CS-438 Decentralized Systems Engineering

Fall 2024

Week 12

Advanced consensus & blockchain architectures

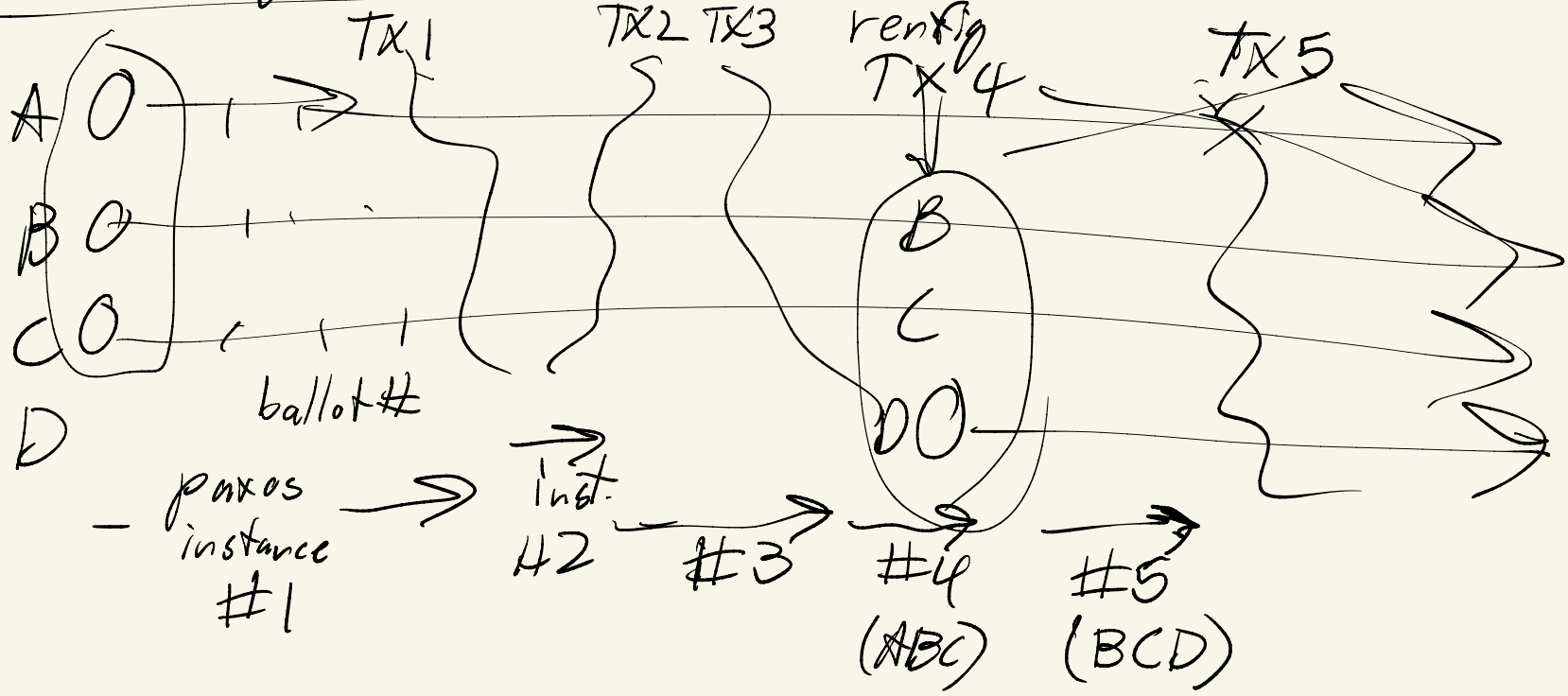
Motivation — problems w/ existing blockchains, e.g. Bitcoin

- Limited TX capacity, congestion/competition, high fees
- Latency: 10 mins (min) → 1 hr
  - Delayed/probabilistic finality
- Huge energy use of PoW
- Smart contract VM limitations
  - Determinism, no external-world input w/o oracles
  - Can't "hold secrets" on blockchain
  - Public randomness is hard

Topics for detail:

- Reconfiguration & committe-based blockchains
- Sharding

Reconfiguration in Paxos



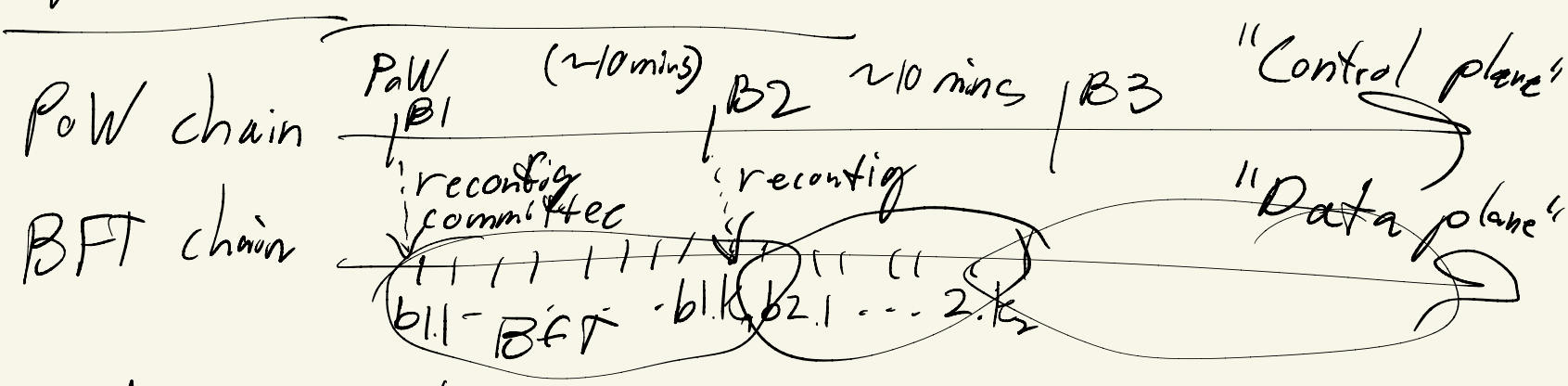
Committee-based blockchains

Bitcoin: 1 leader at a time, does 1 thing per block

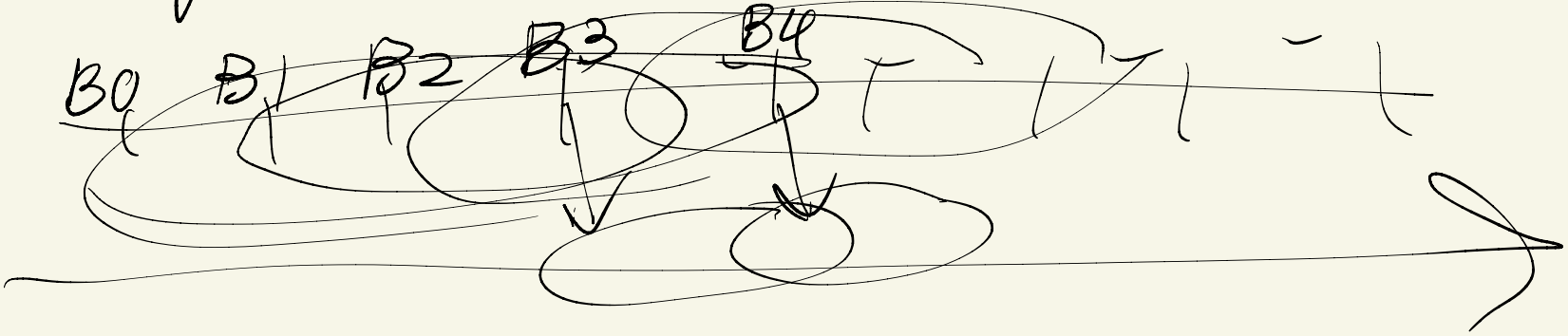
Byzcoin: improve capacity & commit latency via PoW-selected committies for BFT

PoS: stake instead of crypto-puzzles as basis

Byzcoin - 2 chains



Sliding window



Robustness to liveness loss

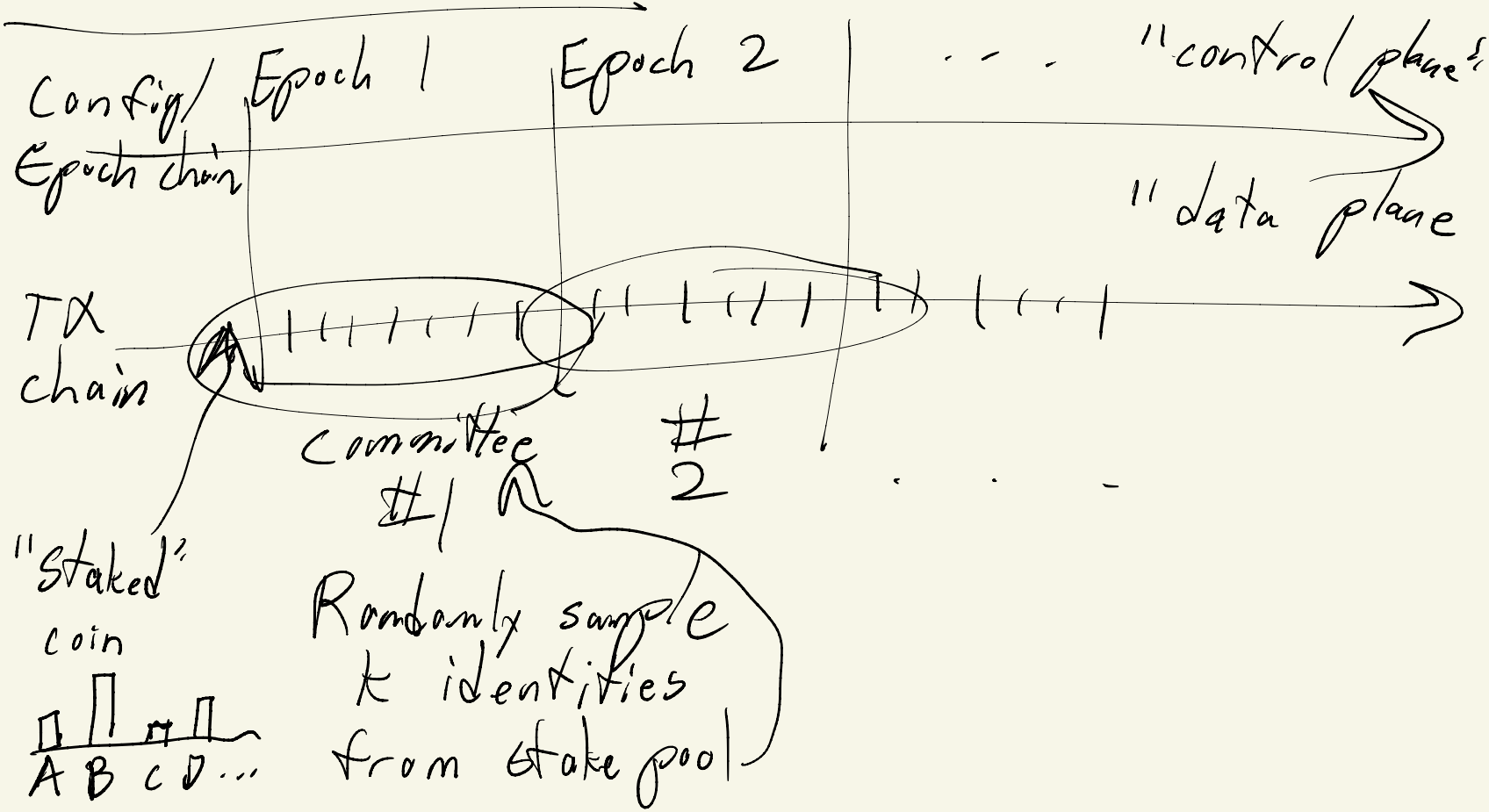
2 choices (design)

- Bitcoin tradition: Liveness over safety
- Paxos tradition: Safety over liveness

Proof of Stake

- Generic committee-based PoS
- Algorand

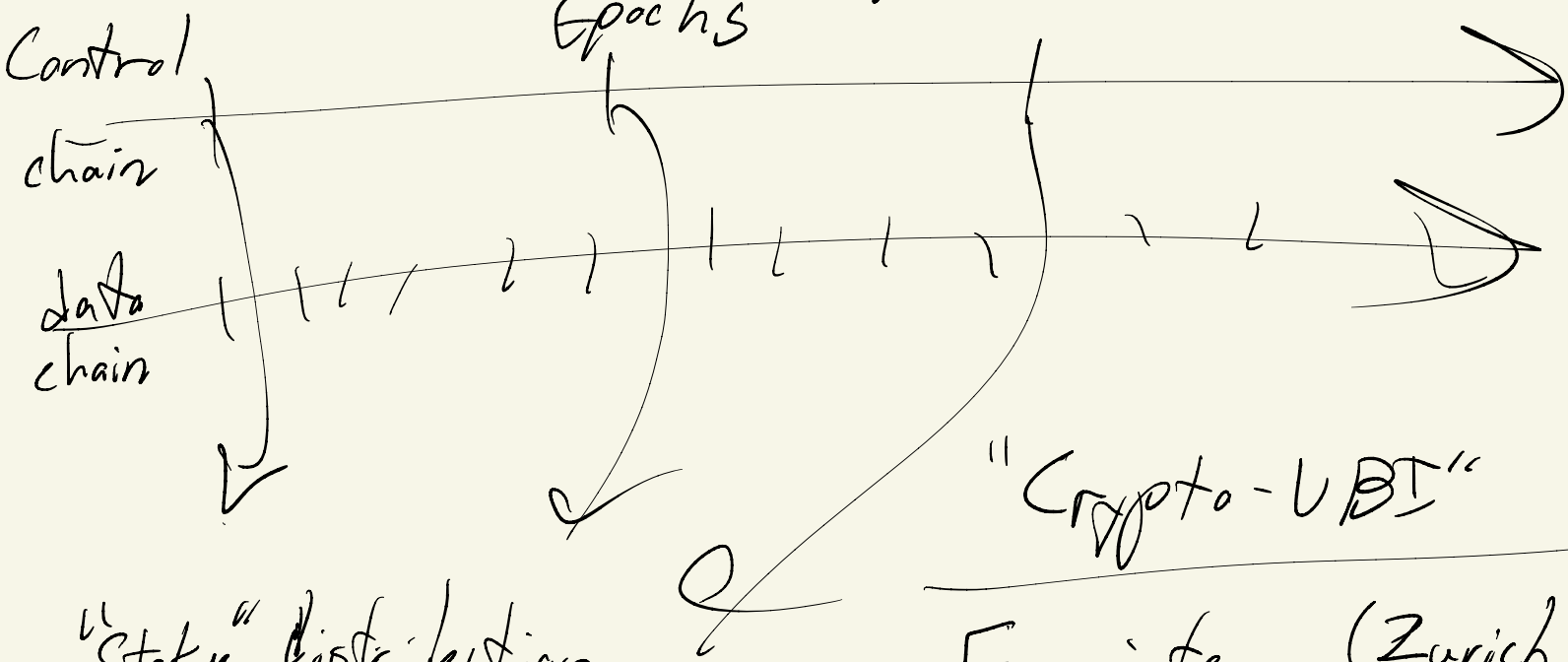
Generic PoS


Config/
Epoch chain
Epoch 1
Epoch 2
. . .
"control plane"
"data plane"
TX
chain
committee #1
committee #2
. . .
"Staked" coin
A B C D ...
Randomly sample k identities from stake pool

Algorand PoS

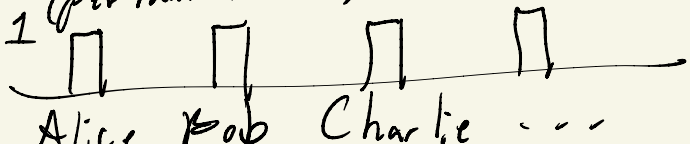
- "~~Fast~~ adaptive adversary"
  Instantly
- ~~Ephemeral~~ committees — "do 1 thing"
  "only speak once"
- Verifiable Random Function (VRF)

Alternatives to PoS - eg. PoP (personhood)



"Crypto-UBI"

"Stake" distribution



- Encointer (Zurich)
- IDENA (online)
- ⋮