Metaverse and Blockchain

Mike McBride

A DLT, such as Blockchain, will be a key element in a secure, transparent, Metaverse ecosystem. It determines who owns what.

Key points of Blockchain in a Metaverse

- Blockchain as a trust technology in the virtual world.
- Blockchain provides decentralized safe data storage.
- Everyone sees the same virtual world and blockchain allows all nodes to synchronize on the same information.
- Smart contracts help regulate relations and rules within a metaverse.
- Supports transfer of value between worlds.
- Provides a society where people immutably own assets.
  - Information, along with money, is an asset.
- Provides society with agreed upon rules and history of events.
- VR is one of many ways to access and experience a metaverse.
  - Whatever the access devices, identity can be provided by blockchain.
- ERC-20, ERC-721 Blockchain protocol standards.

Disrupt the bad guys

- Criminals have their own ecosystem and blockchain will help disrupt that ecosystem with it’s 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.

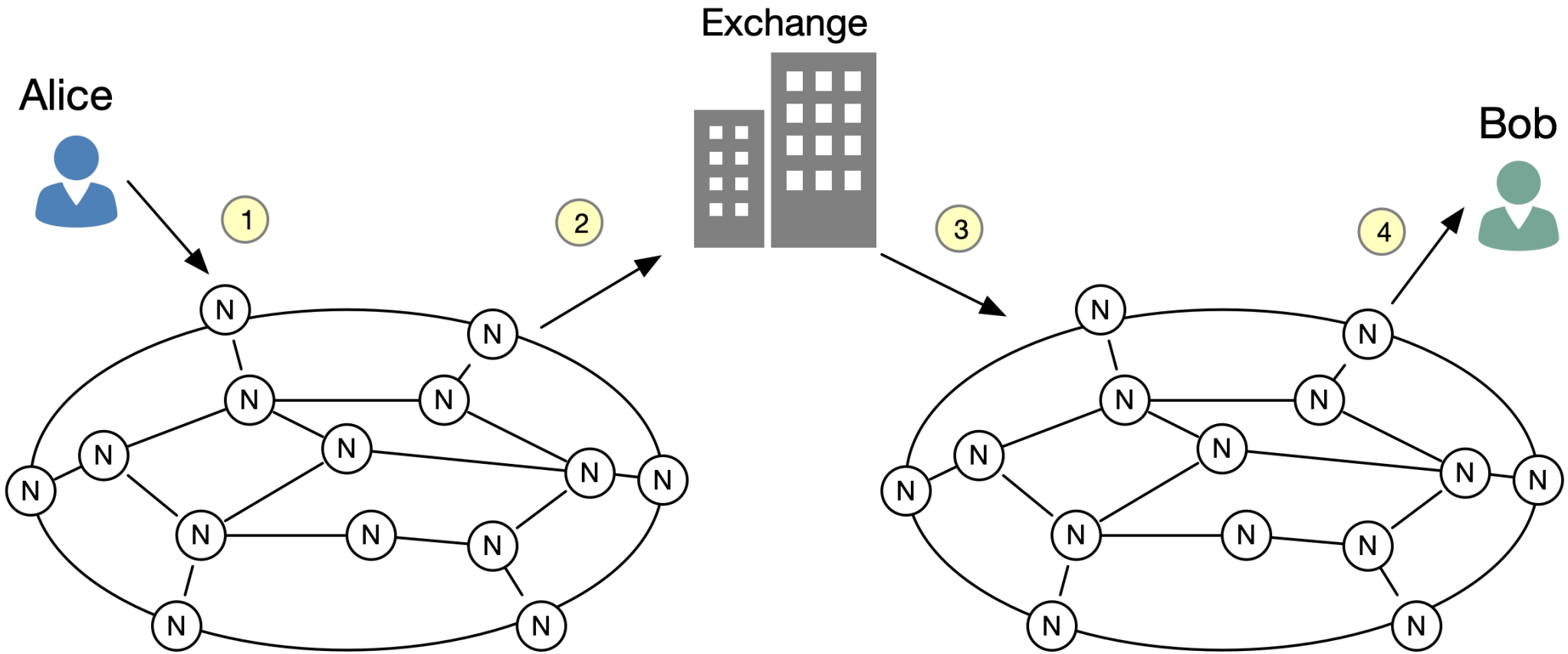
Could you use a regular database? Yes…

- 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
- Easy to implement and maintain
- Fast and scalable
  - draft-trossen-rtgwg-impact-of-dlts

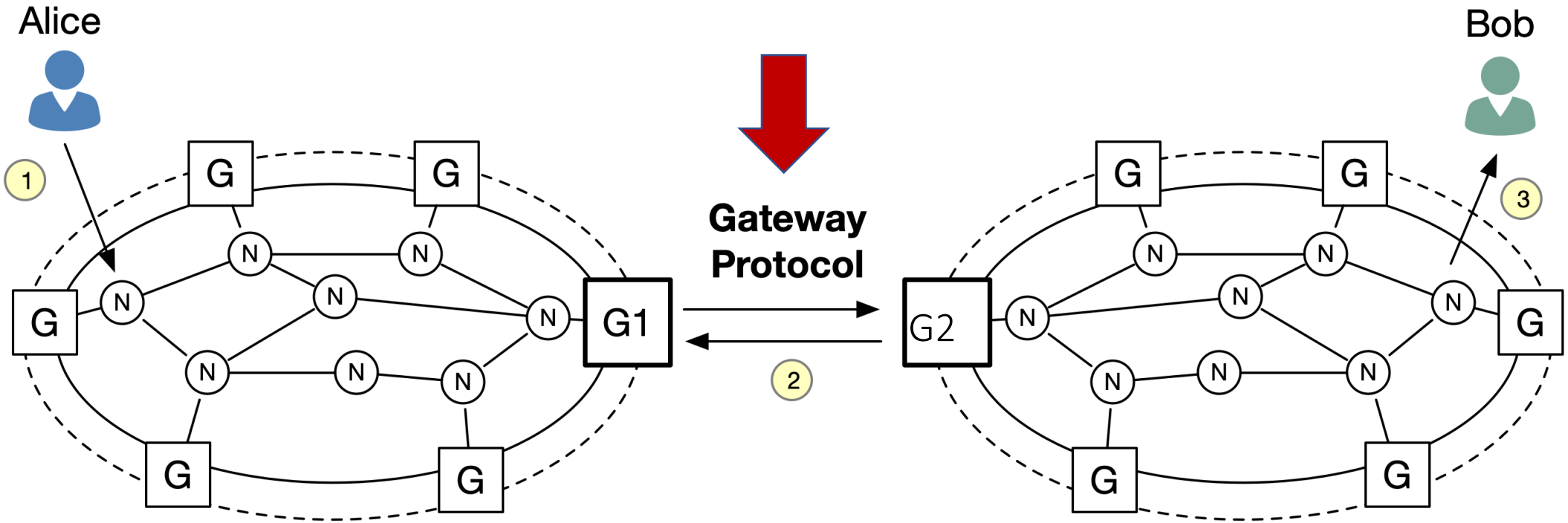
Use Case: Metaverse currency

- Purchase of property
- In fact the virtual purchase of anything you can buy in the real world.
- Create an avatar and digital identity to manage all assets.
- Use Bitcoin or Ethereum or something new (MANA, Robux) to make purchases within both a metaverse and the real world.
- NFT’s offer proof of students academic credentials ie degrees.
- Games, voting, art, event ticketing, clothing, music…

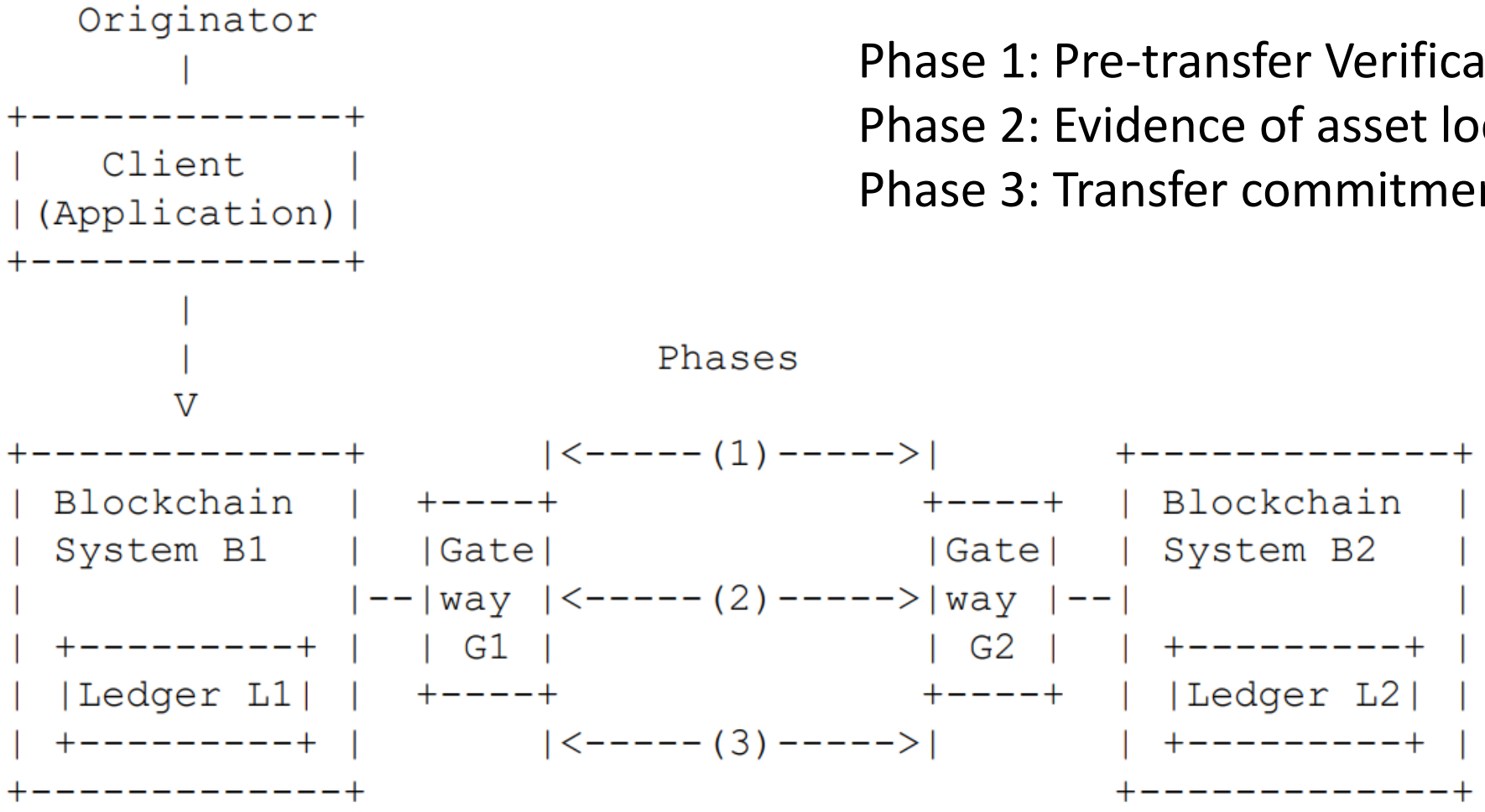
draft-hardjono-sat-architecture



IETF Proposed Solution

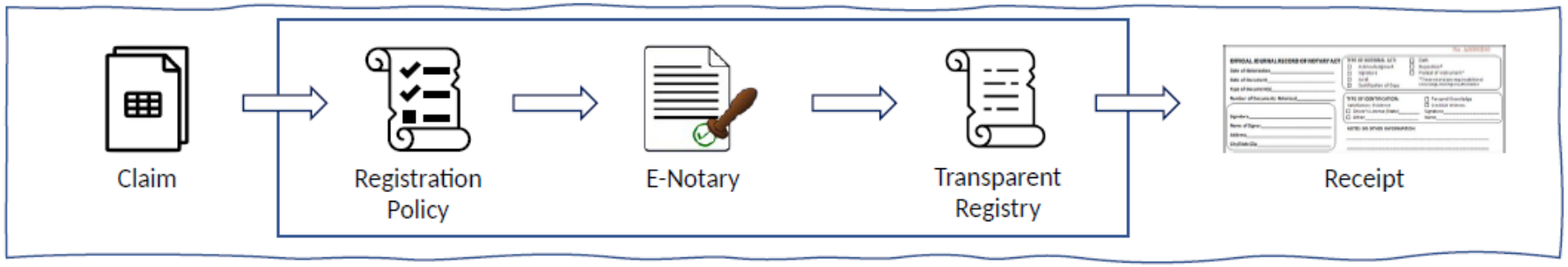


IETF Proposed Solution:



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

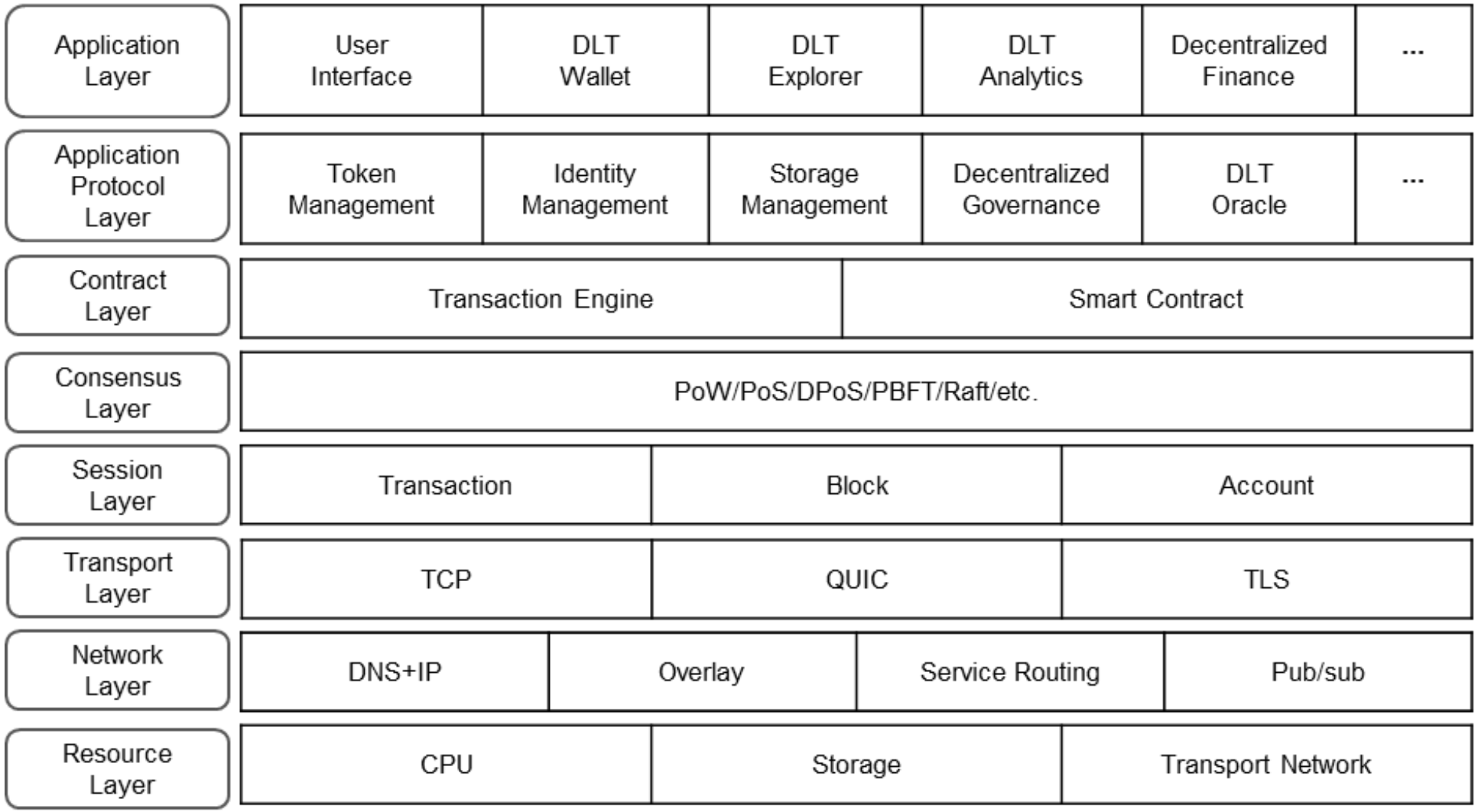
Registration Policy: Configuration for the types of identifiers representing issuers that may be verified, or rejected, by the notary before being placed on the registry

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


Application Layer
User Interface
DLT Wallet
DLT Explorer
DLT Analytics
Decentralized Finance
...
Application Protocol Layer
Token Management
Identity Management
Storage Management
Decentralized Governance
DLT Oracle
...
Contract Layer
Transaction Engine
Smart Contract
Consensus Layer
PoW/PoS/DPoS/PBFT/Raft/etc.
Session Layer
Transaction
Block
Account
Transport Layer
TCP
QUIC
TLS
Network Layer
DNS+IP
Overlay
Service Routing
Pub/sub
Resource Layer
CPU
Storage
Transport Network