Interoperability Architecture for Blockchain/DLT Gateways

IETF109 SecDispatch WG
Nov 16, 2020

Thomas Hardjono (MIT), Martin Hargreaves (Quant) & Ned Smith (Intel)

Contents

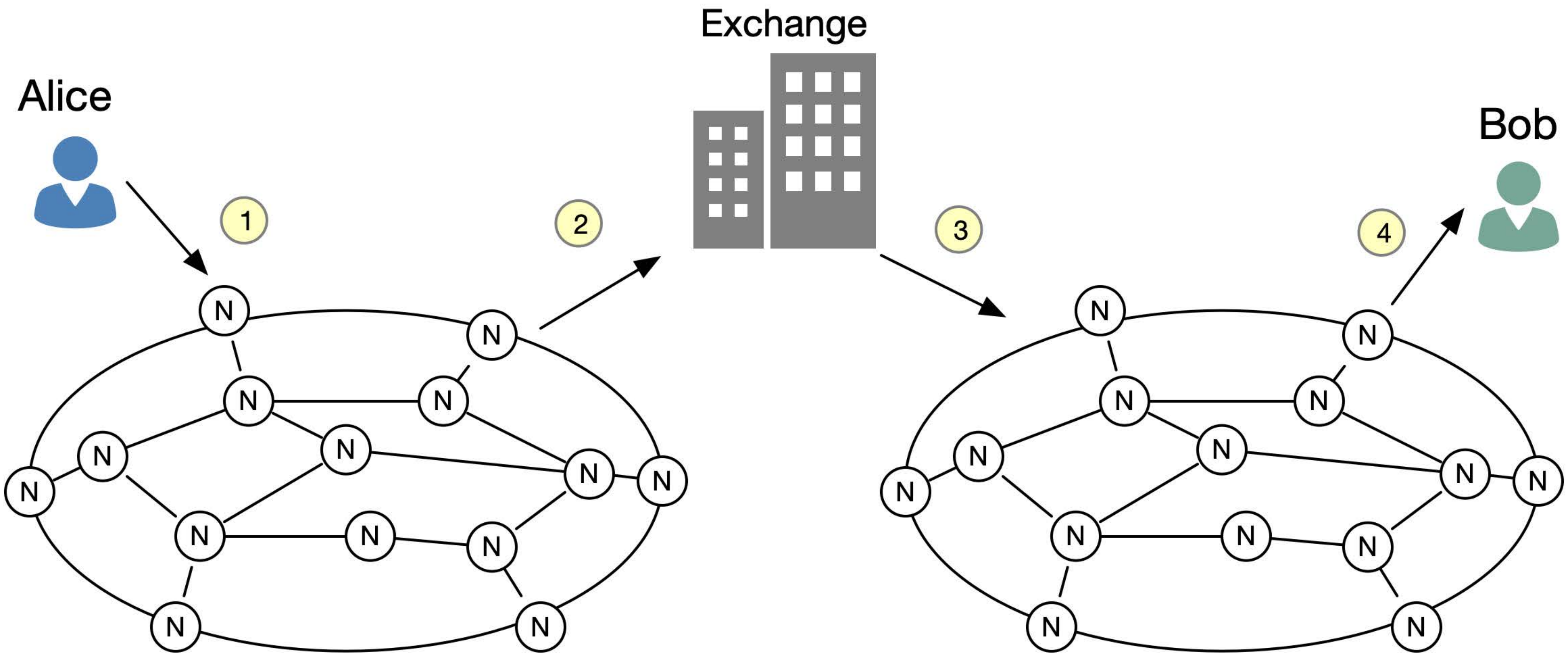
- Problem Statement
- Scope of work
- Out of scope
- Proposed Deliverables
- Proposed Roadmap

Problem Statement

- Poor interoperability of Blockchain & DLT systems
- Transfers of virtual assets must be mediated by 3rd party entities (e.g. crypto-exchanges)
- Centralization (choke point)
- Lack of system autonomy & limited scalability
- Asset lock-in

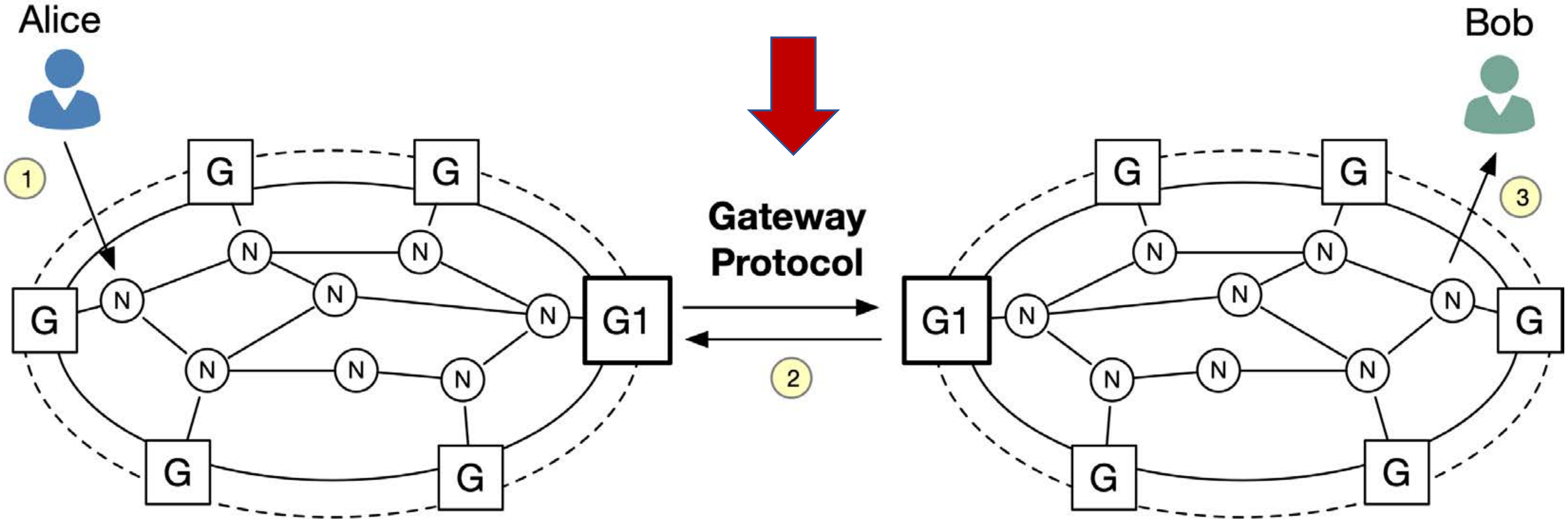
Problem Statement

- Transfers mediated by Third Party (Exchange)

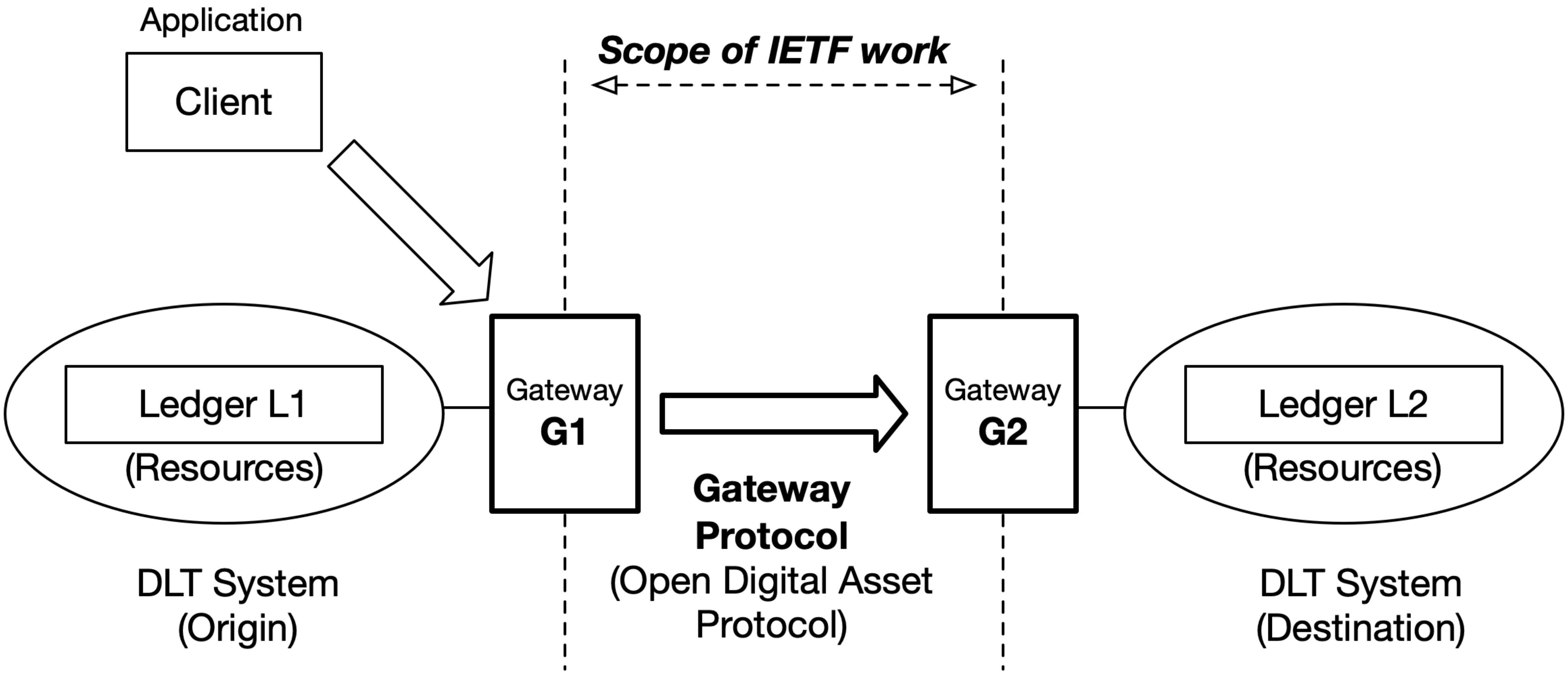


Proposed Solution: Gateway-to-Gateway Protocol

- Standardized protocol
- Agnostic to economic value
- Stands in front of DLT system



Gateway-to-Gateway Protocol



Gateway-to-Gateway Protocol

- Protocol between gateways to securely transfer the digital representation of an asset,
- unidirectional,
- satisfying requirements of atomicity and non-repudiation,
- agnostic to the higher-layer economic value of the asset

Proposed Scope of Work

- Gateway API definitions (RESTful APIs)
- Resource identifiers
- Payload definition
- Message flows and commands
- Secure channel establishment (e.g. TLS1.3)
- Terminology (extending NISTR-8202)

Out of Scope

- Blockchains and DLT systems
- Consensus & BFT protocols, PoW, PoS, etc.
- Cryptocurrencies, tokenization, etc.
- Incentive mechanisms, economic models; etc.
- Zero-knowledge proof (ZKP) protocols
- Authentication & Authorization protocols
- Concurrency control algorithms
- Identity management & privacy, etc. etc.

Gateway Protocol: Desirable Features

- Must work if one (or both) DLTs are private – interior resources externally inaccessible
- Must work if one side is a Legacy system
- Must result in atomic settlement with sufficient evidence (in case of disputes)
- Support for different client modes for resource access (see ODAP draft)

Gateway Protocol: General Transfer Requirements

- *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 DLT only
- *Isolation*: While transfer occurring, asset ownership cannot be modified (no double-spend)
- *Durability*: Once transaction committed, must remain so regardless of gateway crashes

Proposed Deliverables

- Architecture specification
- Protocol specification (ODAP)
- Use-cases & Requirements

- Optional
  - Asset Profile JSON specification
  - Log-metadata JSON specification (crash recovery)

Proposed Roadmap & Timeline

- November IETF109:
  - SecDispath Presentation & call for participation
- March IETF110: BOF request for WG creation
- Nov 2021 (or earlier): Drafts completed (WG LC)
- Close-down WG or Recharter

`www.ietf.org/mailman/listinfo/blockchain-interop`

Why the IETF

- Neutrality
- History of gateway protocols (e.g. BGP4, IPsec/IKE)
- Expertise in security protocols
- Home of: TCP/IP, HTTP, IPsec, IKE, Kerberos, TLS, OAuth2.0, JWT, JWE, CoAP, RATS, etc.
- Existing liaisons (e.g. ITU, W3C, 3GPP, etc.)

Call for Participation

www.ietf.org/mailman/listinfo/blockchain-interop