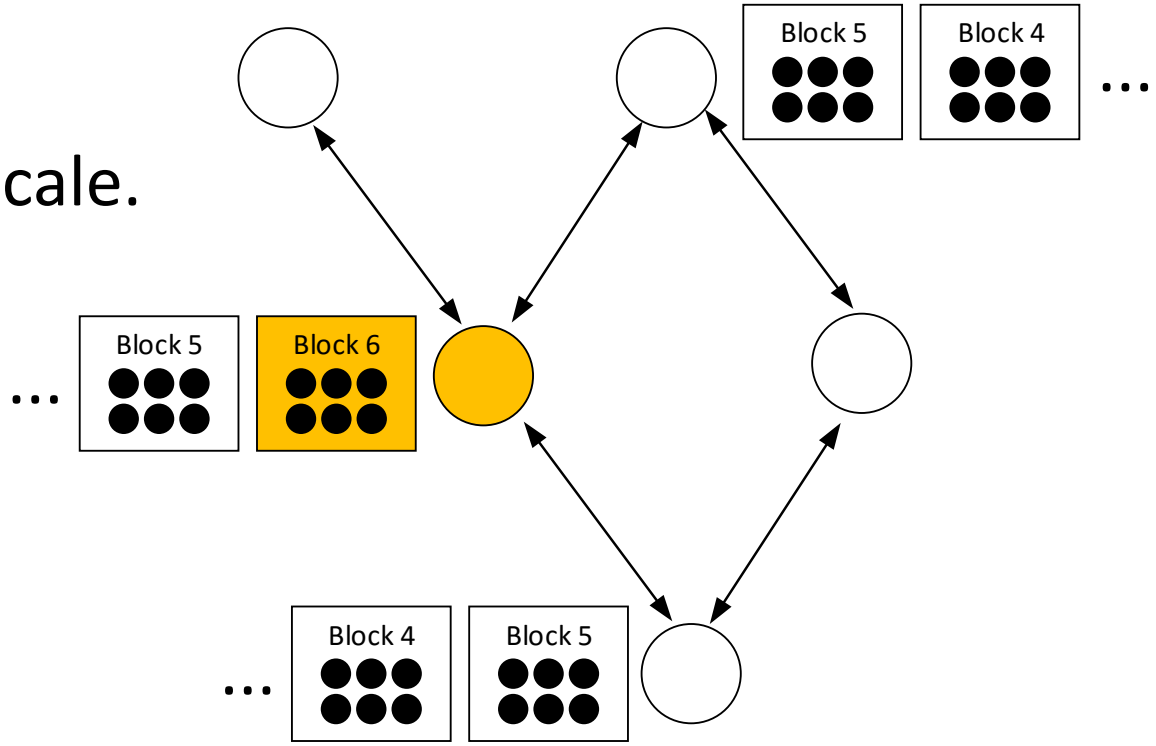
ALTO for the blockchain

draft-hommes-alto-blockchain-01

Stefan Hommes, Beltran Fiz, Radu State - University of Luxembourg
Anton Zuenko, Richard Caetano – Stratumn
Vijay Gurbani - Bell Laboratories

Requirements for blockchain networks

- Large number of *transaction* and *blocks* that need to be propagated, but low throughput.
- Need of being in sync on global scale.
- Low latency.

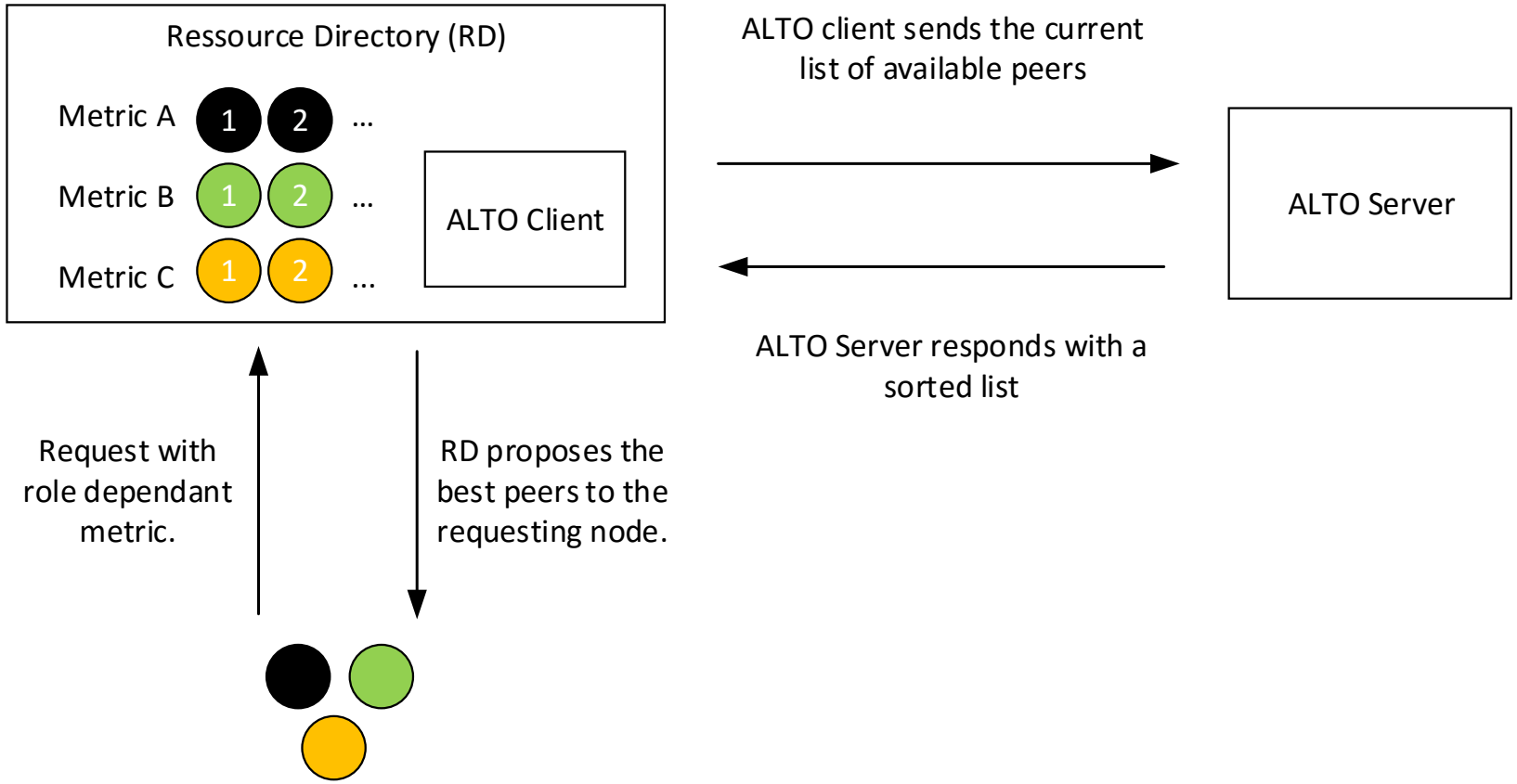


Peer selection mechanism in bitcoin network

- The Bitcoin network relies on a DNS seed list, which is hardcoded in the client. All six seeds are controlled by Bitcoin's core developers.

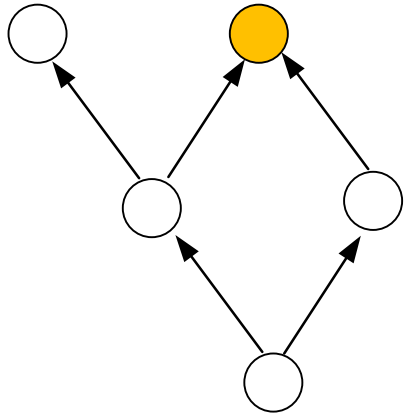
```
115         assert(genesis.hashMerkleRoot == uint256S("0x4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b"));
116
117         vSeeds.push_back(CDNSSeedData("bitcoin.sipa.be", "seed.bitcoin.sipa.be", true)); // Pieter Wuille
118         vSeeds.push_back(CDNSSeedData("bluematt.me", "dnsseed.bluematt.me")); // Matt Corallo
119         vSeeds.push_back(CDNSSeedData("dashjr.org", "dnsseed.bitcoin.dashjr.org")); // Luke Dashjr
120         vSeeds.push_back(CDNSSeedData("bitcoinstats.com", "seed.bitcoinstats.com")); // Christian Decker
121         vSeeds.push_back(CDNSSeedData("xf2.org", "bitseed.xf2.org")); // Jeff Garzik
122         vSeeds.push_back(CDNSSeedData("bitcoin.jonasschnelli.ch", "seed.bitcoin.jonasschnelli.ch")); // Jonas Schnelli
123
124         base58Prefixes[PUBKEY_ADDRESS] = std::vector<unsigned char>(1,0);
```

Peer selection mechanism with ALTO



Information propagation

- A typical blockchain service propagates *transactions* and *blocks* by broadcasting their availability to all directly connected neighbours.
- Problem: Many nodes receive duplicates!
- The Tendermint network is limited to 300 nodes due to the excessive communication.
- ALTO can reduce the traffic volume by proposing the relevant neighbour peers during the bootstrap phase.



Benefits for blockchain networks

- A blockchain service provider can optimise the communication between nodes by using ALTO.
- ALTO can provide the best routes for each peer in dependence of its role (e.g. wallet, miner or relay node).
- A shorter propagation time reduces the number of *forks* in the Bitcoin network.

Discussion

Our mailing list for comments:

draft-hommes-alto-blockchain@ietf.org