RECAP OF BITCOIN

- **Transactions:** At any time, any buyer b can generate a transaction to pay d BTC to seller s.
- **Block:** A block consists of
  - A set of transactions
  - A cryptographic hash of the previous block (pointer to previous block
  - An ID of the miner for this block
  - A nonce.
- A set of properly signed transactions is **valid** if no account ever overspent its limit.
- A block is valid if
  - It points to a valid block.
  - All transactions on the chain to B are valid.
  - SHA256(nonce|| info in block) has k leading zeros.

RECAP OF BITCOIN II

- **Mining:** the process of extending the blockchain from some block B.
- Longest Chain Protocol (for miners):
  - Choose B to be the block furthest from the root, tie-breaking in favor of the first block you heard about.
  - Include all valid transactions you've heard about.
  - As soon as valid block created, announce it to the network.
- Miners are paid for creating valid blocks with freshly minted Bitcoins and with transaction fees.
- Difficulty of the puzzle is adjusted every 2016 blocks with the objective of making it so that a block takes 10 minutes to make in expectation.

KEY IDEA

- Trust the ledger that has the most "computational work" put into it.

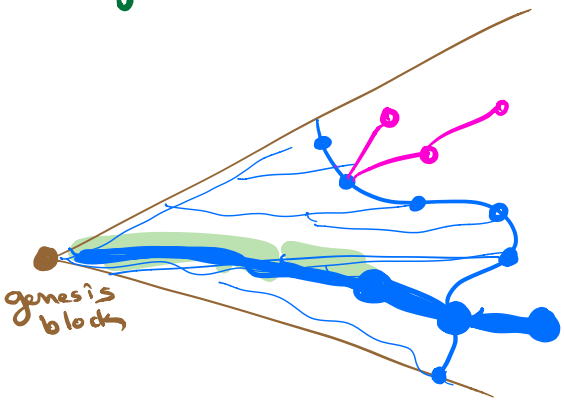
- Ensure that fraudulent transactions/conflicting ledgers would require an infeasible amount of computation to create.

Deviations from protocol

- mine off of any block you want
  - deliberately create forks
  - dishonest tie-breaking
- hide a block once found
- include any transactions you want.

Blockchain mining game

- miner i has fraction x_i of mining power
$$\sum_{i=1} x_i = 1$$
- discrete time model
  - in each step, exactly 1 miner is selected to create a block
  miner i selected with prob x_i
- at all times, each miner m is aware of a directed tree G_m

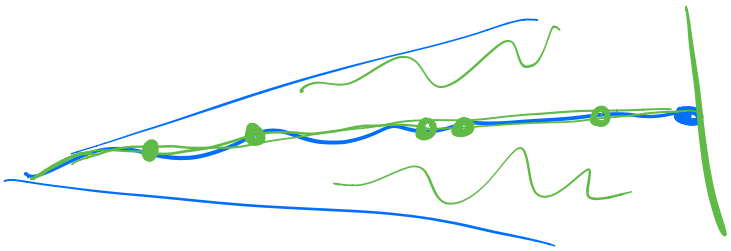


m creates a directed edge to any block in G_m

- in any step, any miner m can broadcast to all other miners any paths in G_m. These paths get added to all $G_{m'}$ $m' \neq m$.

Objective for miner m: maximize $\lim_{T \to \infty}$ $\frac{\#\text{ blocks created by } m \text{ on longest chain}}{\#\text{ blocks on longest chain.}}$

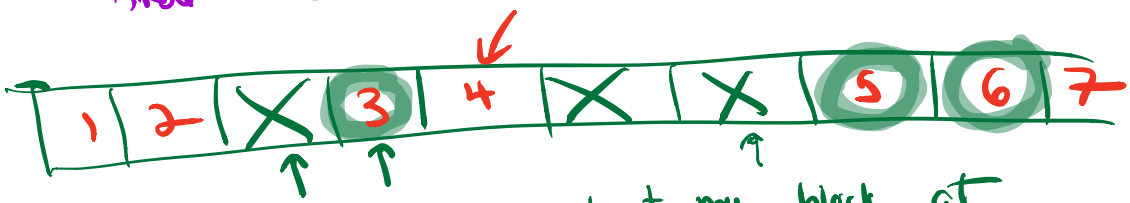
BTC / unit time.



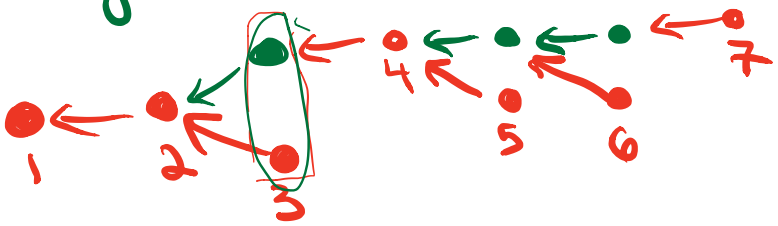
Selfish Mining

- hide blocks you've created to trick other miners into creating blocks that will never be on longest chain

Attacker strategy always mine on longest chain breaking ties in favor of my own blocks but only broadcast any block I've found if there is another block at same distance from root.



if other people hear about my block at same time as they hear about another block at same depth, they break tie in my favor.



my fraction of my power is α

after N blocks created, I've created αN blocks

I've killed αN blocks

blocks on longest chain $(1-\alpha)N$

∴

Ive reated $\frac{\alpha N}{(1-\alpha)N} = \frac{\alpha}{1-\alpha}$

$\alpha = \frac{1}{3}$

$\frac{\frac{1}{3}}{\frac{2}{3}} = \frac{1}{2}$

Selfish mining strategy for miner m.

- Always work on longest chain in G_m
- break ties in favor of m's blocks.
- Block announcing strategy
  - don't announce immediately

depth of longest chain in $G_m \triangleq h_m$

$h_m \geq h$ ↑ length others know about.

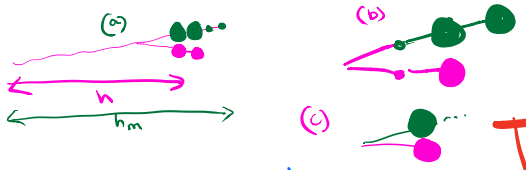
If another miner announces a block at height h, then

(a) if $h_m \geq h+2$, announce block I created at depth h

(b) if $h_m = h+1$, announce h & h+1

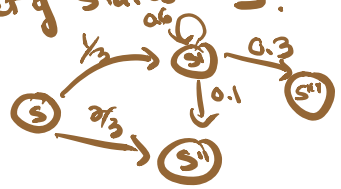
(c) if $h_m = h$, announce h and if m finds next block, announce it immediately.

:!←



Markov chain

set of states S.



q_{uv} : Prob go to state v next if you're currently in state u

$\sum_{v \in S} q_{uv} = 1$

stationary distn. Vec S

long run probability of being in state u.

$\sum p_u = 1$

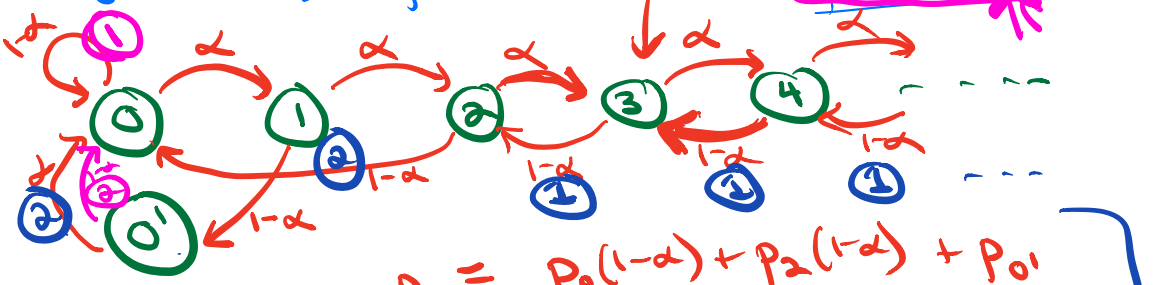
$p_u = \sum_{v \in S} p_v q_{vu}$

State $\{0, 0', 1, 2, \dots\}$

state $i \equiv h_m = h + i$

$0'$: $h_m = h$ but there is fork right now

m has fraction α of mining power



pink: honest payoff

b/w: selfish payoff.

$p_0 = p_0(1-\alpha) + p_2(1-\alpha) + p_{0'}$

$p_{0'} = p_1(1-\alpha)$

$p_1 = \alpha p_0$

$p_i = p_{i-1}\alpha + p_{i+1}(1-\alpha) \quad \forall i \geq 2$

Compute exp payoff

we will count a block when it is first announced & is guaranteed to be on longest chain

$$\text{Honest exp payoff} = p_0(1-\alpha)\cdot 1 + p_0'(1-\alpha)\cdot 2$$

$$\text{Selfish exp payoff} = \sum_{i\geq 3} p_i(1-\alpha)\cdot 1 + p_2(1-\alpha)\cdot 2 + p_0'\alpha\cdot 2$$

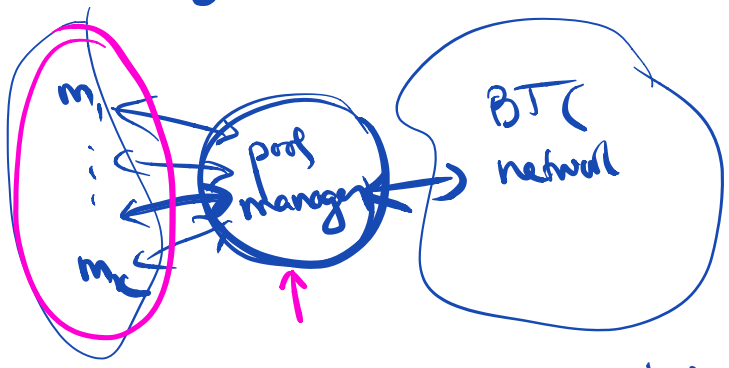
$$\frac{\text{Selfish payoff}}{\text{Honest + Selfish.}} = \frac{4\alpha^2(1-\alpha)^2-\alpha^3}{1-\alpha(1+\alpha(2-\alpha))} > \alpha \quad \alpha \geq 0.3$$

under assumption that lose all ties.

The Miner's Dilemma

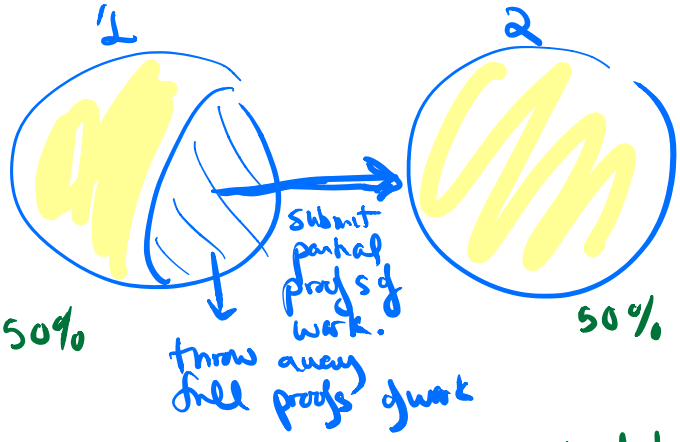
groups of miners join together to form mining pools.

$p_u = \lim_{T\to\infty}$ fraction of first T steps that chain is in state u.



miners in pool submit solns to simpler crypto puzzles

Pool 1 registers with pool 2 (victim) as a regular miner.



Pool 1 attacks pool 2 w/ half of its mining power

Pool 1 makes $\frac{\frac{1}{4}}{\frac{1}{2}+\frac{1}{4}} = \frac{1}{3}$ of valid blocks.

Pool 1 gets. $\frac{\frac{1}{4}}{\frac{1}{2}+\frac{1}{4}} = \frac{1}{3}$ of rewards made by pool 2.

Pool 1 making $= \frac{1}{3} + \frac{2}{3}\cdot\frac{1}{3} = \frac{5}{9}$ of rewards.

Thm For any system with $p > 1$ pools, and no majority pool, not infiltrating is not an equilibrium.

---

optimize infiltration rates to maximize revenue.

x_{ij} fraction of pool i that infiltrates pool j $\quad m_1$, $m = m_1 + m_2$

2 pools: block rewards. $R_1 = \frac{m_1 - x_{12}}{m - x_{12} - x_{21}}$

$R_2 = \frac{m_2 - x_{21}}{m - x_{12} - x_{21}}$

$r_1 = \frac{R_1 + x_{12} r_2}{m_1 + x_{21} m_2}$

choose x'_{12} & x'_{21} to be best responses

$$x'_{12} = \arg\max_{x_{12}} r_1(x_{12}, x'_{21})$$

$$x'_{21} = \arg\max_{x_{21}} r_2(x'_{12}, x_{21})$$

NE: always want to infiltrate (as long as no single pool has too large fraction of mining power)

everyone's worse off.

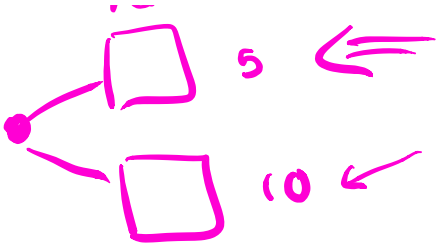
- PD type situation.
- change joining fees.

Transaction fees.

- transactions arrive at const rate.
- blocks are created at const rate.
- if RBTC of transaction fees are available, miners can put any fraction into block.
- miners have enough space for all arriving transactions
- no block reward.

Honest miners protocol
- mine on longest chain (tie-breaking for what I heard about first)
- include all transactions that I've heard about
- publish immediately

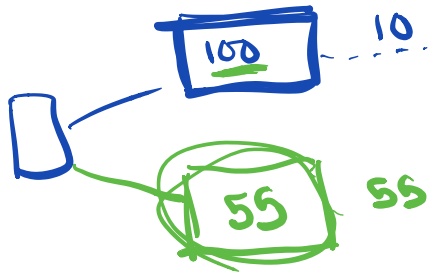
heard about first.

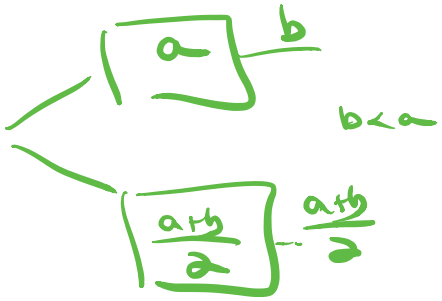


Petty compliant

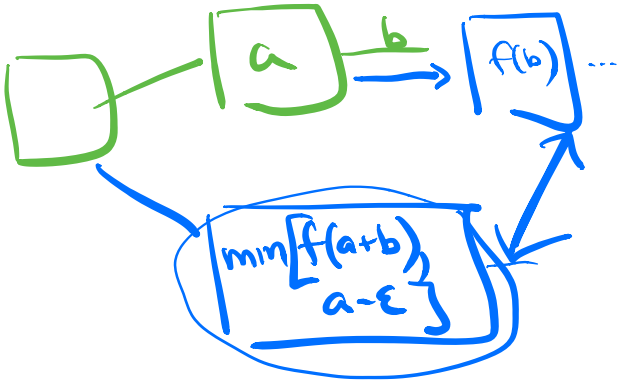
Break ties for chain w/ most leftover trans fees.

"Lazy undercutting"





Using function f to decide how much to include



Find some fn f. for which this behavior is NE.

Revisit selfish mining.

- works even better.

when selfish miner is way ahead (so that next block they create ⟹ longest chain) and block contains lots more transaction fees.