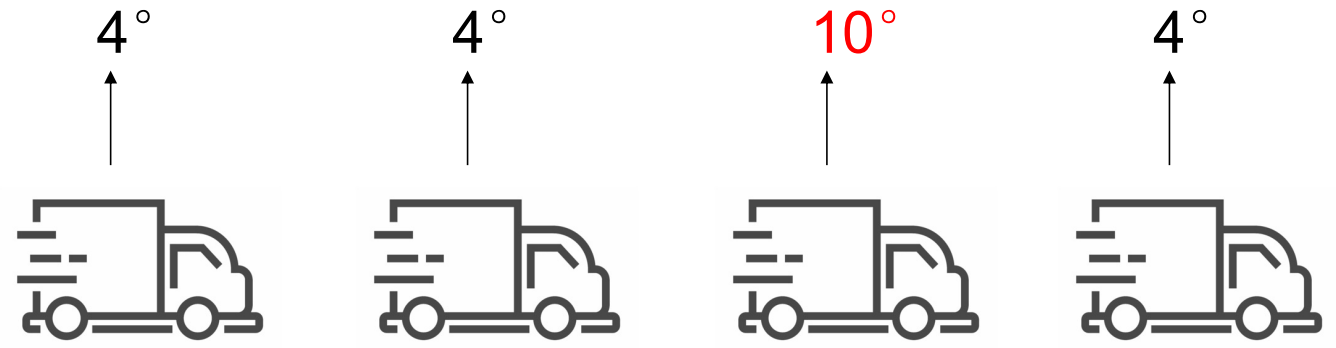
Blockchain in Networking

Mike McBride

Blockchain Standards - Networking

Beyond Cryptocurrency

$Billions tied up in disputes for payments in the transportation industry.



10% of sensitive biopharmaceutical shipments experience temperature deviations. Problems when exceeding acceptable temperature.

Gas sensor solutions for fruit storage and ripening.

Sensor data is captured and radio transmitted to a blockchain.

Blockchains store transactions over a distributed state and help

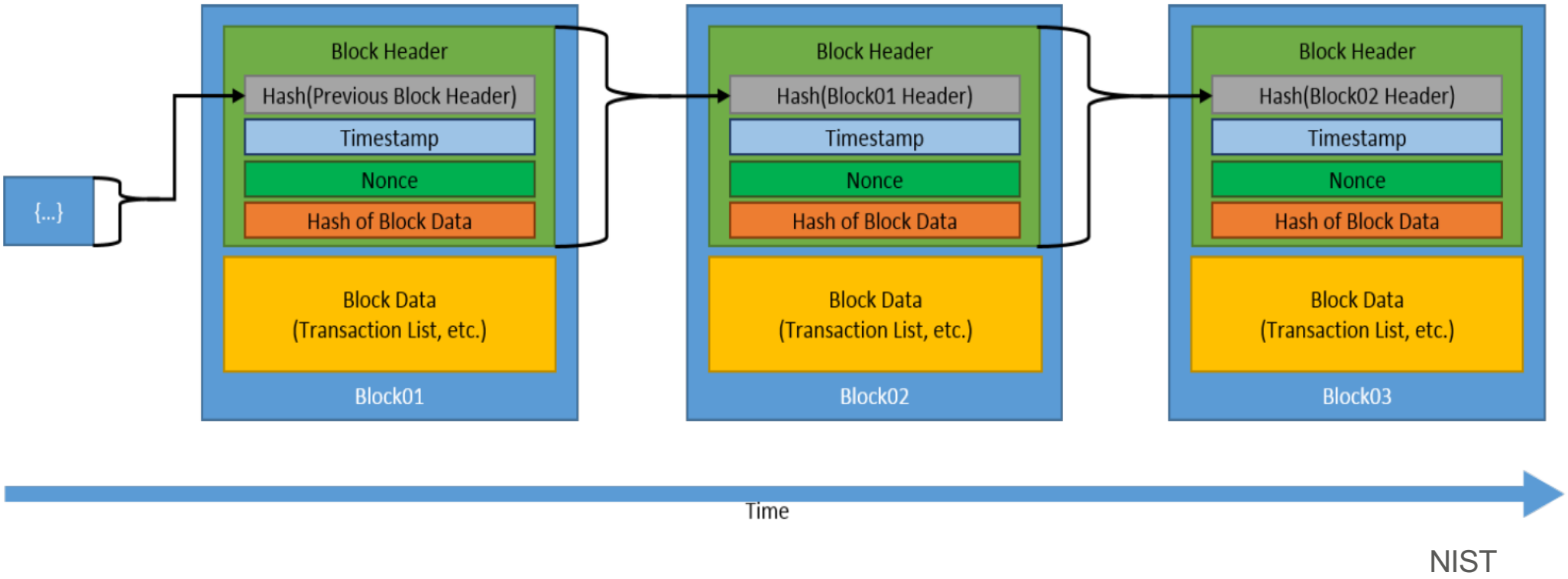
- to determine who owns what,
- to provide asset tracing, and
- to secure digital content and data.

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

Why Blockchain?

- Tamper evident and tamper resistant.
- No transaction can be changed once published.
- Participants agree that transactions are valid. Self policing. Decentralized.
- Distributed. More resilient to attacks by bad actors.
- Cryptographic hashing. Often SHA-256. Use to:
  - Create addresses
  - Secure block data and header
- Can be permissionless or permissioned.
- Smart contract capable.

Blocks


{...}
Block Header
Hash(Previous Block Header)
Timestamp
Nonce
Hash of Block Data
Block Data
(Transaction List, etc.)
Block01
Block Header
Hash(Block01 Header)
Timestamp
Nonce
Hash of Block Data
Block Data
(Transaction List, etc.)
Block02
Block Header
Hash(Block02 Header)
Timestamp
Nonce
Hash of Block Data
Block Data
(Transaction List, etc.)
Block03
Time

NIST

Proof of Work

SHA256(“blockchain” + Nonce) = Hash Digest starting with “000000”

SHA256("blockchain0") =
0xbd4824d8ee63fc82392a6441444166d22ed84eaa6dab11d4923075975acab938
(not solved)

SHA256("blockchain1") =
0xdb0b9c1cb5e9c680dfff7482f1a8efad0e786f41b6b89a758fb26d9e223e0a10
(not solved)

…

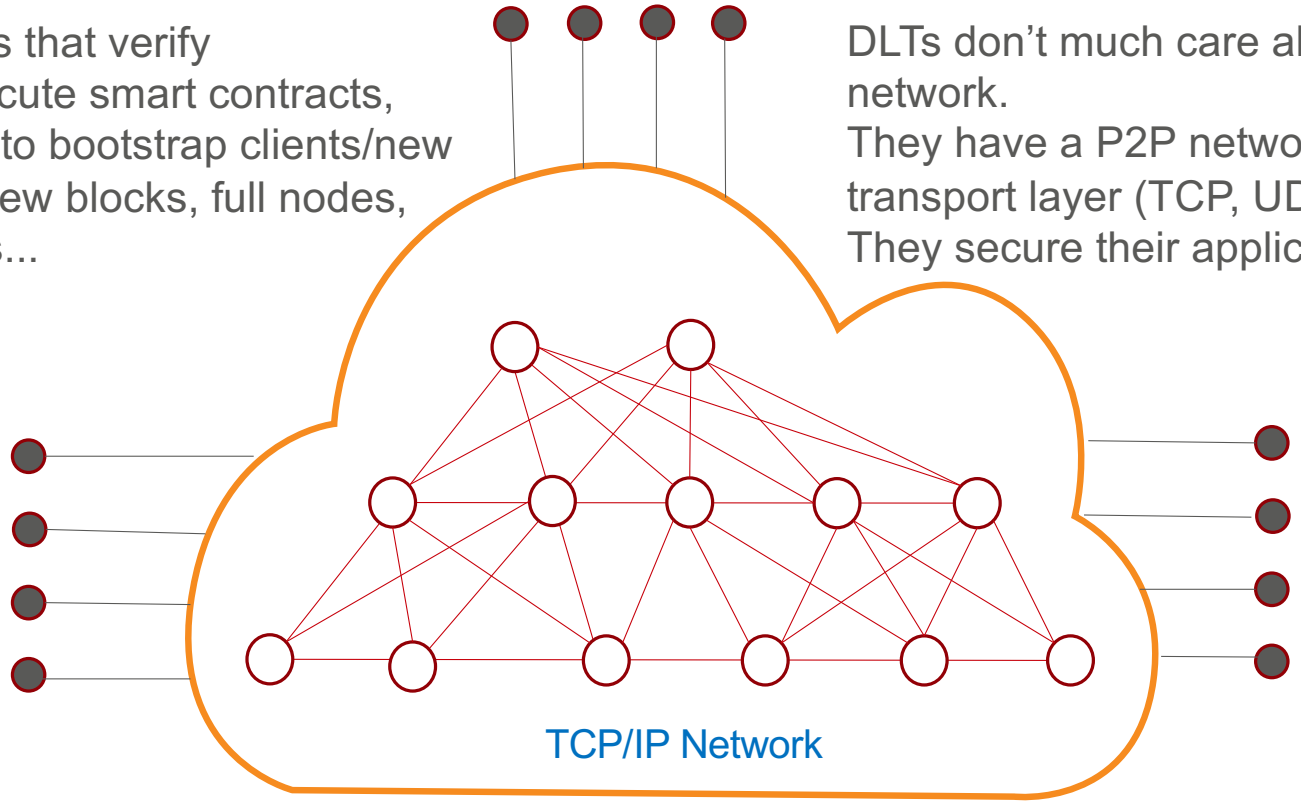
SHA256("blockchain10730895") =
0x000000ca1415e0bec568f6f605fcc83d18cac7a4e6c219a957c10c6879d67587
(solved)

NIST

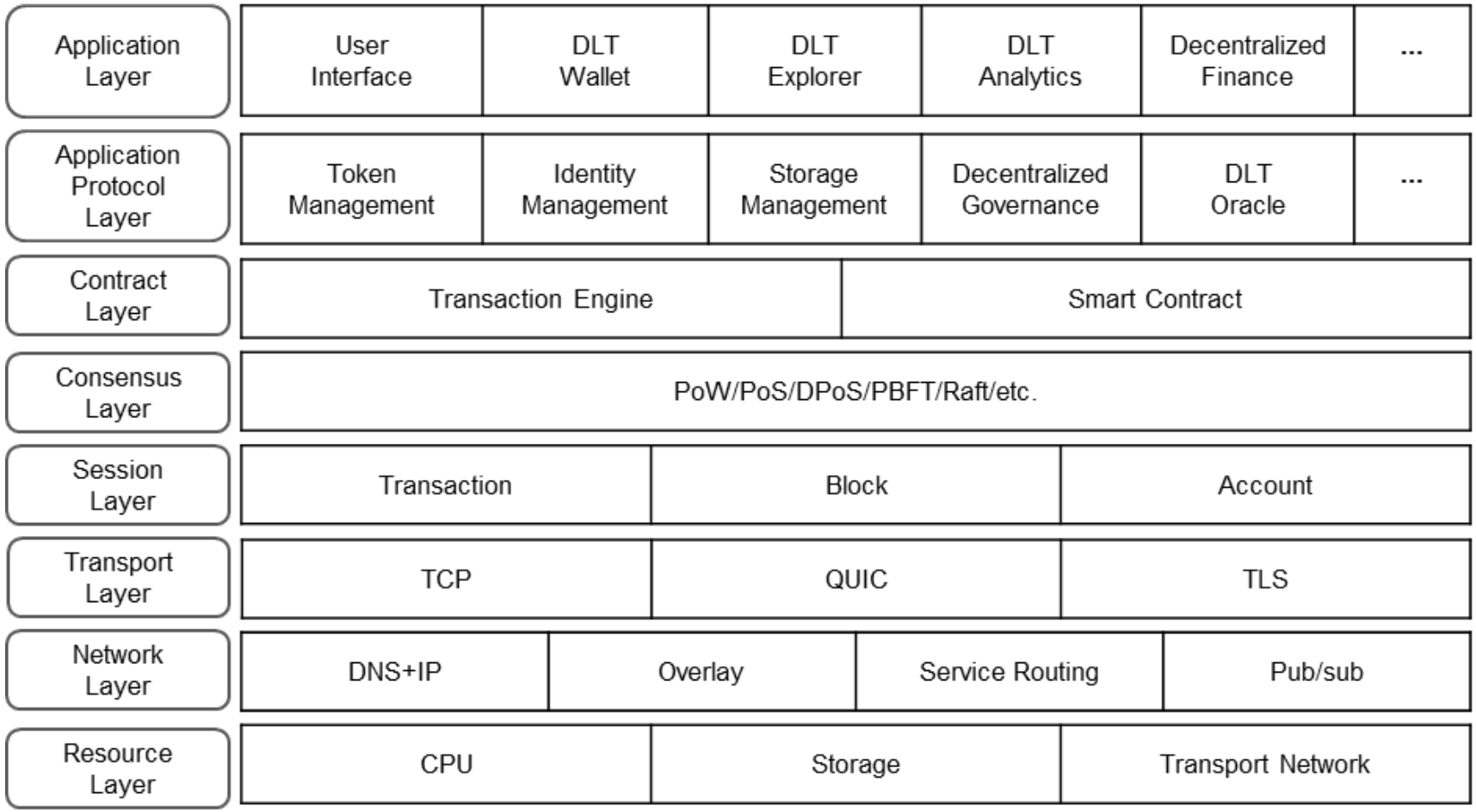
Blockchain P2P Network

Consists of nodes that verify transactions, execute smart contracts, boot/seed nodes to bootstrap clients/new nodes, process new blocks, full nodes, lightweight nodes...

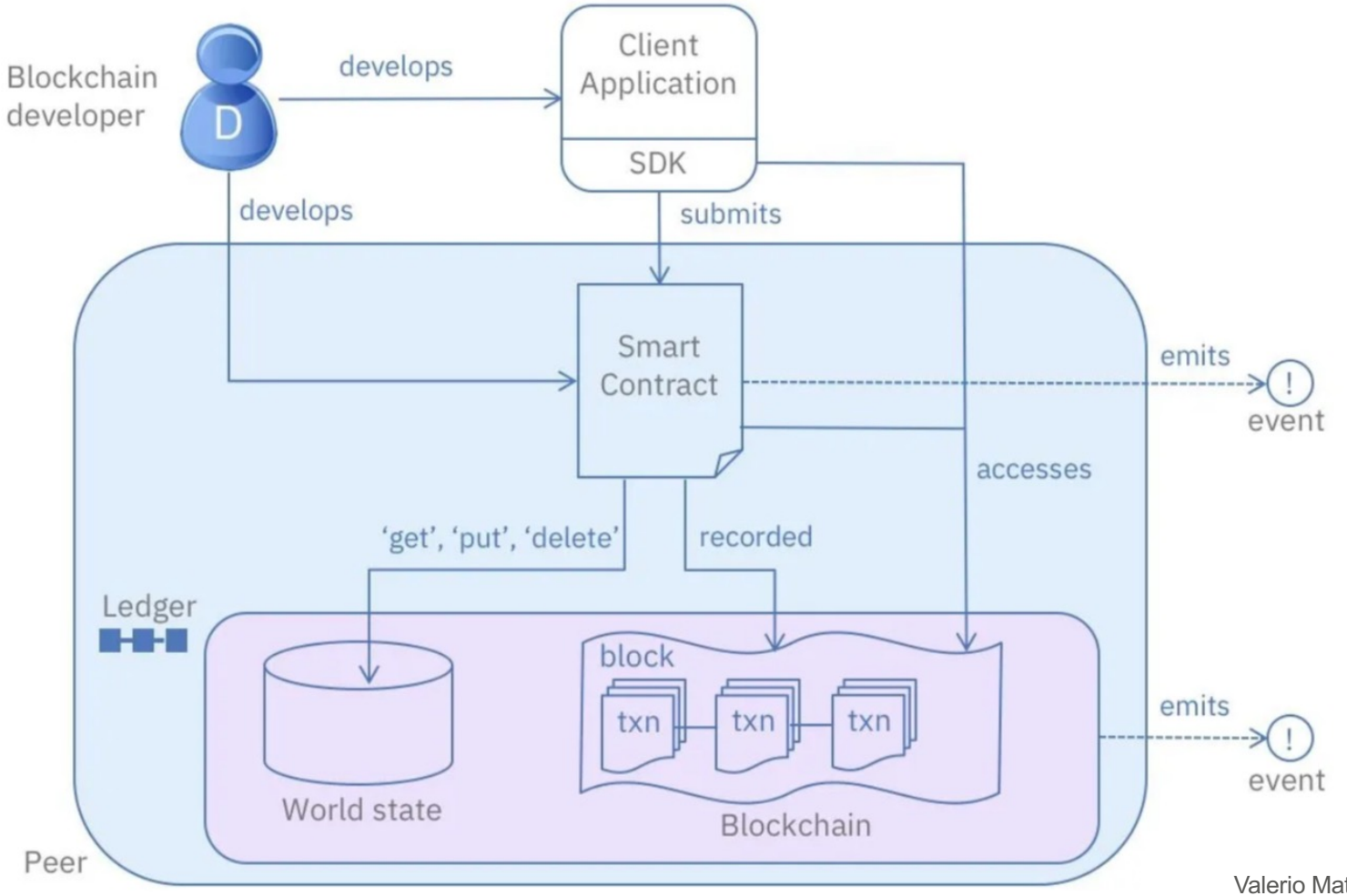
DLTs don’t much care about the underlying network.
They have a P2P network with a pool of transport layer (TCP, UDP) connections.
They secure their application.



IEEE DLT Layering Architecture

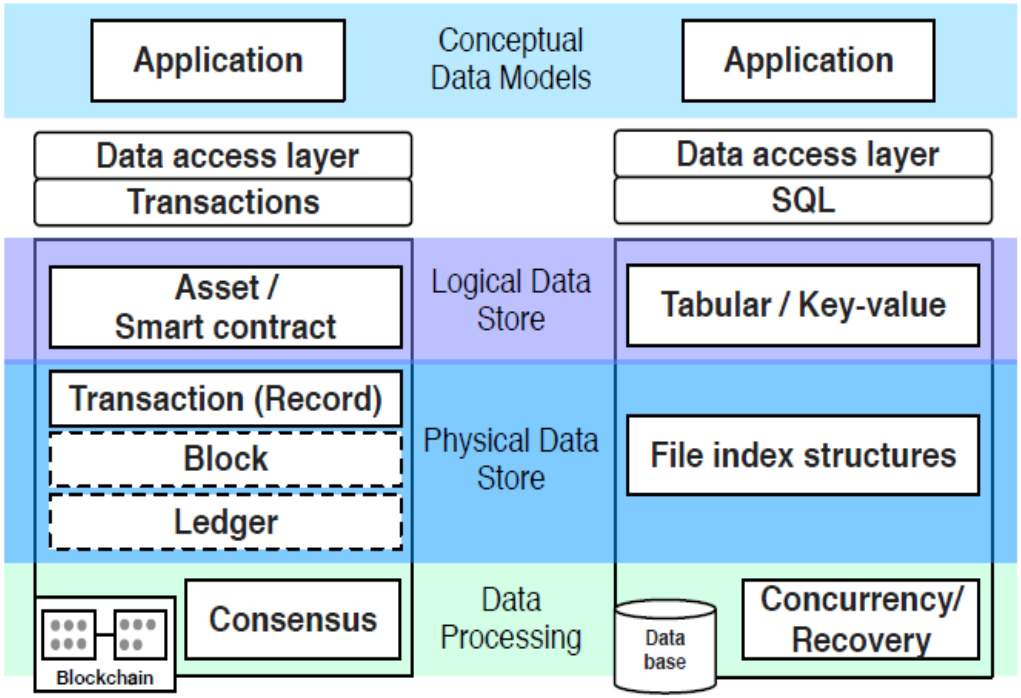


Smart Contract



Valerio Mattioli - Medium

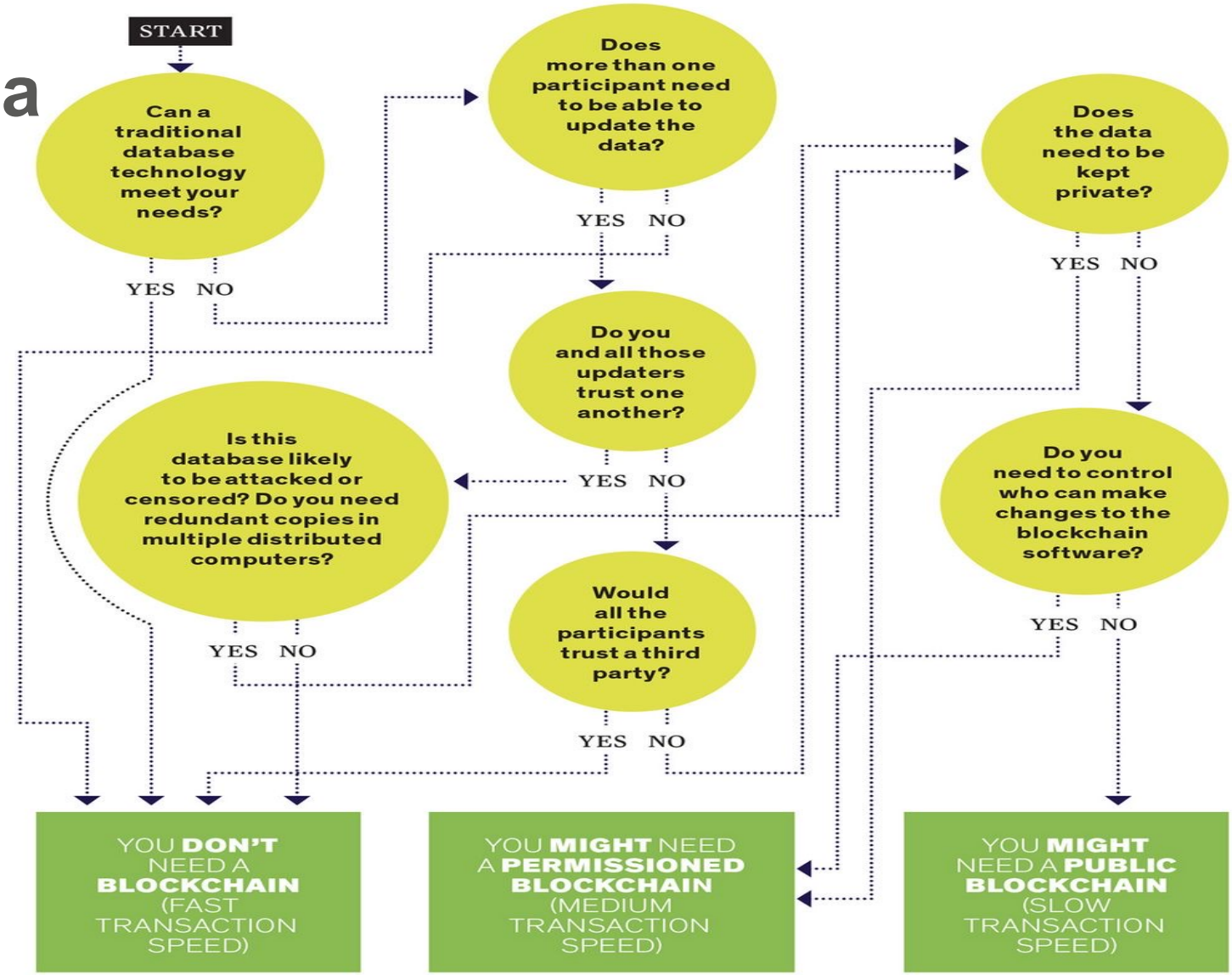
Blockchain vs a Traditional DB?



- Databases are controlled by an admin
  - Client/server in nature
  - Malicious actors can alter data
  - Administrator decides which data is accessible and visible
- They are easy to implement and maintain
  - They are fast and scalable
- Blockchains are decentralized and allow permissionless participation.
  - Nearly impossible to alter data
  - No central administrator authority
  - But not particularly fast

Do You Need a Blockchain?

spectrum.ieee.org



IETF, IEEE, ISO… Opportunities

Consensus algorithms

- 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)...IETF DCS?

Interoperability

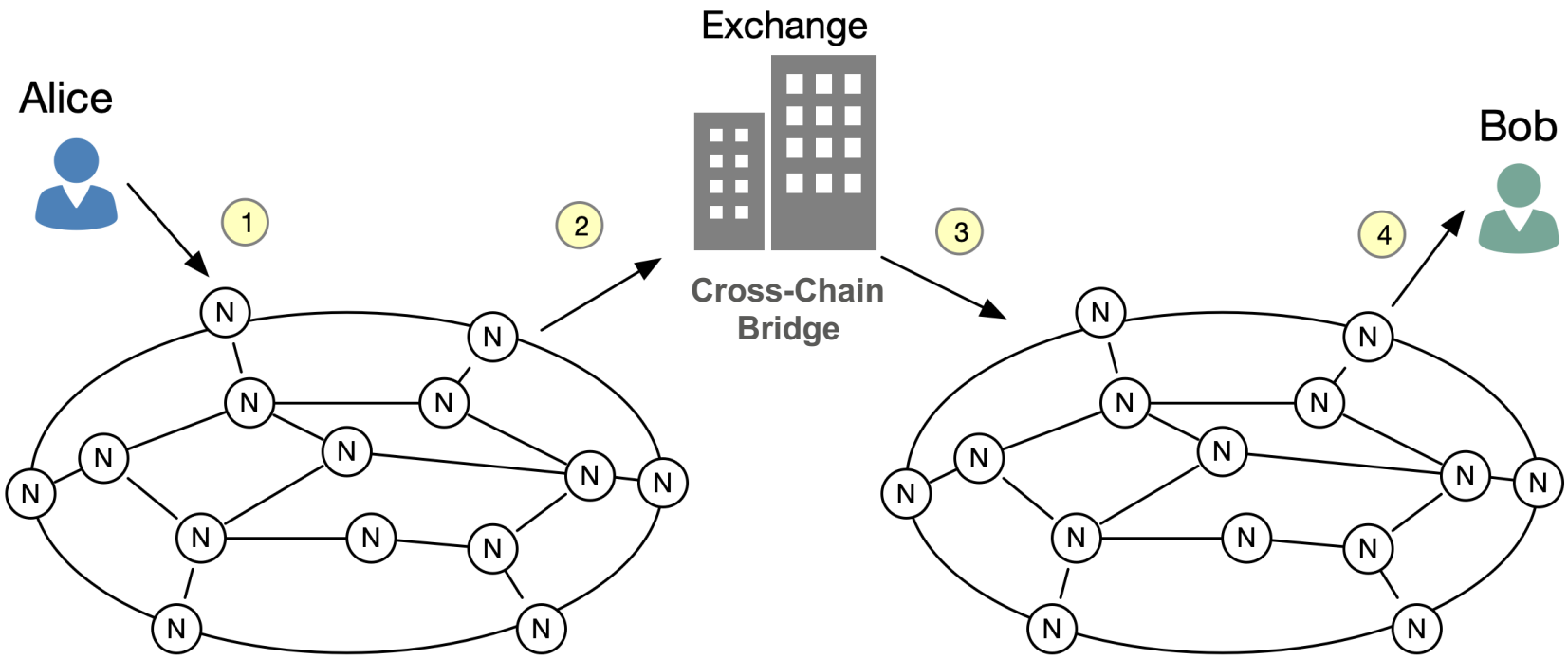
- Cross-Chain Bridges, SATP WG

Integration with network functions

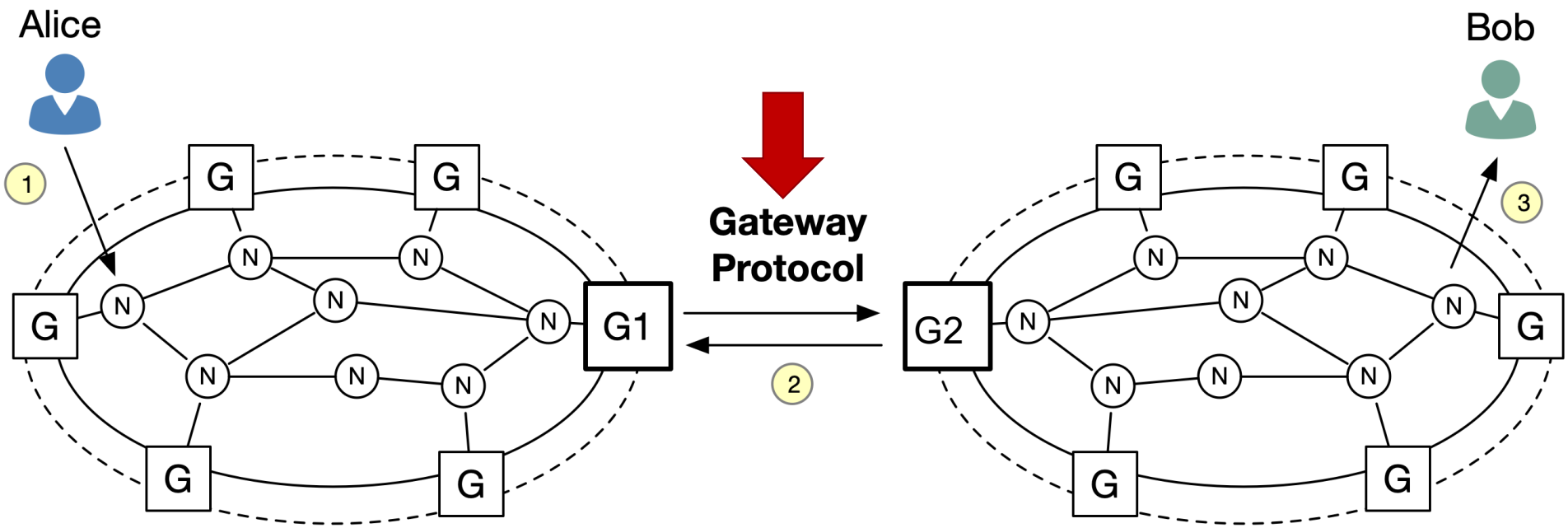
IPv6 Blockchain

Metaverse, BaaS…

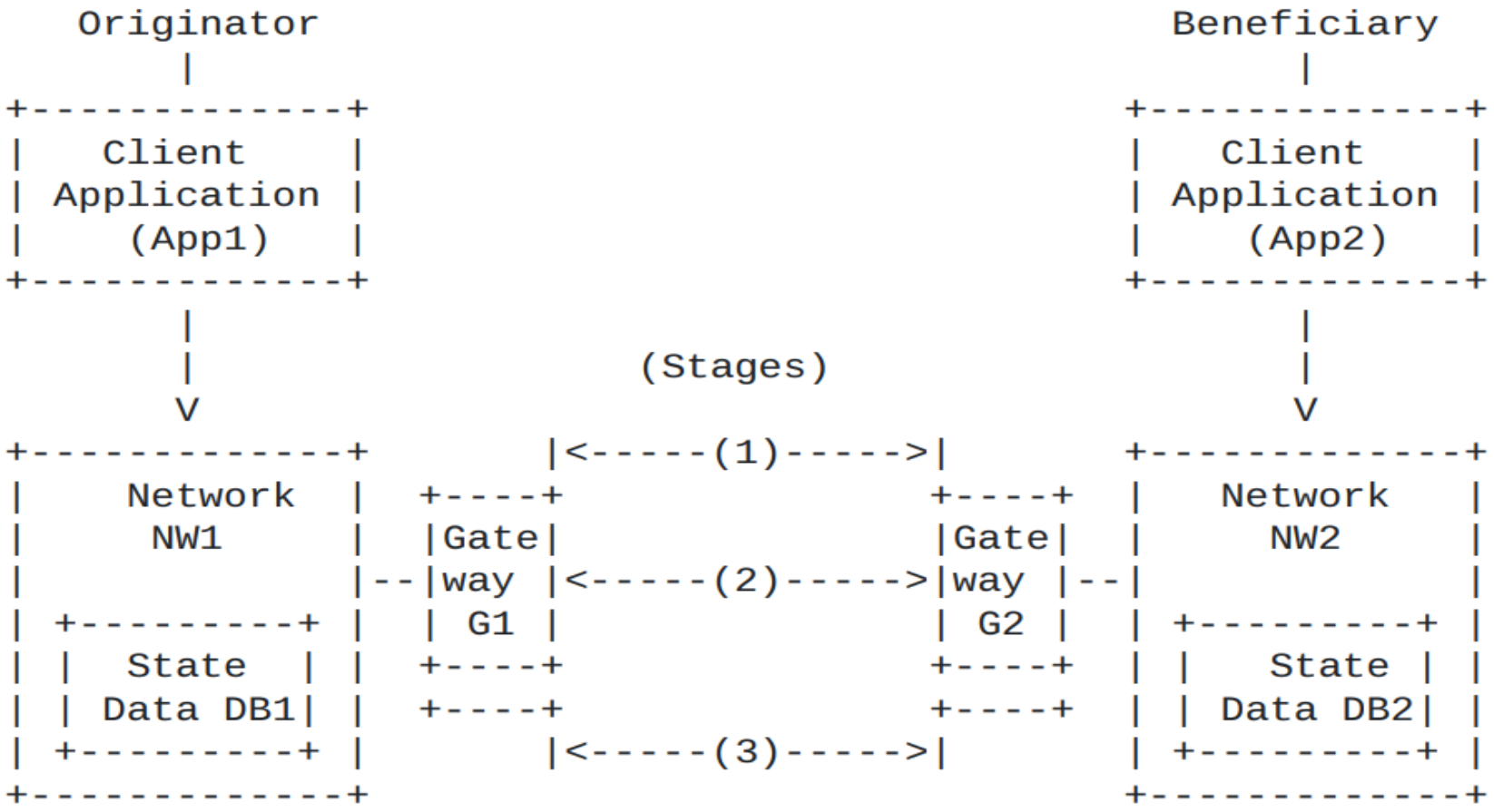
Blockchain Interoperability



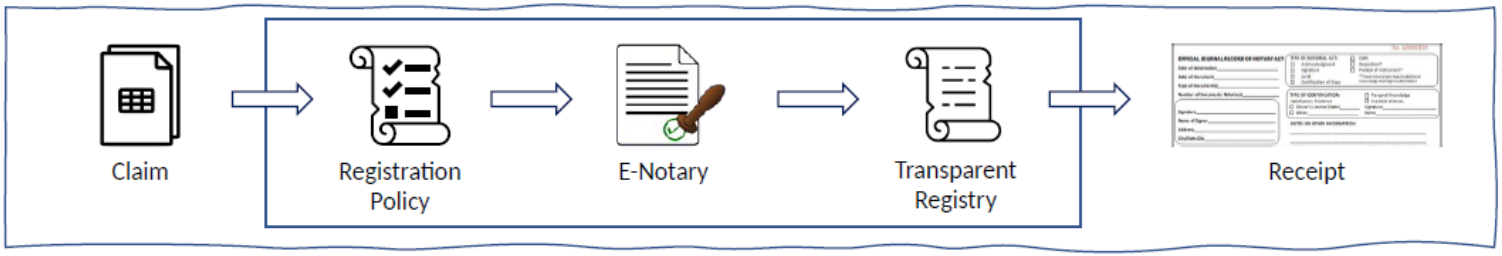
IETF – SATP (Secure Asset Transfer Protocol)



IETF – SATP WG


Originator
Beneficiary
Client Application (App1)
Client Application (App2)
(Stages)
Network NW1
Network NW2
Gateway G1
Gateway G2
State Data DB1
State Data DB2
(1)
(2)
(3)

IETF – SCITT (Supply Chain Integrity Transparency & Trust)



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

Networking Opportunities

- Trust packet capture data
- Network mgmt moves to a decentralized, smart contract-based system
- Signing routing advertisements, proof of transit.
  - BGP/RPKI. ROA's in a blockchain
- Overlays, such as LISP, to find best DLT peer
- Blockchain email
  - Cryptamail, ProtonMail, Mail Chain, Ledger Mail

draft-mcbride-rtgwg-bgp-blockchain

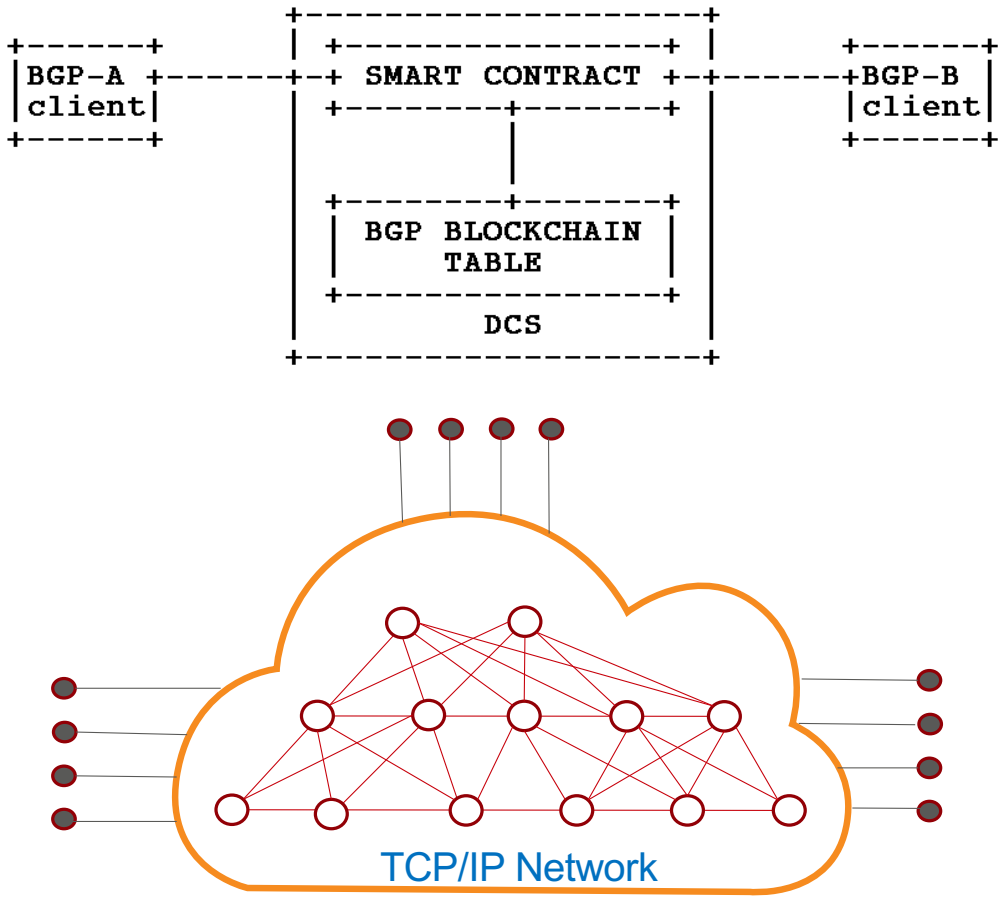
Review possible **opportunities** of using *Distributed Consensus Systems* (DCSs) to secure BGP policies within a domain and across the global Internet

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

BGP-Blockchain 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...



RIR – RPKI Blockchain Options

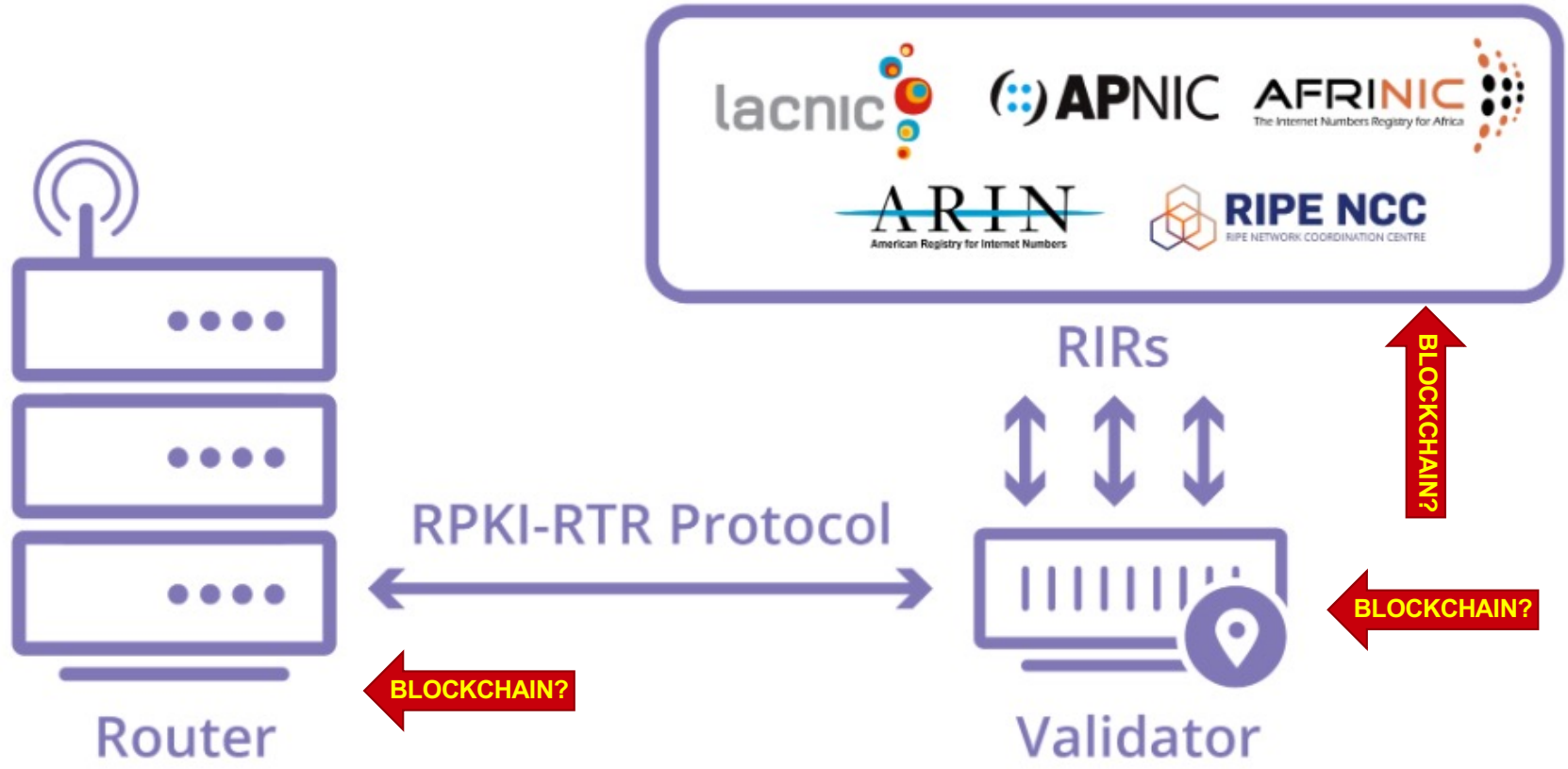


Image: Cloudfare

State Transition Function

The state transition function `APPLY(S,TX) -> S'` can be defined roughly as follows:

1. For each input in TX:
    i. If the referenced UTXO is not in S, return an error.
    ii. If the provided signature does not match the owner of the UTXO, return an error.
2. If the sum of the denominations of all input UTXO is less than the sum of the denominations of all output UTXO, return an error.
3. Return S with all input UTXO removed and all output UTXO added.

State Transition Function (for BGP?)

The state transition function `APPLY(S,TX) -> S'` can be defined roughly as follows:

1. For each input in TX:
    i. If the referenced UTXO (prefix) is not in S, return an error.
    ii. If the provided signature does not match the owner of the UTXO (prefix), return an error.
2. Accept UTXO (prefix) in S’ and add to BGP Blockchain table or Smart Contract.

S = AS 1
S’ = AS 2
TX = Prefix announcement
UTXO = BGP prefix

draft-trossen-rtgwg-impact-of-dlts

Perspective of the DLT Application:

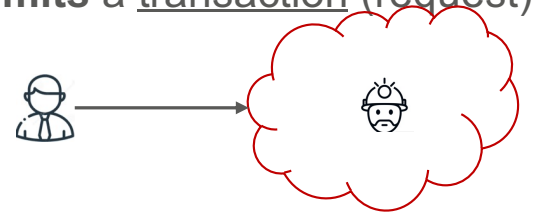
- DLTs do not typically care about the underlying TCP/IP network
- They have a P2P overlay network (TCP, UDP based) and that is their focus
- They focus on securing their application and do not worry about the network

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.?

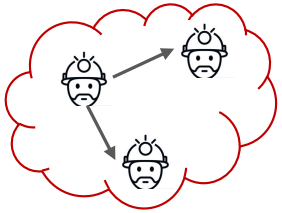
Our work aims to understand the impact of DLTs on provider networks and the possible opportunities to improve on those impacts

DLT Interactions

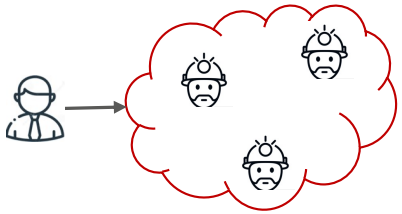
- A client **commits** a transaction (request) to the DLT



- A miner **commits** a found block to the DLT

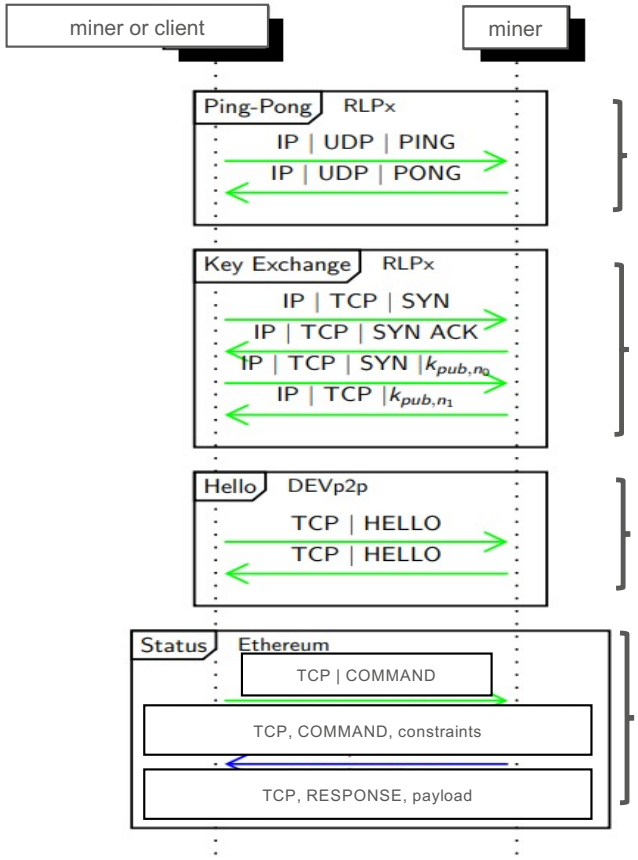


- Any client or miner can **read** the blockchain in the DLT



All of those interactions are between originator and *N* peers, i.e. inherently **multipoint** in nature

Communication Patterns



Node discovery

Transport security

Keep alive, used to maintain a given sized (about 1500) **pool of peers** to communicate with for the transactions

Transactions to be executed at miners with RESPONSE specific to transaction type with miners selected from pool of peers

This may lead to disconnects with ***reachable miners*** if constraints do not match

Challenges of DLT in Networking

Problem 1: Information is required to reach other peers

- Bootstrap nodes maintain IP addresses of all peers (plus port information)
- New DLT members ***need to download routing information*** upon joining and for regular update

Problem 2: Clients know nothing about peers' capability to serve requests

- Approach is to (1) contact potential peer, (2) wait for connection, (3) inquire capabilities, (4) disconnect if not matching
- Peers ***may never reply*** to connection establishment (step 2)

Problem 3: Peers map sending of transactions onto unicast communication

- Negatively impacts ***efficiency*** (bandwidth usage) and ***completion time***

Problem 4: Need to expose IP address to Bootstrapping Node

- Sending IP address during DLT sign-up may lead to ***privacy*** and/or ***security*** issues

On Using Multicast for DLTs…

- **Highly individualized** operations
  - > Seeding from bootstrap nodes, discovery of other peers, constantly changing pool of transport connections

    -> **frequently changing multicast** trees if multicast were to be used.
- **Highly distributed** DLT network
  - > Discovered nodes, i.e. potential members of DLT pool, may reside ANYWHERE within the geo spread of the DLT
    -> **inter-domain support** for multicast poses a problem, possibly requiring hybrid approaches (e.g., replay nodes)
- **Highly dynamic** pools per peer
  - > Pools are constantly refreshed to randomize membership
    -> meaning the pool of peers undergoes **constant changes**, possibly incurring **high membership signaling**
- **Highly diverse peers** in overall DLT network
  - > May range from individual at home over hosted VM in cloud to entire private clouds
    -> **multicast may or may not be supported** in local domain or enabled for peer

Reality Check

- Immutability is not strictly true
- Oracle problem
- Unpublished transactions
- Malicious mining
- Trust in cryptographic technologies
- Resource usage

Summary

- SDO's are specifying blockchain standards
- Blockchain is the backbone for crypto assets
  - Non-cryptocurrency (supply chains) gaining momentum
- Could be opportunities for blockchain in networking
  - Networking DCS
  - Private Blockchain to secure data
  - Replace RIR Database
  - New PKI application (Blocks)
  - Supplement (or replace) RPKI
  - Interoperability
  - Scalability
  - Multicast
  - Supply Chain Integrity
  - Mail
- DLTs have an impact on provider networks
  - Understanding traffic impact is important for network innovations

Thank You.

FUTUREWEI
Technologies