The Ripple Protocol Consensus Algorithm

Authors: David Schwartz, Noah Youngs, and Arthur Britto

Presenter: Tianran Wang
Blockchain protocol, like Bitcoin and Ethereum

Provides fast, scalable, and stable payment services

XRP

A native cryptocurrency

Acts as a central for money transferal

RPCA

A fast and low-cost consensus algorithm

Can tolerate \((n-1)/5\) Byzantine failures
RPCA Components

Unique Node List (UNL):
- Lists other servers queried by this server
- A subset of the network trusted by this server

Last-Closed Ledger:
- Represents the most recent consensus among all servers
- Should be identical

Open Ledger:
- Represents current status of this server
- Different among servers

Once consensus is reached, a set of transactions will be applied on the open ledger. Then it becomes the last-closed ledger.
Correctness

A transaction is only approved if 80% of the UNL of a server agrees with it.

The protocol will maintain correctness if \( f \leq \frac{n-1}{5} \).

\( P_c \): the probability that servers in the UNL will be fraudulent

\( P^* \): the probability of correctness

\[
p^* = \sum_{i=0}^{\left\lceil \frac{n-1}{5} \right\rceil} {n \choose i} p_c^i (1 - p_c)^{n-i}
\]

To achieve correctness:
Make sure \( P_c \) is smaller than 20%
Use a large UNL
**Agreement**

Correctness cannot guarantee agreement.

Correctness: no malicious transactions  
Agreement: maintain a single global truth set of txns

The Requirement on the UNL Size:  
\[ \text{Size}(\text{UNL}) > 0.2 \times N \]

The Requirement on the connectivity:  
\[ |\text{UNL}_i \cap \text{UNL}_j| \geq \frac{1}{5} \max(|\text{UNL}_i|, |\text{UNL}_j|) \forall i, j \]
Utility & Conclusion

To make sure consensus is reached in finite time. High latency nodes will be removed from all UNLs.

A default UNL is provided to minimize Pc.

A network split function algorithm is employed to avoid a fork in the network.

Can tolerate only \((n-1)/5\) Byzantine failures.

Utilizes collectively-trusted subnetworks within the whole network.

A fast and low-cost distributed payment consensus algorithm.