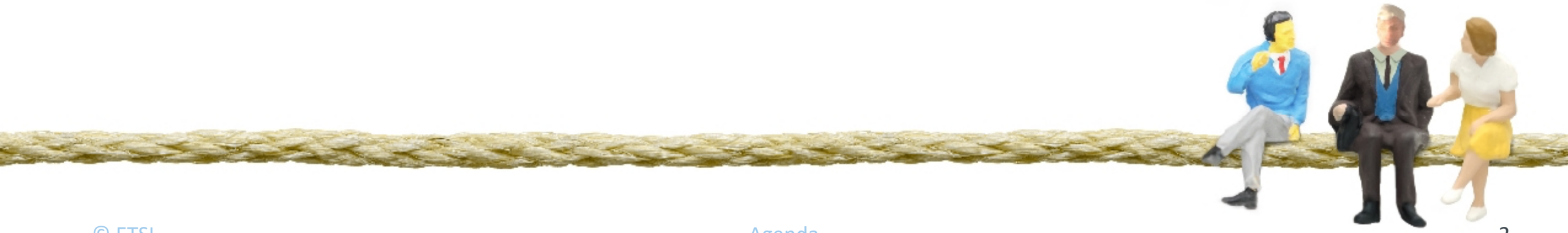
ETSI The Standards People

Decentralised Trust on the Internet Infrastructure: Securing Inter-Domain Routing

Presented by: **Prof. Albert Cabellos** For: **FINE (UPC)**

Agenda

- How does Inter-Domain Routing Works?
- Security issues of Inter-Domain Routing
- Centralized security for Inter-Domain Routing
- Decentralized Internet Infrastructure (DII)
- DII: Demo
- Conclusions

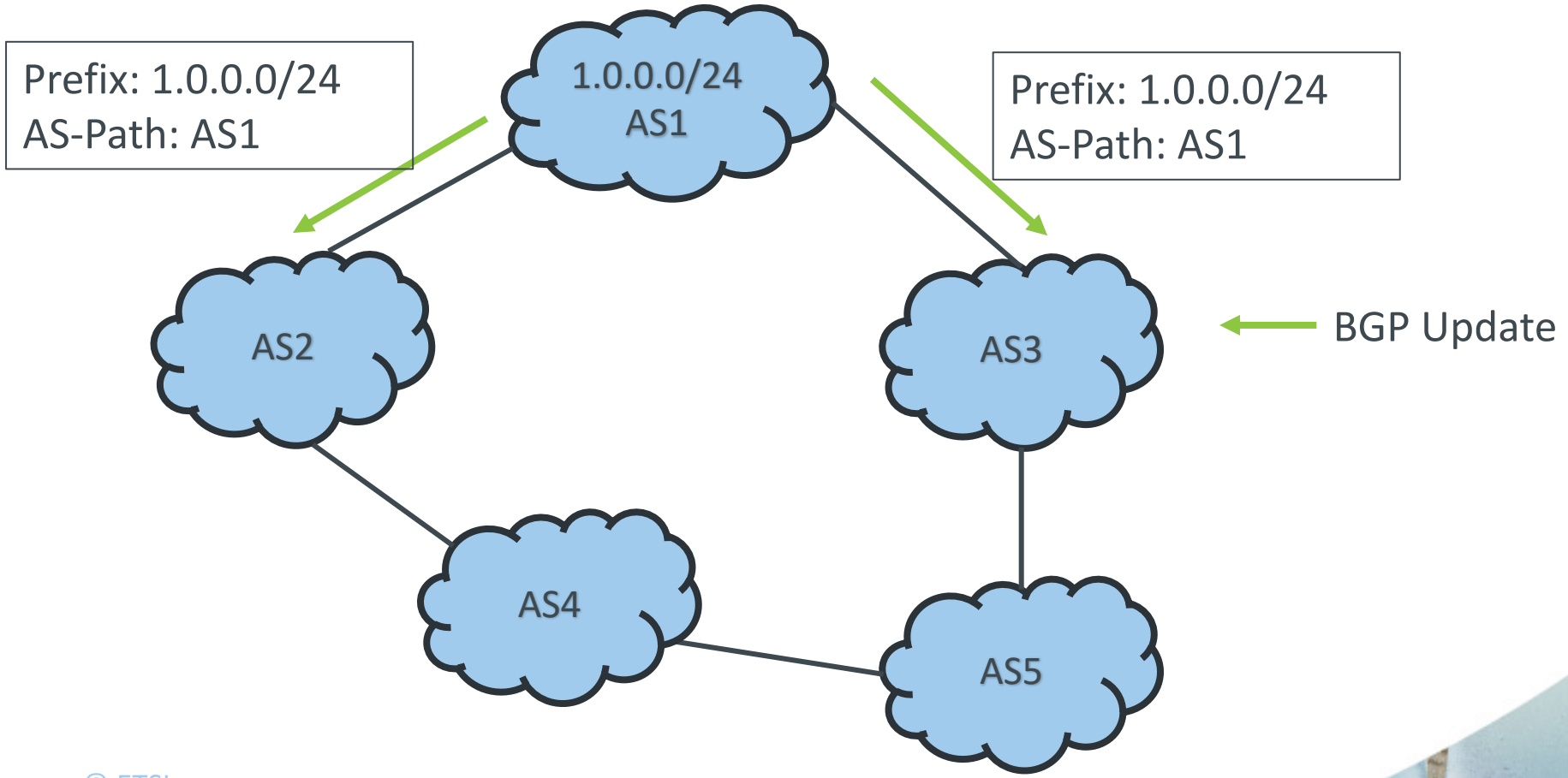


How does Inter-Domain Routing Works

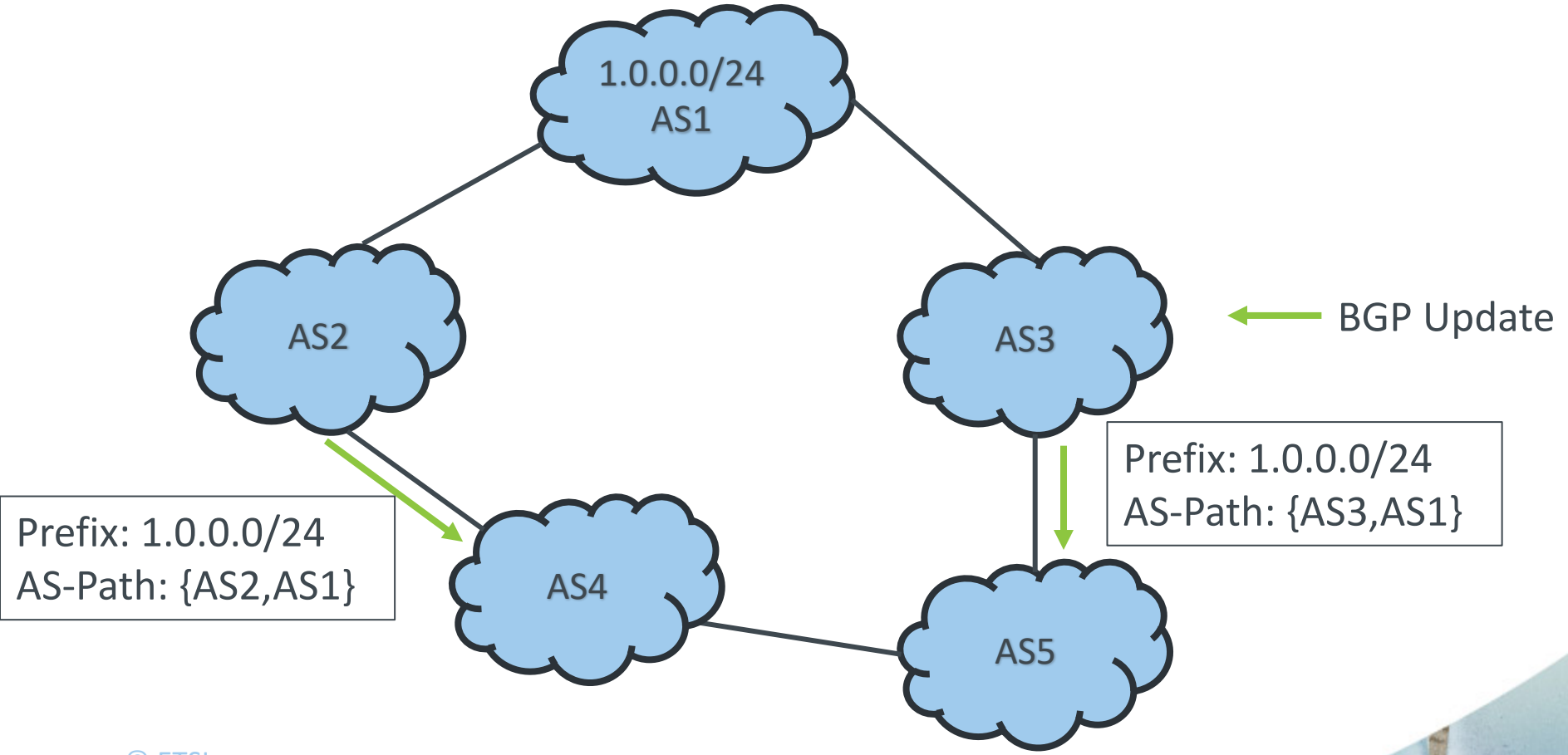
How does Inter-Domain Routing Works?

- Border Gateway Protocol (BGP, RFC4721) **glues** the Internet
- Provides **reachability** and **path selection** to Autonomous Systems (AS)
  - Helps an **AS** to **choose** the right **path** to reach a particular **IP address**
- It was initally designed back in 1989 **without security**
- The Internet infrastructure as well as the services offered over it **strongly depend** on the correct operation of **BGP**

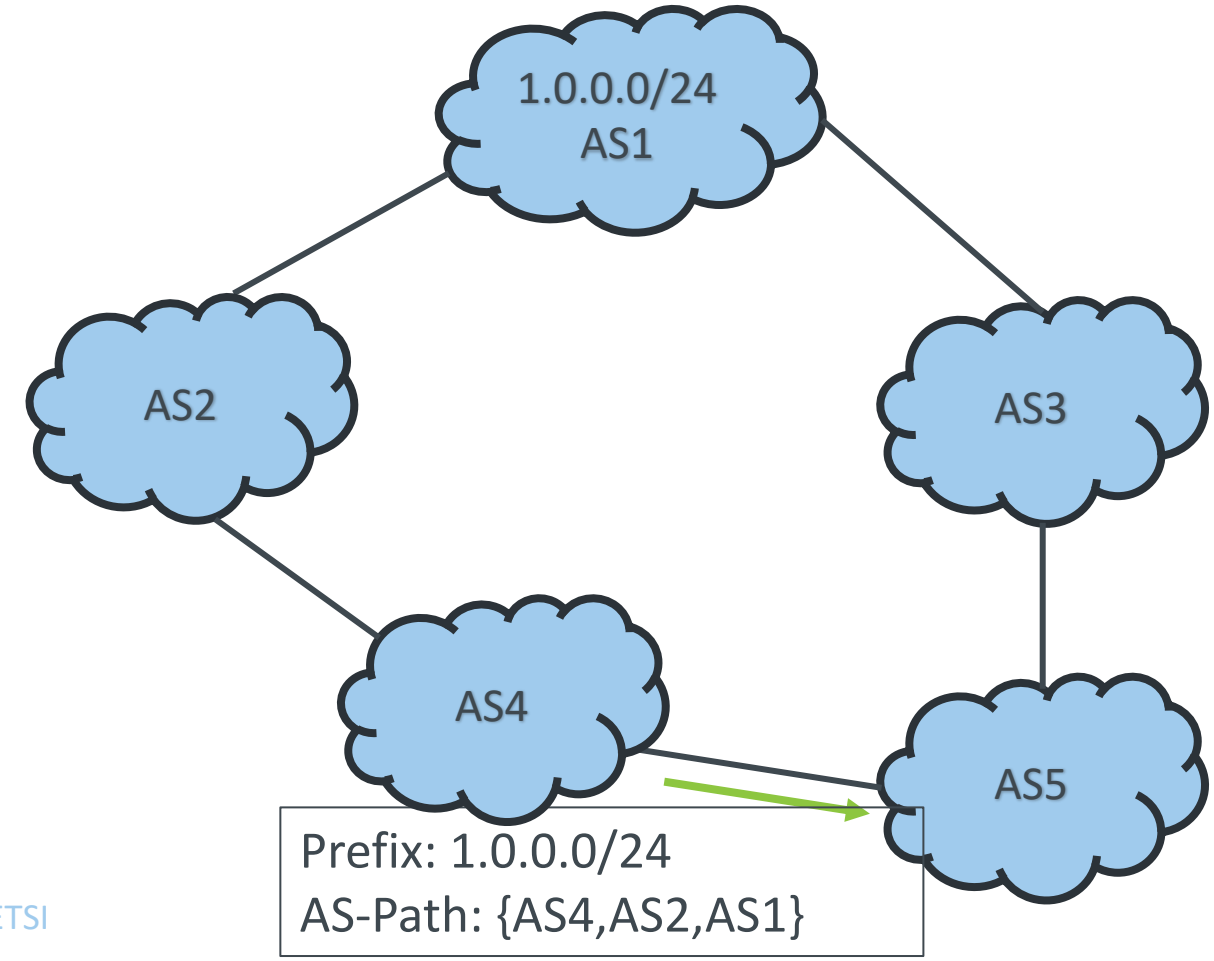
How does Inter-Domain Routing Works?



How does Inter-Domain Routing Works?

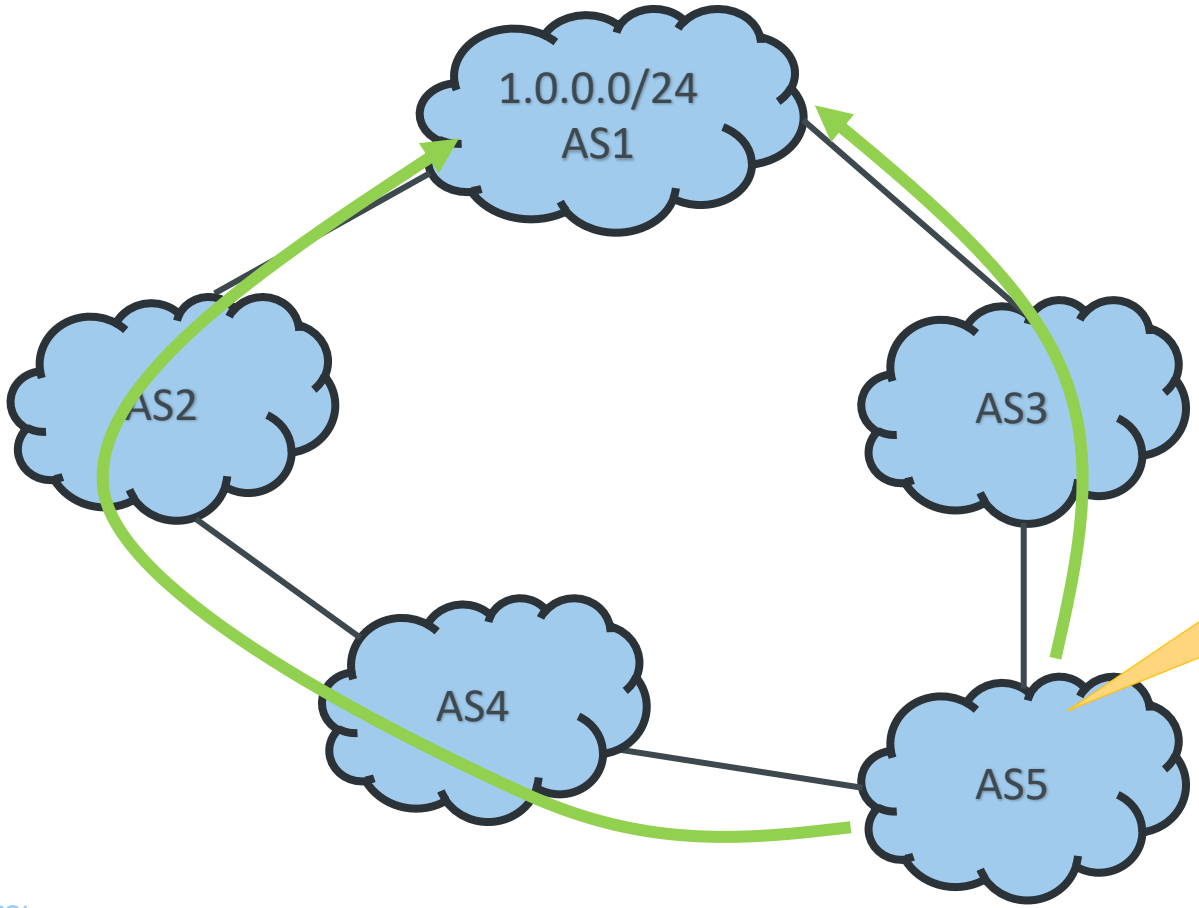


How does Inter-Domain Routing Works?



BGP Update

How does Inter-Domain Routing Works?



AS5 has two paths to reach AS1
- {AS5,AS3,AS1}
- {AS5, AS4, AS2, AS1}

AS5 will run the BGP decision process (simplified):

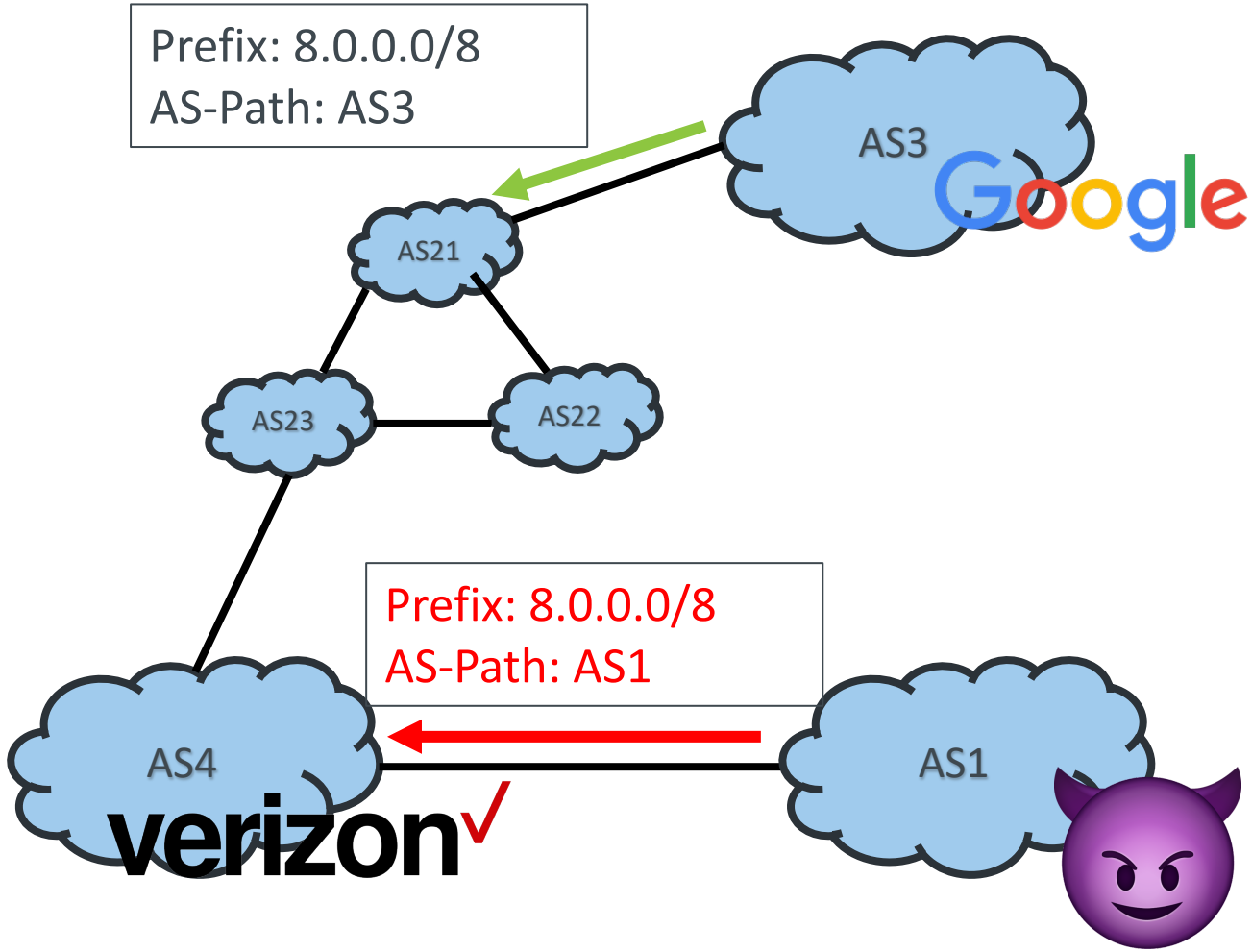
1) Local preference
   - **Business relationships**
2) Shorter paths

Security Issues of Inter-Domain Routing

Security Issues of Inter-Domain Routing

- BGP was not designed with security in mind
- BGP introduces critical security threats:
  1. Prefix Hijack
  2. Path Hijack
  3. Route Leak
- These are not just academic issues, but real-world threats that have been repeteadly exploited and have resulted in disruption of Internet-based services

Security Issues of Inter-Domain Routing: **Prefix Hijack**



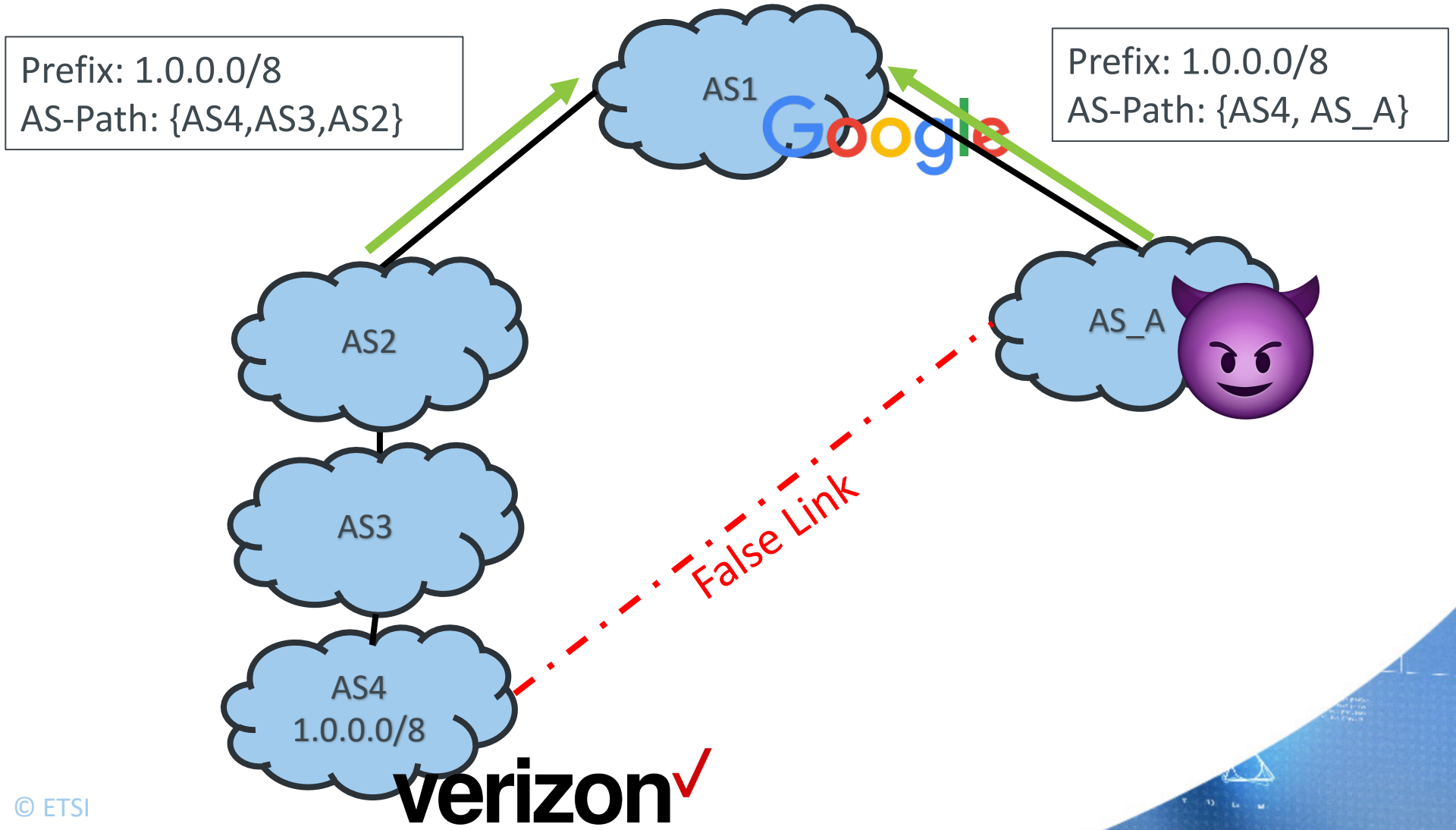
Security Issues of Inter-Domain Routing: **Prefix Hijack**

- A Prefix Hijack occurs when an AS announces a prefix that it does not hold
  - The attacker AS impersonates the victim AS
  - Attracts traffic intended to the victim's AS
- *December 2017: Eighty high-traffic prefixes normally announced by Google, Apple, Facebook, Microsoft, Twitch, NTT Communications, Riot Games, and others, were announced by a Russian AS, DV-LINK-AS (AS39523) [1]*
- See a list of public indicents here [2]
- We need to **authenticate** the mapping between AS Number (identifies the **holder**) and the prefix (the **resource holder**)

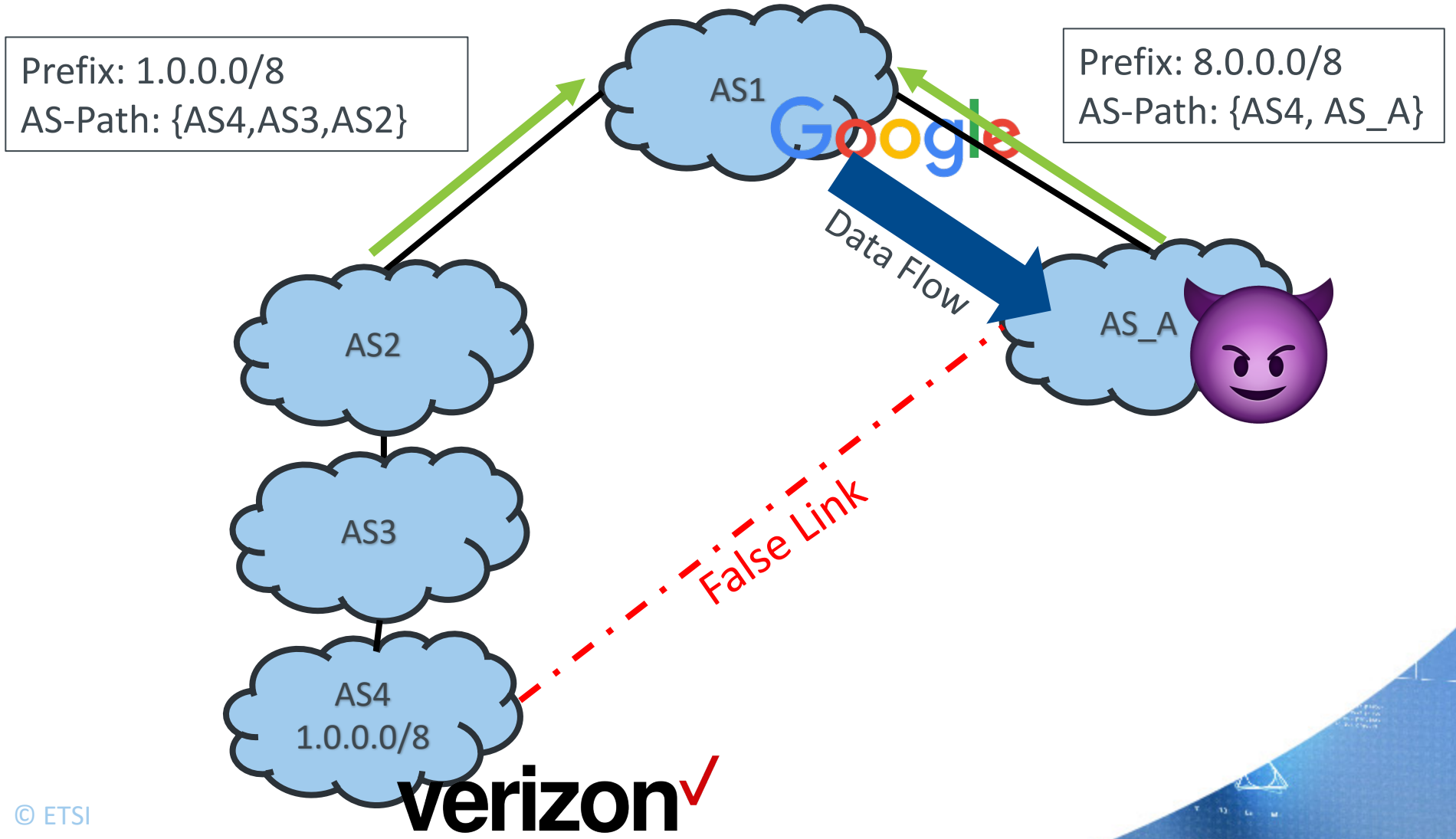
Prefix: 8.0.0.0/8 AS-Path: AS3	Vs.	Prefix: 8.0.0.0/8 AS-Path: AS1

[1] https://radar.qrator.net/blog/born-to-hijack
[2] https://en.wikipedia.org/wiki/BGP_hijacking

Security Issues of Inter-Domain Routing: **Path Hijack**

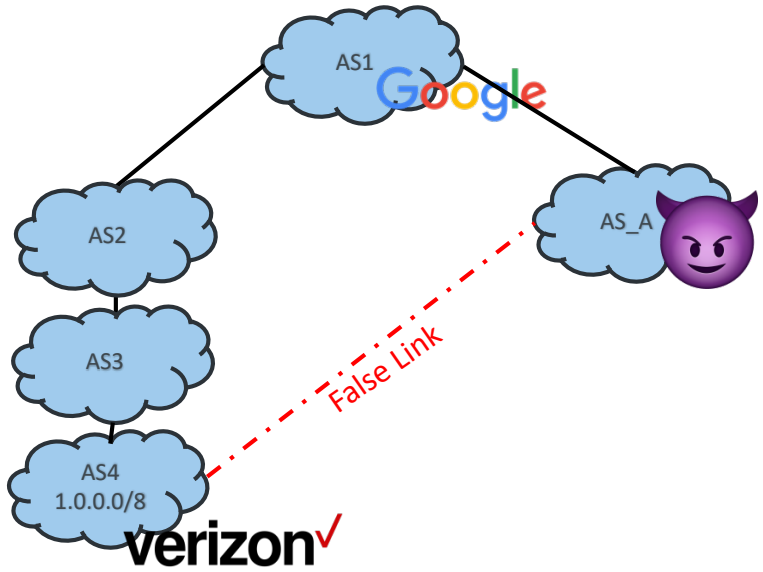


Security Issues of Inter-Domain Routing: **Path Hijack**

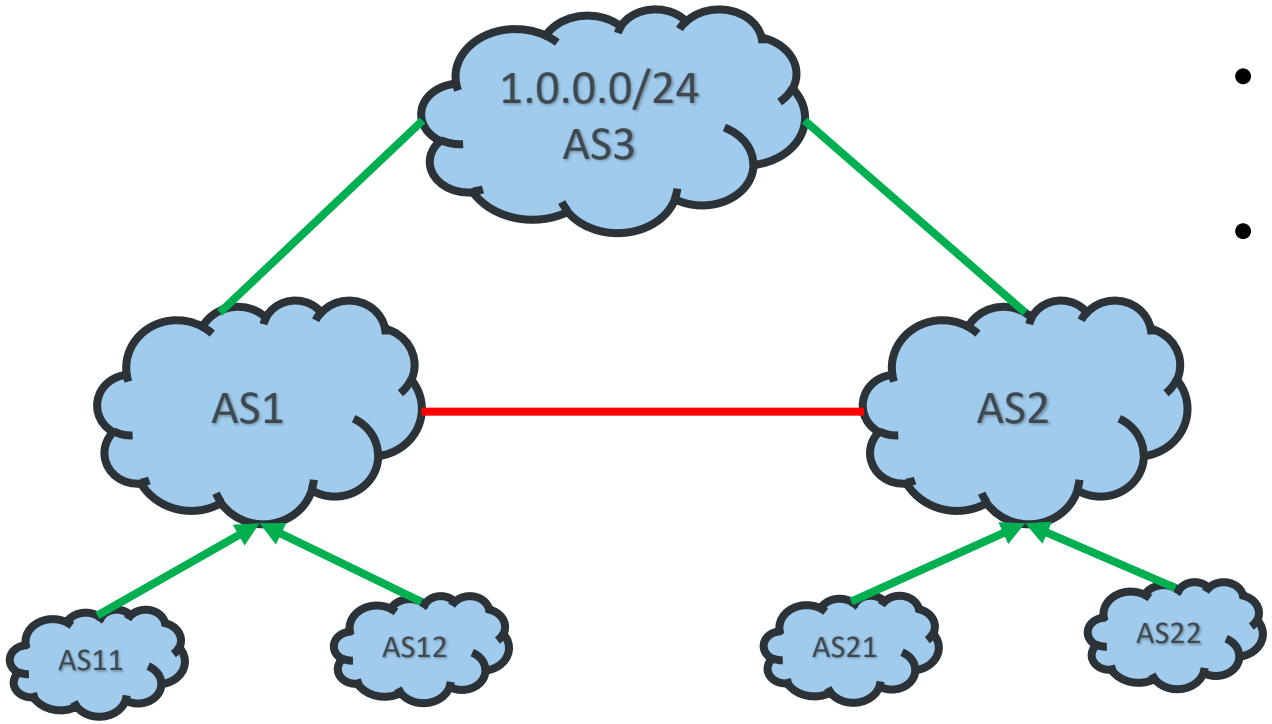


Security Issues of Inter-Domain Routing: **Path Hijack**

- A Path Hijack occurs when an As announces an incorrect path or link
- We need to **authenticate** AS adjacencies
- AS4 is not connected to AS_A

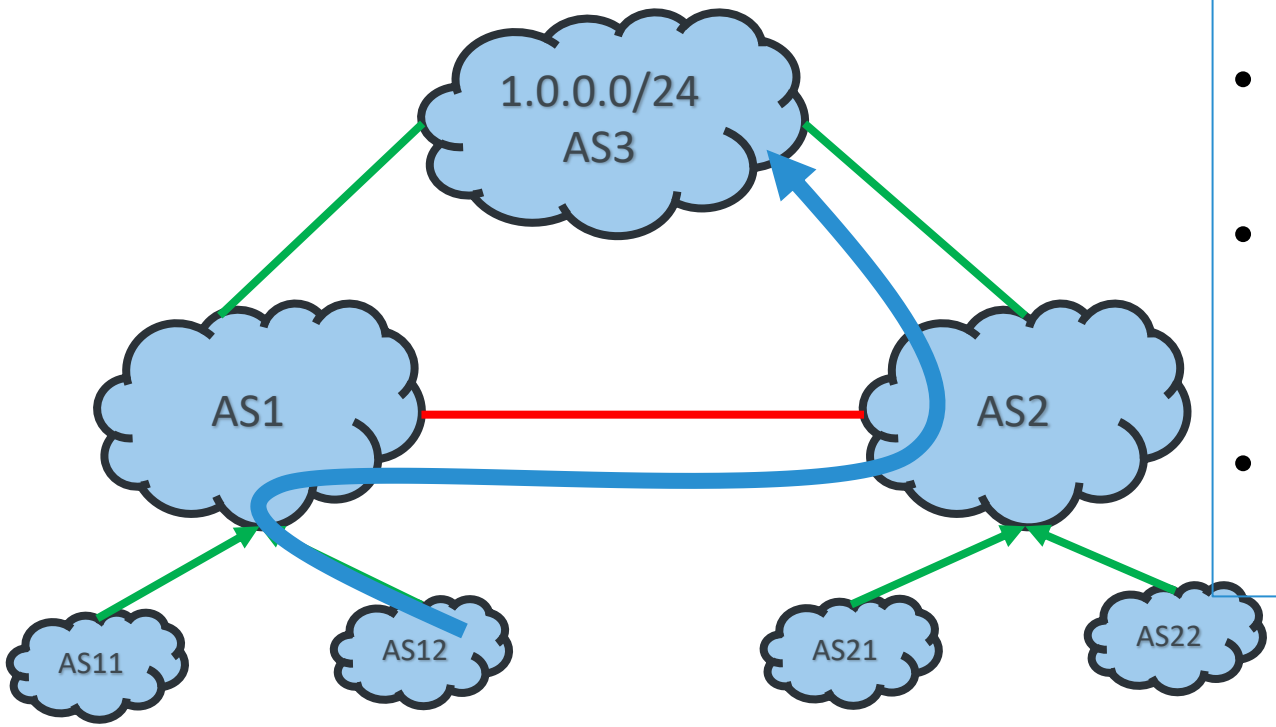


Security Issues of Inter-Domain Routing: **Route Leaks**



- **Customer Provider** links are typically paid
- The costs of **Peering** links is typically shared
- Routes learnt from upstream customer-provider links are not propagated through peering links

Security Issues of Inter-Domain Routing: **Route Leaks**



- **Customer Provider** links are typically paid
- The costs of **Peering** links is typically shared
- Routes learnt from upstream customer-provider links are not propagated through peering links
- Otherwise AS2 will offer free **transit** to AS1 (and its customers)

Security Issues of Inter-Domain Routing: **Route Leaks**

- A Route Leak is an (un)intended violation of ASes' business relationships
- Route Leaks are very common and often occur due to misconfiguration
- In February 2008 Pakistan Telecom brought down the entire Youtube site for 2 hours. It propagated the leak to an ISP in Hong Kong that further propagated it to the rest of the Internet [1]
- We need to **protect** and **enforce** the routing policy of ASes.

[1] https://www.lacnic.net/innovaportal/file/4016/1/cloudflare---anatomy-of-a-route-leak.pdf

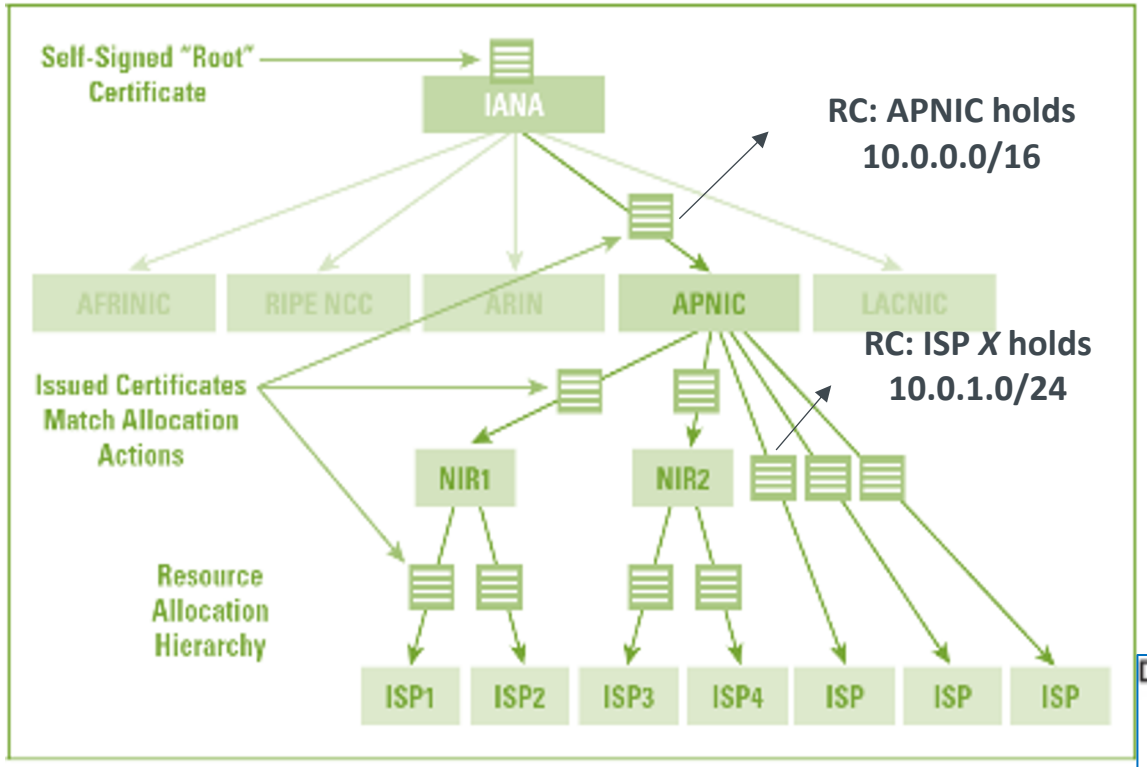
Centralized Security for Inter-Domain Routing

Centralized Security in Inter-Domain Routing

- Current solutions to fix the security threats of Inter-Domain Routing are
  - Resource Public Key Infrastructure (RPKI)
  - BGP-SEC
- RPKI is a traditional certificate-based architecture
  - RIRs issue a certificate to IP-prefix and AS# holders
  - IP-prefix and AS# holders authorize routers to announce AS#→IP-prefix (ROA)
- RPKI was initially proposed in 2012
- According to current estimates [1], approximately 10% of BGP announces are covered by RPKI

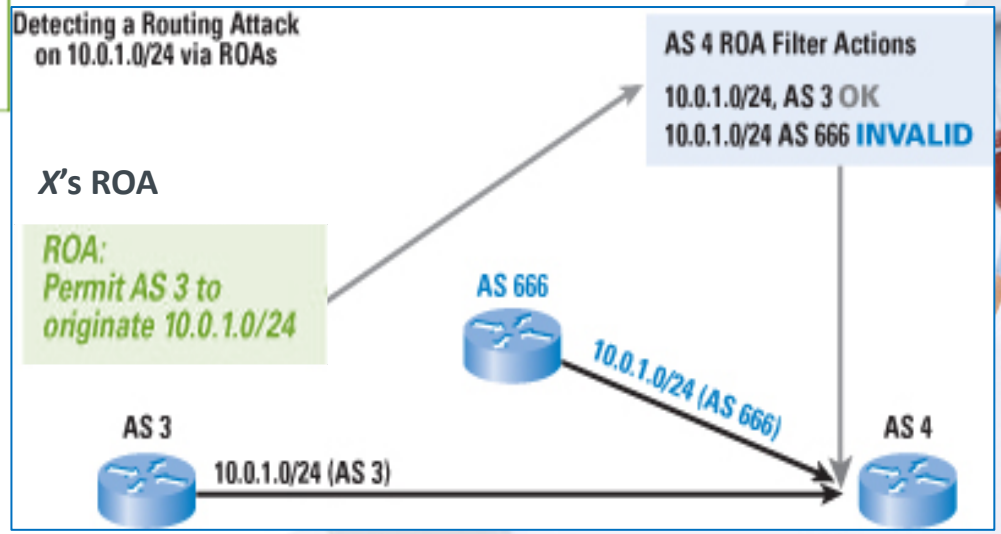
[1] https://blog.apnic.net/2020/01/29/is-rpki-ready-for-the-big-screen/

How does RPKI work?



Resource Certificate (RC) certifies ownership of IP prefixes and AS numbers.

Route Origin Authorization (ROA) certifies an ASN can announce an IP prefix.



Images from here and here

Centralized Security in Inter-Domain Routing

Centralization may have fundamental issues

- Entities rely on central authorities as trust anchors
- **An authority has the privilege to unilaterally remove descendants' trust anchors**
  - *A central authority can be hacked or compromised to perform malicious actions.*
  - *A central authority may not be fully neutral.*
    It may have bias due to conflicts of interests, politics, or domestic laws.

A central authority can cause globally damaging impacts

- Entities, relying on centralization, may become untrusted. Services may become unavailable, resulting in economic losses and even damaging impacts
- An authority in one country can also damage the trust anchors of organizations in other countries, because trust chains are often across countries

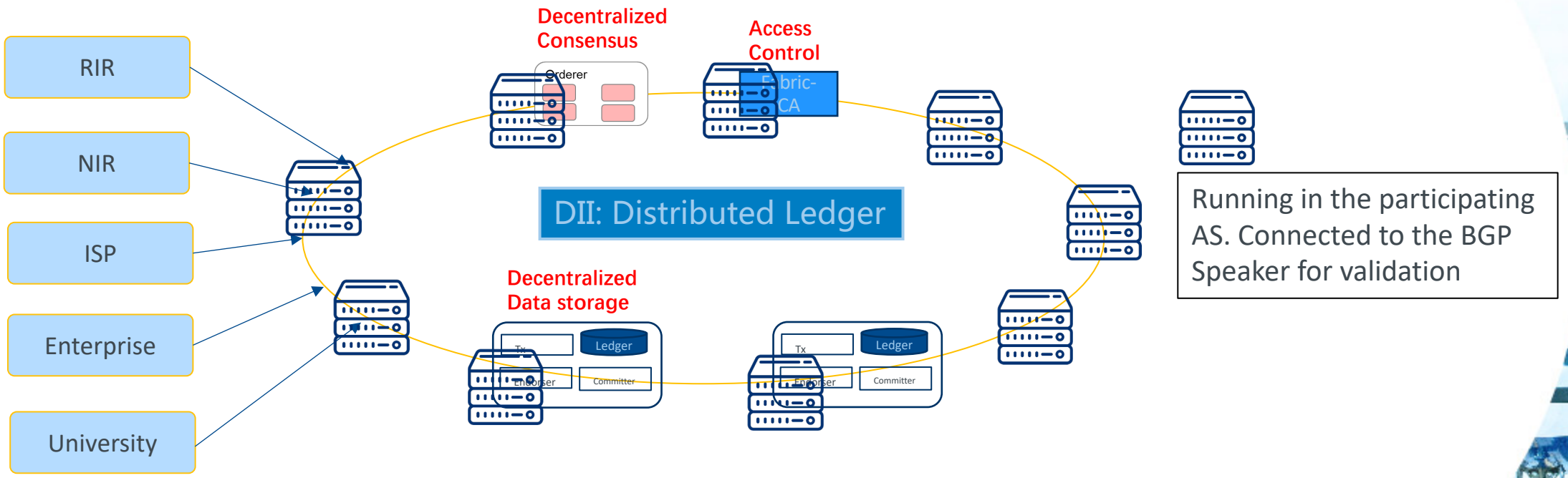
Centralized Security in Inter-Domain Routing

- Centralized solutions require **centralized trust**
- Misbehaved RPKI authorities assert legitimate BGP routes invalid [1]
  - *Dec 2013, ARIN (mis-)added a ROA, authorizing prefix 173.251.0.0/17 with maxlength 24 to AS 6128. This caused a large portion of the address space to become "invalid", including several legitimate routes.*
  - *Dec 2013, a ROA was (mis-)deleted by an RPKI authority. Since a covering ROA mapping the prefixes to another ISP. The covering ROA caused the route of the whacked ROA to become invalid.*
- *RPKI provides protection against **prefix hijacking***
- *But it does **NOT** offer protection against **path hijack or route leak** [2]*

[1] From the Consent of the Routed: Improving the Transparency of the RPKI, SIGCOMM 14
[2] Cohen, A., Gilad, Y., Herzberg, A., & Schapira, M. (2016, August). Jumpstarting BGP security with path-end validation. In *Proceedings of the 2016 ACM SIGCOMM Conference* (pp. 342-355).

Decentralized Internet Infrastructure (DII)

Decentralized Distributed Infrastructure (DII)



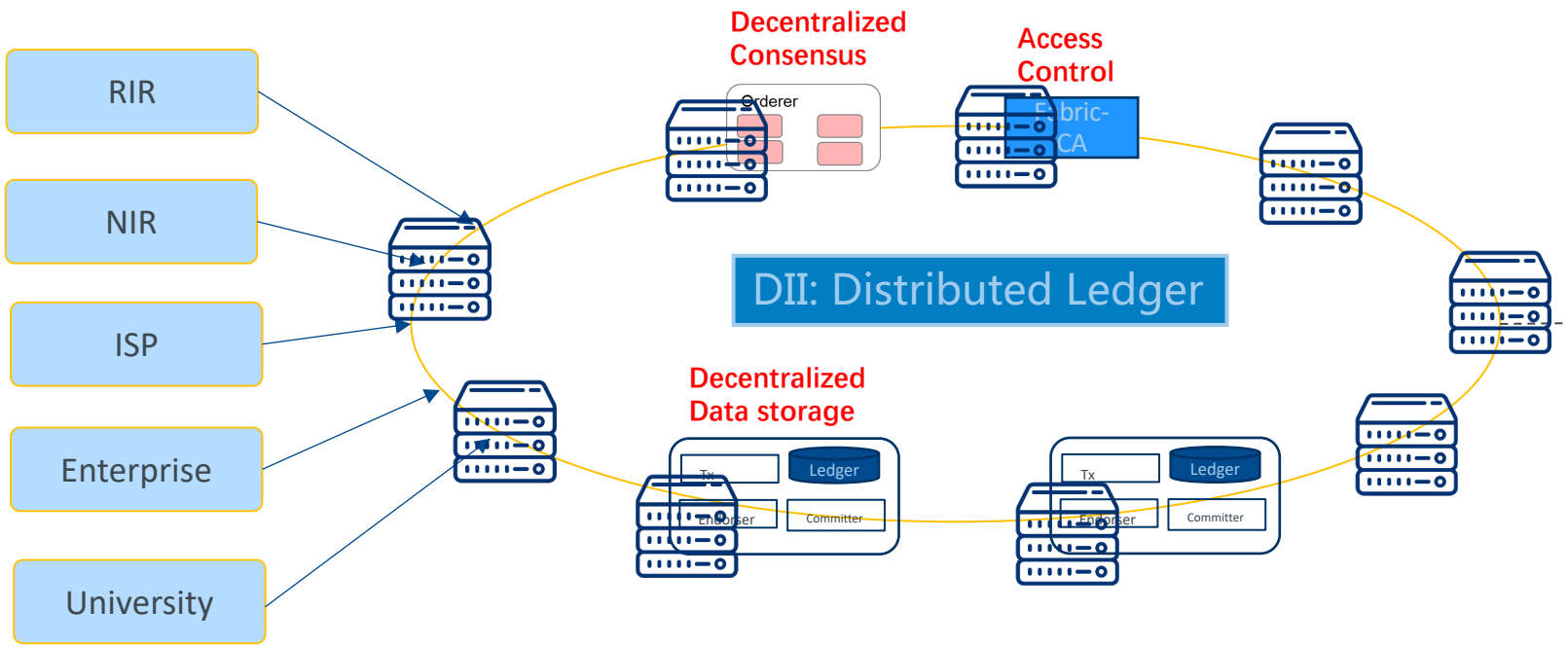
Distributed Ledgers: Participants are RIRs, NIRs, ISPs, Enterprise and Universities, in general IP-prefix and ASN holders participating in BGP.

Decentralized Data Storage: Data is distributed among participants.

Access control: Only authenticated participants can read/write in the ledger.

Distributed Consensus: Participants agree on adding a new transaction to the ledger.

Decentralized Distributed Infrastructure (DII)



Store IP Ownership, ROA and AS Neighbor Info in world state.

IP Ownership

IP	Owner	Exp date
1.1.1.1/32	ISP1	19/10

ASN Ownership

ASN	Owner	Exp date
AS100	ISP1	19/10

Only owner can create ROA record

ROA (IP->ASN)

IP	Maxlength	ASN
1.1.1.1/32	32	100

Only owner can create Neighbor record.

AS Neighbor(ASN->ASN)

Source	Target
AS100	AS200
AS200	AS300

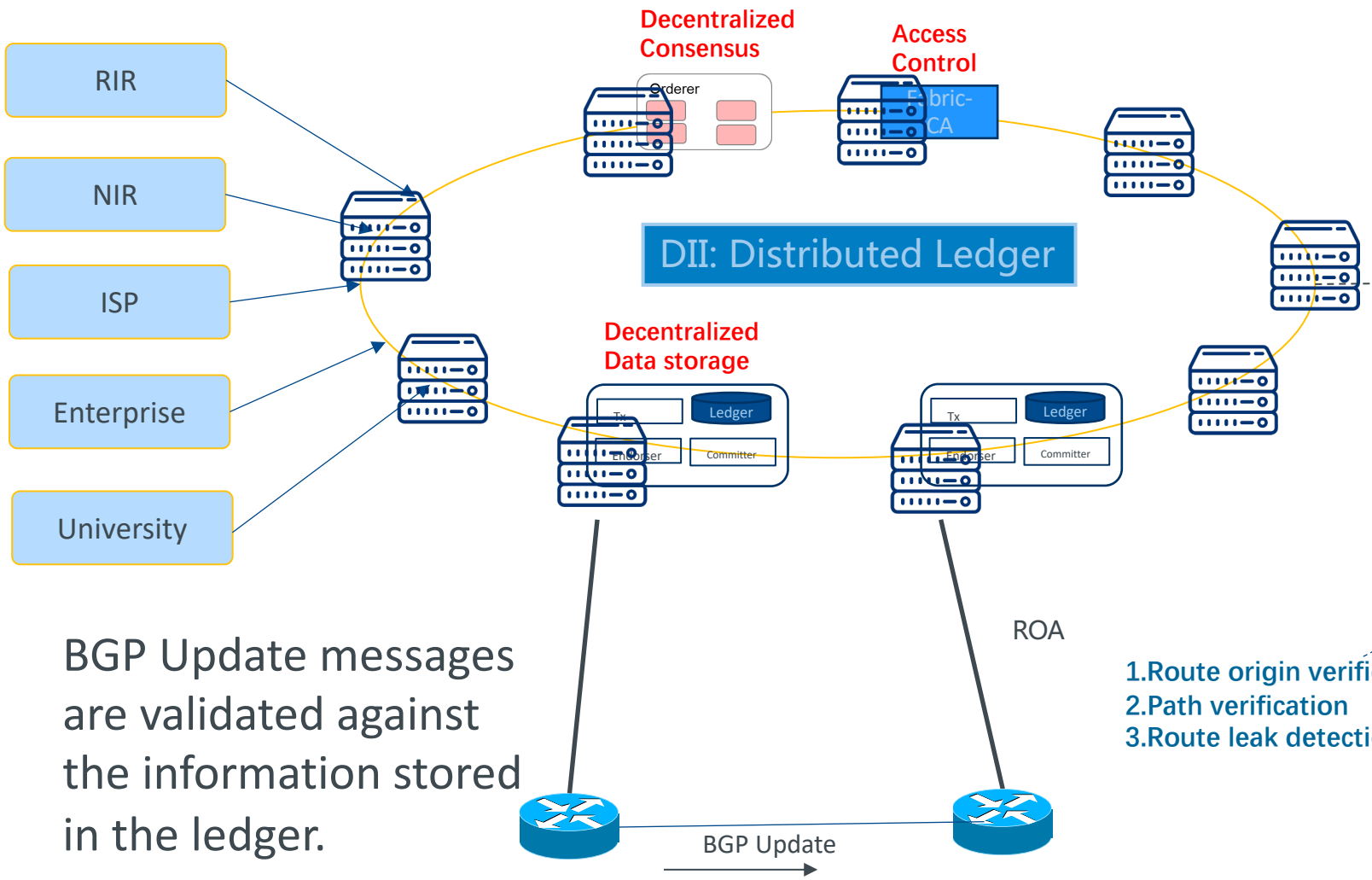
AS Business Relationship(ASN->ASN)

Source	Target	Type
AS100	AS200	P2P
AS200	AS300	P2P

Transactions are produced by participants and stored in the ledger.

Transactions provide (1) IP and (2) ASN ownership, (3) IP to ASN mapping (ROA), (4) AS adjacency as well the type of (5) business relationship

Decentralized Distributed Infrastructure (DII)



BGP Update messages are validated against the information stored in the ledger.

Store IP Ownership, ROA and AS Neighbor Info in world state.

Only owner can create ROA record

IP Ownership

IP	Owner	Exp date
1.1.1.1/32	ISP1	19/10

ASN Ownership

ASN	Owner	Exp date
AS100	ISP1	19/10

ROA (IP->ASN)

IP	Maxlength	ASN
1.1.1.1/32	32	100

Only owner can create Neighbor record.

AS Neighbor(ASN->ASN)

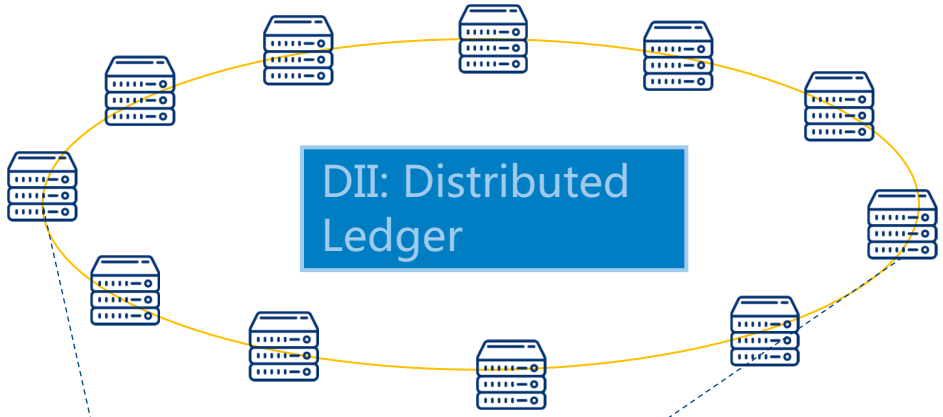
Source	Target
AS100	AS200
AS200	AS300

AS Business Relationship(ASN->ASN)

Source	Target	Type
AS100	AS200	P2P
AS200	AS300	P2P

1.Route origin verification
2.Path verification
3.Route leak detection

DII: Protection against **prefix hijack**



IP Ownership

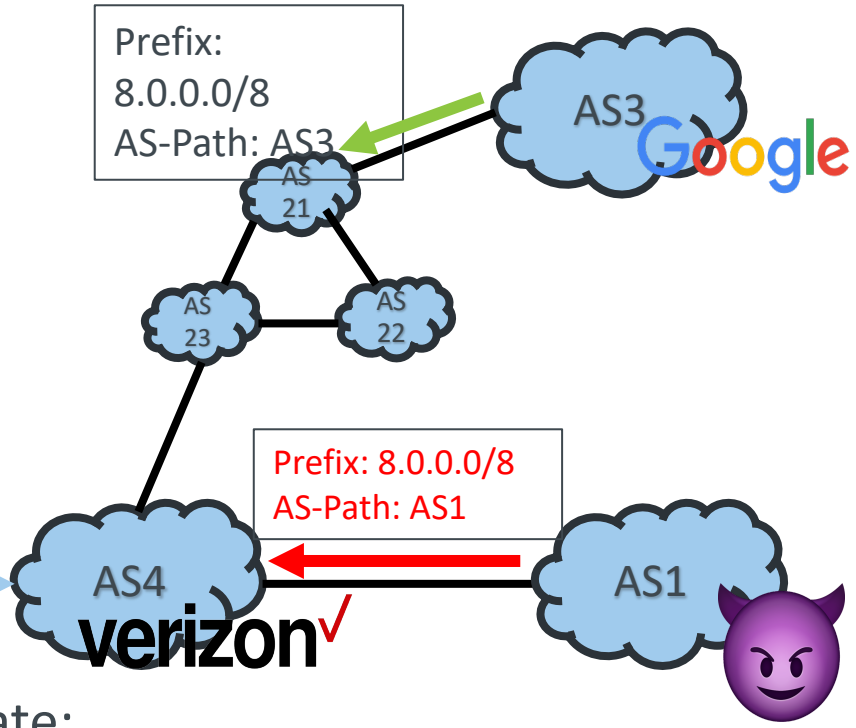
IP	Owner	Exp date
8.0.0.0/8	Google	12/30

ASN Ownership

ASN	Owner	Exp date
AS3	Google	12/30

ROA (IP->ASN)

IP	Maxlength	ASN
8.8.8.8/32	32	AS3



DII invalidates incorrect BGP update:

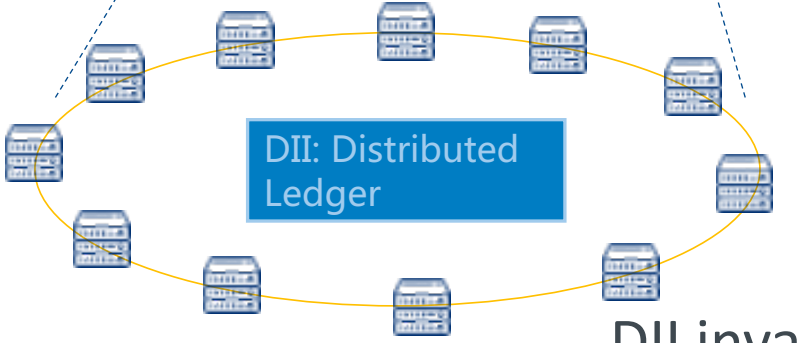
AS1 does not hold 8.0.0.0/8.

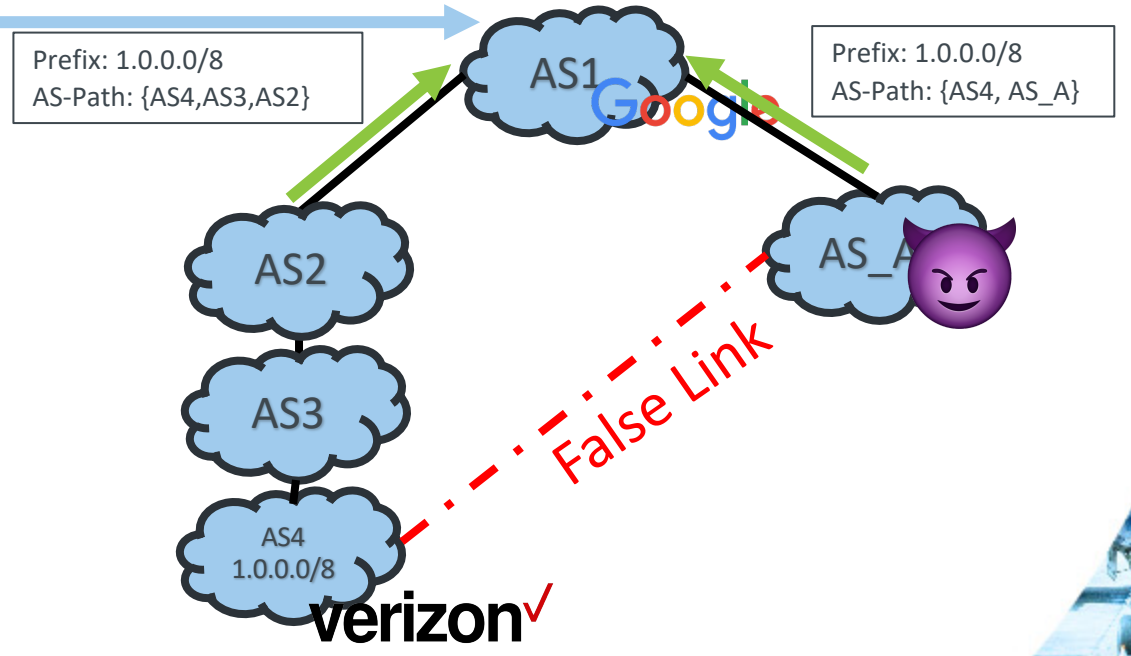
Only owner can create Neighbor record.

DII: Protection against **path hijack**

AS Neighbor(ASN->ASN)

Source	Target
AS1	AS2
AS1	AS_A
AS2	AS3
AS3	AS4





DII invalidates incorrect AS Path:

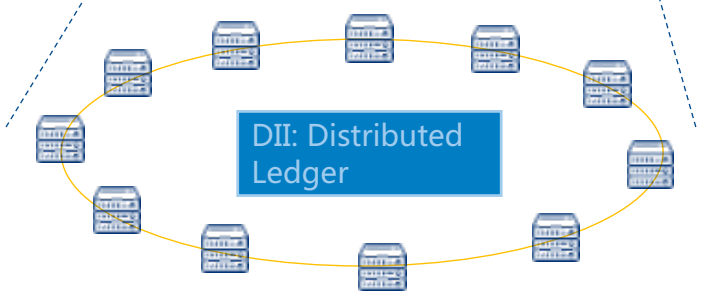
AS_A is **NOT** adjacent to AS4

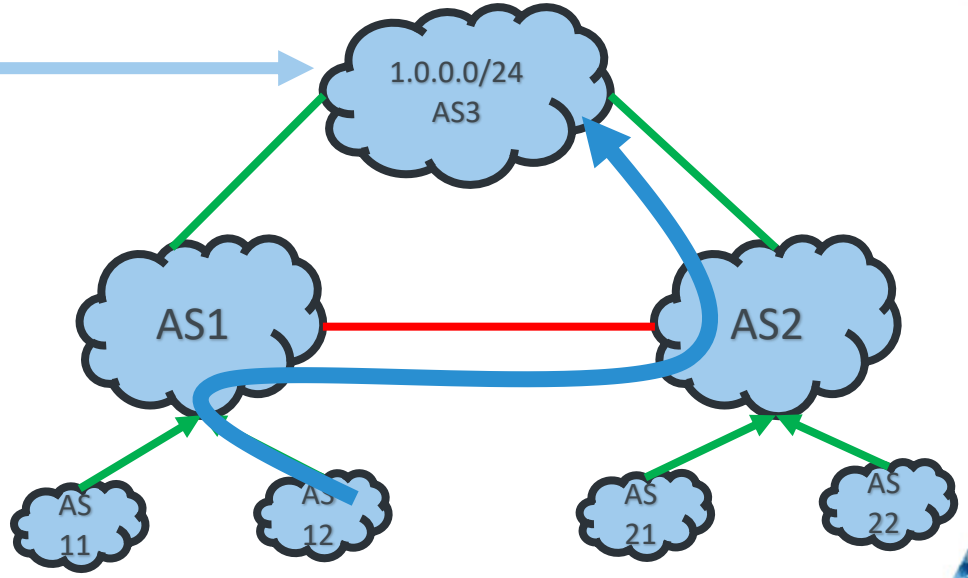
Only owner can create Neighbor record.

DII: Protection against **route leaks**

AS Business Relationship(ASN->ASN)

Source	Target	Type
AS3	AS1	CP
AS3	AS2	CP
AS1	AS2	P2P
AS1	AS11	CP
AS1	AS12	CP
AS2	AS21	CP
AS2	AS22	CP





DII invalidates incorrect AS announcement:

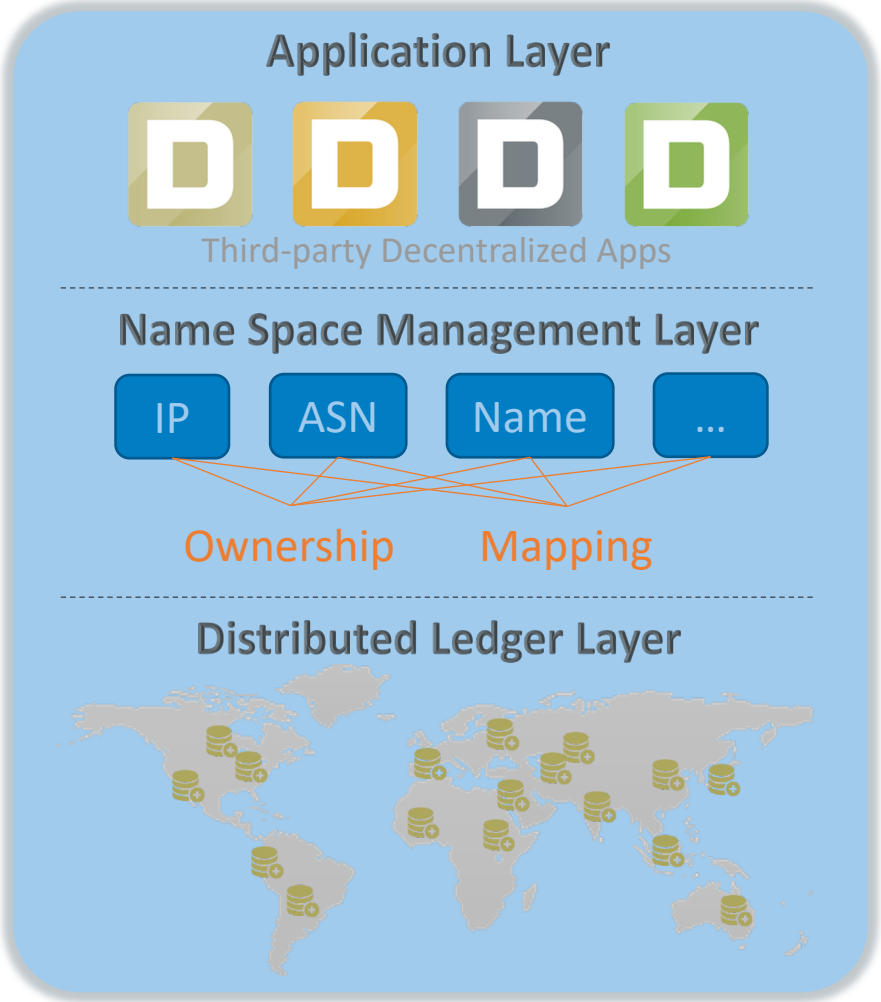
AS1 and AS2 have a P2P relationship.

AS2 should not propagate routes learnt from AS1

Only owner can create Neighbor record.

Beyond DII: Decentralized Internet

DII Architecture



3rd-party developers can build trusted dApps:

- Decentralized PKI for trusted identity
- Purchasing remote DDoS mitigation services on-demand
- Cross-domain end-to-end QoS

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, …

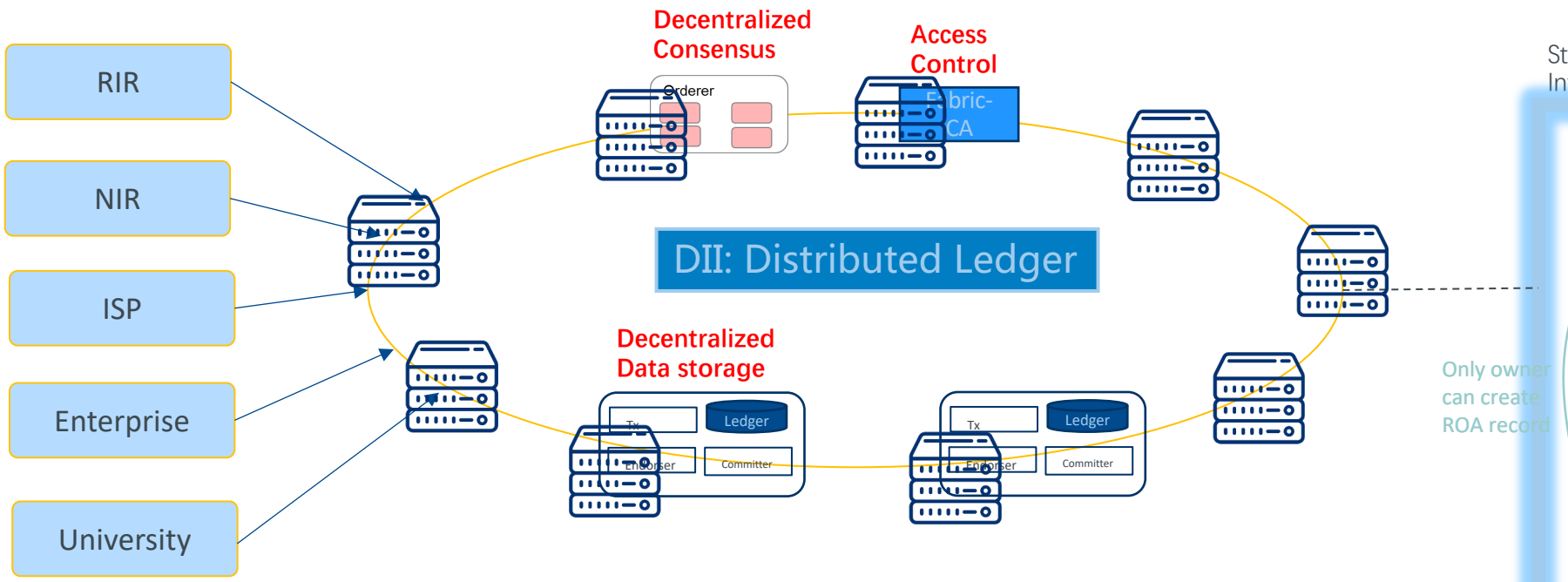
Distributed ledger enables a decentralized infrastructure

- Decentralized (peer-to-peer) network structure and trust model
- Consensus protocol
- Smart contract for computation model
- Transaction capability for monetization of network services

DII: Demo

DII: Global Testbed

DII: Demo



Store IP Ownership, ROA and AS Neighbor Info in world state.

IP Ownership

IP	Owner	Exp date
200	ISP1	19/10

ASN Ownership

ASN	Owner	Exp date
AS100	ISP1	19/10

Only owner can create ROA record

ROA (IP->ASN)

IP	Maxlength	ASN
1.1.1.1/32	32	100

AS Neighbor(ASN->ASN)

Source	Target
AS100	AS200
AS200	AS300

Only owner can create Neighbor record.

AS Business Relationship(ASN->ASN)

Source	Target	Type
AS100	AS200	P2P
AS200	AS300	P2P

In the demo we show:

(1) Applying for an IP prefix

(2) Apply for an AS Number

(3) Specify a ROA (IP-ASN)

(4) State an AS Adjacency and its type

Conclusions

Conclusions

- Inter-domain routing was designed without security in mind
- It is a critical component of the Internet infrastructure
  - Attacks to inter-domain infrastructure are disruptive to its services
- Current approach to secure Inter-domain routing are centralized
  - Single point of trust
- We present the Decentralized Distributed Infrastructure
  - Flexible distributed consensus
  - Protects against critical attacks on the inter-domain routing infrastructure

Further Reading

- Paillisse, Jordi, Miquel Ferriol, Eric Garcia, Hamid Latif, Carlos Piris, Albert Lopez, Brenden Kuerbis et al. "IPchain: Securing IP prefix allocation and delegation with blockchain." In *2018 IEEE Blockchain*
- Galmés, Miquel Ferriol, et al. "Preventing Route Leaks using a Decentralized Approach." *2020 IFIP Networking Conference (Networking)*. IEEE, 2020.
- Internet-level Consensus http://www.scs.stanford.edu/~dm/talks/20170424-dotscale.pdf
- Cohen, Avichai, et al. "Jumpstarting BGP security with path-end validation." *Proceedings of the 2016 ACM SIGCOMM Conference*. 2016.

Debate

- This project is part of the NewIP initiative
- NewIP has raised significant push-back in the western media
- Please, read more about New IP
  - https://www.huawei.com/en/industry-insights/innovation/new-ip
- Please, read the Financial Times article
  - https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f
  - https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2
- Let´s debate!

ETSI The Standards People

Decentralised Trust on the Internet Infrastructure: Securing Inter-Domain Routing

Presented by: **Albert Cabellos** For: **FINE**