CS 731: Blockchain Technology And Applications

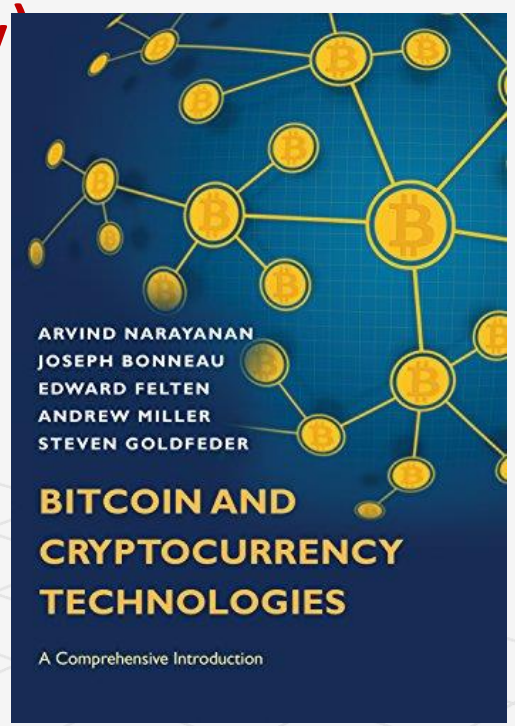
Sandeep K. Shukla

IIT Kanpur

C3I Center

Acknowledgement

- The material of this lecture material is mostly due to Prof. Arvind Narayanan's Lecture at Princeton and his book on Bitcoin (Chapter 5 mostly)



Recap: Bitcoin miners

Bitcoin depends on miners to:

- Store and broadcast the block chain
- Validate new transactions
- Vote (by hash power) on consensus

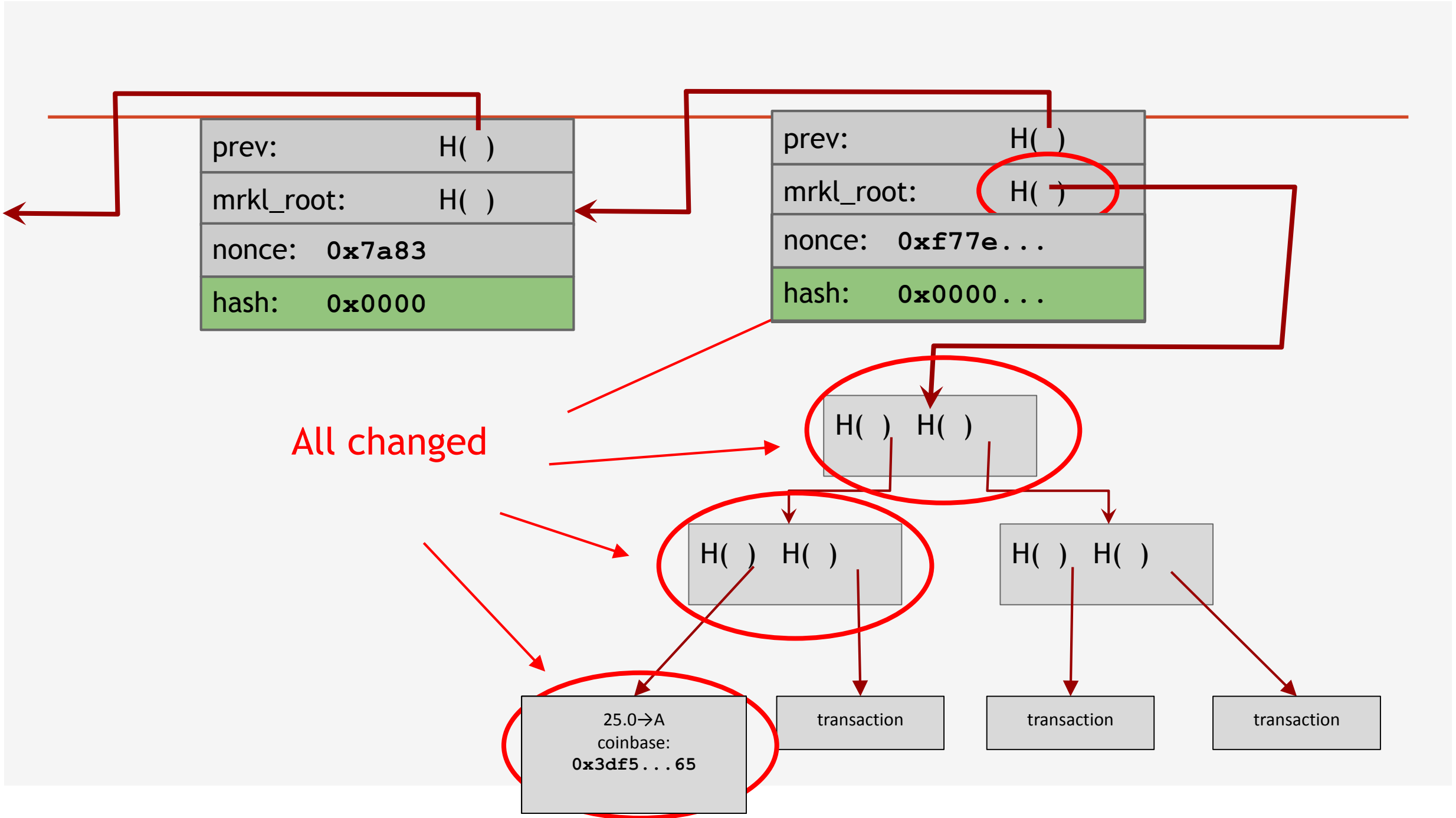
But who are the miners?

The task of Bitcoin miners

Mining Bitcoins in 6 easy steps

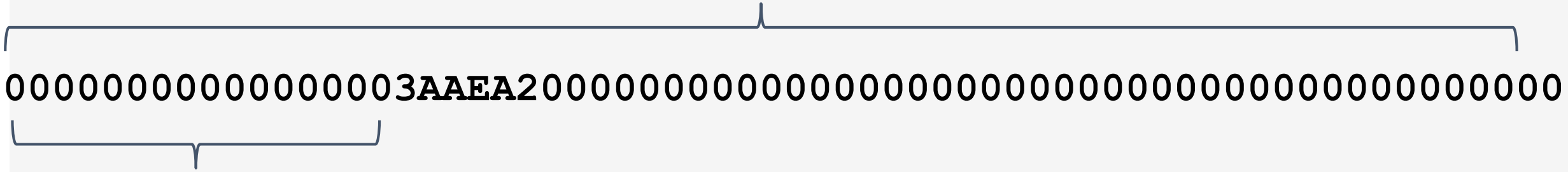
1. Join the network, listen for transactions
    a. Validate all proposed transactions
2. Listen for new blocks, maintain block chain
    a. When a new block is proposed, validate it
3. Assemble a new valid block
4. Find the nonce to make your block valid
5. Hope everybody accepts your new block
6. Profit!

Useful to Bitcoin network


prev: H( )
mrkl_root: H( )
nonce: 0x7a83
hash: 0x0000
prev: H( )
mrkl_root: H( )
nonce: 0xf77e...
hash: 0x0000...
All changed
H( ) H( )
H( ) H( )
H( ) H( )
25.0→A
coinbase:
0x3df5...65
transaction
transaction
transaction

Mining difficulty “target” (2014-08-07)

256 bit hash output



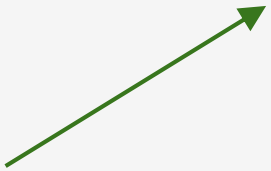
Current difficulty = $2^{66.2}$

=84,758,978,290,086,040,000

Setting the mining difficulty

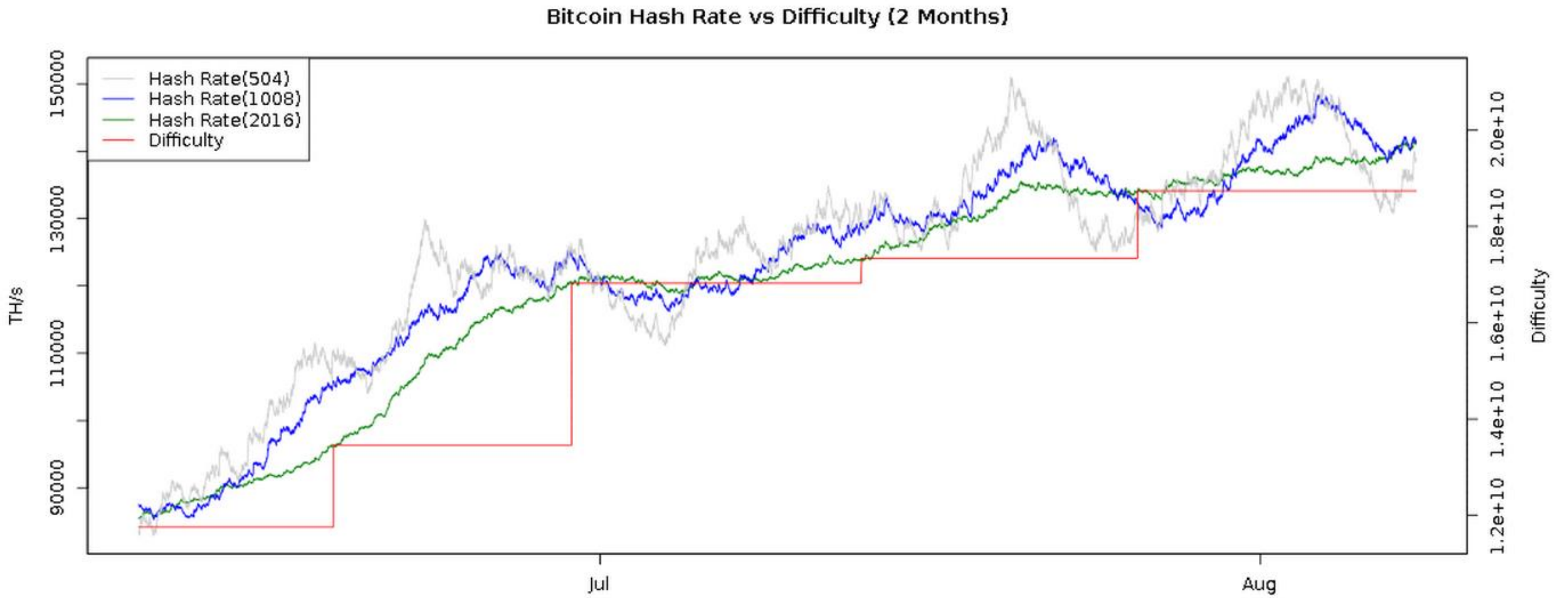
Every two weeks, compute:

```
next_difficulty= previous_difficulty *
                 (2 weeks)/(time to mine last 2016 blocks)
```



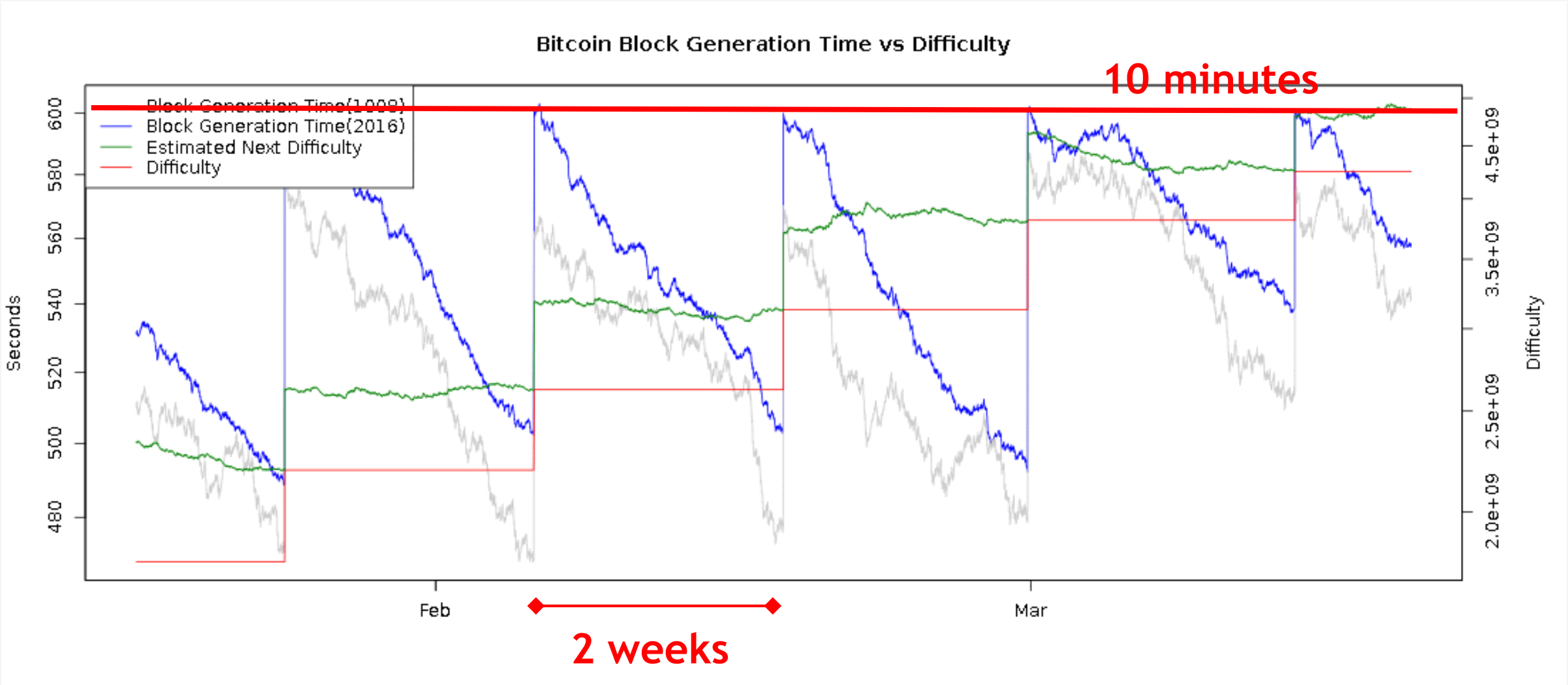
Expected number of blocks in 2 weeks at 10 minutes/block

Mining difficulty over time



bitcoinwisdom.com

Time to find a block



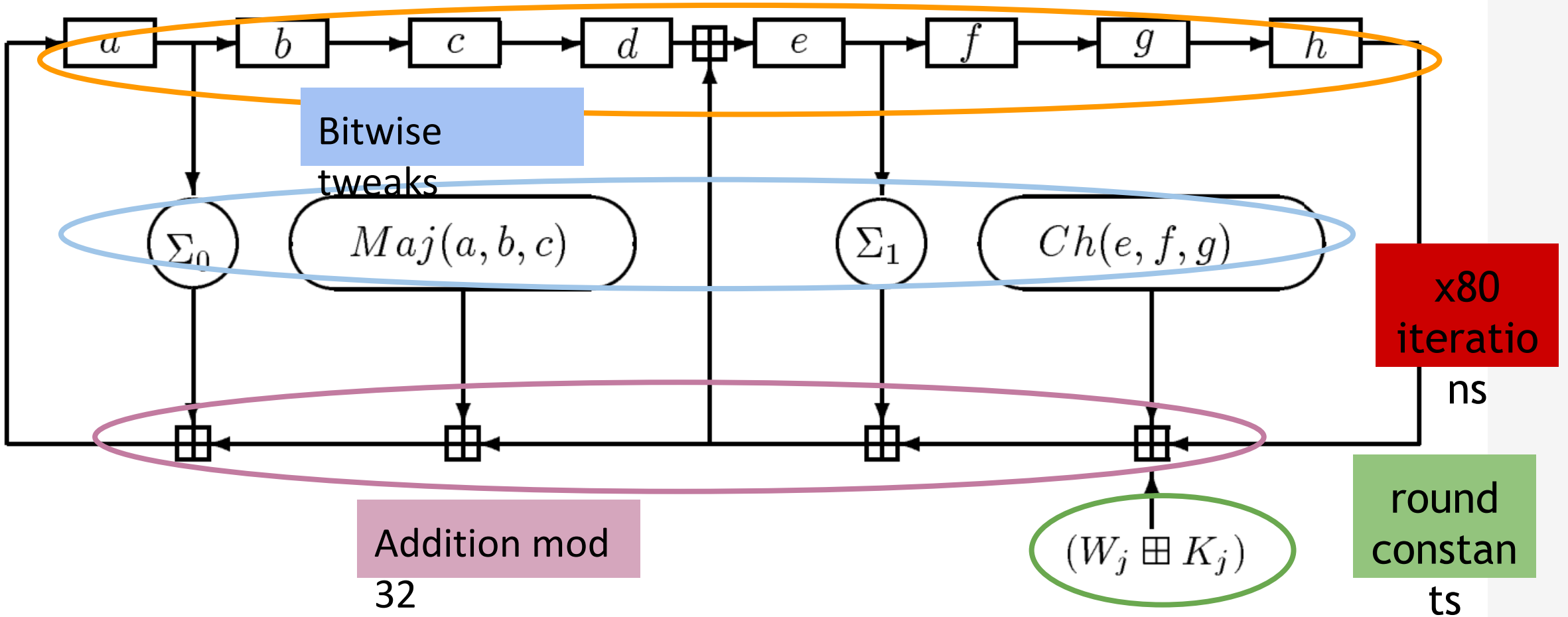
Mining hardware

SHA-256

- General purpose hash function
  - Part of SHA-2 family: SHA-224,SHA-384,SHA-512
- Published in 2001
- Designed by the NSA
- Remains unbroken cryptographically
  - Weaknesses known
- SHA-3 (replacement) under standardization

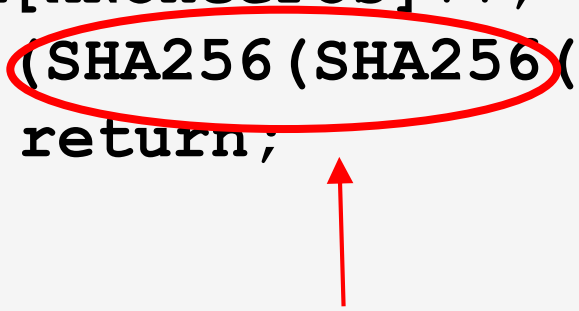
SHA-256 in more depth

256-bit state



CPU mining

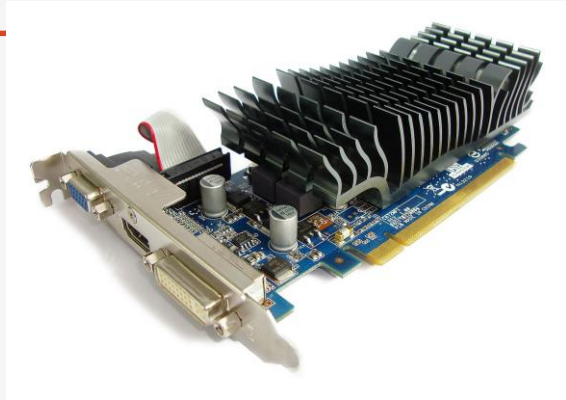
```
while (1){
    HDR[kNoncePos]++;
    IF (SHA256(SHA256(HDR)) < (65535 << 208)/ DIFFICULTY)
        return;
}
```



Throughput on a high-end PC = 10-**20 MHz** ≈ 2^{24}

139,461 years to find a block today!

GPU mining



- GPUs designed for high-performance graphics
  - high parallelism
  - high throughput
- First used for Bitcoin ca. October 2010
- Implemented in OpenCL
  - Later: hacks for specific cards

GPU mining advantages

- easily available, easy to set up
- parallel ALUs
- bit-specific instructions
- can drive many from 1 CPU
- can overclock!

“Goodput”

Observation: *some* errors are okay (may miss a valid block)

Goodput: throughput × success rate

Worth over-clocking by 50% with 30% errors!

Source: LeonardH, cryptocurrencies talk.com

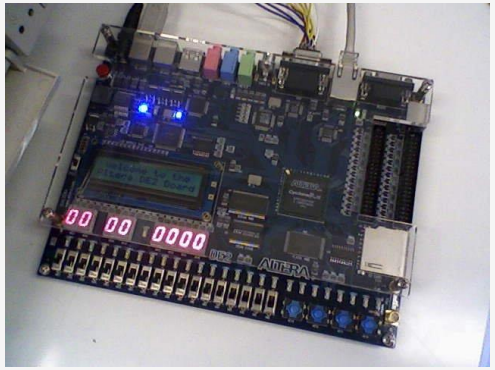
GPU mining disadvantages

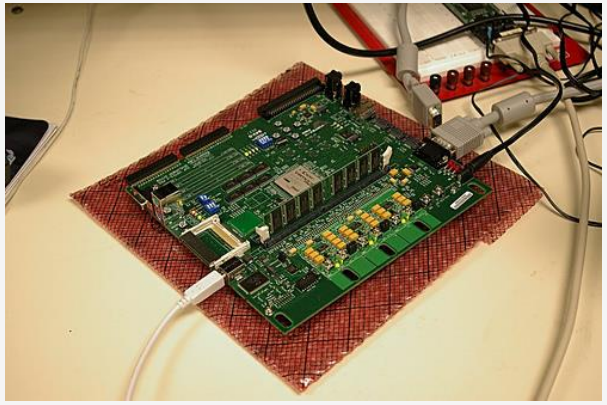
- poor utilization of hardware
- poor cooling
- large power draw
- few boards to hold multiple GPUs

Throughput on a good card = 20-**200 MHz** ≈ 2^{27}

≈**173 years** to find a block w/100 cards!

FPGA mining





- **F**ield **P**rogrammable **G**ate **A**rea
- First used for Bitcoin ca. June 2011
- Implemented in Verilog

FPGA mining advantages

- higher performance than GPUs
  - excellent performance on bitwise operations
- better cooling
- extensive customisation, optimisation

Bob Buskirk, thinkcomputers.org

FPGA mining disadvantages

- higher power draw than GPUs designed for
  - frequent malfunctions, errors
- poor optimization of 32-bit adds
- fewer hobbyists with sufficient expertise
- more expensive than GPUs
- marginal performance/cost advantage over GPUs

Throughput on a good card = 100-**1000 MHz** ≈ 2^{30}

25 years to find a block w/100 boards!

Bitcoin ASICs

TerraMiner™ IV – 2TH/s Networked ASIC Miner

$5,999

Shipping June 2014

300 GH Bitcoin Mining Card

The Monarch BPU 300 C

$1,497.00

Qty: 1 ADD TO CART

Pre-Order Terms: This is a pre-order. 28nm ASIC bitcoin mining hardware products are shipped according to placement in the order queue, and delivery may take 3 months or more after order. All sales are final.

THE LEOPARD

DETAILS :

- **2,5 TH/s**
- Dimensions:
  15“ x 13.3“ x 13.7“
  (38cm x 34cm x 35cm)
- 28nm ASIC technology
- Silent Cooling
- In-built WiFi Connection (without Antenna)
- Less than 750 watt (0.3 per GH)
- 1 Year Guarantee
- $ 5.800

COMES WITH :

1. Power Supply
2. Free Remote Power Outlet & Smartphone App
3. Free User Guide
4. Free Personal Assistance for Setup

SHIPPING :

- Worldwide, Express
- Included in the price
- Available:
  100 Units: Shipping April (Week 3)

Bitcoin ASICs

- special purpose
  - approaching known limits on feature sizes
  - less than 10x performance improvement expected
- designed to be run constantly for life
- require significant expertise, long lead-times
- perhaps the fastest chip development ever!

Case study: TerraMiner IV

- First shipped Jan 2014
- 2 TH/s
- Cost: US$6,000

Still, 14 months to find a block!

Market dynamics (2013/2014)

- Most boards obsolete within 3-6 months
  - Half of profits made in first 6 weeks
- Shipping delays are devastating to customers
- Most companies require pre-orders
- Most individual customers should have lost...

But... rising prices have saved them!

Professional mining centers

Needs:

- cheap power
- good network
- cool climate

BitFury mining center, Republic of Georgia

The future

- Can small miners stay in the game?
- Do ASICs violate the original Bitcoin vision?
- Would we be better off without ASICs?

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

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$15,000**
- Approximately **$25/s** generated
- Industrial electricity (US): **$0.03/MJ**
  - **$0.10/kWh**

Upper bound on electricity consumed:

900 MJ/s = **900 MW**

Estimating energy usage: bottom-up

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

Lower bound on electricity consumed:

150 MW

How much is a MW?

Three Gorges Dam = 10,000 MW
typical hydro plant ≈ 1,000 MW

Kashiwazaki-Kariwa
nuclear power plant = 7,000 MW
typical nuclear plant ≈ 4,000 MW

major coal-fired plant ≈ 2,000 MW

All payment systems require energy

Data furnaces

- **Observation:** in the limit, computing devices produce heat almost as well as electric heaters!
- Why not install mining rigs as home heaters?
- Challenges:
  - Ownership/maintenance model
  - Gas heaters still at least 10x more efficient
  - What happens in summer?

Open questions

- Will Bitcoin drive out electricity subsidies?
- Will Bitcoin require guarding power outlets?
- Can we make a currency with no proof-of-work?

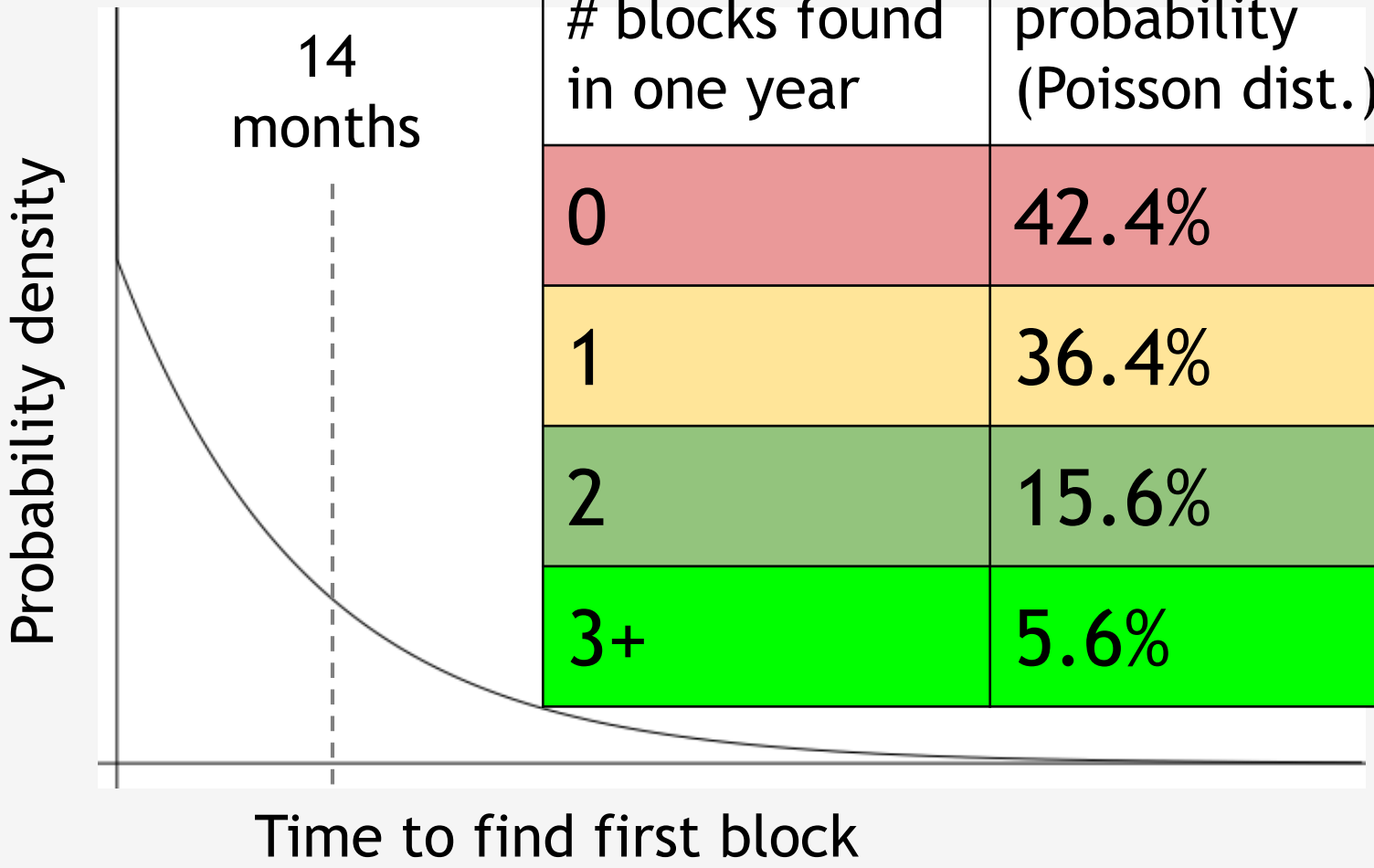
Mining pools

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
009048813377 9E7E98177AF1C765CF02D01AB4848DF555533B6C4CFCA201CBA1
460BEFA43B7083E502D36D9D08D64AFB99A100B3B80D4EA4F7B38E18174A0BFB
000000000000000078FB7E1F7E2E4854B8BC71412197EB1448911FA77BAE808A
652F374601D149AC47E01E777613845 6181FA4F9D0EEDD8C4FDE3BEF6B1B7ECE
785526402143A291CFD60DA09CC80DD066BC723FD5FD20F9B50D614313529AF3
000000000041EE593434686000AF77F54CDE839A6CE30957B14EDEC10B15C9E5
9C20B06B01A0136F192BD48E0F372A4B9E6BA6ABC36F02FCED22FD9780026A8F
```

Mining pools

Hey folks! Here's our next block to work on

Pool manager

prev: H( )
mrkl_root: H( )
nonce:
hash:

coinbase:
25→pool

$$$

$

$$

0x00000000000a87790
2e...

0x00000000001e8709
ce...

0x00000000000490c6b
00...

0x0000000000007313f
89...

**0x0000000000000003
f89**
4...

0x00000000000045a161
1f...

Mining pool variations

- **Pay per share:** flat reward per share
  - Typically minus a significant fee
  - What if miners never send in valid blocks?
- **Proportional:** typically since last block
  - Lower risk for pool manager
  - More work to verify
- **“Luke-jr” approach:** no management fee
  - Miners can only get paid out in whole BTC
  - Pool owner keeps spread

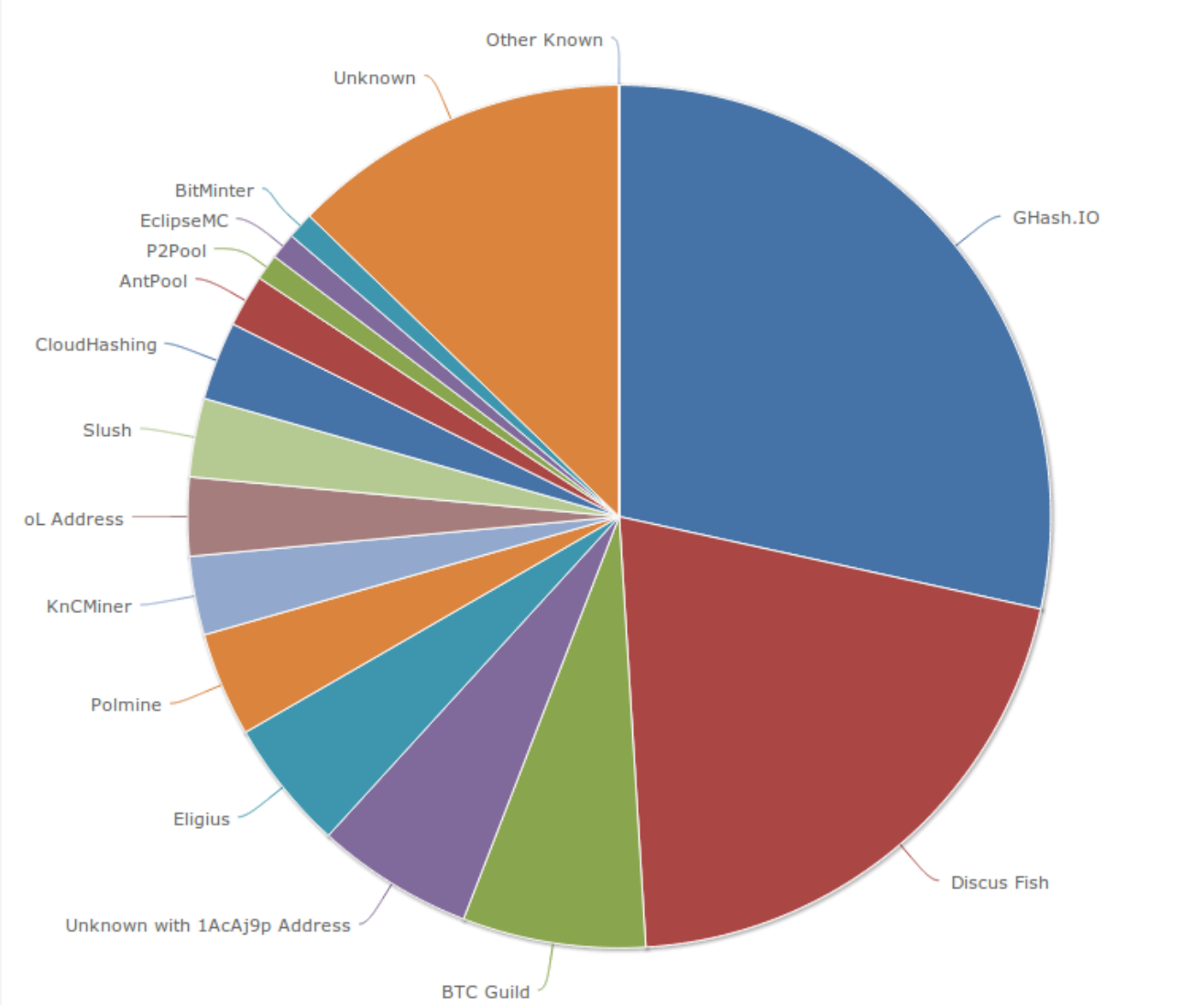
Mining pool protocols

- API for fetching blocks, submitting shares
  - Stratum
  - Getwork
  - Getblockshare
- Proposed for standardization with a BIP
- 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 (as of 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

Can we prevent pools?

Stay tuned for our lecture on alt-mining!

Mining incentives and strategies

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

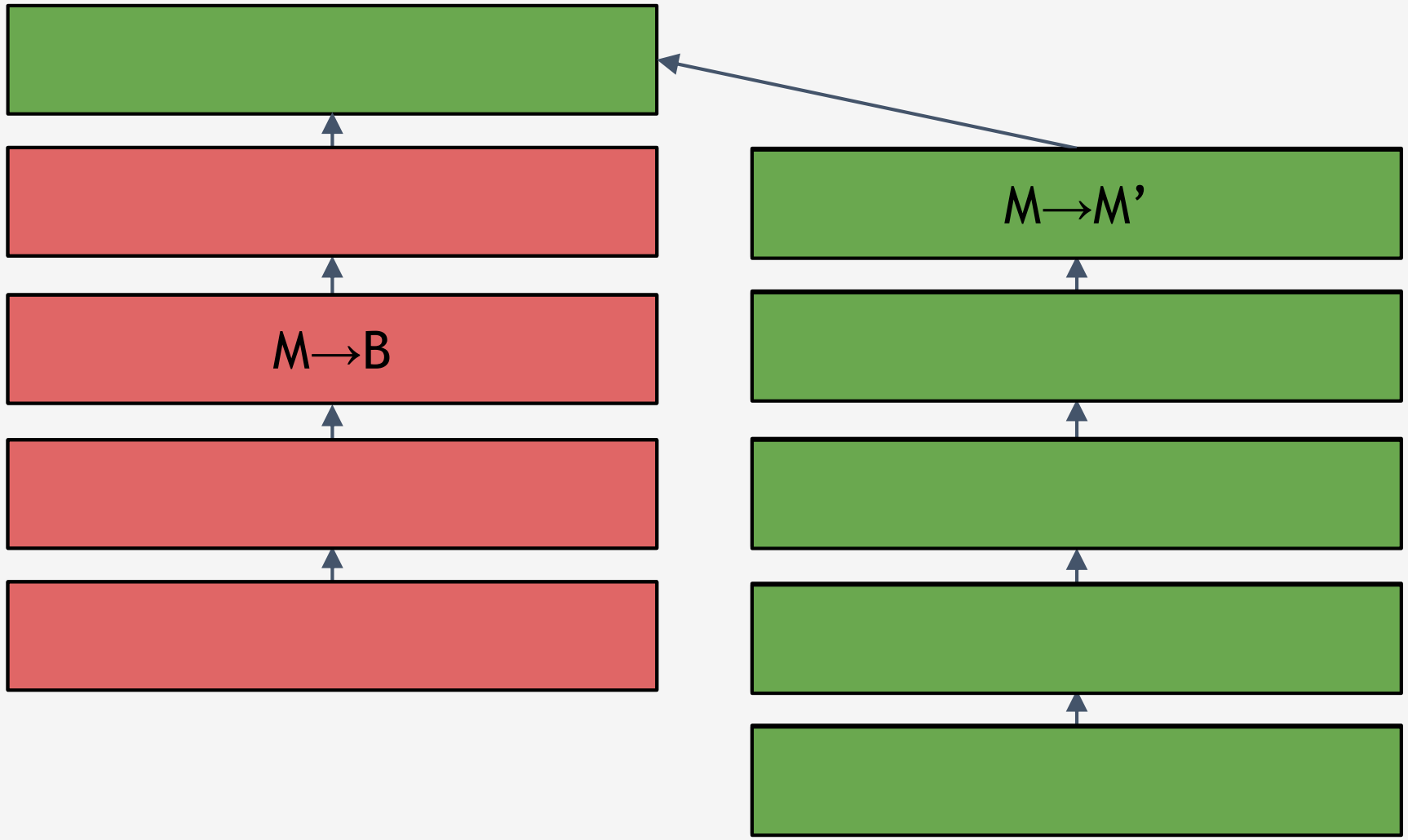
Game-theoretic analysis of mining

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

Goldfinger Attack?

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!

Checkpointing

satoshi
Founder
Sr. Member

Activity: 364

Bitcoin 0.3.2 released
July 17, 2010, 09:35:51 PM

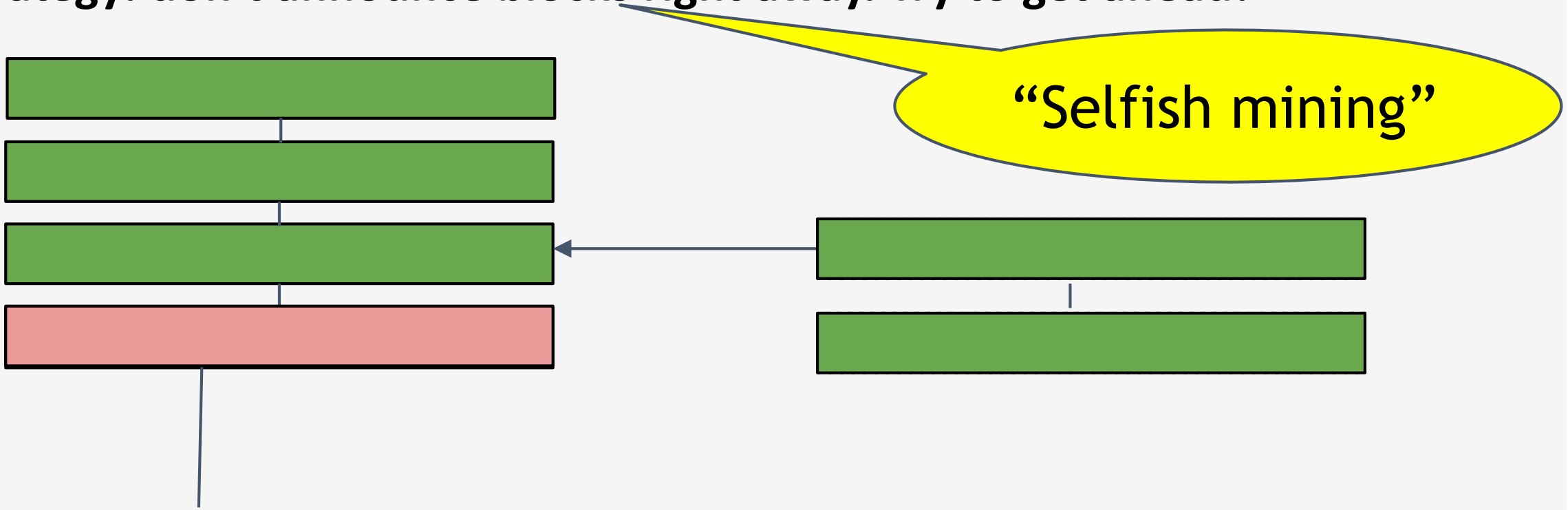
Download links available now on bitcoin.org. Everyone should upgrade to this version.

- Added a simple security safeguard that locks-in the block chain up to this point.
- Reduced addr messages to save bandwidth now that there are plenty of nodes to connect to.
- Spanish translation by milkiway.
- French translation by aidos.

Default clients ship with built-in checkpoint

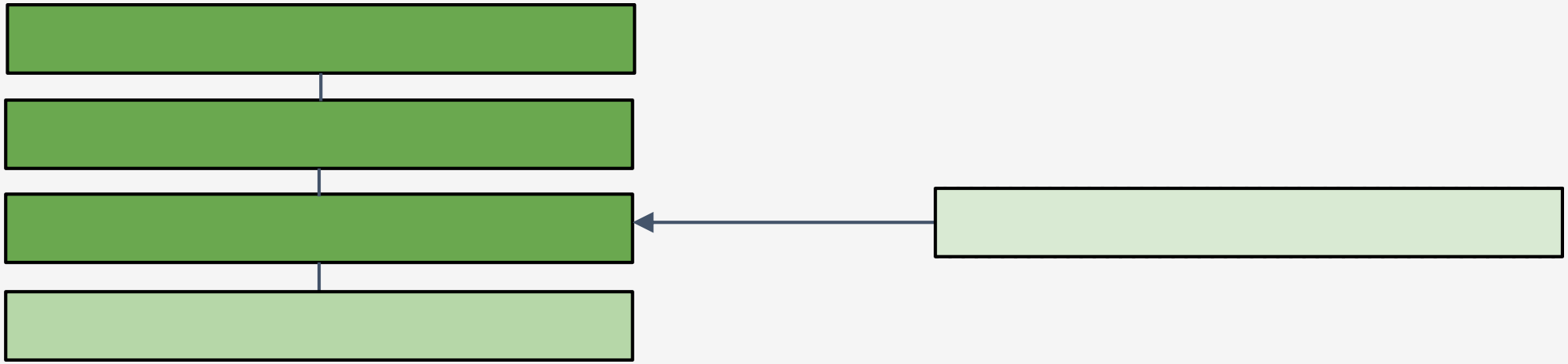
Block-withholding attacks

Strategy: don't announce blocks right away. Try to get ahead!



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

Punitive forking

- Suppose you want to blacklist transactions from address *X*
  - Freeze an individual's money forever
- **Extreme strategy:** announce that you will refuse to mine on any chain with a transaction from *X*

With $\alpha < 0.5$, you'll soon fall behind the network

Feather-forking strategy

- **To blacklist transactions from X,** announce that you will refuse to mine *directly* on any block with a transaction from *X*
  - but you'll concede after *n* confirming blocks

- Chance of pruning an offending block is $\boldsymbol{\alpha^2}$

Response to feather forking

- **For other miners,** including a transaction from *X* induces an α^2 chance of losing a block
- Might be safer to join in on the blacklist
- Can enforce a blacklist with $\alpha < 0.5$**!**

Success depends on convincing other miners you'll fork

Feather-forking: what is it good for?

- Freezing individual bitcoin owners
  - ransom/extortion
  - law enforcement?
- Enforcing a minimum transaction fee...

A second look at transaction fees

Default policy:

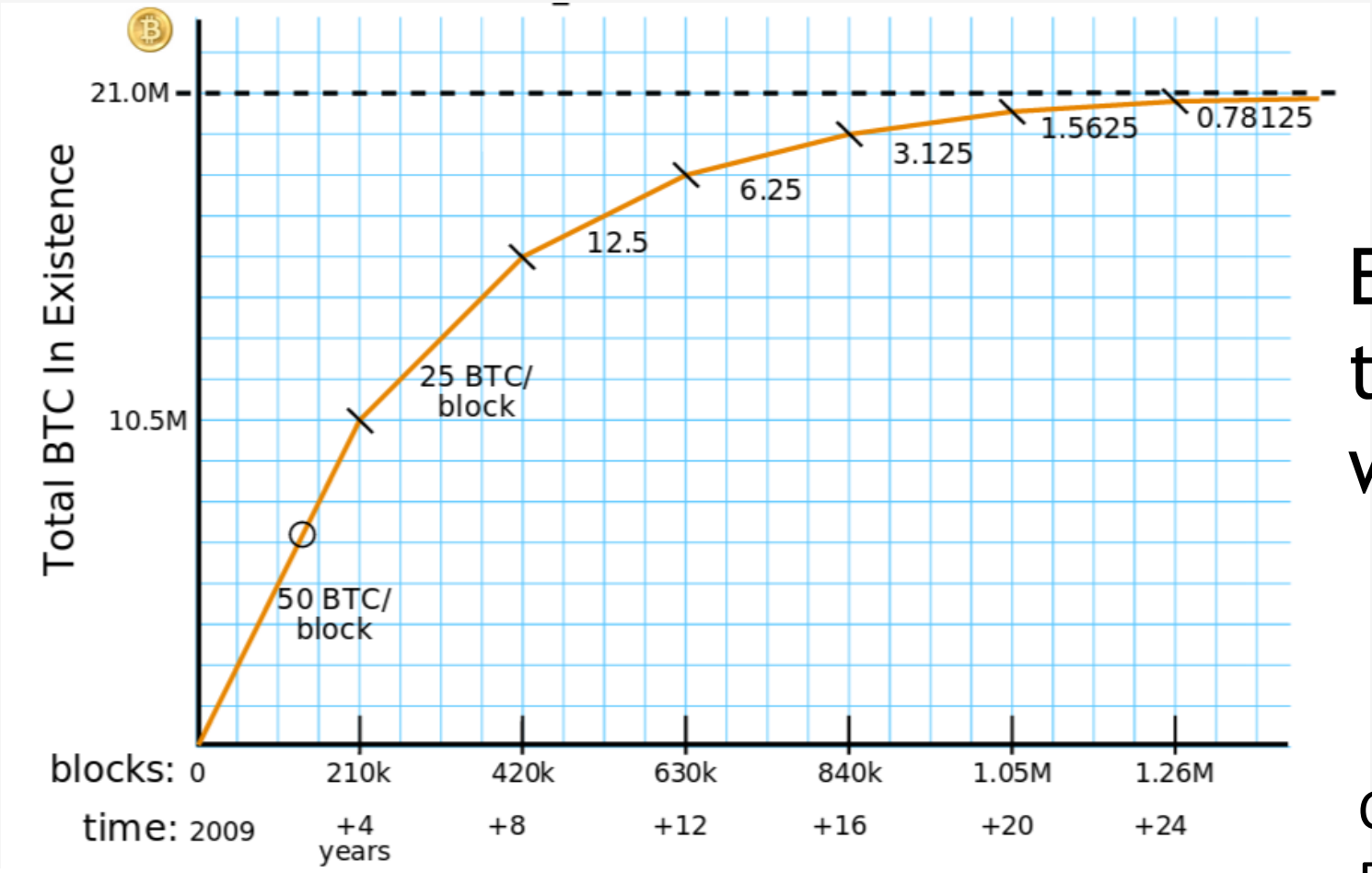
```
priority = sum(input_value * input_age)/size_in_bytes
```

Accept without fees if:

```
priority > 0.576
```

Transaction fees will matter more

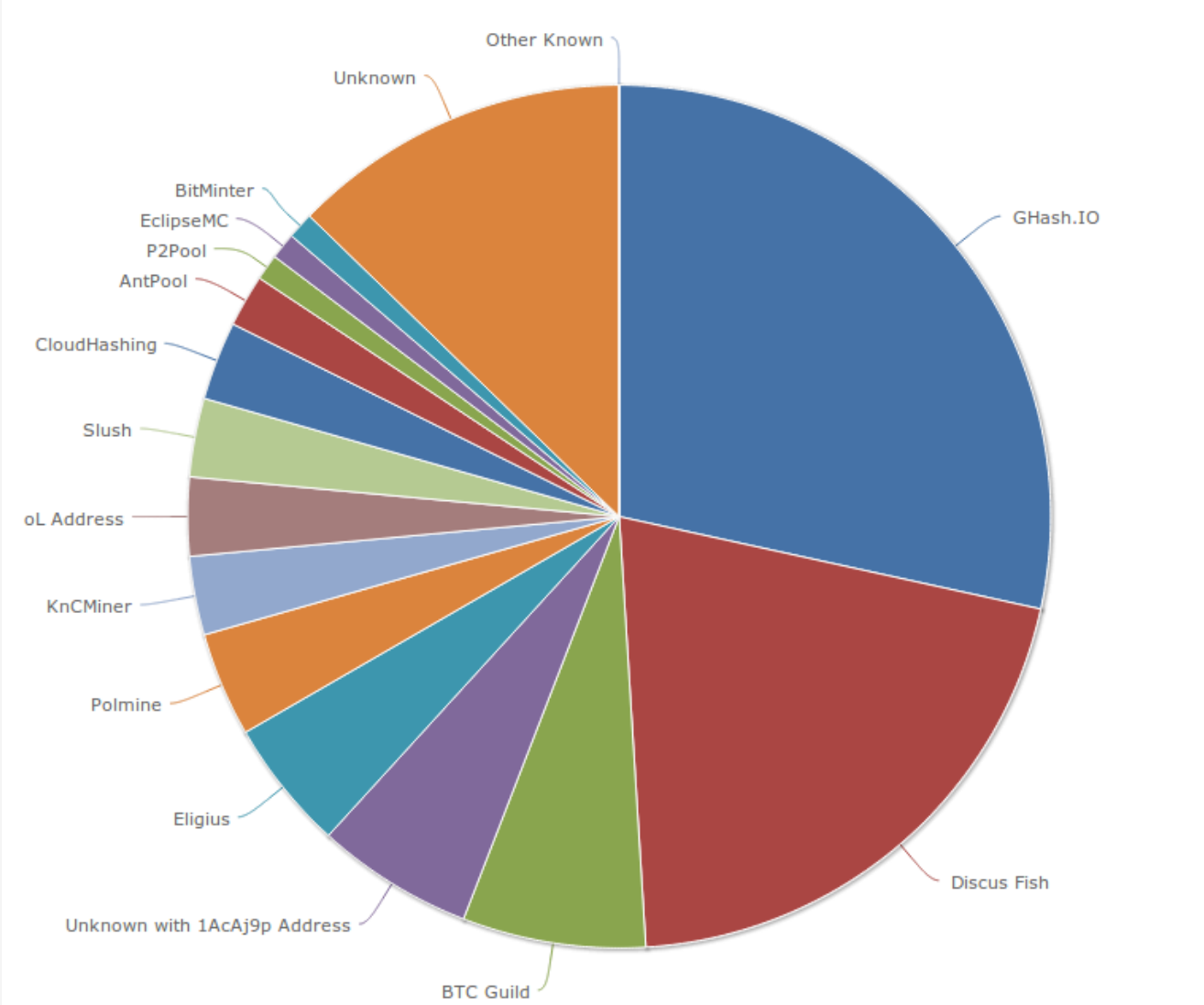
Currently, block rewards are > 99% of miner revenue. But:



Eventually, transaction fees will dominate

Courtesy:
Brian Warner

Will miners cooperate to enforce fees?



Bribery attacks

- Start a new mining pool paying 25+ε
  - Guarantee payment instead of dividing up wins
  - Mutual trust issues
- Pay miners directly
  - Potentially cheaper
  - Trust/information issues
- Kickbacks
  - Solve some trust issues
  - Complicated technically

Summary

- Miners are free to implement any strategy
- Very little non-default behavior in the wild
- No complete game-theoretic model exists

Things might be about to get interesting…