

BGP Blockchain

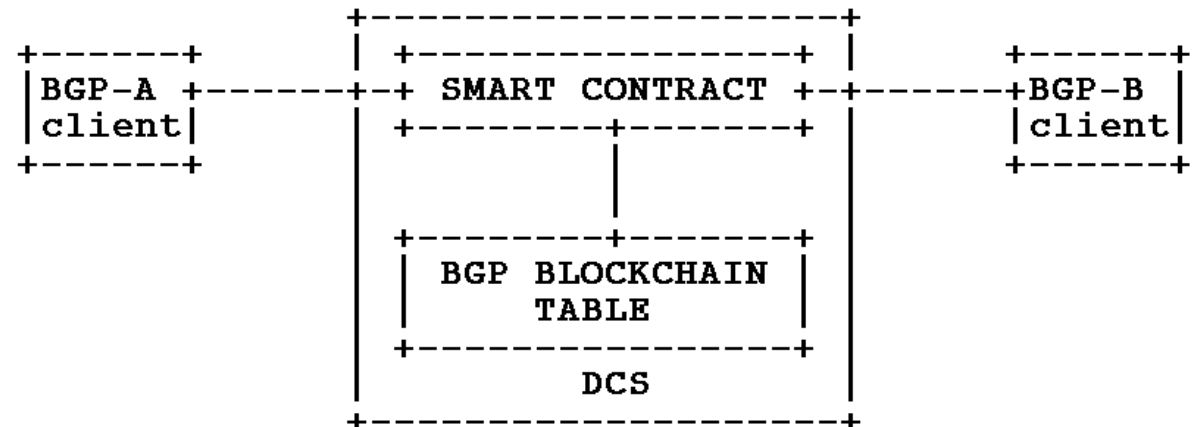
draft-mcbride-rtgwg-bgp-blockchain

Background

- DLT proposals happening in IETF (SCITT, SATP).
- Inquiries 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.
- This bgp blockchain draft is informational and not an endorsement.
- Asks: “Is it possible to use a distributed consensus system, like blockchain, to further secure BGP?”

Overview

- 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



Potential BGP Opportunities

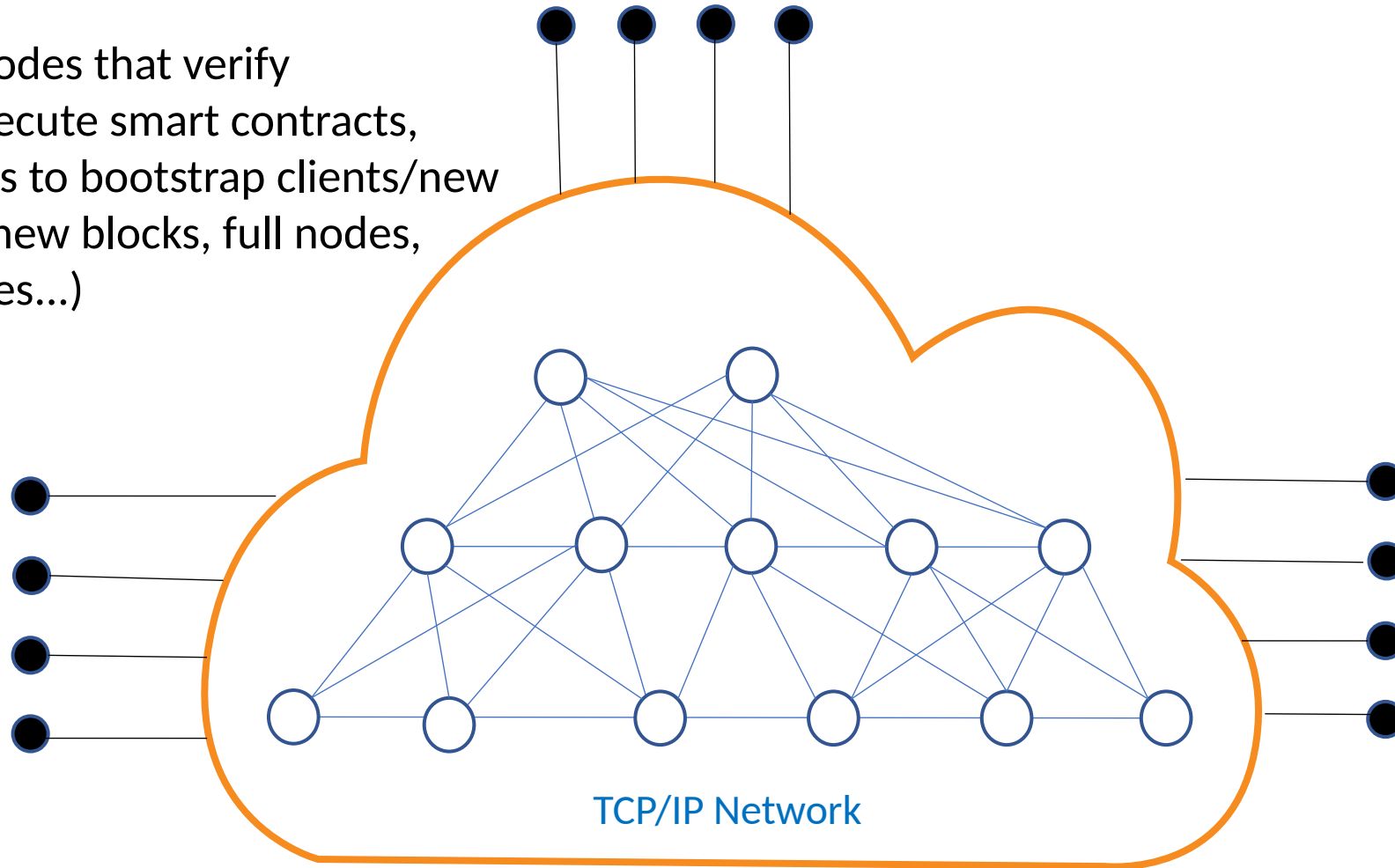
- Preventing fraudulent BGP origin announcements
- Validating incoming BGP updates
- Providing routing policy such as QoS
- Protecting BGP config files
- Providing path validation
- Securing BGP Controllers
- Securing Blockchain compromised by BGP vulnerabilities
- BGP functional resilience and reliability

The DLT Network — if time permits

- 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...)



Opportunities

- Trust packet capture data
- Network mgmt moves to a decentralized, smart contract-based system. Web 3.0.
- Signing routing advertisements, proof of transit.
- BGP/RPKI. ROA's in a blockchain.
- Overlays such as LISP

DLT Layering Architecture

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	