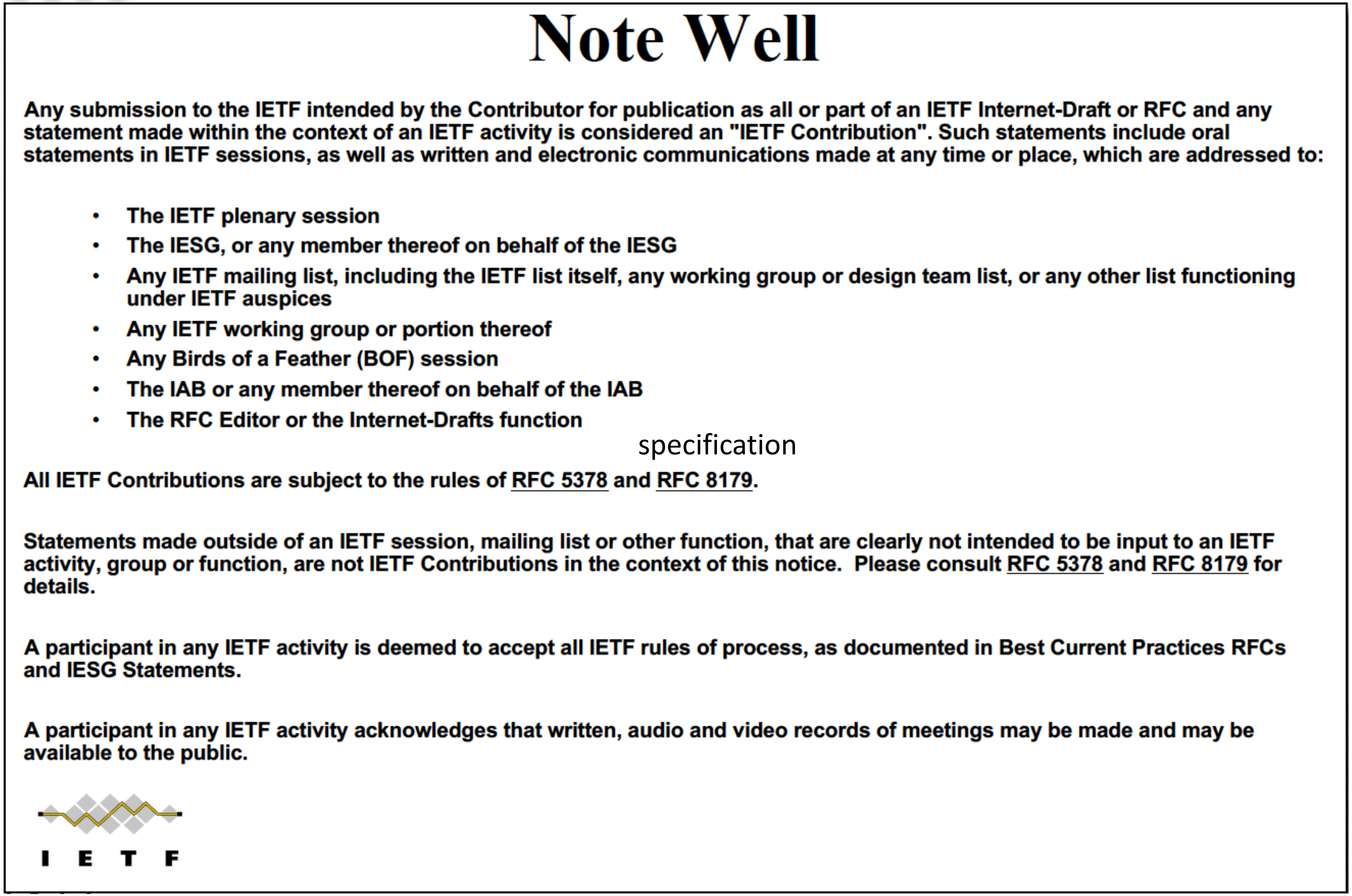
IETF Forming Working Group

DLT Gateway Interoperability Protocol

Group Meeting

16 February, 2021



Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- Any Birds of a Feather (BOF) session
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

specification

All IETF Contributions are subject to the rules of RFC 5378 and RFC 8179.

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 8179 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

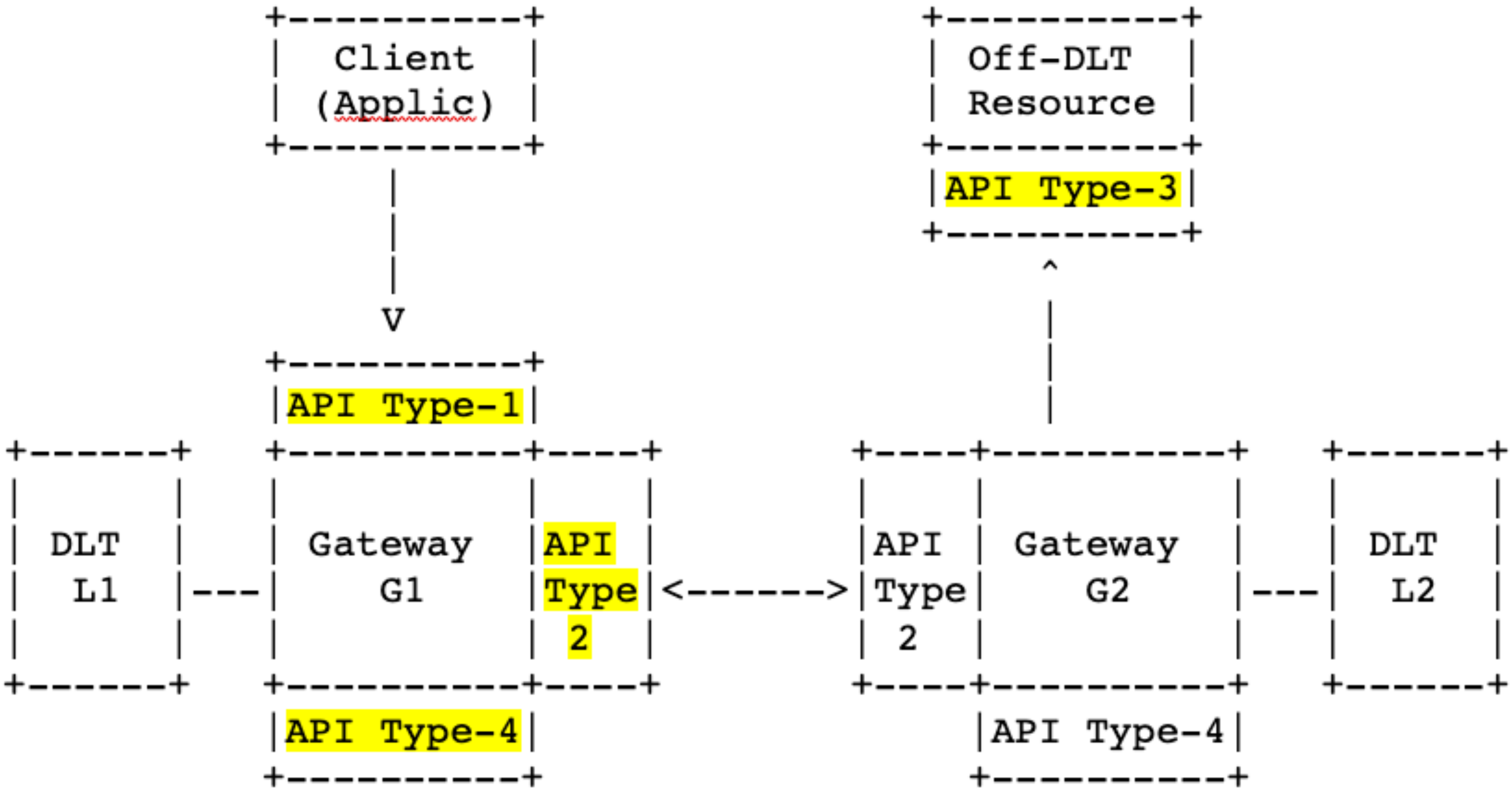
IETF

Flows and API Definitions

- Type-1 APIs: Client to gateway APIs
- Type-2 APIs: Gateway-to-Gateway APIs
- Type-3 APIs: Gateway to off-chain DLTs resources APIs
- Type-4 APIs: Crash log-storage/recovery APIs

- Each type may have multiple flows and APIs, depending on the purpose/action

Four types of APIs



```
          +-----------+                     +-----------+
          |  Client   |                     |  Off-DLT  |
          | (Applic)  |                     |  Resource |
          +-----------+                     +-----------+
                |                           |API Type-3 |
                |                           +-----------+
                |                                 ^
                V                                 |
          +-----------+                           |
          |API Type-1 |                           |
+------+  +-----------+----+           +----+-----------+    +------+
|      |  |           |    |           |    |           |    |      |
| DLT  |  |  Gateway  |API |           |API |  Gateway  |    | DLT  |
|  L1  |--|     G1    |Type|<--------->|Type|     G2    |----|  L2  |
|      |  |           | 2  |           | 2  |           |    |      |
+------+  +-----------+----+           +----+-----------+    +------+
          |API Type-4 |                     |API Type-4 |
          +-----------+                     +-----------+
```

Gateway-to-Gateway APIs (Type-2)

- Phase 1: transfer initiation
- Phase 2: lock evidence agreement
- Phase 3 : final commitment

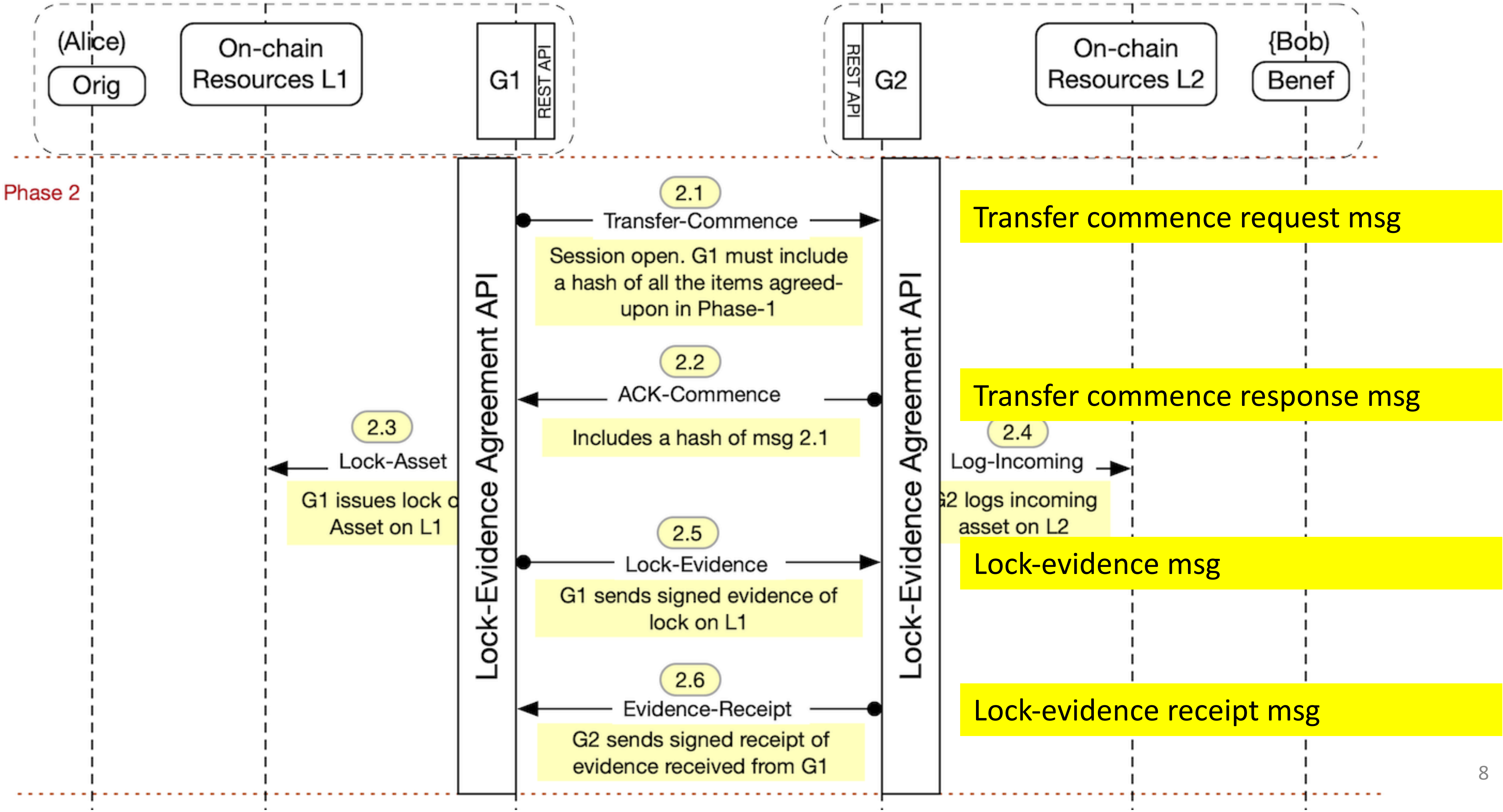
Phase 1 – Transfer Initiation [defer to last]

- Transfer Request API
  - Purpose: ask remote gateway if open to transfer
- Entity-identity verification API
  - Purpose: validate the identities of the Originator, Beneficiary (i.e. Travel Rule)
- Gateway-identity verification API
  - Purpose: validate the X509 cert of the gateway-device and the VASP who owns it
- Asset verification API
  - Verify legal status of asset

Phase 2 – Lock Evidence Agreement

- API name: Lock-Evidence Agreement API
- Four (4) message-types:
    1. Transfer commence request message (G1 -> G2)
    2. Transfer commence response message (G2 -> G1)
    3. Lock-evidence message (G1 -> G2)
    4. Lock-evidence receipt message (G2 -> G1)

Lock-Evidence Agreement API (Phase 2)



(Alice)

Orig

On-chain Resources L1

G1

REST API

REST API

G2

On-chain Resources L2

{Bob)

Benef

Phase 2

Lock-Evidence Agreement API

Lock-Evidence Agreement API

2.1 Transfer-Commence

Session open. G1 must include a hash of all the items agreed-upon in Phase-1

Transfer commence request msg

2.2 ACK-Commence

Includes a hash of msg 2.1

Transfer commence response msg

2.3 Lock-Asset

G1 issues lock o
Asset on L1

2.4 Log-Incoming

2 logs incoming
asset on L2

2.5 Lock-Evidence

G1 sends signed evidence of lock on L1

Lock-evidence msg

2.6 Evidence-Receipt

G2 sends signed receipt of evidence received from G1

Lock-evidence receipt msg

1. Transfer Commence Request message

- message_type REQUIRED urn:ietf:odap:msgtype:transfer-commence-req
- originator_pubkey REQUIRED
- beneficiary_pubkey REQUIRED
- sender_dlt_system_number REQUIRED – do we need this ?
- recipient_dlt_system_number REQUIRED – do we need this ?
- client_identity_pubkey REQUIRED – gateway who sent this msg
- server_identity_pubkey REQUIRED – gateway for whom this is intended
- hash_asset_profile REQUIRED
- asset_unit REQUIRED
- hash_prev_mesg REQUIRED
- client_transfer_number OPTIONAL – client local tx numbering
- client_signature MANDATORY – G1 signature using identity priv-key

2. Transfer Commence Response message

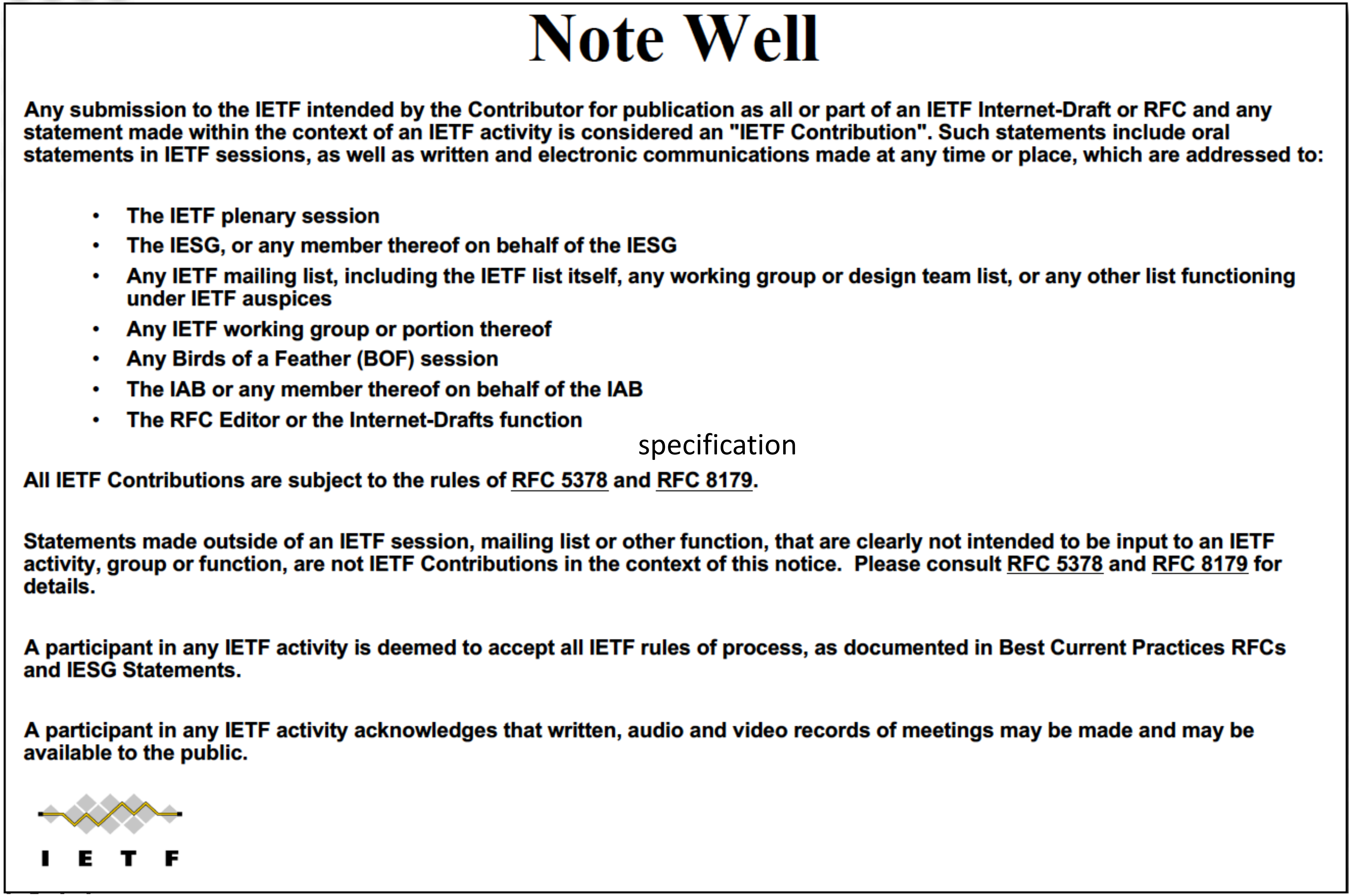
- message_type REQUIRED urn:ietf:odap:msgtype:transfer-commence-resp
- client_identity_pubkey REQUIRED – gateway who sent this msg
- server_identity_pubkey REQUIRED – gateway for whom this is intended
- hash_commence_request REQUIRED. – hash of previous request msg
- server_transfer_number OPTIONAL – server local tx numbering
- server_signature MANDATORY – G2 signature using identity priv-key

3. Lock Evidence Message

- message_type REQUIRED urn:ietf:odap:msgtype:lock-evidence-req
- client_identity_pubkey REQUIRED – G1 who sent this msg
- server_identity_pubkey REQUIRED – G2 for whom this is intended
- lock_evidence_claim REQUIRED. – lock or escrow evidence
- lock_claim_format OPTIONAL.
- lock_evidence_expiration REQUIRED. – duration of time of lock
- hash_commence_response REQUIRED. – hash of previous message
- client_transfer_number OPTIONAL
- client_signature MANDATORY – G1 signature using identity priv-key

4. Lock Evidence Receipt message

- message_type REQUIRED urn:ietf:odap:msgtype:lock-evidence-resp
- client_identity_pubkey REQUIRED – G1 who sent this msg
- server_identity_pubkey REQUIRED – G2 for whom this is intended
- hash_lockevidence_msg REQUIRED – hash of previous message
- server_transfer_number OPTIONAL
- server_signature MANDATORY – G1 signature using identity priv-key



Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- Any Birds of a Feather (BOF) session
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

specification

All IETF Contributions are subject to the rules of RFC 5378 and RFC 8179.

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 8179 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

IETF