Altenative and scaling PoW

Leander Jehl

Scaling PoW

Scaling PoW - Bitcoin Throughput

What throughput has Bitcoin?

Scaling PoW - Bitcoin Throughput

What throughput has Bitcoin?

< 3000 transactions per block

- 5 transactions per second

Scaling PoW - Reparametrization Bitcoin

Bitcoin parameters:

- Block size
- Block delay

Scaling PoW - Reparametrization Bitcoin

Bitcoin parameters:

- Block size
- Block delay

Increazing throughput with reparametrization gives more forks!

- bad for security (e.g. selfish mining)
- bad for small miners (loose block rewards in forks)

GHOST

Greedy heaviest-observed subtree

Increazing throughput with reparametrization gives more forks!

- bad for security (e.g. selfish mining)

GHOST: *Instead of longest chain, always select block with the heaviest subtree* (i.e. most blocks in subtree).

GHOST

Greedy heaviest-observed subtree

Increazing throughput with reparametrization gives more forks!

- bad for security (e.g. selfish mining)

GHOST: *Instead of longest chain, always select block with the heaviest subtree* (i.e. most blocks in subtree).

- same as Longest chain if a single fork
- in selfish mining, attackers chain does not have forks
- causing forks, e.g. through network attack does not help attacker

GHOST

Greedy heaviest-observed subtree

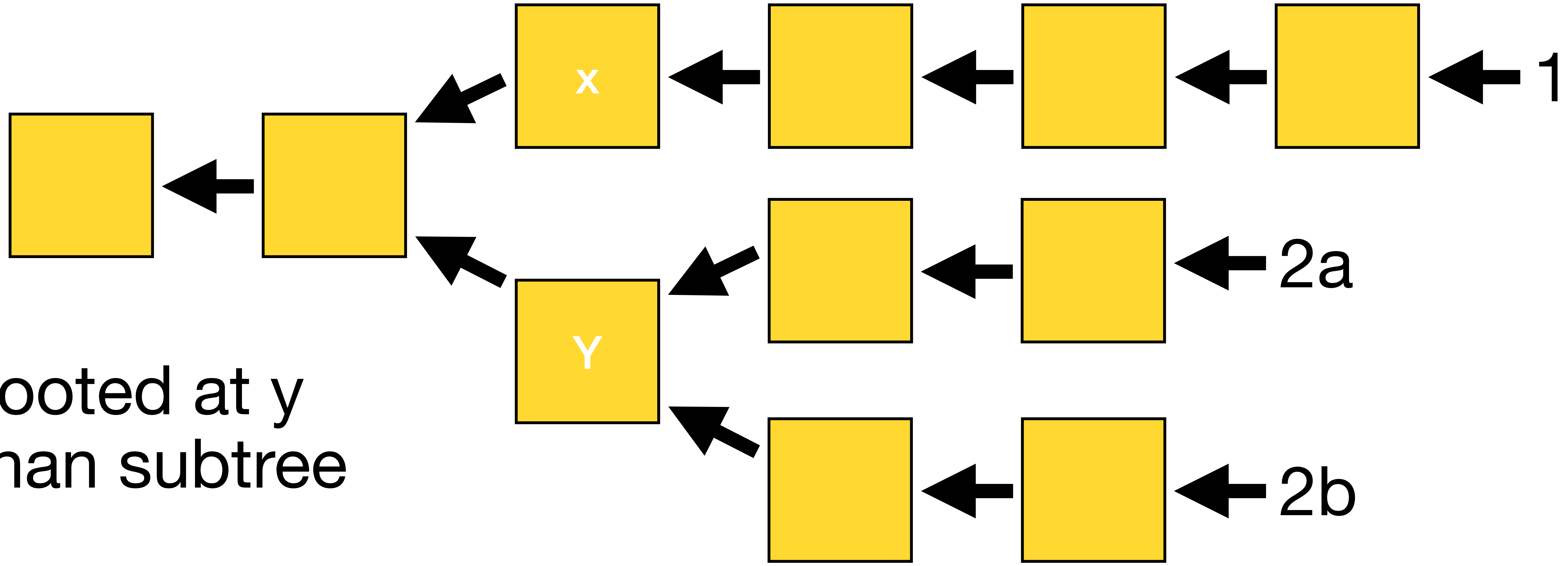
Example:

Longest chain rule:
Mine at 1

GHOST:

Mine at 2a or 2b

- Because subtree rooted at y has more blocks than subtree rooted at x



Inclusive blockchain

Uncle blocks

Increazing throughput with reparametrization gives more forks!

- bad for small miners (loose mining reward)

Inclusive blockchain

Uncle blocks

Increazing throughput with reparametrization gives more forks!

- bad for small miners (loose mining reward)

Uncles: Additional to the parent pointer, a node can point a child/descendant of one of his ancestors as *uncle* if

- The uncle has lower depth
- The uncle is not an uncle of an ancestor

Inclusive blockchain

Uncle blocks

Increazing throughput with reparametrization gives more forks!

- bad for small miners (loose mining reward)

Uncles: Additional to the parent pointer, a node can point a child (descendant) of one of his ancestors as *uncle* if

- The uncle has lower depth
- The uncle is not an uncle of an ancestor

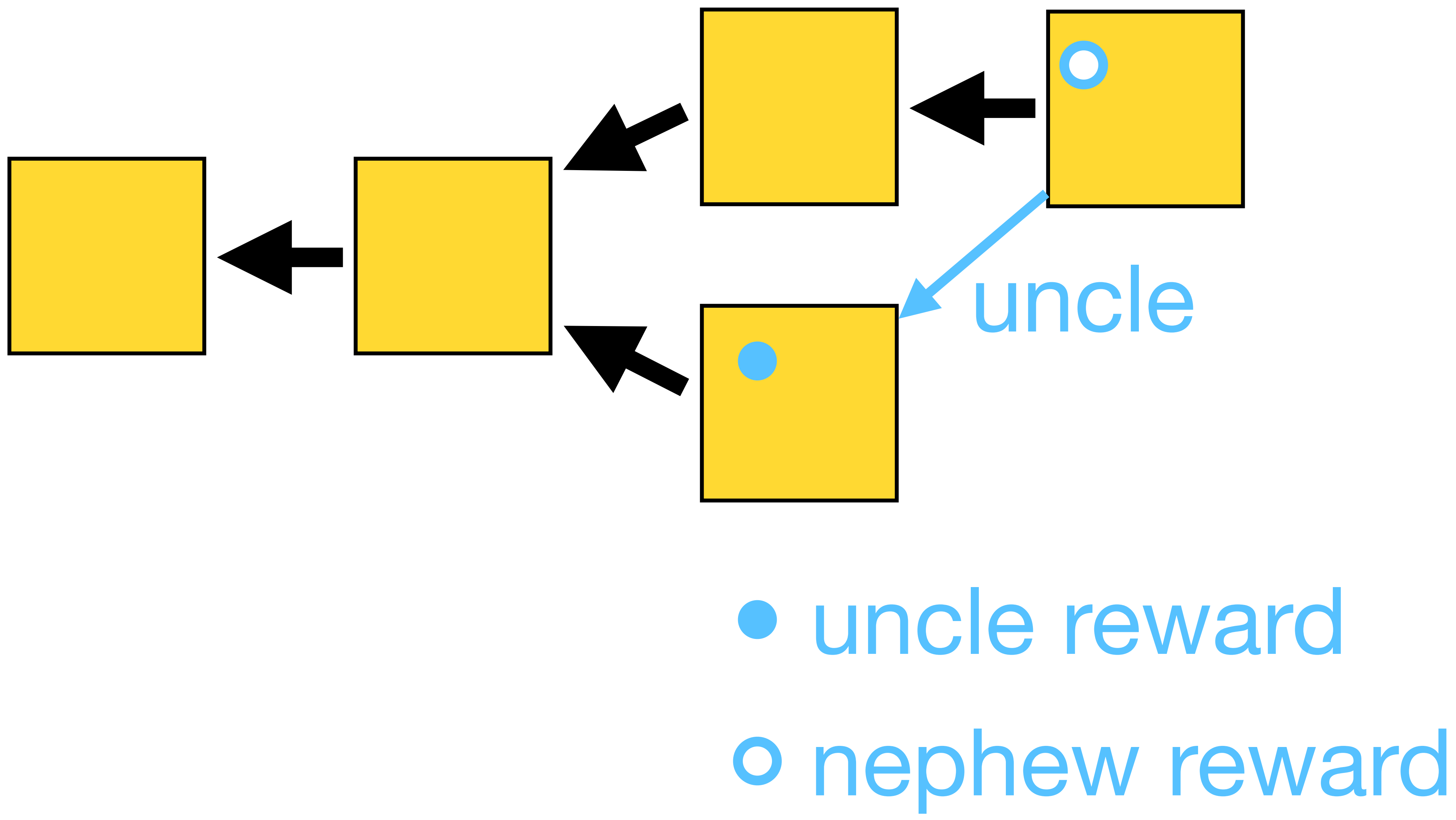
An uncle receives a fraction of his block reward.

The miner including the uncle receives a fraction of the uncles block reward

Inclusive blockchain

Uncle blocks

Example



● uncle reward

○ nephew reward

Inclusive blockchain

Uncle blocks

Analysis

- Uncle and nephew rewards create money
- Uncle rewards may make selfish mining more efficient

Need to adjust difficulty
according to total money created!

Alternative PoW

Alternative PoW

What to improve

Idea: Use alternative PoW to achieve

- ASIC resistance
- Usefull PoW
  E.g. use computing power to:
  - Find prime numbers?
  - Train machine learning models?
  - Protein folding

Alternative PoW

How to improve

PoW function must have:

- Adjustable difficulty

Possible to adjust difficulty if system grows.

- Fast verification

Easier to verify then compute.

- Progress freedome

Not possible to make “progress” towards a solution.
Winning chances are the same after trying for 1h.

Alternative PoW

What is the scarce resource?

Problem: Distribute “voting” power in an anonymous system with sybils.

PoW: computation is scarce resource.

one CPU one vote (Satoshi)

Alternative PoW - Proof of Storage

What is the scarce resource?

Use **storage capacity** as scarce resource.

one disc one vote

Alternative PoW - Proof of Storage

What is the scarce resource?

Use **storage capacity** as scarce resource.

one disc one vote

- Can use merkle-proof
- Idea: PoW difficulty is lower, if you store files
  Invest in more storage, rather than more computation.

Alternative PoW - Proof of Storage

What is the scarce resource?

Use **storage capacity** as scarce resource.

one disc one vote

- Can use merkle-proof
- Idea: PoW difficulty is lower, if you store files
  Invest in more storage, rather than more computation.

Problems:

- What to store?
- Is the storage proof fresh?
- Storage vs. download on demand?

Alternative PoW - Proof of Storage

What is the scarce resource?

Use **storage capacity** as scarce resource.

one disc one vote

- Can use merkle-proof
- Idea: PoW difficulty is lower, if you store files
  Invest in more storage, rather than more computation.

Problems:

- What to store?
- Is the storage proof fresh?
- Storage vs. download on demand?

What is usefull Proof of Storage?

Does it use less energy?

Alternative PoW - Proof of Stake

What is the scarce resource?

Use currency as scarce resource.

one dollar one vote

(the rich get richer)

Alternative PoW - Proof of Stake

What is the scarce resource?

- Idea: Freeze a certain amount of money to be able to mine.
- PPCoin (Peercoin)

$$H(\texttt{prevblockhash}||addr||\texttt{timeinsec}) < d_0 \cdot \text{coin}(addr)$$

- Base difficutly d_0 adjusted based on deposit coin$(addr)$
- `timeinsec` ensures only one try every second

Alternative PoW - Proof of Stake

What is the scarce resource?

- PPCoin (Peercoin)

$$H(\texttt{prevblockhash}||addr||\texttt{timeinsec}) < d_0 \cdot \text{coin}(addr)$$

Problems:

- **Predictability** (will I get the next block)
- **can PoW** (change transactions to get next block)
- **Non deciding** (can mine on two forks)
- **History rewrite** (can rewrite complete history)