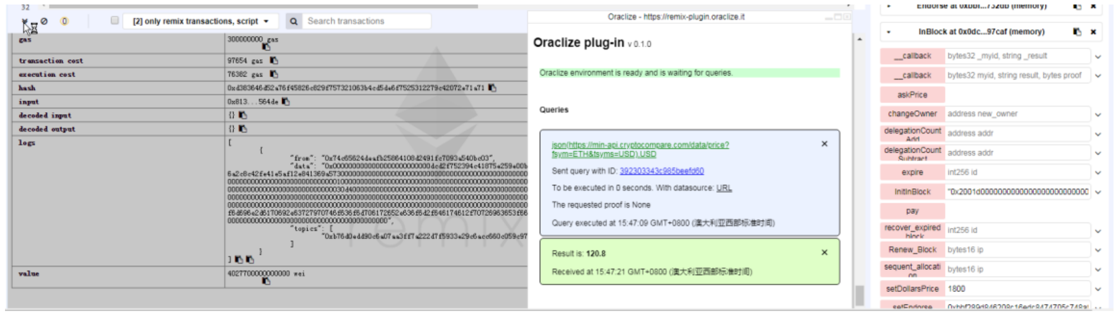
Endorsement: RIR endorses the ISP User.

IP Allocation: allocate IP to ISP by sparse_allocation



ROA: ISP announces the ROA

Askprice: get the realtime ether price



- UI & Relying party work is ongoing.

HUAWEI

Standardized work

- ITU-T SG13 Q2 WI， Framework and Requirements of Decentralized Trustworthy Network Infrastructure， https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=15083
- ITU-T DLT FG use case, https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx
- IETF dinrg Presentation
  - https://datatracker.ietf.org/doc/slides-102-dinrg-decentralized-internet-resource-trust-infrastructure-bingyang-liu/
  - https://datatracker.ietf.org/meeting/105/materials/slides-105-dinrg-a-blockchainbased-testbed-for-bgp-verification-00
- ETSI PDL ISG， https://portal.etsi.org/TB-SiteMap/PDL/List-of-PDL-Members-and-Participants

Summary

- Decentralized Trust Model can improve the network trust scheme
  - Protect the whole system from single trust anchor failure
  - Improve the privacy and security
  - Co-work with the current trust model
- The BlockChain is not the key but the decentralized idea
- CALL for Joint research and deployment

THANK YOU