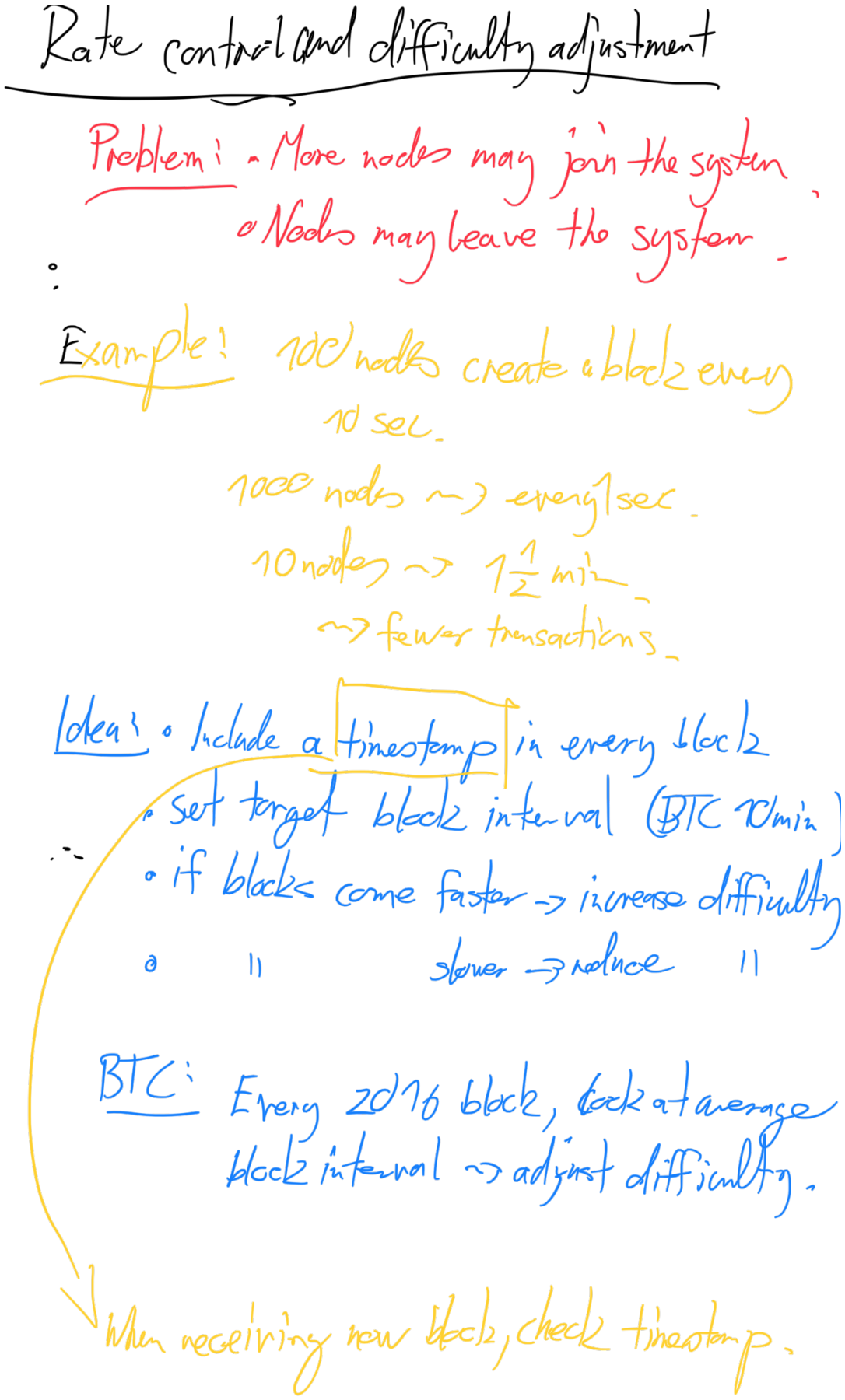
Forks


Rate control and difficulty adjustment
Problem: - More nodes may join the system
- Nodes may leave the system
Example: 100 nodes create a block every 10 sec.
1000 nodes ~> every 1 sec.
10 nodes ~> 1 1/2 min.
~> fewer transactions.
Idea: - Include a timestamp in every block
- set target block interval (BTC 10 min)
- if blocks come faster -> increase difficulty
- " slower -> reduce "
BTC: Every 2016 block, look at average block interval -> adjust difficulty.
When receiving new block, check timestamp.

In BTC Expected time to next block is 10 min

$P[\text{block is created in one sec}] = p_{sec}$

$$\frac{1}{p_{sec}} = 600 \qquad p_{sec} = \frac{1}{600}$$

Bitcon Blocks: https://www.blockchain.com/explorer?view=btc
Ethereum Blocks: https://ethblockexplorer.org/blocks?page=1

Fees

- What transaction to put into a block?
- Why not publish an empty block?

→ Transactions pay a fee:

$$\sum \text{Input}_{\text{value}} - \sum \text{Output}_{\text{value}} = \text{Fee}$$

- Creator of a block gets

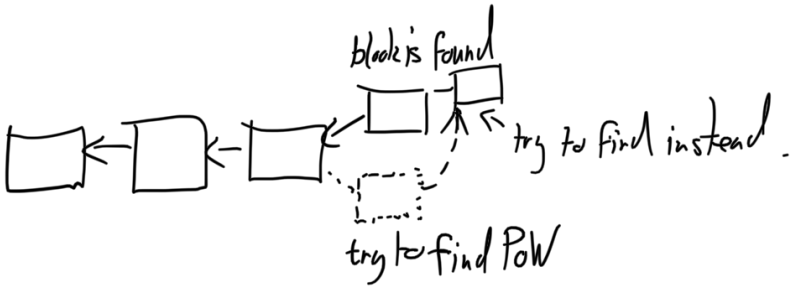
$$\sum_{\text{tx in block}} \text{Fee} + \text{block reward}$$

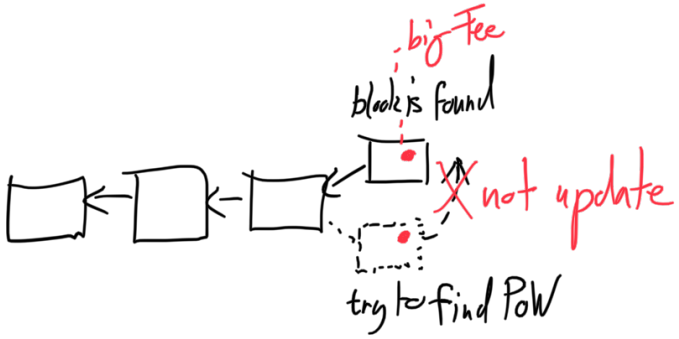
Block reward

- creates money
- pays for mining (PoW)
- gives small fees

Bitcoin:

- Initially block reward was 25 bitcoin
- Halved every 4 years.





Coin base transaction

C, Fees + reward new output, no input
includes miners pub key

→ No two miners have the same block.

How big is the fee

- Mining payed for by reward
- Fee covers cost (send/verify/apply)
- Independent of amount
- Cost depends on size

  Many inputs/outputs → high fee
- High fee ⇝ fast inclusion

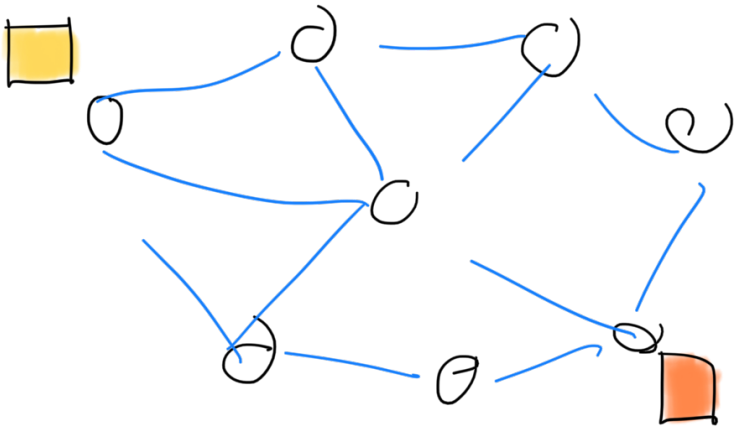
Ex 1

Forks

Def Fork is if multiple blocks have same predecessor

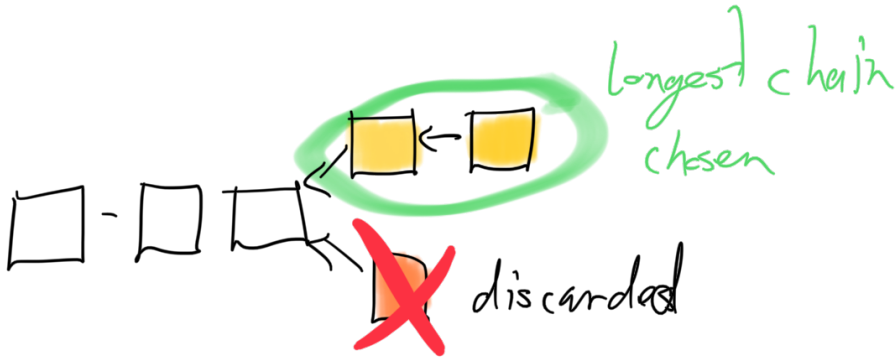
Why: Two blocks are found at the

same time.



Bitcoin: 2013

~ 12.6 sec to receive a block.



Longest Chain Rule:

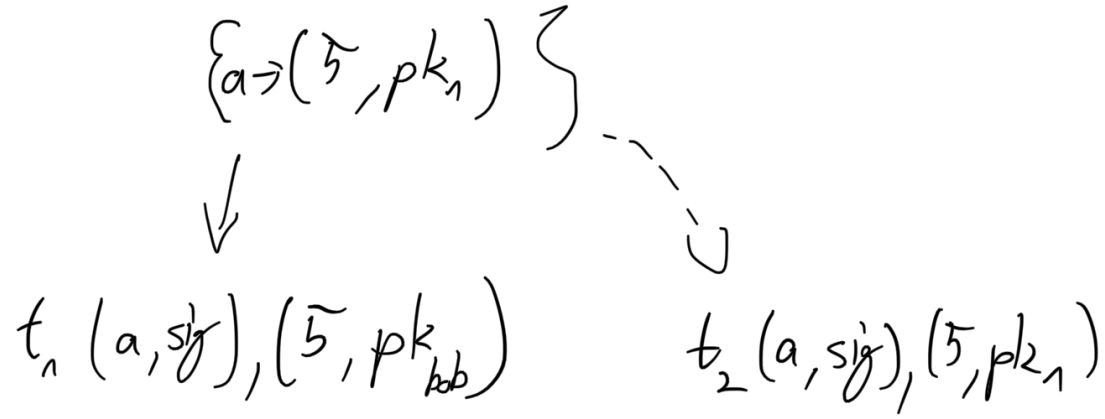
If a fork exists, all nodes should adopt longest chain

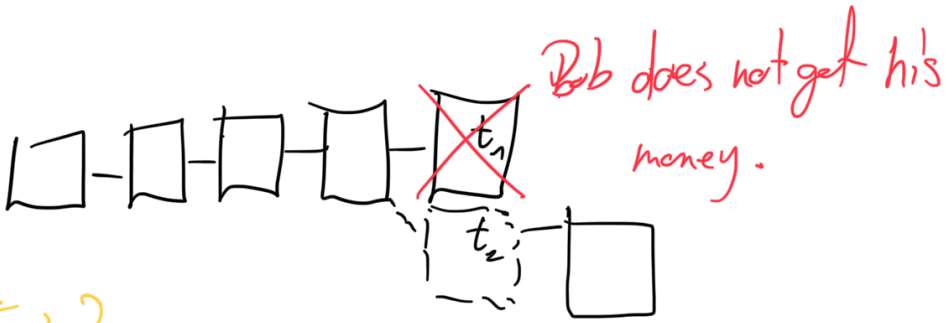
Fork problems:

Smaller chain is discarded

- Miner looses reward
- Some transactions may be only in the fork.
- Double spend:
  - Two transactions spending the same output may be in different forks.

Double spend:

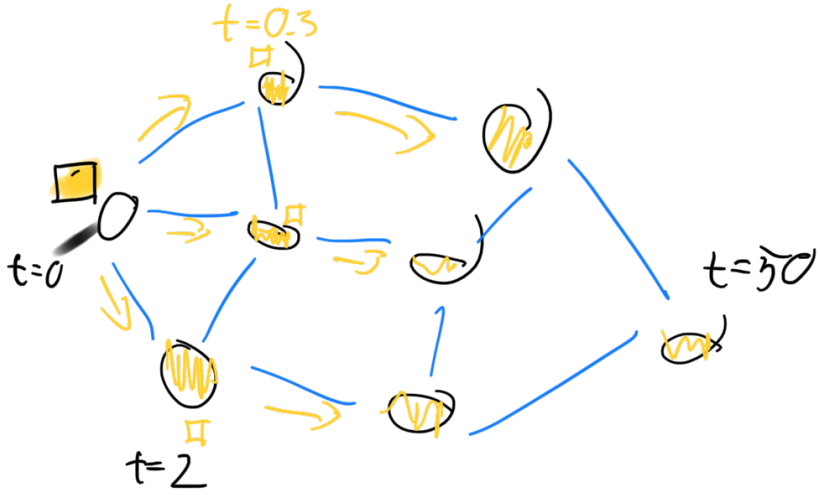




#2

Forks & Network latency

Let δ be avg. time until a miner receives a new block.



Bitcoin (2013) $\delta = 12{,}6$ sec

Theorem:

$$P[\text{fork}] = 1 - (1-p)^{\delta}$$

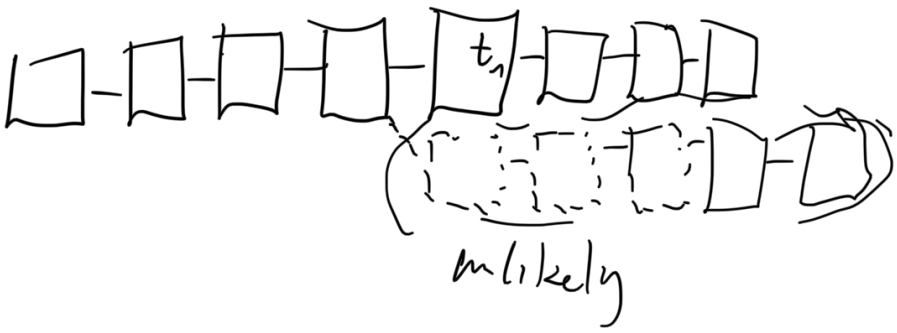
$p = P[\text{block is found in 1 sec}]$

$1 - \left[(1-p)^{\delta} \right]$ — no block in δ sec

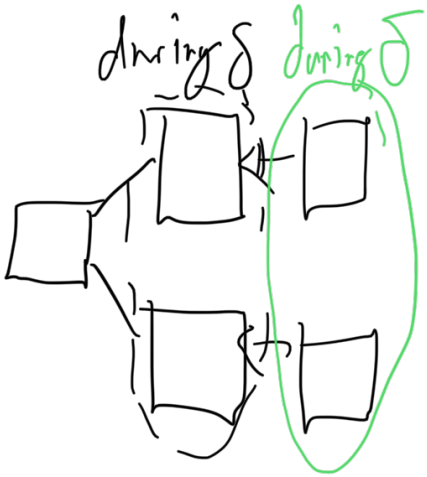
$(1-p)$ — no block in 1s

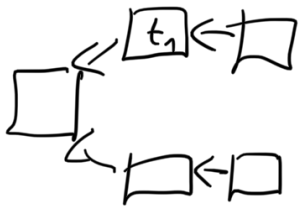
1 — block in δ sec

Bob should wait for more blocks



why



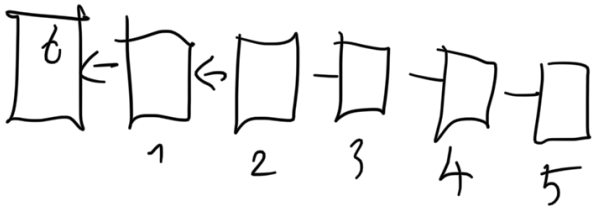


Corrolary: Length ℓ fork has

$$P[\ell\text{-fork}] \leq P[\text{fork}]^{\ell}$$

Bitcoin: Transaction is confirmed, if

$\hat{b}$ blocks are added on top



Ex 3