CS-234
Technologies for Democratic society

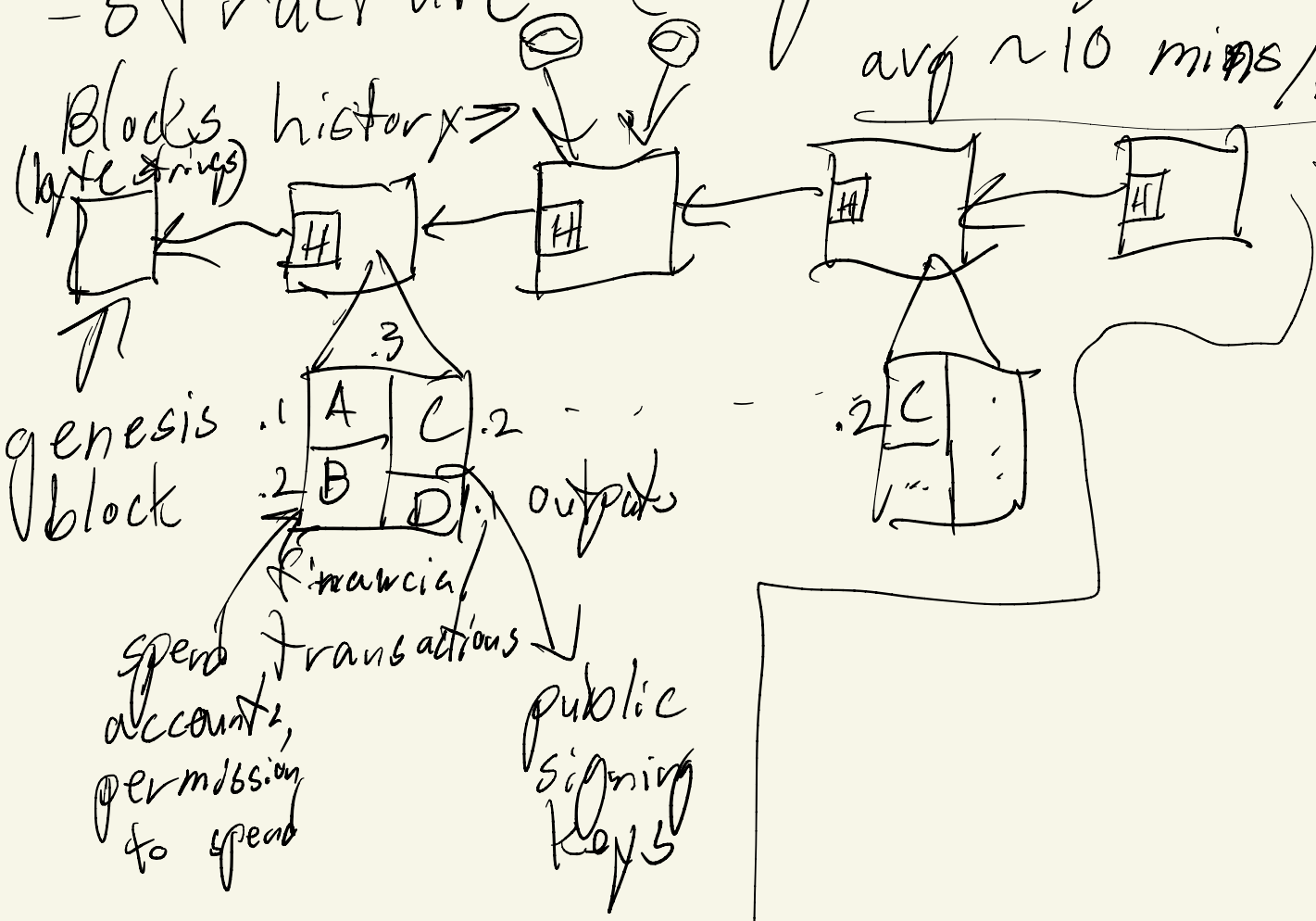
Fall 2021

Week 6

Blockchain - what is it?

- Bitcoin (2008)
- structure (long before): tamper-evident log via hashes

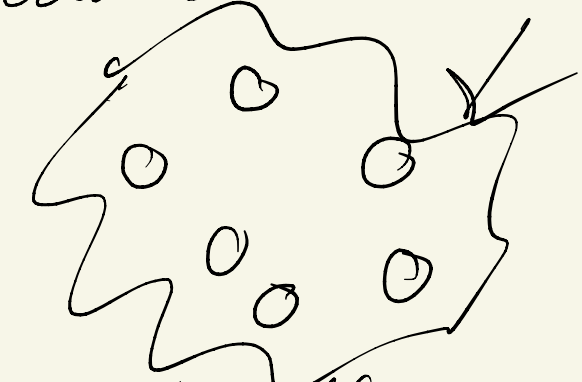
avg ~10 mins/block



Consensus: establishing linear ordering

Consensus Categories

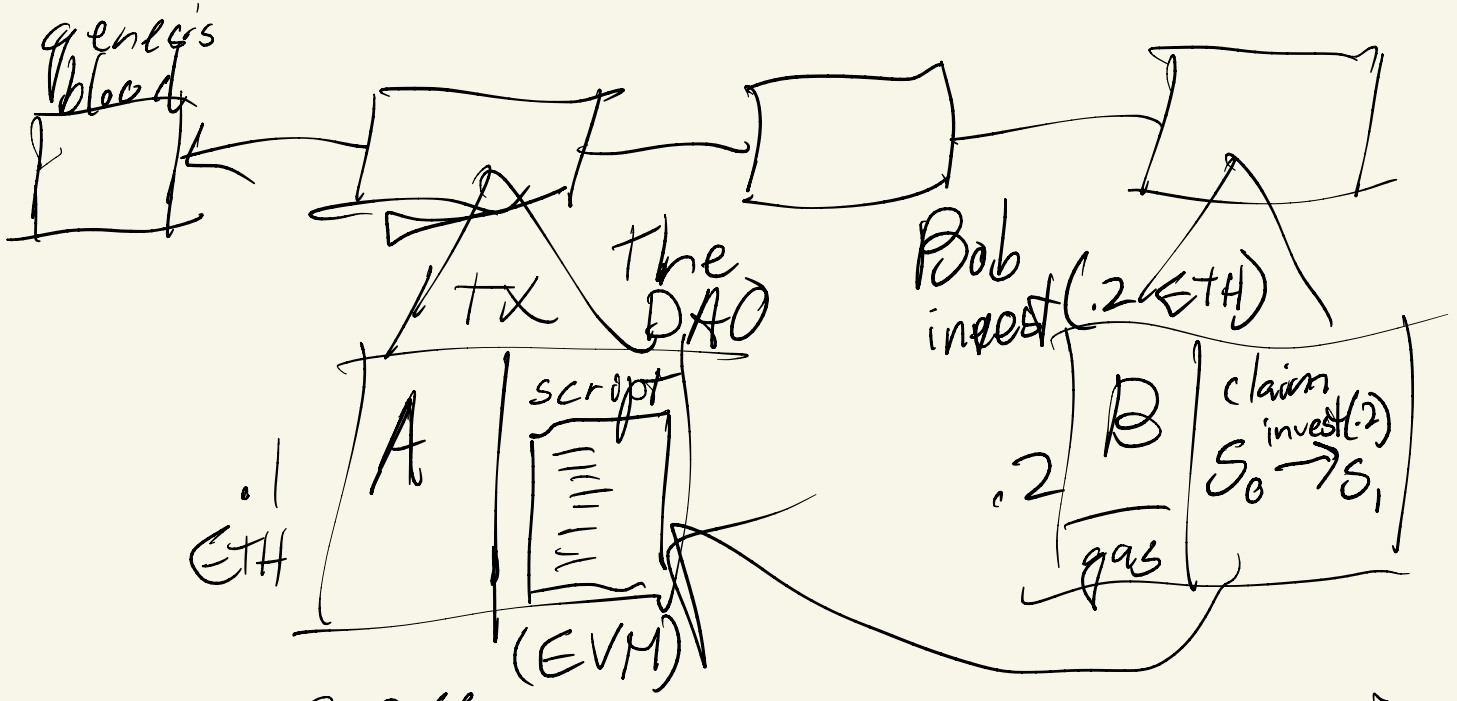
- Permissioned: assumes "a committee" established
  - closed group
  - usually small (3-10)
  - Paxos, Raft, PBFT, HotStuff, ...

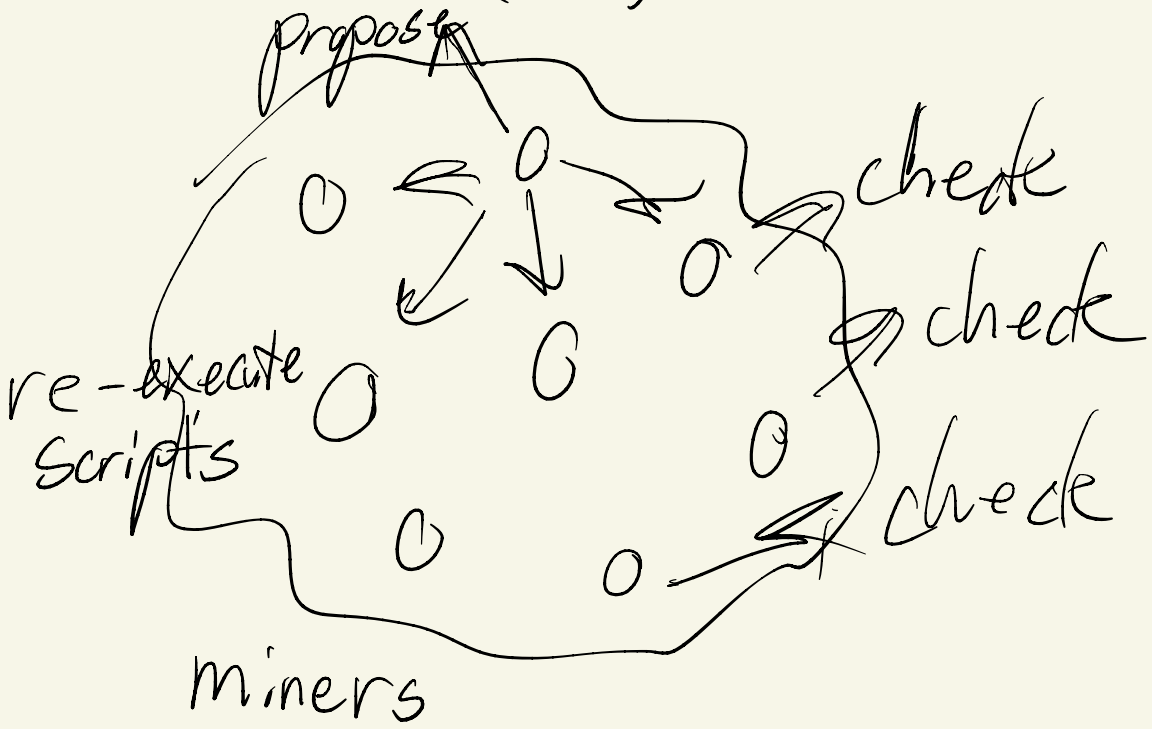


- Permissionless: "anyone" can join at any time
  - Proof-of-Work: to join, must invest "work"
  - Proof-of-Storage: invest in storage
  - Proof-of-Stake: invest in existing coin (ETH 2.0)

proof-of-investment

Smart Contracts





Decentralized Finance (DeFi)

services like
- trading coin/NFT/...

The DAO

- Crowdsourcing smart contract ("like Kickstarter but decentralized")
- Hacked in 2016
- Majority hard forked to recover
- Minority forked ETC

Questions / issues

- Is a smart contract a "contract"? (legal?)
  - A few exceptions (eg. Arizona)
- Deterministic code: no external input
  - Solution: "oracles" (decentralized oracles)
- Smart contract governance: investment-based (the DAO) vs. democratic: personhood-based
- can we get "more decentralized" basis?
  - ID / AS
  - phone numbers
  - email addresses

} identity proxies