CS-438
Decentralized Systems Engineering

Fall 2022

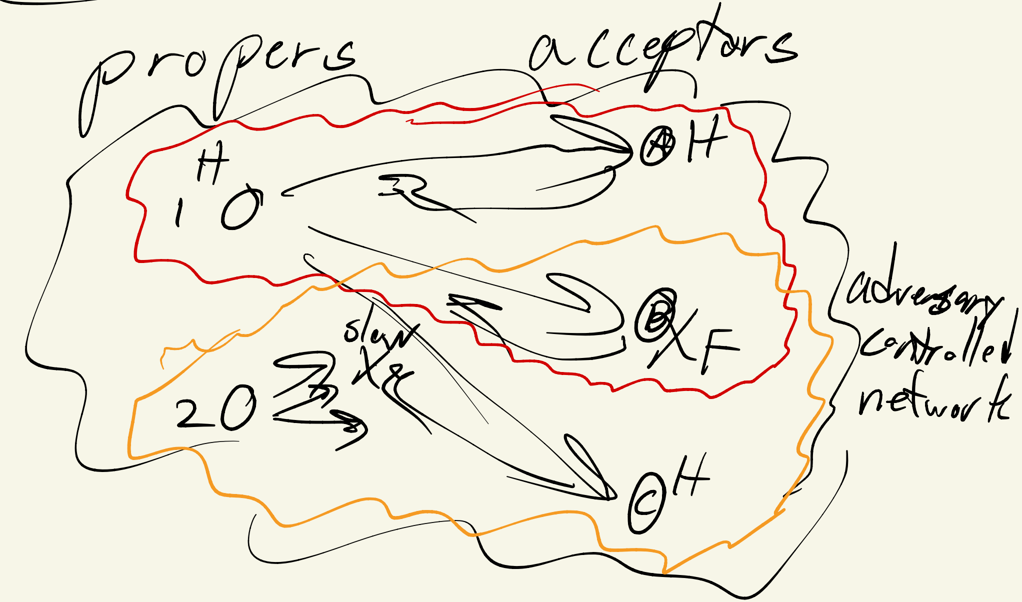
Week 10

Byzantine consensus - permissioned, -less

Permissioned / "Classic" consensus

- assume fixed group of n nodes, threshold t
- Paxos, Raft, ...: fail-stop model f can fail $t = n - f$
- Byzantine consensus: f nodes can do "anything"
    - PBFT: "Practical Byzantine Fault Tolerance"
    - HotStuff, HoneyBadger, ...

Paxos - review



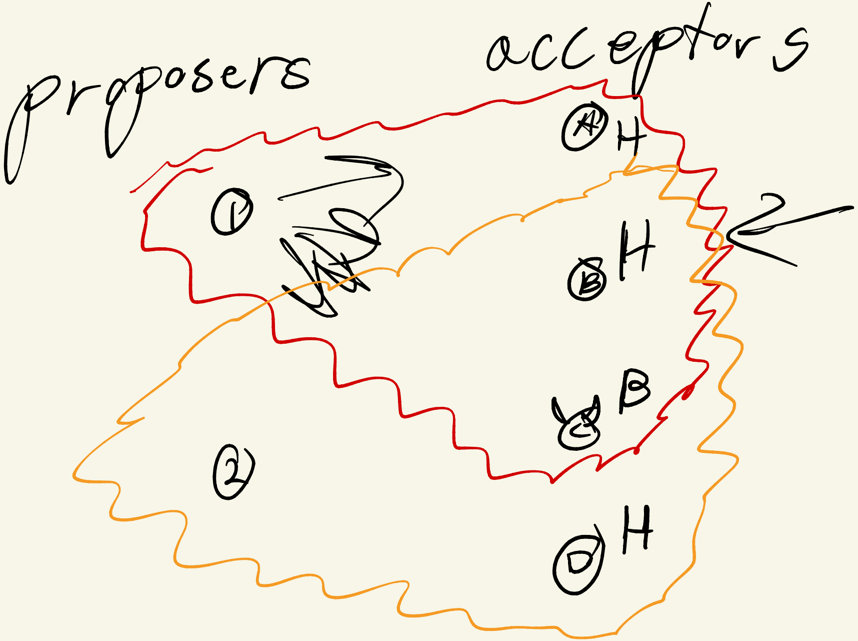
$n = 3$
$f = 1$
$t = n - f = 2$

properties:

- safety - all nodes agree on decision
- liveness - eventually something is decided

Byzantine consensus thresholds

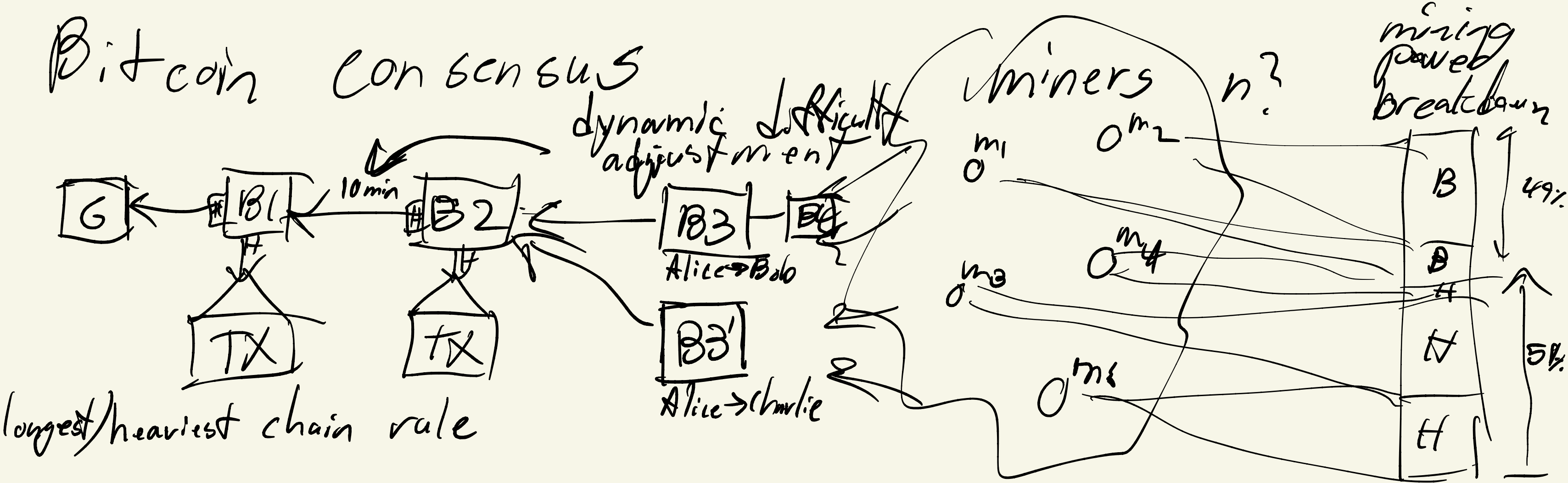
- Paxos $n \geq 2f+1$ insufficient
- must have $n \geq 3f+1$ (PBF, HotStuff...)



1 honest node intersection

Permissionless PoW consensus (Bitcoin, ...)

Bitcoin consensus



Assumptions:

- threshold assumption: majority (>50%) of mining power honest
- Economic incentive compatibility
- network connectivity /propagation – synchrony