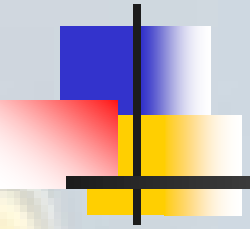
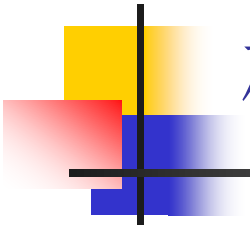
区块链基础及应用



Chapter 5 比特币挖矿

苏 明



概览

- 5.1 比特币矿工的任务
- 5.2 挖矿所需硬件
- 5.3 能源消耗和生态环保
- 5.4 矿池
- 5.5 挖矿的激励和策略

5.1 比特币矿工的任务

- 比特币挖矿 VS 淘金

为了挖矿，加入比特币网络，完成任务

1. 监听交易广播；
2. 维护区块链网络和监听新的区块；
3. 组装一个备选区块；
4. 找到一个有效的随机数；
5. 希望你的区块被全网接受；
6. 利润

5.1 比特币矿工的任务

- 第一类任务: **验证交易和区块**

  比特币网络赖以生存和运转的基础

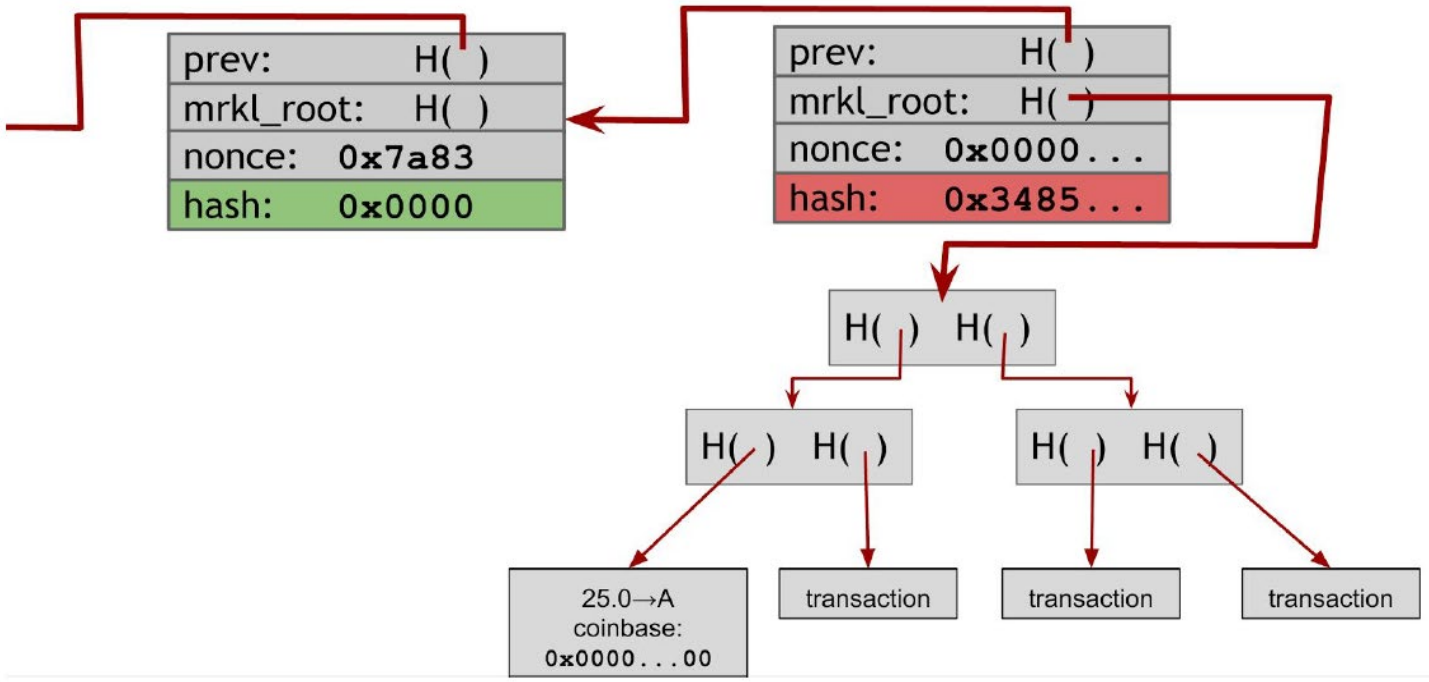
- 第二类任务：**竞争出块并获得奖励**

  鼓励矿工去完成第一类任务而设置

5.1 比特币矿工的任务

寻找有效区块

- 矿工首先从个人交易池中选出一系列有效的交易→Merkel Tree

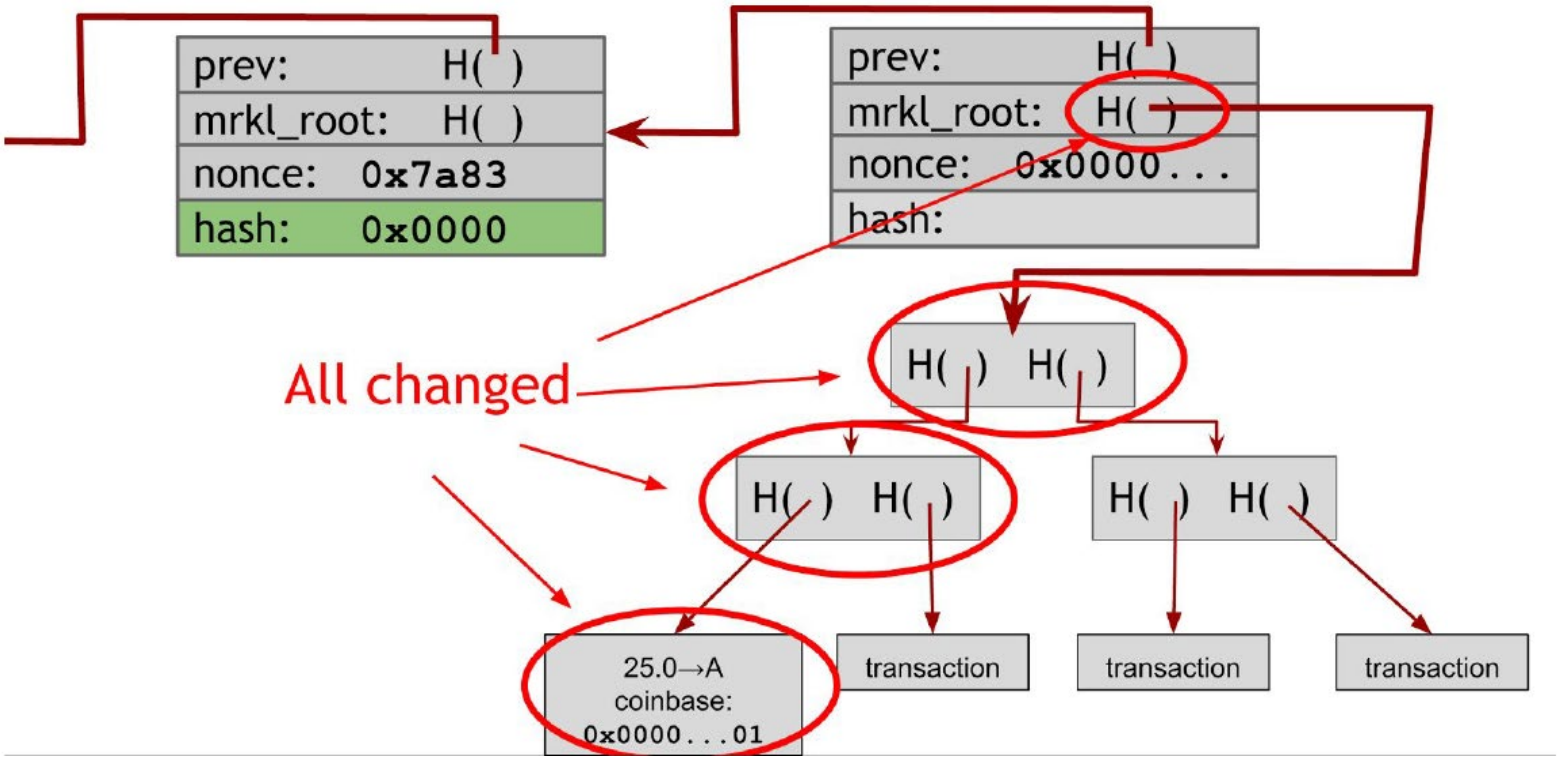


Finding a valid block

5.1 比特币矿工的任务

- 矿工： 挖矿通常使nonce 从0开始，每次增加1， 直到使得区块有效(Consecutive 0s in the front)
- nonce：32 bit
- 如何满足挖矿难度? (比如72个头部连续的0)

5.1 比特币矿工的任务



Changing a nonce in the coinbase transaction propagates all the way up the Merkle tree

5.1 比特币矿工的任务

- 如果遍历nonce的取值空间还没有找到一个有效区块时，改动coinbase中的随机数
- **正确的临时随机数组合：**头部随机数(nonce)+币基随机数(coinbase)
- **立即宣布：**希望得到出块奖励

5.1 比特币矿工的任务

- 求解谜题**不同**

每个矿工会把数目不同、次序不同的交易放进区块；币基交易里，接收地址通常也不一样

- 区块难度**相同**

00000000000000172EC0000000000000000000000000000000000000000000000000000000 (Mar. 2015)

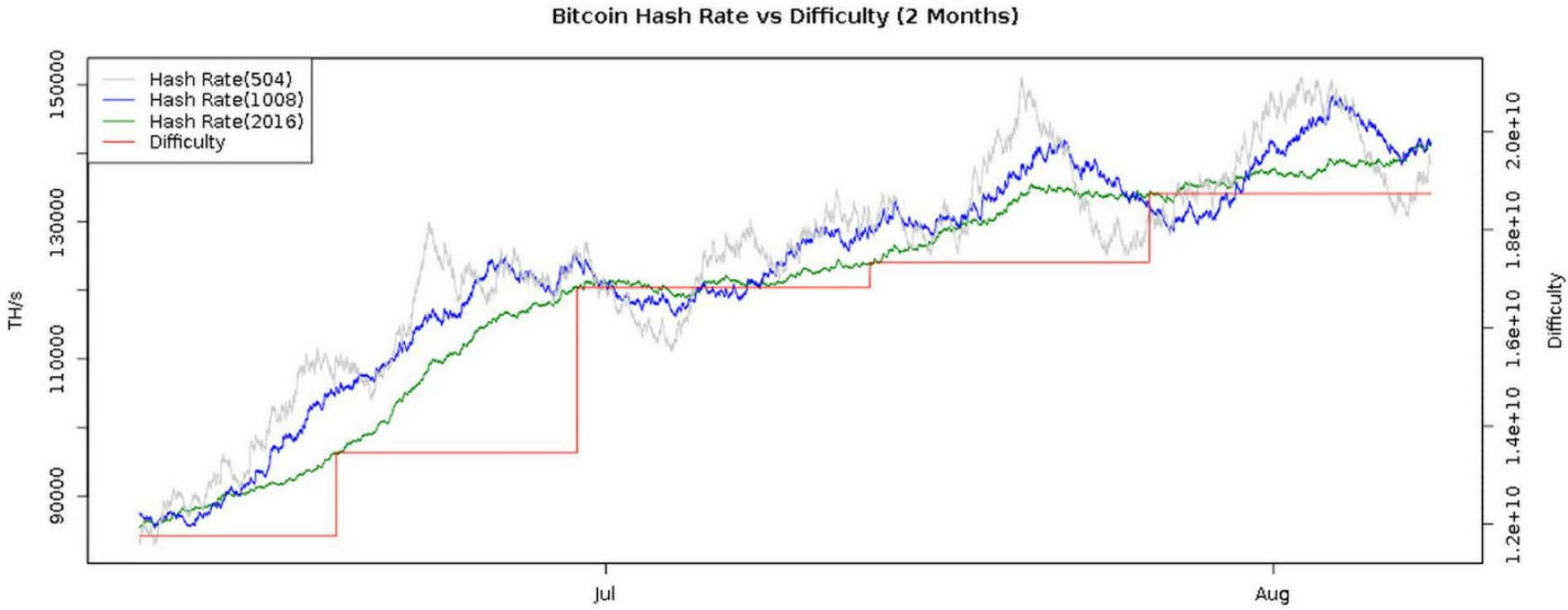
5.1 比特币矿工的任务

- 难度调整

next_difficulty = (previous_difficulty * 2016 * 10 minutes) / (time to mine last 2016 blocks)

5.1 比特币矿工的任务

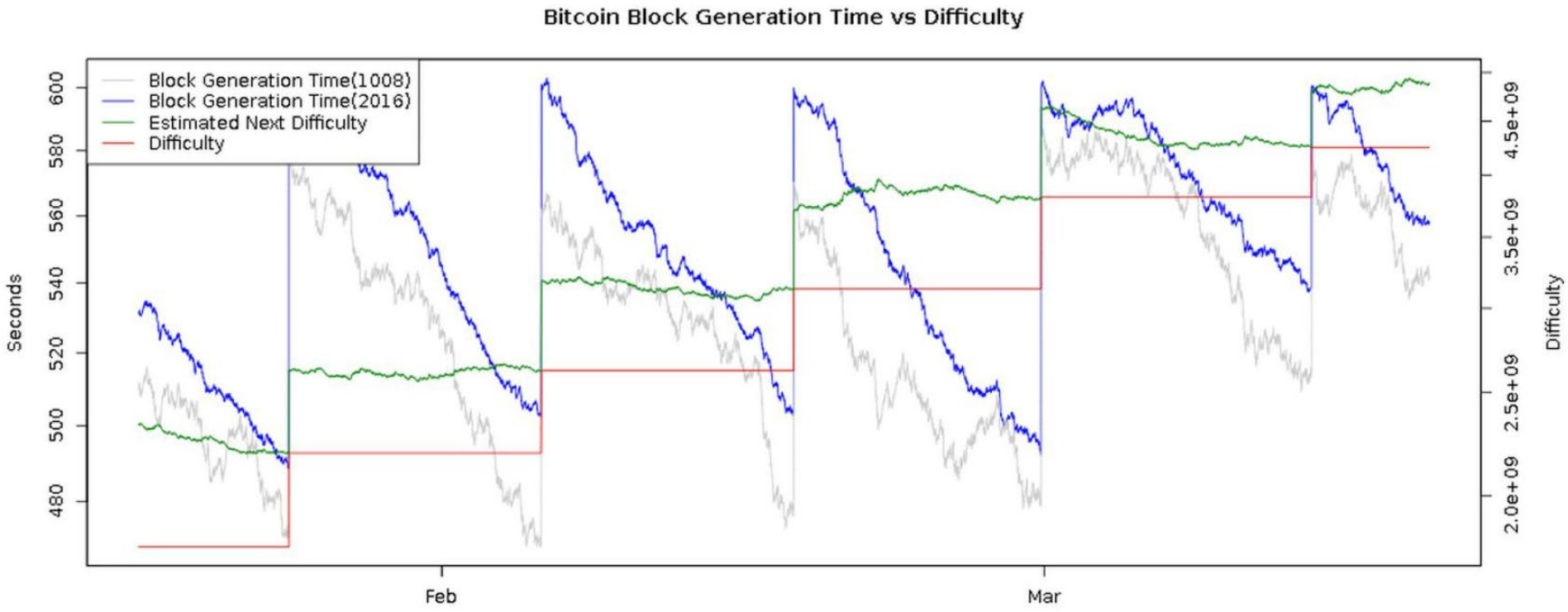
- 难度调整



Mining difficulty over time (mid-2014).

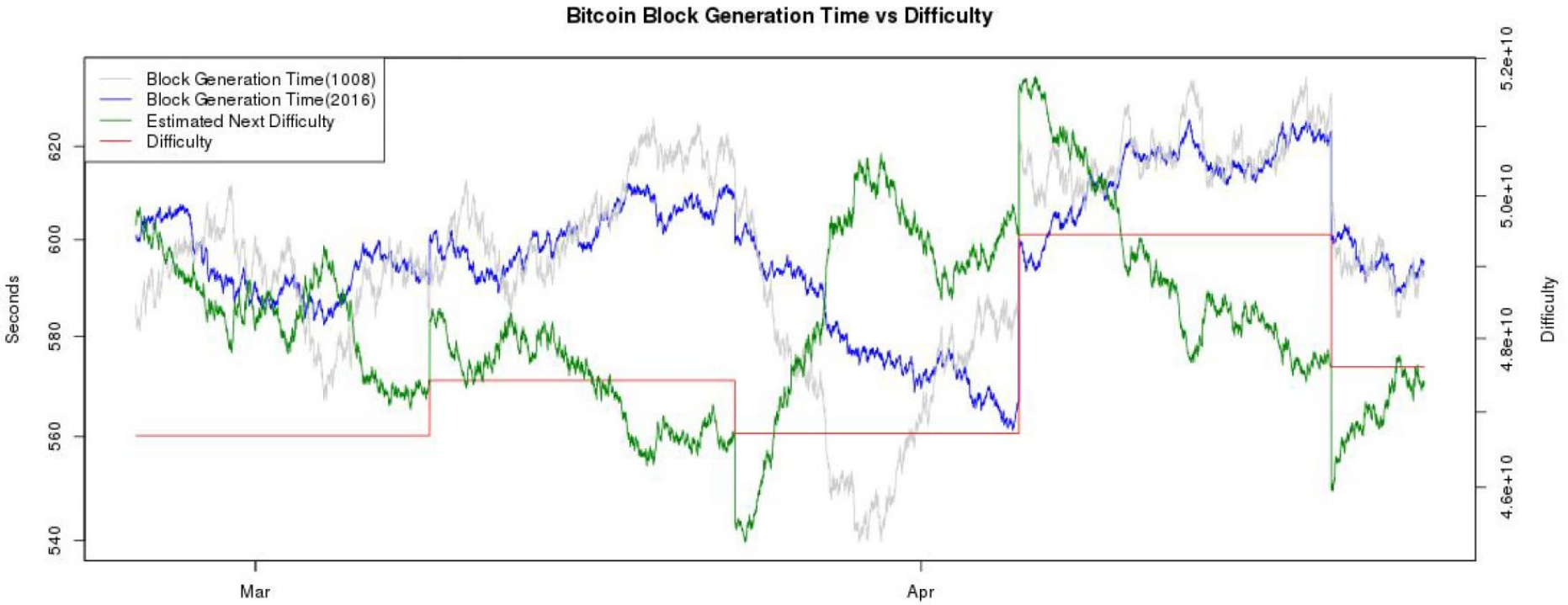
5.1 比特币矿工的任务

- 难度调整



Time to find a block (early 2014).

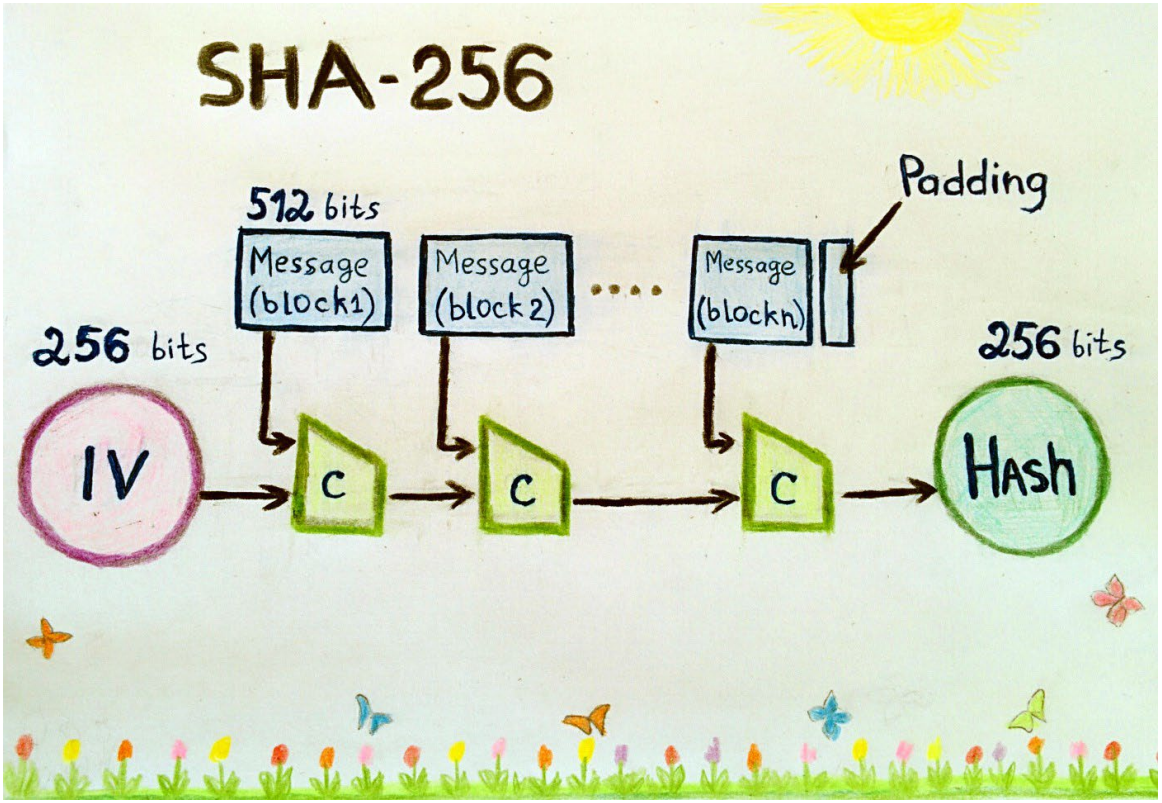
5.1 比特币矿工的任务



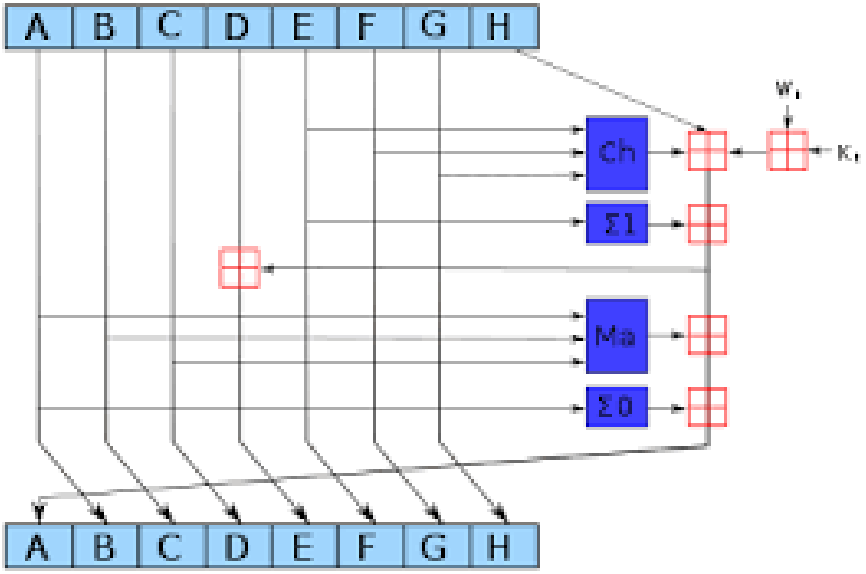
Time to find a block (early 2015).

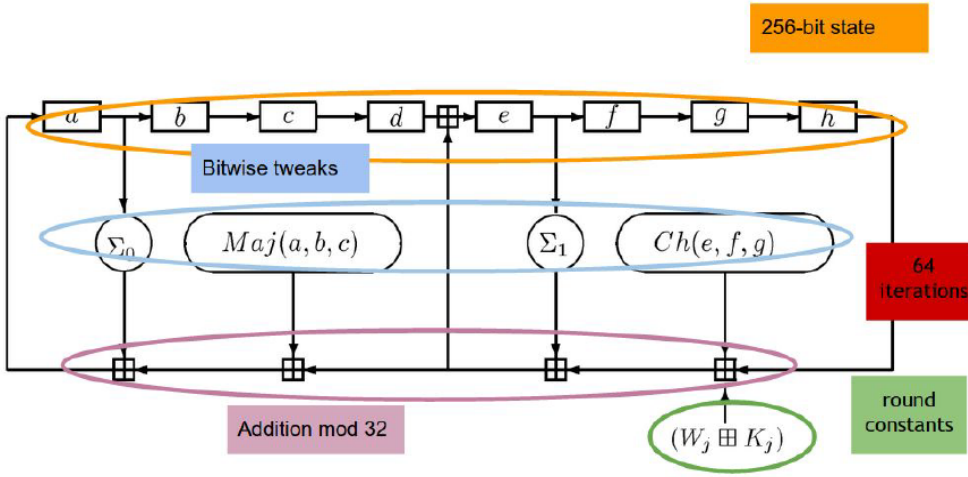
5.2 挖矿所需硬件

- SHA-256 (designed by the United States National Security Agency (NSA))



5.2 挖矿所需硬件


A
B
C
D
E
F
G
H
Ch
Σ1
Ma
Σ0
W_t
K_t
A
B
C
D
E
F
G
H


256-bit state
a
b
c
d
e
f
g
h
Bitwise tweaks
Σ0
Maj(a,b,c)
Σ1
Ch(e,f,g)
64 iterations
round constants
Addition mod 32
(W_j ⊞ K_j)

5.2 挖矿所需硬件

CPU挖矿

```
TARGET = (65535 << 208) / DIFFICULTY;
coinbase_nonce = 0;
while (1) {
      header = makeBlockHeader(transactions, coinbase_nonce);
      for (header_nonce = 0; header_nonce < (1 << 32); header_nonce++){
            if (SHA256(SHA256(makeBlock(header, header_nonce))) <
      TARGET)
                  break; //block found!
      }
      coinbase_nonce++;
}
```

CPU mining pseudocode

5.2 挖矿所需硬件

CPU挖矿

个人电脑： 20MH/s

2015年难度水平： 2^{67}

大约要几十万年找到一个区块！

5.2 挖矿所需硬件

- GPU挖矿
- 图形处理器(GPU) 适合做数据密集型的计算；适合并行
- **CPU 驱动多个GPU**

5.2 挖矿所需硬件

5.2 挖矿所需硬件

- 2015年： 200MH/S
- 100块显卡集成在一起进行运算
- 非常耗电
- **大约要几百年才能找到一个有效区块！**

5.2 挖矿所需硬件

- FPGA (Field-Programable Gate Array)

5.2 挖矿所需硬件

- 精心设计： 1GH/s
- 100块 FPGA 板→100年才能找到一个有效区块
- 故障和报错；性能功耗比方面不理想

5.2 挖矿所需硬件

- 专用集成电路技术挖矿 (ASIC)
- 应用需求驱动
- 集成电路芯片：需要专业的知识，设计的芯片寿命十分短暂
- 运营成本很高(电力、冷却)

5.2 挖矿所需硬件

如今--**专业挖矿**的天下

- 大型专业挖矿中心：专门运营
- 采购打过折的功效更高的ASIC矿机

5.2 挖矿所需硬件

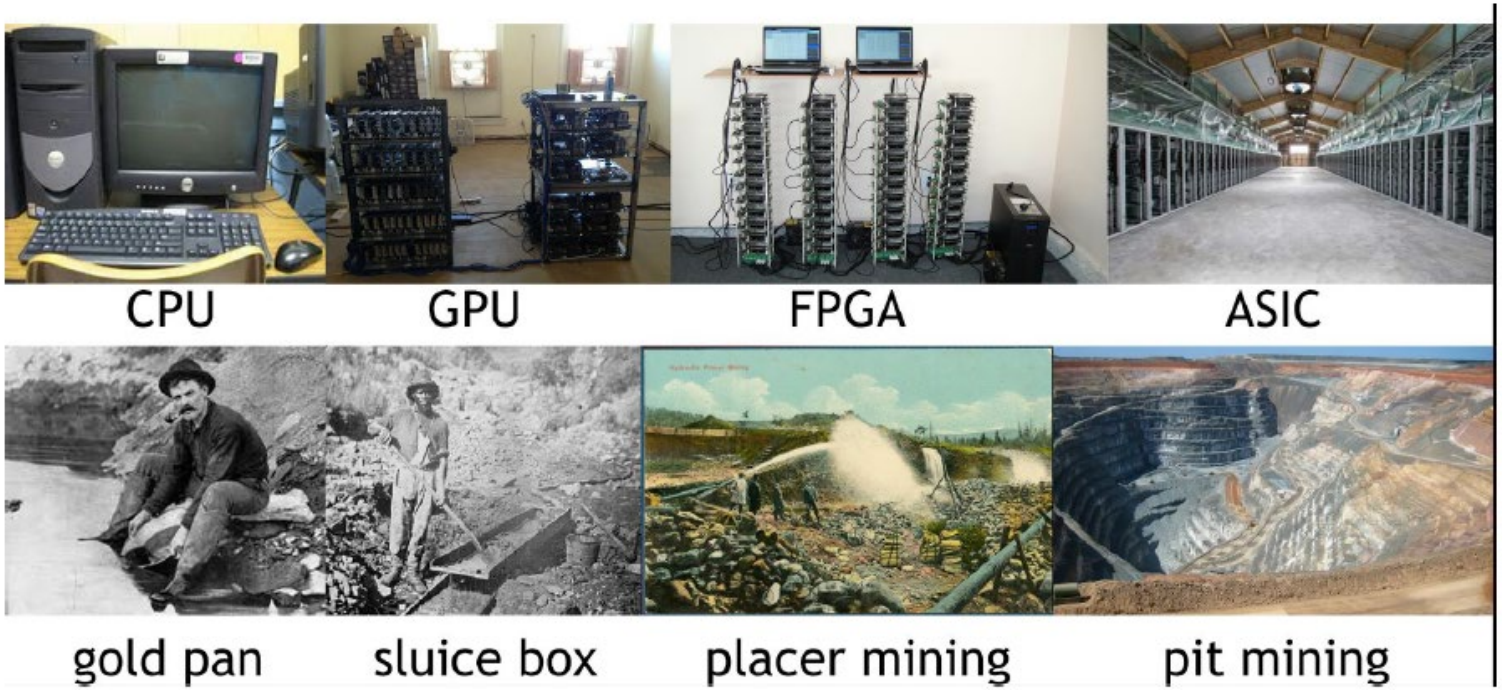
BitFury mining center, a professional mining center in the republic of Georgia.

5.2 挖矿所需硬件

- 建立挖矿中心的三个重要因素：
- **气候、电费、网络接入速度**
- 格鲁吉亚、冰岛；中国内蒙古

5.2 挖矿所需硬件

- Bitcoin Mining VS Gold Mining



Evolution of mining

5.2 挖矿所需硬件

未来

- ASIC和专业挖矿中心违反了当时设计的初衷：完全**去中心化**的系统

另类币的挖矿发展轨迹：

- 也许谜题会变，但是循环周期类似

  CPU->GPU->FPGA->ASIC->...

5.3 能源消耗和生态环保

- 每进行一个不可逆的bit flip运算就会消耗能源

- 比特币的挖矿过程必定消耗能源

1. 内涵能源 （生产矿机）
2. 电能 （挖矿）
3. 冷却 （防止矿机出故障）

5.3 能源消耗和生态环保

- 能源消耗估计(数量级)

- 2015

自上而下

- 收入用来支付电能
- 每秒所有的11美元收入购买电费，可以购买367 百万焦耳-→MW 数量级

5.3 能源消耗和生态环保

自下而上

- 最好的矿机：1W—3G/s
- 全网算力是350PH/s

---->

每秒中全网计算消耗 117 MW

总而言之，比特币挖矿当时（2015）是MW的数量级

5.3 能源消耗和生态环保

- 2020，比特币挖矿的能耗

1KB=1024B
1MB=1024KB
1GB=1024MB
1TB=1024GB
1PB=1024TB
1EB=1024PB
1ZB=1024EB
1YB=1024ZB

The BTC network's hashrate has touched close to 140 exahash per second (EH/s) in 2020. Today, according to charts.Bitcoin.com data the hashrate is hovering around 120EH/s.

5.3 能源消耗和生态环保

- 比特币挖矿—浪费能源？
- 能源的循环使用—数据火炉(Data Furnace)
- 电力转换成现金的途径

5.4 矿池

单个矿工的挖矿风险

- 发现区块的数目可以用帕松分布(Poisson distribution)来逼近

- Binomial distribution can be approximated by the Poisson distribution

$$P(X = k) = \frac{e^{-\lambda}\lambda^k}{k!}$$

5.4 矿池

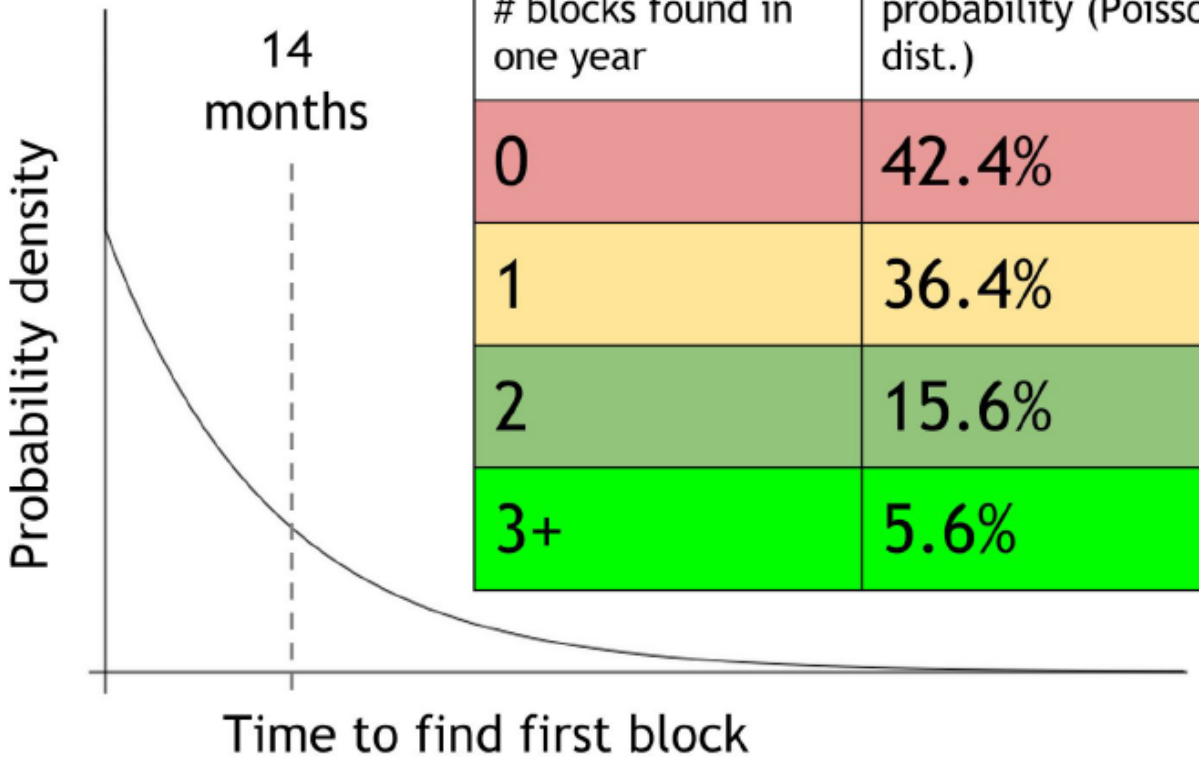
$$令p=\lambda/n, \qquad \lim_{n\to\infty} P(X=k)=\lim_{n\to\infty}\binom{n}{k}p^k(1-p)^{n-k} =\left(\frac{\lambda^k}{k!}\right)\exp(-\lambda)$$

- 比如你用6000 US Dollars买了一台矿机

根据矿机性能，平均每14个月找到一个区块

$$\lambda=\frac{6}{7}$$

5.4 矿池



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

```
>> power(2.71828, -6/7)*6/7

ans =

    0.3637

>> power(2.71828, -6/7)*(6/7)^2/2

ans =

    0.1559
```

Illustration of uncertainty in mining

5.4 矿池

- 对于一个小矿工而言，挖矿就是**赌博游戏**
- 矿池：比特币矿工互相之间的**保险**
- 一组矿工可以形成一个矿池共同挖矿，并指定一个币基接收人-*矿池管理员*

5.4 矿池

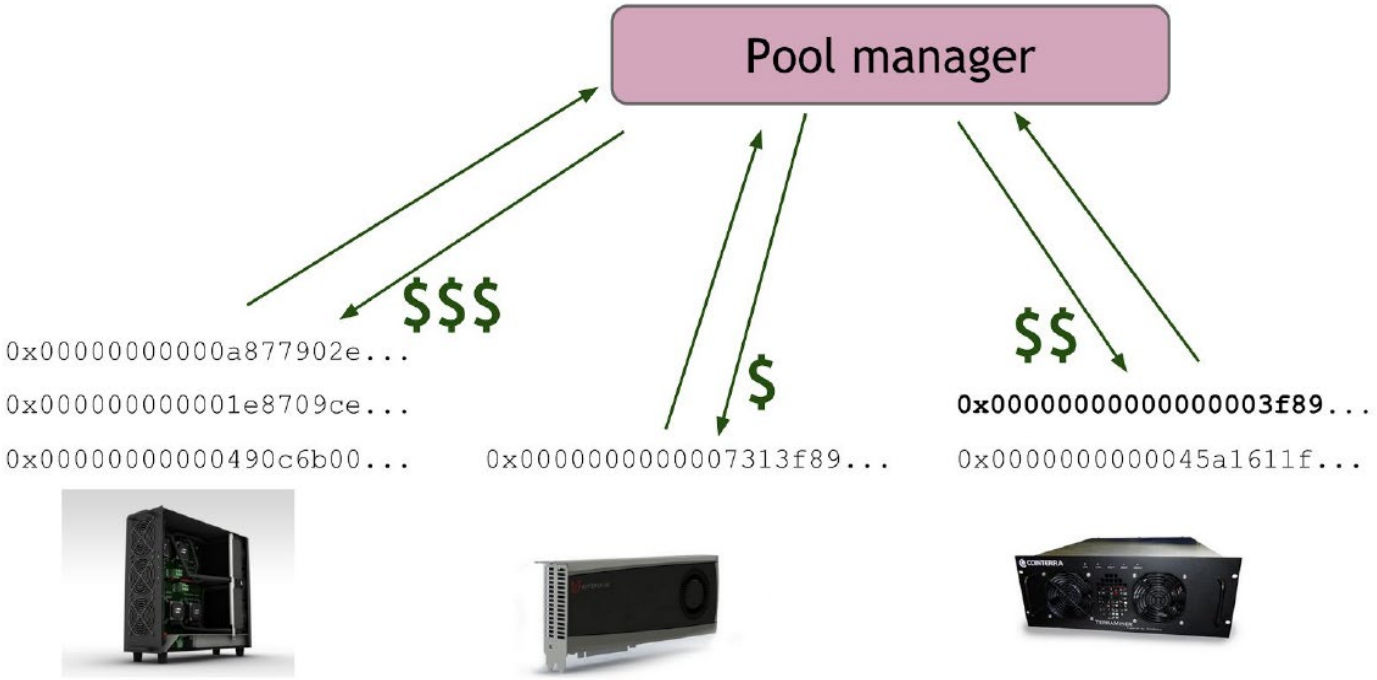
- 矿工通过输出挖矿工分来证明他的工作量
- 比如目标值前面有67个0；一个合格的工分需要40-50个0

```
4AA087F0A52ED2093FA816E53B9B6317F9B8C1227A61F9481AFED67301F2E3FB
D3E51477DCAB108750A5BC9093F6510759CC880BB171A5B77FB4A34ACA27DEDD
00000000008534FF68B98935D090DF5669E3403BD16F1CDFD41CF17D6B474255
BB34ECA3DBB52EFF4B104EBBC0974841EF2F3A59EBBC4474A12F9F595EB81F4B
00000000002F891C1E232F687E41515637F7699EA0F462C2564233FE082BB0AF
0090488133779E7E98177AF1C765CF02D01AB4848DF555533B6C4CFCA201CBA1
460BEFA43B7083E502D36D9D08D64AFB99A100B3B80D4EA4F7B38E18174A0BFB
0000000000000000078FB7E1F7E2E4854B8BC71412197EB1448911FA77BAE808A
652F374601D149AC47E01E777613845618 1FA4F9D0EEDD8C4FDE3BEF6B1B7ECE
785526402143A291CFD60DA09CC80DD066BC723FD5FD20F9B50D614313529AF3
000000000041EE593434686000AF77F54CDE839A6CE30957B14EDEC10B15C9E5
9C20B06B01A0136F192BD48E0F372A4B9E6BA6ABC36F02FCED22FD9780026A8F
```

Mining Shares

5.4 矿池

- 矿池管理员根据大家的工作量按照比例分配奖励



Mining rewards

5.4 矿池

分红方案

- 工分分红：

  矿工发送工分，管理员马上支付奖励

  管理员承担了所有风险

- 按实际比例分红：

  每次找到一个有效区块，区块奖励按照矿工工作量按比例分配；**降低管理员风险**

5.4 矿池

矿池跳换

- 投机矿工：

挖矿早期(上一个区块刚刚被发现)加入按实际比例分红的矿池；

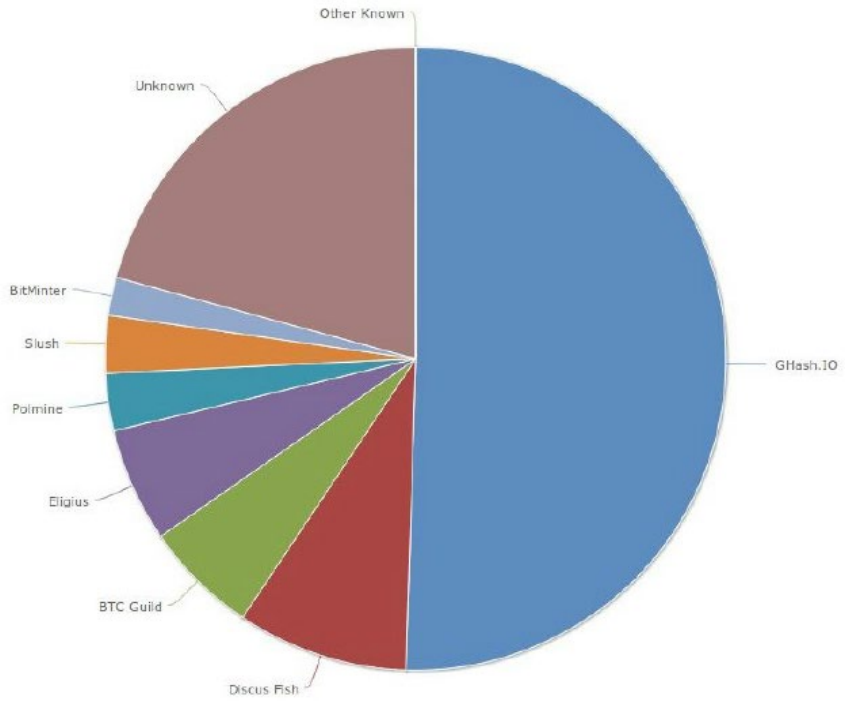
挖矿后期跳到一个按工分分红的矿池。

- 研究问题：如何设计一个矿池方案，避免矿工的投机？

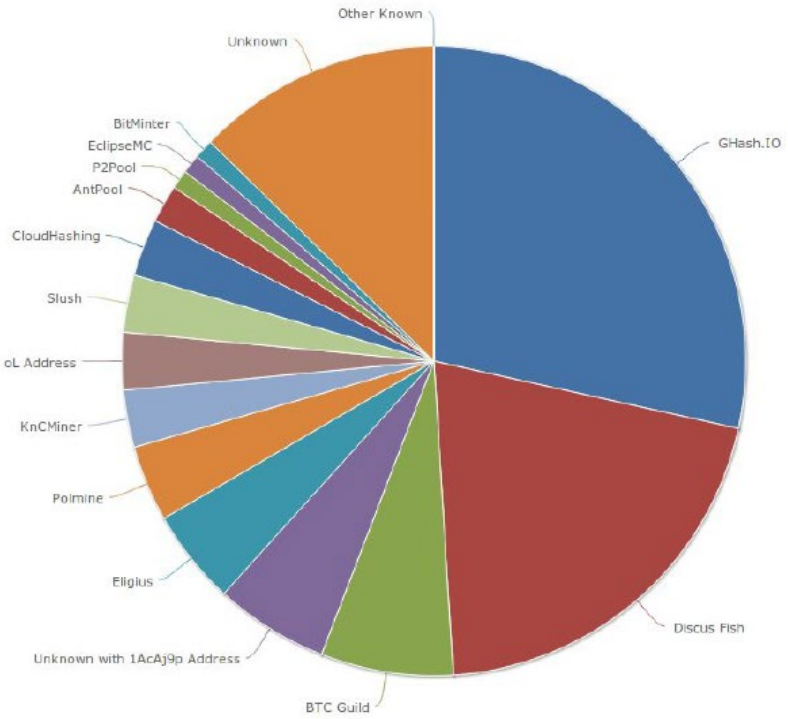
根据*最近若干个工分*提交的结果才分配

5.4 矿池

- 51%矿池

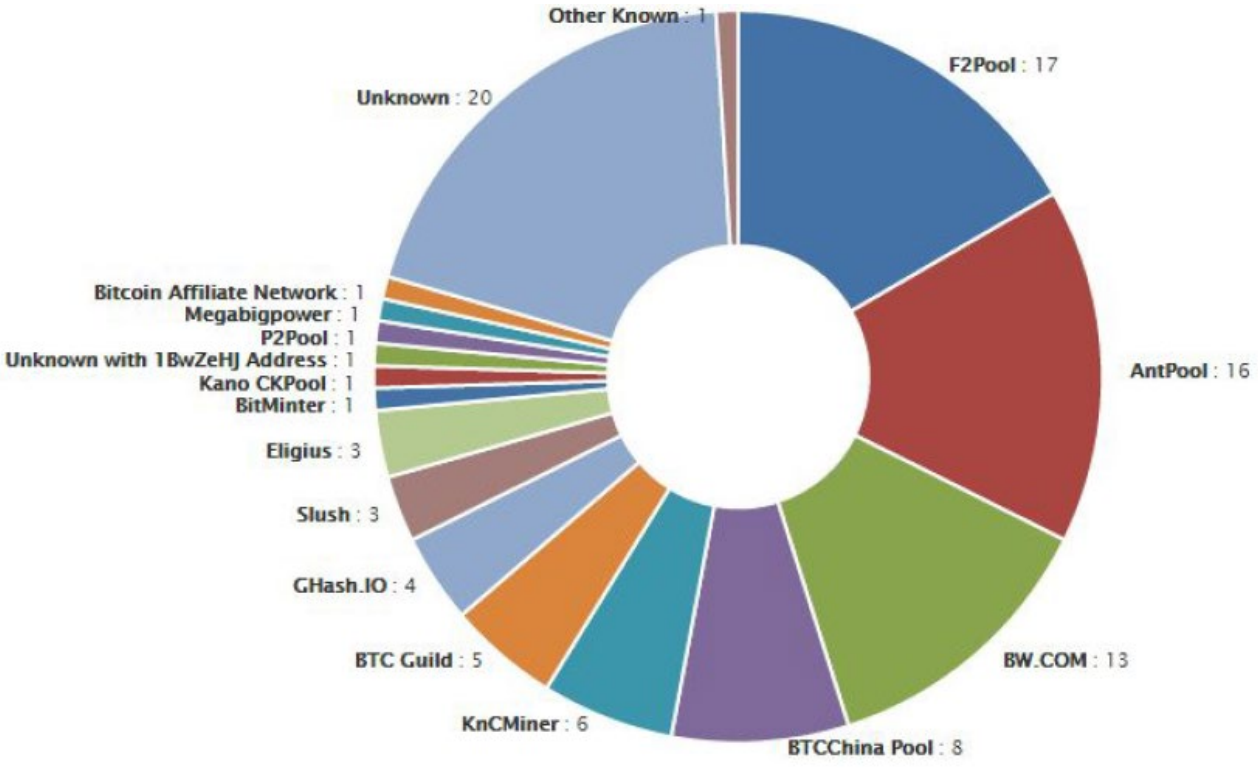


Hash power by mining pool, via blockchain.info (June 2014)



Hash power by mining pool, via blockchain.info (August 2014)

5.4 矿池



实际上的算法可能集中在几个大的机构手中，即使‘洗算力’

Hash power by mining pool, via blockchain.info (April 2015)

5.4 矿池

- 优点

  小矿工容易参与，也有一定的收益；

  网络管理员负责组装区块，网络更新变得更加容易

- 缺点

  （算力）*中心化*管理；

  整个网络中进行*校验交易*的**全节点**数目在下降

5.5 挖矿的激励和策略

- 在挑选一个区块开挖之前，矿工做策略上的选择：

1. 需要包括哪些交易？ （优先选择交易费高的交易）
2. 对哪一个区块进行挖矿运算？ （优先选择最长的区块链上继续下挖）
3. 在同一高度的多个区块中做选择？ （优先选择被监听到的那一个区块）
4. 什么时候宣布新的区块？ （默认做法是立刻宣布）

5.5 挖矿的激励和策略

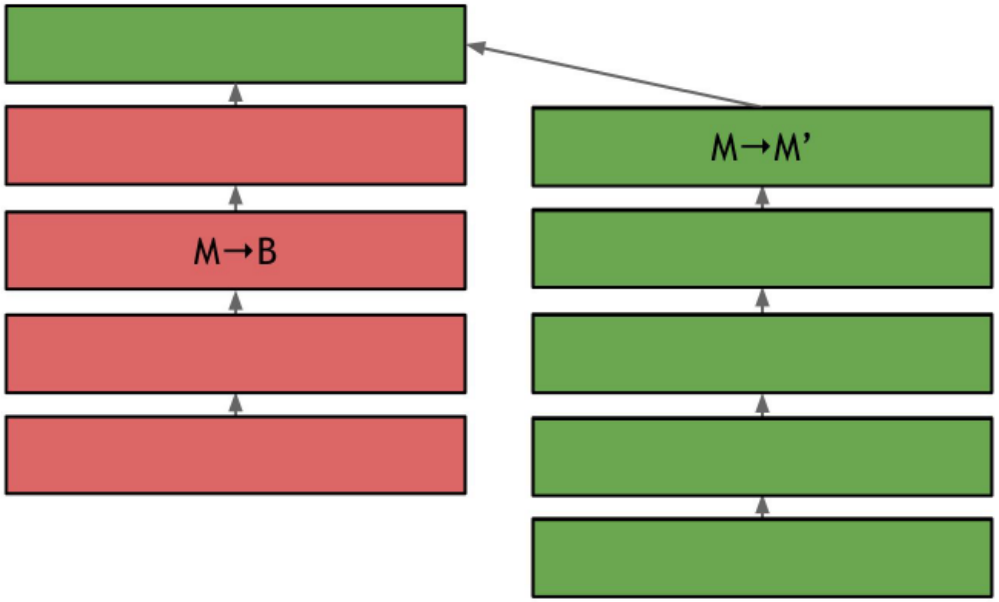
分叉攻击(forking attack)

- 双花：重复支付

A malicious miner sends a transaction to Bob and receives some good or service in exchange for it. The miner then forks the block chain to create a longer branch containing a conflicting transaction. The payment to Bob will be invalid in this new consensus chain.

5.5 挖矿的激励和策略

- 分叉攻击



Forking attack

5.5 挖矿的激励和策略

- 51%是必要的吗？
- 51%会影响大家对‘去中心化’的信任
- 实际上，稍低算力也可以发起攻击，因为有网络拥塞、延迟等因素：

  中心化的攻击者能够快速通信从而节省一些算力

5.5 挖矿的激励和策略

- 贿赂攻击

  有别于直接获得算力，攻击者贿赂已经具有算力的人，以分叉出一条最长链

- 临时保留区块攻击(*自私挖矿*)

5.5 挖矿的激励和策略

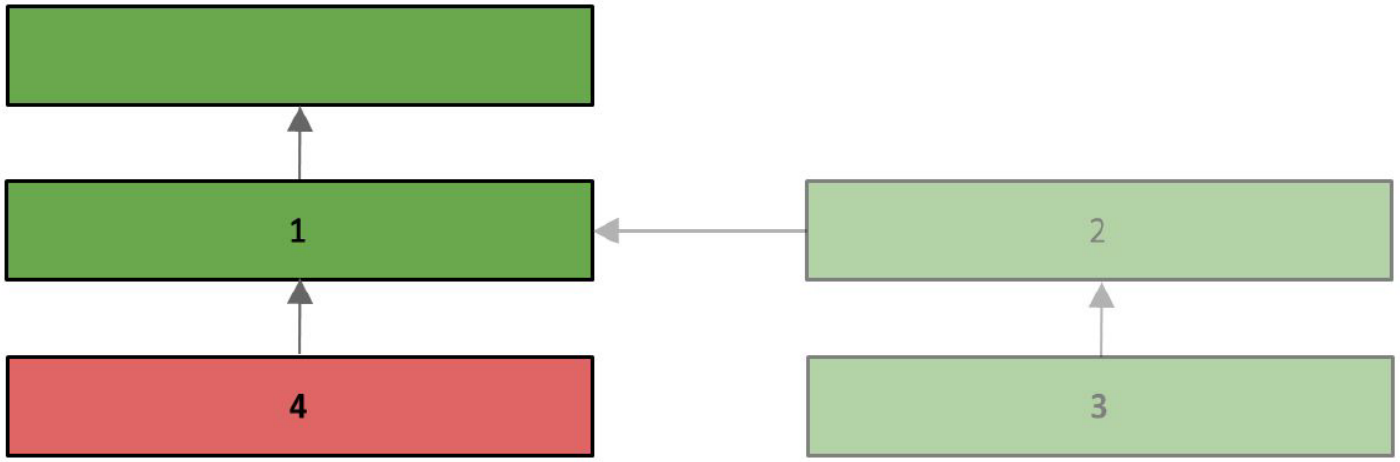


Illustration of selfish mining

(1) Block chain before attack.
(2) Attacker mines a block, withholds it, starts mining on top of it.
(3) Attacker gets lucky, finds a second block before the rest of the network, continues to withhold blocks.
(4) Non-attacker finds a block and broadcasts it. In response, the attacker broadcasts both his blocks, orphaning the red block and wasting the mining power that went into finding it.

5.5 挖矿的激励和策略

- 黑名单与惩罚分叉攻击

宣布拒绝在包含来自该地址的交易的区块链上工作；（类似美国制裁伊朗）

- 羽量级分叉

如果胆敢把来自地址X的交易加入自己的区块，便有α^2的可能会丧失自己已经发现的区块

5.5 挖矿的激励和策略

- 目前，区块奖励在矿工收入里面占比超过99%；
- 但是区块奖励每4年减半，最终出块奖励会变得很低；
- 从长期来看，比特币奖励将从固定的挖矿奖励为主，转变为交易费为主