CS-438 Decentralized Systems Engineering

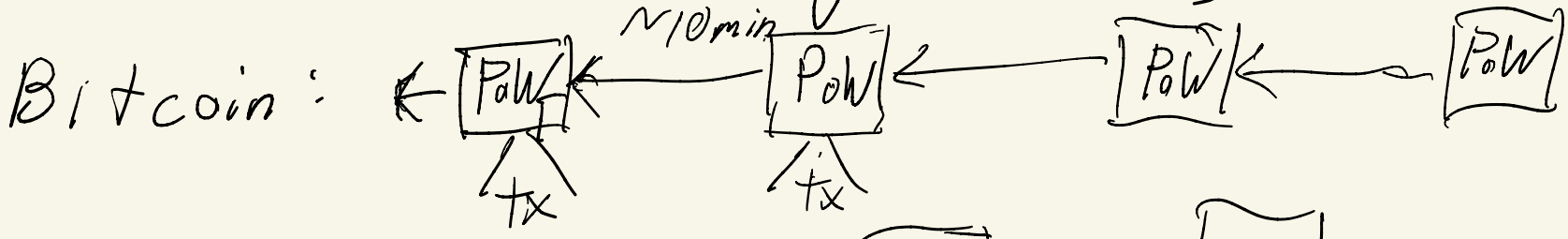
Week 13

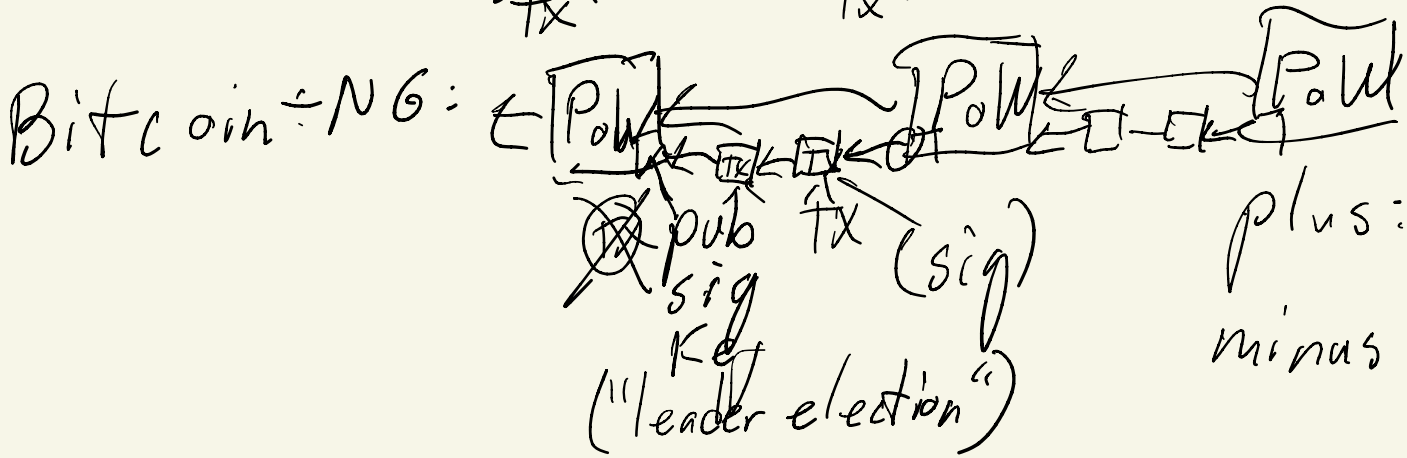
Limitations of Bitcoin

- High energy cost from PoW
- Low throughput (TPS): only ~4.7
- Smart contracts: non-Turing complete, inefficient
- power distributed by investment (not by people)
- privacy / confidentiality: account/transaction anonymity
- 51% attack problem (hostile takeovers)

Increase Throughput / TPS:

- Bitcoin-NG: ("next generation")



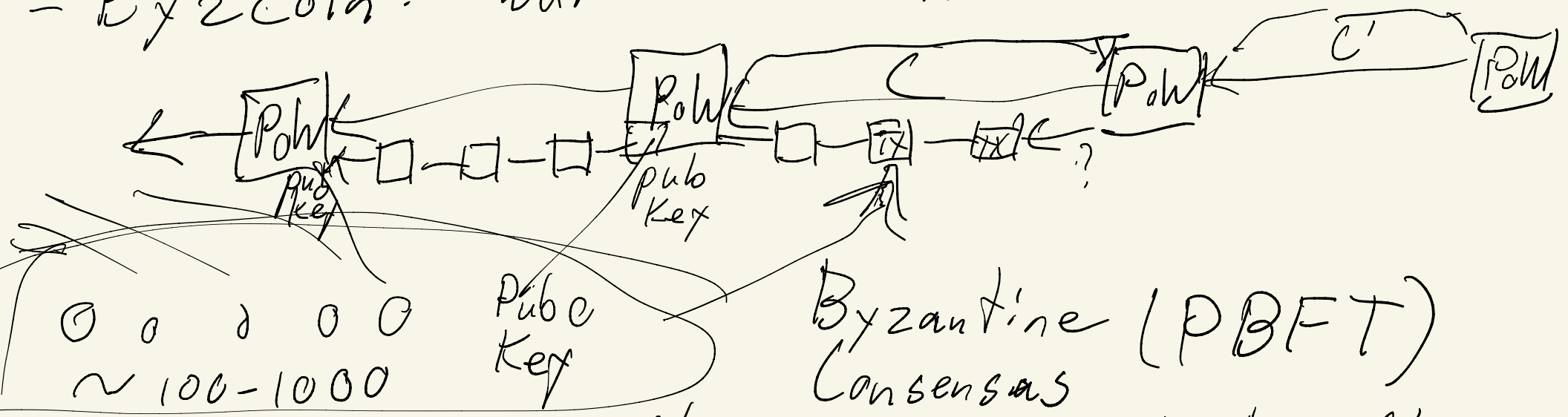


plus: higher TPS

minus: "temporary distortion" (DoS)

Increasing TPS

- Byzcoin: builds on Bitcoin-NG



~100-1000 Pube Key

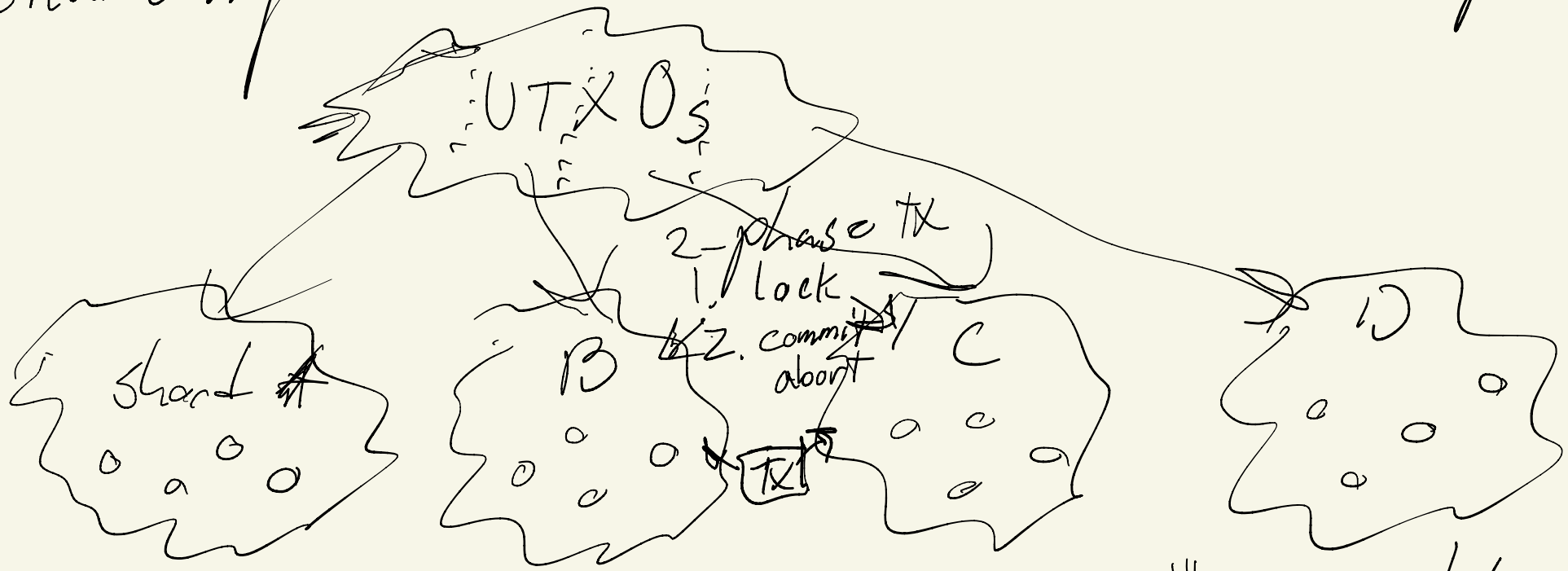
Byzantine (PBFT) Consensus

consensus committee C rotating to C'

- challenge:
  - even with consensus, how do clients know & verify which microblocks were committed?
    - A: collective signing (threshold of committee)
- challenge: liveness vs safety
  - Q: how to rotate committee?
    - Choice 1: via PBFT commit TX C → C' (safety)
    - Choice 2: via PoW alone (liveness)

Increasing TPS

- problem: no "scale-out" - everyone processes everything
  we want more miners → more agg. capacity
- sharding architectures: Ouroborus, Omniledger



malicious takeover?

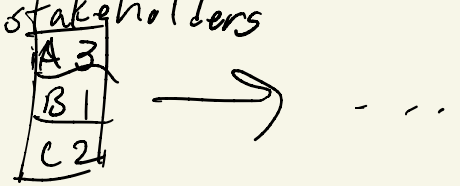
Challenge: shard takeover.

Challenge: cross-shard TXs

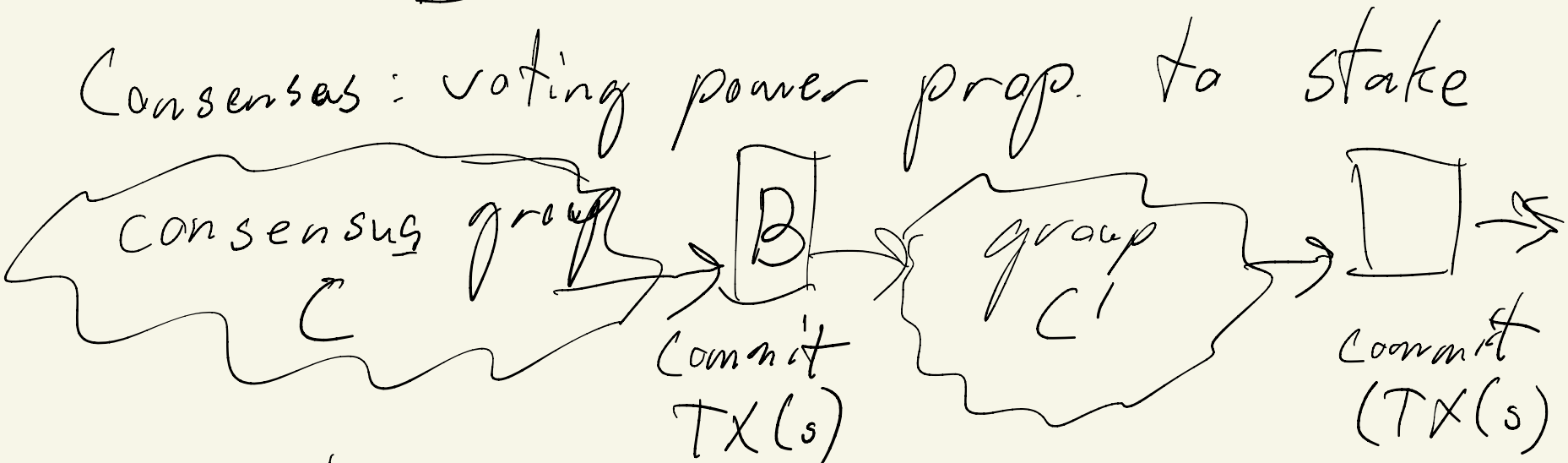
→ Solution: (1) "big enough"
(drand) → (2) random, represent...
→ each shard Safe+Live

Reducing energy - Proof-of-Stake

- Algorand,
- Main idea: have "stakeholders" → stake funds



Consensus: voting power prop. to stake



- how to form group?
  - random sample of existing stakeholders
  - Algorand: everybody uses VRF to "print" a "ticket"
    - "winning" if below threshold
    - reveal winning ticket w/ consensus vote