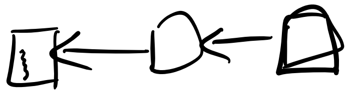
Permissionlessness:

Byzantine parties < 50%.

Fraction of Byzantine computatation power < 50%.



In expectation, next block is produced in 10 mins

⟹ 20 CPUs → 10 mins.

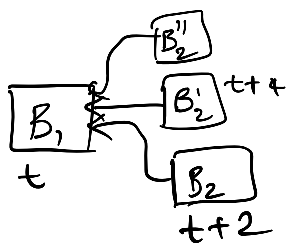
40 CPUs → 5 mins.

~ 2 × 7 × 24 × 6.

000000 (x+1) ⟼

Dynamic availbility:

- 1 block in expectation every 10 mins ⟸ 12 secs; 2 secs
- The time to propagate a block is ~ 10 secs.



10 mins >> 10 secs.

4

Q: forking rate observed in Bitcoin vs. Etheaum.

Network assumption:

synchrony: any message sent by a party will arrive within some bounded delay Δ. (10secs).

Economic incentives:

Block rewards: 6.25 BTC

\$19K $\approx$ \$120K

Transaction fees:

Network connectivity.

Peer-to-peer network.

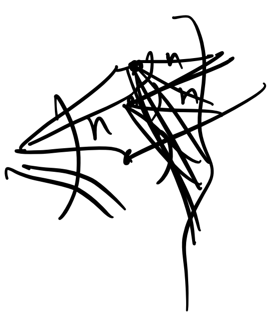
Communication complexity:

every party is connected to every other party.

Adding block : $O(n^2)$.

Committing a block : $O(n^2 k)$

n^2



Latency of a commit: k blocks (k confirmations)

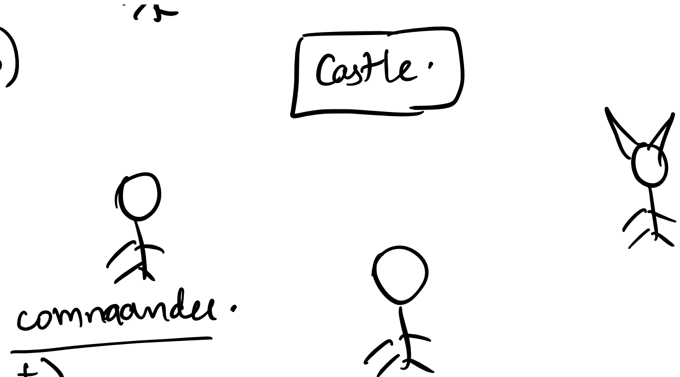
---

n parties, t are corrupt.

Lamport, Shostak, Pease 1980: Byzantine General Pease.

Byzantine

Broadcast (BB)



(Attack, retreat).

Agreement: No two honest generals take different actions.

Termination: Eventually every honest general to attack or to retreat.

Validity: If commander is honest, then all honest generals follow commander's input.

Byzantine agreement: every party$_i$ has an input. v_i

Agreement: same as BB

Termination: same as BB.

Validity: if all honest parties have input $v_i = v$, then all honest parties output v.

Bitcoin: - general changes.
- validity:

BB	Bitcoin
– Only parties interested in	convincing an external

the result.

- Validity:
- Single-shot.

~~E~~ world.

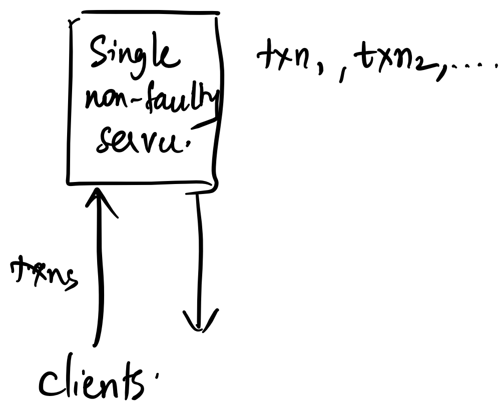
External validity.

Sequence/log of transaction

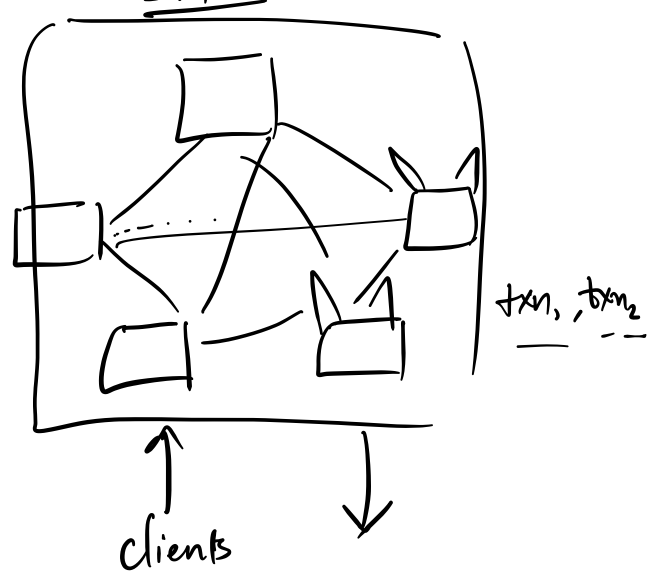
State machine replication:

Multiple server replicas (parties), some of which may be faulty, and they provide you with an interface of a single non-faulty server.

Ideal world



SMR



Safety: No two non-faulty server replicas output
(Agreement) different values at the same position of the log.

Liveness: Non-faulty server replicas keep
(Termination, validity). committing new client transactions (valid).

Dolev-Strong Protocol for Byzantine Broadcast (1982).

Intuition: If at any point, a party receives a value/txn, then that party will share it with everyone.

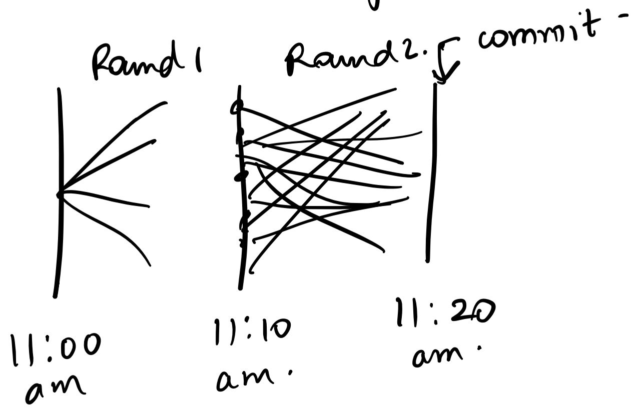
If I know something in round r, all other parties will know it in $r+1$.

Round 1: Commander (sender) sends some value v to all parties.

Rand 2: If I receive a value v in round 1, ~~share~~ send that value to all other parties.

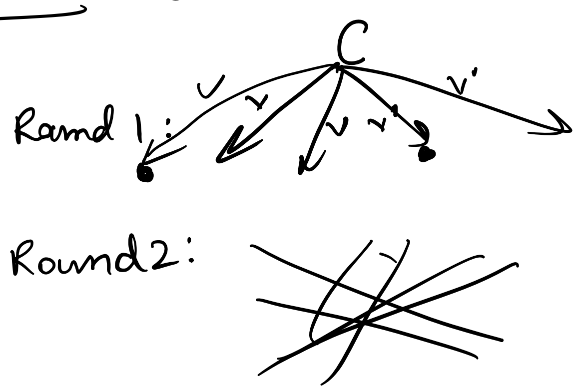
Commit: (Output) If I receive exactly one value v', then output v'.

O.W. output $\perp$.



Attack 1: Commander does not send anything. ✗

Attack 2: Commander sends 2 different values



All honest see v & v'; output $\perp$.

Attack 3: Commander sends v to half the parties.

Attack 3': Commander sends nothing to honest parties; sends ~~me~~ value v to only malicious parties.