DAT650 Lecture

Transaction fees and longest chain rule

Leander Jehl

Fees

Fees

- Each transaction pays:

$$\sum Inputs - \sum Outputs = Fee$$

- Every block has a **<u>coinbase transaction</u>** with no input and outputs with value

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

Fees

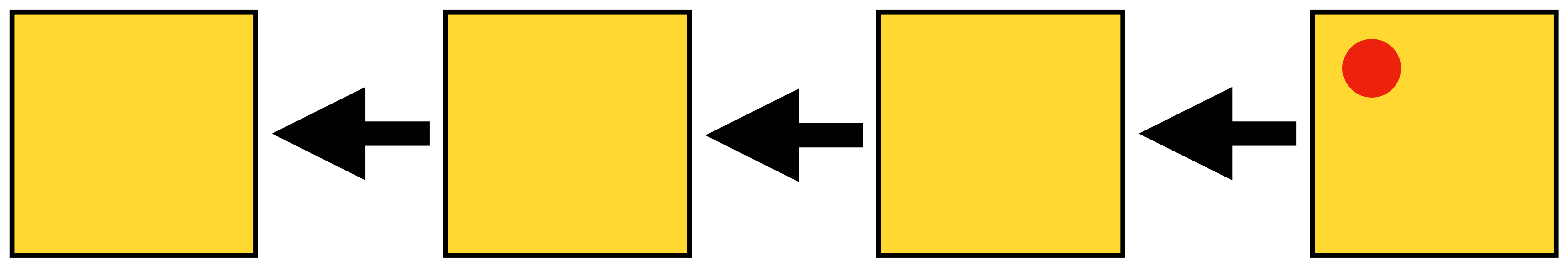
- Block reward creates money.
    - Brings the currency in circulation
- Block reward + fees pay for the mining
- Block reward gives small fees
    - I.e. miners would mine anyway

Bitcoin:

- Initially block reward was 25 bitcoin
- Block reward is halfed every 4 years
- -> Only finitely many bitcoin will be created

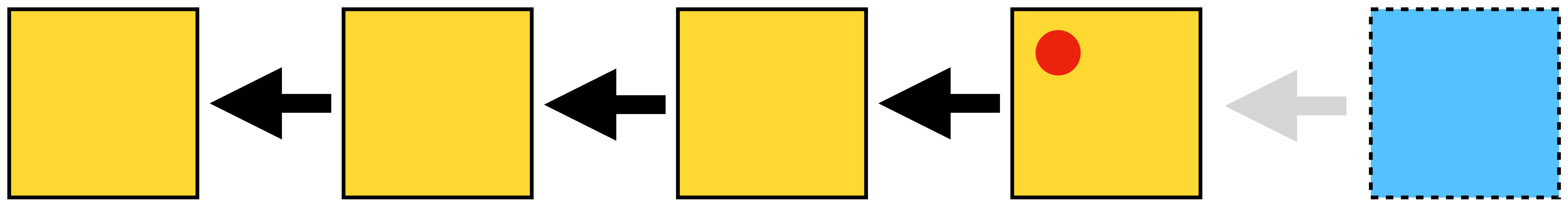
Fees

- If block reward is small miners might fight over fees:



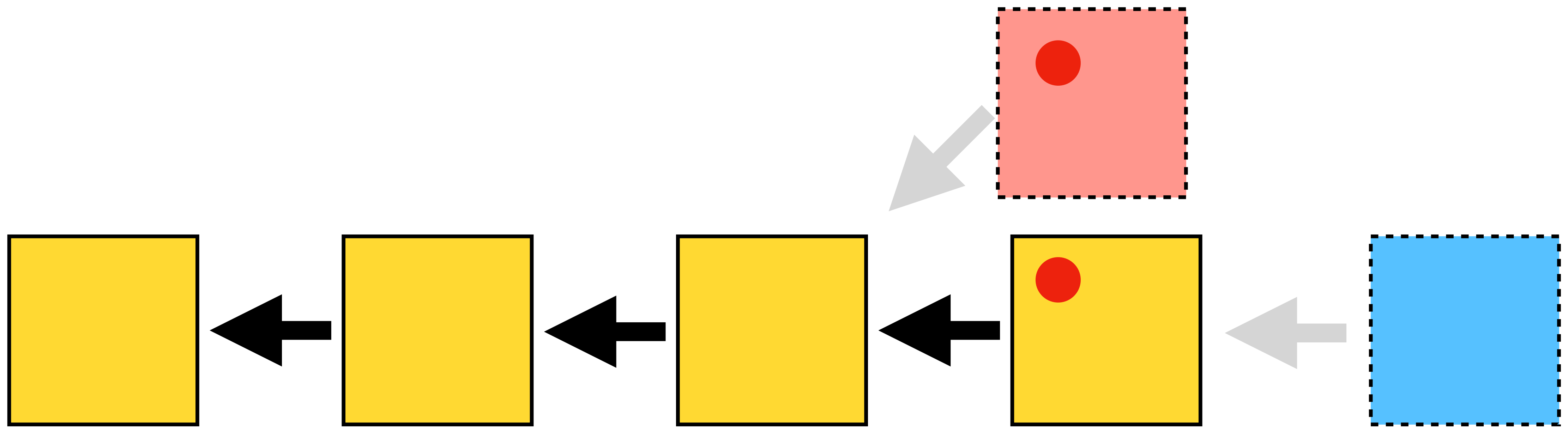
Fees

- If block reward is small minors might fight over fees:



Fees

- If block reward is small minors might fight over fees:



- Mine for the red or blue block?
    - Red might give more reward.

Coinbase transaction

- Includes the address of the miner
    - No two miners mine the same block
    - Cannot steal a PoW solution

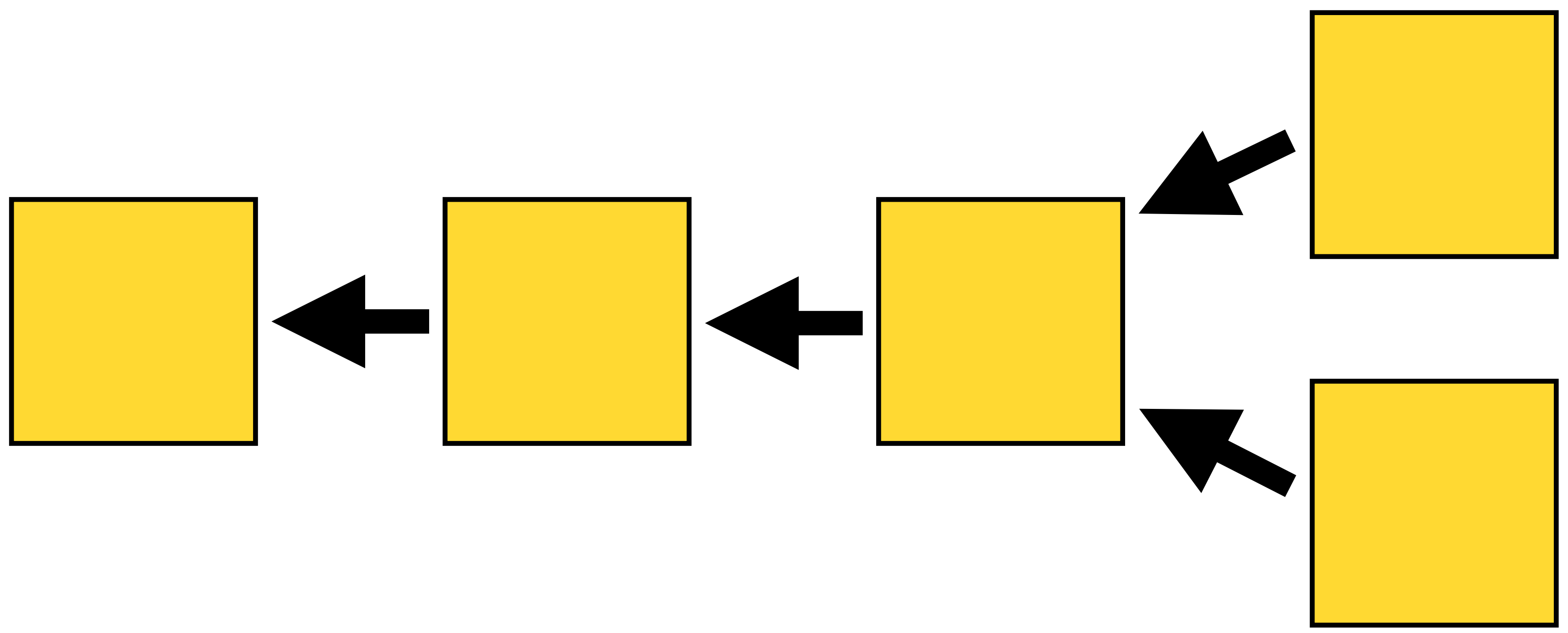
How big is the Fee?

- If mining is payed by block reward
- Fee covers cost (send/verify/apply transaction)
- Cost is independent of amount
- Cost depends on size
  - Many inputs/outputs give high fee.
- High fee gives faster transactions.

Forks and longest chain rule

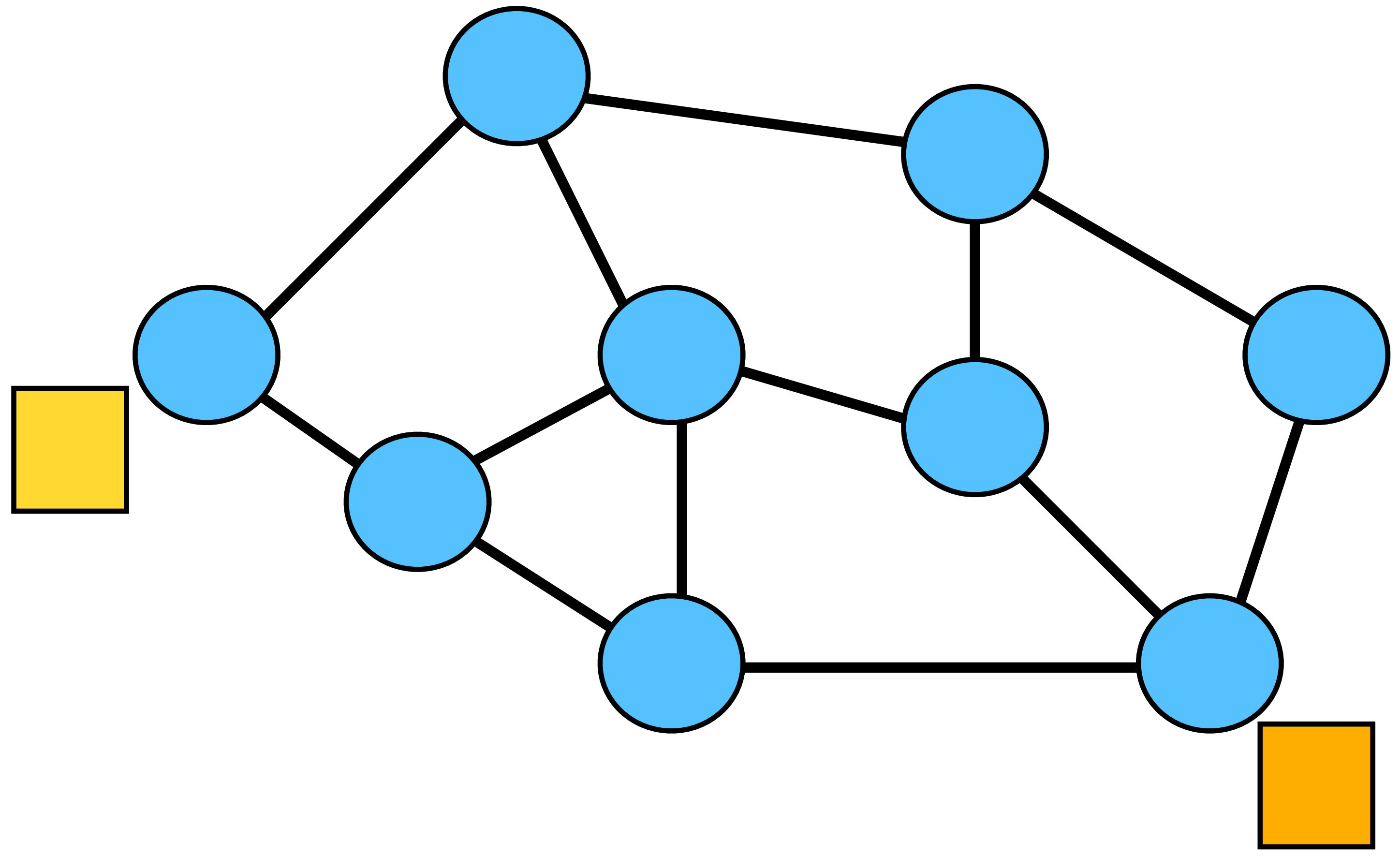
Forks

- A fork is if multiple blocks have the same predecessor



- Why: Two blocks found “concurrently”

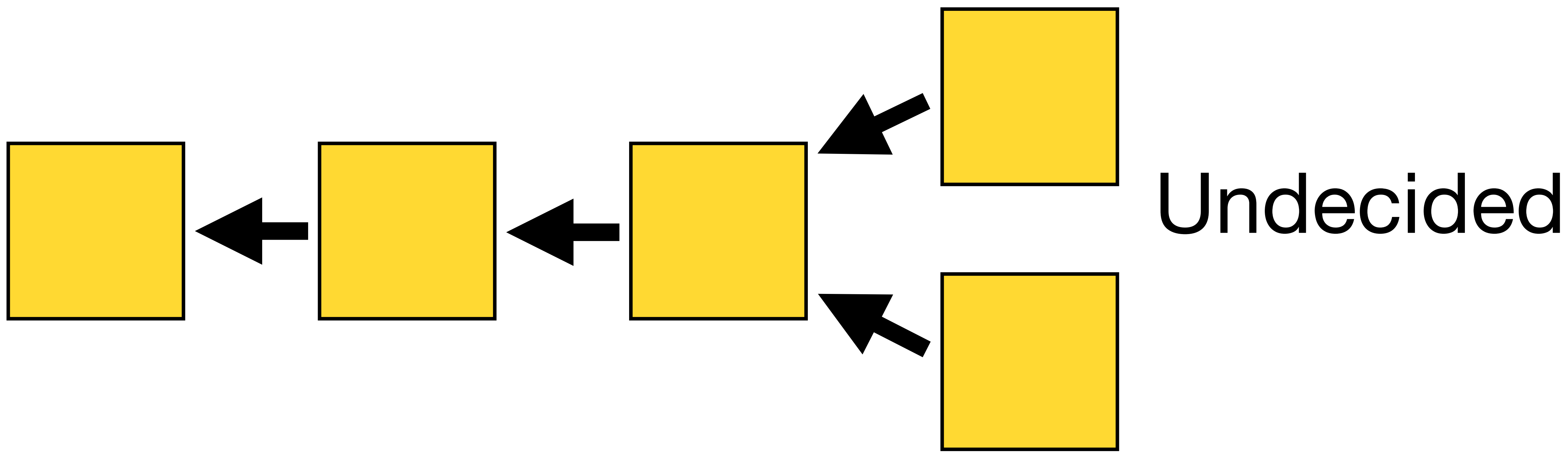
Forks



- Why: Takes time until every node knows about the new block.
  - Bitcoin: 2013 ~ 12.6sec

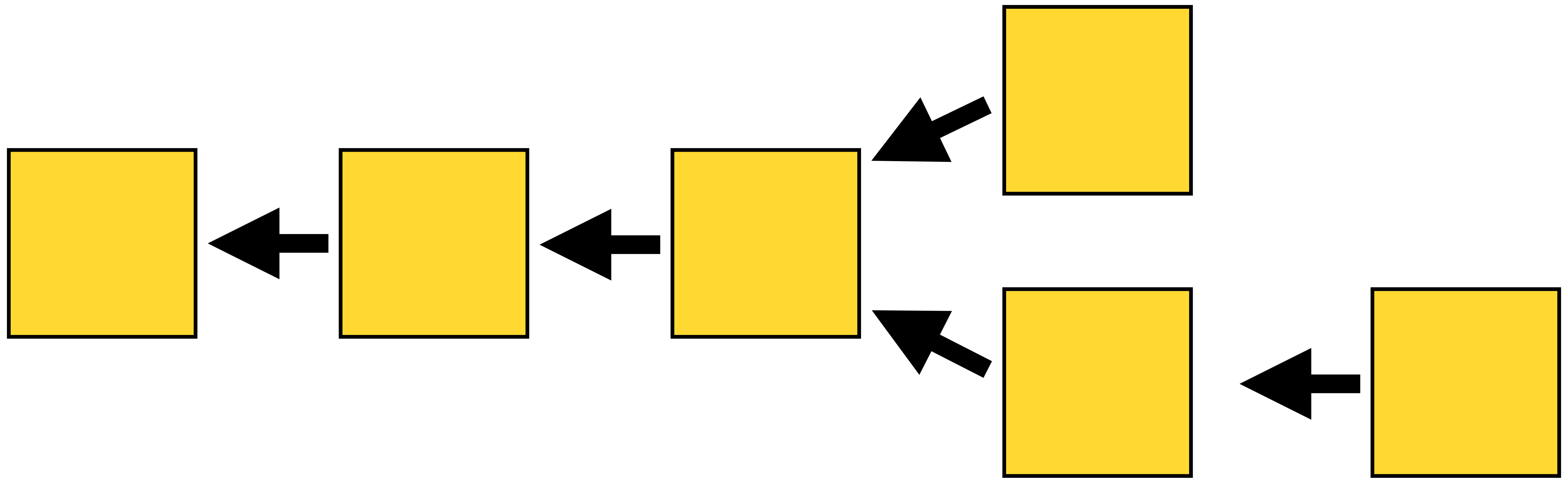
Forks: Longest chain rule

- If a fork exists, all nodes should adopt longer chain



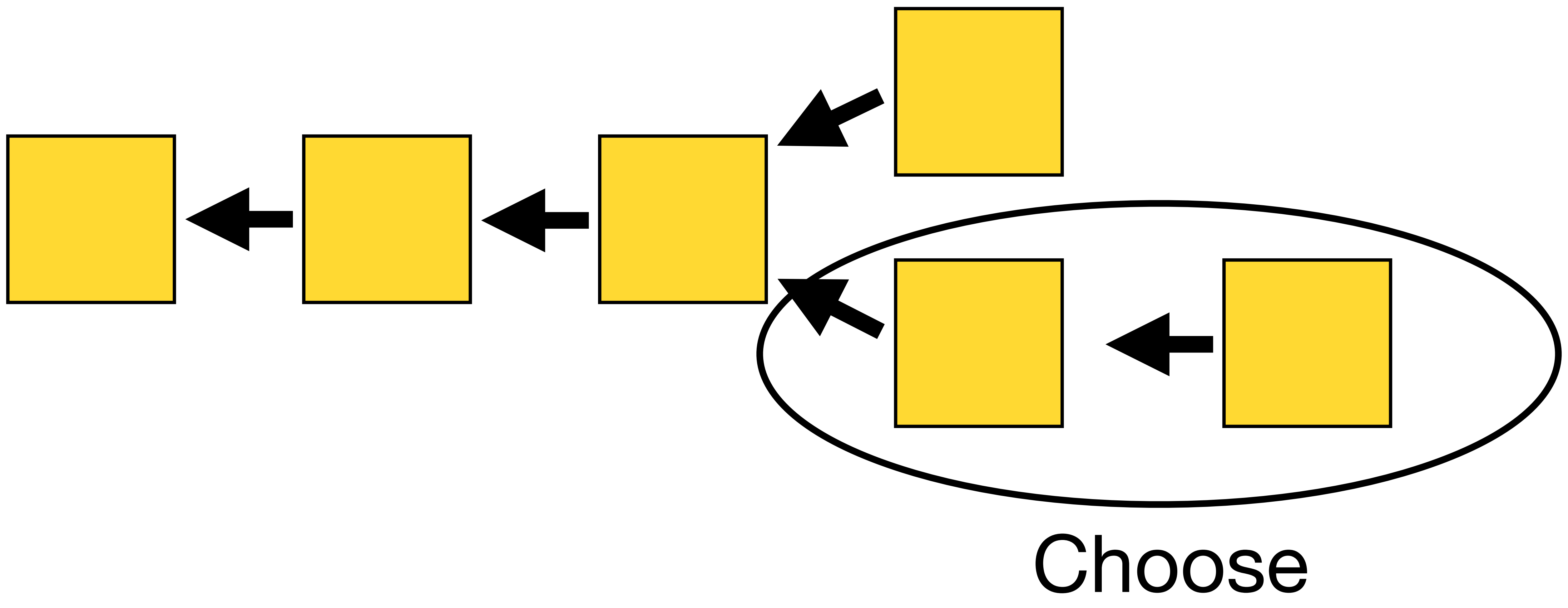
Forks: Longest chain rule

- If a fork exists, all nodes should adopt longer chain



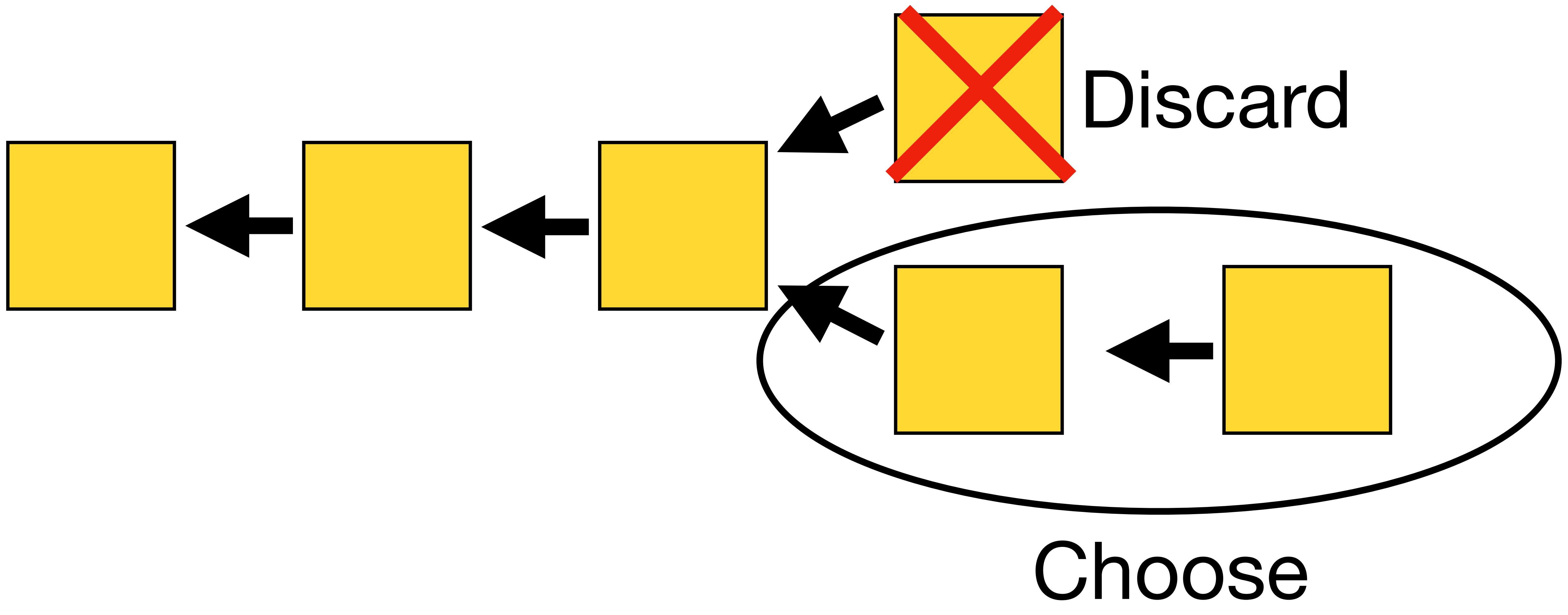
Forks: Longest chain rule

- If a fork exists, all nodes should adopt longer chain



Forks: Longest chain rule

- If a fork exists, all nodes should adopt longer chain



Forks: Longest chain rule

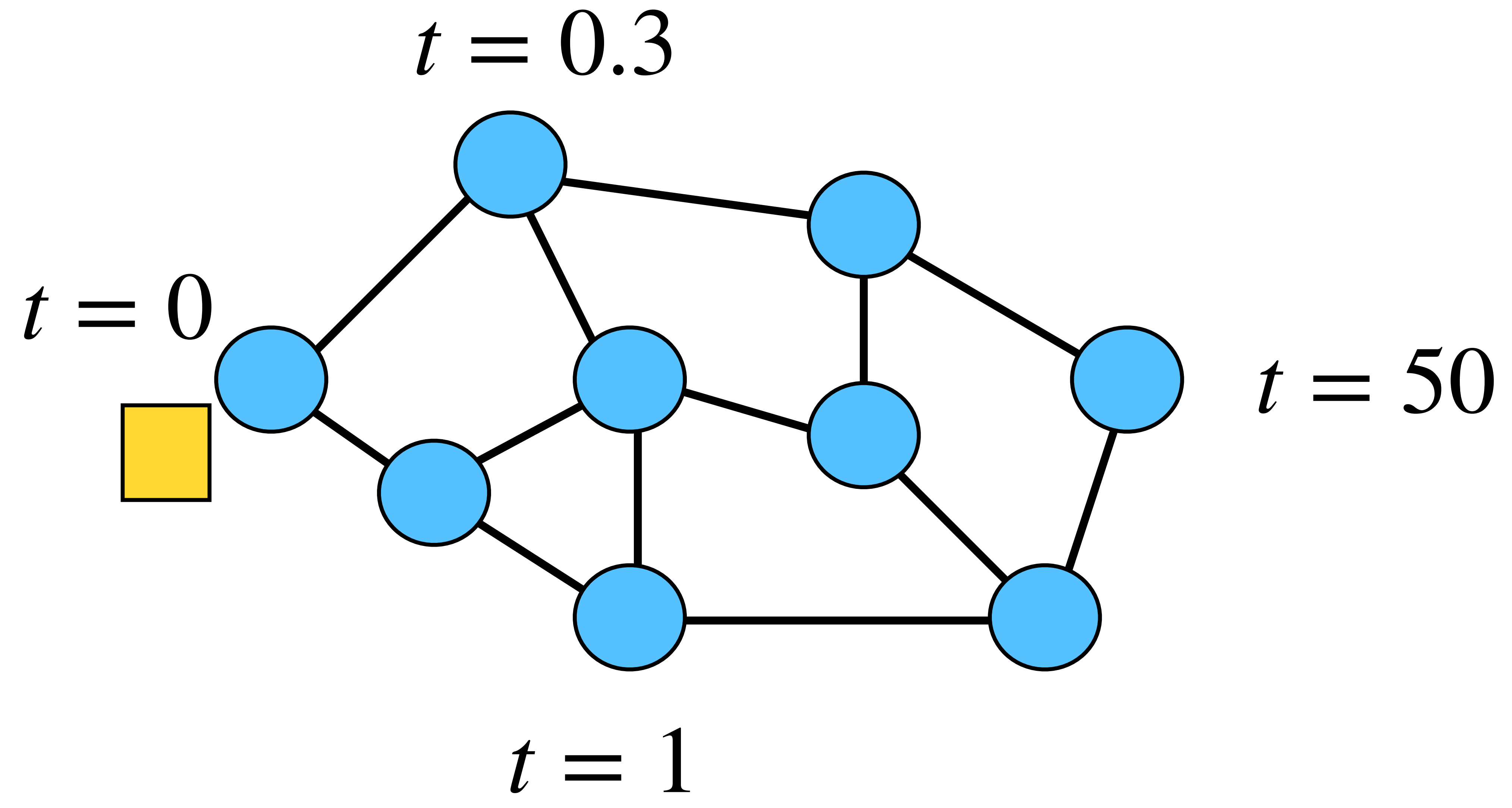
Problems

- Blocks & Transactions in smaller chain are discarded
  - Miners loose reward
  - Some transactions may be only in one fork
  - In case of double spend, two conflicting transactions may be included in different forks

PoW & Network latency

PoW & Network latency

- Let δ be the avg. time for a block to arrive at a node in the network.



- **Bitcoin:** $\delta = 12.6$sec (2013)

PoW & Network latency

Theorem: If we assume equal distribution of mining power, then

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

with $p = P[\textit{block found in 1 sec}]$

Proof: Nodes spend δ time mining on old block, after block is found.

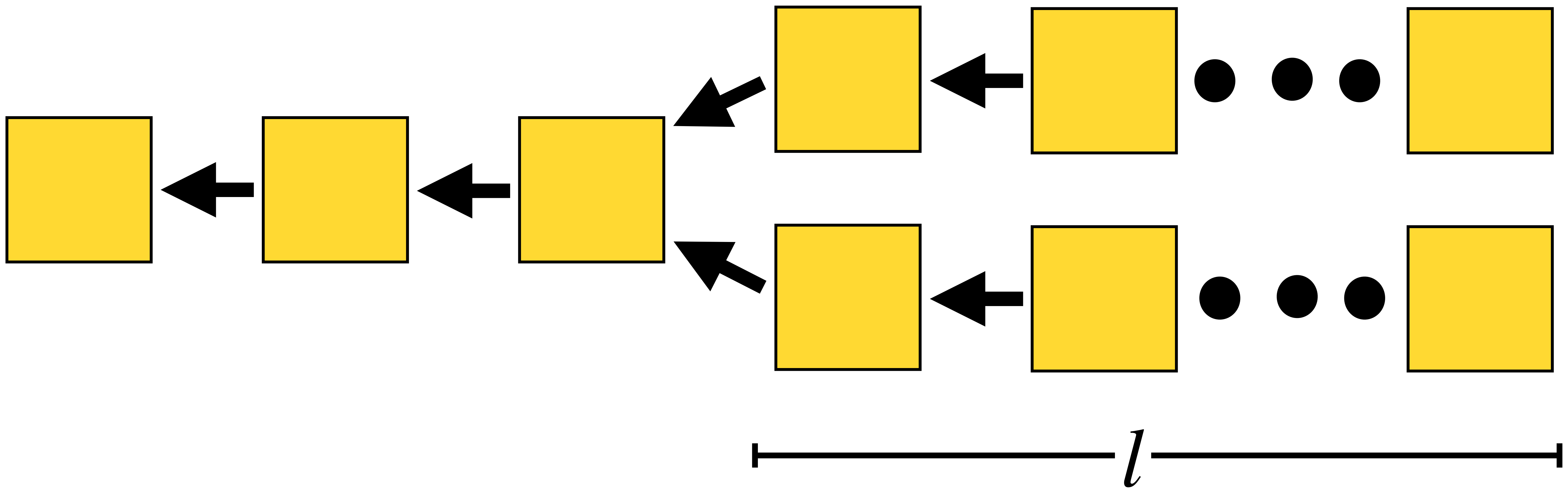
PoW & Network latency

Corrolary: Probabiliy for two chains of length l is

$$P[l \times fork] \leq P[fork]^l$$

drops exponentially.

.

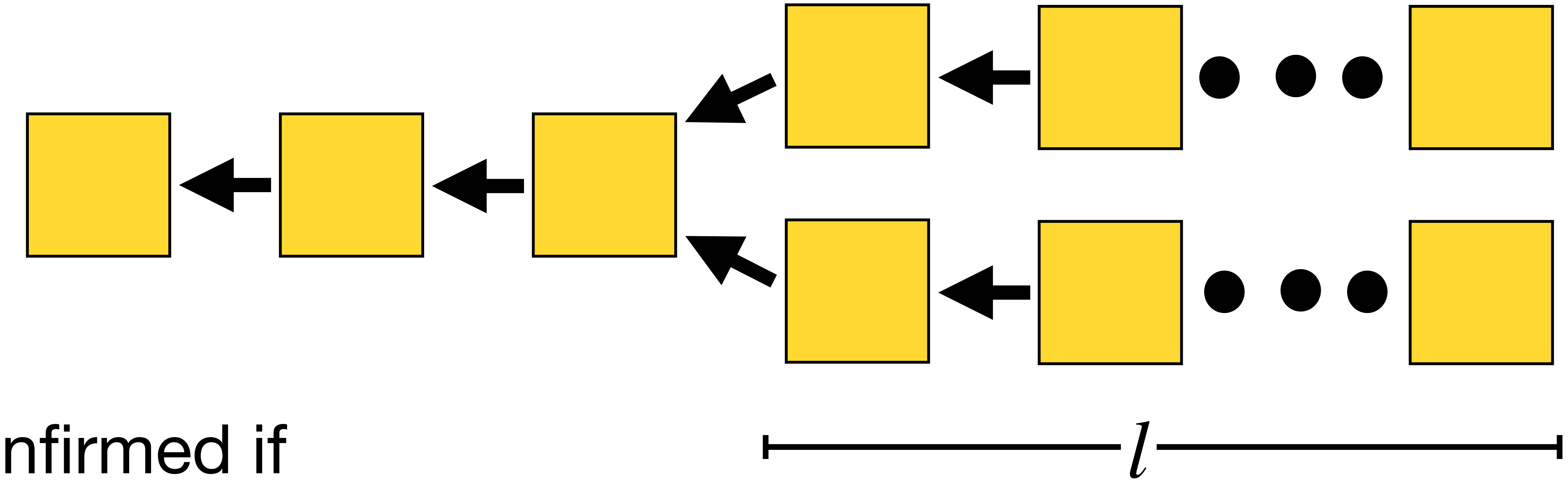


PoW & Network latency

Corrolary: Probabiliy for two chains of length l is

$$P[l \times fork] \leq P[fork]^l$$

drops exponentially.



Bitcoin: Transaction confirmed if
5 blocks are added on top.

Attacks

Attacks

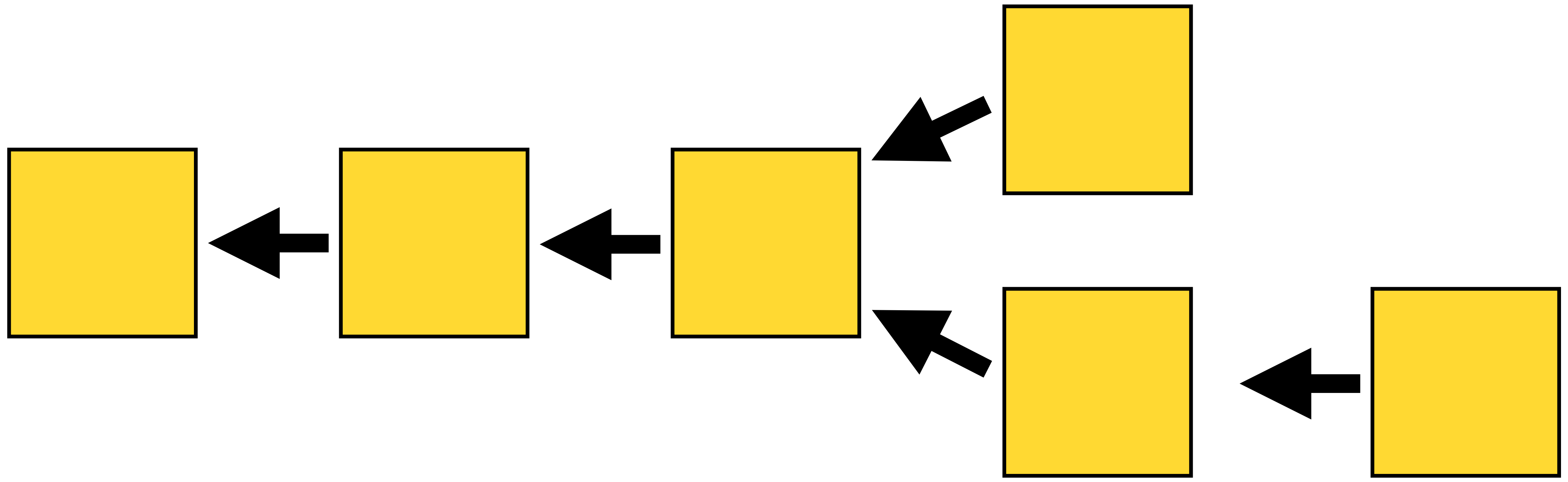
Attacks on bitcoin mining

- Longest chain rule is not enforced.

Attacks

Attacks on bitcoin mining

- Longest chain rule is not enforced.

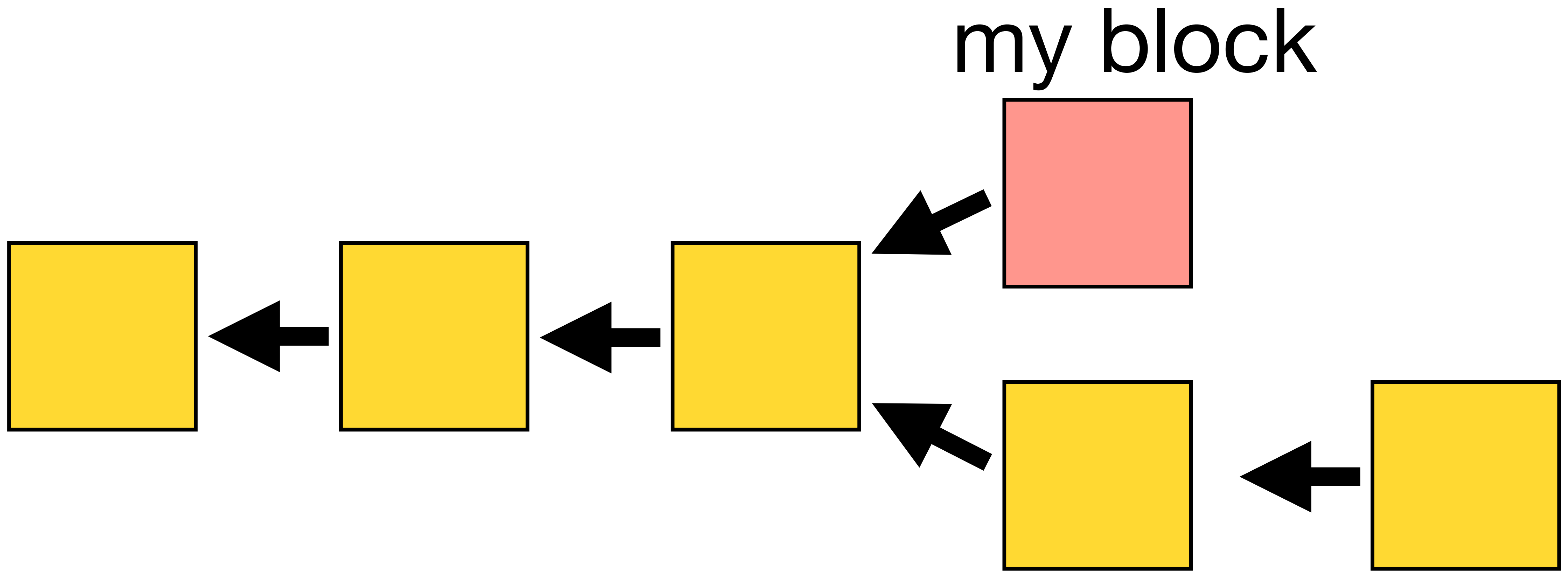


Switch to longest chain!

Attacks

Attacks on bitcoin mining

- Longest chain rule is not enforced.



Switch to longest chain!

But want to safe my block!

Stubborn mining

- Let α be the percentage of the systems mining power, that the attacker controls.
- Assume:
  - $p = \alpha$, attacker mines next block
  - $p = 1 - \alpha = \beta$, not-attacker mines next block

Stubborn mining

- $p = \alpha$, attacker mines next block
- $p = 1 - \alpha = \beta$, not-attacker mines next block
- First: Run attack for the next two blocks:

P	**Outcome attack**	**Outcome no attack**
$\alpha\alpha$	3	2
$\beta\beta$	0	0
$\alpha\beta$	0	1
$\beta\alpha$	1	1

Stubborn mining

- $p = \alpha$, attacker mines next block
- $p = 1 - \alpha = \beta$, not-attacker mines next block
- First: Run attack for the next two blocks:

P	Outcome attack	Outcome no attack
$\alpha\alpha$	3	2
$\beta\beta$	0	0
$\alpha\beta$	0	1
$\beta\alpha$	1	1

Stubborn mining

- $p = \alpha$, attacker mines next block
- $p = 1 - \alpha = \beta$, not-attacker mines next block
- First: Run attack for the next two blocks:

  Profitable if $E[\text{attack}] \geq E[\text{no attack}]$

$$3\alpha^2 + \alpha\beta \geq 2\alpha^2 + 2\alpha\beta$$
$$\alpha^2 \geq \alpha\beta$$

$$\alpha \geq 0.5$$

P	Outcome attack	Outcome no attack
$\alpha\alpha$	3	2
$\beta\beta$	0	0
$\alpha\beta$	0	1
$\beta\alpha$	1	1

Stubborn mining

- Run attack for 2 blocks: profitable for $\alpha \geq 0.5$
- Run attack for 4 blocks: profitable for $\alpha \geq 0.455$
- Run attack without early stop: profitable for $\alpha \geq 0.42$

Stubborn mining

- Running the attack forever, can be analysed using Markov models:

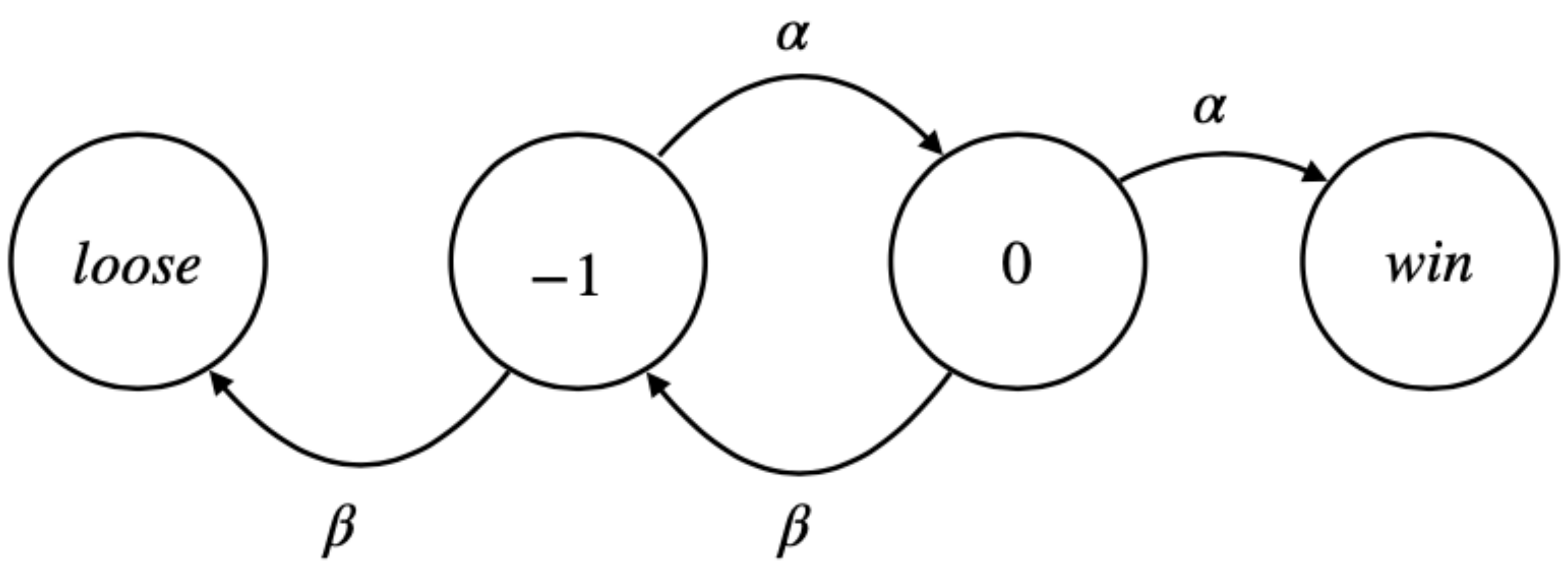


Figure 3.4: Stubborn mining states and transitions.