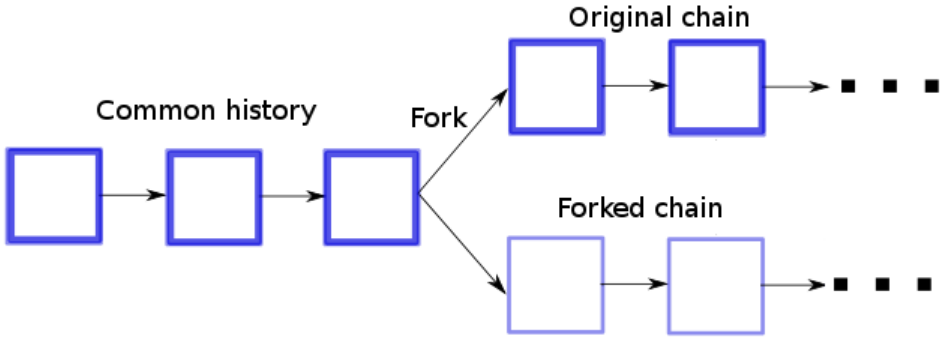
How Bitcoin Achieves Decentralization

Forks and Attacks



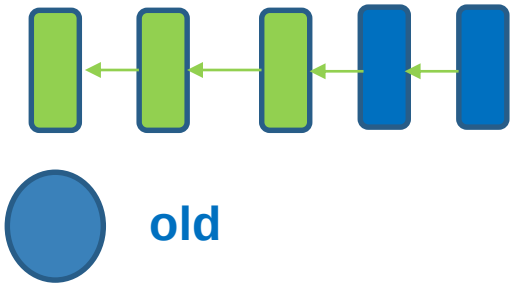
Hard forks

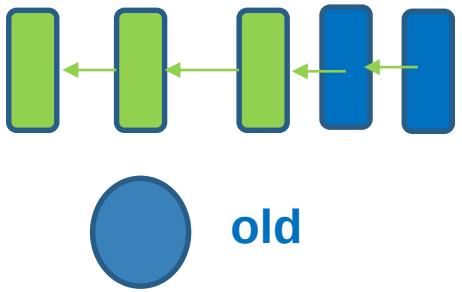
Relaxing the rules

Hard fork possibilities

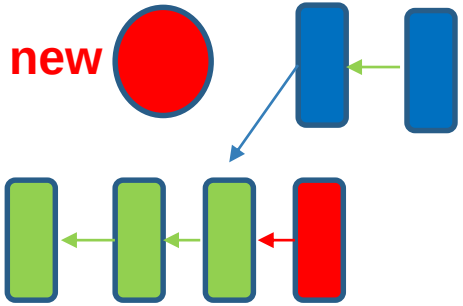
- New op codes
- Changes to size limits (increasing)
- Changes to mining rate
- Many small bug fixes

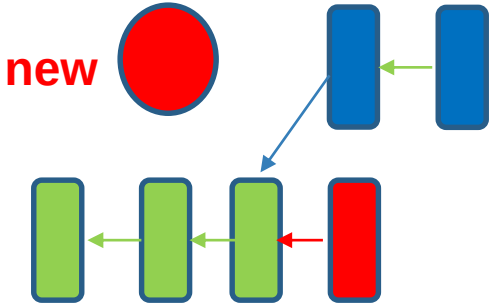
- 1 M bytes/block (10 min)
- >250 bytes/transaction
- 7 transactions/sec ☹





HARD FORK (block-size limit increased)



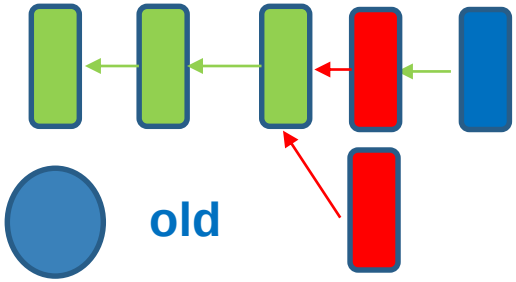


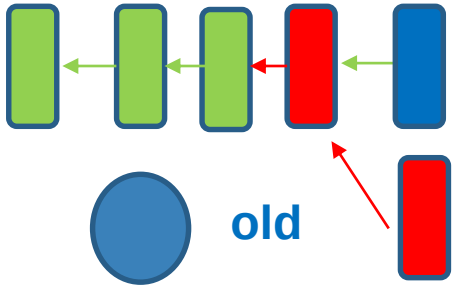
Soft forks

We can add new features which only *limit* the set of valid transactions

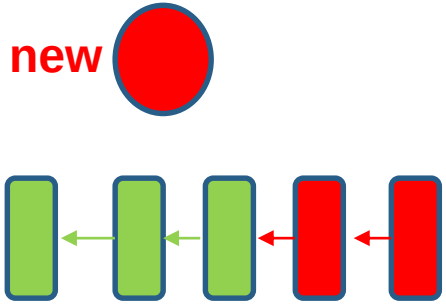
Soft fork possibilities

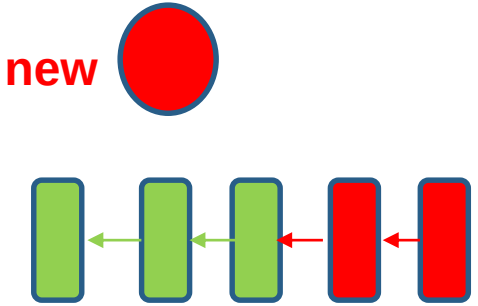
- New signature schemes
- Changes to size limits (decreasing)
- Extra per-block metadata
  - Shove in the coinbase parameter
  - Commit to UTXO tree in each block





SOFT FORK (block-size limit decreased)





Energy consumption & ecology

Thermodynamic limits

Landauer's principle: Any non-reversible computation must consume a minimum amount of energy.

Specifically, each bit changed requires (kT ln 2) joules. K is Boltzman Constant and T is the Temperature of the circuit in kelvins

SHA-256 is not reversible

Energy consumption is inevitable

Energy aspects of Bitcoin mining

- **Embodied energy:** used to manufacture mining chips & other equipment
  - should decrease over time
  - returns to scale
- **Electricity:** used to perform computation
  - should increase over time
  - returns to scale
- **Cooling:** required to protect equipment
  - costs more with increased scale!

Estimating energy usage: top-down

- Each block worth approximately **US$6,500**
- Approximately **$11/s** generated
- Industrial electricity (US):
  $0.03/megajoule or $0.10/kilowatt-hour

Upper bound on electricity consumed:

367 MJ/s = **367 MW**

1 watt (power)=1 joule/s (energy)

Estimating energy usage: bottom-up

- Best claimed efficiency: **1 gigahashes/sec/watt**
- Network hash rate: **150,000,000 gigahashes/sec**
  (excludes cooling, embodied energy)

Lower bound on electricity consumed:

150 MW

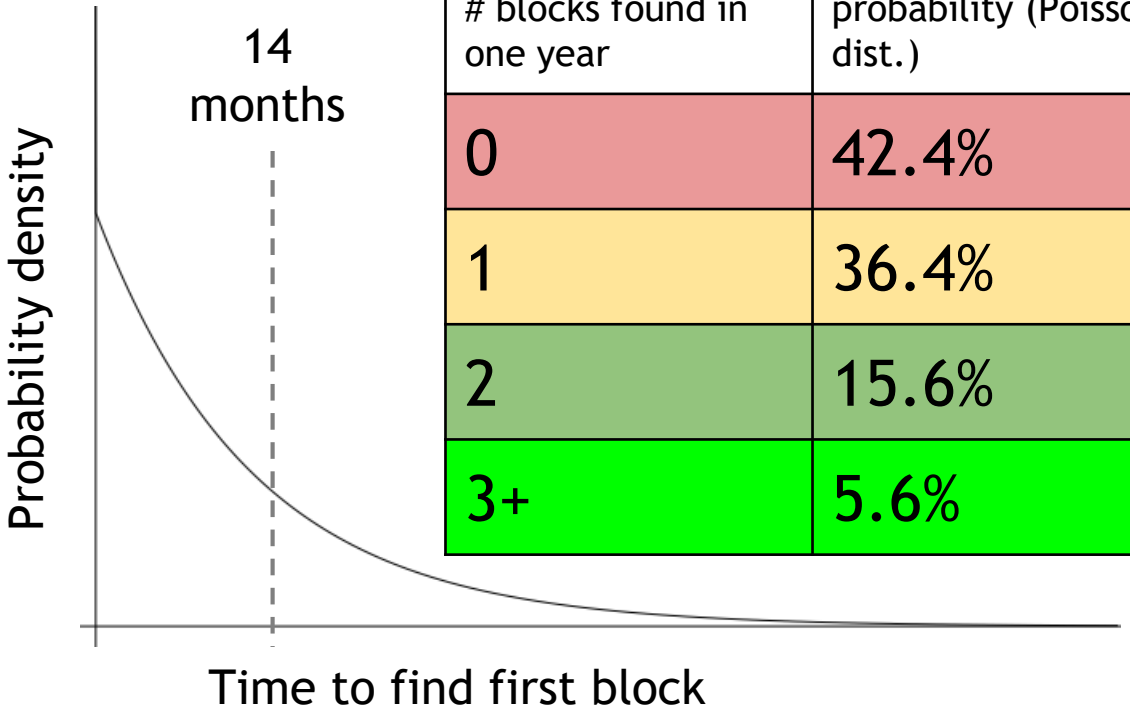
Mining pools

Economics of being a small miner

TerraMiner IV

- Cost: ≈US$6,000
- Expected time to find a block: ≈14 months
- Expected revenue: ≈$1,000/month

Mining uncertainty



# blocks found in one year	probability (Poisson dist.)
0	42.4%
1	36.4%
2	15.6%
3+	5.6%

Mining pools

- **Goal:** pool participants all attempt to mine a block with the same coinbase recipient
  - send money to key owned by pool manager
- Distribute revenues to members based on how much work they have performed
  - minus a cut for pool manager

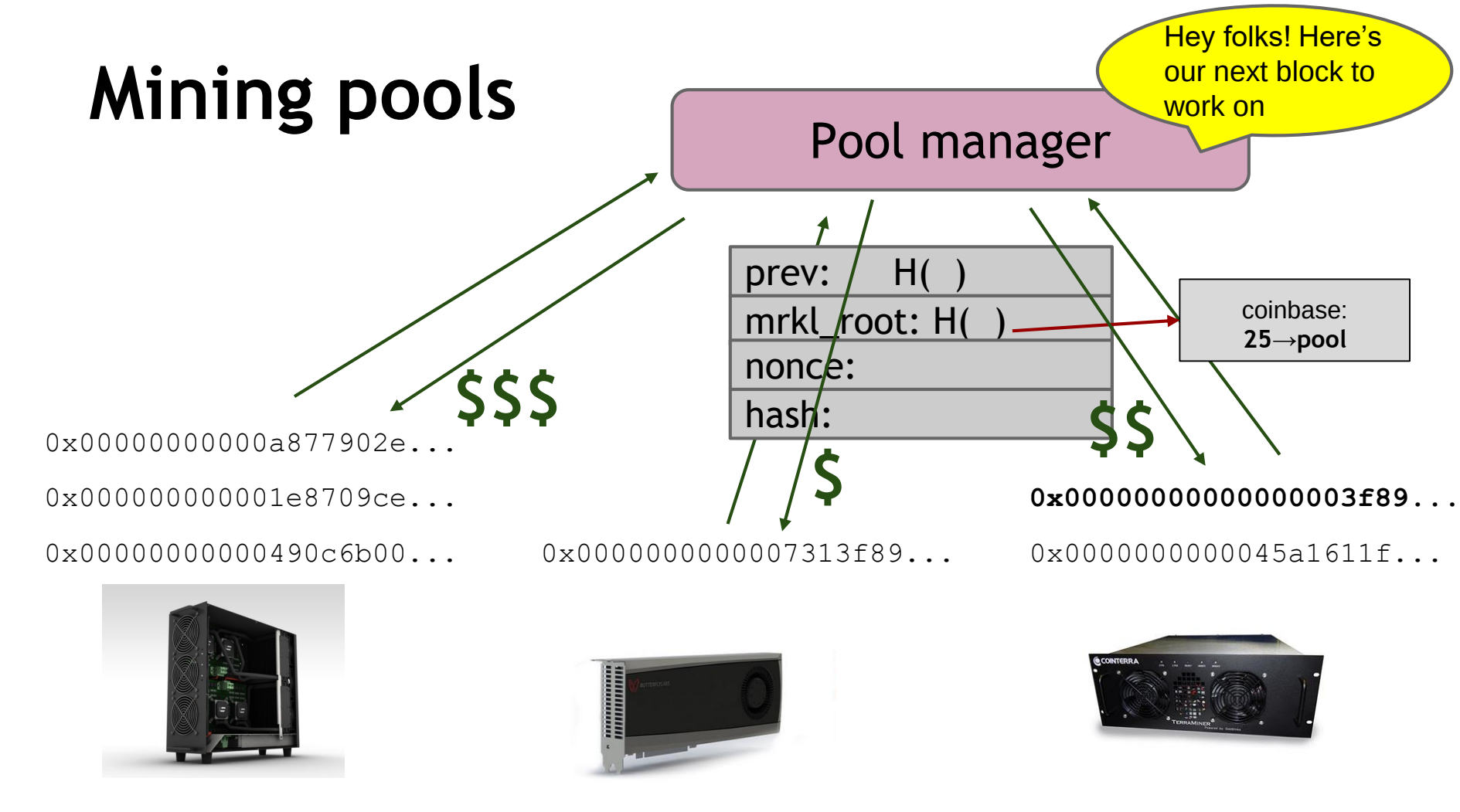
How do we know how much work members perform?

Mining shares

Idea: prove work with “near-valid blocks” (shares)

```
4AA087F0A52ED2093FA816E53B9B6317F9B8C1227A61F9481AFED67301F2E3FB
D3E51477DCAB108750A5BC9093F6510759CC880BB171A5B77FB4A34ACA27DEDD
00000000008534FF68B98935D090DF5669E3403BD16F1CDFD41CF17D6B474255
BB34ECA3DBB52EFF4B104EBBC0974841EF2F3A59EBBC4474A12F9F595EB81F4B
00000000002F891C1E232F687E41515637F7699EA0F462C2564233FE082BB0AF
0090488133779E7E98177AF1C765CF02D01AB4848DF555533B6C4CFCA201CBA1
460BEFA43B7083E502D36D9D08D64AFB99A100B3B80D4EA4F7B38E18174A0BFB
00000000000000078FB7E1F7E2E4854B8BC71412197EB1448911FA77BAE808A
652F374601D149AC47E01E777613845618 1FA4F9D0EEDD8C4FDE3BEF6B1B7ECE
785526402143A291CFD60DA09CC80DD066BC723FD5FD20F9B50D614313529AF3
000000000041EE593434686000AF77F54CDE839A6CE30957B14EDEC10B15C9E5
9C20B06B01A0136F192BD48E0F372A4B9E6BA6ABC36F02FCED22FD9780026A8F
```

Mining pools



Mining pool variations

- **Pay per share:** flat reward per share
  - Typically minus a significant fee
  - What if miners never send valid blocks?
- **Proportional:** typically since last block
  - Lower risk for pool manager
  - More work to verify and distribute rewards

- Many others….

Mining pool protocols

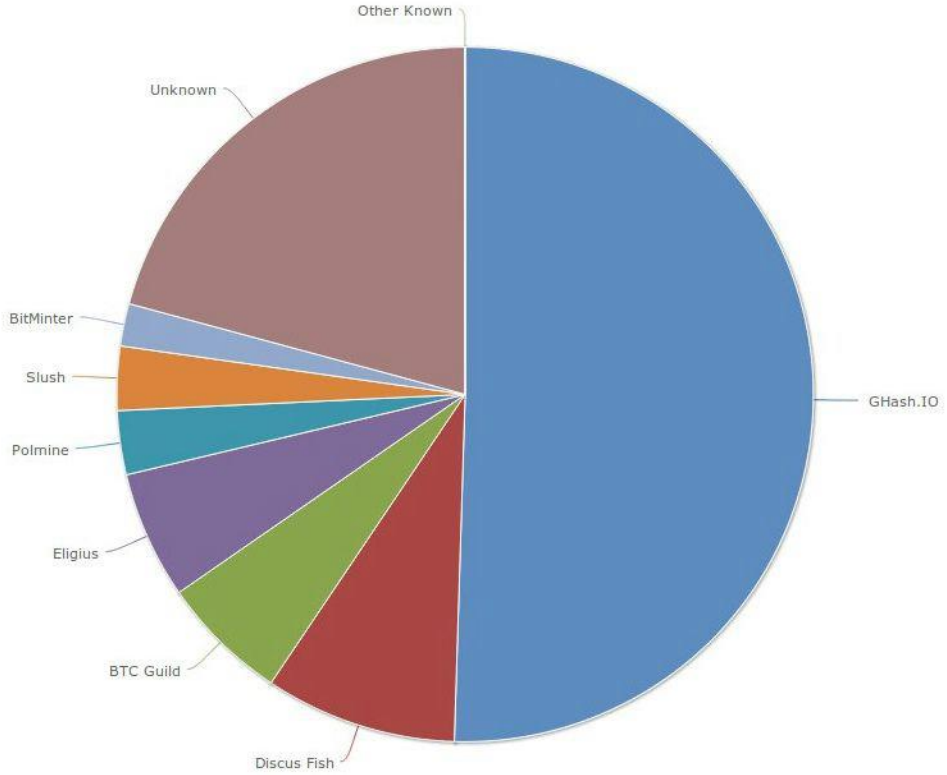
- API for fetching blocks, submitting shares
  - Stratum
  - Getwork
  - Getblockshare
- Proposed for standardization with a BIP (Bitcoin Improvement Proposal)
- Increasingly important; some hardware support

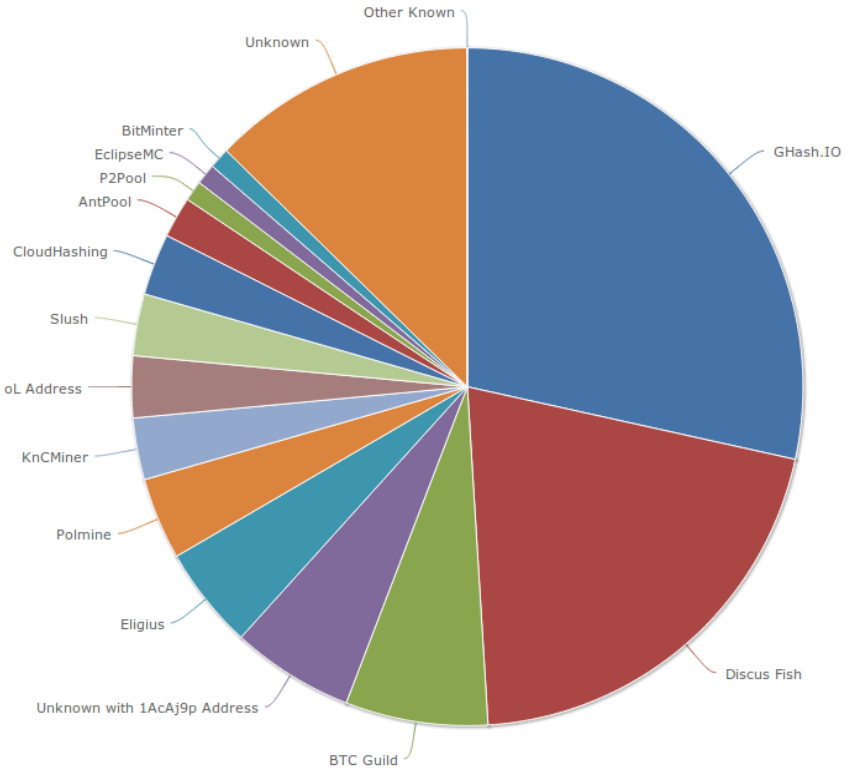
Mining pool history

- First pools appear in late-2010
  - Back in the GPU era!
- By 2014: around 90% of mining pool-based
- June 2014: GHash.io exceeds 50%

Mining pools Hash Power

(as of June 2014,August 2014)





Are mining pools a good thing?

- Pros
  - Make mining more predictable
  - Allow small miners to participate
  - More miners using updated validation software
- Cons
  - Lead to centralization
  - Discourage miners from running full nodes (offload the validation tasks to pool mangrs)

Mining incentives and strategies

Why identity?

Pragmatic: some protocols need node IDs

Security: assume less than 50% malicious

Why don’t Bitcoin nodes have identities?

No Central Authority

Identity is hard in a P2P system — Sybil attack

Pseudonymity is a goal of Bitcoin

Weaker assumption: select random node

Analogy: lottery or raffle

When tracking & verifying identities is hard, we give people tokens, tickets, etc.

Now we can pick a random ID & select that node

Key idea: implicit consensus

In each round, random node is picked

This node proposes the next block in the chain

Other nodes implicitly accept/reject this block
- by either extending it
- or ignoring it and extending chain from earlier block

Every block contains hash of the block it extends

Game-theoretic analysis of mining

Several strategic decisions

- Which transactions to include in a block
  - Default: any above minimum transaction fee
- Which block to mine on top of
  - Default: longest valid chain
- How to choose between colliding blocks
  - Default: first block heard
- When to announce new blocks
  - Default: immediately after finding them

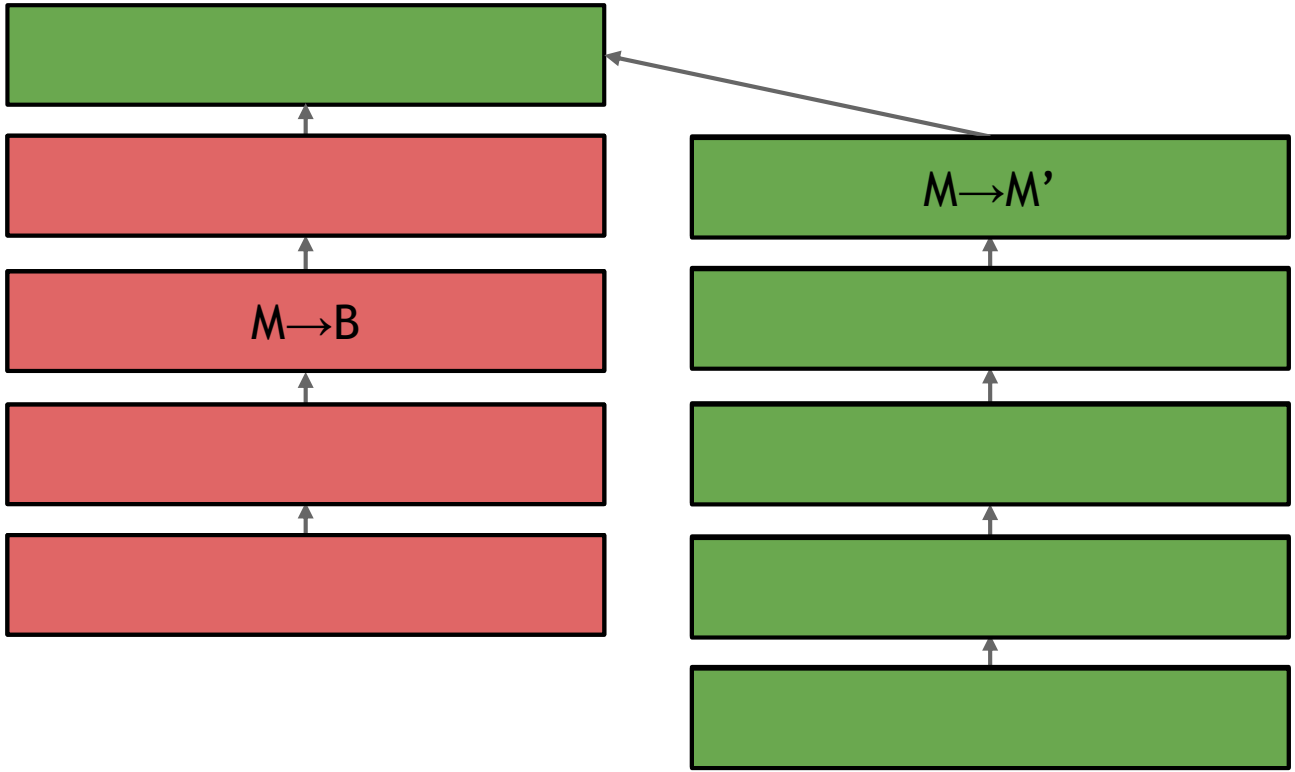
Game-theoretic analysis of mining

Assume you control $0 < \alpha < 1$ of mining power

Can you profit from a non-default strategy?

For some α, **YES**, though analysis is ongoing!

Forking attacks



Forking attacks

- Certainly possible if $\alpha > 0.5$
  - may be possible with less
  - avoid block collisions
- Attack is detectable
- Might be reversed
- Might crash exchange rate

Forking attacks via bribery

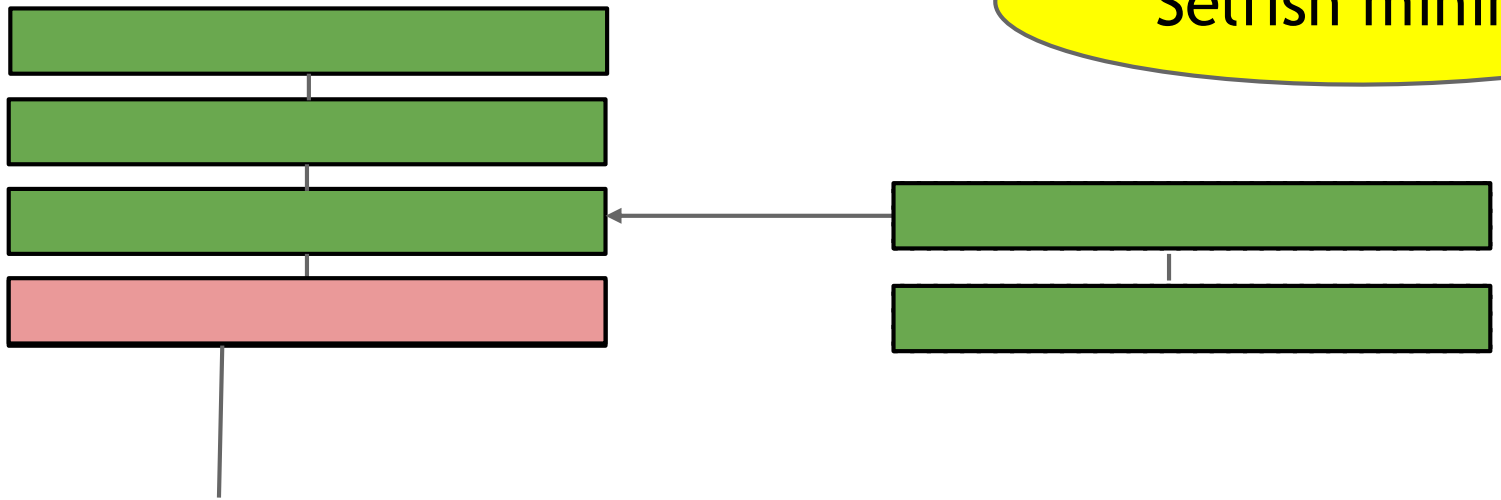
- **Idea:** building $\alpha > 0.5$ is expensive. Why not rent it instead?

- Payment techniques:
  - Out-of-band bribery
  - Run a mining pool at a loss
  - Insert large “tips” in the block chain

This is an open problem!

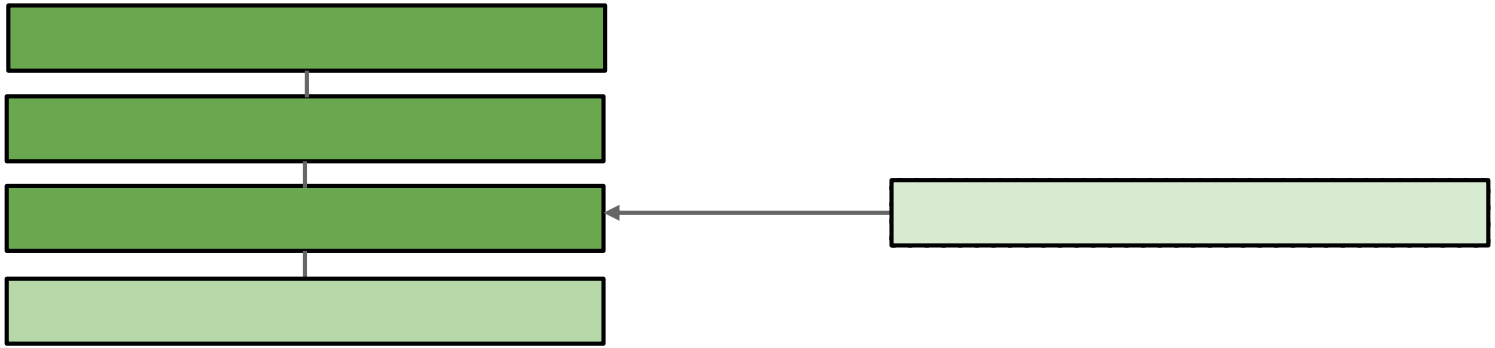
Block-withholding attacks

Strategy: don't announce blocks right a



Block-withholding attacks, take 2

What happens if a block is announced when you're ahead by 1?



The race is on!

Block-withholding attacks

- Improved strategy for any **α** if you can win every race
  - Ideal network position
  - Bribery?
- With a 50% chance of winning races, improved strategy for **α > 0.25**
- Not yet observed in practice!

Surprising departure from previous assumptions