Ebb-and-Flow Protocols

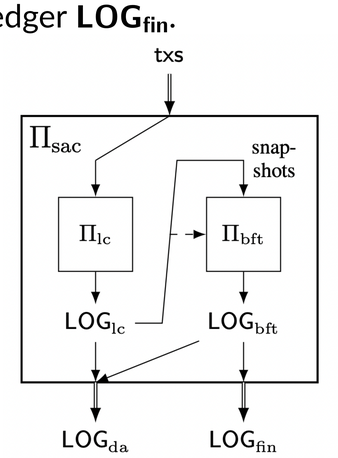
Chaitanya Agarwal
Yajur Ahuja
Swapnil Sharma

Introduction

- Blockchain consensus protocls can require **dynamic availability** and **finality** both.
- But can't guarantee both due to CAP theorem.

Snap-and-Chat [1]

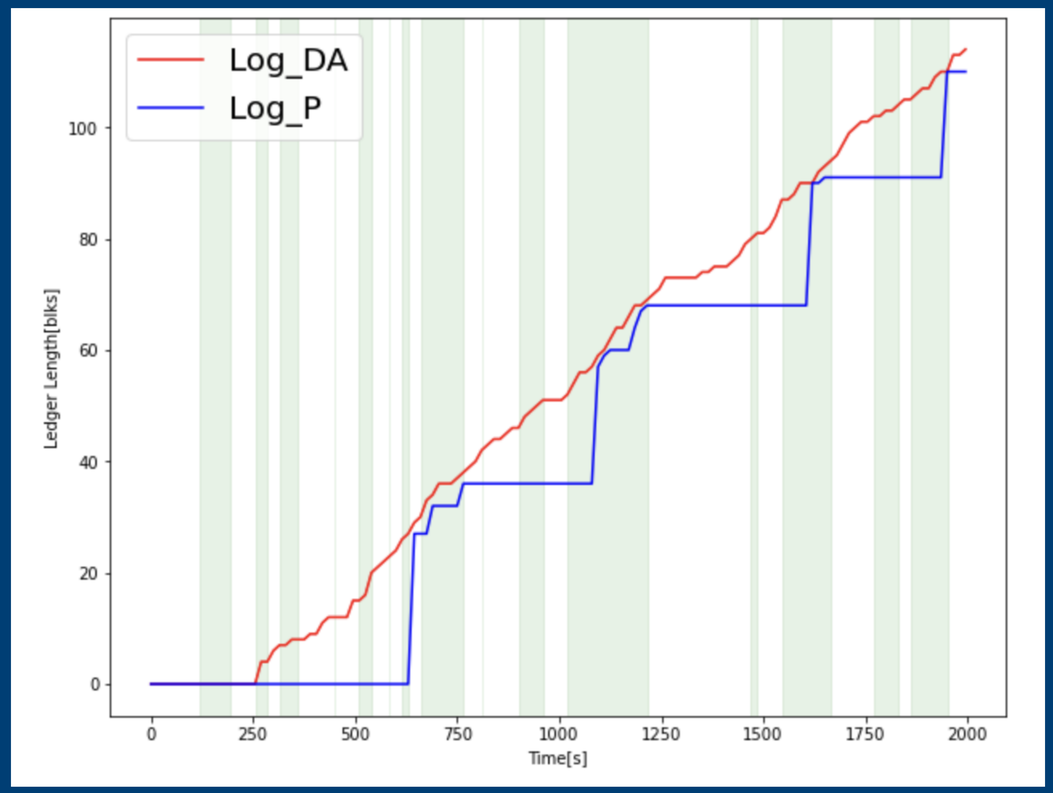
- Maintain **2 ledgers**: Final ledger $\mathbf{LOG_{da}}$, Available ledger $\mathbf{LOG_{fin}}$.



Protocol Guarantees

- Available ledger is safe if $< 50\%$ network is adversarial.
- Final ledger is safe if $< 33\%$ network is adversarial.

On network partitions, or when majority is not awake, **Final ledger stalls**, but **Dynamic ledger grows.**



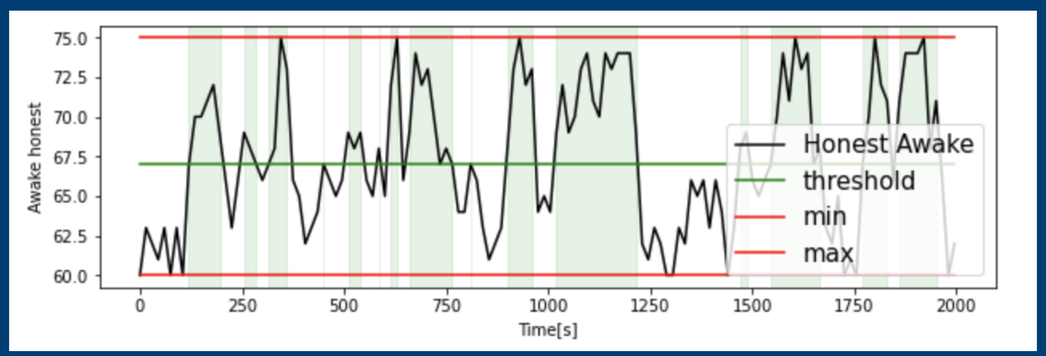


Figure 1: Dynamic Participation

Experiments

Intermittent Network Paritions

- Network paritioned intermittently into groups.
- Intra-group communication delayed until after partition.

Dynamic Participation

- Number of awake/asleep nodes follow Brownian motion.

Our Work

- Re-implemented protocol in **Elixir**.
- Learnt about **Longest-Chain** and **Byzantine-Fault-Tolerant** Protocols in depth.

References

[1] Joachim Neu, Ertem Nusret Tas, and David Tse. Ebb-and-flow proto- cols: A resolution of the availability- finality dilemma. Cryptology ePrint Archive, Paper 2020.