Metaverse and Blockchain

116 Yokohama

Blockchains store transactions over a distributed state and may help

- to determine who owns what,
- to provide asset tracing, and
- to secure digital content and data.

Consensus protocols are the backbone of blockchains, validating transactions, adding blocks, and working on inconsistent state (PoW, PoS).

Could you use a regular database? Yes

- But databases are controlled by the administrator
  - Databases are client/server in nature
  - Malicious actors can alter data
  - The administrator decides which data is accessible and visible

- But they are easy to implement and maintain
  - They are fast and scalable

- Blockchains are decentralized and allow for permissionless participation:
  - Decentraland metaverse uses Ethereum blockchain to store/verify info about land parcel ownership and content. It doesn’t run its own blockchain.

Key points of Blockchain in a Metaverse

- Blockchain as a trust technology in the virtual world
  - Provides decentralized, possibly permissionless, and safe data storage

  -> Everyone sees the same virtual world, with blockchain allowing all nodes to synchronize on the same information.
- VR is one of many ways to access and experience a metaverse.
  - Whatever access device, identity can be provided by blockchain.
- Smart contracts help regulate relations and rules within a metaverse
  - Support transfer of value between worlds.
  - Provide a society where people immutably own assets, such as information, along with money

-> Blockchain provides (metaverse) society with agreed upon rules and history of events.

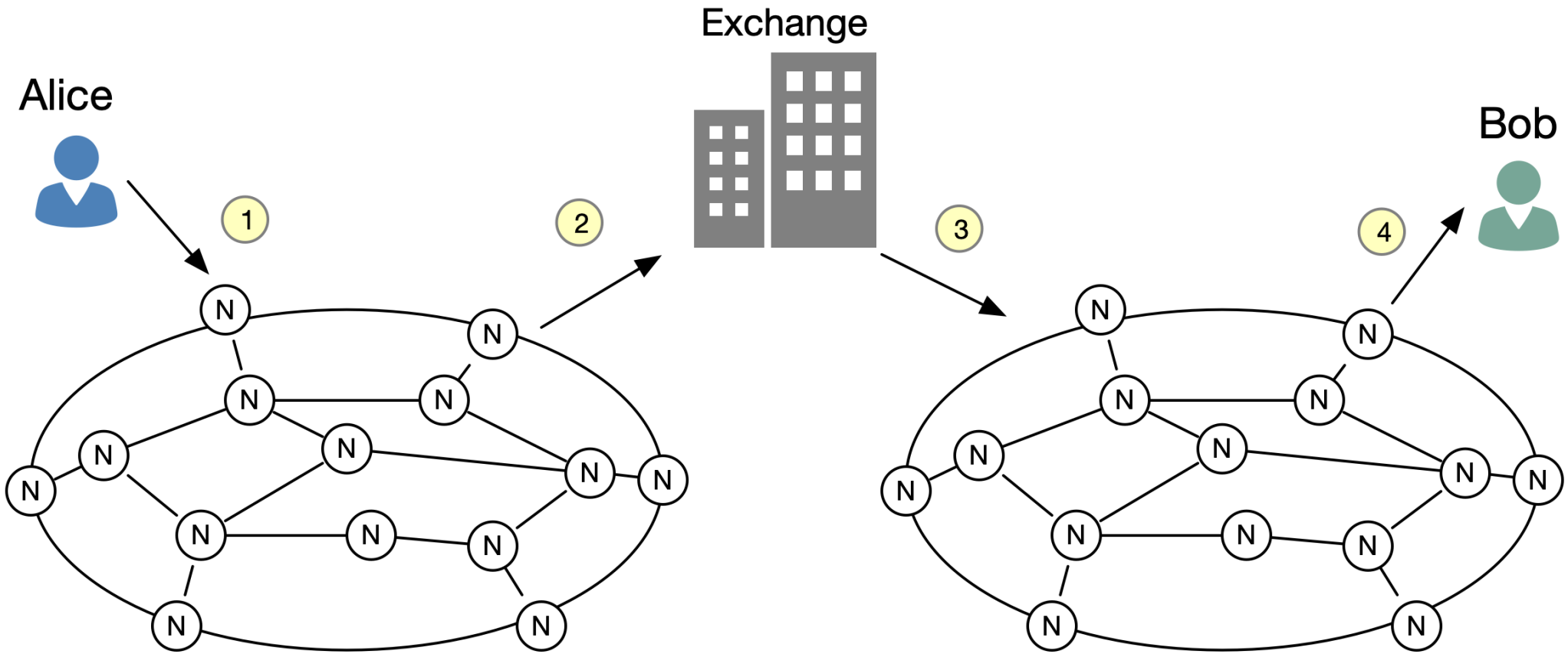
Disrupt the bad guys

- Attack surface expands with Metaverse. Criminals have their own ecosystem and blockchain will help disrupt that ecosystem with its own.
- Blockchain can help show proof of where criminal activity is occurring.
- Blockchain will make the bad guys expend more effort than perhaps intelligence gained.
- Whole idea of a blockchain is to make it publicly visible, perhaps we can use that to our advantage.

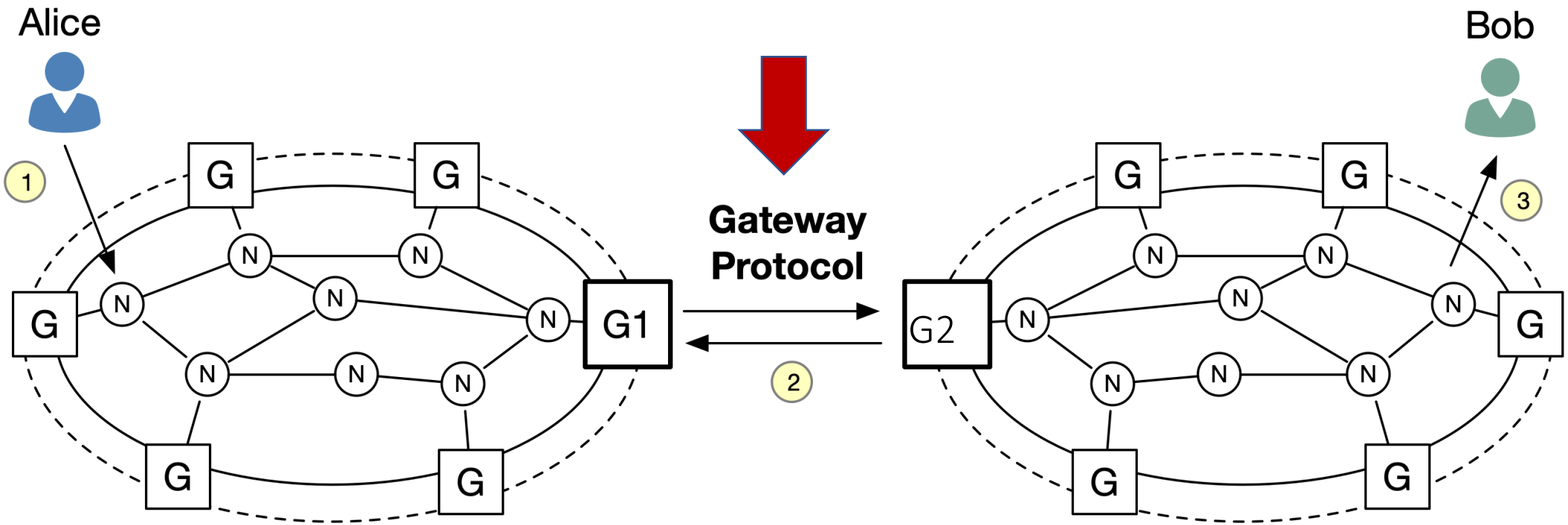
IETF Opportunities

- Consensus algorithms
  - Diffusion protocols
  - Proof of Work (PoW), Proof of Stake (PoS), Proof of Capability, Proof of Space, Leased PoS, Stellar consensus protocol, Delegated Proof of Stake (DPoS), Transaction as Proof of Stake (TaPoS), Delegated Byzantine Fault Tolerance (dBFT), Casper PoS, Proof of Importance (PoI), Proof of Elapsed Time (PoET), Proof of Burn (PoBr)
- Interoperability
  - ~~Cross-Chain Bridges~~
  - SATP WG
- Integration with network functions, such as routing protocols
- Improve on, e.g., scalability and costs, through network innovations
- BaaS

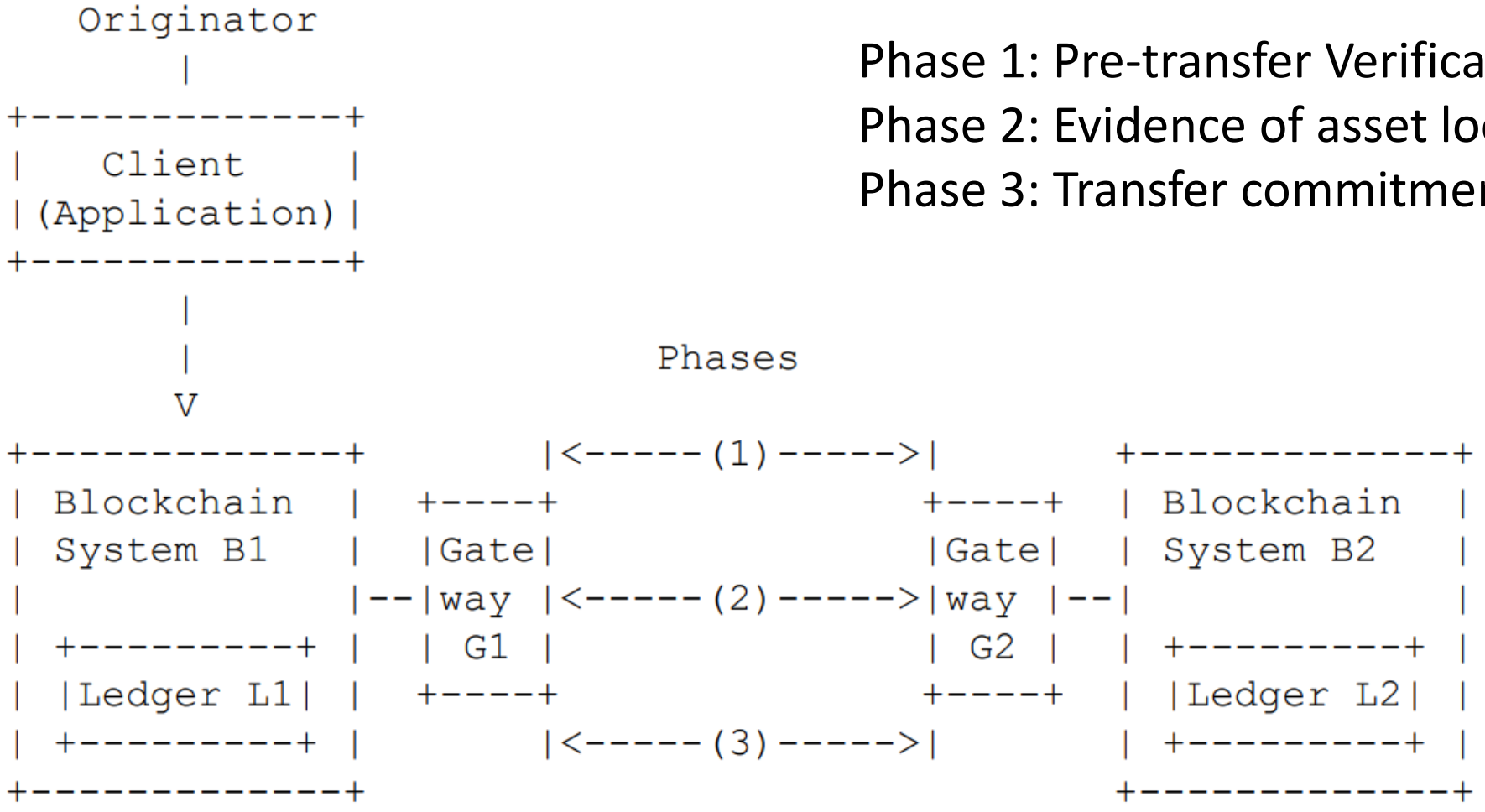
Before SATP



SATP

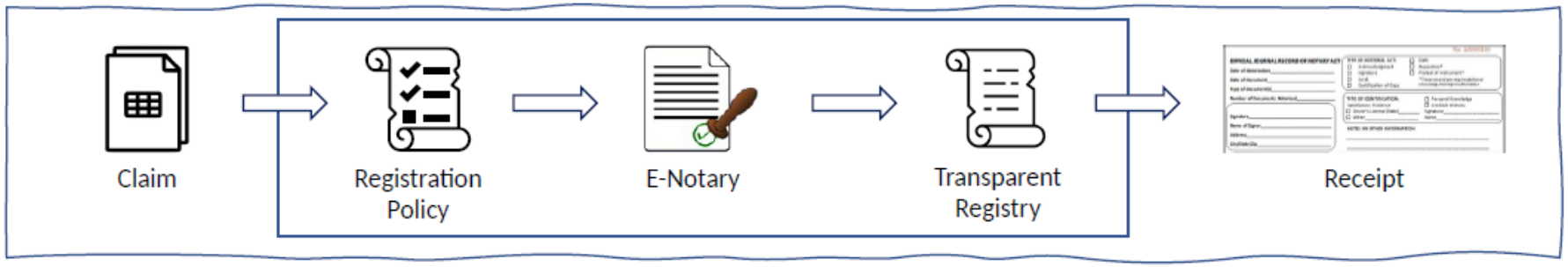


SATP



Phase 1: Pre-transfer Verification of Asset and Identities
Phase 2: Evidence of asset locking or escrow
Phase 3: Transfer commitment

SCITT Definitions and Terms



Claim: An identifiable and non-repudiable statement about an artifact made by an Issuer

Registration Policy: Configuration for the types of identifiers representing issuers that may be verified, or rejected, by the notary before being placed on the registry

E-Notary: The act of verifying the identity of an issuer, submitting content to the system (storage + registry), based on policy, issuing a receipt for valid entry in a registry

Transparent Registry: A verifiable data structure that provides a consistent, append-only, record of all registered claims. Transparency does not *necessarily* mean public access; the notary may implement an access control policy.

Receipt: An offline, universally-verifiable proof that an entry is recorded in the registry. Receipts do not expire, but it is possible to append new entries that subsume older entries

https://ietf-scitt.github.io/draft-birkholz-scitt-architecture/draft-birkholz-scitt-architecture.html#name-definition-of-transparency

Goal for draft-mcbride-rtgwg-bgp-blockchain

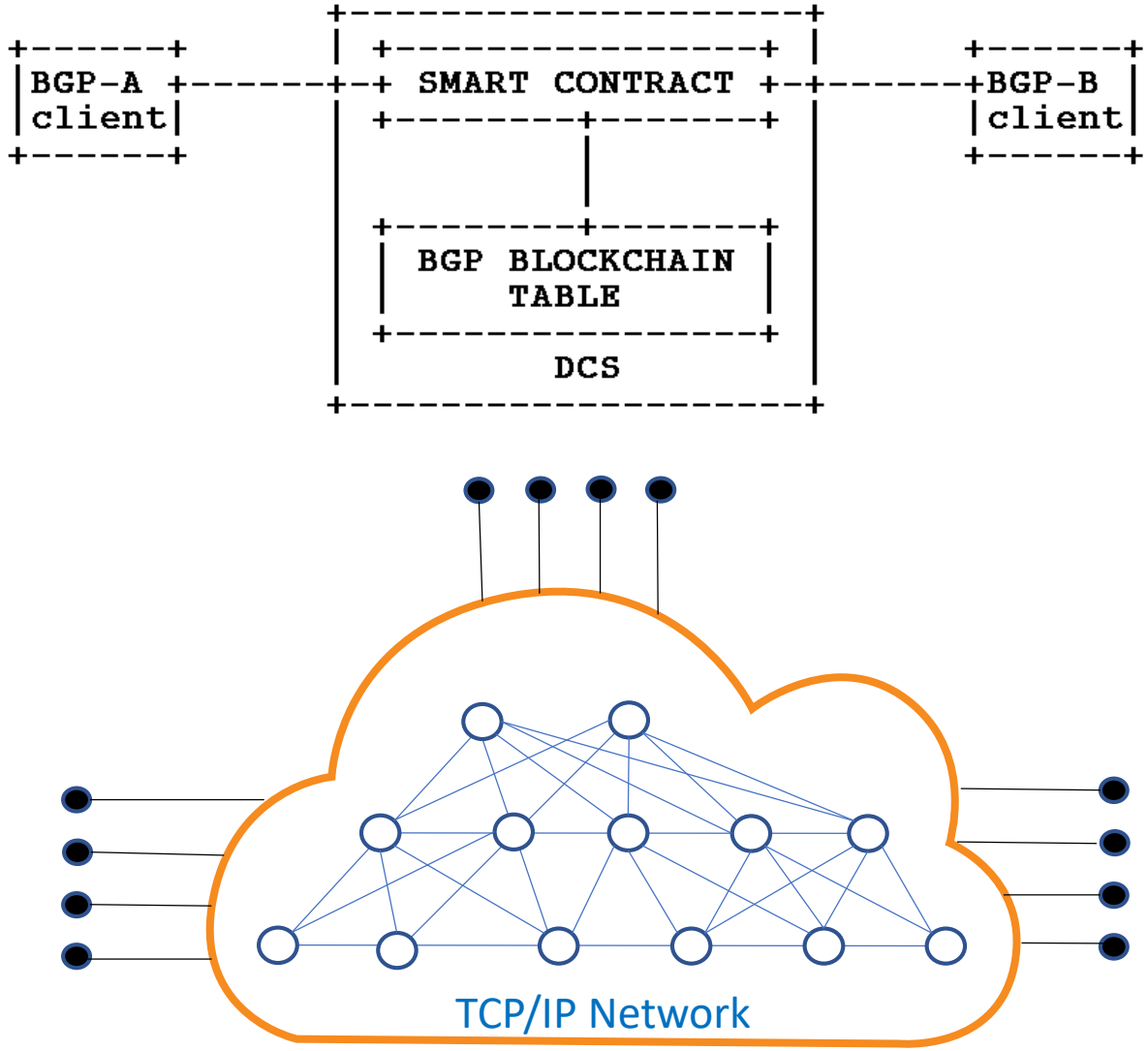
Review possible **opportunities** of using *Distributed Consensus Systems* (DCSs) to secure BGP policies within a domain and across the global Internet

Propose that BGP data could be placed in a DCS and smart contracts can **control how the data is managed**

Create a **single source of truth**, something for which DCSs are particularly well suited, as a **complement** to existing IRR and RPKI mechanisms

Bit of Background

- **Smart contracts** are programs realizing BGP-related operations and store their (distributed) state in a DCS
  -> A DCS could be used to supplement existing BGP management
- A **BGP related smart contract** could be executed when some condition such as receiving an update with too many prepends or hijacking detection
- DCS realized through a **P2P Network** where participating nodes verify transactions, execute smart contracts, boot/seed nodes to bootstrap clients/new nodes, process new blocks, full nodes,lightweight nodes...



Goal for draft-trossen-rtgwg-impact-of-dlts

Perspective of the DLT Application:

- DLTs do not typically care about the underlying TCP/IP network
- They have a P2P overlay network (TCP, UDP based) and that is their focus
- They focus on securing their application and do not worry about the network

Perspective of the Network: What is the impact of choices made by the application design on the network, e.g., in terms of costs, traffic generated etc.?

Our work aims to understand the <u>impact</u> of DLTs on provider networks and the possible <u>opportunities</u> to improve on those impacts

Summary

- Blockchain is currently the backbone for Metaverse assets
    - Various DCSs in use
- There are several opportunities for network innovation and standardization including within the IETF
    - DCS, Routing, Scalability, BaaS
- We’ve been presenting in RTGWG and submitting papers in various conferences. Please join us.