SATP Architecture

Updates & Overview

draft-hardjono-sat-architecture-03

IETF116 Yokohama

Thomas Hardjono, Martin Hargreaves, Ned Smith, Venkatraman Ramakrishna

Updates to Draft -03

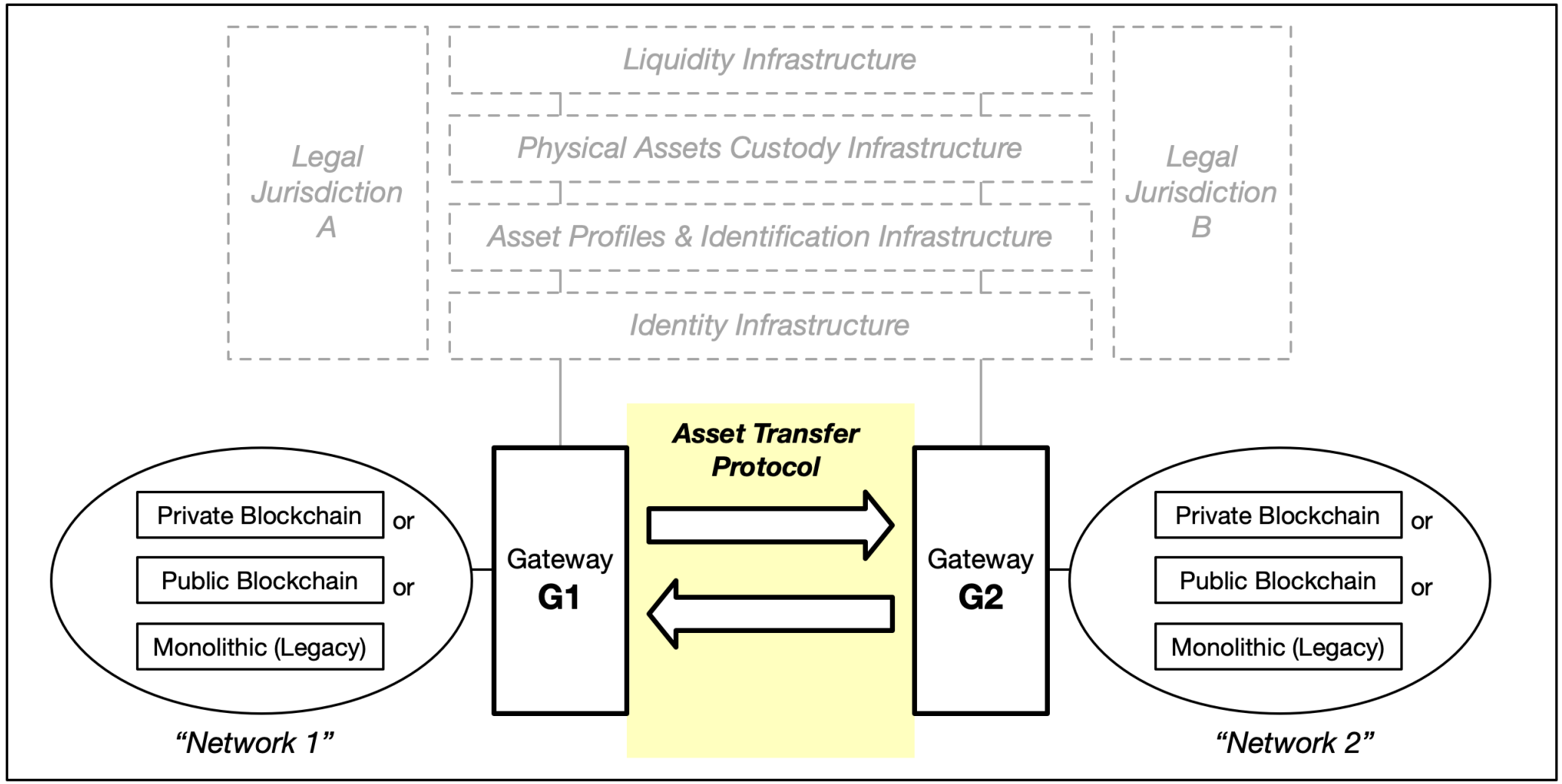
- High level flow matches v16 of the annotated detailed flow diagram (in Github repo)
- Assumptions text added:
  - Gateway is trusted
  - Session-ID is derived from shared context between App1 and App2 – but out-of-scope for WG
- Request WG to adopt as Work Item

Annotated message flow diagram: https://bit.ly/3Lzeup1

Overview of SATP: Problem Statement

- Poor interoperability of Digital Asset Networks
  - Difficult to securely move assets across networks
- Poor scalability:
  - Bilateral agreements
  - Proprietary & weak cross-chain “bridges”
- Lack of standards for security
  - Increases risks and inhibits industry growth

Gateways Paradigm



SATP Goal

- An interoperability protocol that permits the secure movement of a unique *value-bearing data-object* (“asset”) from one network to another,
- while guaranteeing that the data-object is *valid* in one network only at any one time, and that
- the transfer is *verifiable* by an independent authorized 3rd party

Desirable Properties and Constraints

- *Support Private DLTs*: must work if one (or both) blockchain networks are private (opaque)
- *Support legacy infrastructures*: must work if one side is a Legacy System (e.g. mainframe; RTGS)
- *ACID properties of transfers*: atomicity, consistency, isolation, durability

Design Principles

- Autonomous Systems Principle
- End-to-End Principle

- Opaque Resources principle:
  - The interior resources of each network is assumed to be opaque to (hidden from) external entities
  - Analog of the *Autonomous Systems* principle
- Externalization of Value principle :
  - Transfer protocol must be agnostic (oblivious) to the economic value of the digital asset being transferred
  - Analog of the *End-to-End* principle

The Autonomous Systems (AS) Principle

- Independence of each network
  - Unambiguous network boundary/domain
  - Each network has a unique identification (AS number)
  - Must not rely on data or code located in other networks
- Standardized protocol between networks
  - Standardized higher-layer data format/semantics
  - Standardized cross-domain protocol (BGP)

The End-to-End Principle

- Function & context at the endpoints
  - Reliability requirements implemented at endpoints
  - Network oblivious to semantics of payload
- Payload data protection outside the network
  - Endpoints implement encryption, signatures, etc.

Saltzer, Reed, & Clark (1981) "End-to-End Arguments in System Design". IEEE Comput.

3 Stages of Protocol (Burn-Mint)

- Stage 1: Transfer Initiation:
  - Gateways agree on the asset to be transferred
- Stage 2: Lock Assertion & Receipt:
  - Asset Lock Assertion from sending Gateway
- Stage 3: Commitment Establishment
  - Three-Phase Commit (3PC) for ACID properties

Annotated message flow diagram: https://bit.ly/3Lzeup1

ACID Properties

- *Atomicity*: Transfer must either commit or entirely fail (failure means no change to asset ownership)
- *Consistency*: Transfer (commit or fail) always results in asset located in one blockchain network only
- *Isolation*: While transfer occurring, asset ownership cannot be modified (no double-spend)
- *Durability*: Once transaction committed, must remain so regardless of gateway crashes

Thank You and Q&A

Contact: hardjono@mit.edu

Blank

- Header 1