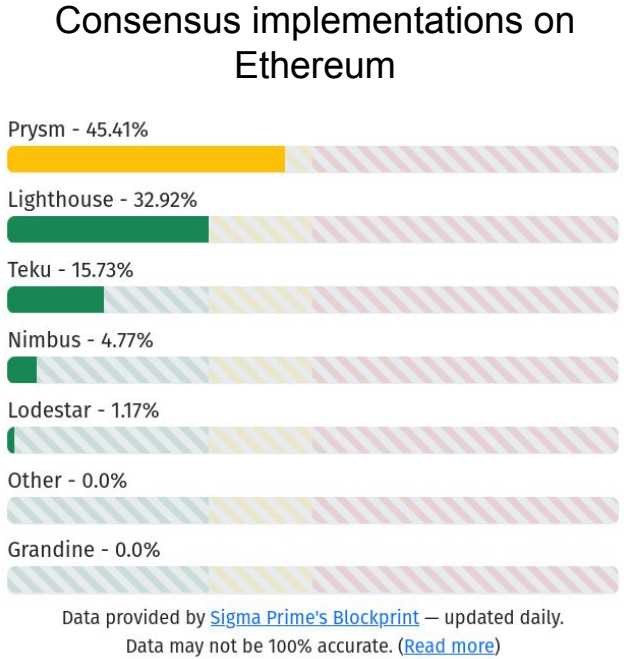
Byzantine Consensus Under Dynamic Participation with a Well-Behaved Majority

Giuliano Losa, Stellar Development Foundation

Eli Gafni, UCLA

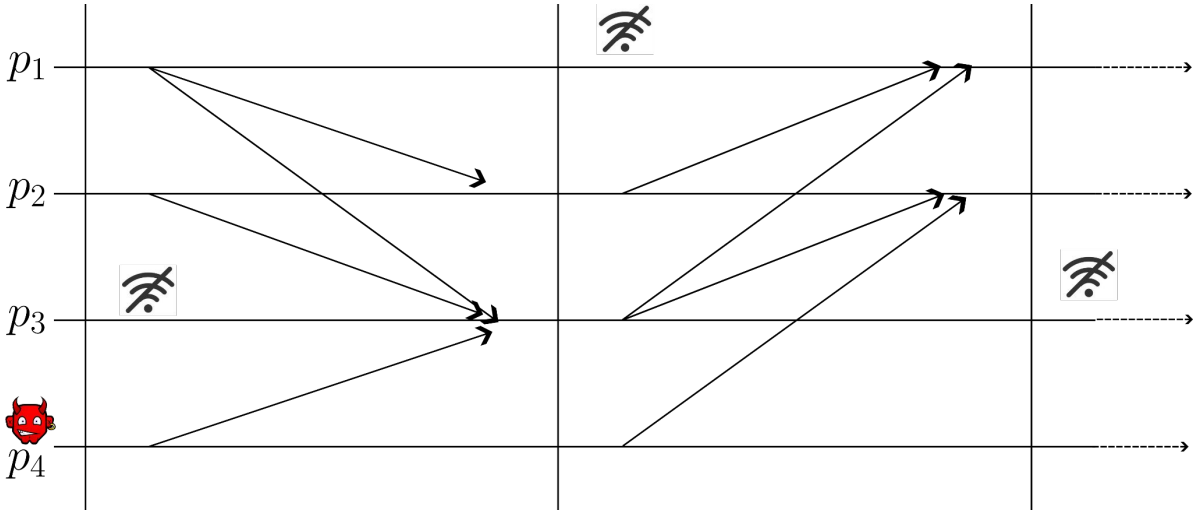
Motivation: Ethereum wants to tolerate bugs that crash more than 50% of the network. Fixed-size quorums do not work

- Large fraction of the participants could crash due to a software bug
- In May 2023, ~60% of the participants (Prysm+Teku) went offline for 25 minutes; the system kept working
- Traditional reconfigurable consensus with fixed-sized quorums would get stuck



The sleepy model: synchronous, dynamic participation with ½ malicious failures

- Synchronous, reliable network
- Participants are known but, each round, some participants may be offline
- Each round, less than ½ of the online participants are malicious

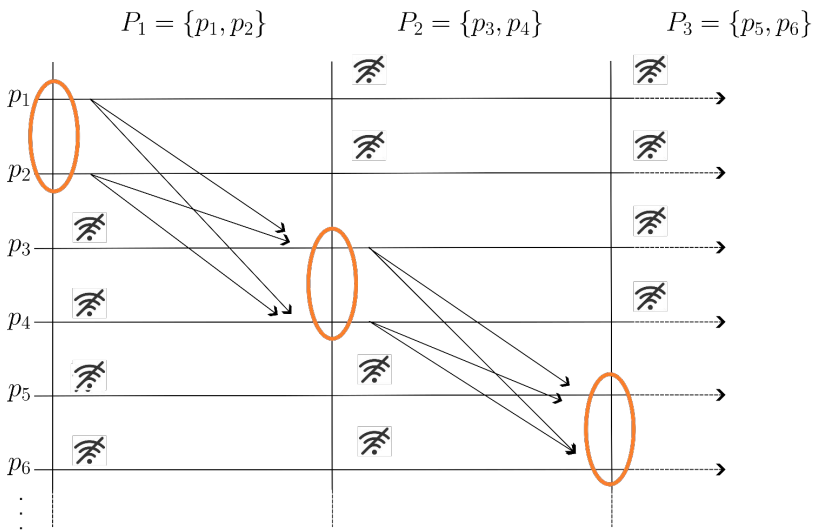


Can we solve sleepy consensus with deterministic safety and constant latency in expectation?

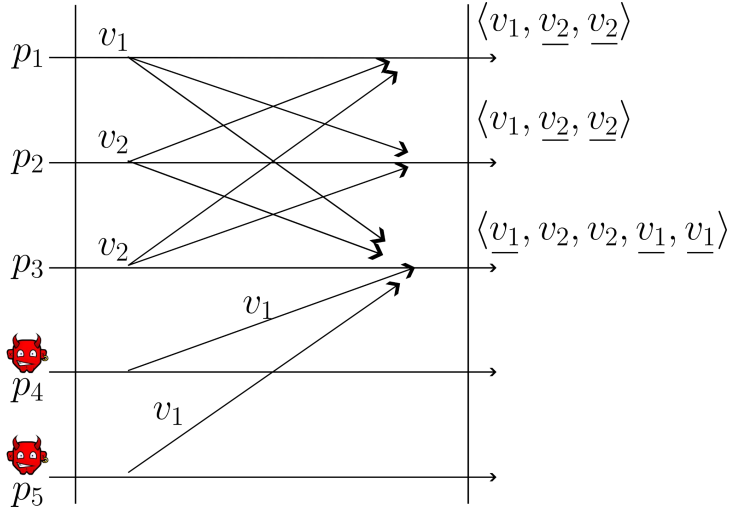
This work	Bitcoin, Ethereum
Safety in all executions	Safety violations with some probability
Decision in a constant number of rounds in expectation (regardless of the number of participants)	Decision in a number of rounds N (a parameter); probability of safety violation depends on N

It seems that traditional solutions do not apply

Dolev-Strong? No, local state is useless



Relative quorums? But processes can witness contradictory majorities



We present a solution using a PKI and verifiable random functions

First we simulate an easier model (the no-equivocation model), then we use the classic “adopt-commit + conciliator” pattern.

Decides in 20 rounds in expectation; each participant send ~n_r^2 messages per round r