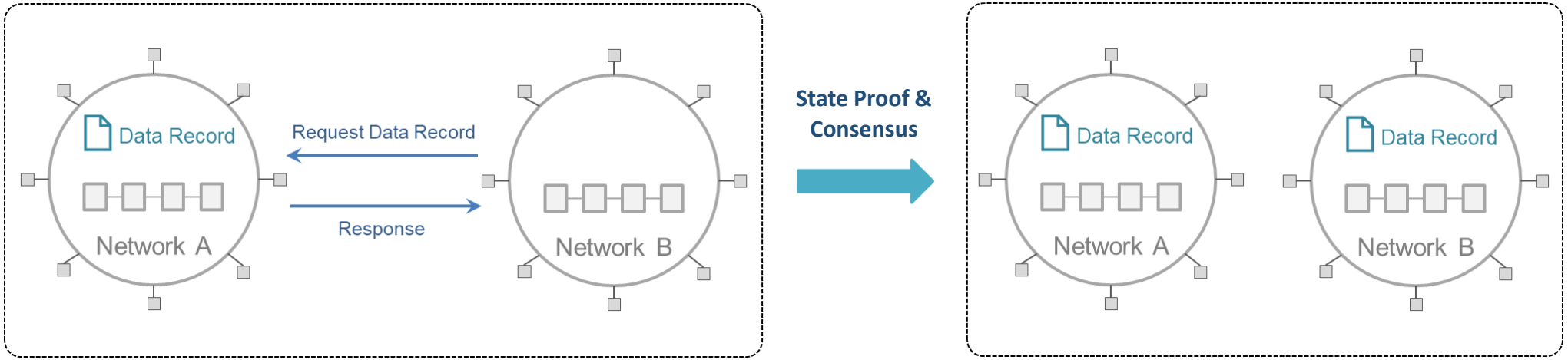
Blockchain Network Identity and Discovery

Bishakh Chandra Ghosh, IIT Kharagpur
Venkatraman Ramakrishna, IBM Research – India
Chander Govindarajan, IBM Research – India
Dushyant Behl, IBM Research – India
Dileban Karunamoorthy, (formerly in IBM Research – Australia)
Ermyas Abebe,Consensys (formerly in IBM Research – Australia)
Sandip Chakraborty, IIT Kharagpur

Background: Data Transfer/Sharing

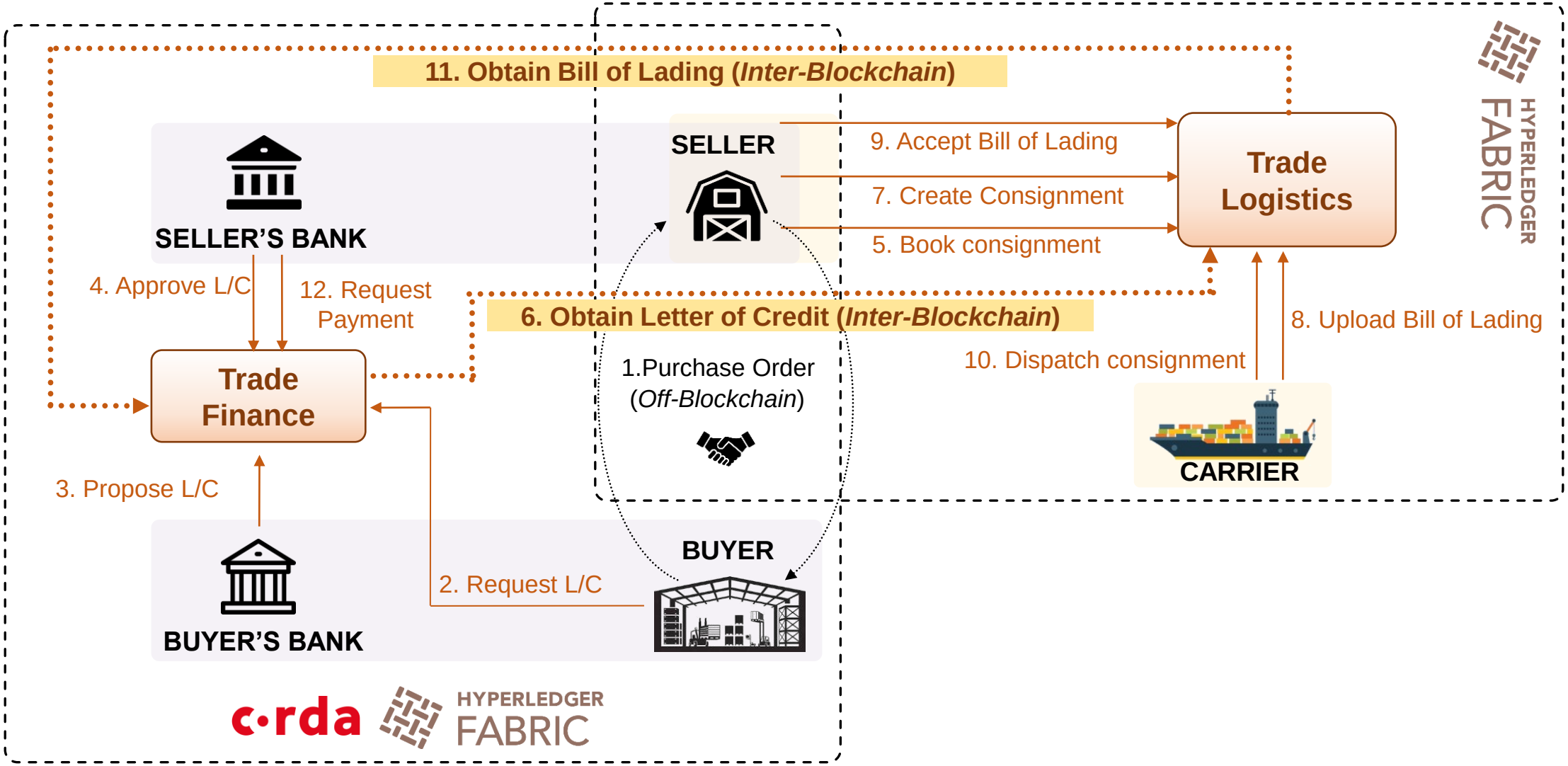


The transfer/sharing of data from a source ledger to a consuming ledger.

The data transfer can either be a result of a transaction in the source network, or an explicit request from a consuming network.

Presently being drafted for standardizing views, view addresses and request-response protocol

Use Case: Trade Finance and Logistics



Background and Summary

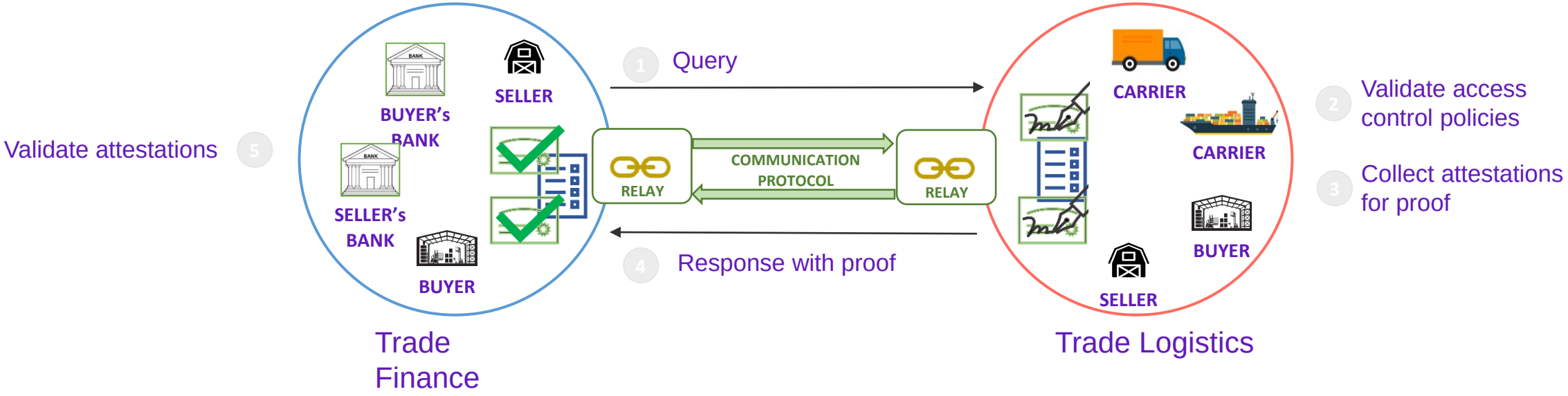
- Work started as an internship project in the summer of 2020
  - We had a decentralized protocol for cross-network transactions relying on trustworthy data sharing across ledgers
  - Which relied on each network somehow knowing the other's roots of trust (certification authorities)
  - *Goal*: a decentralized way of sharing trust/certification info, relying on existing identity records and credentials possessed by network members
  - *Dependencies*: decentralized identifiers, DID registries, VC/VP
  - *Output*: PoC for identity exchange backing data transfer protocol using HL Indy as a DID registry
- Presented a paper on the concept and protocol in ICBC 2021
- After interoperability project morphed into the Weaver framework in March 2021
  - Extrapolated specifications from PoC for generic DLT- and registry-agnostic system of identity exchange into Weaver RFCs (late 2021)
  - Implementation based on these specifications is ongoing: target is end of March 2022

System and PoC Developed in 2020 and Presented in ICBC 2021

Proof by Attestation

Abebe, et al. "Enabling enterprise blockchain interoperability with trusted data transfer (industry track)." *Middleware* 2019.

- **Relay-Based Interoperability Using Proofs and Attestations**
- Supports Multi-party trust
- Uses existing endorsement / validation mechanisms of the blockchain platforms such as Fabric, Corda etc.

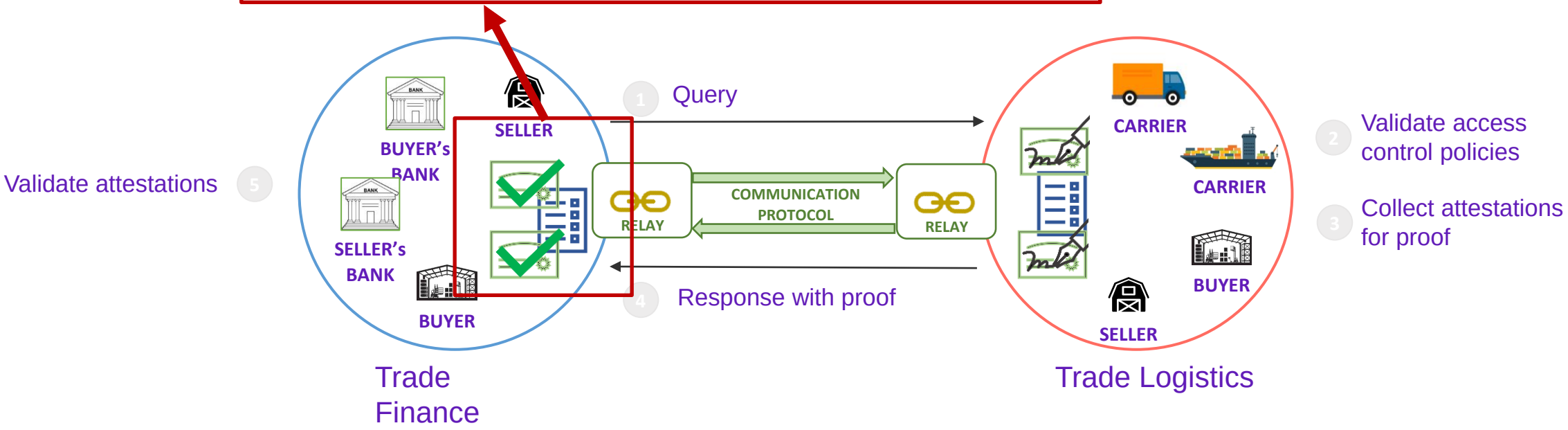


Proof by Attestation

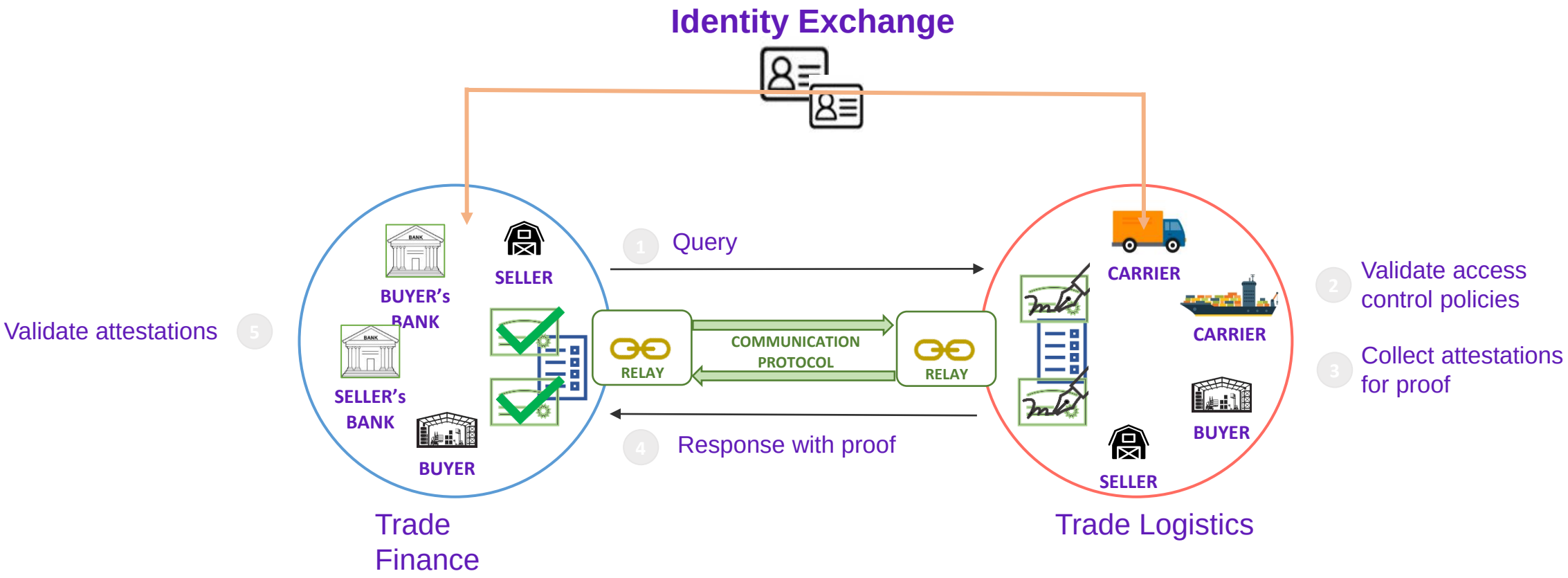
Abebe, et al. "Enabling enterprise blockchain interoperability with trusted data transfer (industry track)." *Middleware* 2019.

- Relay-Based Interoperability Using Proofs and Attestati
- Supports
- Uses exis
  the block

- Depends on public key / certificates of participants of foreign network.
- **Identity configuration is a requirement**

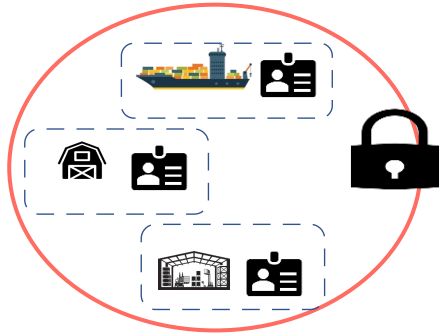


Identity Configuration



Challenges

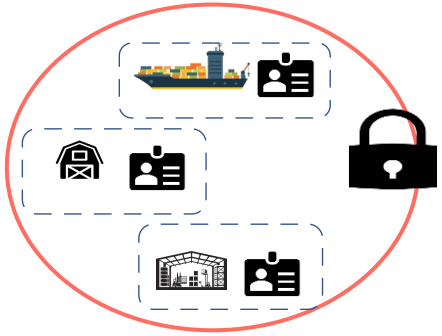
- **Identity within closed networks have no manifestation outside**
- **Platform heterogeneity**
- **Identity management heterogeneity**
- **Lack of common identity infrastructure**
- **Security**
- **Consensus on identity**



HYPERLEDGER FABRIC

HYPERLEDGER BURROW

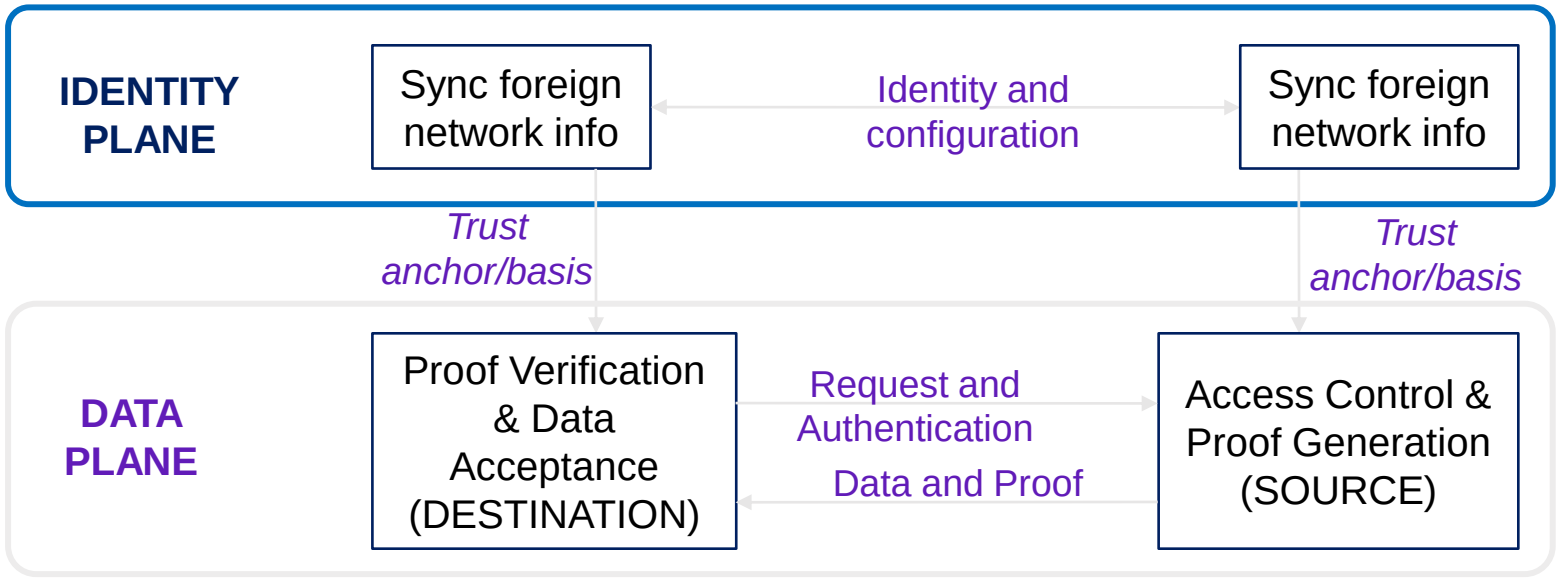
corda



Design Goals

- **DLT Agnostic**
  - The solution should not be tied to, or only applicable for, any particular DLT.
- **No central identity registry**
  - Networks should be free to choose identity registries and providers (or use their existing ones).
- **Networks remain autonomous**
  - Networks must retain their autonomy while gaining the ability to interoperate universally.
- **Minimal change to existing code and configurations**
  - No change should be required in a network’s regular operations.
  - Minimal changes to existing code and configurations of already deployed networks.

Solution Overview



Exchange and configuration of identity

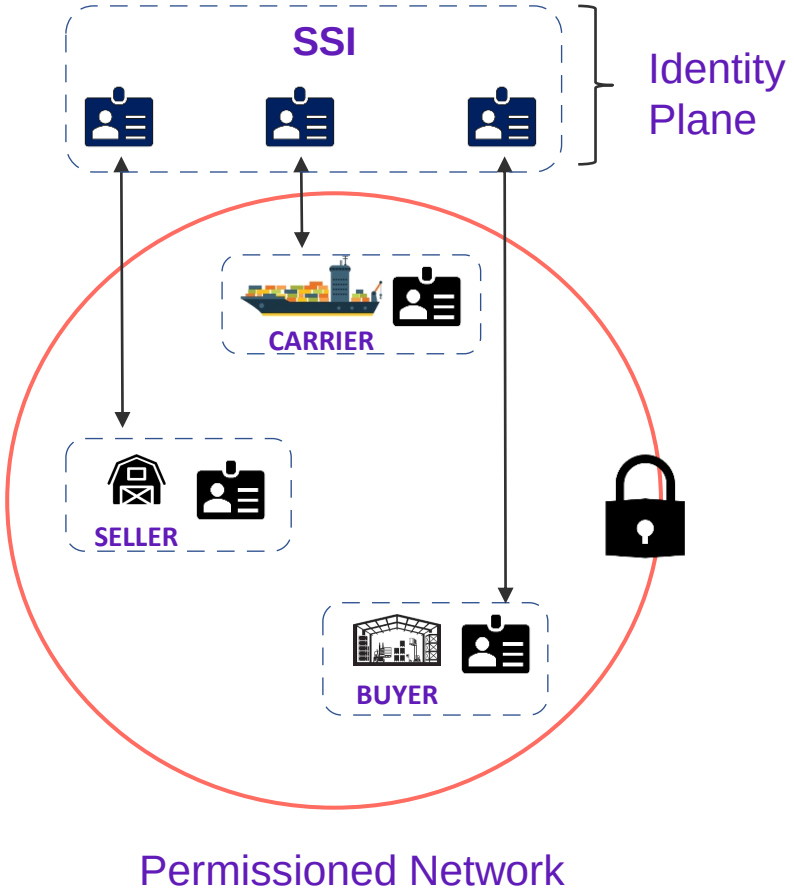
Data requests and proof validation.

Decoupling Identity from Network

- Blockchain network specific identity is confined within its boundary.

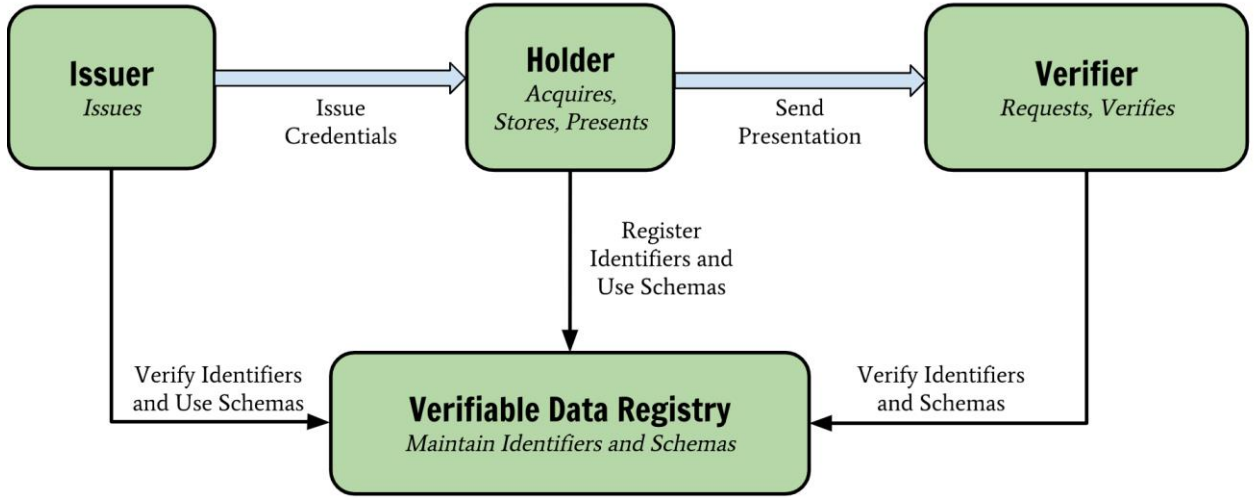
- For identity exchange identity needs to be:
  - Platform agnostic
  - Decoupled from the network

- We use **self-sovereign identity (SSI)** in the identity plane.



Building Blocks

- **Decentralized Identifiers (DIDs)**
  - SSI independent of any registry or provider
- **Verifiable Credentials (VCs)**
  - Digital credentials issued to a DID
- **Verifiable Data Registry (VDR)**
  - Decentralized implementation –DLT based
  - Schema of VCs
  - Revocation lists



https://www.w3.org/TR/vc-data-model/

Trust Anchors

- No central identity provider
- Trust anchors act as basis for identity validation

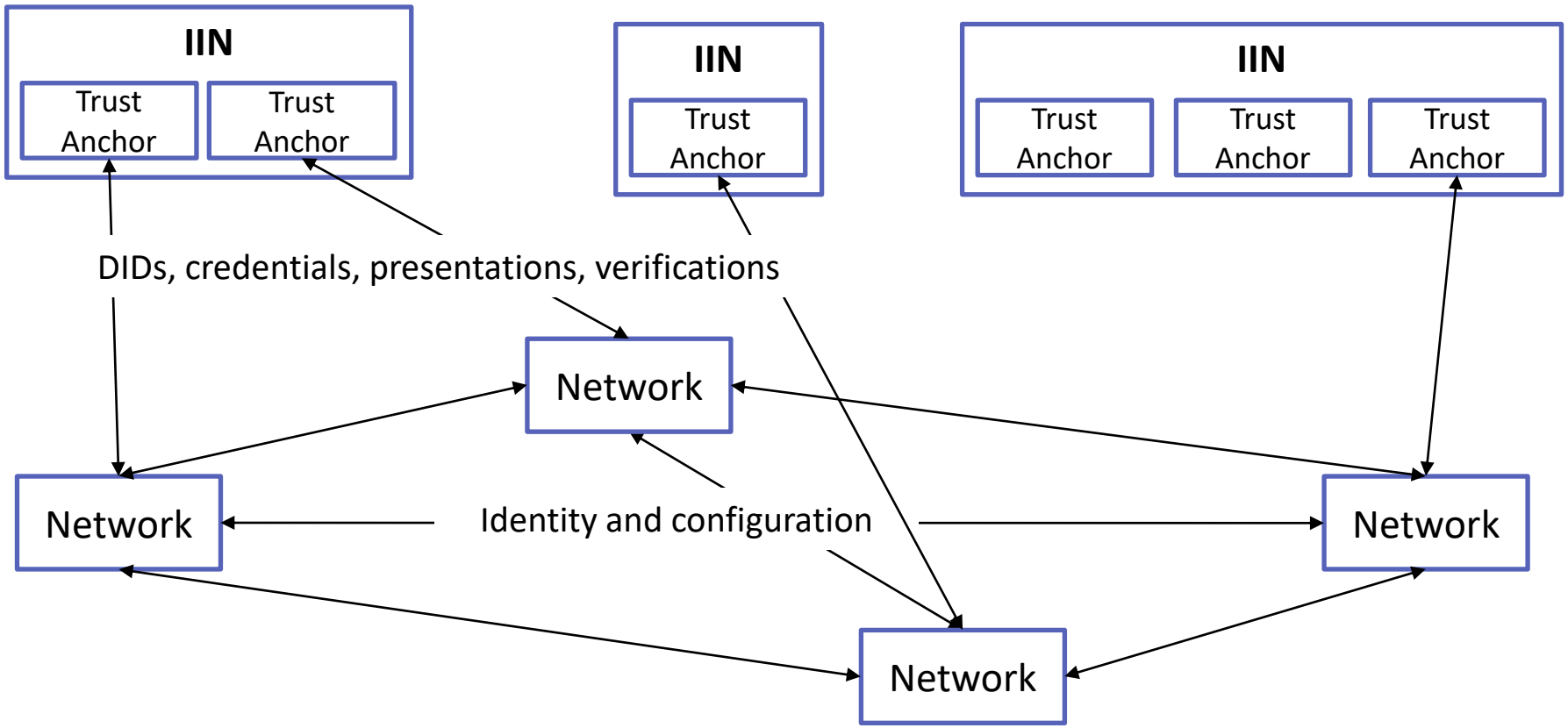
A. Organization Identity validators (OINs)

- DID by default is not associated with any real-world identity.
- OINs are trust anchors with well known real world identities.
- OINs associate DIDs to their real-world identity.

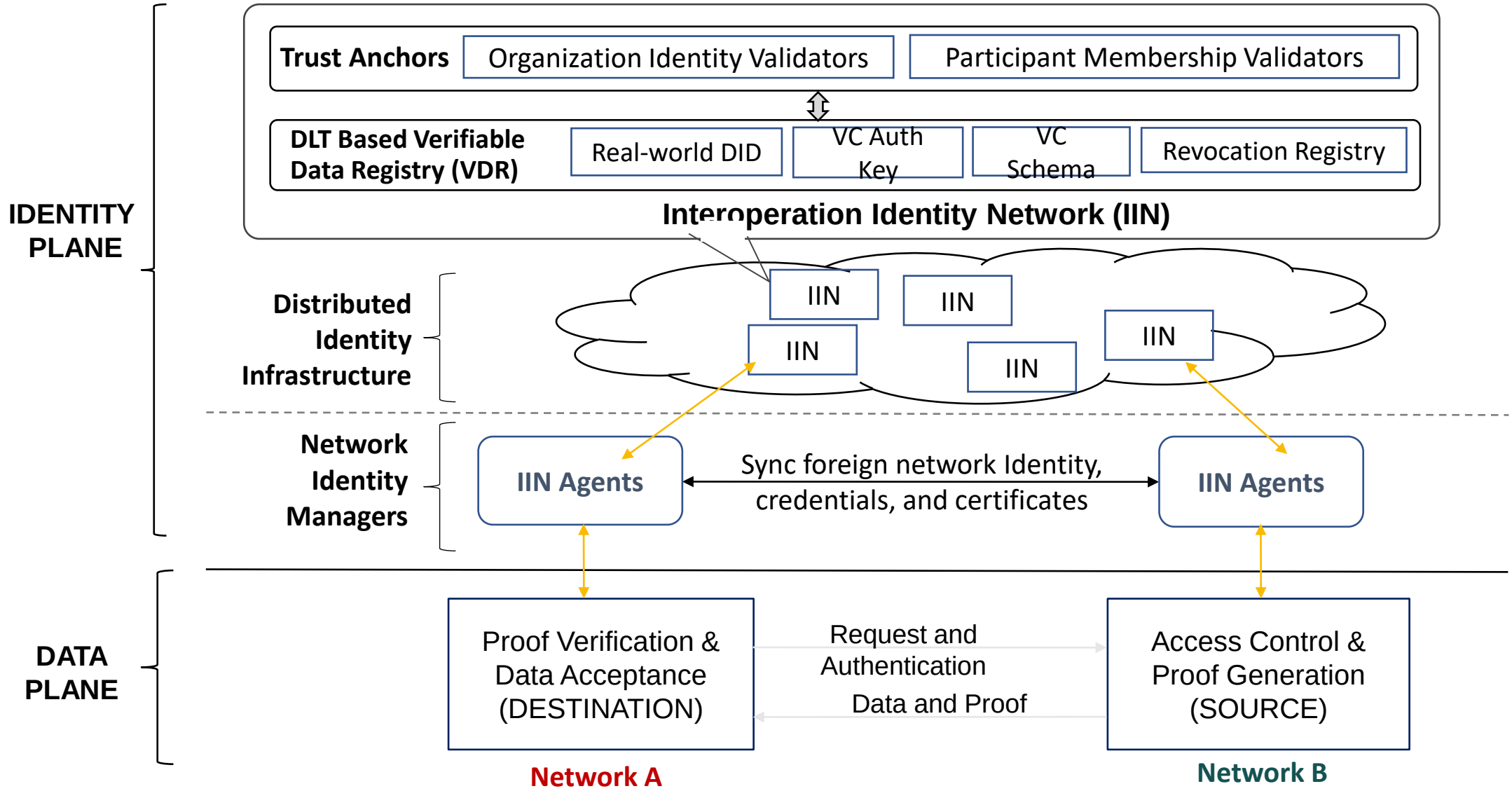
B. Participant membership validators (PMVs)

- Validate membership of a DID owner in a permissioned consortium.
- PMVs are trust anchors that are well known representatives of certain networks.
  Eg: IBM or Walmart, both reputed entities, could act as validators for the membership of the *IBM Food Trust* network, since they are well k[illegible]ticipants in the same.

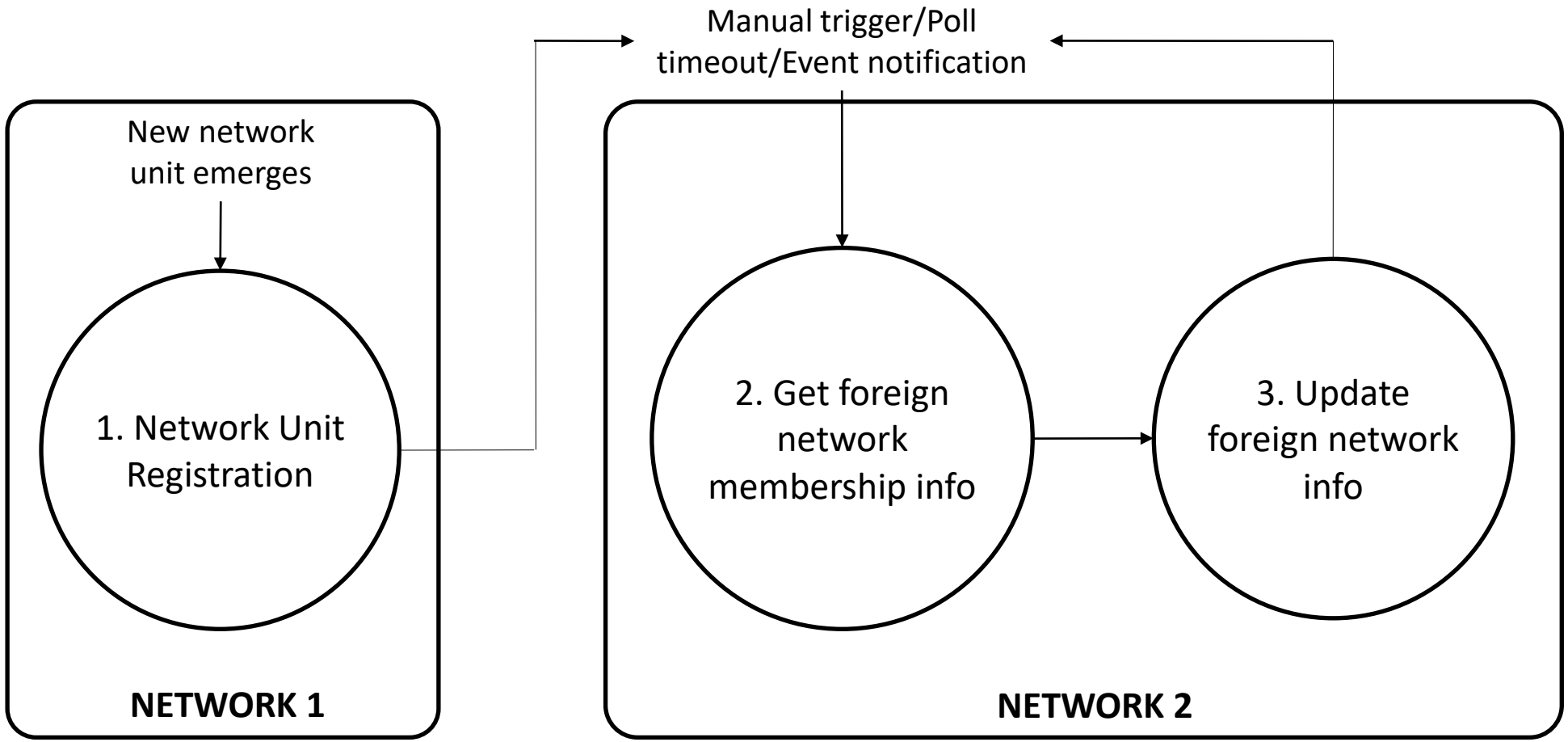
Identity Plane Architecture



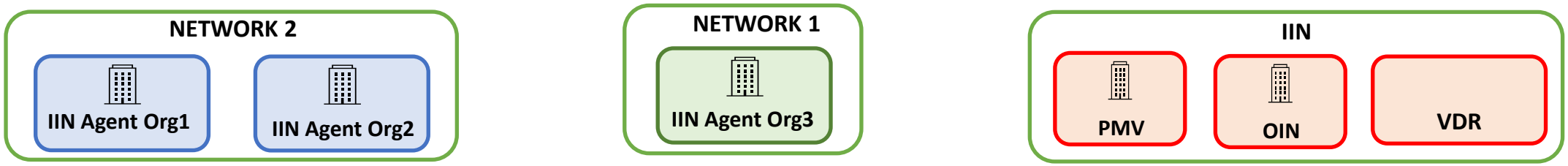
Identity Plane Architecture



Protocol Phases

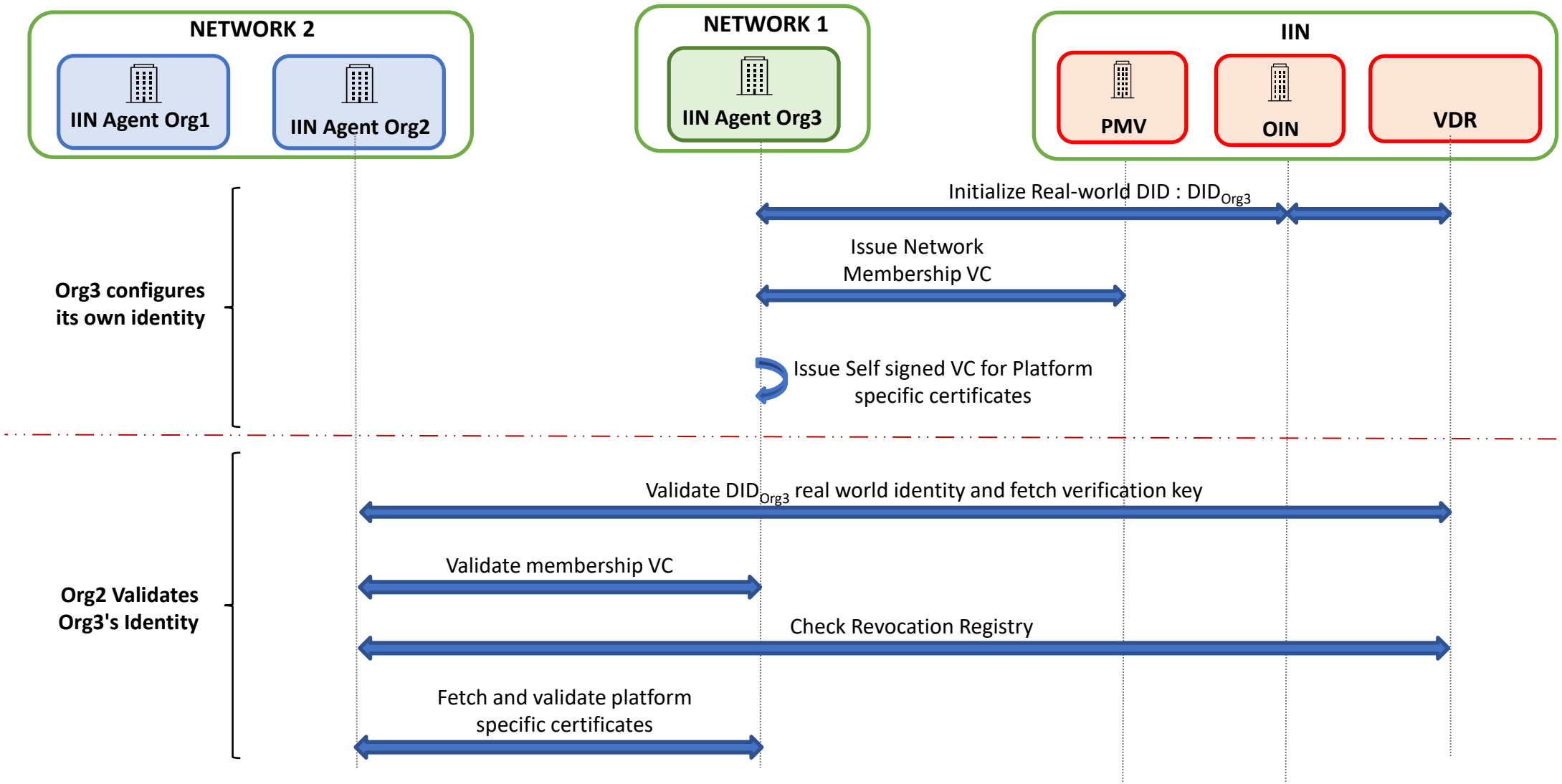


Cross-Network Participant Validation Protocol Overview

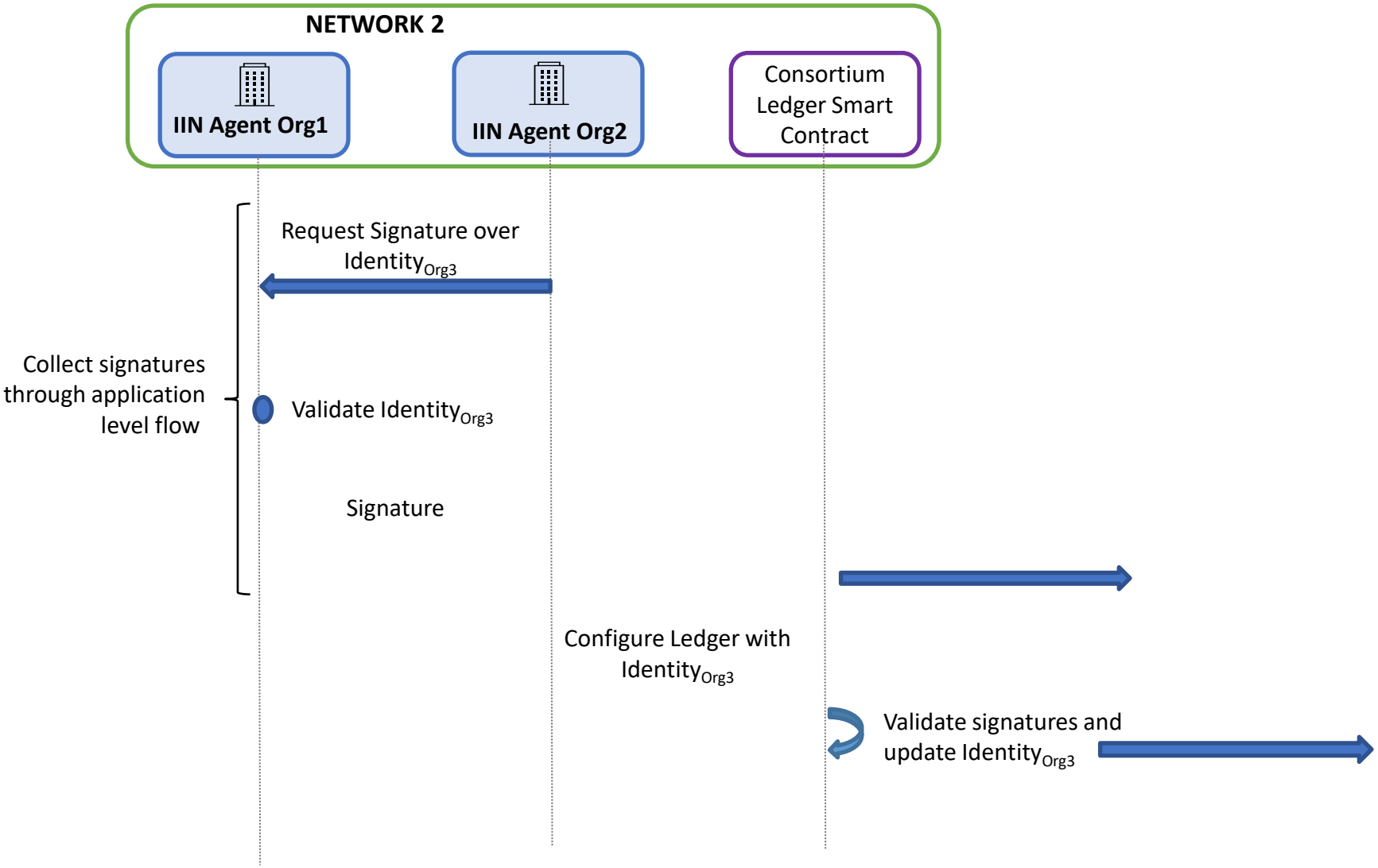


- **NETWORK 2 is configuring the identity of Org3 of NETWORK 1**

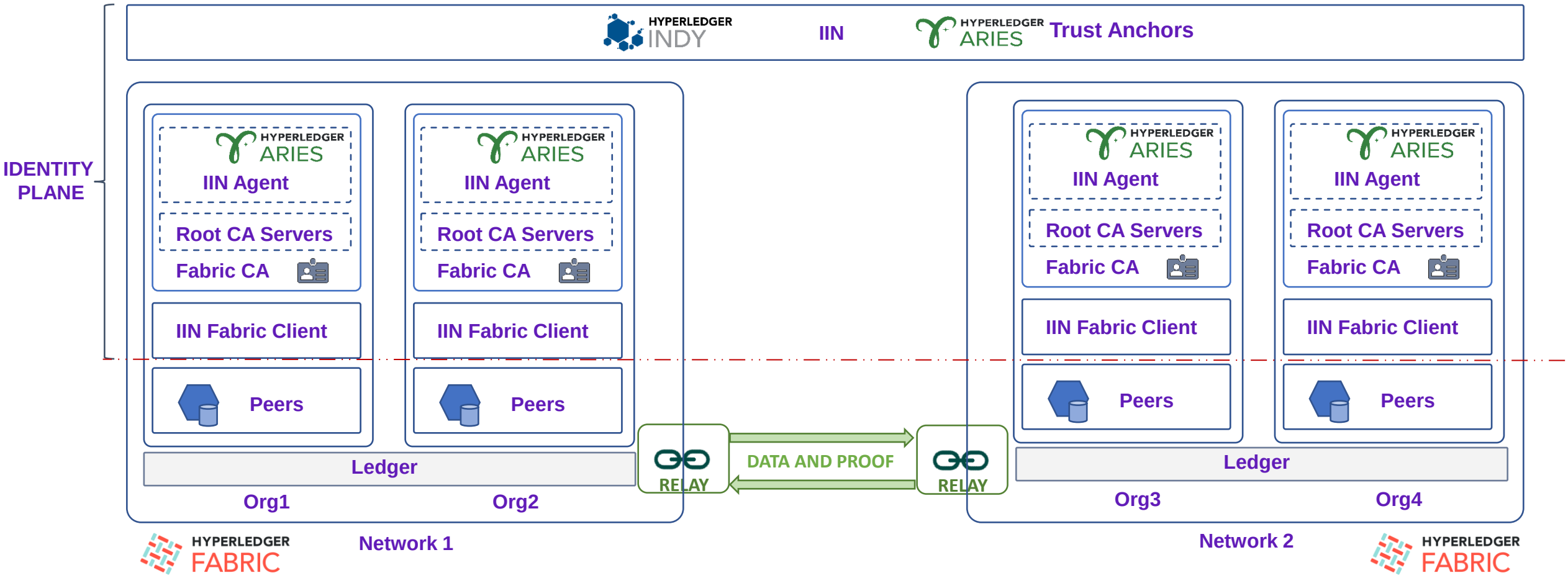
Cross-Network Participant Validation Protocol Overview



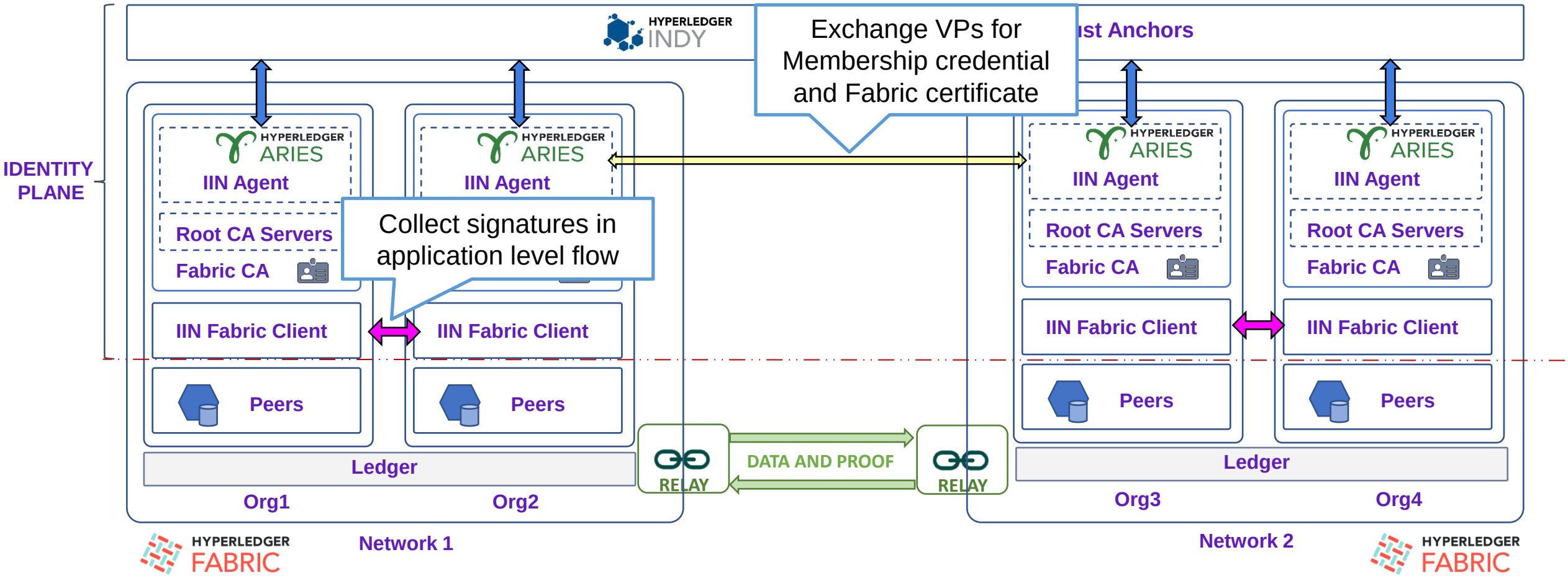
Cross-Network Participant Validation Protocol Overview



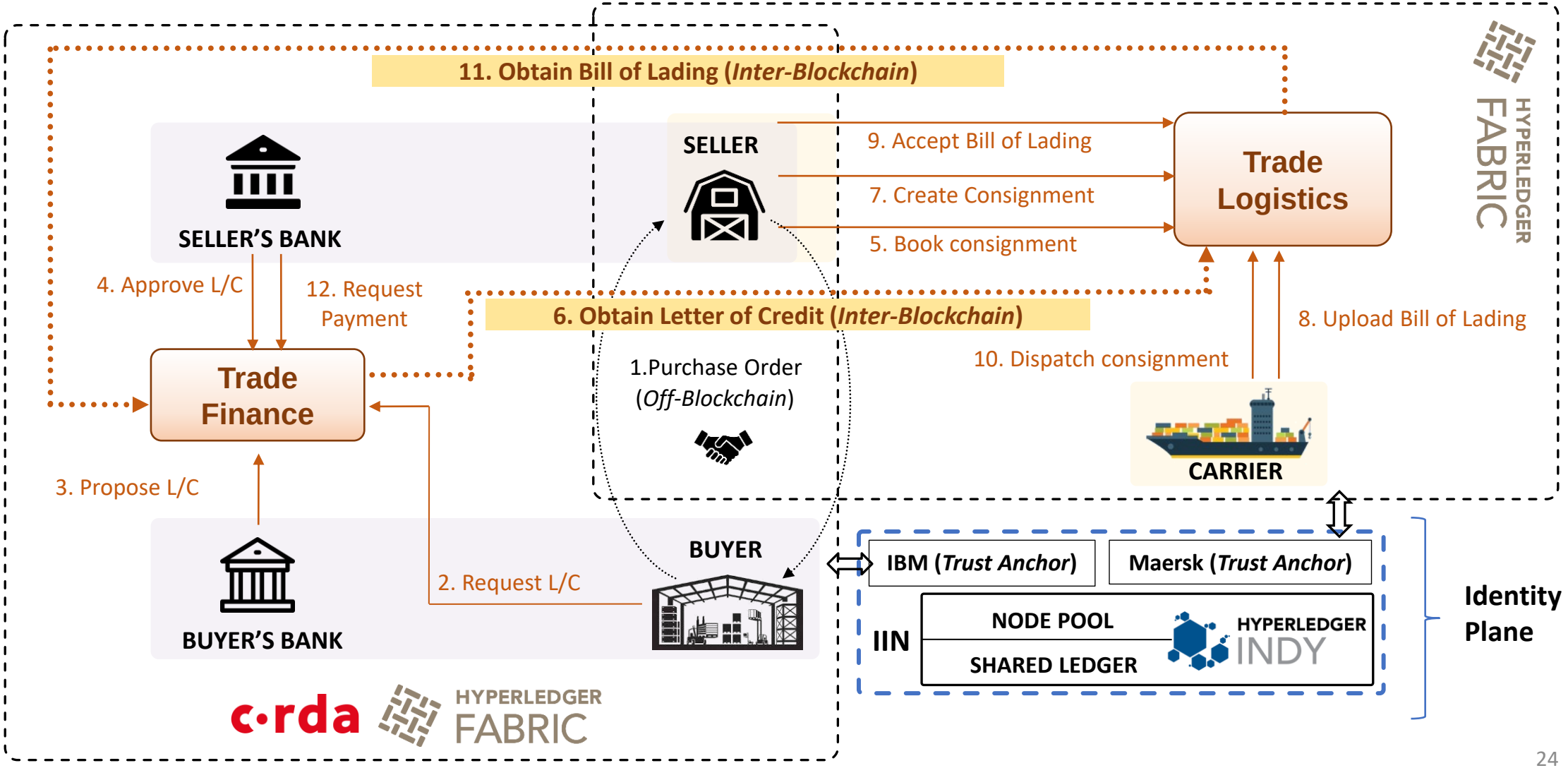
Implementation



Implementation



Use Case Augmented



Weaver RFC Specifications for Cross-Network Identity Exchange (Extrapolated from PoC)

From PoC to Specs (and Possibly Draft Standards)

- Support arbitrary number of IINs rather than a single global registry-on-a-ledger
- Specify the capabilities of an IIN as an augmentation of existing decentralized identity registries but also support existing registries in exchange protocols
  - Allow network participants and network consortiums to use existing decentralized identity registries instead of necessarily having to create one or more just for interoperation
  - (Reuse existing DIDs and VCs similarly)
- Provide different ways of creating and discovering network groups instead of just depending on some well-known trust anchor
  - Move from using an arbitrarily defined VC for a network group (i.e., member-list) to using a group DID that aligns with W3C draft proposals
  - Allows different trust models (traded off with simplicity) to be used by networks that wish to trade data and assets (i.e., interoperate)

Network DID

- Identity of a network as a single entity.
- Network discovery and validation without involving individual members.

Network DID Document

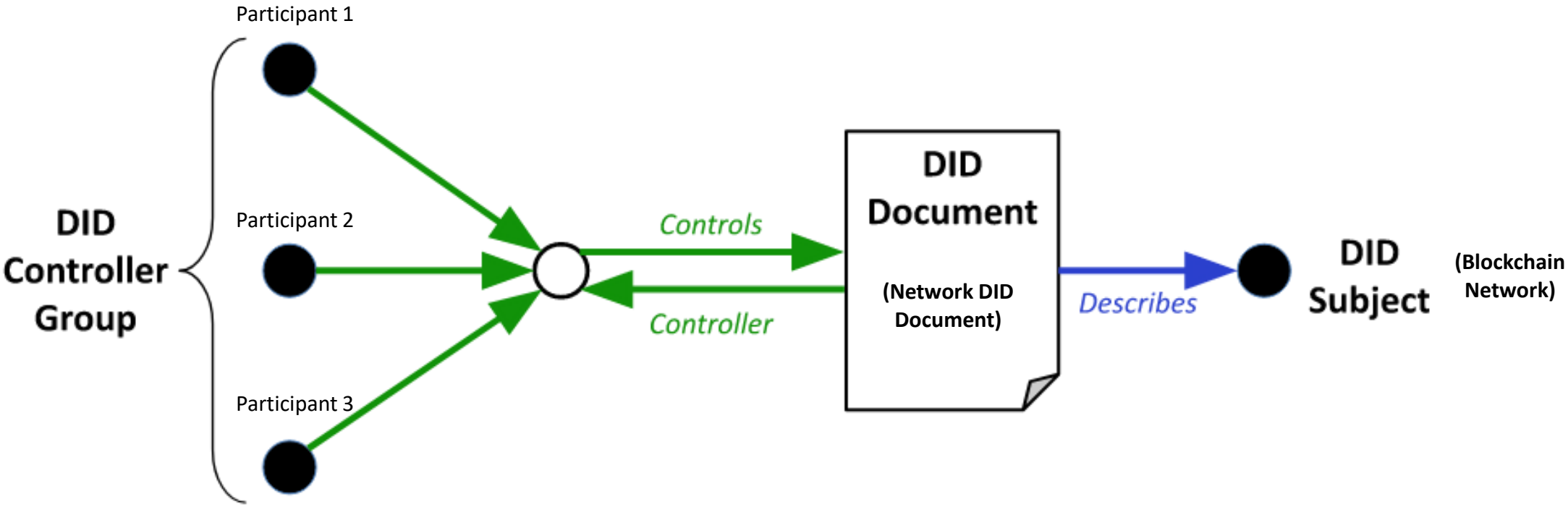
did:iin:tradelens

networkParticipants

verificationMethod:
- Group Controller
  - did:iin:participant1
  - did:iin:participant2
  - did:iin2:participant 3
  - …

relayEndpoints

Group Control



Group Creation and Updates

- Network DID Creation
  - Requires attestation by **each** network participant.

    IIN Ledger validates each participant's signature by resolving their individual DIDs.

- Network DID Updates
  - DID Document has Verification method type - "BlockchainNetworkMultiSig"
  - Contains "updatePolicy"
    - Follows "VerifiableCondition2021" (https://www.w3.org/TR/did-spec-registries/#verifiablecondition2021)
  - Update requests requires attestation to satisfy the update policy + attestation by any new members included in the network.

Group Creation and Updates

- Example: (Participant1 and (Participant2 OR Participant3))

```
"updatePolicy": {
  "id": "did:<iin_name>:<network_name>#updatepolicy",
  "controller": "did:<iin_name>:<network_name>",
  "type": "VerifiableCondition2021",
  "conditionAnd": [{
      "id": "did:<iin_name>:<network_name>#updatepolicy-1",
      "controller": "did:<iin_name>:<network_name>",
      "type": "VerifiableCondition2021",
      "conditionOr": ["did:<iin_name>:<network_participant_3>#key1",
        "did:<iin_name>:<network_participant_2>#key3"
      ]
    },
    "did:<iin_name>:<network_participant_1>#key1"
  ]
}
```

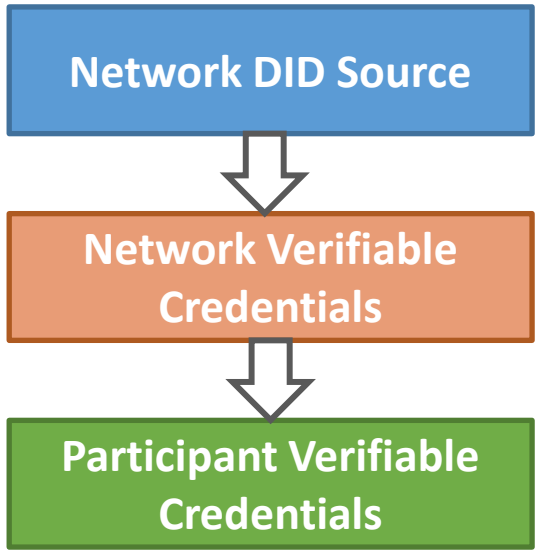
Discovery

- Obtaining the Network DID is sufficient to start configuring identities for interoperation.
  - Eg: **did:iin:tradelens** resolves to the DID document containing DIDs of all its participants.
  - The IIN DID registry acts as the network name resolver.

- The Network DID may be distributed by various means:
  - Website of the network / network participants (Might not be trustworthy).
  - Trusted source such as offline physical agreements with the concerned participant entities.
  - Advertisements, etc..

Identity Validation

- Trust Basis



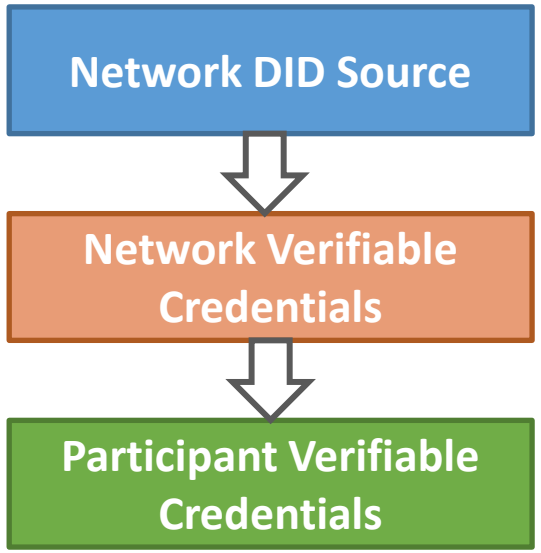
Eg: Offline Agreements, Trusted Website

VCs attesting the identity of the Network DID
e.g. VC attesting *did:iin:tradelens* is the *TradeLens* network.

VCs identity and memberships of individual participants.

Identity Validation

- Trust Basis



- Resolve DID Document from IIN registry.

- Trust anchors issue VC to the Network DID attesting its identity.
- Network presents VP to the validator.
  - Presentation can only be made by multisignature attestation of the group controller.

- - Same as older approach.
- Trust anchors issue identity and membership VC to participants.
- Validator validates VP from each participant.

Configuring Network Specific Identities

Same protocol as covered in the earlier slides

Conclusion

- Decentralized identity management plane for facilitating interoperation.
- DLT agnostic architecture
- Based on SSI and Verifiable Credential concepts
- No changes to existing DLT platform is required. Only some additional smart contracts for identity registry is required.

Thank You