# SATP Core Protocol

## Updates & Overview of Flows

draft-hargreaves-sat-core-02

IETF116 Yokohama

Martin Hargreaves, Thomas Hardjono and Rafael Belchior

# Updates to Draft

- Flows in draft-02 now matches v16 of the annotated flow diagram (in Github repo)
  - Session-ID in each message
- Lock (burn) Assertion and Receipt
  - Claims body carries AssetID & AssetProfileID
- Request WG to adopt as Work Item

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

# Lock (Burn) Assertion Fields (Section 8.3)

- message_type REQUIRED urn:ietf:satp:msgtype:lock-assert-msg.
- session_id REQUIRED: 128-bit value identifying the current transfer-session
- client_identity_pubkey REQUIRED. The client who sent this message.
- server_identity_pubkey REQUIRED. The server for whom this message is intended.
- lock_assertion_claims REQUIRED. The lock assertion claim or statement by the client.
- lock_assertion_format OPTIONAL. The format of the assertion.
- lock_assertion_expiration REQUIRED. Duration of validity of assertion.
- hash_prev_message REQUIRED. The hash of the previous message.
- client_transfer_number OPTIONAL. This number is meaningful only to the client.
- client_signature REQUIRED. The digital signature of the client.

# Information in lock_assertion_claims


"gatewayId": "did:gateway:tz:tz1aaYoabvj2DQtpHz74Z83fSNjY29asdBfZ",

"networkId": "tezos:NetXdQprcVkpaWU",

"assets": [{

"assetId": "tezos:NetXdQprcVkpaWU/tzip16:tz1YWK….mVre7xC/1",

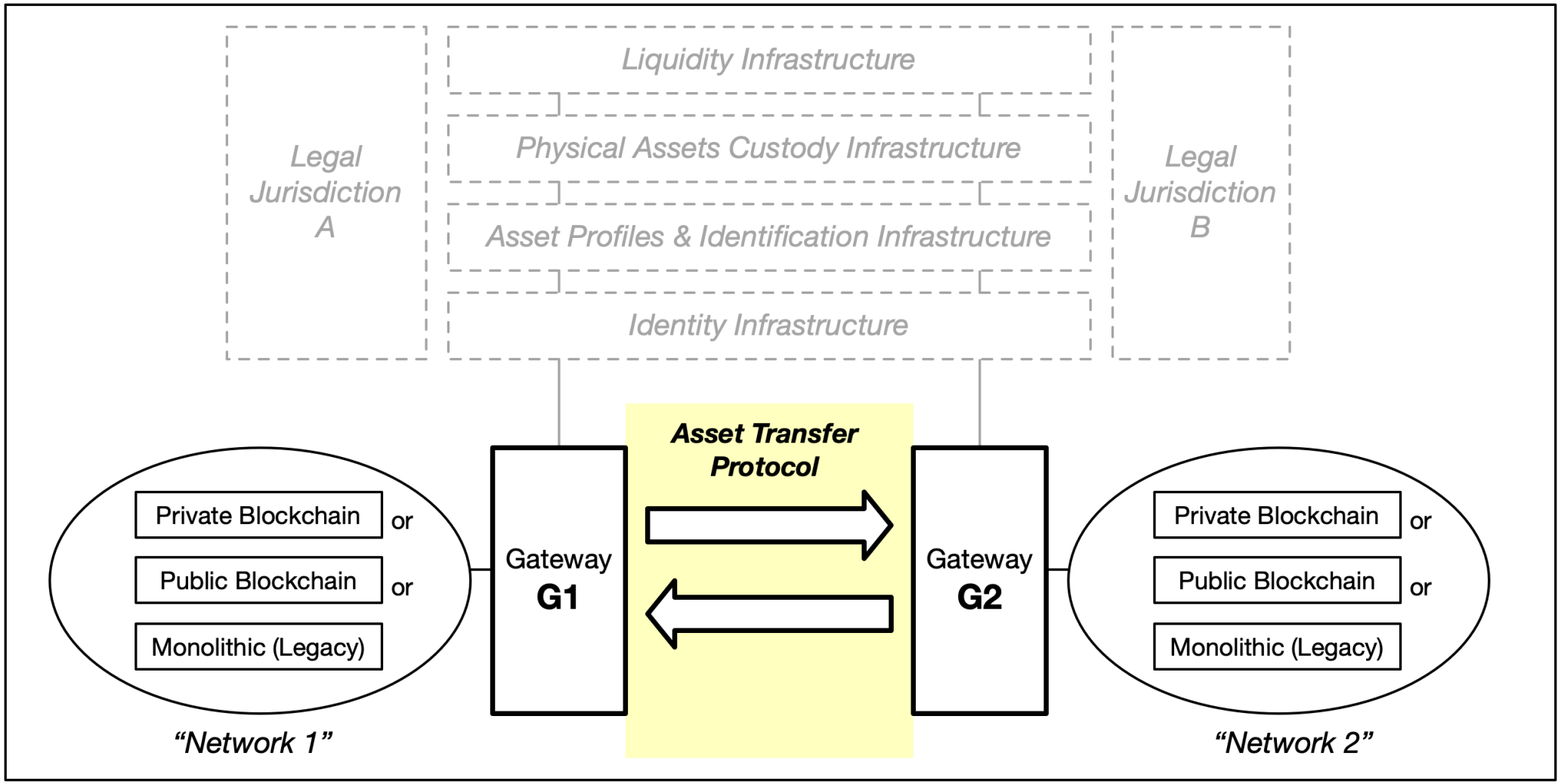
"assetData": {},

"assetProfileId": "tezos:NetXdQprcVkpaWU/tzip16:tz1CAK1..GG433/1",}

"assetState": "Burned",

"assetStateTimestamp": "2023-02-22T20:20:39+00:00"

# Overview of Message Flows

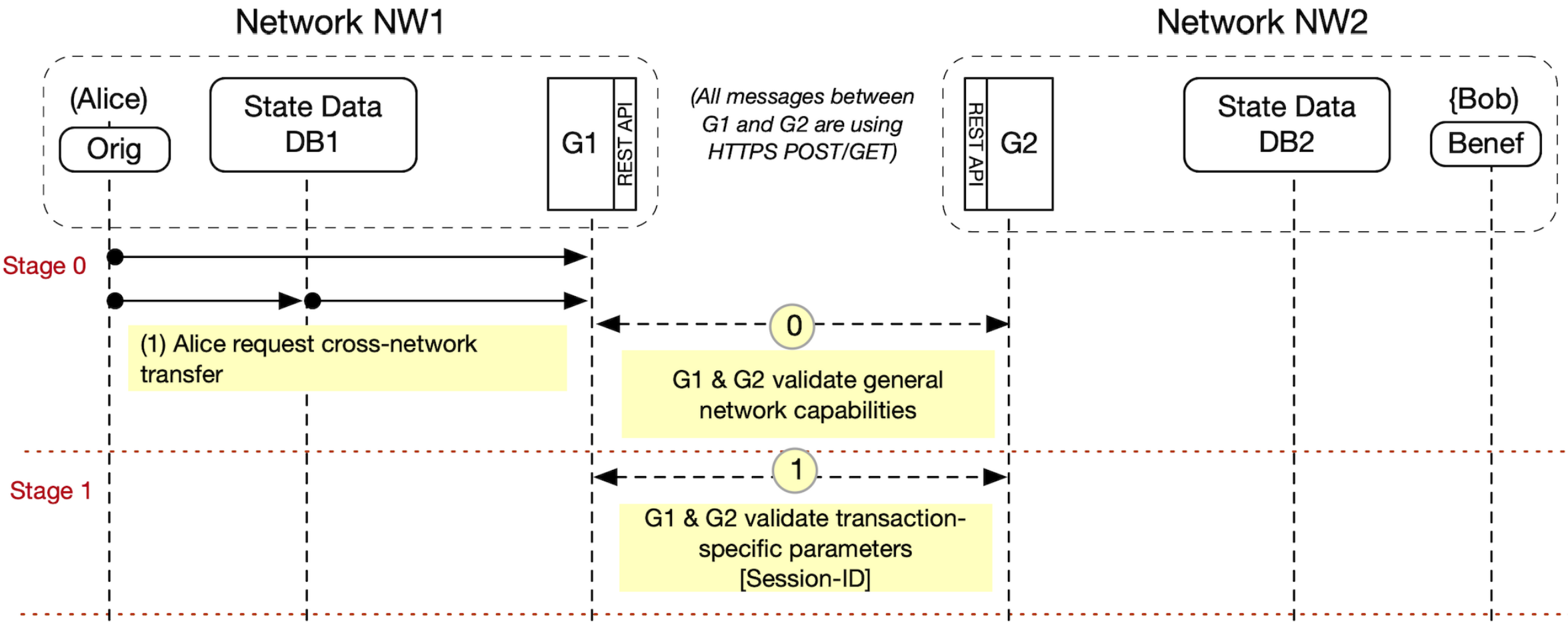


# 3 Stages of Protocol (Burn-Mint)

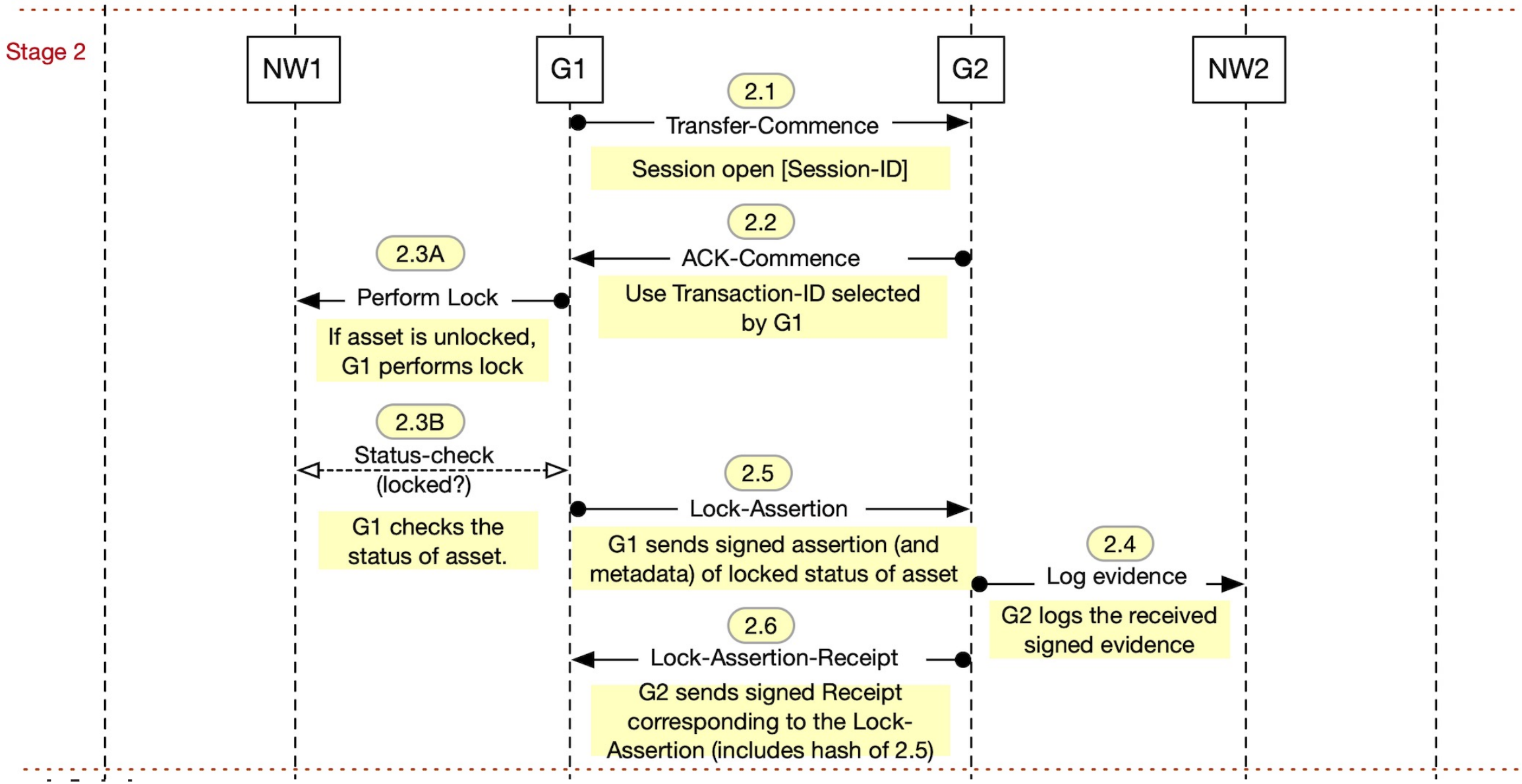
- Stage 1: Transfer Initiation:
  - Gateways agree on the asset to be transferred
- Stage 2: Lock Assertion & Receipt:
  - Asset Lock Assertion from sending Gateway
- Stage 3: Commitment Establishment
  - Three-Phase Commit (3PC) for ACID properties

Message Flow Diagram: https://bit.ly/3Lzeup1

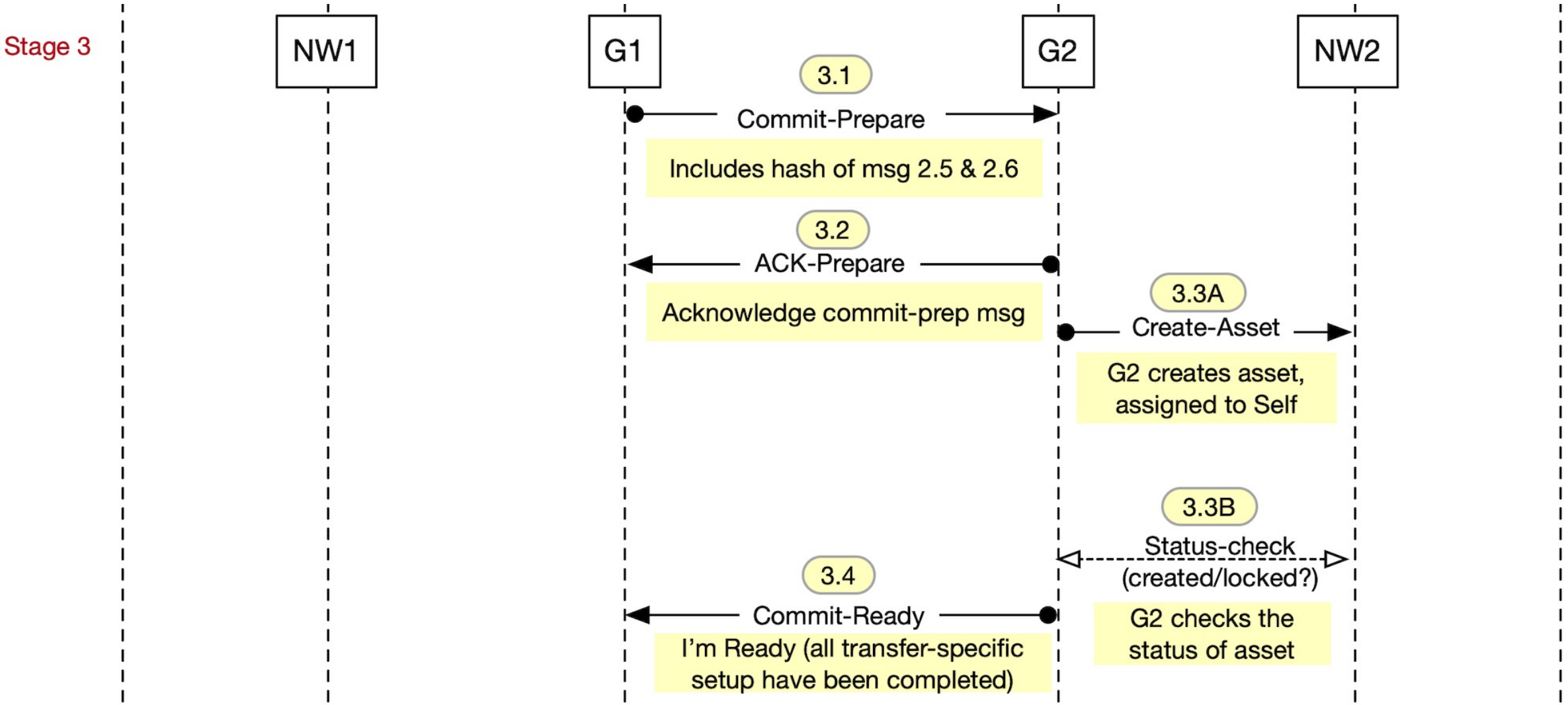
# Stage 1: Transfer Initiation



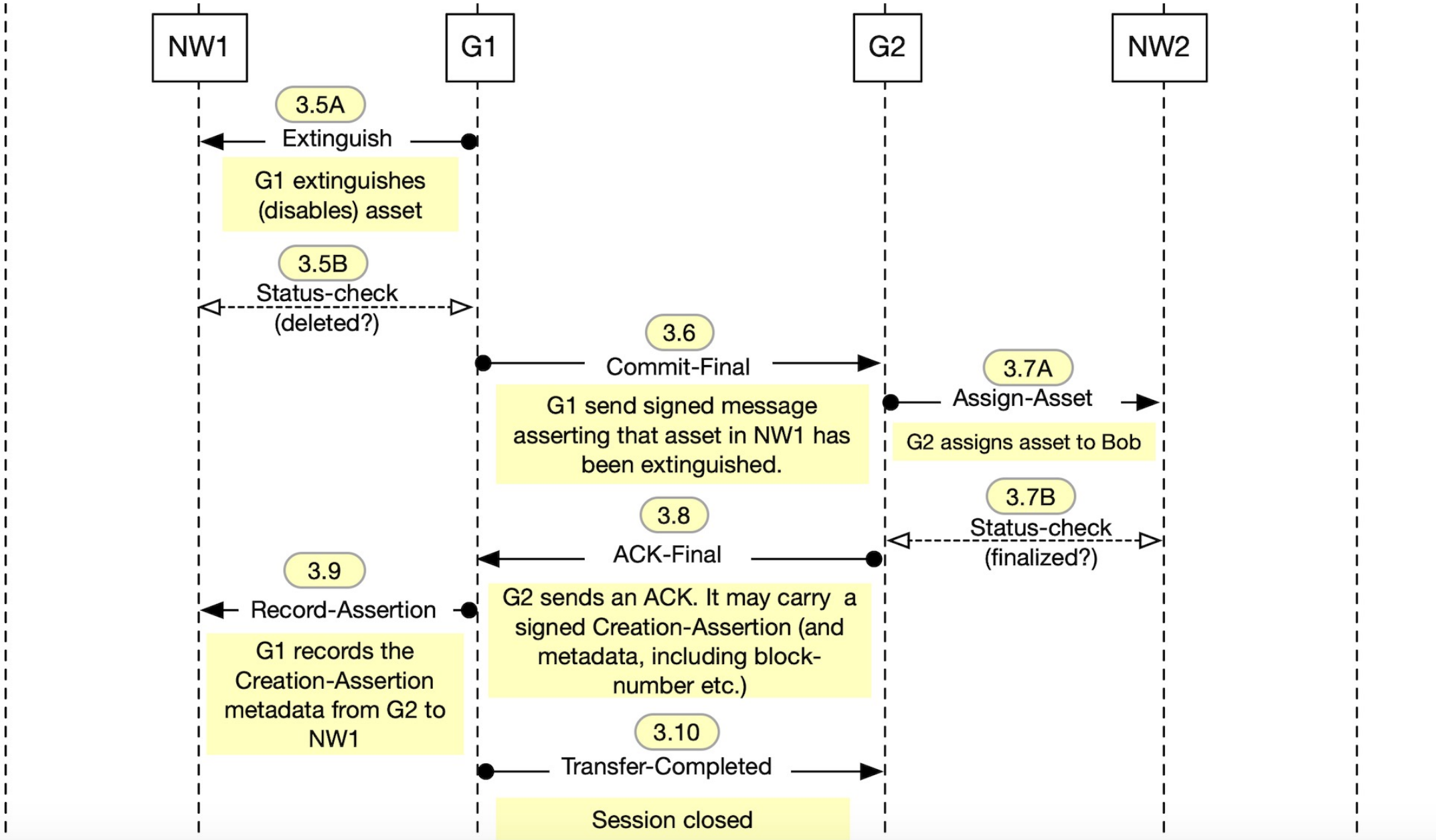
# Stage 2: Lock-Assertion & Receipt



# Stage 3: Commitment Establishment



# Stage 3 (cont)


NW1
G1
G2
NW2
3.5A
Extinguish
G1 extinguishes (disables) asset
3.5B
Status-check (deleted?)
3.6
Commit-Final
G1 send signed message asserting that asset in NW1 has been extinguished.
3.7A
Assign-Asset
G2 assigns asset to Bob
3.7B
Status-check (finalized?)
3.8
ACK-Final
G2 sends an ACK. It may carry a signed Creation-Assertion (and metadata, including block-number etc.)
3.9
Record-Assertion
G1 records the Creation-Assertion metadata from G2 to NW1
3.10
Transfer-Completed
Session closed

# 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
  - Subheader
- Header 2