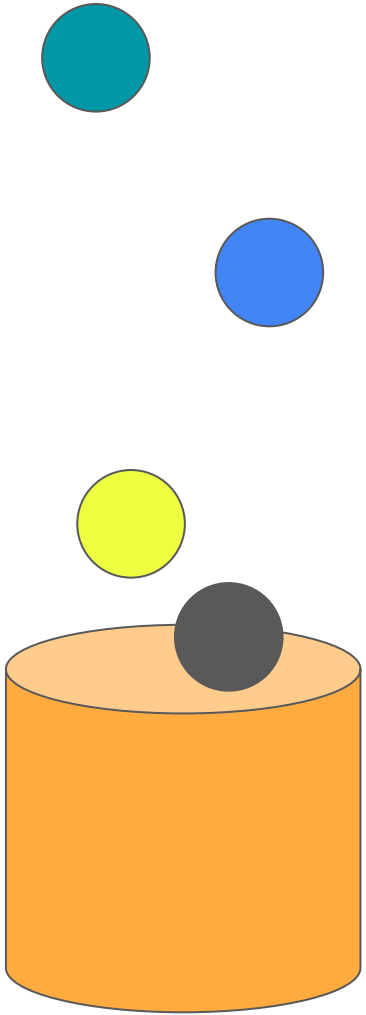


Token Containers

Justin Richer and Orie Steele

WIMSE BoF

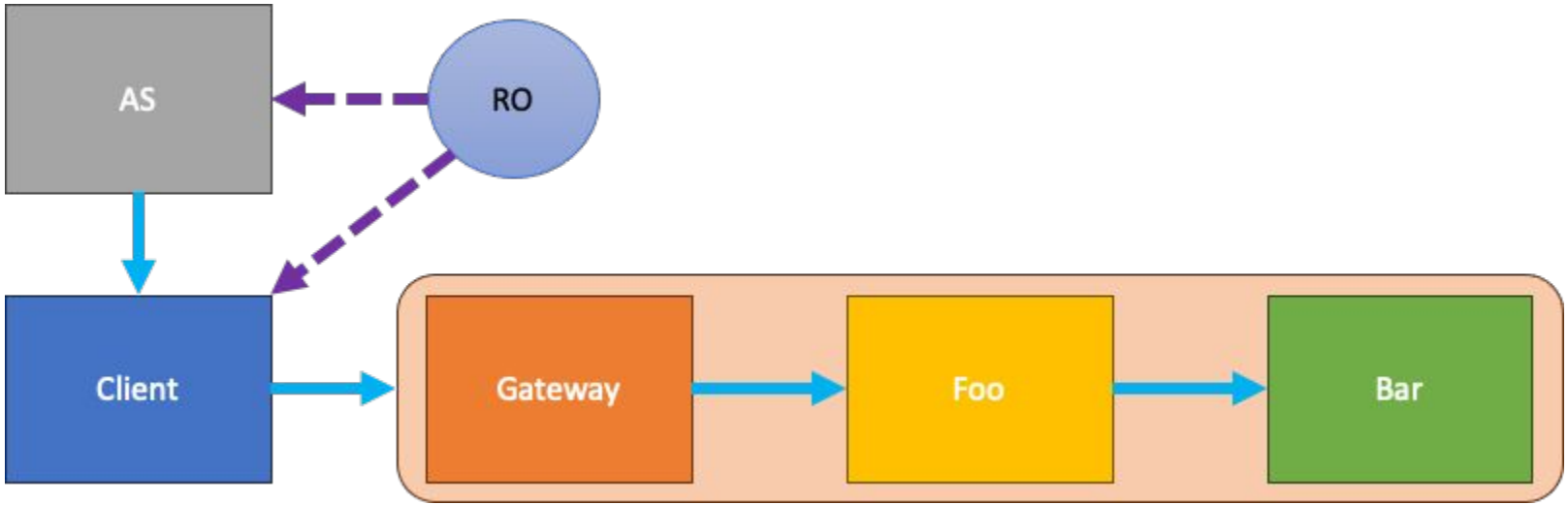
IETF118

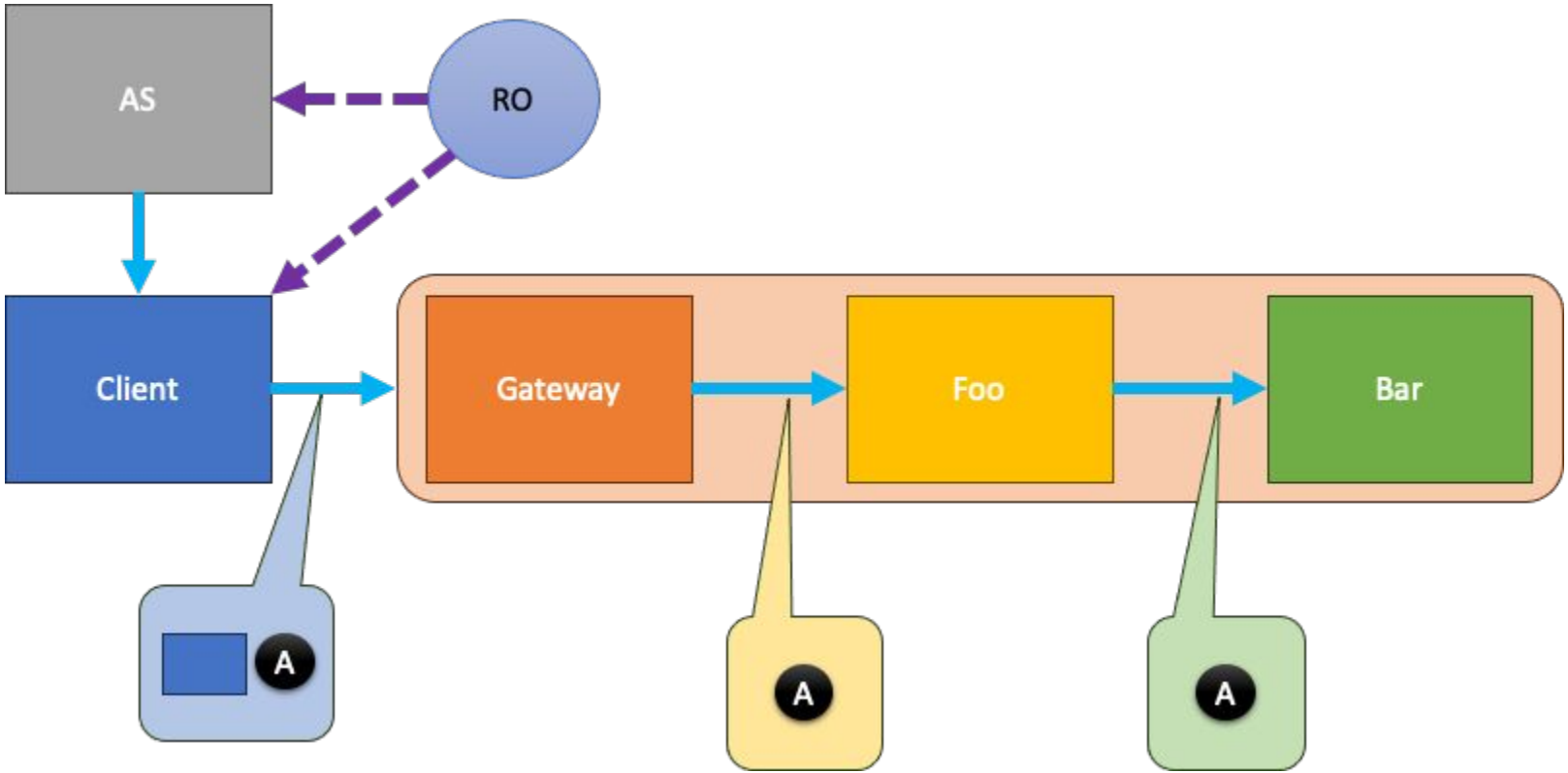
The Problem

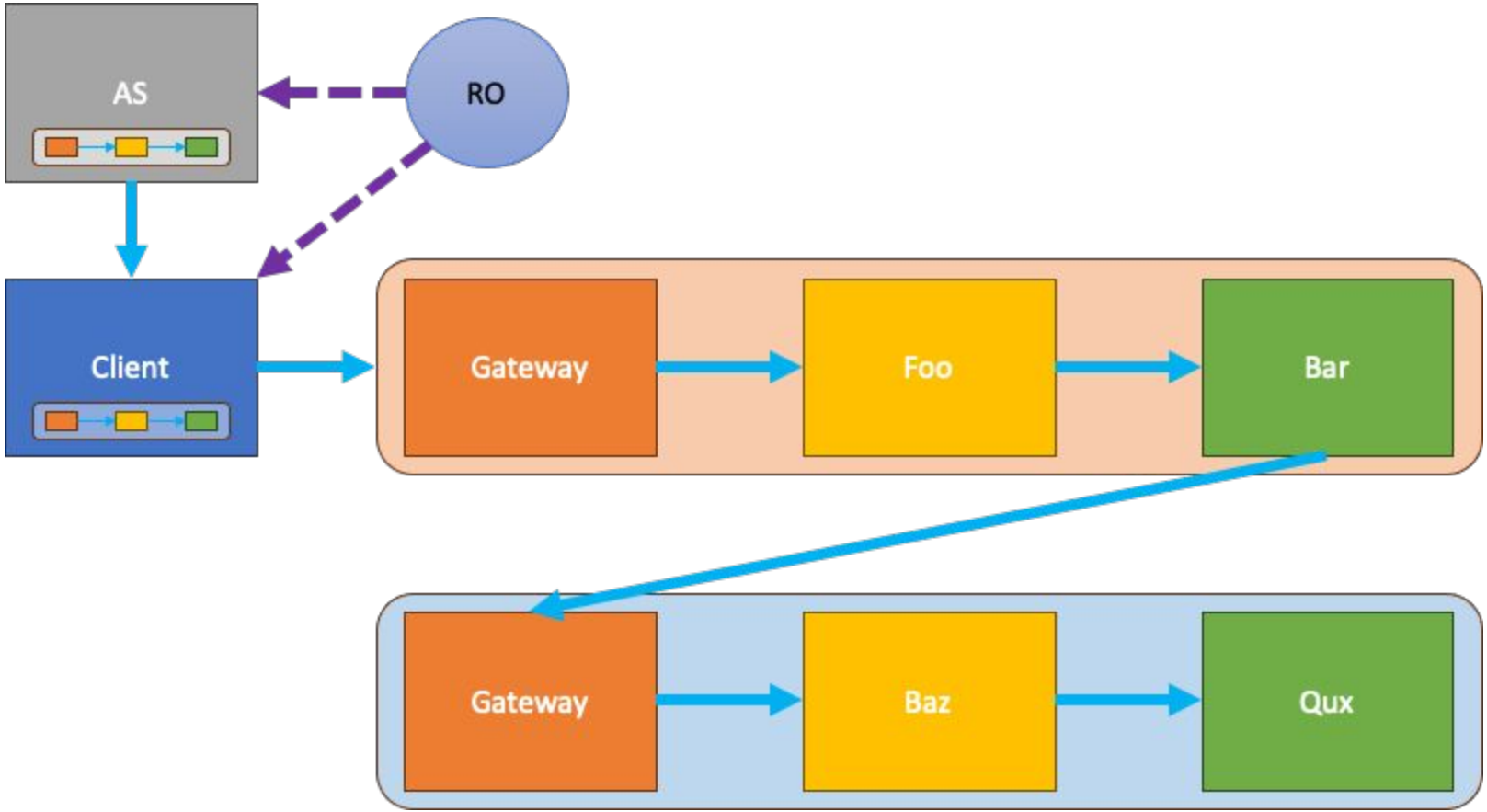
- We use tokens to limit access to APIs
- HTTP gives us a place to put **one token in a request**
  - Authorization: Foo token.goes.here-probably
  - *?access_token=token.goes.here-but.not.if.you.follow.best.practices*
- What if we need more than one object like this?

Why would we need more than one security object?

- Workload processing
  - Each stage can augment the request
  - Trusted nodes attest to the state of the request at that point
- Auditing
  - The fully disclosed token can be proven to have been witnessed by the transparency service
- SBOM
  - Enabled progressive disclosure of software bill of materials
- Reality
  - Treating everything like an access token is an anti-pattern


AS
RO
Client
Gateway
Foo
Bar

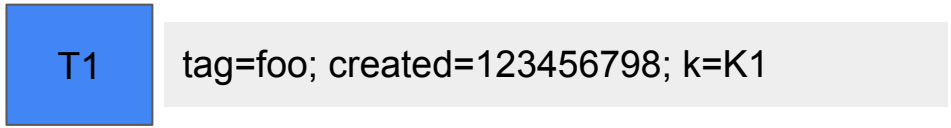

AS
RO
Client
Gateway
Foo
Bar
A
A
A


AS
RO
Client
Gateway
Foo
Bar
Gateway
Baz
Qux

A Multi-Token Data Structure

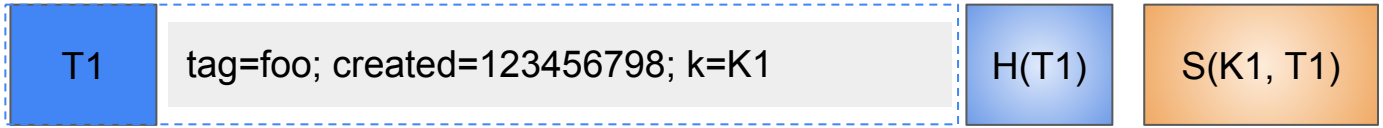
- Anyone can add a new token value to the structure (as a node)
- Each node can have metadata parameters (external to the token)
- Any token node can reference other nodes in the structure
- Once values and parameters are set, they can’t be changed
- Anyone can sign a token node in the graph

A Crate full of Token Buckets

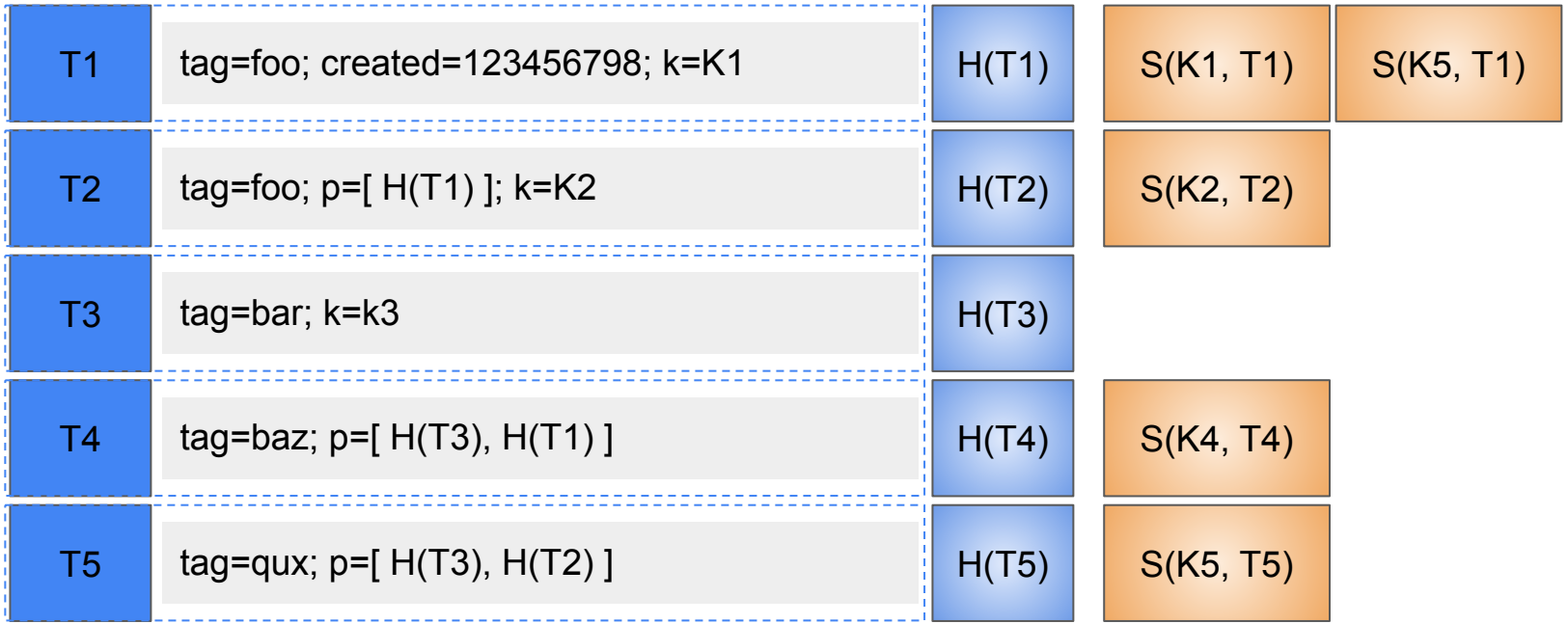


A Crate full of Token Buckets

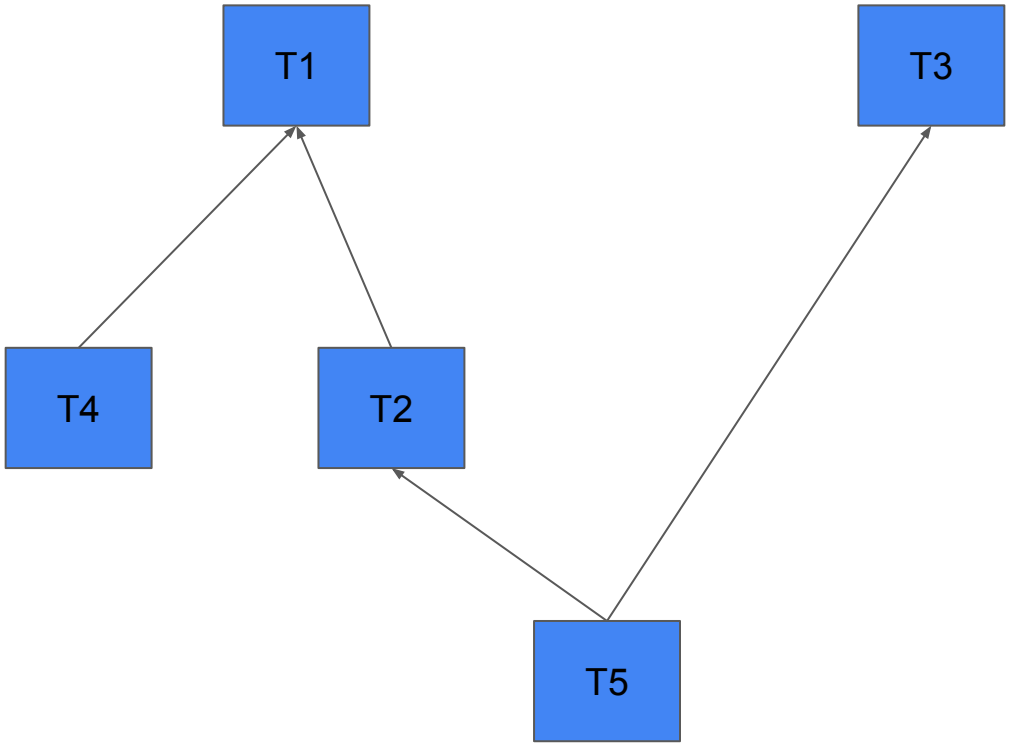
A Crate full of Token Buckets



A Crate full of Token Buckets



A Crate full of Token Buckets




GRAPHS
are
SNAKES

Notable attributes

- All node references are via (fixed) hash
- Signatures are over hash
- Signatures not included in hash
  - To protect a signature, include key identifier in metadata
- Can be pruned if needed

Digital Credential Workflows

Workflow:

The sequence of industrial, administrative, or other processes through which a piece of work passes from initiation to completion.

Credential Workflows:

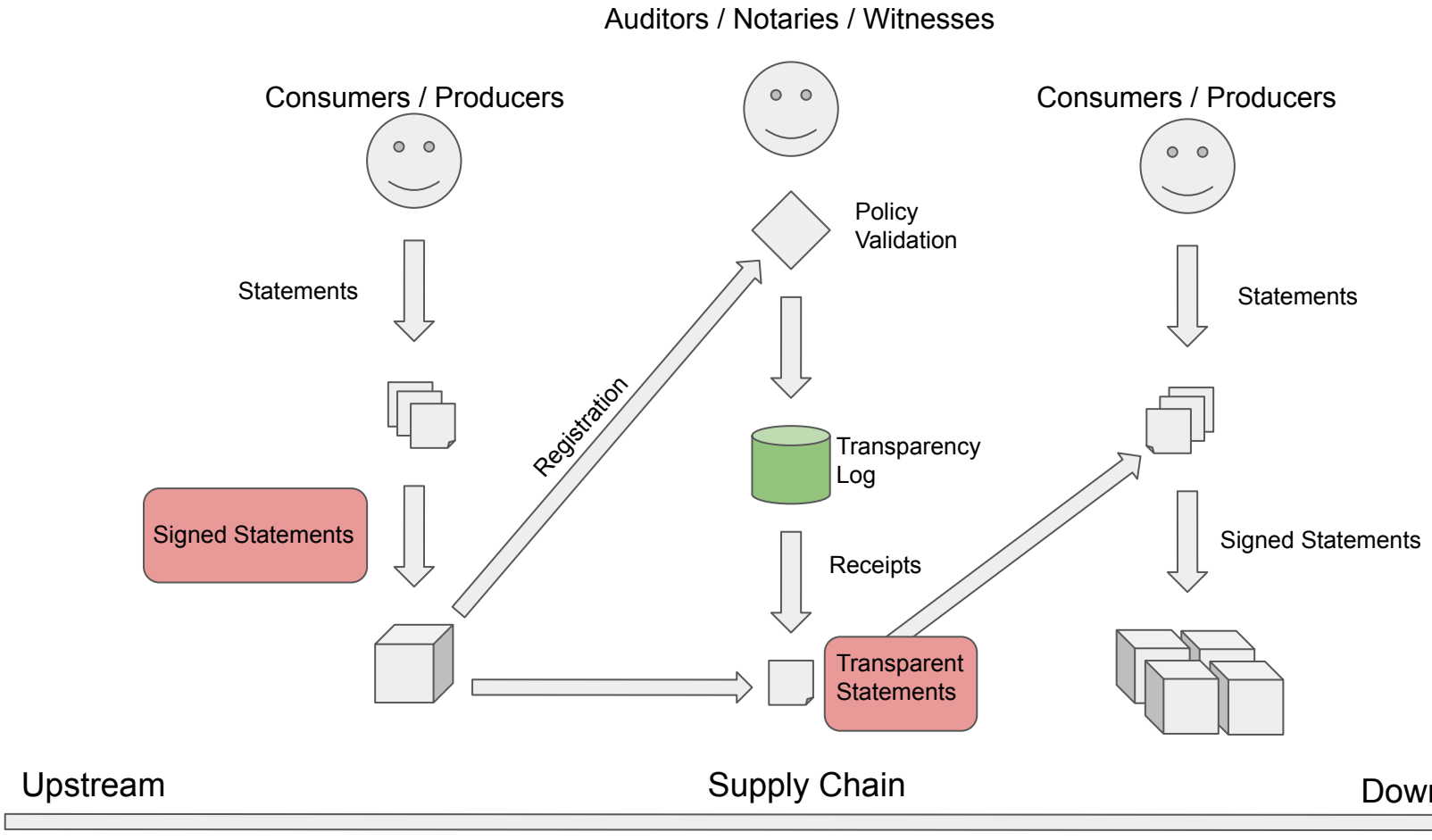
A workflow executed through the use of digital credential technologies, including identity documents, digital signatures and encrypted envelopes.

Transparent Workflows:

Credential workflows, where messages are stored in a verifiable data structure, which enables new messages representing proofs of inclusion, consistency, or “receipts”, “endorsements” or “evidence”.

Infosec personnel might audit a transparency service provider to ensure that they witnessed specific supply chain activity, or certify that a digital compliance policy is in place and being leveraged to secure an industry use case, such as software supply chain, physical supply chain, or digital content provenance.

Transparent Workflow Basics



Transparent Statement

```
18(                                 / COSE Single Signer Data Object        /
    [
      h'a3013822...6c61696e',       / Protected header                      /
      {                             / Unprotected header                    /
        300: [                      / Receipts (1)                          /
          h'd284585f...419c8ec0'    / Receipt 1                             /
        ]
      },
      h'',                          / Detached payload                      /
      h'b8552367...e8235a07'        / Signature                             /
    ]
 )
```

Receipt

```
18(                                 / COSE Single Signer Data Object        /
    [
      h'a2013822...5f636838',       / Protected header                      /
      {                             / Unprotected header                    /
        100: [                      / Inclusion proofs (1)                  /
          h'83020181...c6bf0202',   / Inclusion proof 1                     /
        ]
      },
      h'',                          / Detached payload                      /
      h'6140da0f...419c8ec0'        / Signature                             /
    ]
)
```

Inclusion Proof

```
[                                   / Inclusion proof 1                   /
  2,                                / Tree size                           /
  1,                                / Leaf index                          /
  [                                 / Inclusion hashes (1)                /
     h'5979d2d8...c6bf0202'         / Intermediate hash 1                 /
  ]
]
```