Blockchain
区块链

2018.03.20

比特币挖矿

北京大学 软件与微电子学院
School of Software and Microelectronics, Peking University

Huiping Sun(孙惠平)
sunhp@ss.pku.edu.cn

课堂测试时间

课堂测试03

- 1、比特币是如何解决双重支付的问题的?
- 2、比特币的数据上限是多少？这个数据上限是如何计算出来的？如何扩大这个上限?
- 3、比特币挖矿设备是如何演化的?
- 4、比特币的工作量证明有什么用？是通过什么方式进行工作量证明的?
- 5、如何攻击比特币，简单描述可能的攻击方法?
- 6、谈谈你对智能合约的理解和看法，智能合约有哪些优点和缺点?

上次课程内容回顾

- 交易
- 脚本
- 区块
- 网络
- 限制
- 存储

- 比特币交易、合并、联合支付
- 比特币脚本、多重签名、P2SH、托管、绿色地址、小额多次交易、锁定时间
- 区块结构、币基础交易
- 比特币网络、加入、交易信息传播、存储花费
- 时间限制、块限制、激励限制、频率限制、分叉
- 冷热存储、威胁、交易所

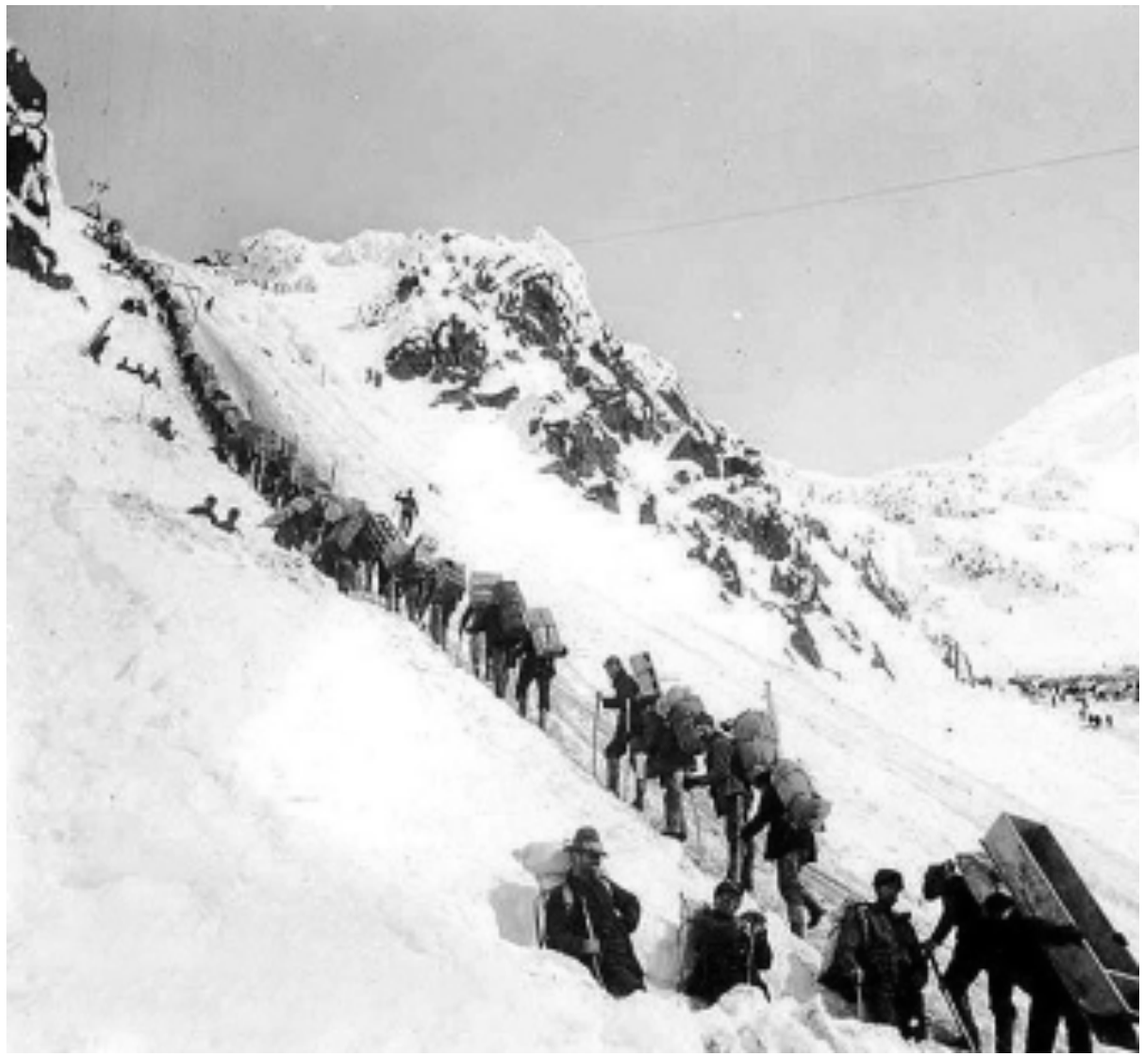
课程项目选题

报告内容和问题收集

矿工任务

矿工

- 比特币需要矿工
  - ✴ 存储和广播区块
  - ✴ 验证交易有效性
  - ✴ 对区块进行共识投票



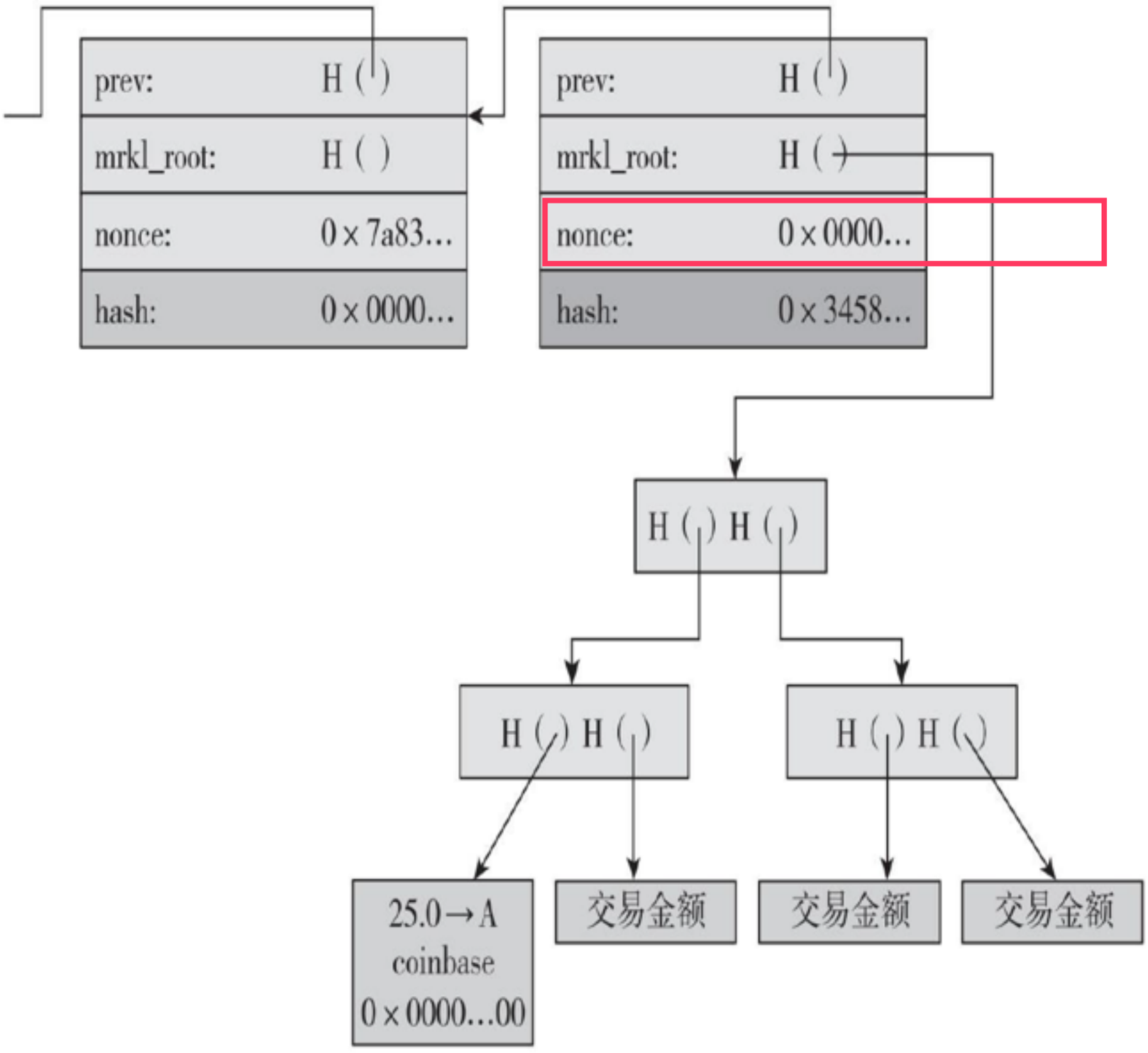
但为什么成为一个矿工！

矿工的任务

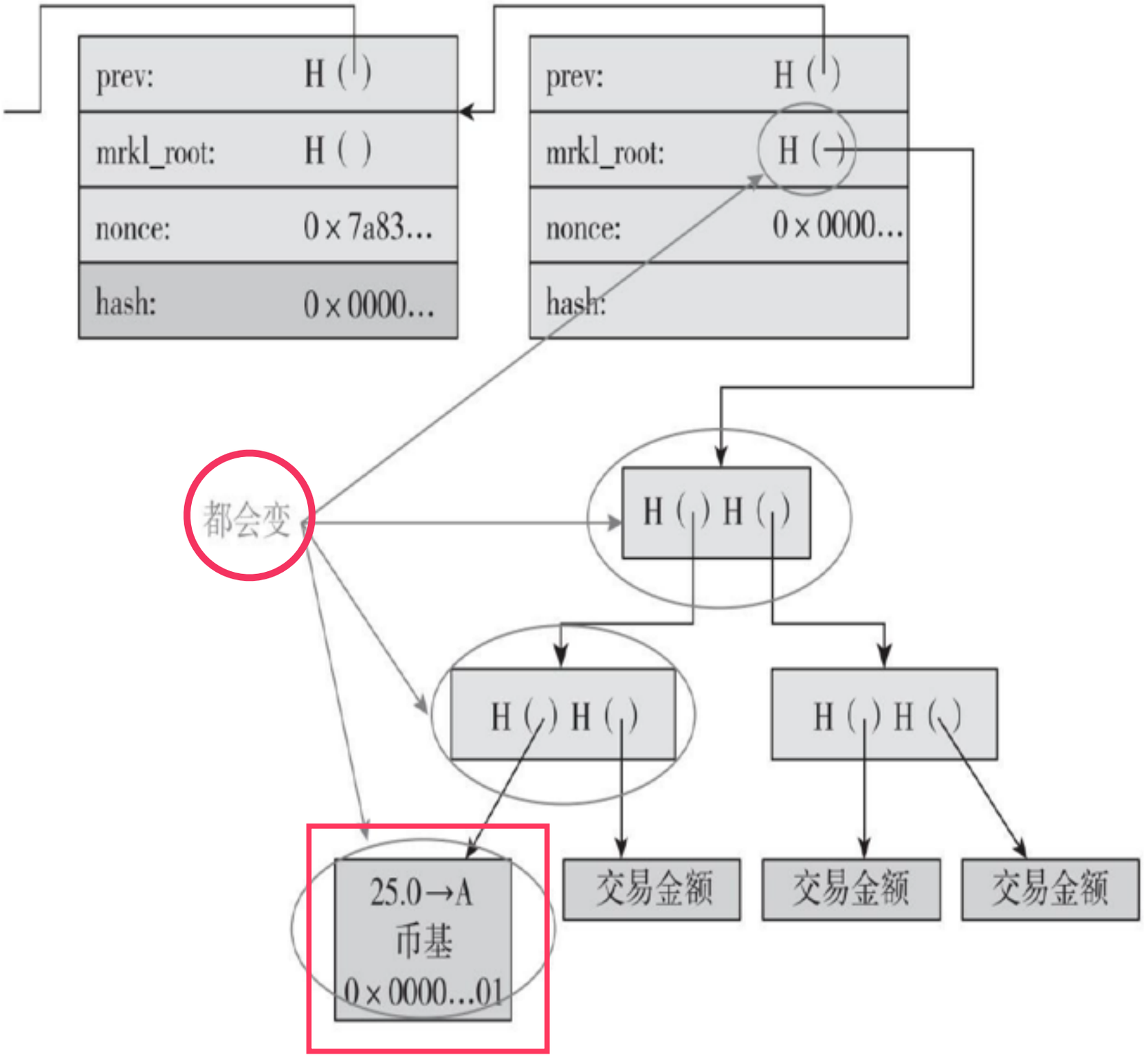
- 监听交易广播
- 维护区块链网络和监听新的区块
- 组装一个备选区块
- 找到一个让你的区块有效的随机数
- 希望你的区块被全网接受
- 利润

验证交易和区块 vs. 和其余矿工竞争

寻找有效区块

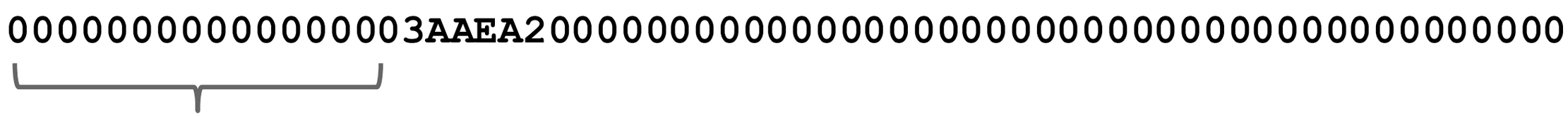

prev: H ( )
mrkl_root: H ( )
nonce: 0 x 7a83…
hash: 0 x 0000…
prev: H ( )
mrkl_root: H ( )
nonce: 0 x 0000…
hash: 0 x 3458…
H ( ) H ( )
H ( ) H ( )
H ( ) H ( )
25.0→A
coinbase
0 x 0000…00
交易金额
交易金额
交易金额

改变临时随机数


prev:
H ( )
mrkl_root:
H ( )
nonce:
0 x 7a83…
hash:
0 x 0000…
prev:
H ( )
mrkl_root:
H ( )
nonce:
0 x 0000…
hash:
都会变
H ( ) H ( )
H ( ) H ( )
H ( ) H ( )
25.0→A
币基
0 x 0000…01
交易金额
交易金额
交易金额

挖矿难度

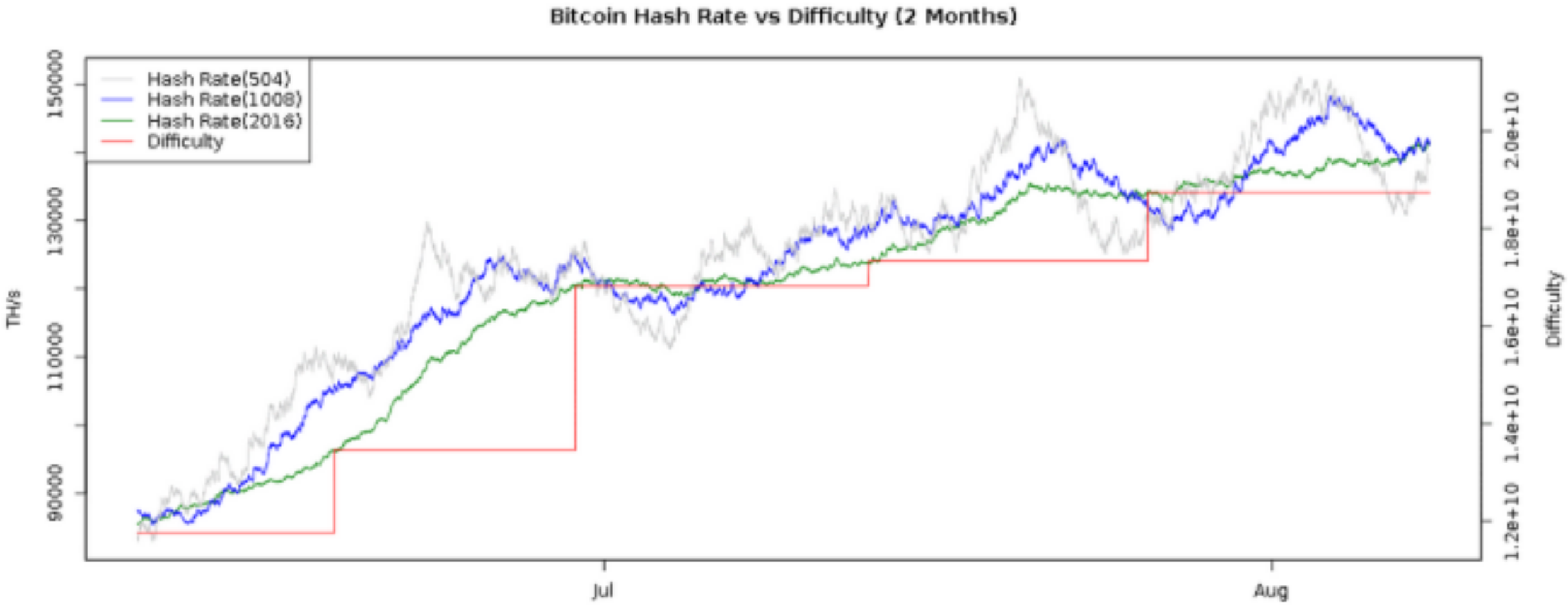
256 bit hash output



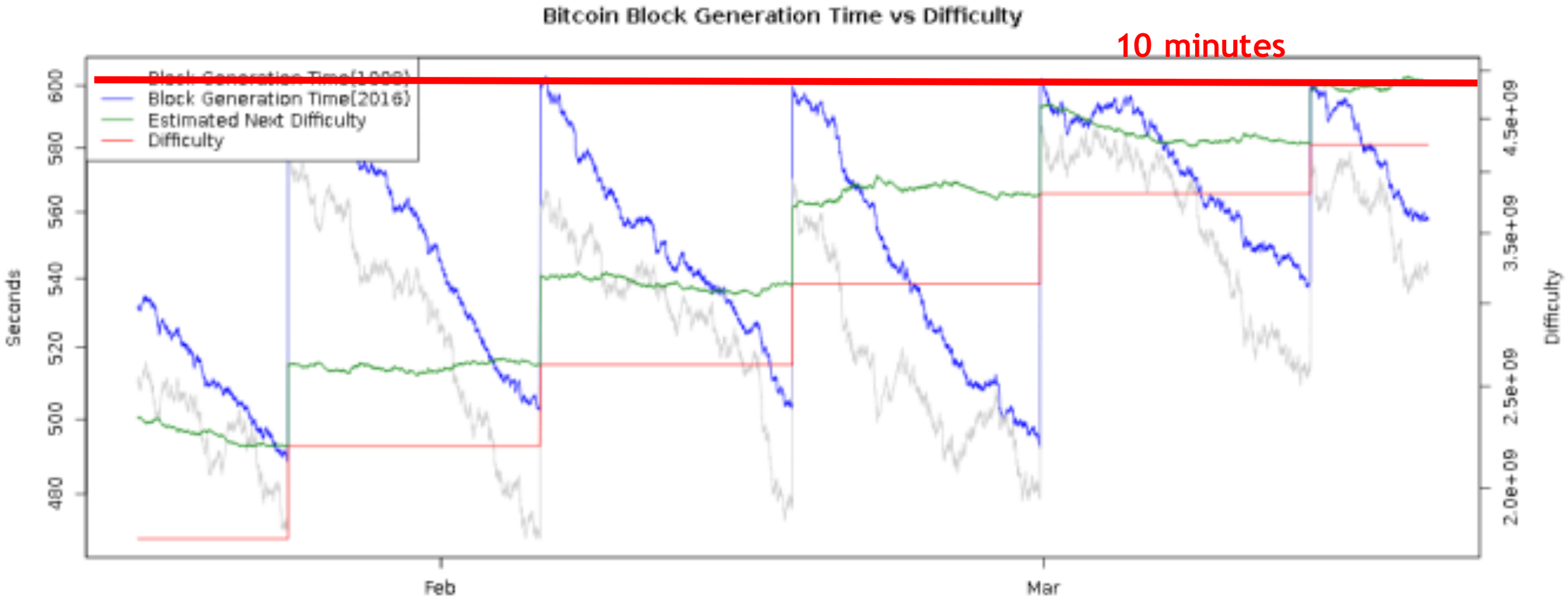
Current difficulty = $2^{66.2}$

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

难度随时间变化


Bitcoin Hash Rate vs Difficulty (2 Months)
Hash Rate(504)
Hash Rate(1008)
Hash Rate(2016)
Difficulty
TH/s
150000
130000
110000
90000
Difficulty
2.0e+10
1.8e+10
1.6e+10
1.4e+10
1.2e+10
Jul
Aug

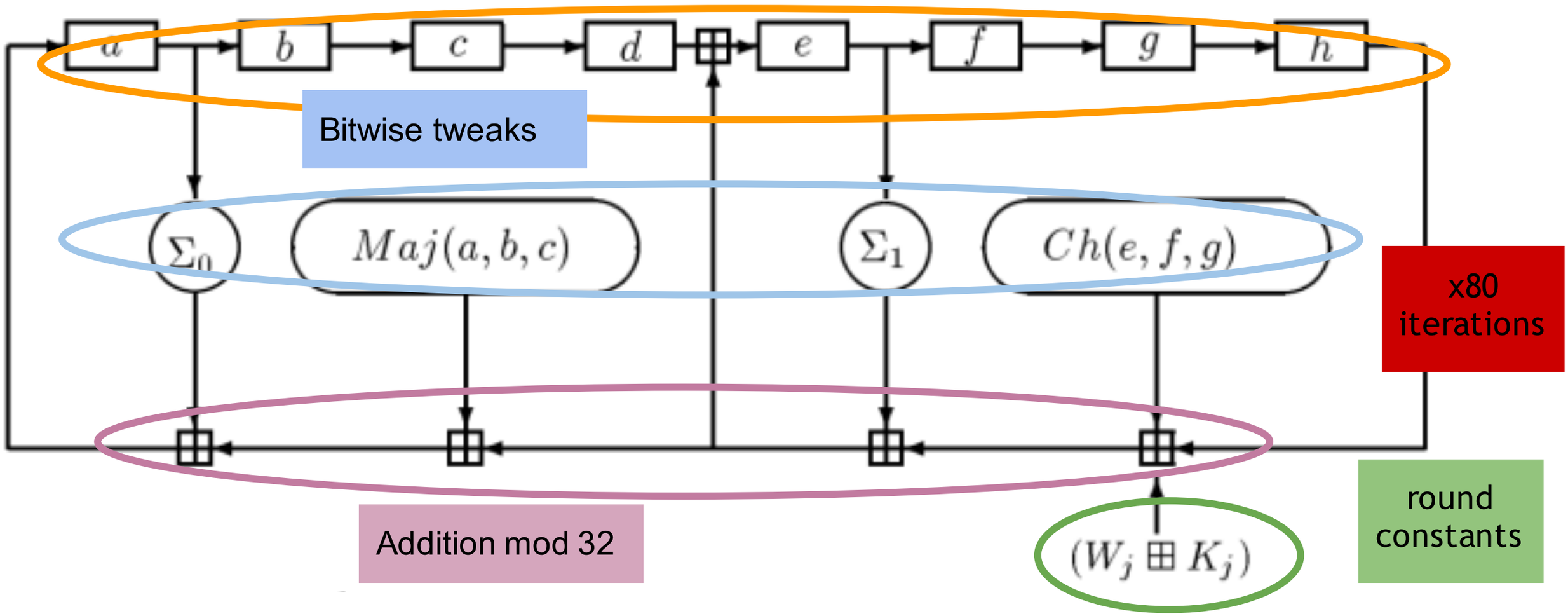
发现一个有效区块的时间



挖矿硬件

SHA256

256-bit state



CPU挖矿

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

two hashes

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

139,461 years to find a block today!

GPU挖矿

OpenCL

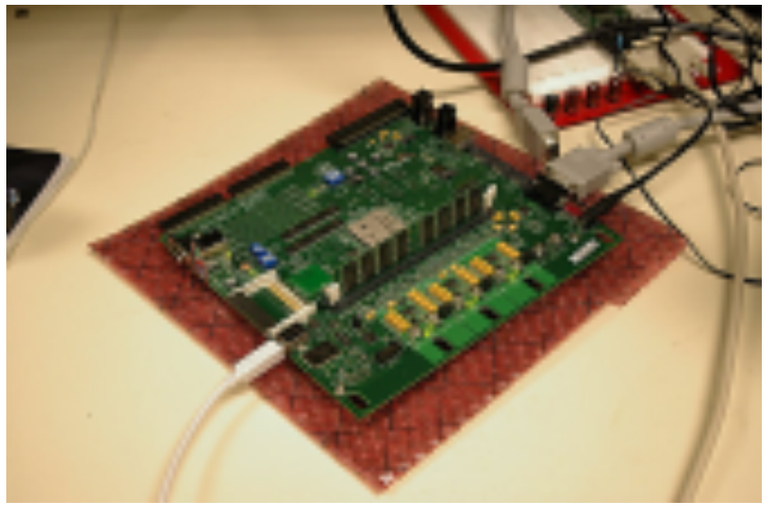
2010

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

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

FPGA挖矿

Field **P**rogrammable **G**ate **A**rea 2011



Throughput on a good card = 100-**1000 MHz** ≈

2^{30} **25 years** to find a block w/100 boards!

ASIC挖矿

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.

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

Still, **14 months** to find a block!

矿场

Bitcoin Mining

挖矿发展

CPU

GPU

FPGA

ASIC

gold pan

sluice box

placer mining

pit mining

矿池

为什么需要矿池

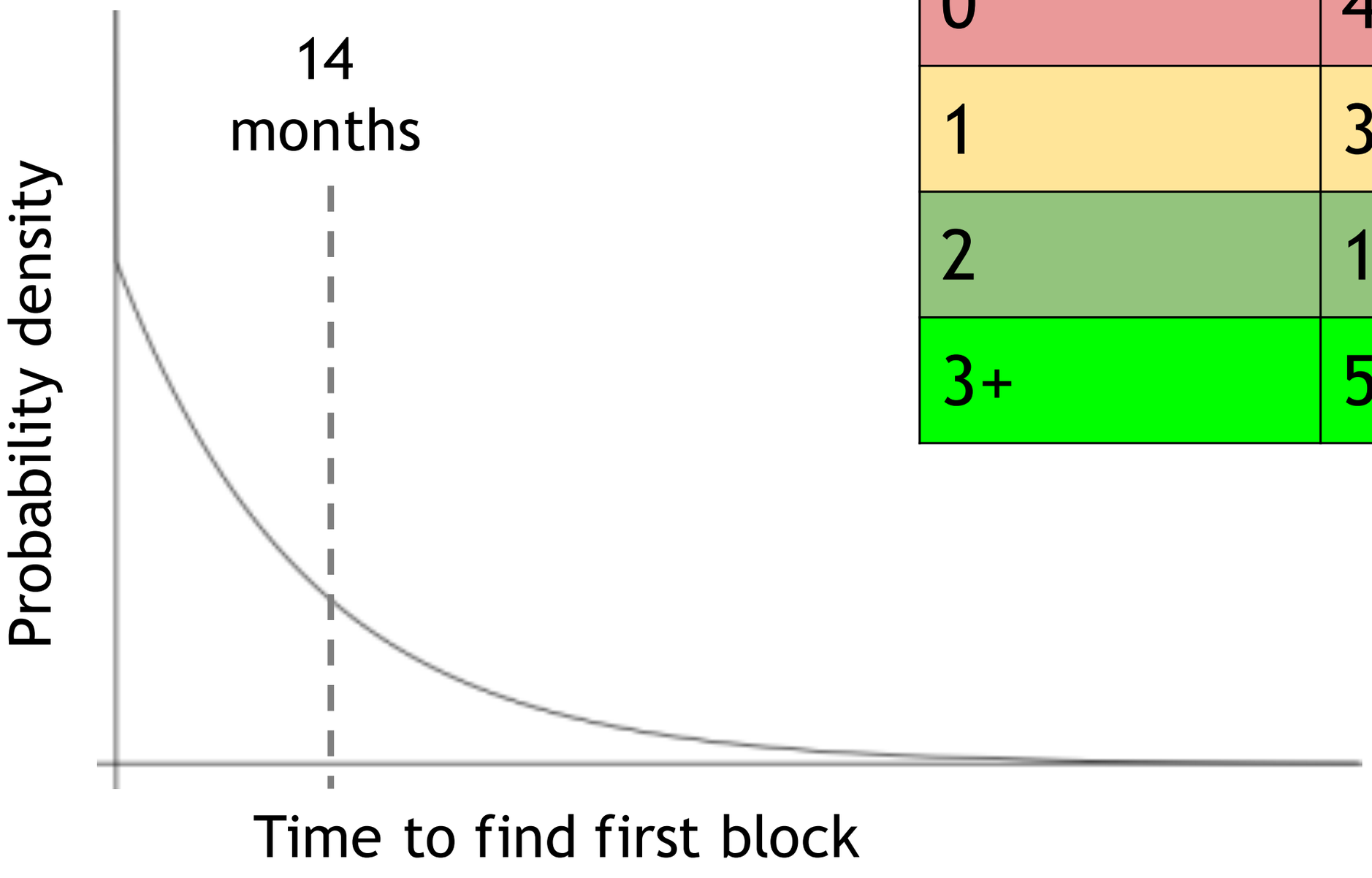
TerraMiner IV

Cost: ≈US$6,000

Expected time to find a block: ≈14 months

Expected revenue: ≈$1,000/month

挖矿不确定性



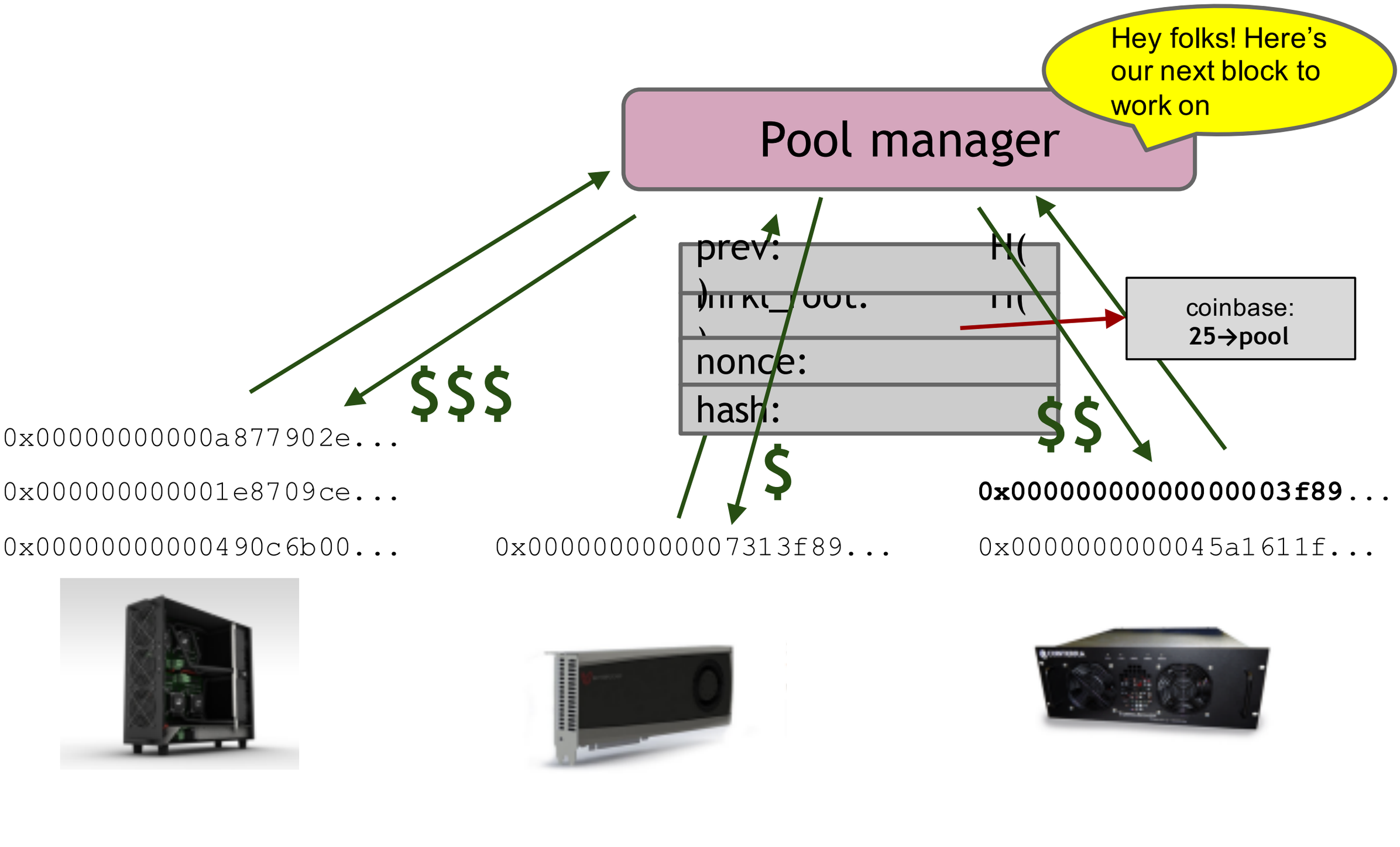
# blocks found in one year	probability (Poisson dist.)
0	42.4%
1	36.4%
2	15.6%
3+	5.6%

挖矿互助

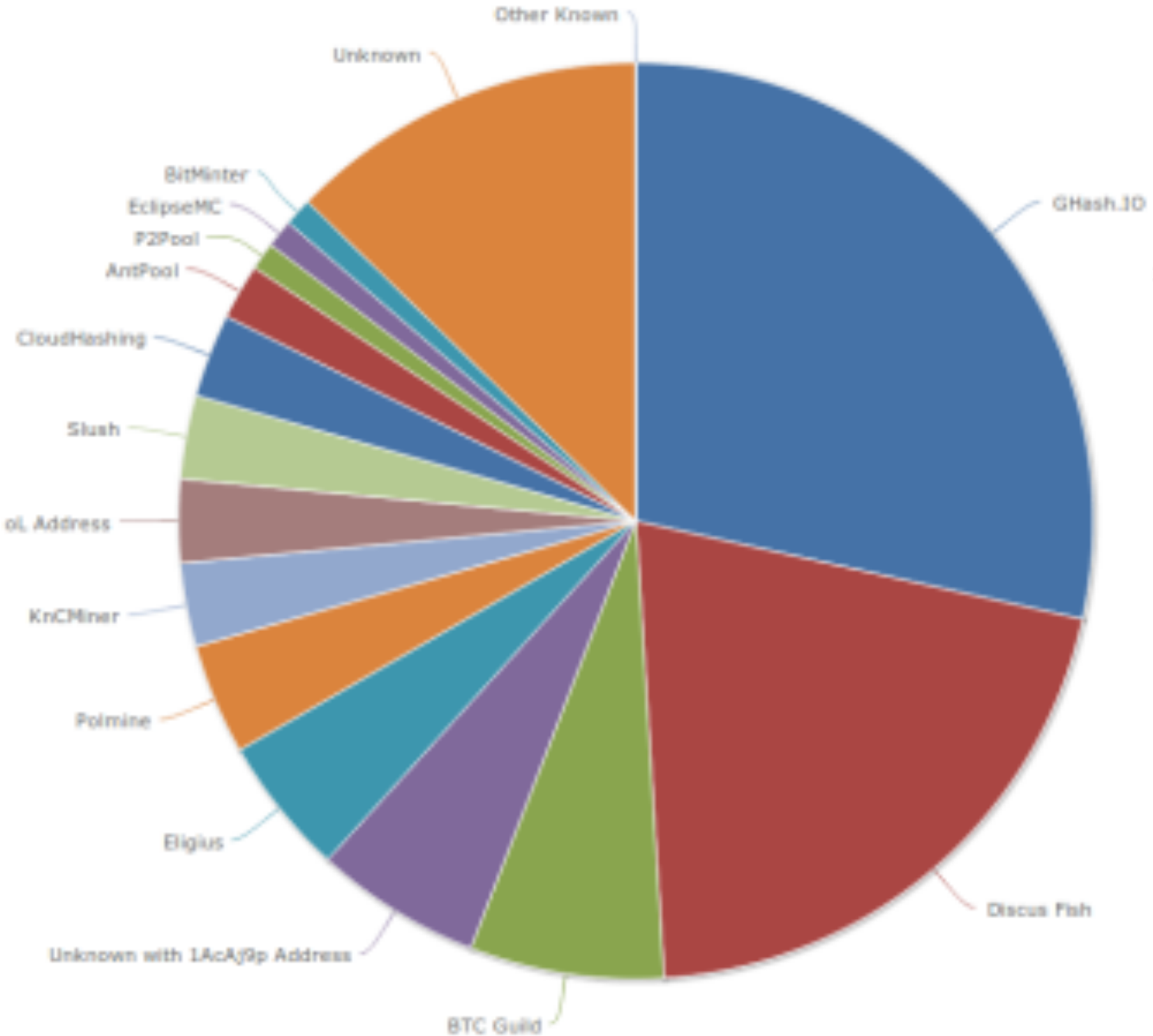
Idea: prove work with “near-valid blocks” (shares)

```
4AA087F0A52ED2093FA816E53B9B6317F9B8C1227A61F9481AFED67301F2E3FB
D3E51477DCAB108750A5BC9093F6510759CC880BB171A5B77FB4A34ACA27DEDD
00000000008534FF68B98935D090DF5669E3403BD16F1CDFD41CF17D6B474255
BB34ECA3DBB52EFF4B104EBBC0974841EF2F3A59EBBC4474A12F9F595EB81F4B
00000000002F891C1E232F687E41515637F7699EA0F462C2564233FE082BB0AF
009048813379E7E98177AF1C765CF02D01AB4848DF555533B6C4CFCA201CBA1
460BEFA43B7083E502D36D9D08D64AFB99A100B3B80D4EA4F7B38E18174A0BFB
00000000000000078FB7E1F7E2E4854B8BC71412197EB1448911FA77BAE808A
652F374601D149AC47E01E7761384561 81FA4F9D0EEDD8C4FDE3BEF6B1B7ECE
785526402143A291CFD60DA09CC80DD066BC723FD5FD20F9B50D614313529AF3
00000000041EE593434686000AF77F54CDE839A6CE30957B14EDEC10B15C9E5
9C20B06B01A0136F192BD48E0F372A4B9E6BA6ABC36F02FCED22FD9780026A8F
```

矿池模式


Hey folks! Here's our next block to work on
Pool manager
prev:
H(
)
mrkl_root:
H(
)
nonce:
hash:
coinbase:
25→pool
$$$
$
$$
0x00000000000a877902e...
0x000000000001e8709ce...
0x0000000000490c6b00...
0x0000000000007313f89...
0x0000000000000003f89...
0x0000000000045a1611f...

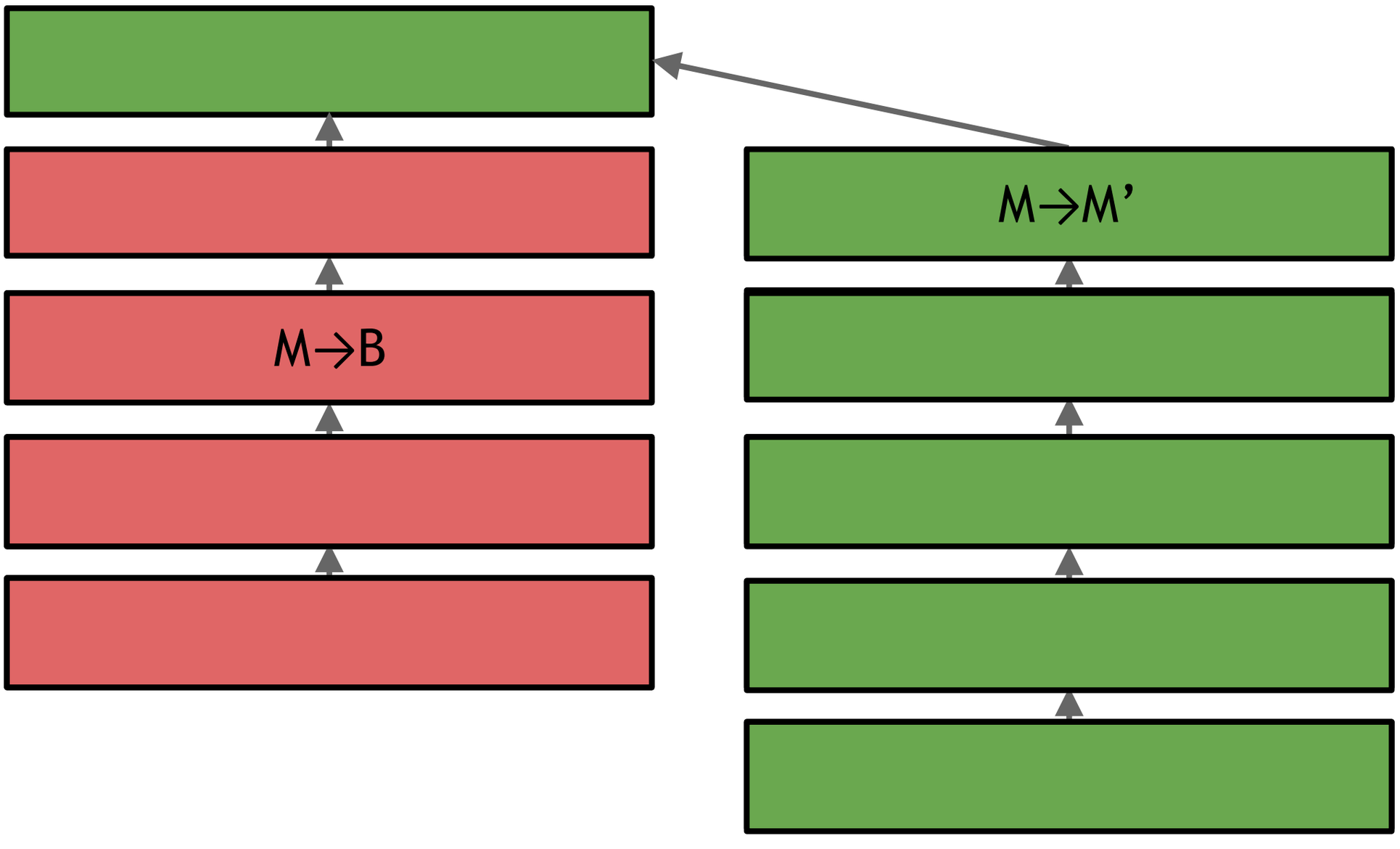
矿池算力



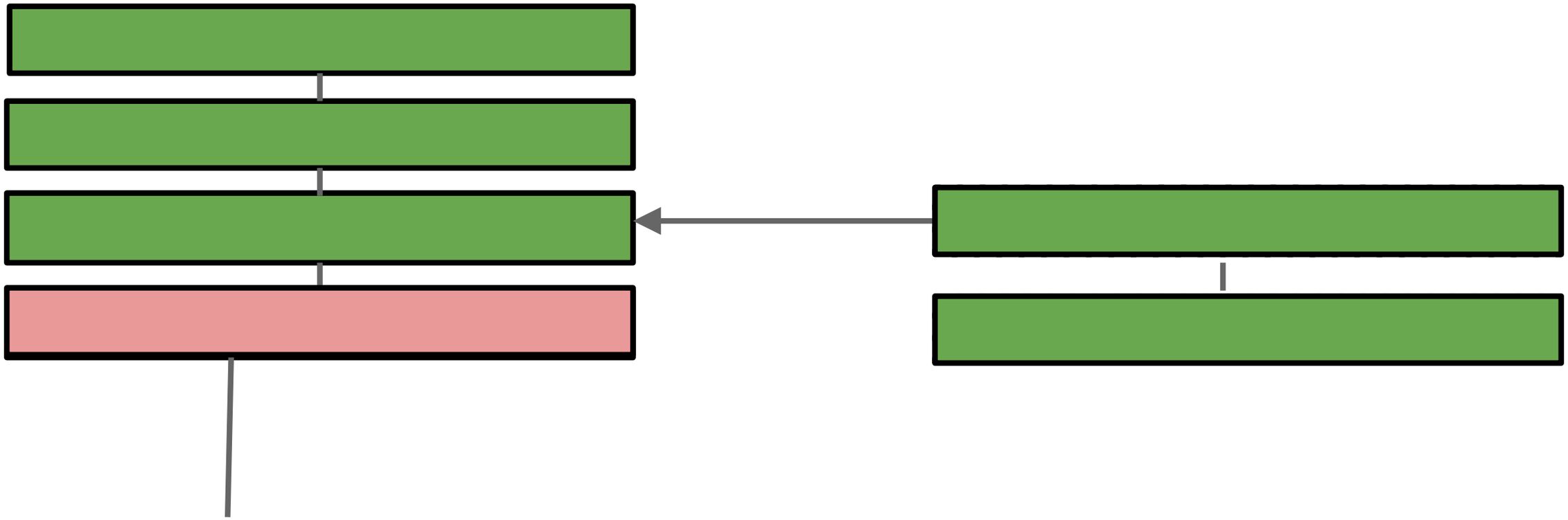
GHash.IO

策略

分叉攻击

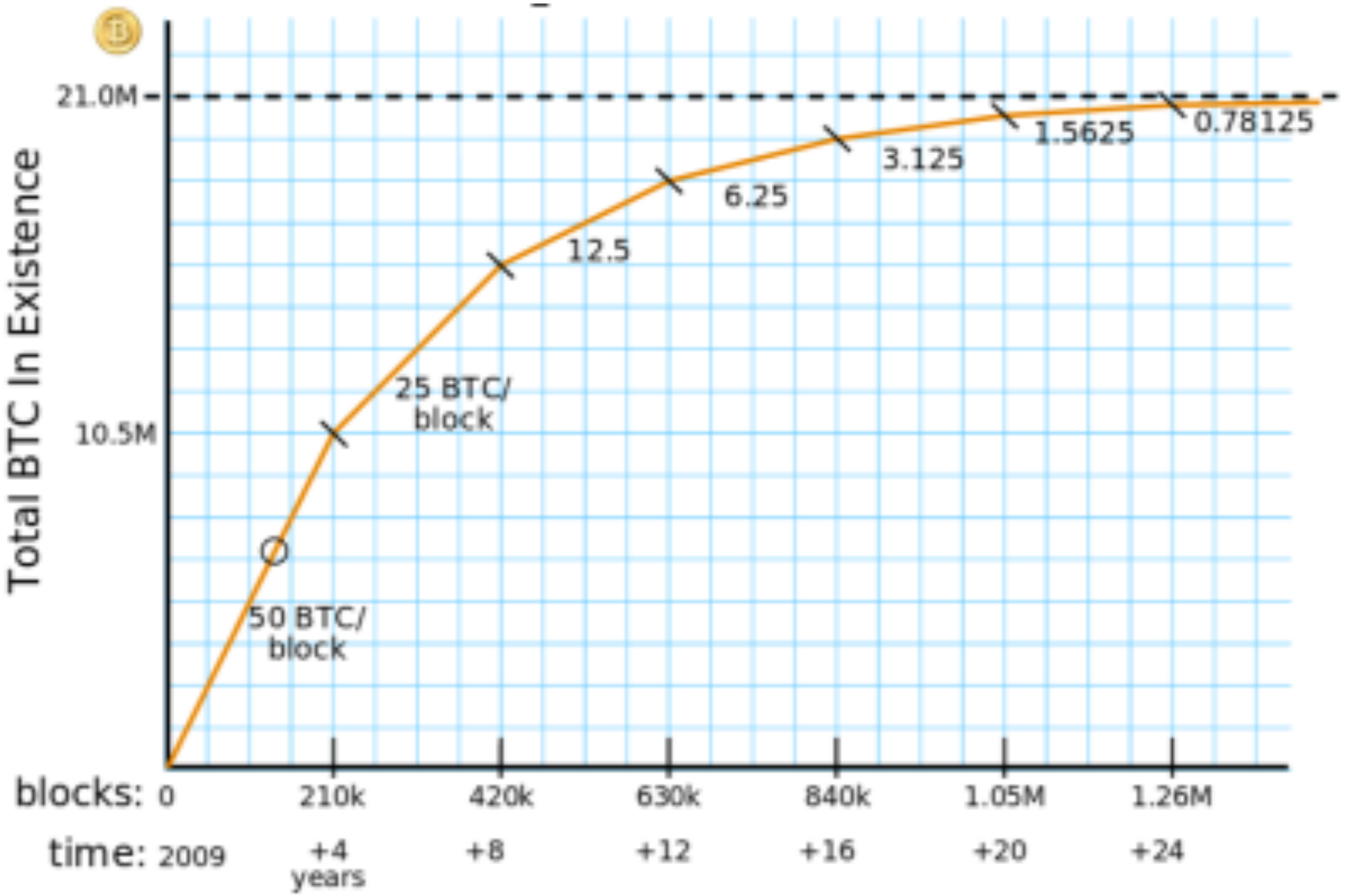


临时保留区块攻击



All other miners are wasting effort here!

交易费

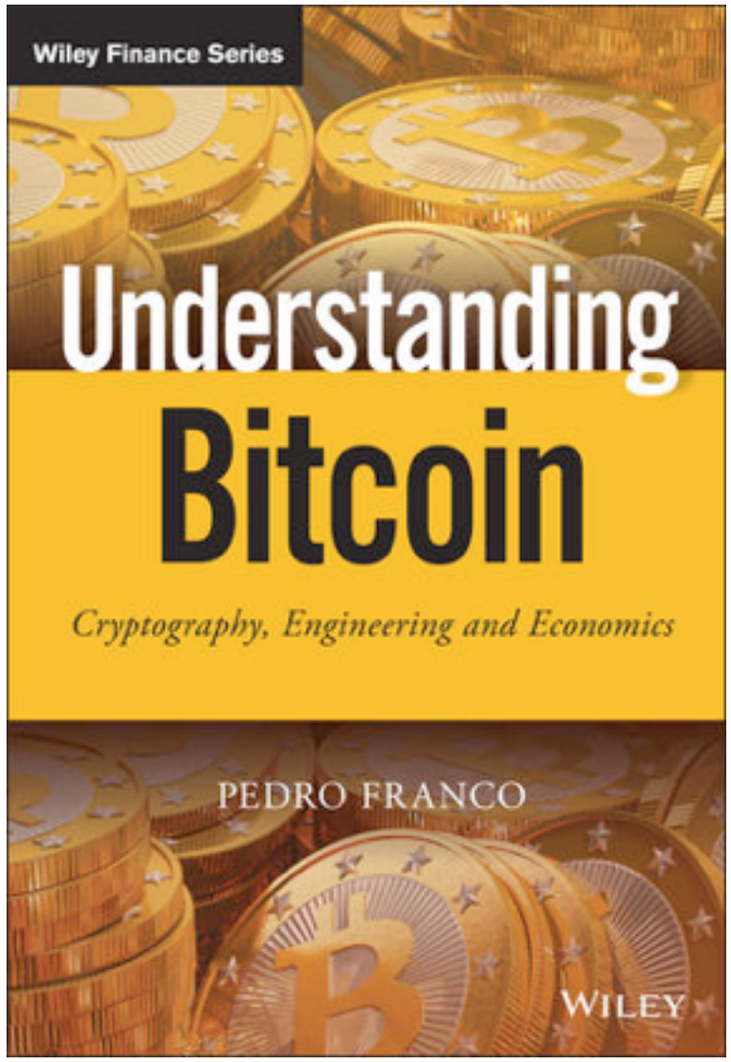

21.0M
10.5M
Total BTC In Existence
50 BTC/ block
25 BTC/ block
12.5
6.25
3.125
1.5625
0.78125
blocks: 0
210k
420k
630k
840k
1.05M
1.26M
time: 2009
+4 years
+8
+12
+16
+20
+24

提问时间！

Home work

Homework 课后作业

第五章、第八章



第九章

Homework 课后作业

- 要求阅读所选项目白皮书，提交阅读报告。

谢谢！

孙惠平

sunhp@ss.pku.edu.cn