Proof of Stake
(alternative consensus mechanisms)

Reminder: Proof of Work

- usually a hash puzzle
- scalable difficulty
- buy more hw + electricity, increase odds of mining a block
- Incentive to form consensus

Problem: Wasteful

Proof of Stake

- Want strong consensus with less wasteful work

Idea: Next block "lottery"

- PoW: computational power buys raffle tickets
- PoS: Use holdings of the currency itself to increase odds of mining

Proof of Stake

Raffle with Refunds

- Buy tickets "staking"
- One winner chosen (to mine new block)
- Turn in unused tickets for refund
- Keep drawing new winners every X seconds

Peercoin PoS

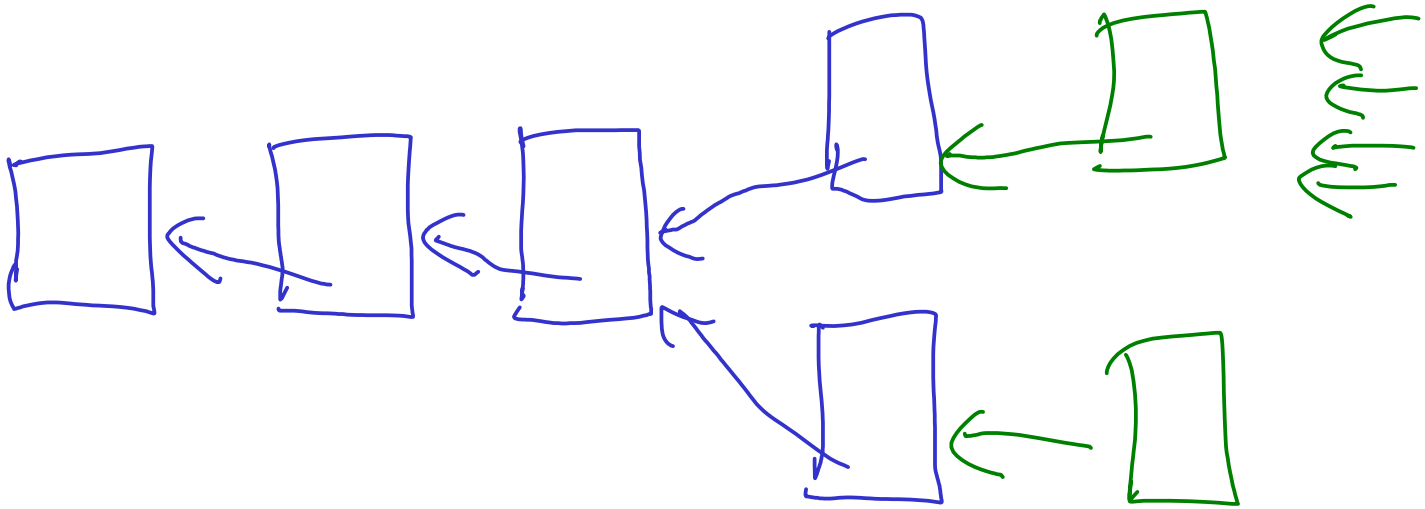
- Special staking trans
- Difficulty scales down with more stake

Staking "punishment"

Why would you forfeit stake?

- Propose a "bad block"
  - ↳ not following rules
- Often stake "burned" if you are "caught"

Nothing at Stake Problem



No cost to maintain both chains

Solution: Punishment ("slasher")

→ Stake committed on any other chain is forfeit.