货币和比特币
CURRENCY AND BITCOIN

Sam Wong
2017-05-26

说明

这个Deck有小量动画和大量文字笔记作补充

可以在这里下载其他格式

https://github.com/sam0737/brownbag

我的Bitcoin钱包: 1J9MKzB2KNoPofgACqXwtNb48DMyeDCAoT

本Deck以CC-SA 3.0发佈

图片使用的着作权在笔记栏详细说明

- 放弃金本位 CC-SA 3.0: Will O'Neil


CONG HOA XA HOI CHU VIET NAM
NAM TRAM DONG
500
2000
1988
MOT TRAM NGHIN DONG
100.00
10000
CK 470553 V
日本銀行券
壱万円
TEN HONG KONG DOLLARS
HONG KONG
SINGAPURA
Australia
FIVE DOLLARS

什么是钱？

糧食

银圆

金/银本位货币问题？

矿产地分佈不平均

挖矿速度、生产力变化、需求不协调

- 发现新金矿带来币值衝击
- 20世纪生产力高速上升
- 战争

部份准备金制度
FRACTIONAL-RESERVE BANKING

1. 存100元进银行
2. 银行只需按法例留10% (x%)
3. 90元借出去
4. 90元存进来又能把81元借出去
5. 最终100元变成100/x%即1000元。

2016年中国存款准备金规定

- 大型金融机构: 16.50%
- 中小金融机构: 13.00%

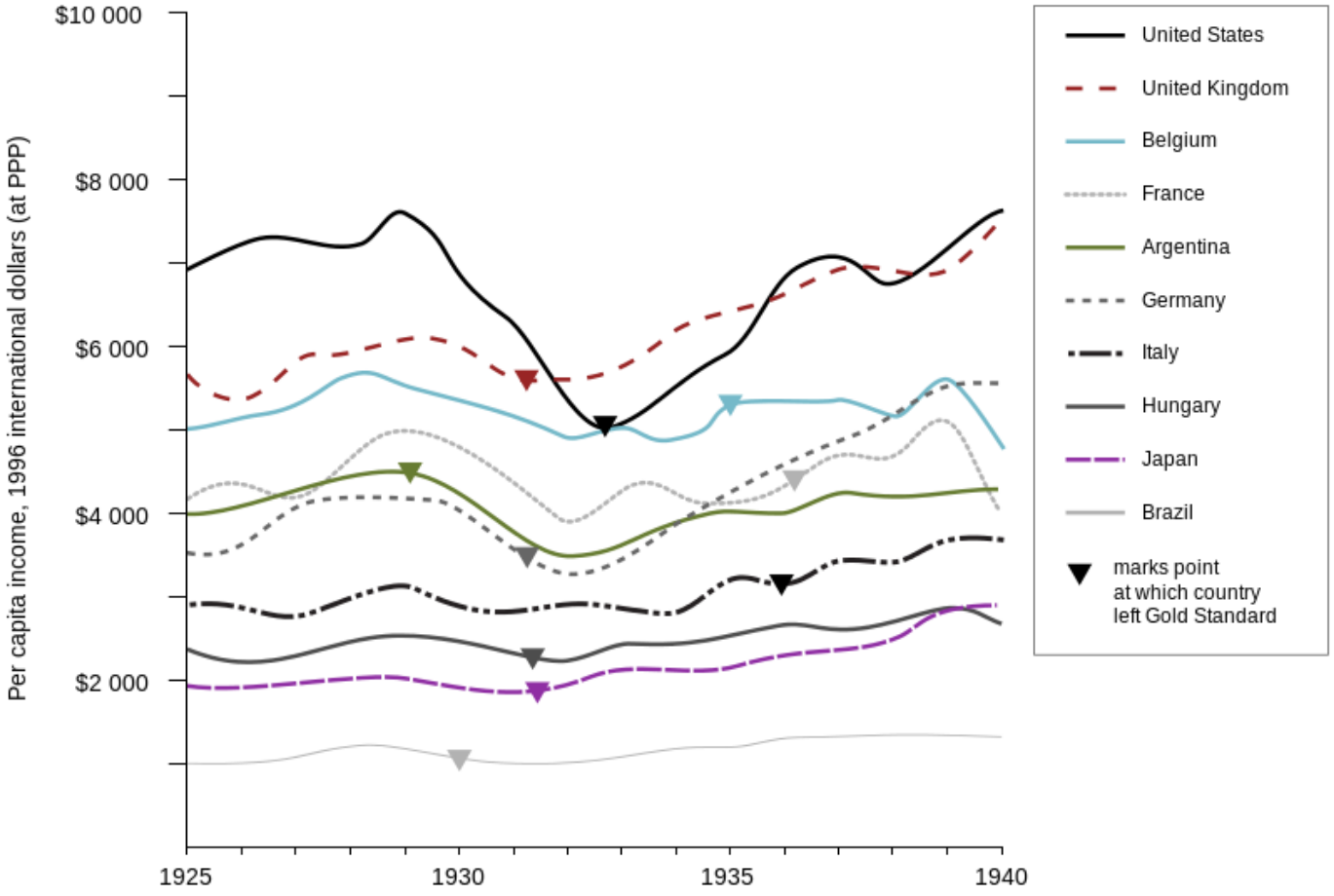
纸币

第一次世界大战

1914-1918

经济大萧条

1929-1940


$10 000
$8 000
$6 000
$4 000
$2 000
Per capita income, 1996 international dollars (at PPP)
1925
1930
1935
1940
United States
United Kingdom
Belgium
France
Argentina
Germany
Italy
Hungary
Japan
Brazil
marks point at which country left Gold Standard

放弃金本位

第二次世界大战

1939-1945

BRETTON WOODS
布雷顿森林体系

1944年7月在布雷顿森林公园开会所定的协议

美元作为储备货币

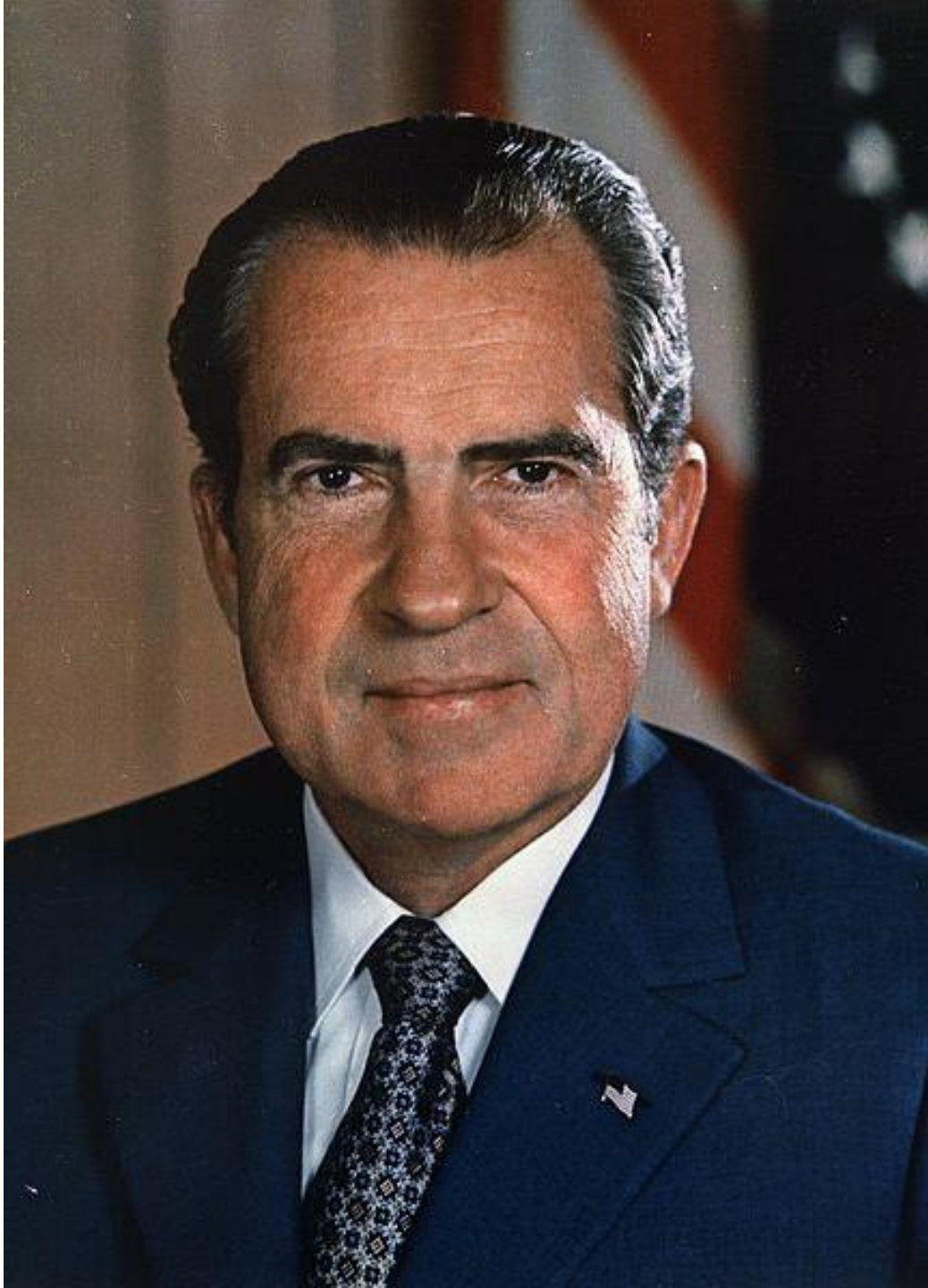
- 美联储保证美元按照官价兑换黄金
- 提供足够的美元作为国际清偿手段

越战

1955-1975

尼克松冲击
NIXON SHOCK

1971



法定货币
FIAT CURRENCY

不能吃、什么也不是

但至少能用来交税

货币总结

比特币

比特币
BITCOIN/BTC

首只Cryptocurrency (加密货币)

2009-01-03开始

由中本聪(Nakamoto Shatoshi)发明

目前看过最细交易单为是百万份之一个BTC，亦称一个Shatoshi

- 但技术上可以更细

比特币兑人民币

比特币价值

信则有不信则无

有很多交易所，与法币兑换

因中国政府管制，2017年2月起国内交易所不能提币

比特币特性

无人监管、亦无单一人能干预

发行量固定且可预知

账目公开

钱包匿名

比特币规则

生产

- 平均每10分钟挖出个区块(Block)
- 挖出区块者可以得到奖励金。也是唯一的比特币生产方法
- 奖励金开始时是50BTC，随后每挖出210000个区块(约4年)后减半
  - 现时是12.5BTC一个区块，已挖出约80%
- 每挖2016个区块(每2周)会调整计算难度
  - 无论多少人挖也是平均每10分钟挖出一个

消费限制

- 不能双重消费 (Double Spend)

PROOF OF WORK (POW)

$$x^2 - 15x + 54 = 0$$

$$x = 6 \; or \; x = 9$$

HASH 哈希

sha256(“UCO IS GOOD”) =
a603ecea9c7efa4f27f32d2ca3f6deb508a8d95c4ad562db3e66c44d061ced9f

sha256(“UCO IS GOOD!”) =
d5aac8c5f0a407bc8fcd75cac423dbcd585133c80a11dfcfbfc42e7c13c72a41

sha256(“UCO IS GOOD0”) =
6ee2f7f9b8904aa51339fafba4d8618b35f9dabaa06e0afb27b16266dc24b57c

sha256(“UCO IS GOOD1”) =
9a659c5b991cae2a4e3012a4d7d63872d02ae94212de7e29b82177ec42fb3dd1

问题: “UCO IS GOOD”后带个什么数字，sha256出来才能是0开头？

答案: 3

sha256(“UCO IS GOOD3”) =
0c578d1440d99dc601730cfb2f0c9ebe36b63b0d04ec1d00d413b3b72dc5e25f

3就是这一次的nonce

区块

最大1MB的文件

哈希内容:

- N条交易数据，包括奖励金入账交易
- 上面这堆数据的32 bytes哈希值 (Merkle Tree的根节点)
- 上一个节点的支针

挖矿是什么？

- 找一个nonce而且其sha256(区块内容+nonce)是比难度值小
- 找到后向其他电脑广播这区块+nonce内容

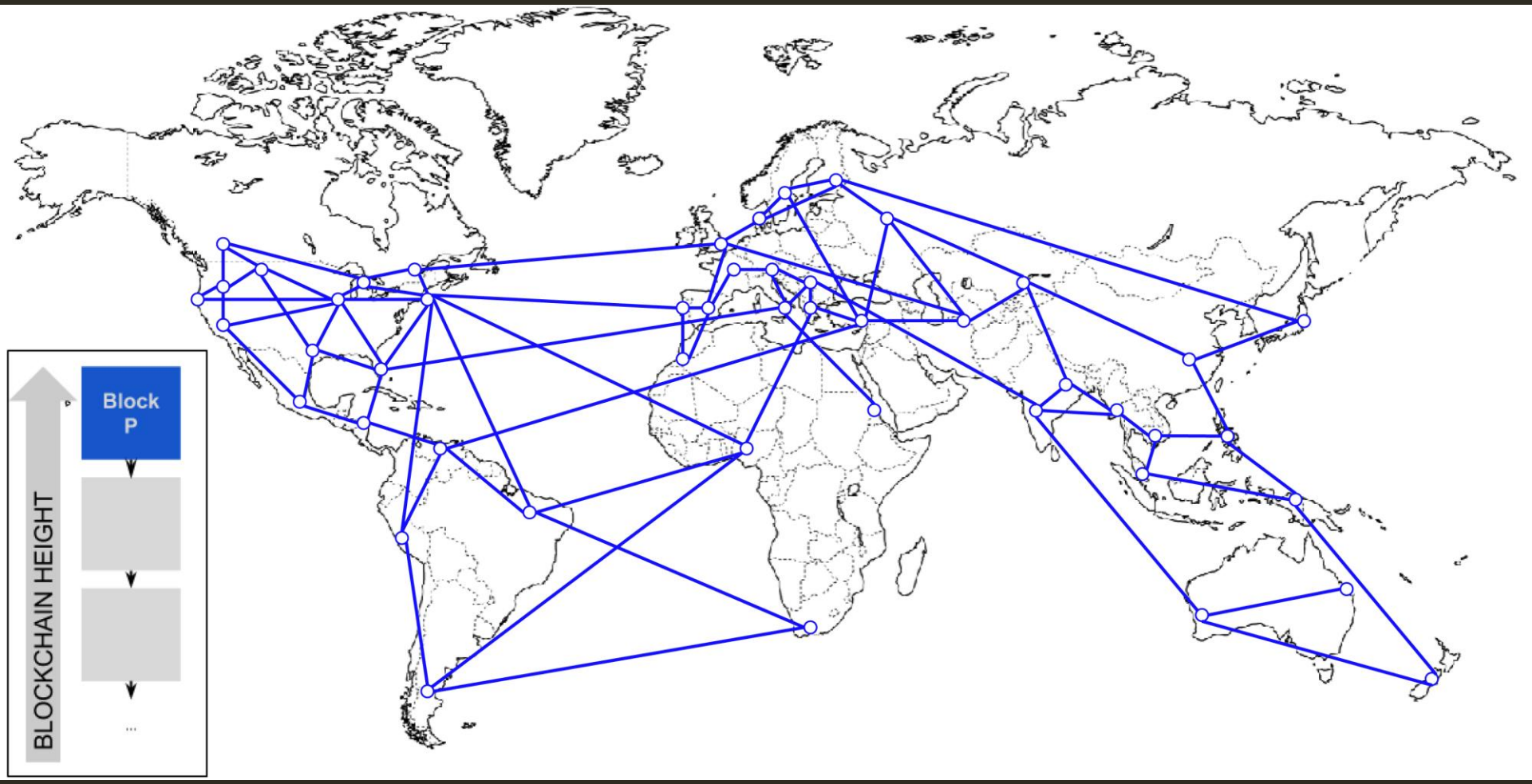
节点 NODE – 执行规则者

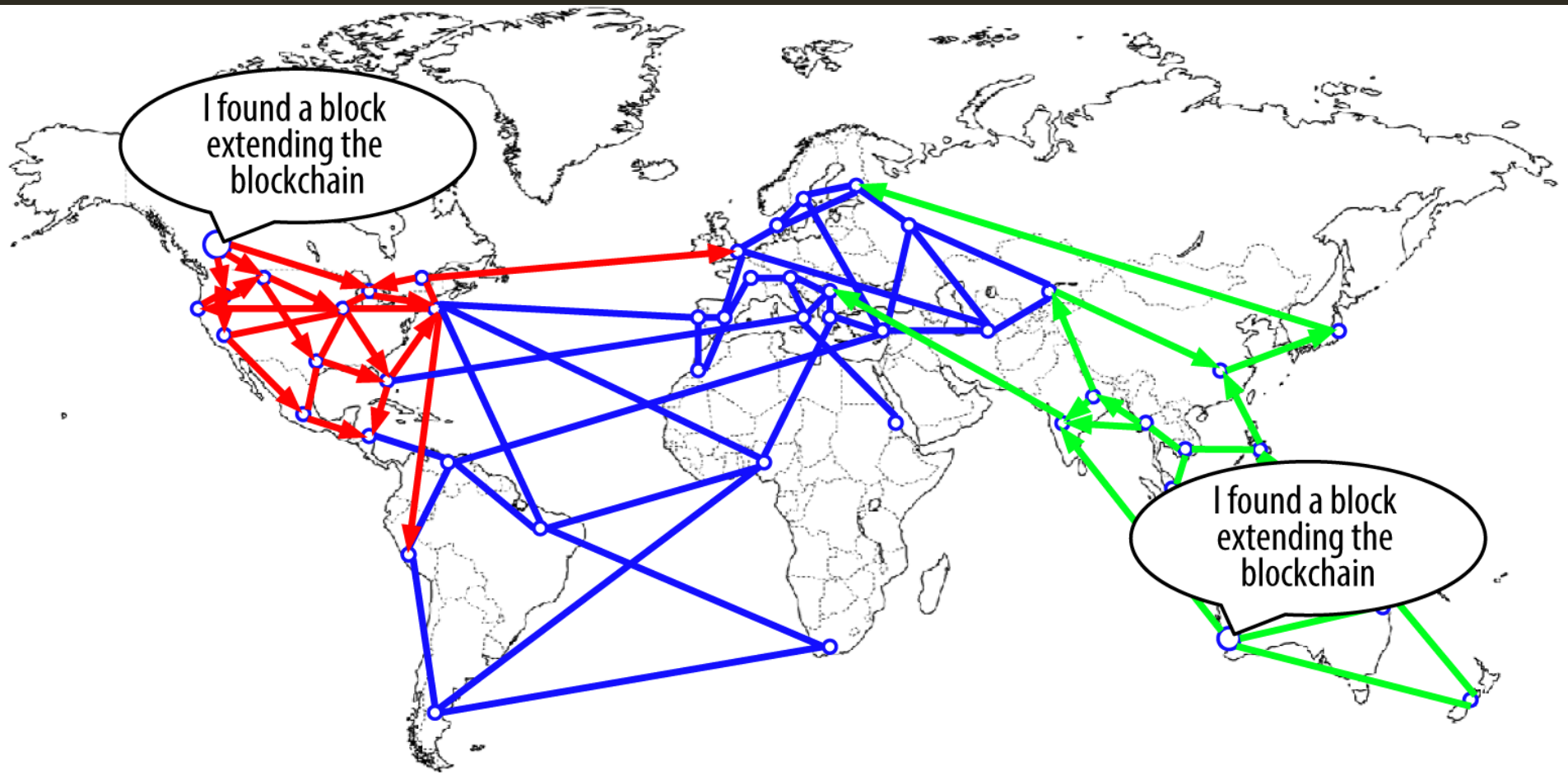
1. 接收挖矿结果
2. 验正规则
   1. 确保区块的信息正确
   2. 验证nonce计算无误、sha256出来符合当前难度要求
   3. 确保交易信息符合规则，包括奖励金、有没有多花钱等

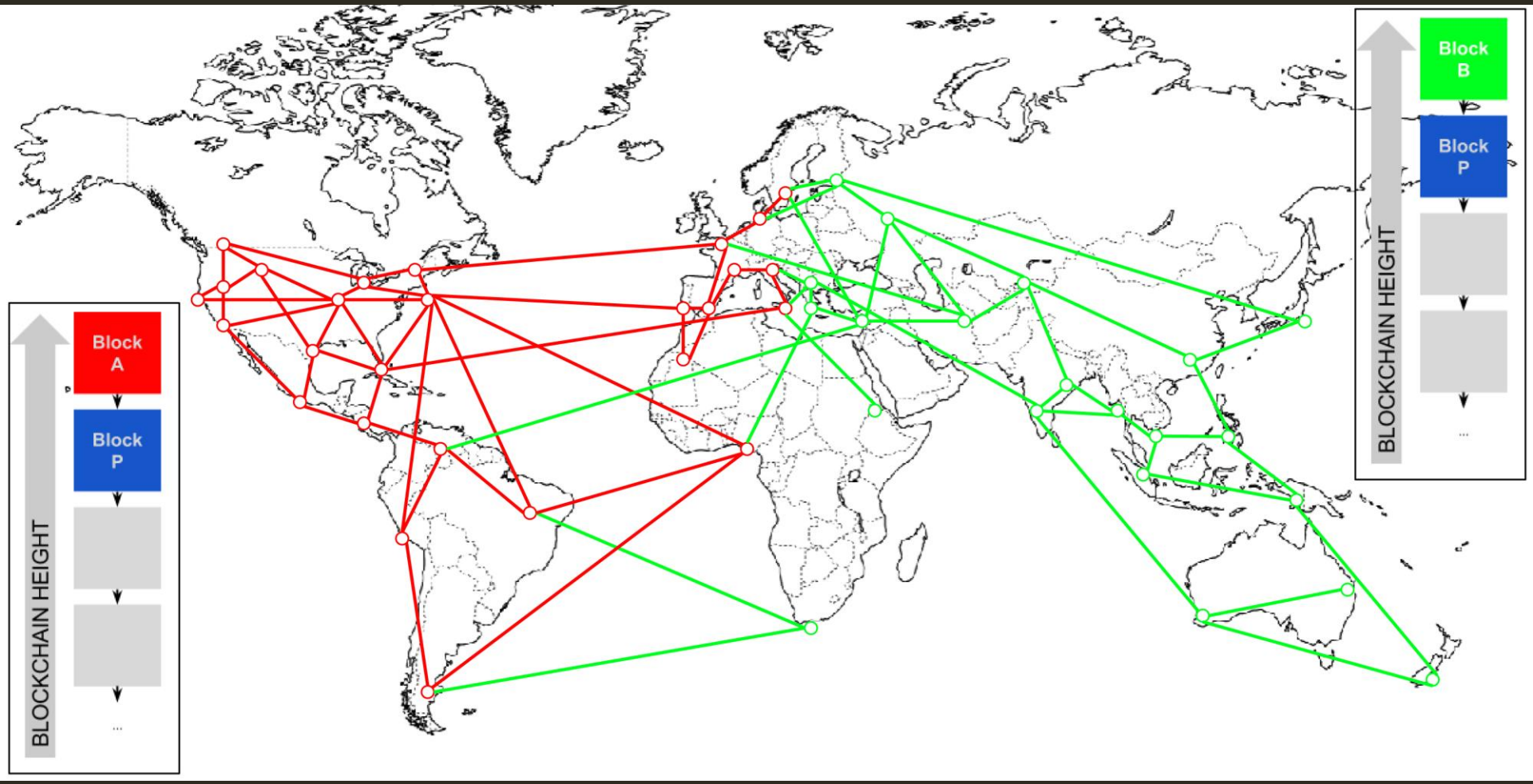
信息正确 → 加到区块链，再广播出去

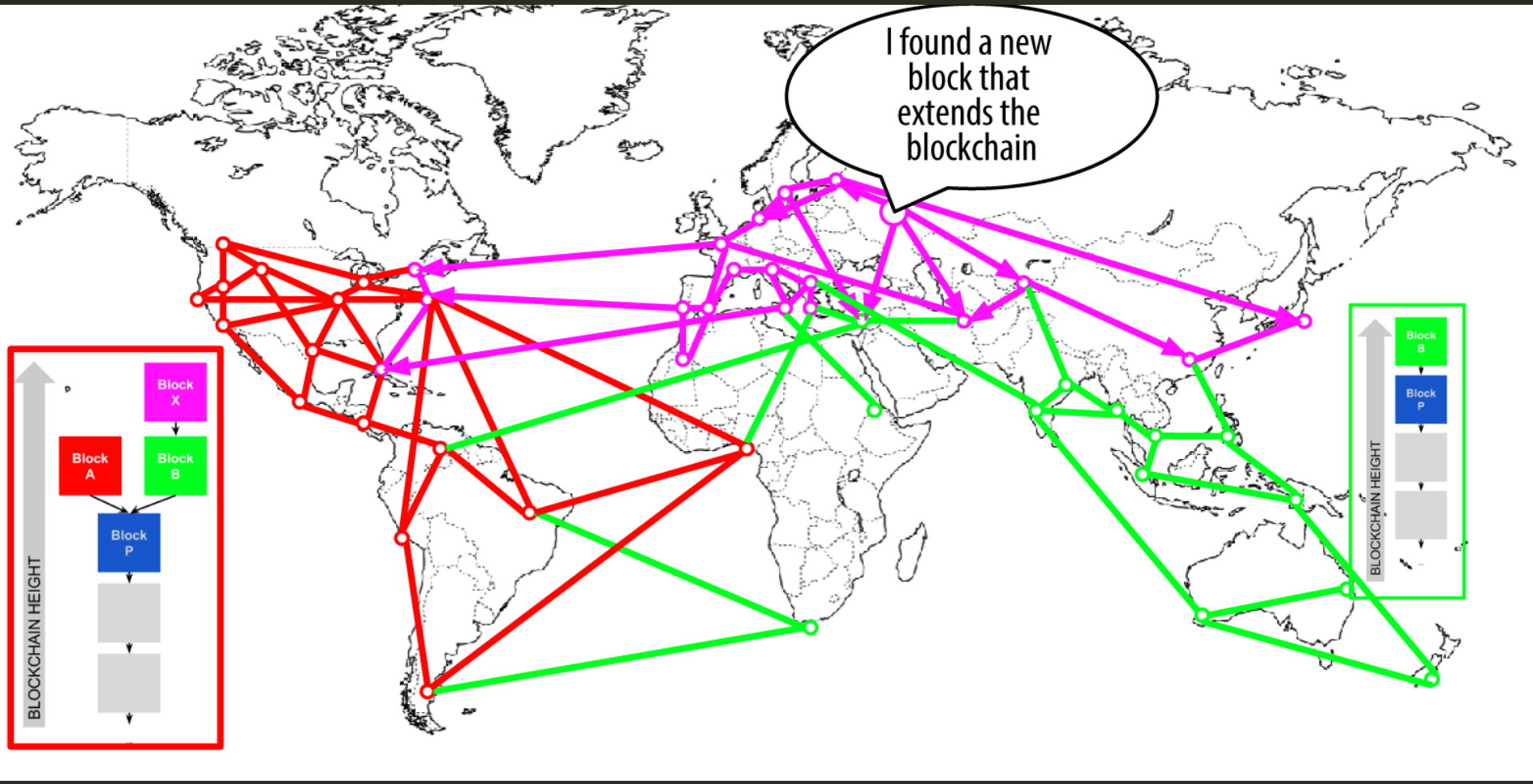
长的最高的区块链就算”公认”的状态

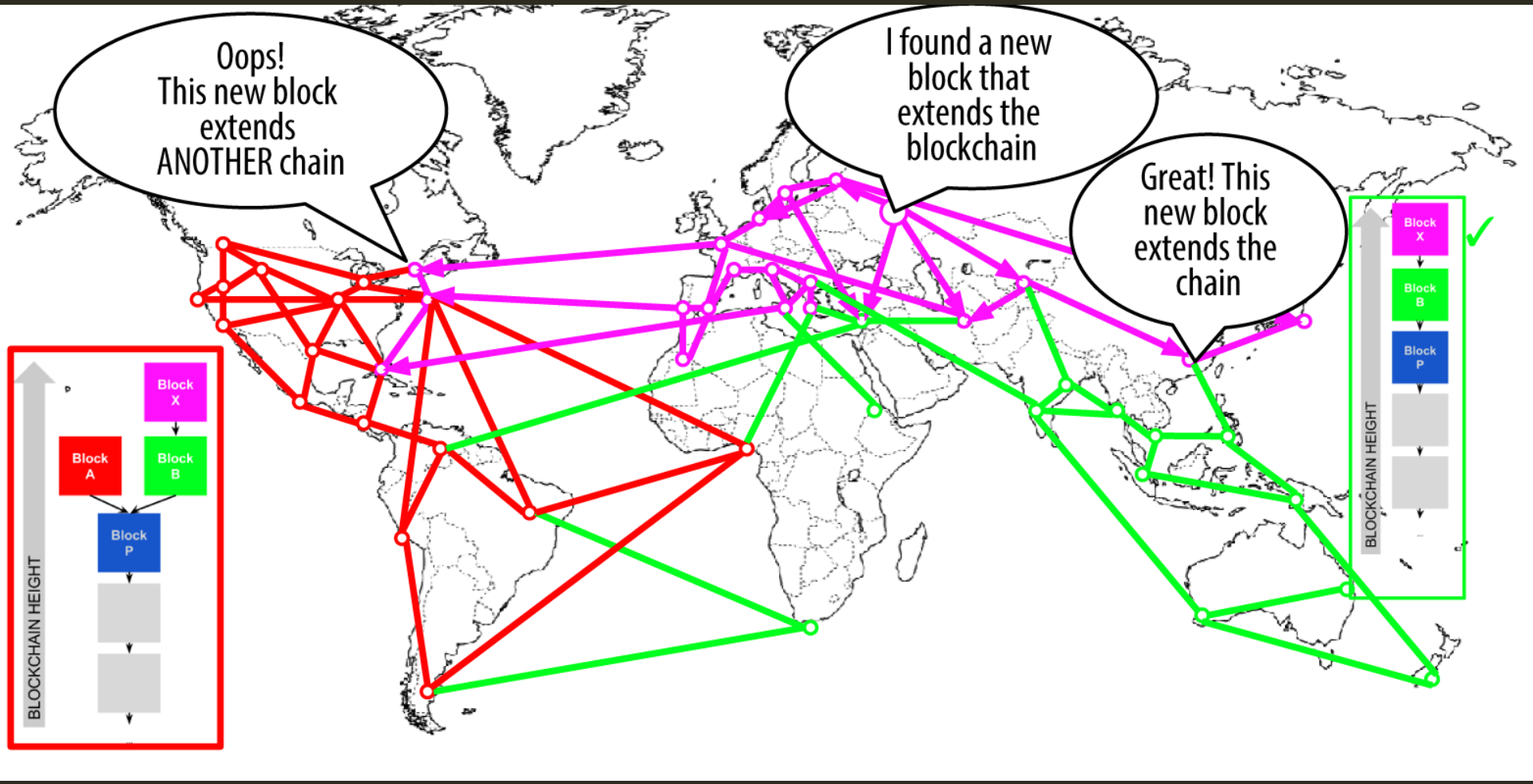
BLOCKCHAIN分岐


BLOCKCHAIN HEIGHT
Block P
...


I found a block extending the blockchain
I found a block extending the blockchain


BLOCKCHAIN HEIGHT
Block A
Block P
...
BLOCKCHAIN HEIGHT
Block B
Block P
...


I found a new block that extends the blockchain
Block X
Block A
Block B
Block P
BLOCKCHAIN HEIGHT
Block B
Block P
BLOCKCHAIN HEIGHT


Oops!
This new block
extends
ANOTHER chain
I found a new
block that
extends the
blockchain
Great! This
new block
extends the
chain
Block
X
Block
A
Block
B
Block
P
BLOCKCHAIN HEIGHT
Block
X
Block
B
Block
P
BLOCKCHAIN HEIGHT

BITCOIN=就是那一套规则

>50%节点认为对的就是对

出Bug时、改规则 – 需要>50%节点升级 (Hard Fork)

Bitcoin 2013年3月

- v0.7版不能应对某交易，v0.8可以
- 两个版本使用节点相当 (按挖矿能力计)
- 区块链变成有两个头，维持了几小时
- 大矿池(后面提及)共识回滚到0.7，重新达成一种共识
  0.8那头直接算没法生过。

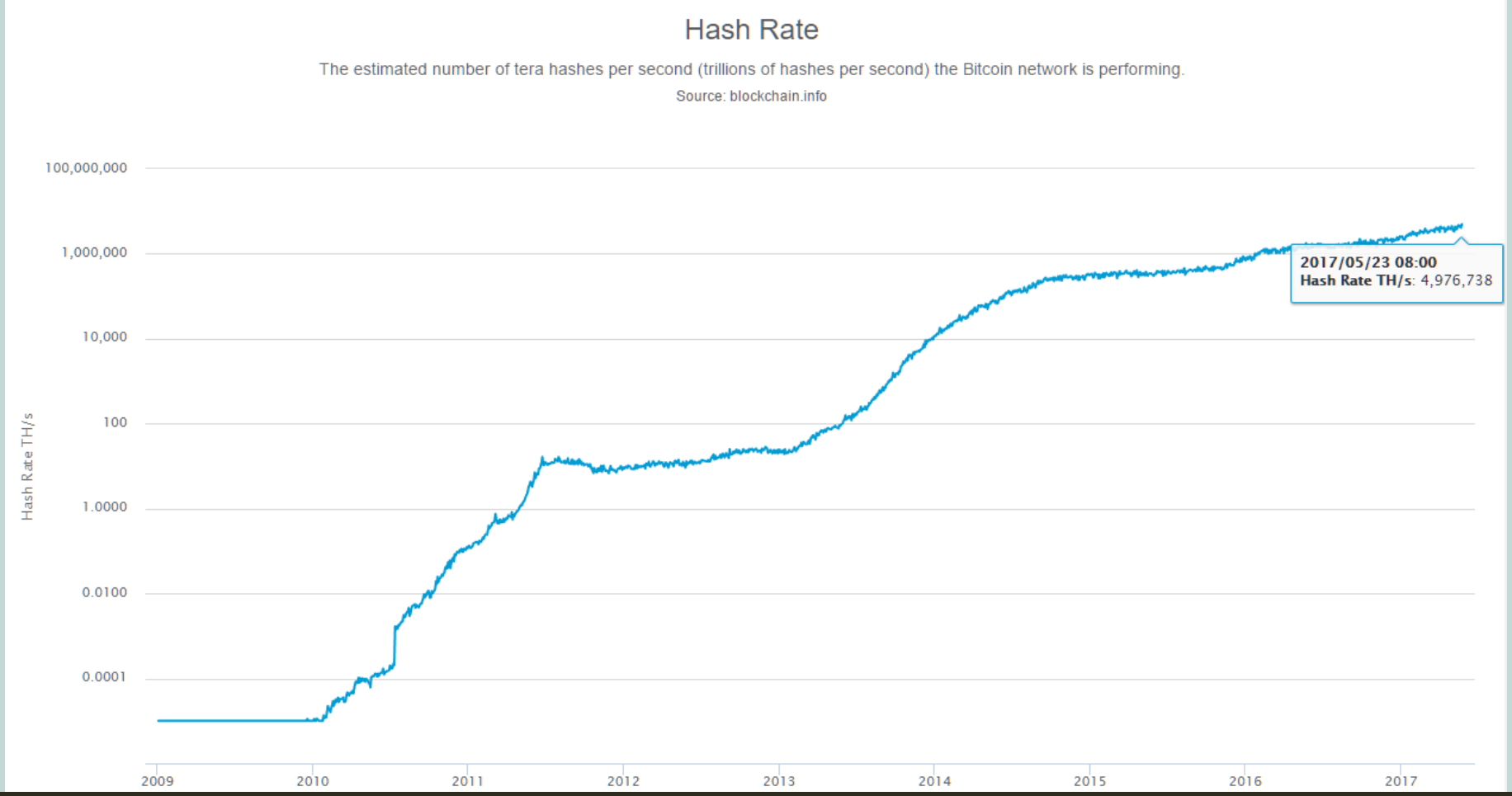
Ethereum 以太坊 2016年6月

- 有bug，被hack
- 现在变成两种货币 (Ethereum Classic和Ethereum)

怎么得到BTC？

交易所买卖

存入法币，买卖贵金属、股票一样


Hash Rate
The estimated number of tera hashes per second (trillions of hashes per second) the Bitcoin network is performing.
Source: blockchain.info
Hash Rate TH/s
100,000,000
1,000,000
10,000
100
1.0000
0.0100
0.0001
2009
2010
2011
2012
2013
2014
2015
2016
2017
2017/05/23 08:00
Hash Rate TH/s: 4,976,738

挖矿速度

挖矿池
MINING POOL

一起挖，中奖后按各人运算速度分成

公私钥加密

产生两组很特别的数字

- 公钥(Public Key)是公开给人的一组
- 私钥(Private Key)是自己保存的一组

用法

- 内容X → 用公钥加密 → 内容Y → 用私钥解密 → 内容X
- 内容X → 用私钥加密 → 内容Z → 用公钥解密 → 内容X

签名

- 原始数据的哈希 → 用私钥加密 → 得出内容Signature，即签名
- 签名 → 通过公钥解密，和原始数据的哈希比较是否一样
- 不用透露私钥但能向外证明我拥有私钥

交易 TRANSACTION (TX)

生成新钱包
公钥: 6274cd 私钥: 86a022
公钥哈希后: fe1883

TX 1

输入:
从...5BTC

输出:
5BTC给fe1883

签名:
...

TX 2

输入:
从这里的5BTC

输出:
1BTC给fe1883
4BTC给60ad38

签名:
哈希(公钥6274cd)就是fe1883
上面所有信息的签名是ab5663

输入:
从这里的1BTC

输出:
4BTC给...

签名:
我的公钥哈希
就是60ad38
签名是...

哈希(输入:从这里的5BTC
输出:1BTC给fe18834,BTC给60ad38)
→ 私钥86a022 = 签名ab5663

ab5663 → 公钥6274cd解密 等于
哈希(输入:从这里的5BTC
输出:1BTC给fe18834,BTC给60ad38)

意即我真拥有86a022

进行交易

1. 签好名，把TX广播出去
2. 祈求挖矿者把TX放到他们在挖的区块中
   - 提供交易费作诱因...，通常是0.001BTC
   - 所以挖矿者会希望包含更多TX到区块中

PAY TO SCRIPT HASH (P2SH) & SMART CONTRACT

生成新钱包
公钥: 6274cd 私钥: 86a022
脚本: *签名*是由6274cd所签的
公钥6274cd和脚本哈希后: fe1883

TX 1

输入:
从...5BTC

输出:
5BTC给fe1883

签名:
...

TX 2

输入:
从这里的5BTC
脚本:*签名*是6274cd所签的
输出:
1BTC给fe1883
4BTC给60ad38
签名:
哈希(公钥6274cd+脚本)就是fe1883
上面所有信息的签名是ab5663
欢迎运行脚本看看是不是True

比特币特性

无人监管
- 要>50%节点达成共识，非一人可控制

发行量固定且可预知
- 由规则控制，规则是>50%节点的共识

账目公开
- 区块链

钱包匿名
- 公私钥随意生成

ALT-COIN (其他货币)

Litecoin (2011年)

- 采用scrypt而非sha256作为pow
- 2.5分钟一个block

还有不下几十种，有各种参数，但大同小异

Ethereum 以太坊

- 脚本语言是Turning Complete的，使POW不只是费电而是演算东西

Q & A