IEEE ICBC
IEEE International Conference on Blockchain and Cryptocurrency
3-6 May 2021 // Virtual Conference

Decentralized Cross-Network Identity Management for Blockchain Interoperation

Bishakh Chandra Ghosh, Venkatraman Ramakrishna, Chander Govindarajan, Dushyant Behl, Dileban Karunamoorthy, Ermyas Abebe and **Sandip Chakraborty**

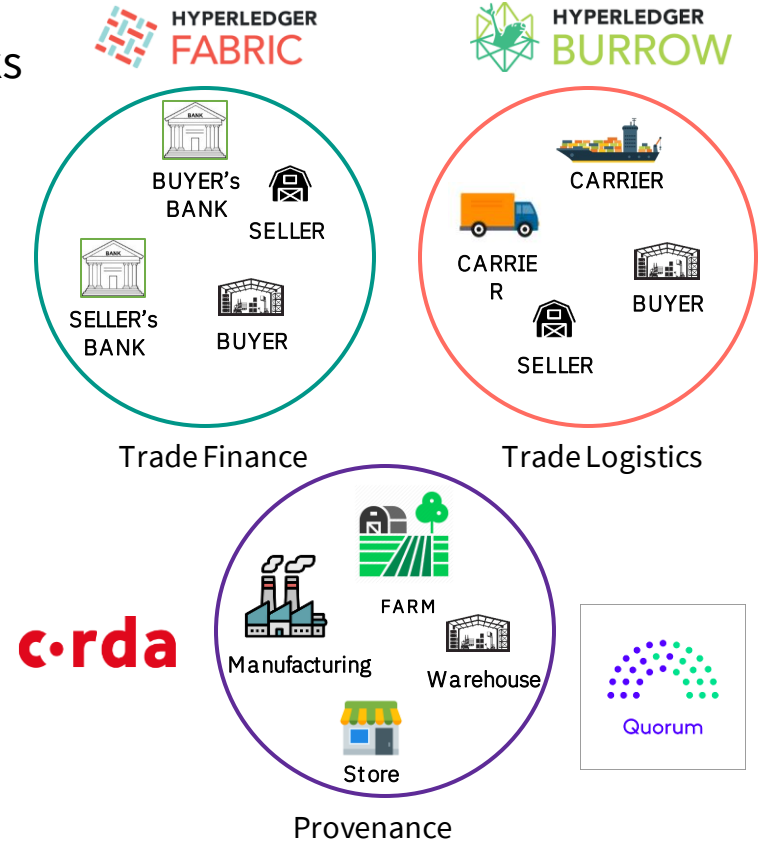
Indian Institute of Technology Kharagpur and IBM Research

IBM

Presenter: Bishakh Chandra Ghosh

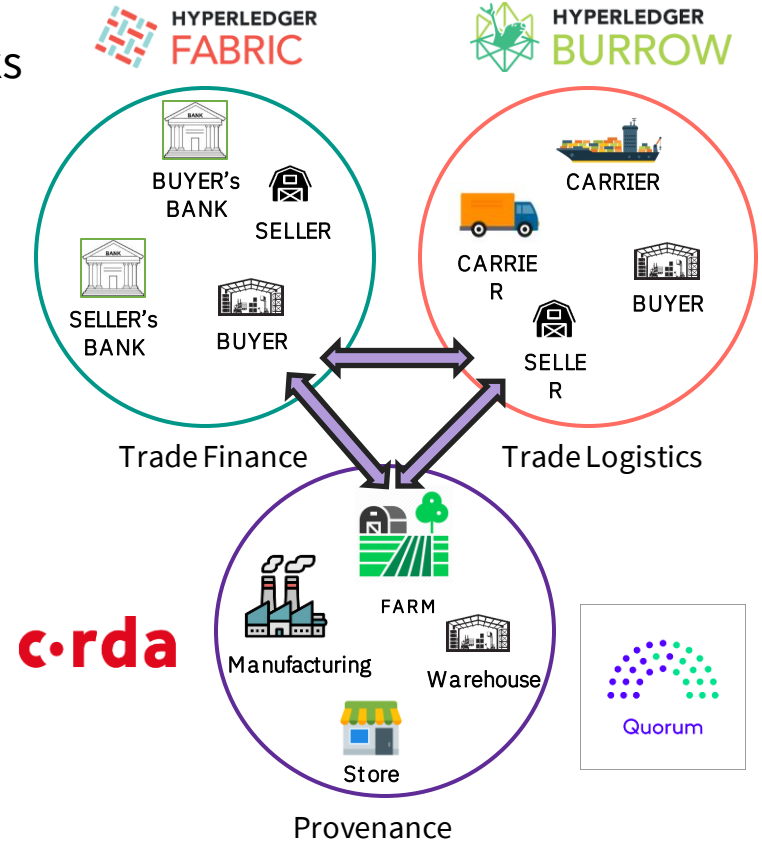
Blockchain Interoperability

- Industry trend to create consortium networks as **minimum viable ecosystems**
  - with the minimum set of participants required to demonstrate short-term benefits
- **Different blockchain platforms**



Blockchain Interoperability

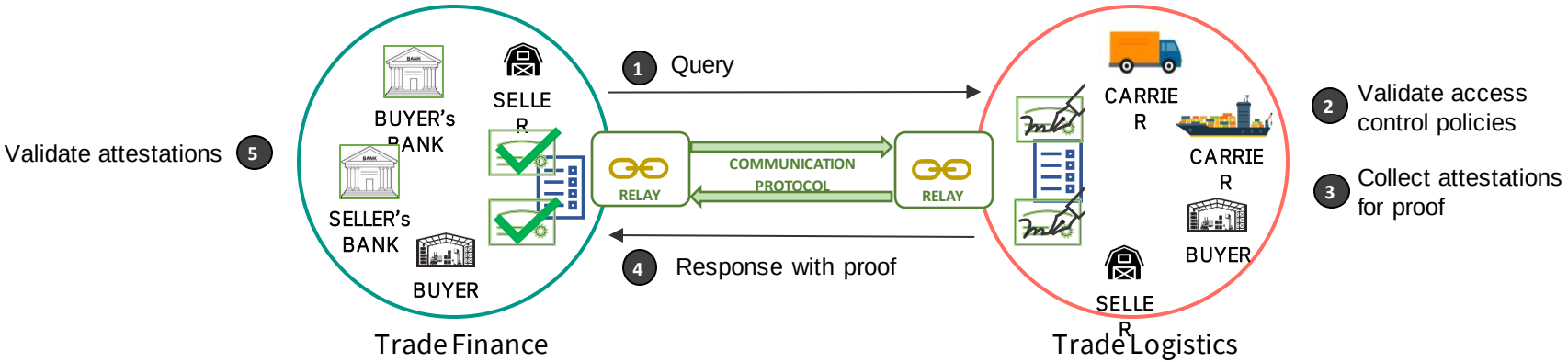
- Industry trend to create consortium networks as **minimum viable ecosystems**
  - with the minimum set of participants required to demonstrate short-term benefits
- **Different blockchain platforms**
- **Interoperability**
  - For business goals.
  - **Verifiable Data transfer**



Proof by Attestation

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

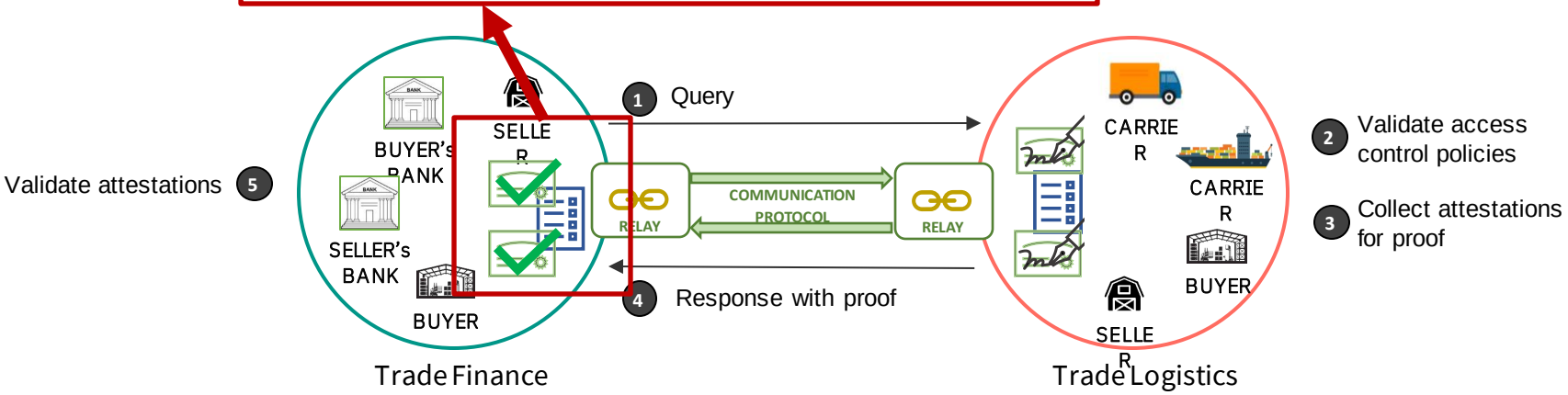
- **Relay-Based Interoperability Using Proofs and Attestations**
- Supports Multi-party trust
- Uses existing endorsement / validation mechanisms of the blockchain platforms such as Fabric, Corda etc..



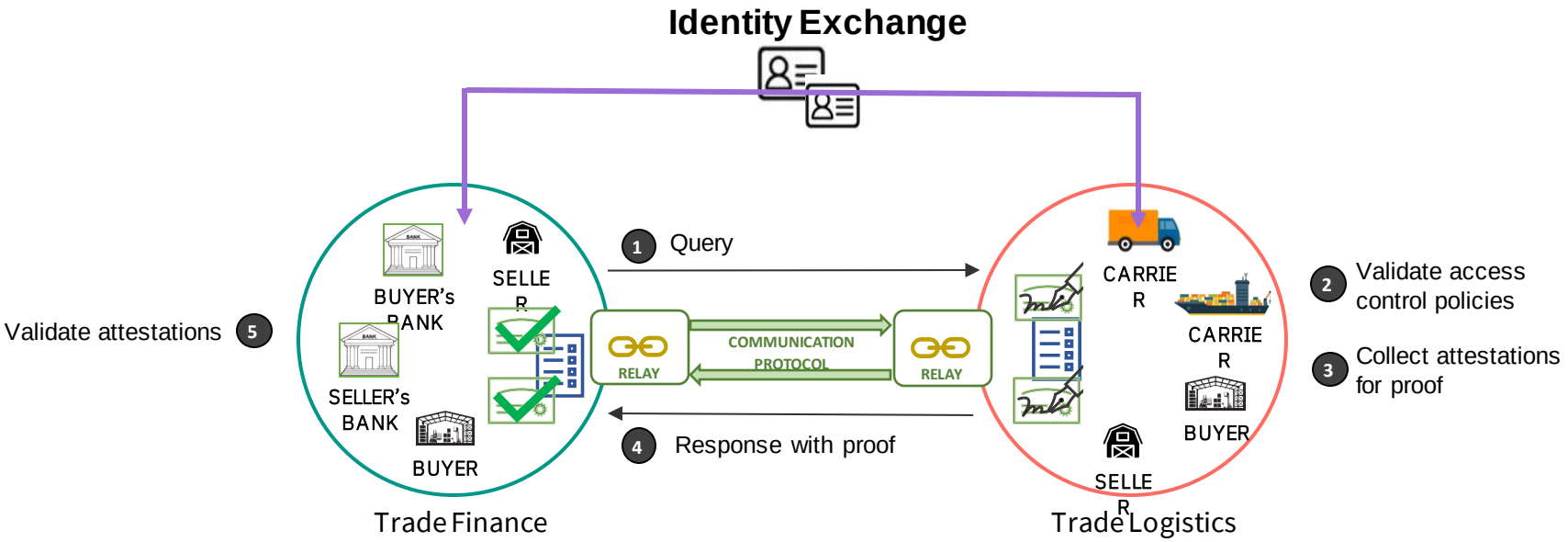
Proof by Attestation

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

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



Identity Configuration

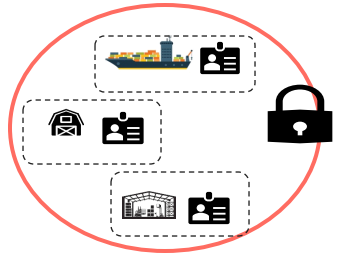


Objective

To design a secure distributed identity management infrastructure with a set of protocols linking permissioned networks, laying the basis for blockchain interoperation.

Challenges

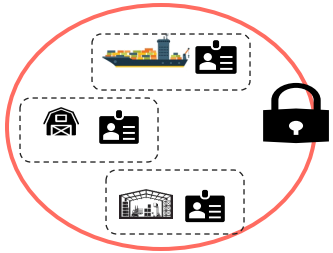
- **Identity within closed networks have no manifestation outside**
- **Platform heterogeneity**
- **Identity management heterogeneity**
- **Lack of common identity infrastructure**
- **Security**
- **Consensus on identity**



HYPERLEDGER FABRIC

HYPERLEDGER BURROW

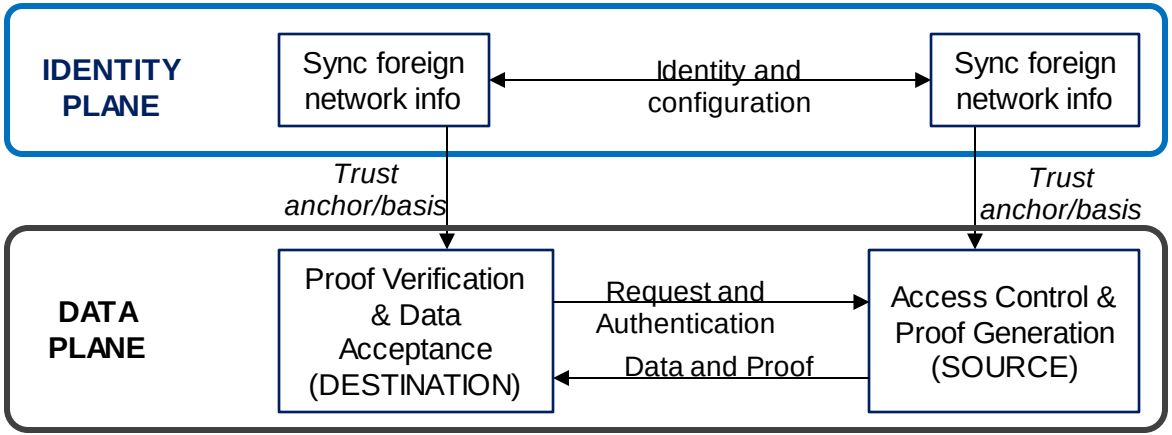
corda



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



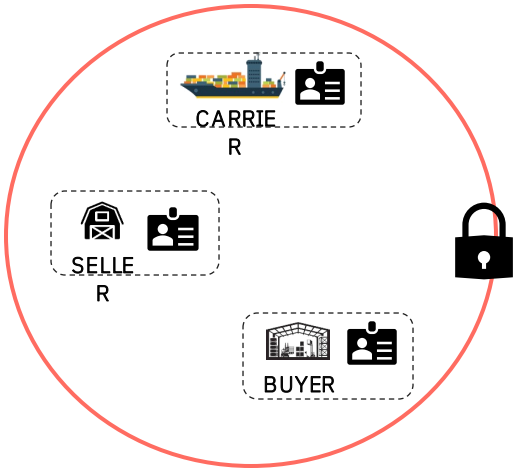
Exchange and configuration of identity

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



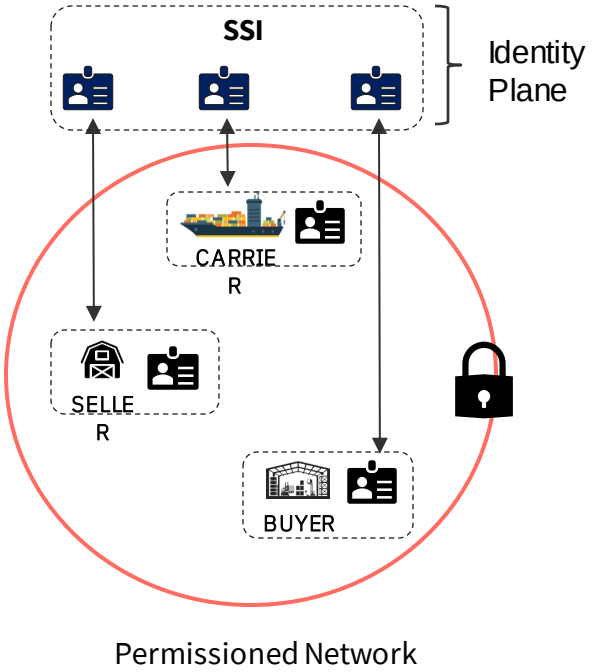
Permissioned Network

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

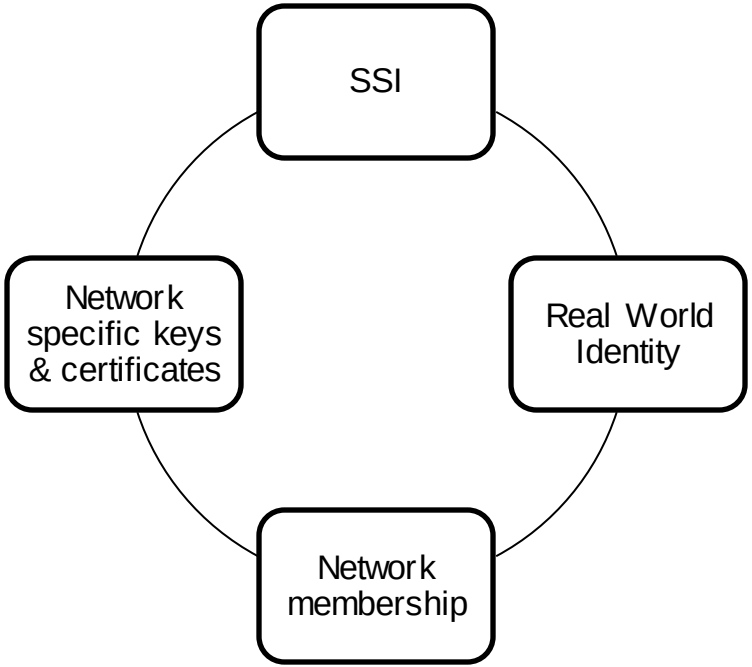
- We use **self-sovereign identity (SSI)** in the identity plane.



Identity Mappings

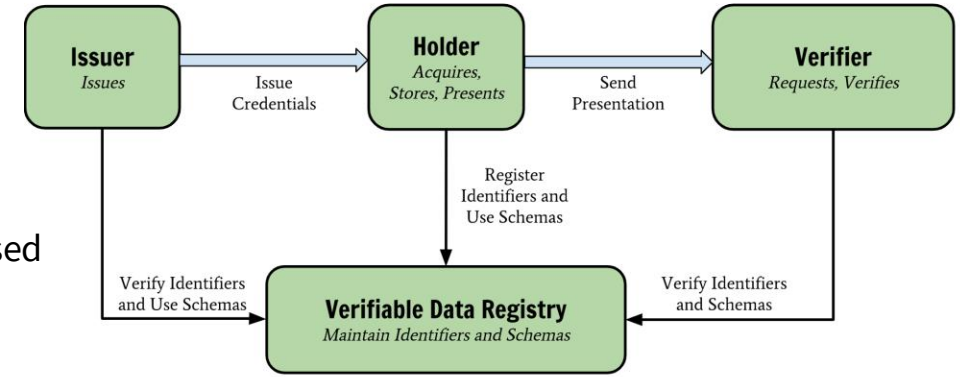
For interoperation, the following identity information of a participant must be validated:

- Real World Identity
  - Eg. Company name, address, etc..
- Network membership
  - Proof that the subject is a participant of the concerned network.
- Blockchain platform specific cryptographic keys & certificates
  - For validating attestations in data 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

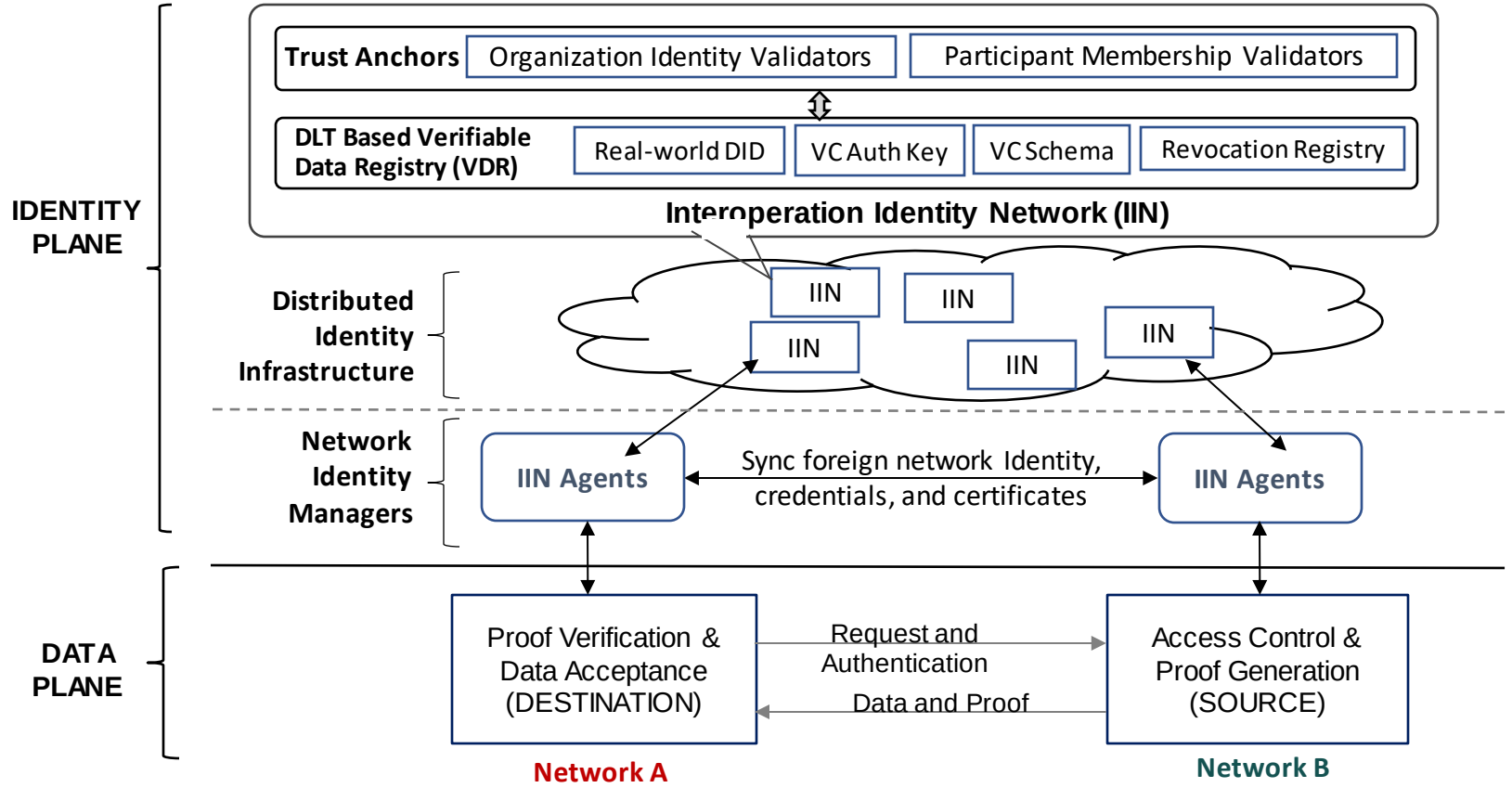
A. Organization Identity validators (OINs)

- 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.

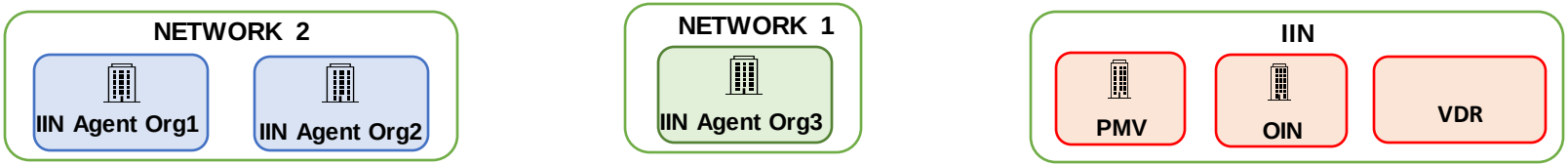
B. Participant membership validators (PMVs)

- 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 known key participants in the same.

Identity Plane Architecture

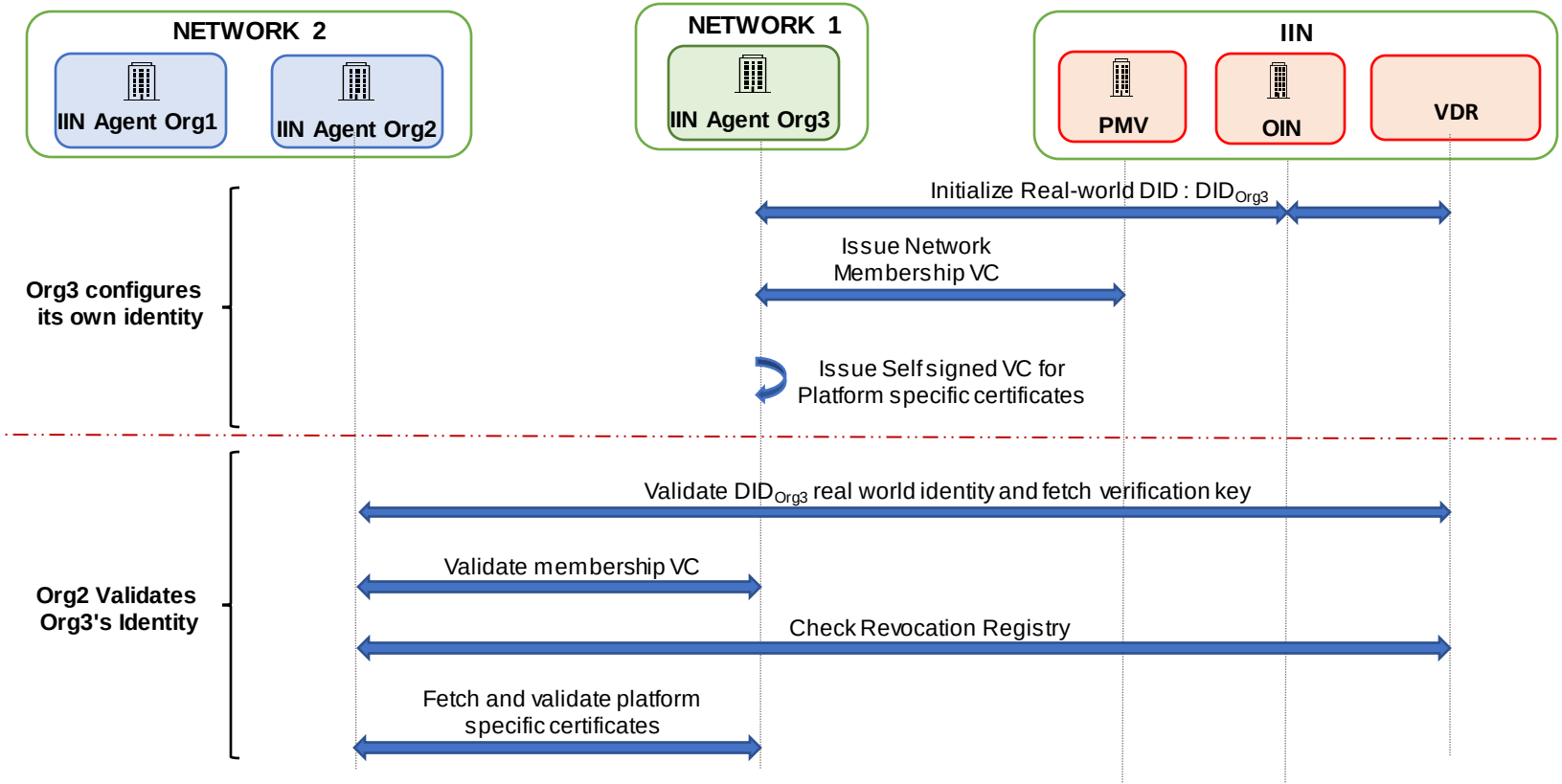


Cross-Network Participant Validation Protocol Overview

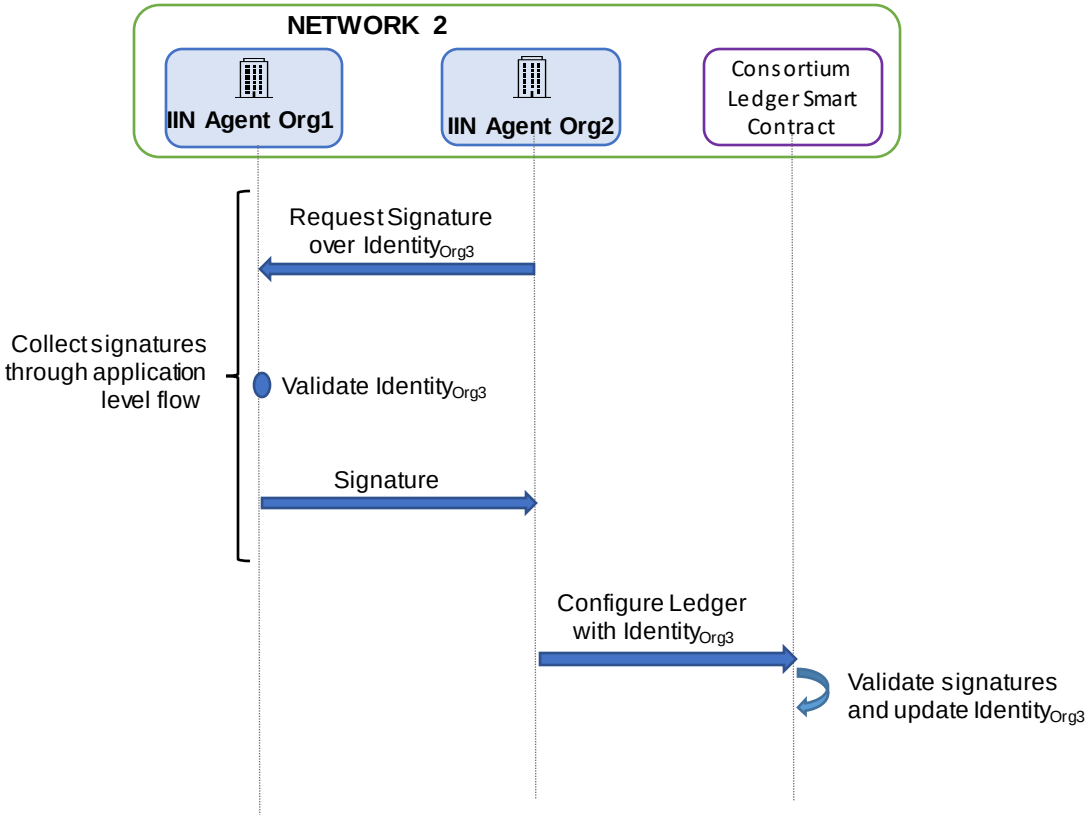


- **NETWORK 2 is configuring the identity of Org3 of NETWORK 1**

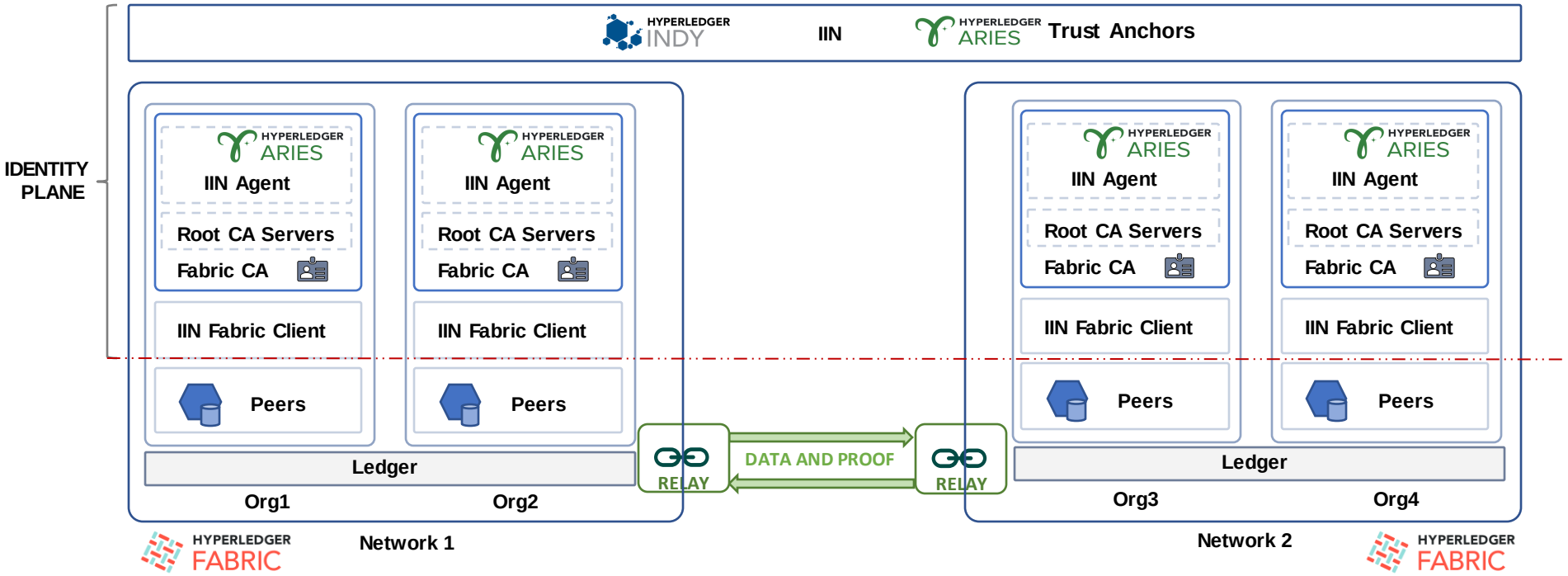
Cross-Network Participant Validation Protocol Overview



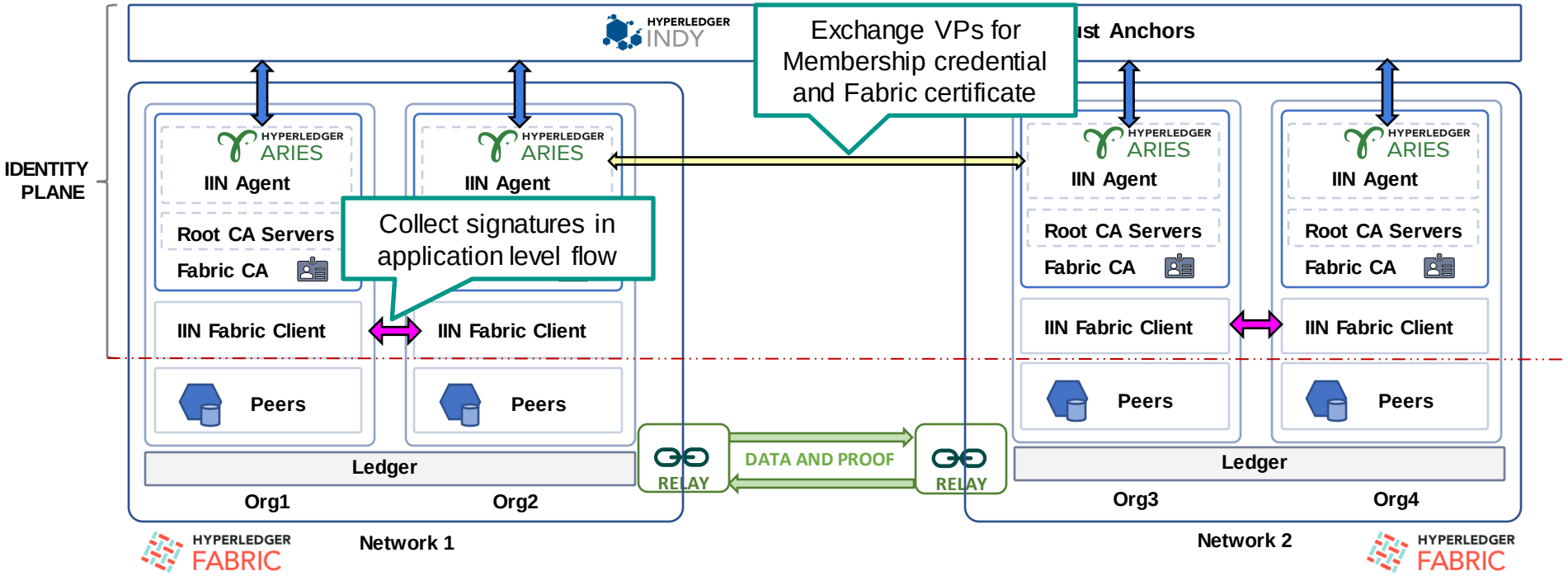
Cross-Network Participant Validation Protocol Overview



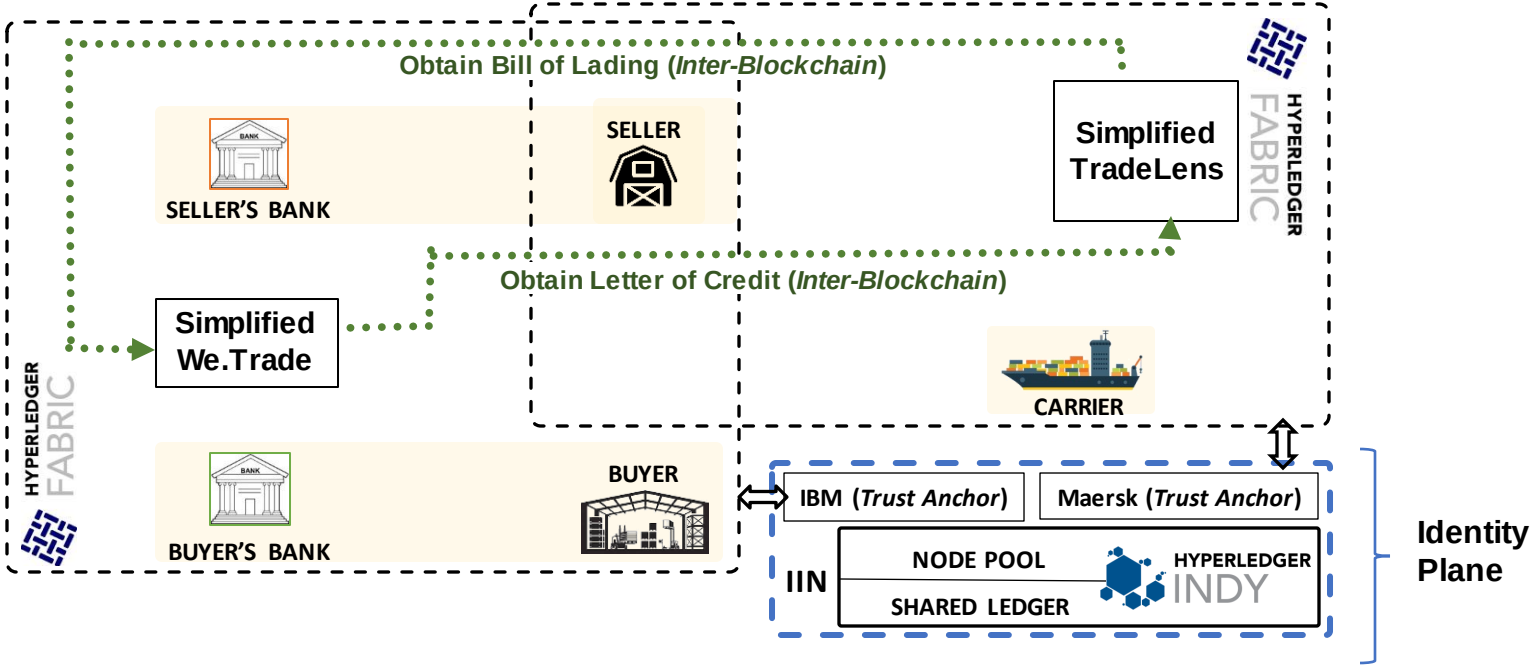
Implementation



Implementation



Use Case Implementation



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.

Future Work

- Protocols for Network Formation and Discovery without external trust anchors.
- Implementation with Corda and Besu
- Performance evaluations

Thank You

Feel free to send your questions at: ghoshbishakh@gmail.com