ETSI PDL
Proof of Concept Framework

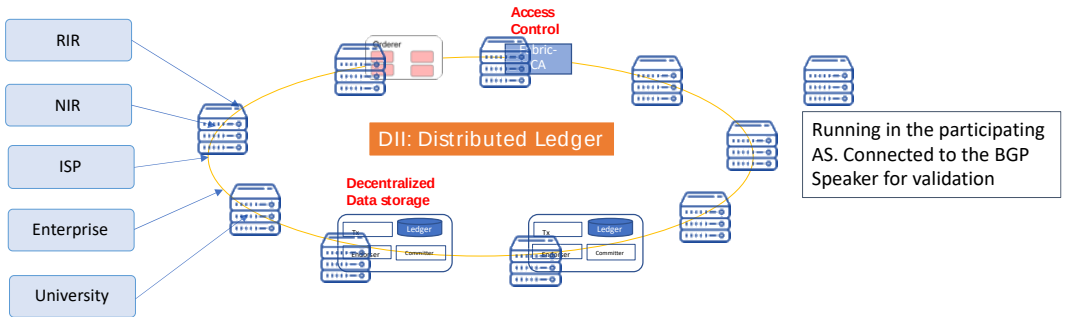
Final Report

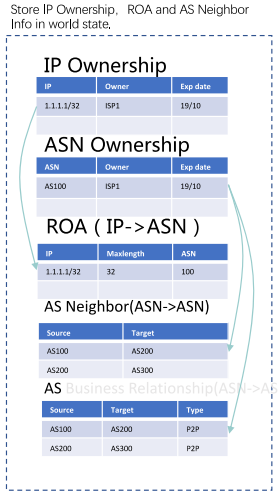
Prof. Albert Cabellos

May 2021

ETSI PDL – Proof of Concept Summary

Blockchain for Inter-Domain Security





Inter-Domain Security

Protects against the following attacks

- Prefix Hijack
- Path Hijack
- Route Leak

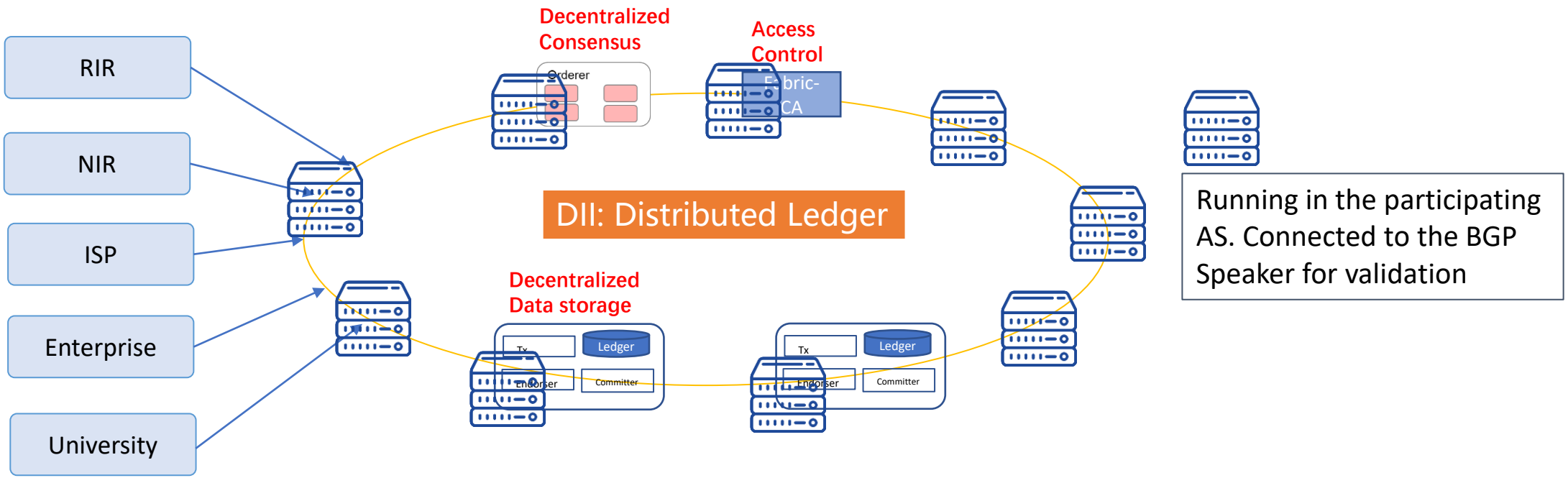
Proof-of-Concept Testbed

Proof of Concept Stages and Milestones

- Project Start: 01/07/2020
- PoC Demo 1: ETSI BrighTalk 15/09/2020
  - https://www.brighttalk.com/webcast/12761/433364
- PoC Demo 2 and 3: Cancelled due to COVID (see note 1 and 2 on original proposal)
- PoC Demo 3: Submitted Demo PoC to IEEE INFOCOM (15/01/2021)
  - IEEE INFOCOM is ranked Core A+ (http://portal.core.edu.au/conf-ranks/)
  - Strong impact on the Networking Academic and Industrial communities
- PoC Expected Contribution 1 – Smart contracts use and validation 01/08/20202
- PoC Expected Contribution 2 – Interconnection of Ledgers 01/09/20202
- PoC Expected Contribution 3 – Interconnection proof of requirements 01/11/20202

Proof-of-Concept

Proof-of-Concept: Architecture



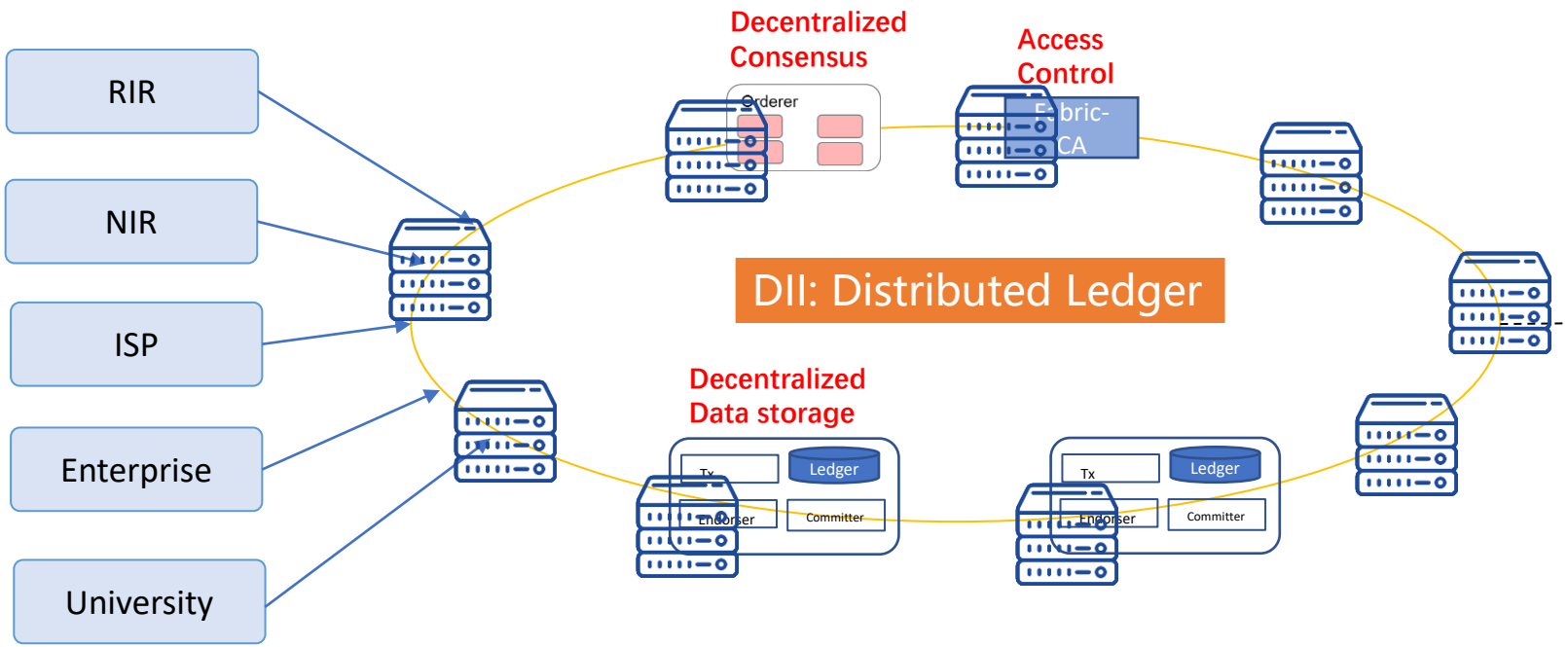
Distributed Ledgers: Participants are RIRs, NIRs, ISPs, Enterprise and Universities, in general IP-prefix and ASN holders participating in BGP.

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.

Information stored in the ledger



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

Only owner can create ROA record

Only owner can create Neighbor 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

AS Neighbor(ASN->ASN)

Source	Target
AS100	AS200
AS200	AS300

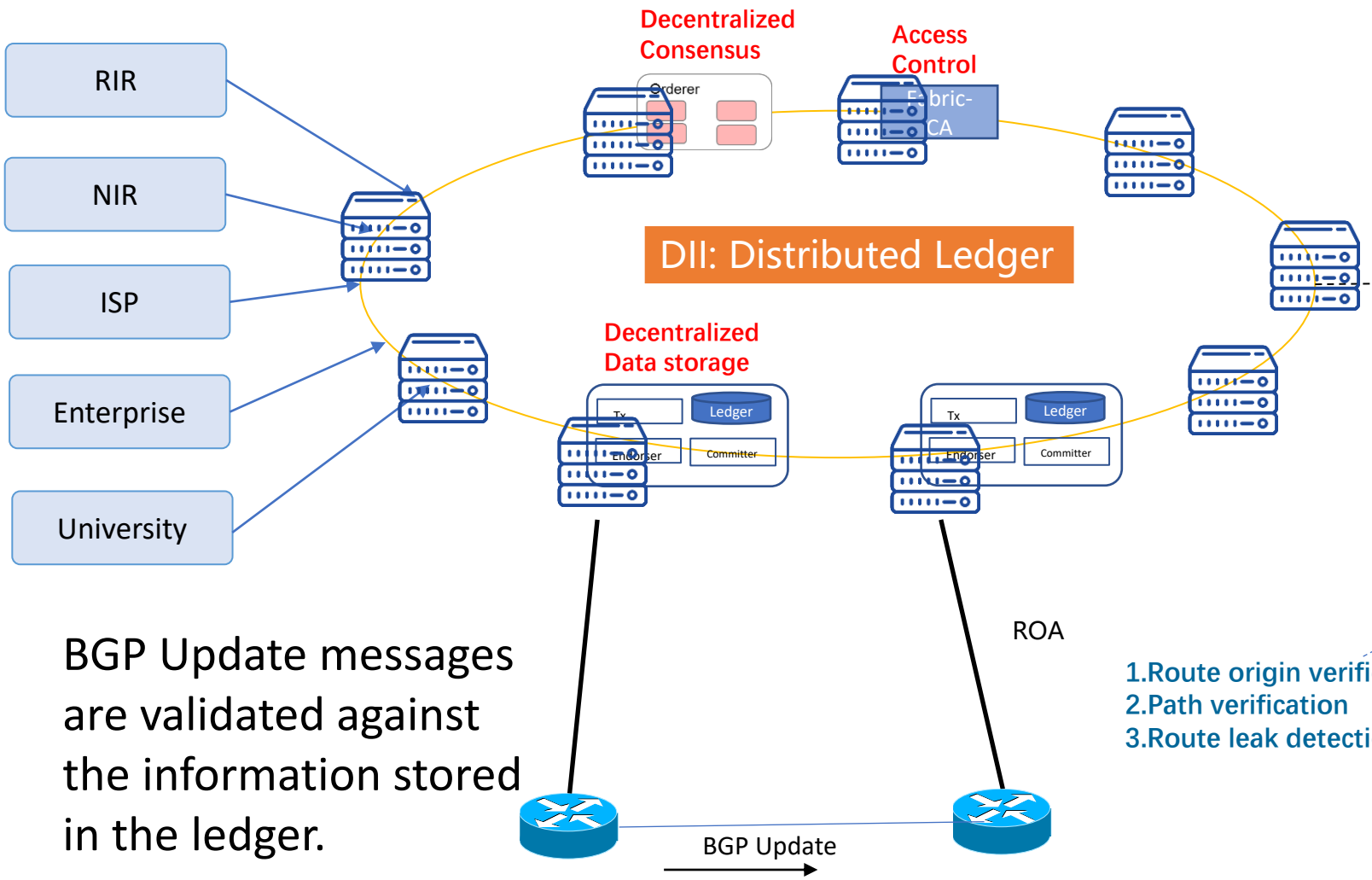
AS Business Relationship(ASN->ASN)

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

Interface with the Data-Plane



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

AS Neighbor(ASN->ASN)

Source	Target
AS100	AS200
AS200	AS300

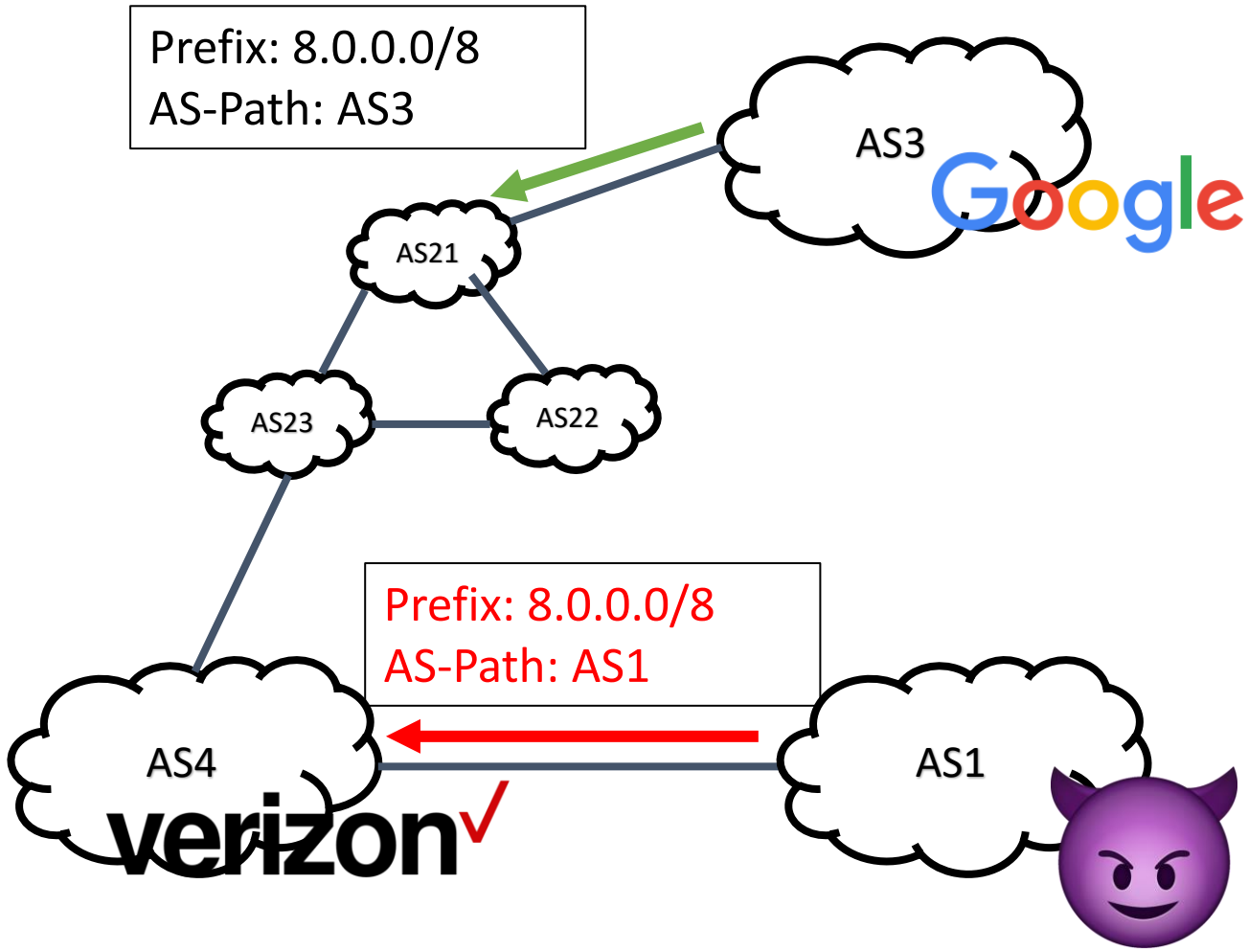
AS Business Relationship(ASN->ASN)

Source	Target	Type
AS100	AS200	P2P
AS200	AS300	P2P

Only owner can create Neighbor record.

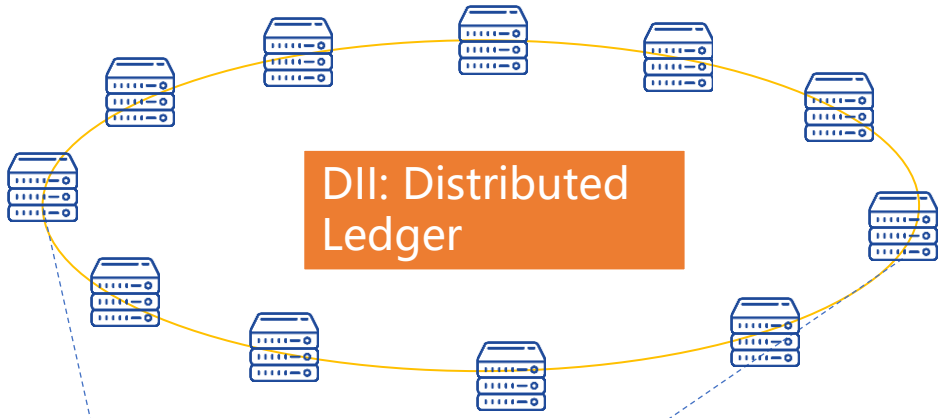
1.Route origin verification
2.Path verification
3.Route leak detection

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)*
- We need to **authenticate** the mapping between AS Number (identifies the **holder**) and the prefix (the **resource holder**)

Protection against **prefix hijack**



IP Ownership

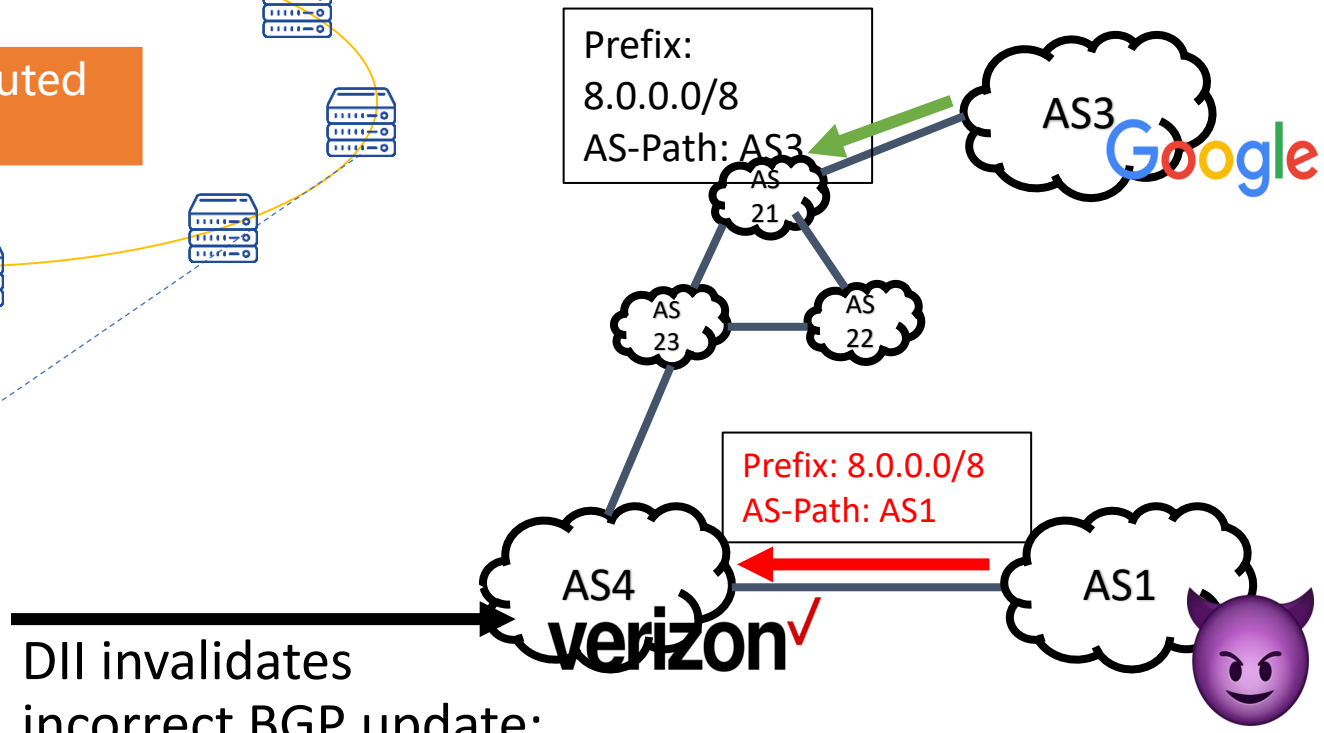
IP	Owner	Exp date
8.0.0.0/8	Google	12/30

ASN Ownership

ASN	Owner	Exp date
AS3	Google	12/30

ROA (IP->ASN)

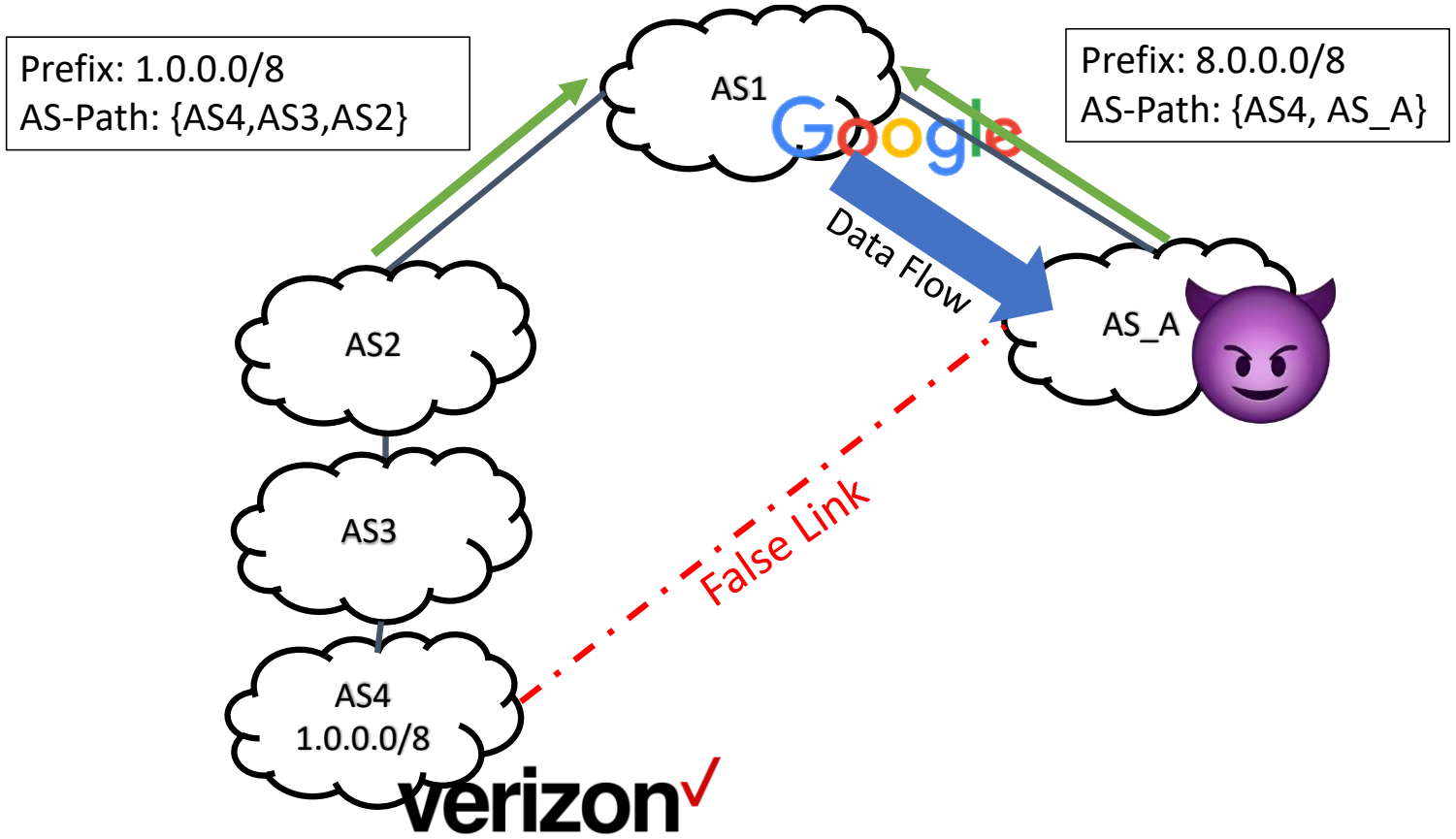
IP	Maxlength	ASN
8.8.8.8/32	32	AS3



DII invalidates incorrect BGP update:

AS1 does not hold 8.0.0.0/8.

Path Hijack

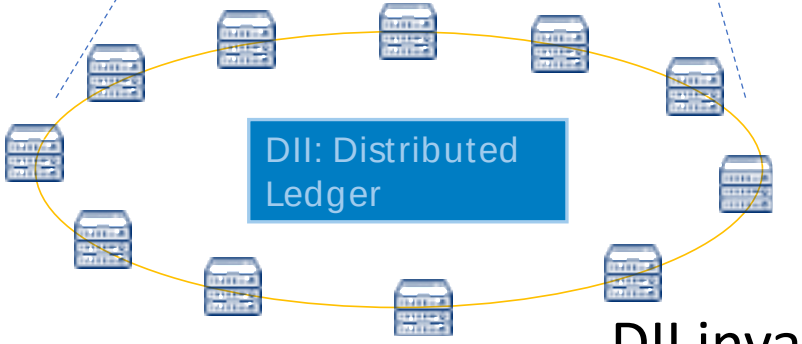


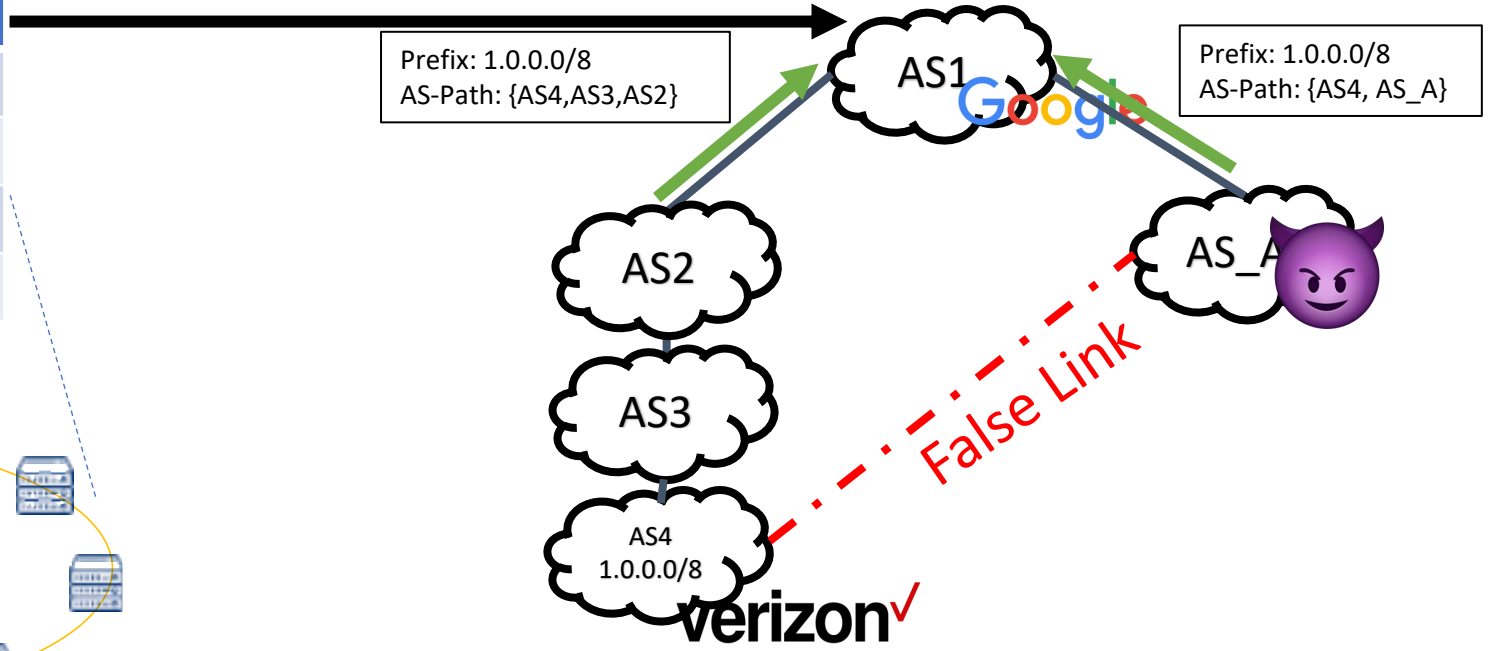
- A Path Hijack occurs when an As announces an incorrect path or link
- We need to **authenticate** AS adjacencies
- AS4 is not connected to AS_A

Protection against **path hijack**

AS Neighbor(ASN->ASN)

Source	Target
AS1	AS2
AS1	AS_A
AS2	AS3
AS3	AS4

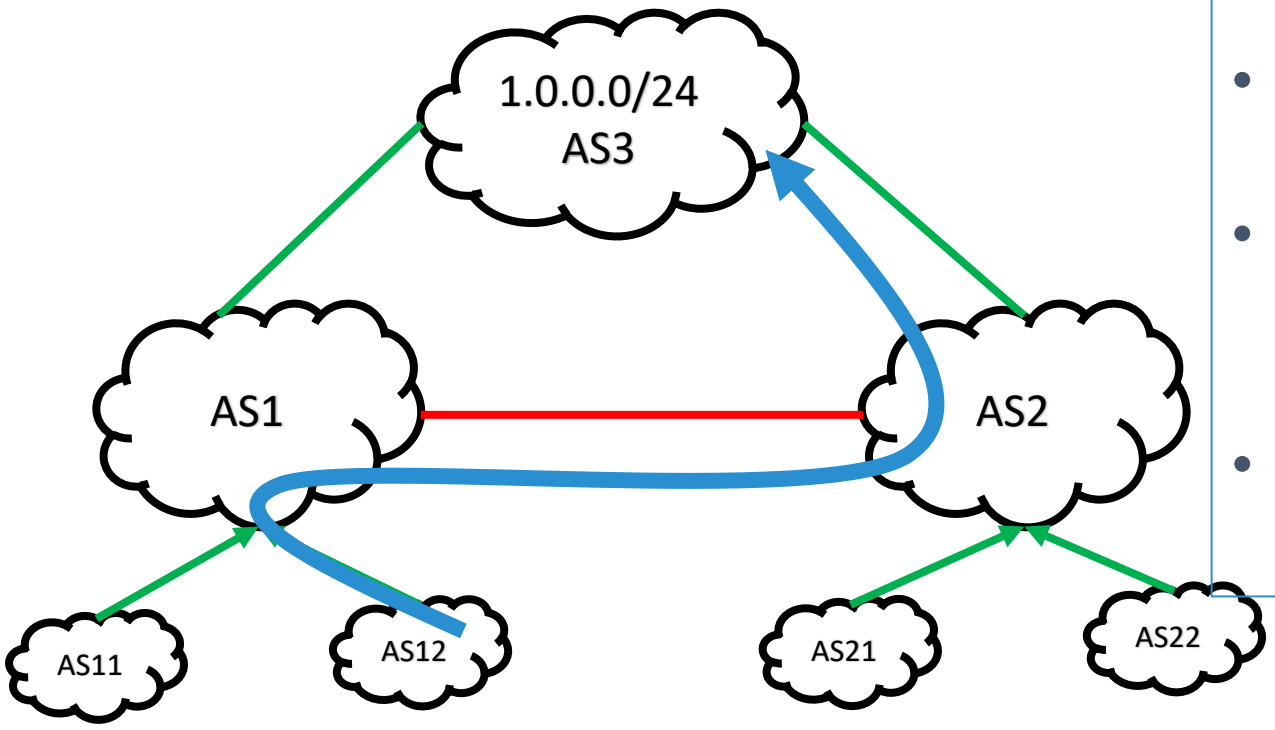




DII invalidates incorrect AS Path:

AS_A is **NOT** adjacent to AS4

Route Leaks

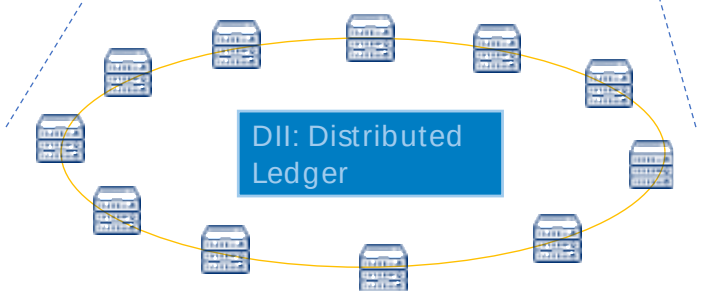


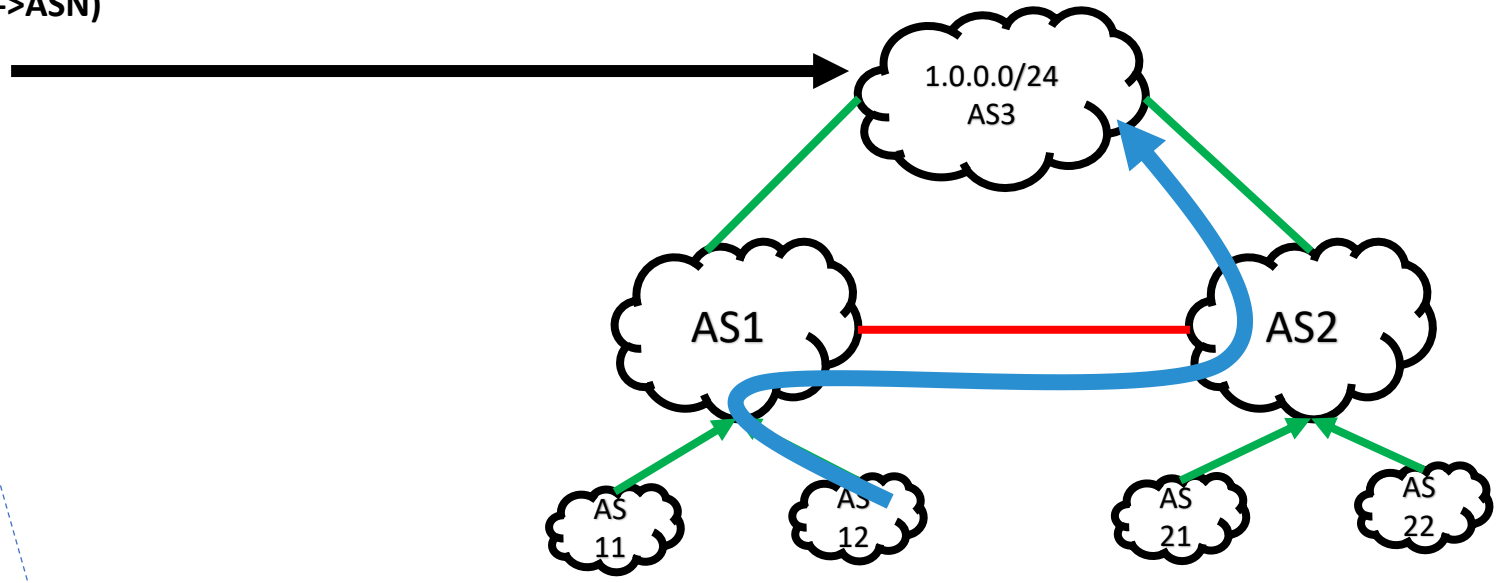
- **Customer Provider** links are typically paid
- The costs of **Peering** links is typically shared
- Routes learnt from upstream customer-provider links are not propagated through peering links
- Otherwise AS2 will offer free **transit** to AS1 (and its customers)

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





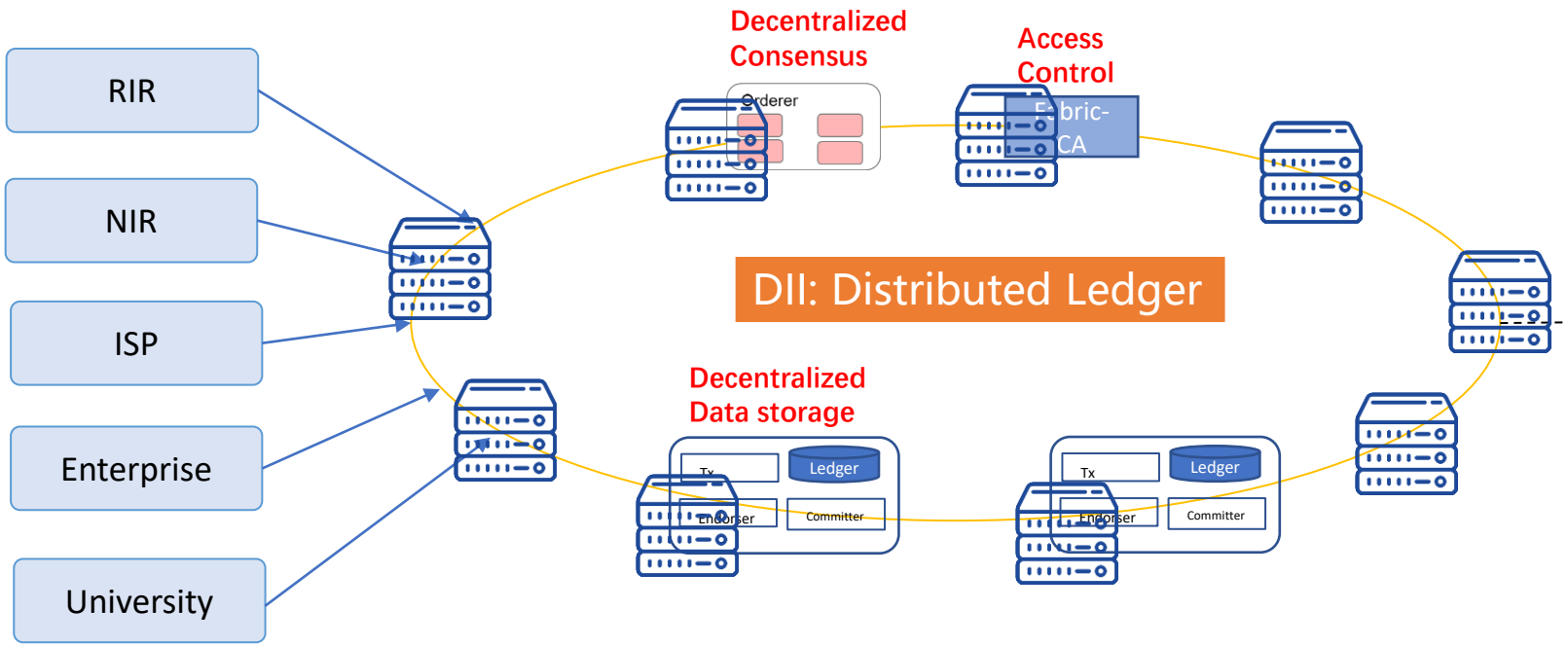
DII invalidates incorrect AS announcement:

AS1 and AS2 have a P2P relationship.

AS2 should not propagate routes learnt from AS1

DII Global Testbed

ETSI Bright Talk Demo



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

Only owner can create ROA record

IP Ownership

IP	Owner	Exp date
200	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

AS Neighbor(ASN->ASN)

Source	Target
AS100	AS200
AS200	AS300

AS Business Relationship(ASN->ASN)

Source	Target	Type
AS100	AS200	P2P
AS200	AS300	P2P

Only owner can create Neighbor record.

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

Completed
Stages and Milestones

PoC Technical Requirements

Requirement of DII	Descriptions	Related Feature of PDL
Permissioned control 	The participants of DII needed to be authorized.	Access Control
Resistance to Single point failure 	The resource management in DII doesn't depend on single authority.	Decentralized consensus protocol Peer-to-peer trust model. Agreement is made by a decentralized consensus protocol, run by all peers.
	The creation of records in DII should be trustable.	
	The records are tamper-resistant.	Decentralized data management Data is maintained by all peer nodes. All data operations are transparent, and data availability is much higher.
Trustable autonomous procedure 	Autonomous procedure can avoid the configuration errors and misbehavior.	Smart contract A Turing-complete computation model to support any decentralized application.
Trustable Transaction Capability 	Trustable transaction capability is important to Internet resource.	Transaction Peer nodes can send transactions between each other, enabling service monetization with inherent trust.

PoC Stages and Milestones

- Project Start: 01/07/2020
- PoC Demo 1: ETSI BrighTalk 15/09/2020
  - https://www.brighttalk.com/webcast/12761/433364
- PoC Demo 2 and 3: Cancelled due to COVID (see note 1 and 2 on original proposal)
- PoC Demo 3: Accepted Demo PoC to IEEE INFOCOM (15/01/2021)
  - IEEE INFOCOM is ranked Core A+ (http://portal.core.edu.au/conf-ranks/)
  - Strong impact on the Networking Academic and Industrial communities
  - Presented on May 12 Wed, 2:00 AM — 4:00 AM CEST
  - Most liked demo in the Demo Session
  - Video can be found at https://infocom.info/day/1 (registration required)
- PoC Contribution 1 – Smart contracts use and validation
- PoC Contribution 2 – Interconnection of Ledgers
- PoC Contribution 3 – Interconnection proof of requirements

Thanks!


Telefónica


UPC
UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH


UNIVERSIDAD CARLOS III DE MADRID
homo
homini
sacra
res


HUAWEI