Blockchain for BGP

draft-mcbride-rtgwg-bgp-blockchain

Trossen, Guzman, McBride

Cut to the Chase

- A DCS, like Blockchain, could be used out of band (like RPKI) to supplement existing BGP management perhaps by using a smart contracts.
- Smart contracts are if/then programs stored on a blockchain that run when predetermined conditions are met. Automate the execution agreements.
- A BGP related smart contract could be executed immediately when some condition such as receiving an update with too many prepends or hijacking detection. Action could be to deny the update after consulting blockchain.
- Could simply use a blockchain to securely store config files or ROA's.
- Tools exist to do this but a blockchain makes it transparent, secure and could be used globally or within a domain.

Before the Chase

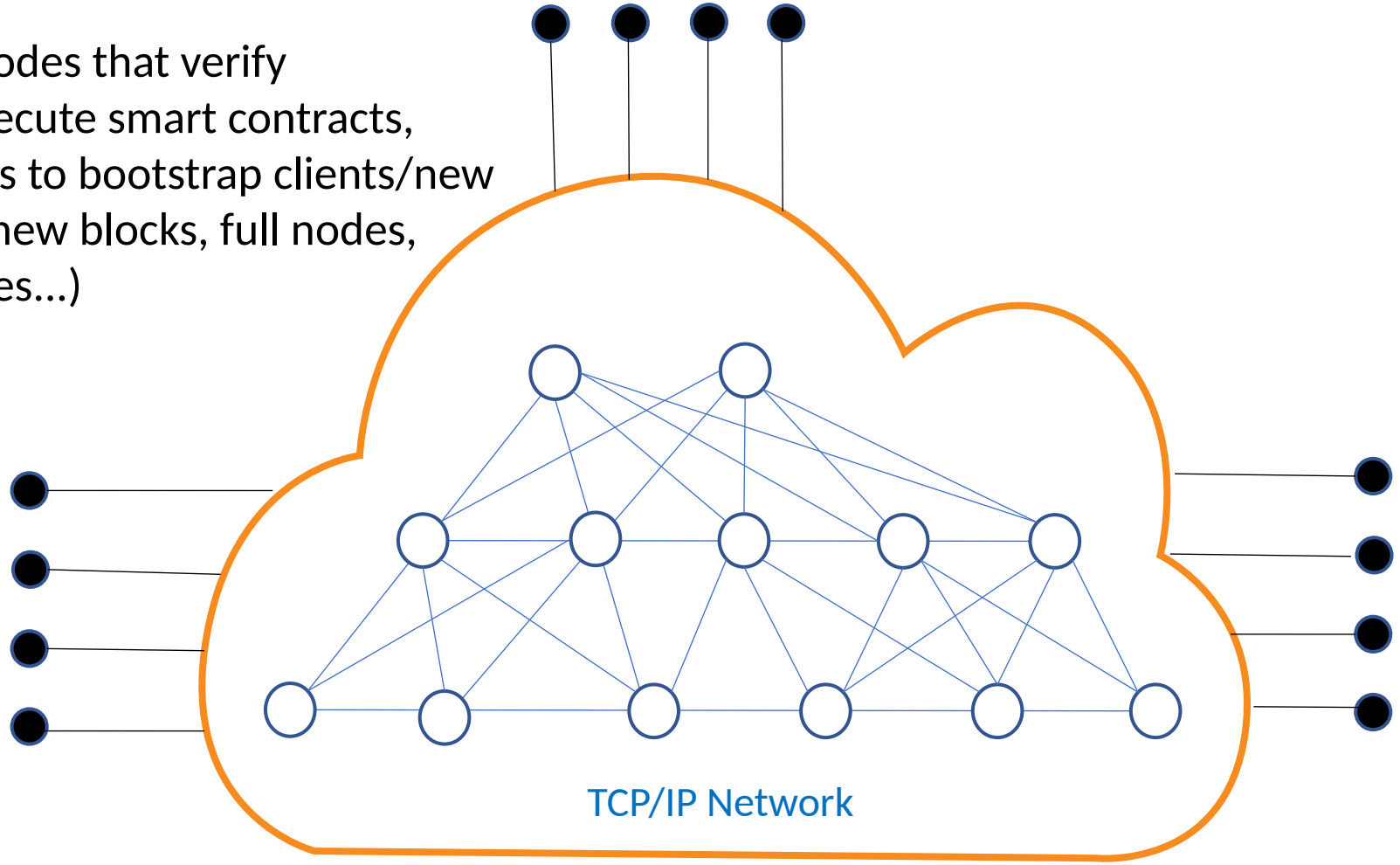
- DLT proposals happening in IETF.
  - draft-mcbride-rtgwg-bgp-blockchain
  - draft-trossen-rtgwg-impact-of-dlts
  - draft-hardjono-sat-architecture
  - draft-birkholz-scitt-architecture
- Q’s about DLT in Networking and what’s going on in the IEEE/IETF/etc.
- Held a side meeting at 113 to discuss DLT in Networking.
  - Networking in a Metaverse side meeting this IETF
- This bgp blockchain draft is informational and not an endorsement.
- Asks: “Is it possible to use a distributed consensus system, like blockchain, to manage (and secure) BGP?”

The DLT Network

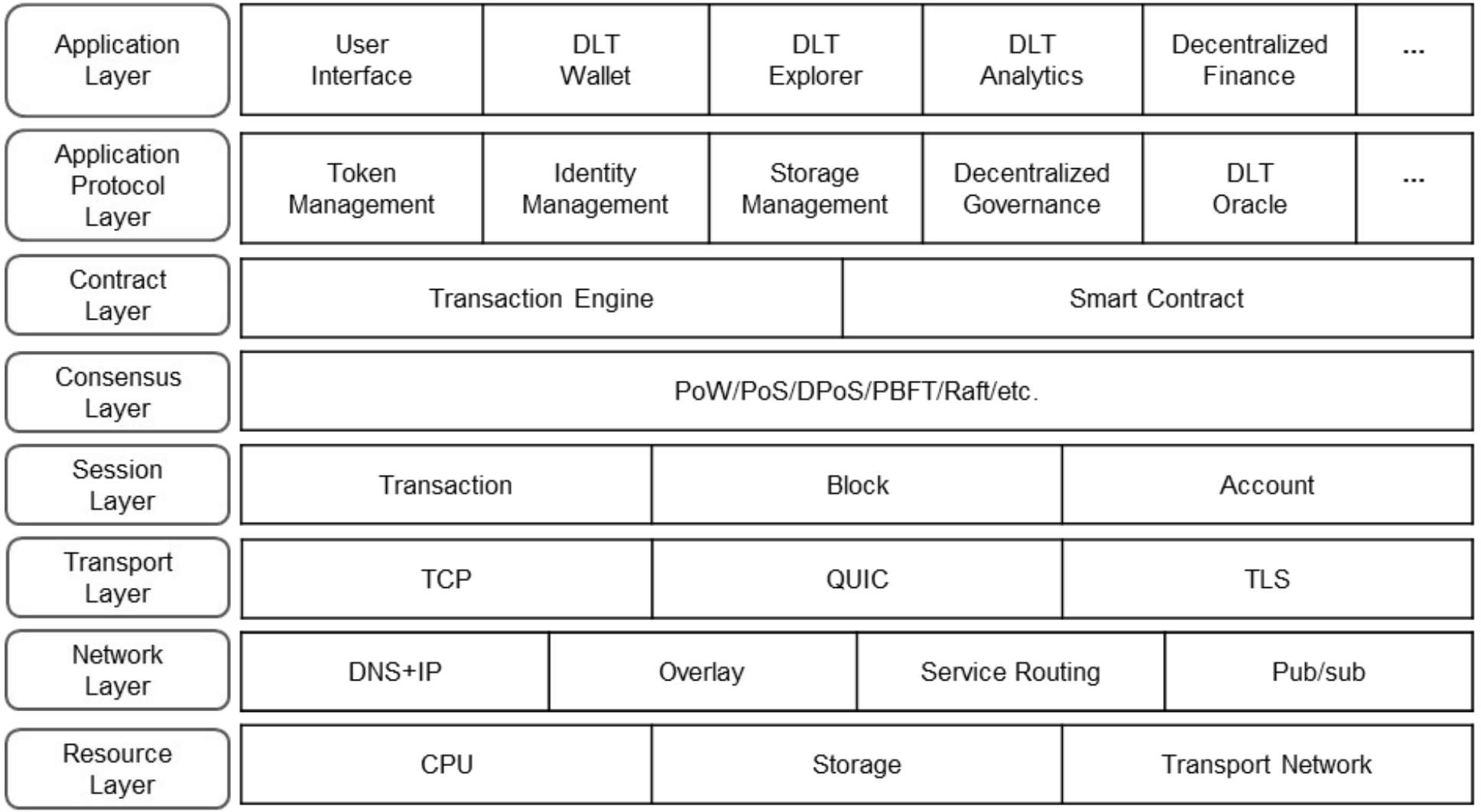
- Crypto currencies and DLTs don’t much care about the underlying provider network.
- They have a P2P network with a pool of transport layer (TCP, UDP) connections.
  - Important to understand the impact of pool management mechanisms on provider network costs, see for instance https://datatracker.ietf.org/doc/draft-trossen-rtgwg-impact-of-dlts/
- They have done a good job securing their application.

The Network

P2P Network (nodes that verify transactions, execute smart contracts, boot/seed nodes to bootstrap clients/new nodes, process new blocks, full nodes, lightweight nodes…)



DLT Layering Architecture



Disrupting 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

Opportunities

- Trust packet capture data
- Network mgmt moves to a decentralized, smart contract-based system.
- Signing routing advertisements, proof of transit.
- BGP management. ROA’s in a blockchain.
- Overlays such as LISP

Potential BGP Opportunities

- Avoiding fraudulent BGP origin announcements
- Validating incoming BGP updates
- Providing routing policy such as QoS
- Protecting BGP config files
- Providing path validation
- Securing BGP Controllers
- Securing Blockchain compromised by BGP vulnerabilities
- BGP functional resilience and reliability

Summary

- Smart contracts are programs executed within a DCS.
  - A BGP DCS could use smart contracts for BGP capabilities.
- N miners, which implement the distributed consensus for a desired smart contract.
  - A DCS may implement more than one smart contract
- DCS could be *permissioned* (e.g., AS owners) or *permissionless*, while client transactions could be separately secured by authorizing any clients (through RPKI)
- ROA entries could be added to the DCS as secure transactions and those transactions would be relied upon by route validators as authoritative